

LANDTAG  
NORDRHEIN-WESTFALEN  
10. WAHLPERIODE

VORLAGE

10/410 A-1



**Der Landesbeauftragte  
für den Datenschutz  
Nordrhein-Westfalen**

## **7. Tätigkeitsbericht**

4 10 ~~11~~ - 2

Siebter Tätigkeitsbericht  
des Landesbeauftragten für den Datenschutz  
Nordrhein-Westfalen

für die Zeit vom 1. April 1985  
bis zum 31. März 1986

4.16.11.3

Herausgeber: Der Landesbeauftragte  
für den Datenschutz Nordrhein-Westfalen  
Elisabethstraße 12, 4000 Düsseldorf 1  
ISSN 0179-2431  
Druck: Rheindruck Düsseldorf GmbH

# Gliederung

410/11-34

<b>A. Aufgaben des Landesbeauftragten für den Datenschutz</b> . . . . .	7
1. Überblick . . . . .	7
2. Umfang der Datenverarbeitung . . . . .	8
3. Kontrolle der Einhaltung der Datenschutzvorschriften . . . . .	8
4. Zusammenarbeit mit anderen Datenschutzkontrollinstanzen . . . . .	9
a) Datenschutzbeauftragte . . . . .	9
b) Aufsichtsbehörden für den nicht-öffentlichen Bereich . . . . .	10
5. Personal . . . . .	10
<b>B. Grundrecht auf Datenschutz und Recht auf informationelle Selbstbestimmung</b> . . . . .	11
<b>C. Datenschutz in den Bereichen der Verwaltung</b> . . . . .	13
1. Meldewesen . . . . .	13
a) Datenspeicherung . . . . .	13
b) Kombination gespeicherter Daten . . . . .	13
c) Datenübermittlung an nicht-öffentliche Stellen . . . . .	14
d) Lohnsteuerkarten . . . . .	16
e) Übertragung anderer Aufgaben . . . . .	16
2. Wahlen . . . . .	17
3. Paß- und Personalausweiswesen . . . . .	19
4. Personenstandswesen . . . . .	19
5. Ausländerwesen . . . . .	19
6. Kommunalwesen . . . . .	21
7. Polizei . . . . .	25
a) Gesetzliche Regelung der Informationsverarbeitung . . . . .	25
b) Datenerhebung . . . . .	25
c) Datenspeicherung . . . . .	27
d) Auskunft und Löschung . . . . .	28
e) Polizeibeamte als Zeugen . . . . .	28
8. Verfassungsschutz . . . . .	29
a) Anforderungen an Datenschutzregelungen . . . . .	29
b) Bundesverfassungsschutzgesetz und Zusammenarbeitsgesetz . . . . .	33
c) Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen . . . . .	33
d) Auskunft und Löschung . . . . .	35

L 10 11 - 5

<b>9. Bauwesen</b>	35
<b>10. Rechtswesen</b>	36
a) Strafsachen	36
b) Ordnungswidrigkeitenverfahren	38
c) Zivilsachen	38
d) Strafvollzug	40
<b>11. Sozialwesen</b>	47
a) Sozialversicherung	47
b) Kriegsopferversorgung	53
c) Sozialhilfe	54
d) Jugendhilfe	62
e) Wohngeld	66
f) Ausbildungsförderung	68
<b>12. Gesundheitswesen</b>	68
a) Krankenhäuser	68
b) Medizinische Forschung	73
c) Gesundheitsämter	76
d) Berufskammern	78
<b>13. Personalwesen</b>	83
a) Feststellung der Eignung	83
b) Personalakten	84
c) Beihilfen	86
d) Hausarbeitstag	86
e) Telefongespräche	87
f) Lehrerdaten	89
g) Datenweitergabe innerhalb einer Stelle	89
h) Datenweitergabe an öffentliche Stellen	91
i) Datenweitergabe an nicht-öffentliche Stellen	95
k) Dienstaussweis	98
<b>14. Statistik</b>	98
a) Volkszählung	98
b) Mikrozensus	99
c) Handels- und Gaststättenzählung	99
d) Hochschulstatistik	102
e) Kommunalstatistik	103
<b>15. Wissenschaft und Forschung</b>	105
a) Hochschulen	105
b) Studienplatzvergabe	108
<b>16. Bildung und Kultur</b>	109
a) Schulwesen	109
b) Bibliotheken	119
c) Archive	120
<b>17. Finanzwesen</b>	121
a) Steuerverwaltung	121
b) Kommunales Finanzwesen	123
<b>18. Wirtschaft</b>	125
a) Bezirksschornsteinfegermeister	125
b) Industrie- und Handelskammern	127
c) Handwerkskammern und Innungen	129

<b>19. Verkehrswesen</b>	131
a) Fahrerlaubnis	131
b) Kraftfahrzeugzulassung	135
c) Personenbeförderung	136
<b>20. Umweltschutz</b>	139
<b>21. Öffentliche Unternehmen</b>	141
a) Kreditinstitute	141
b) Versicherungsunternehmen	144
<b>22. Ordensangelegenheiten</b>	145
<b>23. Medien</b>	146
a) Entwurf eines Landesrundfunkgesetzes	146
b) Fernwirken	147
<b>D. Organisatorische und technische Maßnahmen</b>	148
<b>1. Maßnahmen der Strukturorganisation</b>	148
a) Zuordnen und Abgrenzen von Funktionen	148
b) Freigabe von Anwendungsprogrammen	151
<b>2. Maßnahmen der Ablauforganisation</b>	153
a) Sicherheit der Daten	153
b) Sicherung der Arbeitsdurchführung	155
<b>3. Technische Maßnahmen</b>	156
a) Schutz der Vertraulichkeit am Kassenschalter	156
b) Sicherheitsbereich	157
<b>4. Organisatorisch-technische Maßnahmen</b>	159
a) Beeinträchtigung der Datensicherheit bei Einsatz des Schnittstellenvervielfachers SK 12 der Deutschen Bundespost	159
b) Datensicherung bei On-line-Zugriff	162
c) Datensicherung bei Dateien	165
<b>5. Datensicherung bei Einsatz kleinerer Datenverarbeitungsanlagen</b>	166
a) Abgrenzung des Themas	166
b) Besonderheiten der Datensicherung beim Einsatz kleinerer Datenverarbeitungsanlagen	168
c) Sicherheit der Programme	170
d) Sicherheit der Daten	178
e) Sicherheit bei Ausnahmesituationen	181
f) Organisation und Kontrolle	182
g) Zusammenfassung	187
<b>6. Organisationshilfe zur Datensicherung</b>	187
<b>E. Weiterentwicklung des Datenschutzrechts</b>	189
<b>1. Novellierung des Bundesdatenschutzgesetzes</b>	189
<b>2. Novellierung des Datenschutzgesetzes Nordrhein-Westfalen</b>	189

# A. Aufgaben des Landesbeauftragten für den Datenschutz

## 1. Überblick

Die Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts bestimmten auch im Berichtsjahr die Datenschutzdiskussion. Zahlreiche Gesetzgebungsvorhaben auf Bundes- und Landesebene zeigen das Bemühen, notwendige Folgerungen aus dem Grundrecht auf informationelle Selbstbestimmung zu ziehen. In vielen Bereichen wird damit langjährigen Forderungen der Datenschutzbeauftragten Rechnung getragen. Bei manchen der bekanntgewordenen Vorschläge erscheint allerdings zweifelhaft, ob sie für den Bürger mehr Datenschutz bringen.

Die bei Inkrafttreten der Datenschutzgesetze von vielen gehegte Erwartung, irgendwann könnten alle Datenschutzprobleme abschließend geklärt sein, hat sich nicht erfüllt. So wird auch in diesem Bericht wiederum eine Fülle von neuen Problemen behandelt, die in den Jahren zuvor noch nicht erkannt worden waren. Der rasche, durch den technischen Fortschritt bedingte Wandel in der Datenverarbeitung und eine zunehmende Sensibilität der Bürger lassen einen Abschluß dieser Entwicklung in naher Zukunft nicht erwarten.

Andererseits ist Datenschutz etwas Alltägliches geworden. Er hat damit an Bedeutung noch gewonnen. Wie die Vielzahl von Eingaben wiederum zeigt, werden sich die Bürger ihrer Datenschutzrechte in immer stärkerem Maße bewußt. Gleichzeitig ist aber auch die Sensibilität der Verwaltung für die Wahrung der Datenschutzbelange gestiegen. Es wird immer selbstverständlicher, bei Verwaltungsentscheidungen Datenschutzgesichtspunkte zu berücksichtigen. Allerdings lassen die Ergebnisse häufig noch Mängel bei der Verwirklichung des Rechts auf informationelle Selbstbestimmung und des Grundrechts auf Datenschutz erkennen. Mit meinen Tätigkeitsberichten soll deshalb auch langfristige Überzeugungsarbeit geleistet werden.

Schwerpunkte meiner Tätigkeit im Berichtsjahr lagen in den Bereichen Sozialleistungen, Gesundheitswesen, Personalwesen, Schulen, Verkehr und Strafvollzug. Im Bereich der organisatorischen und technischen Maßnahmen wird erneut auf die besonderen Schwierigkeiten der Datensicherung bei der Durchführung von Verwaltungsaufgaben mit Hilfe kleinerer Datenverarbeitungsanlagen eingegangen. Prüfungen ergaben, daß öffentliche Stellen, die kleinere Datenverarbeitungsanlagen einsetzen, mit den heute zur Verfügung stehenden Mitteln im allgemeinen nicht in der Lage sind, die Datensicherung hinreichend zu gewährleisten.

Schwerwiegende Verstöße gegen den Datenschutz als „Datenschutzskandale“ zu klassifizieren, habe ich bislang und auch im vorliegenden Bericht bewußt vermieden. Eine derartige Etikettierung ist der Sache des Datenschutzes letztlich nicht dienlich. Es wäre jedoch verfehlt, hieraus den Schluß zu ziehen, daß es schwere Verstöße gegen den Datenschutz nicht gegeben habe.

Richtig ist allerdings, daß in einem Rechtsstaat ein bewußt rechtswidriges Vorgehen öffentlicher Stellen nur selten sein dürfte. Um so notwendiger im Sinne eines vom Bundesverfassungsgericht geforderten vorgezogenen Rechtsschutzes ist ein unabhängiges externes Kontrollorgan gerade für die Vielzahl der Datenschutzverstöße, bei denen die Verwaltung ihr Verhalten in Verkenntung der Rechtslage für zulässig hält.

## 2. Umfang der Datenverarbeitung

Einen Überblick über den Umfang der Datenverarbeitung in Dateien im Land Nordrhein-Westfalen gibt das vom Landesbeauftragten für den Datenschutz nach § 27 DSG NW geführte **Dateienregister**. Die Zahl der speichernden Stellen, die Dateien zu diesem Register angemeldet haben, hat sich auf 2997 erhöht. Insgesamt sind 22916 Dateien angemeldet worden. Dennoch sind immer noch nicht alle speichernden Stellen ihrer gesetzlichen Anmeldepflicht nachgekommen.

Von den bisher vorliegenden Anmeldungen entfallen auf

- das allgemeine Register nach § 27 Abs. 1 und 2 DSG NW 18253 Dateien.
- das gesonderte Register nach § 27 Abs. 4 Satz 2 DSG NW für Staatsanwaltschaft, Polizei sowie bestimmte Dateien der Landesfinanzbehörden 1835 Dateien,
- das gesonderte Register nach § 27 Abs. 5 DSG NW für Eigenbetriebe und öffentlich-rechtliche Unternehmen 2828 Dateien.

Die nicht-automatisiert geführten Dateien, deren Daten nicht zur Übermittlung an Dritte bestimmt sind (§ 1 Abs. 2 Satz 3 DSG NW), sind in diesen Zahlen nicht enthalten, da sie nicht der Anmeldepflicht unterliegen. Das gleiche gilt für alle Datensammlungen, die keine Dateien (§ 2 Abs. 3 Nr. 3 DSG NW) sind.

Wiederholt haben Gemeinden angefragt, welche Stelle für die in den Schulen für Zwecke der inneren Schulangelegenheiten geführten Dateien als speichernde Stelle nach § 2 Abs. 3 Nr. 1 DSG NW anzusehen ist und die Anmeldung zum Dateienregister nach § 27 Abs. 3 DSG NW vorzunehmen hat. Unter Berücksichtigung des Rechtscharakters der öffentlichen Schulen als nichtrechtsfähige öffentliche Anstalt des Schulträgers sind der Kultusminister und der Innenminister der Auffassung, daß für die in den Schulen geführten Dateien die jeweilige Gemeinde/Gemeindeverband speichernde Stelle im Sinne von § 1 Abs. 2 Satz 1 in Verbindung mit § 2 Abs. 3 Nr. 1 DSG NW ist. Diese Auffassung wird von mir geteilt (unten C.16.a).

In meinem sechsten Tätigkeitsbericht (A.2.c) habe ich mich zu der Frage der Anmeldepflicht für Datensammlungen der Notare geäußert. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit dieser Frage befaßt. Die Datenschutzbeauftragten vertreten übereinstimmend die Auffassung, daß die Notare als Träger eines öffentlichen Amtes öffentliche Stellen sind und deshalb in vollem Umfang den Bestimmungen der Datenschutzgesetze unterliegen. Die Verpflichtung zur Verschwiegenheit (§ 18 der Bundesnotarordnung) schließt die Geltung der Datenschutzgesetze nicht aus. Soweit die Datenschutzgesetze dies vorsehen, sind die Notare verpflichtet, die von ihnen geführten automatisierten und manuellen Dateien zu den von den Datenschutzbeauftragten geführten Dateienregistern anzumelden.

## 3. Kontrolle der Einhaltung der Datenschutzvorschriften

Bei meiner Kontrolltätigkeit sind im Berichtsjahr wiederum zahlreiche Verstöße gegen Datenschutzvorschriften offenbar geworden (vgl. unten C. und D.). Zum weitaus überwiegenden Teil habe ich mich zur Durchsetzung meiner Vorstellungen auf **Empfehlungen** nach § 26 Abs. 2 DSG NW beschränken können. Meinen Empfehlungen ist weitgehend gefolgt worden.

In sieben Fällen hielt ich es wegen der Bedeutung der Angelegenheit, der Schwere des Verstoßes oder der datenschutzrechtlichen Beurteilung durch die datenverarbeitende Stelle für notwendig, eine förmliche **Beanstandung** nach

§ 30 DSGVO auszusprechen. In einer Reihe von Fällen konnte ich hiervon nur im Hinblick auf die aufgeschlossene Haltung der Verantwortlichen und die besonderen Umstände des Einzelfalles, die eine Wiederholung der Verstöße nicht befürchten ließen, absehen.

Anlaß für die förmlichen Beanstandungen war:

- die Erteilung von Auszügen aus dem Wählerverzeichnis über die seit einem bestimmten Zeitpunkt zugezogenen Bürger an Parteien bei der Landtagswahl 1985,
- die Verletzung des Sozialgeheimnisses durch die Weitergabe einer Jugendamtsakte an eine Sonderkommission der Kriminalpolizei und an die Staatsanwaltschaft,
- das weitere Aufbewahren von Unterlagen über lange zurückliegende strafgerichtliche Verurteilungen in einer Ausländerakte,
- die Verwendung der zu Zwecken der Verwaltung von Darlehen nach dem Honnefer Modell verfügbaren Daten von Hochschulabsolventen für Spendenappelle zugunsten eines Härtefonds,
- die Zusammenfassung von Unterstützungsunterschriften in Listen, deren Weitergabe an die Beisitzer des Wahlausschusses sowie das Belassen der Listen der Unterstützungsunterschriften bei den Beisitzern nach der Sitzung des Wahlausschusses,
- die erkennungsdienstliche Behandlung eines strafunmündigen Kindes sowie die weitere Aufbewahrung der dabei gefertigten Unterlagen,
- die Weitergabe von Personaldaten eines Bewerbers um einen Ausbildungsplatz innerhalb einer Stadtparkasse zu Werbezwecken.

Von der Möglichkeit, mich nach § 31 Abs. 3 DSGVO an den **Landtag** zu wenden, habe ich in drei Fällen Gebrauch gemacht:

- Vorlage 10/114 zum Entwurf eines Gesetzes zur Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen,
- Vorlage 10/221 zur Personalausstattung meiner Dienststelle anlässlich der Beratung des Haushaltsplans 1986 durch den Haushalts- und Finanzausschuß und den Ausschuß für innere Verwaltung,
- Vorlage 10/279 zum Entwurf eines Gesetzes über den Verdienstorden des Landes Nordrhein-Westfalen.

Ferner habe ich auf Wunsch des Ausschusses für Innere Verwaltung zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts auf die Kommunalstatistik Stellung genommen (Vorlage 10/132).

#### 4. Zusammenarbeit mit anderen Datenschutzkontrollinstanzen

##### a) Datenschutzbeauftragte

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Berichtszeitraum fünfmal getagt. In den Sitzungen im Mai, September und November 1985 sowie im Januar und März 1986 wurden unter anderem folgende Themen behandelt:

- Perinatologische Basiserhebung,
- Handels- und Gaststättenzählung 1985,

- Datenschutzregelungen für den Verfassungsschutz,
- Speicherung personengebundener Hinweise im INPOL-System,
- Novellierung des Bundesdatenschutzgesetzes,
- Personalausweisgesetz, Paßgesetz, Bundesverfassungsschutzgesetz, MAD-Gesetz, Zusammenarbeitsgesetz, Straßenverkehrsgesetz,
- Datenschutz im Krankenhaus.

#### **b) Aufsichtsbehörden für den nicht-öffentlichen Bereich**

Bereichsübergreifende Datenschutzfragen im Kreditwesen und in der Versicherungswirtschaft erforderten die weitere Mitarbeit in den Arbeitsgruppen „Bankauskunftsverfahren/Schufa“ sowie „Versicherungswirtschaft“ des „Düsseldorfer Kreises“ der Datenschutzreferenten der obersten Landesbehörden der Bundesländer (unten C.21.a und b).

## **5. Personal**

Nach § 25 Abs. 1 DSG NW ist dem Landesbeauftragten für den Datenschutz die für die Erfüllung seiner Aufgaben notwendige Personalausstattung zur Verfügung zu stellen. Seit dem Haushaltsjahr 1981 habe ich mich um zwei zusätzliche Planstellen des höheren Dienstes und eine Stelle der Vergütungsgruppe Ib/IIa BAT bemüht. Da diese Stellenanforderung auch im Entwurf des Haushaltsplans 1986 wiederum unberücksichtigt geblieben war, habe ich von der Möglichkeit des § 31 Abs. 3 DSG NW Gebrauch gemacht und mich anlässlich der Beratung des Haushaltsplans durch den Haushalts- und Finanzausschuß und den Ausschuß für Innere Verwaltung an den Landtag gewandt (Vorlage 10/221). Im Hinblick auf die Finanzlage des Landes habe ich dabei die Anforderung einer Stelle der Vergütungsgruppe Ib/IIa BAT für das Haushaltsjahr 1986 zurückgestellt.

Der Landtag ist meinen Vorstellungen gefolgt und hat zusätzlich zwei Planstellen des höheren Dienstes bewilligt. Demgegenüber sind zwei Planstellen des gehobenen Dienstes weggefallen, so daß sich die Gesamtzahl der Planstellen des Kapitels 03 630 gegenüber dem Haushaltsjahr 1985 nicht erhöht hat.

## B. Grundrecht auf Datenschutz und Recht auf informationelle Selbstbestimmung

- In ihrer Mitteilung zur Initiative zur Verbesserung des Datenschutzes in Nordrhein-Westfalen (Drucksache 9/3721, S. 8–9) hatte die Landesregierung die Ansicht vertreten, daß Eingriffe in das Recht auf informationelle Selbstbestimmung von sonstigen, nicht grundrechtsrelevanten Arten des Umgangs mit personenbezogenen Daten abzugrenzen seien. Sie ging somit davon aus, daß nicht jeder Umgang öffentlicher Stellen mit solchen Daten einen Informationseingriff darstellt. Inzwischen hat sich die Landesregierung offenbar der von mir vertretenen Auffassung angeschlossen, daß jeder Umgang der Verwaltung mit personenbezogenen Daten als Eingriff in dieses Grundrecht zu werten ist. Ich entnehme dies der allgemeinen Begründung zu dem Gesetzesantrag der Länder Bremen, Hamburg, Hessen, Nordrhein-Westfalen und Saarland für ein neues Bundesdatenschutzgesetz (Bundratsdrucksache 121/86, S. 52).
- Im Berichtsjahr hat sich die Rechtsprechung in verstärktem Maße mit den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts auseinandergesetzt. So hat der Bayerische Verfassungsgerichtshof in einer Entscheidung vom 9. Juli 1985 (NJW 1986, 915) unter Bezugnahme auf dieses Urteil die Auffassung vertreten, daß es für die Führung von Kriminalakten durch die Polizei derzeit an einer hinreichend bestimmten gesetzlichen Grundlage fehlt; der polizeilichen Generalklausel könnten Maßstäbe für Gegenstand, Ausmaß und Begrenzung zulässiger Aktensammlungen für polizeiliche Zwecke nicht mit der gebotenen Klarheit entnommen werden. Der Verfassungsgerichtshof hat allerdings in Anlehnung an die Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 33, 12; 41, 267; 51, 290) der Polizei eine Übergangszeit eingeräumt, innerhalb deren eine Regelungslücke hingenommen werden müsse, um dem Gesetzgeber ausreichend Zeit für die Beratung und den Erlaß der erforderlichen Vorschriften zu lassen. Dies sei notwendig, weil im Fall einer Vernichtung derartiger Unterlagen vor einem Tätigwerden des Gesetzgebers eine Funktionsunfähigkeit staatlicher Einrichtungen entstehen könnte, die der verfassungsmäßigen Ordnung noch ferne stünde als der bisherige, gesetzlich unzureichend geregelte Zustand. Während der Übergangszeit seien staatliche Eingriffe allerdings auf das unerläßliche Maß zu beschränken.

In einem ähnlichen Fall hat das Verwaltungsgericht Frankfurt mit Urteil vom 19. März 1985 (DVR 1985, 234) einen Übergangsbonus verneint. Das Gericht ist der Auffassung, daß die Aufbewahrung von erkennungsdienstlichen Unterlagen zu präventiv-polizeilichen Zwecken gegen das Recht auf informationelle Selbstbestimmung verstoße, da die als gesetzliche Grundlage herangezogene 2. Alternative des § 81 b StPO den Anforderungen an eine hinreichend konkretisierte Eingriffsbefugnis nicht genüge und die polizeiliche Generalklausel wegen Fehlens der danach erforderlichen konkreten Gefahr nicht in Betracht komme. Eine Befugnis der einfachen Gerichte zur zeitweiligen Hinnahme eines Verfassungsverstoßes sei nicht erkennbar; ein derartiges Vorgehen sei mit der Bindung der Rechtsprechung an Gesetz und Recht (Artikei 20 Abs. 3 des Grundgesetzes) schwerlich vereinbar.

Die Vereinbarkeit des Auskunftsverweigerungsrechts der Sicherheitsbehörden (vgl. § 16 Abs. 2 in Verbindung mit § 15 Abs. 2 Nr. 1 DSGVO) mit dem

Recht auf informationelle Selbstbestimmung wird von den Gerichten unterschiedlich beurteilt. Der Verwaltungsgerichtshof München sieht in der Regelung für den Verfassungsschutz eine von dem Einzelnen im überwiegenden Allgemeininteresse hinzunehmende Einschränkung dieses Grundrechts (Beschluß vom 15. Mai 1985, NVwZ 1985, 663). Das Verwaltungsgericht Wiesbaden hält bei einem Auskunftsantrag an das Bundeskriminalamt eine verfassungskonforme, das Recht auf informationelle Selbstbestimmung berücksichtigende Anwendung für geboten (Urteil vom 24. Januar 1984, DVR 1985, 147). Das Oberverwaltungsgericht Berlin sieht unter Hinweis auf die Rechtsprechung des Bundesverfassungsgerichts die Regelung für die Auskunftserteilung durch die Polizei in Verwaltungsvorschriften (den KpS-Richtlinien) für eine Übergangszeit noch als ausreichend an (Urteil vom 31. Juli 1985 – 1 B 45.83 –). Das Verwaltungsgericht Frankfurt leitet einen Auskunftsanspruch unmittelbar aus dem Recht auf freie Entfaltung der Persönlichkeit in Verbindung mit der Rechtsweggarantie nach Artikel 19 Abs. 4 Satz 1 des Grundgesetzes her, wenn vom Landeskriminalamt personenbezogene Daten zur vorbeugenden Verbrechensbekämpfung nach Auffassung des Gerichts ohne Rechtsgrundlage gesammelt, aufbewahrt und weitergegeben werden und nicht ausgeschlossen werden kann, daß der die Auskunft begehrende Bürger davon betroffen ist (Urteil vom 17. Juli 1984, DVR 1985, 273). Das Verwaltungsgericht Schleswig schließlich ist der Auffassung, daß das Auskunftsverweigerungsrecht der Verfassungsschutzbehörde gegen die Rechtsweggarantie des Artikels 19 Abs. 4 Satz 1 des Grundgesetzes verstoße, weil die Regelung einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung darstelle, ohne eine effiziente, einzelfallbezogene Nachprüfung der Rechtmäßigkeit der Auskunftsverweigerung zu ermöglichen. Das Gericht hat deshalb die Sache dem Bundesverfassungsgericht vorgelegt (Beschluß vom 21. Januar 1986 – 3 A 1/85 –).

Auch in anderen Fällen haben Gerichte Folgerungen aus dem Recht auf informationelle Selbstbestimmung gezogen. So hat das Sozialgericht Hildesheim entschieden, daß die Bundesanstalt für Arbeit verpflichtet sei, die interne Offenbarung von ärztlichen und psychologischen Gutachten auf das erforderliche Maß zu begrenzen, da das Recht auf informationelle Selbstbestimmung nur nach dem Grundsatz der Verhältnismäßigkeit beschränkt werden dürfe. Für die Arbeit der Vermittlungs- und der Leistungsabteilung reiche es aus, wenn die abschließende Leistungsbeurteilung des Arztes oder Psychologen vorliege. Die übrigen Teile des Gutachtens (insbesondere soweit sie Angaben über die Diagnose enthalten) seien beim ärztlichen bzw. psychologischen Dienst zu verwahren (Beschluß vom 6. Mai 1985 – S 3 Ar 269/84 –).

Nach Auffassung des Oberlandesgerichts Hamburg folgt aus dem Volkszählungsurteil des Bundesverfassungsgerichts, daß Angaben, die ein Asylbewerber im Rahmen seiner Anhörung über die Einreisemodalitäten macht, nur dann an die Staatsanwaltschaft weitergeleitet werden dürfen, wenn eine Strafverfolgung im überwiegenden öffentlichen Interesse liegt; anderenfalls bestehe hinsichtlich dieser Angaben ein Verwertungsverbot. Das Gericht hält insoweit eine entsprechende Anwendung der Regelung für Steuerdaten (§ 30 Abs. 4 Nr. 5, § 393 Abs. 2 AO) für geboten (Urteil vom 17. Juli 1985, NJW 1985, 2541).

Auch im privatrechtlichen Bereich wird das Recht auf informationelle Selbstbestimmung herangezogen. So stützt das Bundesarbeitsgericht den Anspruch eines erfolglosen Bewerbers auf Vernichtung des von ihm ausgefüllten Personalfragebogens auch auf das Recht auf informationelle Selbstbestimmung (Urteil vom 6. Juni 1984 – 5 AZR 286/81 –).

## C. Datenschutz in den Bereichen der Verwaltung

### 1. Meldewesen

#### a) Datenspeicherung

Zur Erfüllung ihrer Aufgaben speichern die Meldebehörden die in § 3 des Meldegesetzes für das Land Nordrhein-Westfalen (MG NW) genannten Daten einschließlich der zum Nachweis ihrer Richtigkeit erforderlichen Hinweise im Melderegister. Ein Datum „**Haushaltsvorstand**“ ist nicht vorgesehen; seine Speicherung ist deshalb unzulässig. Anlässlich eines Kontrollbesuchs bei einer Gemeinde habe ich festgestellt, daß dort der Datensatz der Personendatei ein Datenfeld „Haushaltsvorstand“ enthielt. Ich habe empfohlen, dieses Datenfeld aus dem Datensatz herauszunehmen.

#### b) Kombination gespeicherter Daten

Anlässlich der Landtagswahl 1985 wurden von einer Gemeinde den im Rat vertretenen Parteien Listen von Wahlberechtigten angeboten, die neben der zulässigen Angabe der Altersgruppe auch Hinweise auf Geschlecht und Haushaltsvorstand enthielten. Das Datum „Haushaltsvorstand“ ist zwar in der Melde-datei nicht gespeichert, wurde aber zum Zweck der Erstellung der Listen durch ein ADV-Programm gebildet. Als Haushaltsvorstand wurde der älteste männliche Familienangehörige ausgewiesen.

Die Übermittlung dieser Angabe war bereits deswegen unzulässig, weil die Daten, die an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen im Zusammenhang mit Parlaments- und Kommunalwahlen übermittelt werden dürfen, in § 35 Abs. 1 Satz 1 und 2 MG NW abschließend festgelegt sind (unten C.2.). In diesem Zusammenhang wurde auch die Frage aufgeworfen, ob die Meldebehörde überhaupt aus einer Kombination der von ihr zulässigerweise gespeicherten Daten ein neues Datum wie „Haushaltsvorstand“ bilden darf. Diese Frage kann nicht unabhängig von der Zulässigkeit der Übermittlung beurteilt werden.

Nach § 31 Abs. 1 Satz 1 MG NW darf die Meldebehörde bestimmte Daten, darunter auch die Anschrift, das Geburtsdatum und das Geschlecht, an andere öffentliche Stellen übermitteln, wenn dies zur rechtmäßigen Erfüllung der Aufgaben des Empfängers zulässig ist. Nach § 31 Abs. 1 Satz 3 MG NW dürfen diese Daten auch für eine Personengruppe listenmäßig übermittelt werden; dabei dürfen für die Zusammensetzung dieser Personengruppe die in § 31 Abs. 1 Satz 1 MG NW genannten Daten zugrunde gelegt werden. Danach wäre es zulässig, eine Liste der durch eine Kombination der genannten Angaben gebildeten Gruppe der „ältesten männlichen Einwohner an einer Anschrift“ zu übermitteln, allerdings nur soweit dies zur rechtmäßigen Aufgabenerfüllung des Datenempfängers erforderlich ist. Bei der Prüfung, ob die Aufgabenerfüllung rechtmäßig ist, ist auch der Grundsatz der Gleichberechtigung zwischen Mann und Frau (Artikel 3 Abs. 2 des Grundgesetzes) zu beachten.

Entsprechendes gilt für Gruppenauskünfte an Personen und nicht-öffentliche Stellen nach § 34 Abs. 3 MG NW. Nach dieser Bestimmung darf eine Melderegisterauskunft über eine Vielzahl nicht namentlich bezeichneter Einwohner (Gruppenauskunft) erteilt werden, soweit sie im öffentlichen Interesse liegt (§ 31 Abs. 3 Satz 1 MG NW). Für die Zusammensetzung der Personengruppe dürfen

Vor- und Familiennamen, Tag der Geburt, Geschlecht, Staatsangehörigkeit, Anschriften, Tag des Ein- und Auszugs, Familienstand, beschränkt auf die Angabe, ob verheiratet oder nicht, sowie der Beruf herangezogen werden (§ 31 Abs. 3 Satz 2 MG NW). Danach wäre die Übermittlung von Personengruppen, die ausschließlich aus den dort genannten Daten gebildet werden (z. B. ältester männlicher Einwohner an einer Anschrift) zulässig, sofern die übrigen Voraussetzungen gegeben sind. Bei der Prüfung, ob die Gruppenauskunft im öffentlichen Interesse liegt, ist ebenfalls der Grundsatz der Gleichberechtigung zwischen Mann und Frau zu berücksichtigen.

### c) Datenübermittlung an nicht-öffentliche Stellen

- Nach einer Pressemeldung sollte unter Hinweis auf die melderechtlichen Bestimmungen eine Meldebehörde dem **Suchdienst** des Deutschen Roten Kreuzes die Unterstützung verweigert haben. Der Suchdienst wollte die Verbindung einer Aussiedlerin zu ihrer früher in dieser Stadt wohnhaft gewesenen Verwandten herstellen. Diese Verwandte war bereits vor etlichen Jahren aus dieser Stadt weggezogen.

Nach Ablauf von fünf Jahren nach Ende des Kalenderjahres, in dem ein Einwohner weggezogen ist, sind die bis dahin gespeicherten Daten gesondert aufzubewahren (§ 11 Abs. 3 Satz 1 MG NW). Während der Zeit der gesonderten Aufbewahrung dürfen die Daten nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zur rechtmäßigen Aufgabenerfüllung der in § 31 Abs. 3 genannten Behörden oder für Wahlzwecke unerlässlich ist oder der Betroffene schriftlich eingewilligt hat (§ 11 Abs. 3 Satz 2 MG NW).

Soweit durch die Auskunft nur ein rein persönlicher Kontakt zwischen Verwandten hergestellt werden soll, ist nach meiner Auffassung die Auskunfterteilung nur mit Einwilligung des Gesuchten zulässig, da nicht auszuschließen ist, daß durch die Auskunfterteilung seine schutzwürdigen Belange beeinträchtigt werden, etwa wenn er gar keinen Kontakt mit Verwandten wünscht. Wird die Auskunft für andere Zwecke, wie Renten- oder Staatsangehörigkeitsangelegenheiten, benötigt, so kann aus der Sicht des Datenschutzes hingenommen werden, wenn bei den Suchdiensten das Erfordernis der bestehenden Beweisnot für eine Auskunft weit ausgelegt und nicht auf ein förmliches Verfahren beschränkt wird.

- In den vergangenen Jahren haben sich immer wieder Bürger an mich gewandt und Einwendungen gegen die Übermittlung ihrer personenbezogenen Daten an **Adreßbuchverlage** erhoben. Bisher konnte ich ihnen nur mitteilen, daß ich mich in meiner Stellungnahme zu dem Entwurf des Meldegesetzes für das Land Nordrhein-Westfalen für ein Widerspruchsrecht des Bürgers gegen die Datenübermittlung an Adreßbuchverlage oder gegen die Veröffentlichung in einem nach Straßen und Häusern gegliederten Einwohnerverzeichnis eingesetzt hatte, um ihn vor Belästigung und Gefährdung zu schützen, meine Vorschläge aber in dem vom Landtag beschlossenen Gesetz keine Berücksichtigung gefunden haben.

In der letzten Wahlperiode hatte die Landesregierung im Landtag den Entwurf eines Gesetzes zur Fortentwicklung des Datenschutzes eingebracht, in dem vorgeschlagen wurde, in § 35 Abs. 4 MG NW entsprechend der Regelung in den Meldegesetzen aller anderen Bundesländer ein Widerspruchsrecht des Betroffenen gegen die Melderegisterauskunft an Adreßbuchverlage vorzusehen. Ich habe den Gemeinden empfohlen, bereits jetzt den Widerspruch eines Einwohners gegen eine solche Datenübermittlung zu beachten. Der Innenminister hat in einem Runderlaß vom 6. November 1985 ausgeführt,

daß er im Hinblick auf die beabsichtigte Änderung des § 35 Abs. 4 MG NW keine Bedenken habe, wenn die Meldebehörden Widersprüche von Einwohnern beachten, die unter Berufung auf das Recht der informationellen Selbstbestimmung die Auskunft über ihre Daten an Adreßbuchverlage nicht wünschen.

- Nach § 35 Abs. 3 Satz 1 MG NW darf die Meldebehörde aus dem Melderegister Auskunft über **Alters- und Ehejubiläen** von Einwohnern erteilen, wenn der Betroffene dieser Auskunft nicht widersprochen hat. Auf das Widerspruchsrecht hat die Meldebehörde durch öffentliche Bekanntmachung mindestens einmal jährlich hinzuweisen (§ 35 Abs. 3 Satz 2 MG NW). Ein Schreiben an den Betroffenen, in dem dieser auf sein Widerspruchsrecht hingewiesen wird, ist nach der gesetzlichen Regelung nicht erforderlich.

Für die Ausübung des Widerspruchsrechts kann eine Frist bestimmt werden, die nicht weniger als drei Monate vor dem Ereignis betragen darf (§ 35 Abs. 3 Satz 3 MG NW). Ein Widerspruch des Betroffenen nach Ablauf der festgelegten Frist ist nach meiner Auffassung zu beachten, solange die Auskunft nicht erteilt worden ist. Dies ergibt sich aus § 7 Satz 1 MG NW, wonach durch eine Auskunft aus dem Melderegister schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden dürfen. Die Frist hat nur die Bedeutung, daß die Auskunft auf keinen Fall früher erteilt werden darf.

- In der Meldedatei einer Gemeinde war bei dem Datensatz einer ehemaligen Einwohnerin eine **Auskunftssperre** nach § 34 Abs. 5 MG NW vermerkt. Eine Bank fragte bei der Meldebehörde nach der jetzigen Anschrift der Einwohnerin an, um eine Forderung geltend machen zu können. Die Meldebehörde hatte wegen der eingetragenen Sperre Bedenken, die gewünschte Melderegisterauskunft zu erteilen.

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

Sind die Voraussetzungen für eine solche Auskunftssperre gegeben, so wirkt sie gegenüber jedermann. Es kommt nicht darauf an, ob dem Antrag auf Eintragung der Auskunftssperre ein konkreter Sachverhalt, der die Verweigerung der Auskunft an eine bestimmte Person zum Gegenstand hatte, zugrunde gelegen hat (Medert/Süßmuth/Schweinoch/Weigert, Melderecht des Bundes und der Länder, MRRG, § 21 Rdnr. 62).

Nach § 11 Abs. 2 Satz 2 MG NW hat die Meldebehörde nach dem Wegzug eines Einwohners mit Ausnahme der Angabe erwerbstätig/nicht erwerbstätig die Daten nach § 3 Abs. 1 MG NW, also auch Übermittlungssperren nach § 3 Abs. 1 Nr. 18 MG NW weiterhin zu speichern. Die Auskunftssperre nach § 34 Abs. 5 MG NW ist daher auch bei weggezogenen Einwohnern weiterhin zu beachten (so auch Medert/Süßmuth/Schweinoch/Weigert, aaO, § 21 Rdnr. 61).

Nach Ablauf von fünf Jahren nach Ende des Kalenderjahres, in dem ein Einwohner weggezogen ist, sind die bis dahin gespeicherten Daten gesondert aufzubewahren (§ 11 Abs. 3 Satz 1 MG NW). Während der Zeit der gesonderten Aufbewahrung dürfen die Daten nicht mehr verarbeitet oder sonst genutzt werden, es sei denn, daß dies zu wissenschaftlichen Zwecken, zur Behebung einer bestehenden Beweisnot, zur rechtmäßigen Aufgabenerfüllung der in § 31 Abs. 3 genannten Behörden oder für Wahlzwecke unerlässlich ist oder der Betroffene schriftlich eingewilligt hat (§ 11 Abs. 3 Satz 2 MG NW).

Auch bei dieser Nutzung der gesondert aufbewahrten Daten ist die Auskunftssperre nach § 34 Abs. 5 MG NW zu beachten. Daher kann nur eine Übermittlung an öffentliche Stellen (§ 31 MG NW) nicht aber eine Melderegisterauskunft an Personen und nicht-öffentliche Stellen (§ 34 MG NW) in Betracht kommen.

#### **d) Lohnsteuerkarten**

In dem Merkblatt über die Ausstellung und Zustellung der Lohnsteuerkarten 1985 durch die Gemeinden war in Nr. 7 Abs. 2 Satz 6 bestimmt, daß, soweit Gemeinden eine Einwohnerdatei erstellt haben, keine Bedenken bestehen, daß das „Personenkennzeichen“ eingetragen wird. Bei dem Personenkennzeichen handelte es sich um das Ordnungsmerkmal, mit dessen Hilfe die Meldebehörden die Melderegister nach § 4 Abs. 1 MG NW führen dürfen. Die Ausführungen in dem Merkblatt veranlaßten eine Gemeinde, die Lohnsteuerkarten mit dem Ordnungsmerkmal zu versehen.

Ordnungsmerkmale dürfen innerhalb der Gemeinde weitergegeben werden und unter bestimmten Voraussetzungen im Rahmen von Datenübermittlungen an Behörden, sonstige öffentliche Stellen und öffentlich-rechtliche Religionsgesellschaften übermittelt werden (§ 4 Abs. 2 Satz 1 und 2 MG NW). Nach § 4 Abs. 3 MG NW dürfen diese Ordnungsmerkmale an nicht-öffentliche Stellen nicht übermittelt werden. Dem widerspricht es, wenn in die Lohnsteuerkarte, die dazu bestimmt ist, unter anderem dem Arbeitgeber vorgelegt zu werden, das Ordnungsmerkmal eingetragen wird. Da eine solche Eintragung mit dem Zweck des § 4 Abs. 3 MG NW nicht vereinbar ist, ist die Aufnahme des Ordnungsmerkmals in die Lohnsteuerkarte nicht zulässig.

Meiner Empfehlung, von einer derartigen Eintragung auf der Lohnsteuerkarte künftig abzusehen, wird gefolgt. Das Merkblatt über die Ausstellung und Zustellung der Lohnsteuerkarten wurde für 1986 entsprechend geändert.

#### **e) Übertragung anderer Aufgaben**

Bei einem Kontrollbesuch bei einer Stadt war unter anderem der Umgang mit personenbezogenen Daten bei dem dort eingerichteten **Bürgeramt** zu prüfen. „Kommen Sie zu uns ins neue Bürgeramt. Wir helfen Ihnen gerne weiter.“ So wirbt die Stadt für das neue Amt, das sich als Ergebnis eines noch laufenden Forschungsprojekts in der Anlaufphase befindet. „Nein, dafür bin ich nicht zuständig.“ Diese Antwort soll der Bürger künftig nicht mehr erhalten. Mit Hilfe moderner Technik sollen viele Aufgaben an Ort und Stelle für den Bürger sofort erledigt werden. Dabei muß allerdings der Datenschutz beachtet werden.

Nach Mitteilung der Stadt und den bei dem Kontrollbesuch gewonnenen Erkenntnissen nimmt das Bürgeramt neben der Auskunfterteilung über Zuständigkeiten der Stadtverwaltung sowie anderer Behörden und Einrichtungen und über Leistungen der Stadt folgende Aufgaben wahr:

- a) Einwohnermeldewesen:
  - An-, Ab- und Ummeldungen;
  - Ausstellung und Verlängerung von Personalausweisen und Pässen;
  - Entgegennahme der Anträge auf Erteilung eines Führungszeugnisses;
  - Auskünfte aus dem Melderegister;
  - Wehrerfassung (§ 15 des Wehrpflichtgesetzes).
- b) Entgegennahme von Anträgen auf Erteilung von Fahrerlaubnissen für den Kreis (Straßenverkehrsamt). Hierbei wird lediglich auf die Einwohnermelde-datei zugegriffen, um die im Antragsvordruck vorgesehenen Personalien mit den Daten im Melderegister abzugleichen. Es erfolgt keine Bearbeitung des Antrags.

Anschriftenänderung auf dem Kraftfahrzeugschein für den Kreis (Straßenverkehrsamt) anlässlich von Anmeldungen bei Umzügen innerhalb des Kreisgebietes und Ummeldungen.

- c) Ausstellung und Änderung von Lohnsteuerkarten.
- d) Beglaubigung von Unterschriften, Abschriften und Fotokopien.
- e) Entgegennahme der Anträge auf Erteilung und Verlängerung von Aufenthaltserlaubnissen für den Kreis (Ausländeramt). Hierbei wird von den Mitarbeitern des Bürgeramtes auf die Einwohnermeldedatei zugegriffen, um die Personalien und die Aufenthalts- und Meldezeiten zu prüfen.  
Entgegennahme der Anträge auf Erteilung von Einreise genehmigungen für Angehörige von Ostblockstaaten für den Kreis (Ausländeramt). Hier werden Name, Vorname und Anschrift der Besuchten mit den Daten in der Einwohnermeldedatei verglichen.
- f) Annahme der Briefwahlanträge, Ausdruck des Wahlscheines und Aushändigung der Briefwahlunterlagen an den Antragsteller.
- g) Ausstellung von Untersuchungsberechtigungsscheinen nach dem Jugendarbeitsschutzgesetz (vgl. § 3 Abs. 2 Nr. 10 MG NW).
- h) Ausstellung von Sonderausweisen für kinderreiche Familien zum Besuch des Hallenbades und der Eissporthalle. Einzige Voraussetzung für die Ausstellung der Ausweise an die Kinder ist, daß die Familie drei oder mehr Kinder unter 18 Jahren hat. Zahl und Alter der in dem Antrag angegebenen Kinder werden in der Einwohnermeldedatei geprüft. Liegt die Voraussetzung nicht vor, so wird der Betroffene darauf hingewiesen, daß das Sozialamt ebenfalls derartige Ausweise ausstellt, wenn die dort geforderten Voraussetzungen (z. B. Berechtigung zum Empfang von Sozialhilfe) vorliegen.

Den Mitarbeitern des Bürgeramtes steht für die Aufgabenerfüllung die Einwohnermeldedatei und eine Informationsdatei zur Verfügung. In der Informationsdatei sind abgesehen von den Namen der zuständigen Bediensteten keine personenbezogenen Daten gespeichert.

Unter der Voraussetzung, daß die Darstellung der Aufgaben des Bürgeramtes und des Zugriffs seiner Mitarbeiter auf personenbezogene Daten erschöpfend ist und die Betroffenen die unter b) und e) genannten Anträge auch weiterhin unmittelbar beim Kreis stellen können, ist die erste Ausbaustufe des Bürgeramtes nach dem derzeitigen Erkenntnisstand nicht zu beanstanden.

Die Aufgaben des Bürgeramtes und der Zugriff seiner Mitarbeiter auf personenbezogene Daten in der zweiten Ausbaustufe sind noch nicht festgelegt. Die zweite Ausbaustufe bedarf weiterer Prüfung. Von einer datenschutzrechtlichen Beurteilung wurde daher derzeit abgesehen. Es erscheint jedoch zweifelhaft, ob eine datenschutzrechtlich unbedenkliche Übertragung weiterer wesentlicher Aufgaben auf das Bürgeramt möglich ist.

## 2. Wahlen

- Für Zwecke der **Wahlwerbung** darf nach § 35 Abs. 1 Satz 1 MG NW die Gemeinde als Meldebehörde Parteien, Wählergruppen und anderen Trägern von Wahlvorschlägen im Zusammenhang mit Parlaments- und Kommunalwahlen in den sechs der Wahl vorangehenden Monaten Auskunft aus dem Melderegister über Vor- und Familiennamen, akademische Grade und Anschriften der Wahlberechtigten erteilen, für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist. Die Geburtstage der Wahlberechtigten dürfen dabei nicht mitgeteilt werden (§ 35 Abs. 1 Satz 2 MG NW).

Die Angabe des Geschlechts, eines Datums „Haushaltsvorstand“ oder über die Zugehörigkeit zu der Gruppe der innerhalb eines bestimmten Zeitraums Zugezogenen ist nicht zulässig.

Ferner kann nach § 17 Abs. 5 Satz 1 der Landeswahlordnung (LWahlO) der Gemeindedirektor innerhalb der Auslegungsfrist die Anfertigung von Auszügen oder Abschriften des Wählerverzeichnisses durch Wahlberechtigte oder Träger von Wahlvorschlägen gestatten, wenn ein berechtigtes Interesse im Zusammenhang mit der Wahl besteht. Die Auszüge oder Abschriften dürfen die Geburtstage der Wahlberechtigten nicht enthalten (§ 17 Abs. 5 Satz 2 LWahlO). Nach § 17 Abs. 5 Satz 4 LWahlO kann der Gemeindedirektor unter den gleichen Voraussetzungen auch selbst Auszüge oder Abschriften des Wählerverzeichnisses an Träger von Wahlvorschlägen erteilen, wobei die Kenntlichmachung bestimmter Altersgruppen möglich ist.

Die Kenntlichmachung sonstiger Personengruppen ist nicht zulässig. Auch der Innenminister hat in Nr. 5 Buchst. d seines Runderlasses vom 7. Januar 1985 zur Vorbereitung und Durchführung der Landtagswahl 1985 (MBl. NW. S. 22) darauf hingewiesen, daß lediglich die Kenntlichmachung von Altersgruppen zulässig ist.

Entgegen der eindeutigen Rechtslage hielt ein Stadtdirektor die Erteilung von Auszügen aus dem Wählerverzeichnis über die innerhalb eines bestimmten Zeitraumes Zugezogenen für zulässig. Ich habe die unzulässige Bekanntgabe der Zugehörigkeit zu dieser Personengruppe als Verstoß gegen das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung beanstandet. Daraufhin hat mir der Stadtdirektor mitgeteilt, daß er künftig bei der Erteilung von Auszügen und Abschriften aus dem Wählerverzeichnis die Bekanntgabe der Zugehörigkeit zu anderen Personengruppen als Altersgruppen unterlassen wird. Auch der in einem anderen Fall ausgesprochenen Empfehlung, die Angabe des Geschlechts und eines Datums „Haushaltsvorstand“ zu unterlassen, wurde gefolgt.

- In meinem sechsten Tätigkeitsbericht (C.2.) hatte ich darüber berichtet, daß bei den letzten Kommunalwahlen mehrfach Parteien Kenntnis davon erhalten haben, daß eigene Parteimitglieder **Unterstützungsunterschriften** für Wahlvorschläge anderer Parteien geleistet hatten. In einem Fall hatte ich mit Zustimmung des Betroffenen Strafantrag gestellt. Das eingeleitete Ermittlungsverfahren wegen Verstoßes gegen § 203 StGB und § 33 DSGVO wurde inzwischen von der Staatsanwaltschaft gemäß § 153a Abs. 1 StPO gegen Zahlung einer Geldbuße eingestellt.

Auch bei der Landtagswahl 1985 ist es vorgekommen, daß Namen derjenigen, die eine Unterstützungsunterschrift geleistet hatten, bekannt wurden. Leider war es mir nicht möglich, mit der für eine Beanstandung nach § 30 DSGVO erforderlichen Sicherheit festzustellen, wie die Tatsache der Leistung von Unterstützungsunterschriften bekanntgeworden war.

- Ein Stadtdirektor hatte als Wahlleiter für die Wahl des Rates dieser Stadt zur Vorbereitung der Entscheidung des Wahlausschusses die geleisteten Unterstützungsunterschriften in Listen zusammenfassen lassen und diese an die Beisitzer weitergegeben. Die Listen wurden nach der Sitzung des Wahlausschusses den Beisitzern belassen. Da der Stadtdirektor bei künftigen Wahlen an seiner Praxis festhalten wollte, habe ich diese als Verstoß gegen Artikel 4 Abs. 2 der Landesverfassung und § 91 Abs. 1 der Kommunalwahlordnung gemäß § 30 Abs. 1 Satz 1 DSGVO beanstandet.

### 3. Paß- und Personalausweiswesen

Der Deutsche Bundestag hat den von den Fraktionen der CDU/CSU und FDP eingebrachten Gesetzentwurf (vgl. sechster Tätigkeitsbericht, C.3.) als Zweites Gesetz zur Änderung personalausweisrechtlicher Vorschriften und der Strafprozeßordnung verabschiedet. Ferner hat er das von der Bundesregierung eingebrachte Paßgesetz beschlossen. Damit hat sich die Bundestagsmehrheit über die Bedenken der Datenschutzbeauftragten des Bundes und der Länder gegen die Einführung eines maschinenlesbaren Ausweises hinweggesetzt. Der behauptete Sicherheitsgewinn durch die Maschinenlesbarkeit ist nach wie vor nicht dargetan.

Zwar wurde darauf verzichtet, die Verwendung eines Ausweises zur automatischen Speicherung von Abfragen für Zwecke der Gefahrenabwehr vorzusehen; dies soll der Regelung in den Polizeigesetzen vorbehalten bleiben. In einem neuen § 163d der Strafprozeßordnung wird jedoch die Speicherung der bei einer grenzpolizeilichen Kontrolle oder einer Personenkontrolle nach § 111 StPO anfallenden personenbezogenen Daten in einer Datei für die Verfolgung bestimmter schwerer Straftaten zugelassen. Eine derartige Regelung, von der auch unverdächtige Bürger betroffen sind, hätte nicht unter Zeitdruck im Rahmen der Beratung der Ausweisgesetze beschlossen werden sollen. Sie hätte vielmehr einer intensiven Beratung und einer Abstimmung mit den anderen noch ausstehenden Regelungen der Datenverarbeitung zu Zwecken der Strafverfolgung in der Strafprozeßordnung bedurft.

### 4. Personenstandswesen

Nach § 104 Abs. 1 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden (alte Fassung) konnte Interessenten auf Antrag eine Aufstellung über die beurkundeten Eheschließungen, Geburts- und Sterbefälle gegen angemessenes Entgelt zur Verfügung gestellt werden. In die Aufstellung durften nur die Personenstandsfälle aufgenommen werden, mit deren Veröffentlichung sich die Beteiligten einverstanden erklärt hatten. In der ab 1. März 1985 geltenden Fassung der Dienstanweisung ist diese Vorschrift gestrichen worden. Einige Gemeinden sind seitdem dazu übergegangen, derartige Aufstellungen nicht mehr an die Presse oder andere Interessenten herauszugeben.

Der Innenminister des Landes Nordrhein-Westfalen hat in seinem Runderlaß vom 9. April 1985 (MBl. NW. S. 689) bestimmt, daß auch nach Streichung des § 104 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden eine im Einklang mit den datenschutzrechtlichen Vorschriften stehende Veröffentlichung von Personenstandsfällen zulässig bleibt. Entsprechenden Wünschen kann daher durch eine den datenschutzrechtlichen Vorschriften gemäß Handhabung (jedenfalls schriftliche Einwilligung der Betroffenen gemäß § 3 Satz 1 DSGVO) Rechnung getragen werden.

Einige Gemeinden sind dazu übergegangen, keine Veröffentlichungen mehr vorzunehmen. Bürgern, denen diese Bekanntmachungen in der Presse fehlten, konnte ich nur mitteilen, daß die Bekanntgabe derartiger Personenstandsfälle mit Einwilligung des Betroffenen zwar zulässig ist, für die Standesbeamten hierzu aber keine rechtliche Verpflichtung besteht.

### 5. Ausländerwesen

Zwei ausländische Bürger sahen in der Aufbewahrung von Mitteilungen über Verurteilungen aus vergangenen Jahren in ihrer Ausländerakte einen Verstoß

gegen Vorschriften über den Datenschutz und haben mich insoweit um Prüfung gebeten.

Das Aufbewahren von Mitteilungen über Verurteilungen in der Ausländerakte stellt einen Eingriff in das vom Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 aus dem allgemeinen Persönlichkeitsrecht nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes hergeleitete Recht des Betroffenen auf informationelle Selbstbestimmung wie auch in sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 Satz 1 der Landesverfassung dar. Das Grundrecht des Artikels 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, und schützt ihn damit gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten (BVerfGE 65, 1, 43).

Eingriffe in diese Grundrechte müssen von den Betroffenen zwar im überwiegenden Interesse der Allgemeinheit hingenommen werden. Sie bedürfen jedoch einer normenklaren gesetzlichen Grundlage; darüber hinaus ist bei solchen Eingriffen der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten (aaO 44).

Zwar kann das Aufbewahren von Mitteilungen über Verurteilungen in der Ausländerakte auf die Vorschriften des Ausländergesetzes über aufenthaltsrechtliche Entscheidungen in Verbindung mit den Vorschriften des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen gestützt werden. Wenn gleich Zweifel bestehen, ob diese Vorschriften insoweit dem Gebot der Normenklarheit entsprechen, wird nach der Rechtsprechung des Bundesverfassungsgerichts für eine Übergangszeit bis zur Schaffung einer hinreichend normenklaren gesetzlichen Grundlage eine auf die genannten Vorschriften gestützte Aufbewahrung derartiger Mitteilungen hingenommen werden müssen, um eine Funktionsunfähigkeit staatlicher Einrichtungen zu vermeiden, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand (vgl. BVerfGE 33, 12, 347; 41, 267).

Jedoch kann aus dem Verhältnismäßigkeitsgrundsatz ein Anspruch auf Entfernung belastender Angaben aus der Ausländerakte hergeleitet werden, wenn das weitere Festhalten dieser Angaben zur Aufgabenerfüllung der Ausländerbehörde nicht mehr erforderlich ist. Dies muß jedenfalls dann gelten, wenn wie in den vorliegenden Fällen die Angaben nicht zu ausländerrechtlichen Entscheidungen geführt haben und auch künftig nicht zu solchen Entscheidungen führen können, weil dem ein gesetzliches Verwertungsverbot entgegensteht.

Dabei ist auch zu berücksichtigen, daß nach § 17 Abs. 3 Satz 2 in Verbindung mit Abs. 2 Satz 2 DSG NW personenbezogene Daten zu löschen sind, wenn ihre Kenntnis zur rechtmäßigen Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich ist und der Betroffene die Löschung verlangt. Zwar findet diese Vorschrift nur auf Daten Anwendung, die in Dateien gespeichert werden. In ihr kommt jedoch ein allgemeines Rechtsprinzip zum Ausdruck, das sich aus dem Verhältnismäßigkeitsgrundsatz ergibt und eine Löschung jedenfalls dann gebietet, wenn die Angaben zur Aufgabenerfüllung nicht mehr erforderlich sind, der Betroffene die Löschung verlangt und das weitere Festhalten der Angaben ihn belastet, auch wenn sie einem Verwertungsverbot unterliegen. Der mit der Löschung verbundene Verwaltungsaufwand kann einem solchen Anspruch jedenfalls dann nicht entgegengehalten werden, wenn dieser Aufwand wie im Falle der Löschung von Angaben über einzelne Verurteilungen nicht unvertretbar ist.

Das Bundesverfassungsgericht hat allerdings in einem Beschluß vom 6. Juni 1983 (NJW 1983, 2135) entschieden, daß die Pflicht der Ausländerbehörde zur

vollständigen Aktenführung nicht nur einer Hintanhaltung von Informationen und Wertungen, sondern auch deren Entfernung aus den Akten entgegenstehe, wenn die Informationen erst einmal rechtmäßig dort hingelangt seien. Diese Entscheidung, nach der der Betroffene die Aufbewahrung derartiger Unterlagen ohne zeitliche Begrenzung hinnehmen müßte, steht jedoch im Widerspruch zu den in dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 entwickelten Grundsätzen und muß durch dieses Urteil als überholt angesehen werden.

Der Auffassung des Oberstadtdirektors, daß der Beschluß vom 6. Juni 1983 vorrangig sei, weil er gegenüber dem Urteil vom 15. Dezember 1983 die speziellere Entscheidung sei und in dem Beschluß die Verhältnismäßigkeit der Aufbewahrung von Informationen in den Ausländerakten ausdrücklich bejaht werde, kann nicht gefolgt werden. Das Urteil vom 15. Dezember 1983 enthält verfassungsrechtliche Aussagen, die über die zu entscheidende Frage der Vereinbarkeit des Volkszählungsgesetzes 1983 mit dem Grundgesetz hinaus grundsätzliche Bedeutung für den Datenschutz haben. Darin hat das Gericht nicht nur allgemein darauf hingewiesen, daß bei Eingriffen in das Recht auf informationelle Selbstbestimmung der Verhältnismäßigkeitsgrundsatz zu beachten ist, sondern auch die Beschränkung des Sammelns personenbezogener Daten auf das erforderliche Minimum verlangt und die Bedeutung von Löschungspflichten als Vorkehrungen gegen die Gefahr einer Verletzung des Persönlichkeitsrechts hervorgehoben (aaO 44, 46). Mit diesen Aussagen ist die in dem Beschluß vom 6. Juni 1983 vertretene Ansicht, daß die Betroffenen bei Beachtung bestimmter vom Gericht formulierter Verwendungsbeschränkungen aus der Aufbewahrung derartiger Informationen in ihren Ausländerakten keine „Nachteile für ihre Grundrechte“ zu befürchten hätten (aaO 2136), nicht vereinbar. Es ist auch keineswegs gewährleistet, daß Verwendungsbeschränkungen immer beachtet werden.

Da der Oberstadtdirektor meiner Empfehlung, die Angaben über die Verurteilungen des Betroffenen aus der Ausländerakte zu entfernen, nicht nachgekommen ist, habe ich den Verstoß gemäß § 30 Abs. 1 Satz 1 DSG NW beanstandet. Der Oberstadtdirektor hält jedoch an seiner bisherigen Verfahrensweise fest.

## 6. Kommunalwesen

- In meinem dritten Tätigkeitsbericht (C.6.a) hatte ich zu der Behandlung von Bauanträgen und Bauvoranfragen in **Rats- und Ausschusssitzungen** Stellung genommen. Auf Grund der inzwischen ergangenen Urteile des Verwaltungsgerichts Köln vom 25. Januar 1985 – 4 K 3729/84 – und des Verwaltungsgerichts Gelsenkirchen vom 5. August 1985 – 15 K 5314/83 – bin ich von vielen Gemeinden hierzu erneut um Stellungnahme gebeten worden.

Der in dem Urteil des Verwaltungsgerichts Köln vertretenen Ansicht, daß bei der Behandlung von Bauanträgen und Bauvoranfragen dem Recht des Bürgers auf Datenschutz im Ergebnis eine geringere Bedeutung beizumessen sei als dem Grundsatz der Öffentlichkeit von Rats- und Ausschusssitzungen, kann ich nicht folgen. Sie trägt der Bedeutung und Tragweite des vom Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes hergeleiteten Rechts auf informationelle Selbstbestimmung wie auch das Grundrechts auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung nicht Rechnung.

Gleiches gilt für die Entscheidung des Verwaltungsgerichts Gelsenkirchen, wonach Bauvoranfragen und Bauanträge generell in öffentlicher Sitzung zu behandeln sind und nur im Einzelfall die Öffentlichkeit gemäß § 33 Abs. 2

Satz 3 der Gemeindeordnung für das Land Nordrhein-Westfalen (GO) durch Ratsbeschluß ausgeschlossen werden darf. Diese Entscheidung geht auf das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Datenschutz, die nicht auf „Geheimnisse“ beschränkt sind, überhaupt nicht ein und nimmt demzufolge auch keine Abwägung zwischen dem Interesse des Betroffenen an dem Schutz seiner Daten und dem Interesse der Allgemeinheit an der Behandlung in öffentlicher Sitzung vor.

Ich halte an der im dritten Tätigkeitsbericht vertretenen Auffassung fest, daß ein überwiegendes Interesse der Allgemeinheit an der Behandlung von Bauanträgen und Bauvoranfragen in öffentlicher Sitzung, demgegenüber die genannten Grundrechte zurückzutreten hätten, im Regelfall nicht vorliegt.

- In einer Ratssitzung wurden unter anderem an die Presse und das Publikum Unterlagen über Erschließungsbeiträge in einem Bebauungsplangebiet verteilt. Bei diesen Unterlagen befand sich eine Aufstellung über die Erschließungsbeiträge mit Namen und Anschriften der Grundstückseigentümer und die Grundstücksbezeichnungen. Für die Bekanntgabe dieser Daten war eine gesetzliche Grundlage nicht vorhanden. Im übrigen hätte eine anonymisierte Liste dem Informationszweck genügt. Der Gemeindedirektor sieht künftig von einer derartigen Bekanntgabe personenbezogener Daten ab.
- In zahlreichen Fällen wurde ich um eine datenschutzrechtliche Prüfung der Weitergabe personenbezogener Daten durch die Verwaltung an Ausschüsse, Fraktionen und einzelne Ratsmitglieder zum Zweck der **Kontrolle der Verwaltung** gebeten.
  - So sollten Angaben über das Ergebnis von Bodenuntersuchungen nach § 3 Abs. 2 der Klärschlammverordnung an eine Ratsfraktion weitergegeben,
  - Auskünfte über Einsätze der Freiwilligen Feuerwehr an eine Ratsfraktion erteilt,
  - Ratsmitgliedern Einsicht in Personalakten gewährt und
  - Auskünfte über von einem Kreis durchgeführte Ordnungswidrigkeitenverfahren an parlamentarische Gremien weitergegeben werden.

Als gesetzliche Grundlage für die Weitergabe personenbezogener Daten zum Zweck der Kontrolle der Verwaltung kommt nur § 40 GO in Betracht. Nach § 40 Abs. 2 Satz 1 GO überwacht der Rat die Durchführungen seiner Beschlüsse und der Beschlüsse der Bezirksvertretungen und Ausschüsse sowie den Ablauf der Verwaltungsangelegenheiten. Zu diesem Zweck kann er vom Gemeindedirektor Einsicht in die Akten durch einen von ihm bestimmten Ausschuß oder einzelne von ihm beauftragte Mitglieder verlangen (§ 40 Abs. 2 Satz 2 GO). Da § 40 GO eine abschließende Regelung enthält und ein Auskunfts- oder Einsichtsrecht für die Fraktionen als solche nicht vorsieht, ist somit wegen Fehlens einer nach Artikel 4 Abs. 2 der Landesverfassung erforderlichen gesetzlichen Grundlage die Weitergabe personenbezogener Daten an eine Fraktion ohne Einwilligung der Betroffenen nicht zulässig.

In Einzelfällen muß auf Beschluß des Rates oder auf Verlangen von mindestens einem Fünftel der Ratsmitglieder auch einem einzelnen, von den Antragstellern zu benennenden Ratsmitglied Akteneinsicht gewährt werden (§ 40 Abs. 3 Satz 1 GO). Das Recht zur Überprüfung der Verwaltungstätigkeit setzt ein Recht zur Akteneinsicht auch in vertraulich zu behandelnde Angelegenheiten, etwa in Personalangelegenheiten, voraus. Es schließt jedoch nicht die Befugnis ein, die Akten aus den Diensträumen zu entfernen. Die Gewährung von Akteneinsicht ist nur dem einen benannten Ratsmitglied in den Diensträumen der Verwaltung, und zwar unter Aufsicht eines Bediensteten gestattet. Diese Auffassung wird auch vom Innenminister geteilt.

Die Ratsmitglieder, die nach § 40 Abs. 2 Satz 2 oder § 40 Abs. 3 Satz 1 GO Akteneinsicht erhalten, sind nach § 30 Abs. 2 in Verbindung mit § 22 Abs. 1 GO zur Verschwiegenheit verpflichtet. Dies gilt in jedem Fall gegenüber Außenstehenden. Ihnen dürfen die durch Akteneinsicht gewonnenen Erkenntnisse nicht mitgeteilt werden. Gegenüber den anderen Ratsmitgliedern, insbesondere der eigenen Fraktion, wird die Verschwiegenheitspflicht durch das in § 40 Abs. 3 GO auch Minderheiten ausdrücklich zugestandene Recht zur Kontrolle der Verwaltung begrenzt. Danach bestehen gegen die Weitergabe den Akten entnommener personenbezogener Daten an andere Ratsmitglieder, soweit sie für eine sachgerechte Unterrichtung zum Zweck der Kontrolle der Verwaltung erforderlich ist, keine durchgreifenden datenschutzrechtlichen Bedenken. Für diese Ratsmitglieder gilt jedoch ebenfalls die Verschwiegenheitspflicht nach § 30 Abs. 2 Satz 1 in Verbindung mit § 22 Abs. 1 GO.

Als gesetzliche Grundlage für Auskünfte über von einem Kreis durchgeführte Ordnungswidrigkeitenverfahren an parlamentarische Gremien zum Zwecke der Kontrolle der Verwaltung kommt nur § 20 Abs. 2 der Kreisordnung (KrO) in Frage. Nach dieser Vorschrift ist der Kreistag durch den Landrat über alle wichtigen Angelegenheiten der Kreisverwaltung zu unterrichten (Satz 1). Zu diesem Zweck kann der Landrat vom Oberkreisdirektor jederzeit Auskunft und Akteneinsicht verlangen (Satz 2). Der Kreistag kann vom Oberkreisdirektor Einsicht in die Akten durch einen von ihm bestimmten Ausschuß oder einzelne von ihm beauftragte Mitglieder fordern (Satz 3). In Einzelfällen muß auf Verlangen von mindestens einem Fünftel der Kreistagsmitglieder auch einem einzelnen, von den Antragstellern zu benennenden Kreistagsmitglied Akteneinsicht gewährt werden (Satz 4). Auch Ausschußvorsitzende können vom Oberkreisdirektor jederzeit Auskunft über die Angelegenheiten verlangen, die zum Aufgabenbereich ihres Ausschusses gehören; sie haben das Recht auf Akteneinsicht nach Maßgabe der Hauptsatzung (Satz 5). Ein Unterrichtsrecht der Fraktion ist hiernach nicht vorgesehen.

Inwieweit die in diesen Vorschriften enthaltenen Unterrichts-, Auskunfts- und Akteneinsichtsrechte als gesetzliche Grundlage für die Bekanntgabe personenbezogener Daten bei Auskünften über Ordnungswidrigkeitenverfahren wegen Verstöße gegen umweltschützende Vorschriften herangezogen werden können, läßt sich letztlich nur im konkreten Einzelfall beurteilen. Sofern für eine sachgerechte Unterrichtung zur Kontrolle der Verwaltung die Bekanntgabe personenbezogener Daten an einen Ausschuß erforderlich ist, folgt nach meiner Auffassung aus dem Grundrecht auf Datenschutz das Gebot, die Auskunft in nicht-öffentlicher Sitzung zu erteilen.

Als gesetzliche Grundlage für personenbezogene Mitteilungen über von anderen Behörden durchgeführte Ordnungswidrigkeitenverfahren, über die der Kreis dienstlich unterrichtet worden ist, an Ausschüsse des Kreistages dürfte § 20 Abs. 2 KrO allerdings in aller Regel nicht in Betracht kommen.

- Der Vorsitzende einer Fraktion einer Bezirksvertretung hatte einen Pressebericht über die Behandlung einer Jugendhilfeangelegenheit (Einzelfallhilfe) durch das zuständige Jugendamt zum Anlaß genommen, die Verwaltung zu bitten, in einer nicht-öffentlichen Sitzung über die Angelegenheit zu berichten.

Die Verpflichtung der Leistungsträger zur Wahrung des Sozialgeheimnisses nach § 35 Abs. 1 und 2 des Ersten Buches des Sozialgesetzbuchs (SGB I) besteht nicht nur gegenüber außenstehenden Dritten. Sie gilt auch innerhalb der Leistungsträger (vgl. dritter Tätigkeitsbericht, C.8.b). Soweit das kommunale Verfassungsrecht eine Weitergabe personenbezogener Daten vorschreibt oder zuläßt, deren Offenbarung nach § 35 Abs. 1 SGB I unzulässig ist, geht diese bundesrechtliche Verbotsnorm nach Artikel 31 des Grundge-

setzes vor. Eine Offenbarung in dem dargelegten Fall wäre daher ohne Einwilligung der Betroffenen nur unter den Voraussetzungen der §§ 68 bis 77 des Zehnten Buches des Sozialgesetzbuchs (SGB X) zulässig.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist die Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch eine in § 35 SGB I genannte Stelle erforderlich ist. Zu den gesetzlichen Aufgaben nach dem Sozialgesetzbuch gehört nach meiner Auffassung auch die gesetzlich vorgesehene Kontrolle der Aufgabenerfüllung (vgl. auch § 35 Abs. 1 Satz 2 SGB I).

Nach § 13 Abs. 3 des Gesetzes für Jugendwohlfahrt (JWG) werden die Aufgaben nach diesem Gesetz durch den Jugendwohlfahrtsausschuß und durch die Verwaltung des Jugendamtes wahrgenommen. Die Aufgabenverteilung ist in der Weise geregelt, daß der Jugendwohlfahrtsausschuß sich anregend und fördernd mit den Aufgaben der Jugendwohlfahrt befaßt und im Rahmen der von der Vertretungskörperschaft bereitgestellten Mittel, der von ihr erlassenen Satzung und der von ihr gefaßten Beschlüsse über die Angelegenheiten der Jugendhilfe beschließt (§ 15 Satz 1 und 2 JWG), während die laufenden Geschäfte des Jugendamtes, zu denen insbesondere die Einzelfallhilfe zählt, von dem Leiter der Verwaltung (dem Hauptverwaltungsbeamten) oder in seinem Auftrag von dem Leiter der Verwaltung des Jugendamtes im Rahmen der Satzung und der Beschlüsse der zuständigen Vertretungskörperschaft und des Jugendwohlfahrtsausschusses geführt werden (§ 16 Abs. 1 JWG). Hiernach scheidet es aus, daß der Rat eine Jugendhilfesache, die ein einfaches Geschäft der laufenden Verwaltung darstellt, gemäß § 28 Abs. 3 GO im Wege des Rückholrechts einer Bezirksvertretung vorbehält. Da die Bezirksvertretung keine Kontrollbefugnis gegenüber dem Jugendamt hat und ihre Aufgaben keine Aufgaben nach dem Sozialgesetzbuch sind, ist die Offenbarung personenbezogener Daten an die Bezirksvertretung ohne Einwilligung des Betroffenen unzulässig. Die Verwaltung könnte bei Anfragen in der Bezirksvertretung allerdings verpflichtet sein, sich um die Einwilligung zu bemühen.

- In meinem ersten Tätigkeitsbericht (C.4.) und meinem dritten Tätigkeitsbericht (C.3.) habe ich zu der Zulässigkeit von Regelungen in der **Ehrenordnung** des Rates der Gemeinden Stellung genommen. Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 bedarf ein Eingriff in das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Datenschutz einer normenklaren gesetzlichen Grundlage. Die Formulierung in einer Ehrenordnung, die die Verwendung der erhobenen Daten „im Rahmen der Geschäftsordnung“ zuläßt, entspricht nicht dem Gebot der Normenklarheit. Auch erlauben der Grundsatz der Erforderlichkeit und die Verpflichtung zum Schutz der Daten gegen Zweckentfremdung eine Datenweitergabe im Regelfall nur an den jeweiligen Ausschußvorsitzenden.

Ich würde es begrüßen, wenn der Gesetzgeber den Zugang zu den erhobenen Daten klar in der Gemeindeordnung regeln würde. Solange dies nicht geschieht, halte ich es für geboten, daß der Rat in der Ehrenordnung festlegt, wer unter welchen Voraussetzungen Zugang zu welchen Daten hat und wann die erhobenen Daten zu löschen sind. Nach meiner Auffassung könnte die Löschung nach Ende der Wahlperiode erfolgen, in der oder mit deren Ablauf das Ratsmitglied ausgeschieden ist. Bei Veränderung von Daten könnte für die Löschung der alten Daten auf das Ende der Wahlperiode abgestellt werden, in der die Veränderung eingetreten ist.

## 7. Polizei

### a) Gesetzliche Regelung der Informationsverarbeitung

Die Innenministerkonferenz hat am 26. April 1985 beschlossen, einen von ihrem zuständigen Arbeitskreis vorgelegten Vorentwurf zur Änderung des Musterentwurfs eines einheitlichen Polizeigesetzes (Stand: 8. Februar 1985) zur Grundlage für die weitere Beratung zur Schaffung bereichsspezifischer Regelungen über die Datenerhebung und -verarbeitung der Polizei zu machen.

Die Schaffung solcher Regelungen ist grundsätzlich zu begrüßen; sie entspricht langjährigen Forderungen der Datenschutzbeauftragten. Der genannte Vorentwurf trägt jedoch den in dem Beschluß der Datenschutzbeauftragten vom 24. Januar 1985 dargelegten Anforderungen (vgl. sechster Tätigkeitsbericht, C.4.a) nur teilweise Rechnung.

Der Entwurf stellt darauf ab, daß die Datenerhebung und -verarbeitung der Polizei im bisherigen Umfang zur Erfüllung der polizeilichen Aufgaben erforderlich sei und deshalb auch in Zukunft in diesem Ausmaß zulässig sein müsse. Nach Auffassung der Datenschutzbeauftragten kann es jedoch nicht darum gehen, die derzeitige, durch eine Ausweitung der Datenverarbeitung gekennzeichnete Praxis festzuschreiben; diese muß vielmehr überprüft und der Umfang zulässiger Informationsverarbeitung begrenzt werden.

Bedenken bestehen insbesondere gegen

- den nach dem Entwurf zulässigen Umfang der Datenerhebung und -verarbeitung zur vorbeugenden Bekämpfung von Straftaten,
- den Umfang der Datenerhebung bei öffentlichen Versammlungen und aus Wohnungen,
- die Regelung für die „Vorsorge zur Gefahrenabwehr“,
- die Geltung der Einschränkungen der Speicherung nur für Dateien,
- das Fehlen einer Regelung für die automatisierte Datenverarbeitung,
- die nach meiner Auffassung mit dem Volkszählungsurteil des Bundesverfassungsgerichts nicht zu vereinbarenden Generalklauseln für die Übermittlung an andere öffentliche Stellen zur Erfüllung von Aufgaben dieser Stellen,
- das Fehlen einer dem Trennungsgebot entsprechenden Regelung für die Datenübermittlung an Nachrichtendienste,
- den vorgesehenen Wegfall der Prüfung der Voraussetzungen der Datenübermittlung durch die übermittelnde Stelle,
- die uneingeschränkte Zulassung des Datenabgleichs zur fahndungsmäßigen Überprüfung auch unverdächtiger Bürger,
- den nach dem Entwurf zulässigen Umfang der Rasterfahndung,
- die Beschränkung des Auskunftsanspruchs des Betroffenen auf Dateien,
- die Beschränkung der Löschungspflicht auf Dateien,
- die fehlende Festlegung von Fristen für die regelmäßige Löschung im Gesetz.

In weitgehender Übereinstimmung mit den Vorschlägen einer Arbeitsgruppe der Datenschutzbeauftragten habe ich in meiner Stellungnahme zu den einzelnen Vorschriften des Vorentwurfs entsprechende Änderungen vorgeschlagen.

### b) Datenerhebung

Auf die Eingabe eines Vaters hatte ich die Rechtmäßigkeit der erkennungs-

dienstlichen Behandlung seines strafunmündigen Sohnes durch eine Kreispolizeibehörde zu prüfen. Dieser war als 13jähriger zweimal wegen einfachen Diebstahls und einmal wegen Anstiftung eines anderen Jungen zum einfachen Diebstahl in Erscheinung getreten.

Die erkennungsdienstliche Behandlung eines strafunmündigen Kindes (bis zur Vollendung des 14. Lebensjahres) kann entgegen der Auffassung der Kreispolizeibehörde nicht auf die 2. Alternative des § 81b StPO gestützt werden, da diese Vorschrift voraussetzt, daß der Betroffene Beschuldigter ist, ein Strafunmündiger aber nicht Beschuldigter sein kann. Bei Strafunmündigen kommt als gesetzliche Grundlage für die erkennungsdienstliche Behandlung allein § 10 Abs. 1 Nr. 2 des Polizeigesetzes des Landes Nordrhein-Westfalen (PolG NW) in Betracht.

Nach dieser Vorschrift kann die Polizei erkennungsdienstliche Maßnahmen vornehmen, wenn dies zur vorbeugenden Bekämpfung von Straftaten erforderlich ist, weil der Betroffene verdächtig ist, eine Tat begangen zu haben, die mit Strafe bedroht ist und wegen der Art und Ausführung der Tat die Gefahr der Wiederholung besteht. Dies gilt grundsätzlich auch bei Strafunmündigen. Bei der Vornahme solcher Maßnahmen ist jedoch der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Danach hat die Polizei von mehreren geeigneten Maßnahmen diejenige zu treffen, die den Betroffenen am wenigsten belastet (§ 2 Abs. 1 PolG NW); die Maßnahme darf auch nicht zu einem Nachteil führen, der zu dem erstrebten Erfolg erkennbar außer Verhältnis steht (§ 2 Abs. 2 PolG NW). Hierzu wird in der Polizeidienstvorschrift für die Bearbeitung von Jugendsachen bestimmt, daß Kinder nur dann erkennungsdienstlich zu behandeln sind, wenn sie wiederholt Straftaten begangen haben, und daß dabei in Bezug auf die Art der Straftaten und die mögliche Entwicklung ein strenger Maßstab anzulegen ist.

Im vorliegenden Fall war bereits zweifelhaft, ob die vorgenommenen erkennungsdienstlichen Maßnahmen als erforderlich (§ 10 Abs. 1 Nr. 2 PolG NW) angesehen werden konnten. Zur vorbeugenden Bekämpfung weiterer Straftaten dürfte die Aufbewahrung von Merkblättern über die drei Vorfälle in der Jugendschutzakte genügen (§ 2 Abs. 1 PolG NW).

Auf jeden Fall steht bei der gebotenen Anlegung eines strengen Maßstabes in Bezug auf die Art der Straftaten die Belastung des Betroffenen durch die erkennungsdienstliche Behandlung außer Verhältnis zu dem erstrebten Erfolg (§ 2 Abs. 2 PolG NW). Zwar schließt der Verhältnismäßigkeitsgrundsatz die erkennungsdienstliche Behandlung von Kindern nicht schlechthin aus. Sie muß jedoch auf schwere Straftaten und ansonsten auf Fälle der gewohnheits- oder bandenmäßigen Begehung von Straftaten beschränkt bleiben. Auch wenn Ladendiebstahl nicht als Bagatelldelikt anzusehen ist, erscheinen erkennungsdienstliche Maßnahmen nach drei einfachen Diebstählen bei einem Kind unverhältnismäßig.

Unabhängig von der Beurteilung der Zulässigkeit der erkennungsdienstlichen Behandlung war die Weitergabe der dabei gefertigten Unterlagen an das Bundeskriminalamt nicht gerechtfertigt, da es sich nicht um überregional bedeutende Straftaten handelte.

Ich habe der Kreispolizeibehörde daher empfohlen, die bei ihr vorhandenen erkennungsdienstlichen Unterlagen über den Betroffenen zu vernichten, die Vernichtung der beim Landeskriminalamt und beim Bundeskriminalamt vorhandenen Unterlagen zu veranlassen und etwaige Hinweise auf diese Unterlagen in den polizeilichen Sammlungen und Dateien zu löschen oder ihre Löschung zu veranlassen. Da die Behörde meiner Empfehlung nicht gefolgt ist, habe ich die erkennungsdienstliche Behandlung, die Weitergabe der dabei gefertigten Unterlagen an das Landeskriminalamt und an das Bundeskriminalamt sowie die

Ablehnung der Vernichtung der Unterlagen gemäß § 30 Abs. 1 Satz 1 DSGVO beanstandet.

### **c) Datenspeicherung**

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Speicherung personengebundener Hinweise in den polizeilichen Informationssystemen erörtert und hierzu am 15. November 1985 folgenden Beschluß gefaßt:

Personengebundene Hinweise, d. h. Daten, die über die Identifizierungsfunktion hinausgehen und eine erste Einschätzung der gespeicherten Person ermöglichen sollen, finden sich zunehmend in polizeilichen Dateien. Im Bereich des Bundeskriminalamtes sind personengebundene Hinweise beispielsweise in den Dateien KAN, Haftdatei, Erkennungsdienst, Daktyloskopie, in den Falldateien sowie in anderen Dateien gespeichert. Auch in den Dateien der Länderpolizei sind derartige Hinweise enthalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, daß die Speicherung derartiger Hinweise die Gefahr der Ergreifung polizeilicher Maßnahmen nur auf Grund des Dateiinhalts hervorruft und daß sie ganz allgemein zu einer sozialen Abstempelung der betroffenen Person führen kann. Sie ist der Ansicht, daß polizeiliche Entscheidungen und insbesondere polizeiliches Einschreiten nur ausnahmsweise auf den Inhalt von Nachweisdateien gestützt werden dürfen, in der Regel jedoch Auskunft aus der Akte eingeholt werden muß. Die personengebundenen Hinweise sind keine geeignete Entscheidungsgrundlage, weil sie nur bruchstückhafte Informationen darstellen und ihre ständige Aktualisierung nicht gewährleistet ist.

Die Datenschutzbeauftragten halten die Speicherung derartiger Hinweise allenfalls dann für zulässig, wenn dies zur Erreichung des mit der betreffenden Datei verfolgten Zwecks im jeweiligen Einzelfall unabdingbar ist. Nach derzeitigem Erkenntnisstand dürfen personengebundene Hinweise also nur noch in solchen Dateien niedergelegt werden, die als alleinige Grundlage für ein polizeiliches Einschreiten in Betracht kommen (z. B. die Personenfahndungsdatei).

Die benutzten Begriffe müssen präzise definiert werden, um eine einheitliche Handhabung sicherzustellen und unangemessene Typisierungen von Betroffenen so weit wie möglich zu vermeiden. Es ist sicherzustellen, daß die vorgenommenen Bewertungen durch Tatsachen belegbar und nachvollziehbar sind. Die Aktualität der Hinweise muß innerhalb kurzer Fristen regelmäßig überprüft werden.

Nach derzeitigem Kenntnisstand sehen die Datenschutzbeauftragten bei einer Abwägung der erkennbaren Interessen der Polizei an schnell verfügbaren Informationen mit der Gefahr unangemessener Stigmatisierung der Betroffenen insbesondere die folgenden personengebundenen Hinweise nicht als erforderlich an:

- geistesschwach
- entmündigt
- Prostitution
- Internationaler Rechtsbrecher
- häufig wechselnder Aufenthalt
- Land- und Stadtreicher.

Diese Aufzählung ist nicht abschließend. Vielmehr müssen alle Kataloge zulässiger personengebundener Hinweise in den Informationssystemen der Polizei in Bund und Ländern auf ihre Erforderlichkeit hin überprüft werden.

Bereits in meinem fünften Tätigkeitsbericht (C.6.b) hatte ich empfohlen, von der Speicherung der Hinweise „Prostitution“ und „Land- oder Stadtstreicher“ abzusehen. Auf Grund der Erörterung durch die Datenschutzbeauftragten halte ich es für geboten, auch auf die Speicherung der anderen in dem Beschluß genannten Hinweise zu verzichten.

#### **d) Auskunft und Löschung**

- Die weitaus überwiegende Anzahl der Eingaben von Bürgern im Bereich der Polizei betrafen in diesem Berichtszeitraum wiederum die Frage, ob und in welchem Umfang bei diesen Behörden personenbezogene Daten über sie in Dateien gespeichert sind oder in Akten festgehalten werden.

In allen Fällen konnte dem Betroffenen Auskunft erteilt werden. In keinem Fall hat die Polizei von ihrem Auskunftsverweigerungsrecht nach § 16 Abs. 2 in Verbindung mit § 15 Abs. 2 Nr. 1 DSGVO Gebrauch gemacht. Die Auskünfte mancher Polizeibehörden sind aber noch zu pauschal abgefaßt. So wurde Bürgern lediglich mitgeteilt, daß personenbezogene Daten zu ihrer Person gespeichert seien, die sich auf die gegen sie gerichteten Strafverfahren beziehen. Nach einem Runderlaß des Innenministers vom 18. März 1982 müssen jedoch die einzelnen Verfahren bezeichnet werden. Die Polizeibehörden haben auf meine Empfehlung die erteilten Auskünfte entsprechend ergänzt.

- In zahlreichen Fällen war die Dauer der Aufbewahrung Kriminalpolizeilicher personenbezogener Sammlungen zu überprüfen. In mehreren Fällen wurden auf meine Veranlassung die über den Betroffenen geführten Kriminalakten ausgesondert und vernichtet und die entsprechenden Hinweise im automatisierten Informationssystem der Polizei gelöscht.

Bei meinen Prüfungen mußte ich auch in diesem Berichtszeitraum feststellen, daß fast ausschließlich die 10-Jahres-Frist nach Nr. 5.2.1 der KpS-Richtlinien als Frist für die Überprüfung zum Zwecke der Aussonderung von Kriminalakten eingegeben war. Diese in weiten Bereichen vorherrschende Praxis entspricht nicht den Vorgaben der KpS-Richtlinien. In von mir aufgegriffenen Fällen war die Polizei allerdings bereit, die Frist abzukürzen. Wie in meinem fünften (C.6.d) und sechsten (C.4.e) Tätigkeitsbericht ausgeführt, ist es aber geboten, bereits bei der Eingabe der Überprüfungsfrist verstärkt nach der Bedeutung der Straftat zu differenzieren.

#### **e) Polizeibeamte als Zeugen**

Das Land Nordrhein-Westfalen, vertreten durch einen Polizeipräsidenten, führte einen Zivilprozeß wegen einer Schadensersatzforderung. In diesem Prozeß sollte ein Polizeibeamter als Zeuge aussagen. Zur Vorbereitung seiner Zeugenaussage hatte der Polizeibeamte Einsicht in den bei dem Polizeipräsidenten angelegten Schadensersatzvorgang genommen und sich daraus Kopien angefertigt.

Eine gesetzliche Grundlage, die einem Zeugen ausdrücklich erlaubt, zur Vorbereitung seiner Zeugenaussage Akten oder sonstige Ermittlungsunterlagen einzusehen, ist nicht vorhanden. Nach § 396 Abs. 1 ZPO ist der Zeuge zu veranlassen, dasjenige, was ihm von dem Gegenstand seiner Vernehmung bekannt ist, im Zusammenhang anzugeben. Der Zeuge ist grundsätzlich nur zur Konzentration während der Vernehmung verpflichtet, nicht aber dazu, sich durch Nachforschungen, Auffrischung des Gedächtnisses usw. auf die Vernehmung vorzubereiten. Nur ausnahmsweise haben auch Zeugen eine der Vernehmung vorausgehende Vorbereitungspflicht, nämlich solche Personen, die in amtlicher Eigenschaft in der fraglichen Sache tätig gewesen sind und über die dabei gemachten

Wahrnehmungen aussagen sollen, wie etwa Polizeibeamte (vgl. Schönke-Schröder, StGB, 20. Aufl., § 163 Rdnr. 3).

Wenn man dieser Auffassung folgt, daß eine Vorbereitungspflicht eines Polizeibeamten auf seine Zeugenaussage besteht, kann dazu auch die Einsichtnahme in die die Aussage betreffenden polizeilichen Unterlagen erforderlich sein. An die Erforderlichkeit sind strenge Anforderungen zu stellen. So kann es als erforderlich angesehen werden, daß ein Polizeibeamter seine früher gemachte schriftliche Aussage oder seine Anzeige nochmals liest. Nicht erforderlich und nach meiner Auffassung daher unzulässig ist jedoch, daß er Einsicht in andere Zeugenaussagen oder Einlassungen des Beklagten oder des Beschuldigten nimmt, zumal die darin enthaltenen Angaben ihn bei seiner Zeugenaussage, die nur **sein** Wissen über bestimmte Tatsachen bekunden soll, beeinflussen können.

Für diese Auffassung spricht auch, daß nach § 299 ZPO nur die Parteien Prozeßakten einsehen können. Dritten Personen, also auch Zeugen, kann ohne Einwilligung der Parteien Einsicht in die Akten nur gestattet werden, wenn ein rechtliches Interesse glaubhaft gemacht wird. Dies muß auch dann gelten, wenn Prozeßunterlagen nicht nur in der Gerichtsakte festgehalten werden, sondern auch in polizeilichen Unterlagen.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich empfohlen, künftig Polizeibeamten zur Vorbereitung einer Zeugenaussage Einsicht in polizeiliche Ermittlungsvorgänge nur insoweit zu gewähren, als sie frühere eigene Aussagen betreffen. Dies gilt nicht nur für Verfahren, in denen das Land selbst Kläger ist, sondern für alle Verfahren, in denen Polizeibeamte als Zeugen auftreten.

## 8. Verfassungsschutz

### a) Anforderungen an Datenschutzregelungen

Gerade für die Datenverarbeitung der Verfassungsschutzbehörden sind präzise gesetzliche Grundlagen erforderlich, da sie in besonderem Maße in das informationelle Selbstbestimmungsrecht eingreift, weil sie fast vollständig im Geheimen und somit unter Ausschluß der Öffentlichkeit und der Kontrolle durch den Betroffenen stattfindet.

Ebenso wie im Polizeirecht kann es auch beim Verfassungsschutz nicht darum gehen, die derzeitige Praxis gesetzlich festzuschreiben. Vielmehr muß der Umfang zulässiger Informationsverarbeitung der Verfassungsschutzbehörden auf der Grundlage des Volkszählungsgesetzesurteils des Bundesverfassungsgerichts überprüft und durch spezielle Aufgaben- und Befugnisnormen konkretisiert und begrenzt werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben am 13. September 1985 einen Beschluß über die Mindestanforderungen für die Neuregelung gefaßt:

1. Die Regelung der Informationsverarbeitung durch den Verfassungsschutz muß den Anforderungen der **Normenklarheit** entsprechen. Da über die Datenverarbeitung im Einzelfall meist nichts bekannt wird, ist es für den Bürger von besonderer Bedeutung, daß er den gesetzlichen Bestimmungen entnehmen kann, aus welchem Anlaß, in welcher Form und zu welchem Zweck der Verfassungsschutz personenbezogene Daten verarbeiten darf.

Diese Vorschriften müssen zwischen den unterschiedlichen Aufgaben der Verfassungsschutzbehörden differenzieren. Was beispielsweise für die Abwehr von Spionen vertretbar ist, ist nicht auch für die Mitwirkung an Sicherheitsüberprüfungen angemessen.

Der Grundsatz der Zweckbindung gilt auch für die Verfassungsschutzbehörden. Das bedeutet: Angesichts der Vielfalt ihrer Aufgaben reicht eine pauschale Bindung an „Zwecke des Verfassungsschutzes“ nicht aus. Vielmehr dürfen die für die unterschiedlichen Aufgaben erhobenen Daten grundsätzlich nur für die jeweilige Aufgabe verwendet werden. Die Regelung der Verarbeitung personenbezogener Daten durch den Verfassungsschutz muß die Erhebung sowie jegliche andere Art der Verarbeitung und Verwendung einbeziehen.

Regelungsbedürftig sind auch die Voraussetzungen für die jeweilige Form der Datenverarbeitung: Wesentliche Schritte der Automatisierung sollten beispielsweise nur zugelassen werden, wenn diese für die Erfüllung der jeweiligen Aufgabe gerechtfertigt sind und hierdurch schutzwürdige Belange der Betroffenen nicht unverhältnismäßig beeinträchtigt werden. Dies gilt insbesondere für Systeme der Datenverarbeitung, die über einen Aktennachweis hinausgehen oder durch Übernahme von Akteninhalten neue Verwendungs- und Verknüpfungsmöglichkeiten eröffnen.

Für jede automatisierte oder manuelle Datei ist eine detaillierte Errichtungsanordnung zu erlassen.

2. Der Einsatz **nachrichtendienstlicher Mittel** muß klar geregelt sein. Dies gilt sowohl für die Voraussetzungen der Anwendung als auch für die Frage, gegen wen nachrichtendienstliche Mittel eingesetzt werden dürfen. Die nachrichtendienstlichen Mittel sollten soweit wie möglich gesetzlich festgelegt werden. Zumindest sollten die Verfassungsschutzbehörden verpflichtet werden, alle in Frage kommenden Mittel im einzelnen intern zu beschreiben und ihren Einsatz zu dokumentieren. Die Anwendung nachrichtendienstlicher Mittel entbindet nicht von der Beachtung der allgemeinen Rechtsordnung.

Holt der Verfassungsschutz bei anderen Behörden **Auskünfte** ein, so soll er sein Ersuchen begründen, wenn nicht besondere Gründe entgegenstehen (z. B. schutzwürdige Belange des Betroffenen oder Sicherheitsinteressen des Staates). Entfällt danach die Begründung, so sind die Gründe des Ersuchens intern zu dokumentieren. Für Kontrollzwecke sollte ein eigenes Verzeichnis eingerichtet werden.

Eine Verpflichtung anderer Behörden, dem Verfassungsschutz von sich aus Informationen zu übermitteln, muß auf solche Bestrebungen beschränkt werden, die auf Anwendung von Gewalt oder geheimdienstliche Tätigkeit gerichtet sind. Darüber hinaus dürfen Behörden von sich aus nur unter weiteren gesetzlich festzulegenden Einschränkungen den Verfassungsschutz über personenbezogene Vorgänge informieren. Übermittlungen „auf Verdacht“ sind unzulässig und können sich schädlich für das Verhältnis des Bürgers zu den Behörden auswirken.

Bei der Regelung der Informationsbeziehungen zwischen Polizei und Verfassungsschutz ist das verfassungskräftige Trennungsgebot zu beachten, das inhaltlicher ebenso wie organisatorischer Natur ist. Der Verfassungsschutz darf deshalb die Polizei z. B. nicht um Maßnahmen ersuchen, die die Anwendung polizeilicher Befugnisse erfordern. On-line-Verbindungen zwischen Polizei und Verfassungsschutz sind mit dem Trennungsgebot nicht vereinbar. Ein geeigneter Maßstab für Datenübermittlungen der Polizei an den Verfassungsschutz im Einzelfall sind die Verwertungsregelungen nach dem Gesetz zu Artikel 10 Grundgesetz.

Es ist sicherzustellen, daß spezielle Verwertungsbestimmungen – z. B. des Strafverfahrensrechts – beachtet werden; dies gilt z. B. für Erkenntnisse, die im Rahmen der Telefonüberwachung oder bei Durchsuchungen gewonnen wurden.

3. Die Befugnis zur **Speicherung** ist differenziert nach den unterschiedlichen Aufgabenbereichen zu regeln.

So muß der Extremismusbezug in der Person desjenigen erfüllt sein, dessen Daten personenbezogen auswertbar im Rahmen der Extremismusbeobachtung gespeichert werden sollen. Hierbei ist außerdem zu beachten, daß Personendaten nur gespeichert werden dürfen, wenn dies zum Zwecke der Beobachtung extremistischer Bestrebungen erforderlich ist. Der Praxis, die immer mehr von der Beobachtung von Organisationen zur Erfassung von Einzelpersonen übergeht, muß entgegengewirkt werden.

Die Gründe für eine Speicherung müssen aus den Unterlagen des Verfassungsschutzes nachvollziehbar sein. Werden Bewertungen gespeichert, so muß erkennbar sein, wer sie vorgenommen hat und welche Unterlagen ihnen zugrundeliegen.

Es sind gesetzliche Regelfristen für die Überprüfung und Löschung der gespeicherten Daten festzulegen. Dabei ist zwischen den einzelnen Aufgabenbereichen (etwa Extremismusbeobachtung/Spionageabwehr), nach der Relevanz der einzelnen Informationen (etwa vager Verdacht/gesicherte Informationen) sowie nach dem Alter der Betroffenen zu differenzieren. Dies gilt auch für die Speicherung in Akten.

4. Im Rahmen von **Sicherheitsüberprüfungen** werden sowohl beim Verfassungsschutz als auch bei einer Reihe weiterer Stellen Daten erhoben und verarbeitet. Hierfür sind besondere gesetzliche Grundlagen erforderlich. Für die Mitwirkung des Verfassungsschutzes sind folgende Prinzipien zu beachten:

Die Sicherheitsüberprüfungen sind auf das erforderliche Maß zu beschränken. Dies gilt insbesondere für die Intensität der Prüfung, die sich nach der Gefährdung im Einzelfall richten muß.

Die Sicherheitsüberprüfung soll erst durchgeführt werden, wenn nur noch davon die Aufnahme der sicherheitsrelevanten Tätigkeit abhängig ist. Für den personellen Sabotageschutz ist zudem die exakte Beschreibung der sicherheitsempfindlichen Bereiche und die Begrenzung der Überprüfung auf tatsächlich in diesem Bereich eingesetzte Personen zu fordern.

Die Verfahrensregelungen müssen andere Ermittlungsformen ausschließen.

Im Rahmen der Sicherheitsüberprüfung ist es nicht Aufgabe des Verfassungsschutzes, die Auskünfte aller beteiligten Stellen zu koordinieren.

Die Voraussetzungen, unter denen im Rahmen der Sicherheitsüberprüfung auch Nachforschungen über Dritte angestellt werden dürfen, sind gesetzlich festzulegen. Soweit Dritte, z. B. Ehegatten, einbezogen werden, ist deren Einwilligung erforderlich. Die Speicherung von Daten über diese Personen ist auf ein Minimum zu beschränken und darf grundsätzlich nicht personenbezogen erschließbar sein.

Das Verfahren muß für die Betroffenen (einschließlich der Dritten) transparent sein. Sie sind über die Tatsache, den Ablauf, die beteiligten Stellen und das Ergebnis der Sicherheitsüberprüfung zu unterrichten. Im Fall von Sicherheitsbedenken ist dem Überprüften Gelegenheit zur Stellungnahme zu geben. Ausnahmen von dieser Unterrichtungspflicht sind eng zu fassen. Auch Auskunftspersonen sind über den Zweck der Befragung zu unterrichten, um Fehlschlüsse zu Lasten des Betroffenen zu vermeiden, und auf die Freiwilligkeit ihrer Angaben hinzuweisen.

Stellt der Betroffene einen Auskunftsantrag nach den Datenschutzgesetzen, so ist diesem zu entsprechen, soweit die Speicherung im Rahmen der Sicherheitsüberprüfung erfolgt ist.

Die speziell für die Sicherheitsüberprüfung beim Betroffenen oder bei anderen Stellen erhobenen Daten dürfen in der Regel nur für diesen Zweck verwendet werden. Die Trennung von Sicherheits- und Personalakten ist strikt zu wahren.

5. Verfassungsschutzbehörden dürfen untereinander personenbezogene Daten nur austauschen, soweit dies zu ihrer jeweiligen gesetzlich festgelegten Aufgabenerfüllung erforderlich und verhältnismäßig ist.

Die **Übermittlung** personenbezogener Daten durch den Verfassungsschutz an andere Sicherheitsbehörden (z. B. Polizei, Staatsanwaltschaft, BND u. a.) muß unter Beachtung des Zweckbindungsgrundsatzes präziser und restriktiver als in den derzeit praktizierten Zusammenarbeitsrichtlinien in Staatsschutzsachen geregelt werden. Die Voraussetzungen einer Übermittlung müssen konkret festgelegt werden. Allein die Begründung, daß die Übermittlung mit „dem Zweck des Verfassungsschutzes“ vereinbar sei, ist nicht ausreichend. An Strafverfolgungsbehörden darf der Verfassungsschutz Informationen, die er mit nachrichtendienstlichen Mitteln erlangt hat, nur weitergeben, wenn tatsächliche Anhaltspunkte für die Einleitung eines Ermittlungsverfahrens wegen einer Straftat der in § 7 Abs. 3 des Gesetzes zu Artikel 10 Grundgesetz genannten Art vorliegen.

Eine Übermittlung an andere Behörden kann nur zur Erfüllung eigener Aufgaben des Verfassungsschutzes in Betracht kommen. Ausnahmen bedürfen einer gesetzlichen Regelung.

Eine Übermittlung von personenbezogenen Daten an private Stellen (z. B. Firmen, Gewerkschaften, Parteien) ist nur im Rahmen der gesetzlich vorgesehenen Sicherheitsüberprüfungen und nur in dem dafür unerläßlichen Rahmen oder aus Gründen der Spionage- und Terrorismusabwehr zulässig. Bei Übermittlungen außerhalb der Sicherheitsüberprüfung ist außerdem die Zustimmung der obersten Dienstbehörde einzuholen.

Eine Übermittlung an ausländische Dienststellen einschließlich der Nachrichtendienste ist an besonders enge Voraussetzungen zu knüpfen. Es ist – längerfristig durch völkerrechtliche Übereinkommen – zu gewährleisten, daß im Inland geltende Schutzrechte des Betroffenen nicht gefährdet werden.

Vor jeder Übermittlung hat die auskunftgebende Verfassungsschutzbehörde die Richtigkeit der vorhandenen Unterlagen und deren Erforderlichkeit für die eigene Aufgabenerfüllung zu überprüfen. In allen Fällen ist die Übermittlung personenbezogener Daten zu dokumentieren. Über die Änderung wesentlicher Gesichtspunkte ist die Empfängerbehörde zu unterrichten, soweit dadurch nicht schutzwürdige Belange des Betroffenen beeinträchtigt werden.

Eine Unterrichtung der Öffentlichkeit über personenbezogene Erkenntnisse des Verfassungsschutzes ist grundsätzlich ausgeschlossen.

6. Die Verfassungsschutzbehörden dürfen **Auskunftsersuchen der Bürger** nicht, wie dies derzeit die meisten Ämter handhaben, schematisch ablehnen. Der Gesetzgeber sollte daher von folgenden Grundsätzen ausgehen:

Die Auskunft ist zu erteilen

- in aller Regel, wenn die Speicherung nur auf einer Sicherheitsüberprüfung beruht,
- im übrigen nach Abwägung im Einzelfall.

Im Falle einer Auskunftsverweigerung sind die Gründe im einzelnen zu dokumentieren.

Die Bearbeitung von Auskunftsersuchen muß getrennt von anderen Informationssammlungen erfolgen. Die Tatsache der Antragstellung darf nicht zum Nachteil der Betroffenen verwertet werden.

7. Die **Kontrollkompetenz der Datenschutzbeauftragten** erstreckt sich auf die gesamte Datenverarbeitung der Verfassungsschutzbehörden und umfaßt auch Akten und sonstige Unterlagen. Auch die Datenverarbeitung im Rahmen des Gesetzes zu Artikel 10 Grundgesetz muß der Kontrolle der Datenschutzbeauftragten unterliegen. Dies ist unerlässlich für die Durchsetzung des Rechts auf informationelle Selbstbestimmung gerade im Bereich des Verfassungsschutzes.

Diese Mindestanforderungen müssen in einem neuen Bundesverfassungsschutzgesetz berücksichtigt werden. Auf ihrer Grundlage ist aber auch eine Überprüfung des Verfassungsschutzgesetzes Nordrhein-Westfalen und der von der Landesregierung hierzu vorgeschlagenen Änderungen notwendig.

#### **b) Bundesverfassungsschutzgesetz und Zusammenarbeitsgesetz**

Die Fraktionen der CDU/CSU und FDP haben im Deutschen Bundestag den Entwurf eines Bundesverfassungsschutzgesetzes eingebracht (Bundestagsdrucksache 10/4737, Artikel 3). Dieser Entwurf trägt den dargelegten Anforderungen an Datenschutzregelungen für den Verfassungsschutz nur zu einem geringen Teil Rechnung und weist schwerwiegende Mängel auf.

So kann dem Bürger nach wie vor jede Auskunft verweigert werden. Es fehlen gesetzliche Fristen für die Löschung personenbezogener Daten. Dem Verfassungsschutz darf nicht das Recht zugestanden werden, in jedes amtliche Register Einsicht zu nehmen und jede Art von Daten anzufordern; im Gesetzentwurf sind davon nicht einmal Gesundheits- und Steuerdaten ausgenommen. Während sich das nachrichtendienstliche Informationssystem bisher auf die Speicherung von Aktennachweisen beschränkte, sollen nach dem Gesetzentwurf auch Textzusätze mit Informationen über den Bürger den Nachrichtendiensten bundesweit automatisiert zur Verfügung stehen. Damit werden zulasten des Bürgers Akteninhalte verkürzt und aus ihrem Entstehungszusammenhang herausgenommen.

Ferner hat die Bundesregierung im Bundesrat den Entwurf eines Gesetzes über die informationelle Zusammenarbeit der Sicherheits- und Strafverfolgungsbehörden in Angelegenheiten des Staats- und Verfassungsschutzes und nachrichtendienstlicher Tätigkeit (Zusammenarbeitsgesetz) eingebracht (Bundesratsdrucksache 66/86).

Die rechtsstaatlichen Grenzen der Zusammenarbeit von Nachrichtendiensten und Polizei werden durch das Trennungsgebot bestimmt. Dieses erschöpft sich nicht in einer bloßen organisatorischen Trennung zwischen Nachrichtendiensten und Polizei. Die Nachrichtendienste dürfen die Polizei auch nicht um Maßnahmen ersuchen, zu denen sie selbst nicht befugt sind. Deshalb bestehen erhebliche Bedenken insbesondere gegen die in dem Gesetzentwurf vorgesehene Befragung von Reisenden bei der Grenzkontrolle für Zwecke der Nachrichtendienste.

#### **c) Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen**

In meinem sechsten Tätigkeitsbericht (C.1.c) habe ich zu der Einsichtnahme der Verfassungsschutzbehörde in Meldekarteien für Zwecke der Spionageabwehr Stellung genommen. Ich habe dargelegt, daß das Meldegesetz eine solche Einsichtnahme nicht zuläßt und deshalb dem berechtigten Informationsbedürfnis des Verfassungsschutzes auf eine datenschutzrechtlich zulässige Weise Rechnung getragen werden muß.

Inzwischen hat der Landtag durch das von ihm am 12. Dezember 1985 beschlossene Gesetz zur Änderung des Verfassungsschutzgesetzes Nordrhein-Westfalen für die Einsichtnahme des Verfassungsschutzes in derartige

Dateien eine gesetzliche Grundlage geschaffen. Mit diesem Gesetz werden die nach bisherigem Recht zulässigen Datenübermittlungen an die Verfassungsschutzbehörde wesentlich erweitert. Durch die Einsichtgewährung in die von öffentlichen Stellen geführten Register werden der Verfassungsschutzbehörde erheblich mehr Daten übermittelt, als sie zur Erfüllung ihrer Aufgaben braucht; sie kann damit von sämtlichen dort gespeicherten Daten aller Einwohner Kenntnis nehmen, obwohl sie nur einen kleinen Teil dieser Daten benötigt.

Gegen eine derartige Regelung, durch die einer anderen Stelle eine ganze Datei zur Einsicht zur Verfügung gestellt wird, bestehen grundsätzliche Bedenken. Dabei ist insbesondere zu berücksichtigen, daß der Umfang der Einsichtnahme und damit die tatsächliche Kenntnisnahme von Daten durch die Mitarbeiter der Verfassungsschutzbehörde praktisch nicht kontrollierbar ist. Wegen dieser Bedenken haben der Bundesgesetzgeber in § 24 des Melderechtsrahmengesetzes (MRRG) und der Landesgesetzgeber in § 43 des Melderechtsrahmengesetzes für das Land Nordrhein-Westfalen (MG NW) die Einsichtnahme der Polizei in das Melderegister (sog. Schlüsselösung) nur für eine Übergangszeit bis zum 31. Dezember 1985 zugelassen.

Aus der Sicht des Datenschutzes kann daher die in dem Gesetz geregelte Einsicht des Verfassungsschutzes in von öffentlichen Stellen geführte Register nicht gutgeheißen werden.

Soweit Einsicht in das Melderegister gewährt wird, bestehen darüber hinaus Zweifel, ob das Gesetz mit dem Melderechtsrahmengesetz vereinbar ist. Der Bundesgesetzgeber hat in § 18 MRRG im einzelnen festgelegt, unter welchen Voraussetzungen und nach welchen Verfahren der Landesgesetzgeber Datenübermittlungen an andere öffentliche Stellen zulassen darf; dem entspricht die Regelung in § 31 MG NW. Ferner hat der Bundesgesetzgeber in § 24 MRRG abweichend von § 18 MRRG für eine Übergangszeit die Einsichtnahme der Polizei in das Melderegister vorgesehen. Dies legt den Schluß nahe, daß nach dem Willen des Bundesgesetzgebers weitere Abweichungen von § 18 MRRG, insbesondere weitere eine Einsichtnahme in der Melderegister zulassende Regelungen ausgeschlossen werden sollen. Jedenfalls besteht insoweit ein verfassungsrechtliches Risiko.

Dem berechtigten Informationsbedürfnis der Verfassungsschutzbehörde sollte auf andere Weise Rechnung getragen werden. Ich habe daher vorgeschlagen, daß, soweit die Bekanntgabe des zu überprüfenden Personenkreises oder der Merkmale für die Auswertung der Register gegenüber der registerführenden Stelle die Aufgabenerfüllung des Verfassungsschutzes beeinträchtigen würde, die Auswertung durch nicht dem Verfassungsschutz angehörende Bedienstete (etwa solche des Regierungspräsidenten) erfolgen könnte, die für die Dauer der Auswertung zur registerführenden Stelle abgeordnet werden. Bei einem solchen Verfahren fände keine Einsichtnahme durch die Verfassungsschutzbehörde sondern nur eine nach § 31 Abs. 1 Satz 1 MG NW zulässige Übermittlung an diese Behörde statt. Der Gesetzgeber ist diesem Vorschlag nicht gefolgt. Er hat eine Einsichtgewährung an die Verfassungsschutzbehörde für erforderlich gehalten.

Für diesen Fall hatte ich dem Landtag vorgeschlagen, die Einsichtgewährung auf die Melderegister, die Personalausweisregister und die Paßregister zu beschränken und nur für Zwecke der Spionageabwehr zuzulassen. Im Hinblick auf die Vielzahl der als Register bezeichneten Datensammlungen verlangt nach meiner Auffassung das Gebot der Normenklarheit, die Register, in die Einsicht genommen werden darf, im Gesetz abschließend aufzuführen. Ein Bedürfnis für eine Einsichtnahme in andere als die drei genannten Register ist nach den Ausführungen des Innenministers im Gesetzgebungsverfahren ebensowenig zu erkennen, wie eine Notwendigkeit für die im Gesetz vorgesehene Ausweitung

auf den Bereich der Terrorismusbekämpfung. Leider ist der Landtag auch insoweit meinen Vorschlägen nicht gefolgt.

Zu begrüßen sind die im Gesetz getroffenen verfahrensmäßigen Vorkehrungen. So wurde entsprechend meinem Vorschlag festgelegt, daß die Verfassungsschutzbehörde über die Einsichtnahme einen gesonderten Nachweis zu führen hat, um einen Einstieg für die datenschutzrechtliche Kontrolle zu ermöglichen. Die Anordnung der Maßnahmen ist dem Minister oder seinem ständigen Vertreter vorbehalten. Eine Einsichtnahme wurde ausdrücklich ausgeschlossen, wenn eine besondere gesetzliche Geheimhaltungsvorschrift oder ein Berufsgeheimnis entgegensteht.

#### d) Auskunft und Löschung

- Zahlreiche Bürgereingaben betrafen die Frage, ob und gegebenenfalls welche personenbezogenen Daten beim Verfassungsschutz festgehalten oder von ihm übermittelt worden 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 Verfassungsschutzbehörde. Diese hat ein Auskunftsverweigerungsrecht.

Das Auskunftsverweigerungsrecht bedeutet nicht, daß die genannte Behörde keine Auskunft erteilen darf. Sie hat vielmehr nach pflichtgemäßem Ermessen zu entscheiden, ob und inwieweit sie dem Auskunftsantrag eines Betroffenen entsprechen will. Dabei ist ein öffentliches Interesse an der Geheimhaltung gegen das Auskunftsinteresse des Betroffenen abzuwägen. Bei Auskunftersuchen an die Verfassungsschutzbehörde wird allerdings zumeist das Geheimhaltungsinteresse überwiegen.

Gleichwohl war es in manchen Fällen möglich, dem Betroffenen Auskunft zu geben. In einigen Fällen konnte erreicht werden, daß zu einer Person gespeicherte personenbezogene Daten gelöscht wurden, da diese zur Aufgabenerfüllung nicht mehr erforderlich waren.

## 9. Bauwesen

- Eine Bauaufsichtsbehörde gab personenbezogene Daten aus erteilten **Baugenehmigungen** an ein Elektrizitätswerk weiter. Die Bauherren wurden von dem Elektrizitätswerk unter Beifügung eines Formularsatzes „Anmeldung für die Stromversorgung“ angeschrieben. Dabei betrieb das Elektrizitätswerk Werbung.

Die Bekanntgabe von Angaben aus Baugenehmigungen an die genannten Stellen ist ein Eingriff in das Grundrecht der Betroffenen auf Schutz ihrer personenbezogenen Daten nach Artikel 4 Abs. 2 der Landesverfassung sowie in ihr Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes, der einer gesetzlichen Grundlage bedarf. Eine solche ist nicht vorhanden.

§ 13 Abs. 1 Satz 1 DSG NW kommt als gesetzliche Grundlage für die Weitergabe schon deswegen nicht in Betracht, weil die Vorschrift nur für in Dateien gespeicherte, nicht aber für lediglich in Akten festgehaltene Daten gilt. Im übrigen kann die 2. Alternative des § 13 Abs. 1 Satz 1 DSG NW jedenfalls seit dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 nicht mehr als gesetzliche Grundlage für Datenübermittlungen herangezogen werden, wenn – wie hier – lediglich

ein einfaches berechtigtes Interesse des Empfängers besteht, da es in diesen Fällen an dem vom Bundesverfassungsgericht für einen Eingriff in die genannten Grundrechte geforderten überwiegenden Interesse der Allgemeinheit fehlt. Die Bekanntgabe personenbezogener Daten aus Baugenehmigungen an diese Stelle muß daher unterbleiben.

- Eine Architektenkammer wandte sich an den zuständigen Regierungspräsidenten mit der Bitte, ihr die Namen derjenigen freiberuflichen Architekten zu benennen, die Bauunterlagen zur Genehmigung vorgelegt hatten, bei denen Behördenmitarbeiter als Planverfasser tätig waren. Die Kammer begründete ihr Ersuchen damit, die Daten seien für die Überprüfung der Einhaltung der Berufsordnung durch ihre Mitglieder erforderlich. Der Regierungspräsident ist dem Anliegen der Kammer nicht nachgekommen.

Eine dem Gebot der Normenklarheit entsprechende gesetzliche Grundlage für die Bekanntgabe der gewünschten Daten an die Architektenkammer ist nicht ersichtlich. Insbesondere kann die Bekanntgabe nicht auf § 9 Abs. 1 des Architektengesetzes gestützt werden. Nach dieser Vorschrift hat zwar die Architektenkammer unter anderem die Aufgabe, die beruflichen Belange der Gesamtheit der Mitglieder zu wahren und die Erfüllung der beruflichen Pflichten zu überwachen. Die Vorschrift läßt jedoch in keiner Weise erkennen, daß zur Erfüllung dieser Aufgabe andere Stellen personenbezogene Daten übermitteln dürfen. Auch die Vorschriften über die Amtshilfe können nach dem Urteil des Bundesverfassungsgerichts als gesetzliche Grundlage für eine Datenübermittlung nicht mehr herangezogen werden, da sie dem Gebot der Normenklarheit nicht entsprechen.

Ich verkenne nicht, daß die Architektenkammer hier zur Erfüllung ihrer Aufgaben auf die Übermittlung personenbezogener Daten angewiesen ist. Solange der Gesetzgeber eine gesetzliche Regelung für eine Datenübermittlung nicht getroffen hat, ist sie jedoch unzulässig. Sie kann bis zur Schaffung einer gesetzlichen Regelung auch nicht auf einen wie auch immer gearteten „Übergangsbonus“ gestützt werden. Das Bundesverfassungsgericht hat die Notwendigkeit einer Übergangsfrist in Fällen gewandelter Verfassungsinterpretation nur als Ausnahme anerkannt, um eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen zu vermeiden, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand (BVerfGE 33, 12, 347; 41, 267). Von einer solchen der verfassungsmäßigen Ordnung noch ferner stehenden Funktionsunfähigkeit staatlicher Einrichtungen kann bei einem zeitweiligen Verzicht auf die Datenübermittlung keine Rede sein. Eine Ausweitung der vom Bundesverfassungsgericht anerkannten Ausnahme halte ich nicht für gerechtfertigt.

## 10. Rechtswesen

### a) Strafsachen

- In einer Eingabe hat sich ein Betroffener dagegen gewandt, daß ein Amtsgericht in einem Beschluß über die Anordnung erkennungsdienstlicher Maßnahmen nach § 81b StPO die Namen, Anschriften, Geburtsdaten und Dienstbezeichnungen aller Beschuldigten aufgeführt hatte. Jeder der zahlreichen Beschuldigten hatte durch die Zustellung dieses Beschlusses Kenntnis von den personenbezogenen Daten der anderen Beschuldigten erhalten.

Zwar erstreckt sich meine Kontrollbefugnis nicht auf das Amtsgericht, da dieses keine Verwaltungsaufgaben wahrgenommen hat, sondern als Organ der Rechtspflege tätig geworden ist (§ 32 Abs. 1 Nr. 1 DSG NW). Die Staatsanwaltschaft hatte jedoch den Beschluß in dieser Form beantragt und ihn

allen Beschuldigten zugestellt, so daß sie die Bekanntgabe der darin enthaltenen Daten an Dritte mit zu verantworten hat. Die Staatsanwaltschaft unterliegt meiner Kontrolle auch insoweit, als sie nicht Verwaltungsaufgaben wahrnimmt (C.8.a meines ersten, C.11.a meines zweiten Tätigkeitsberichts; Bericht des Ausschusses für Innere Verwaltung, Drucksache 9/1314, S. 12).

Die Bekanntgabe der in dem Beschluß enthaltenen, zum Teil höchst sensiblen personenbezogenen Daten eines Beschuldigten an die anderen Beschuldigten stellt einen Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch in sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung dar. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage, die nach dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 dem Gebot der Normenklarheit entsprechen muß; darüber hinaus ist der Grundsatz der Verhältnismäßigkeit zu beachten.

Eine diesen Anforderungen entsprechende gesetzliche Grundlage für die Bekanntgabe der genannten Daten an andere Beschuldigte ist nicht ersichtlich. Insbesondere können die Vorschriften der Strafprozeßordnung über die Verbindung zusammenhängender Strafsachen bei der Erhebung der Anklage oder nach Eröffnung des Hauptverfahrens (§§ 2 bis 4 StPO) hier nicht herangezogen werden, da sie keine Regelung für das Ermittlungsverfahren vor Erhebung der Anklage enthalten. Zur Durchführung der nach § 81b StPO angeordneten Maßnahmen ist ein gemeinsamer Beschluß gegen alle Beschuldigten nicht erforderlich.

Auf jeden Fall belastet ein solcher allen Beschuldigten zuzustellender Beschluß den einzelnen unverhältnismäßig. Dabei ist zu berücksichtigen, daß die Ermittlungen ergeben können, daß kein genügender Anlaß zur Erhebung der öffentlichen Klage besteht, etwa weil der Betroffene als Täter nicht in Frage kommt. Der Umstand, in den Verdacht der Begehung einer Straftat gekommen zu sein, ist dann aber schon vielen bekannt.

Daher sollte für jeden Beschuldigten ein gesonderter Beschluß beantragt, erlassen und zugestellt werden. Ich verkenne nicht, daß dies zu einer Mehrbelastung der Justizbehörden führen würde, halte ein solches Verfahren aber zur Vermeidung einer Verletzung der genannten Grundrechte für geboten.

Der Justizminister setzt die Verbindung zusammenhängender Strafsachen nach den §§ 2 bis 4 StPO auch schon im Stadium des Ermittlungsverfahrens als selbstverständlich voraus. Daß hierbei die verschiedenen Beschuldigten im Laufe des Verfahrens unter Umständen einzelne Angaben über einander erfahren, die ihnen bisher unbekannt waren, sei eine notwendige Folge.

Dieser Auffassung kann ich nicht folgen. Die Erwägungen des Justizministers können die fehlende normenklare gesetzliche Grundlage für eine für die Durchführung der Ermittlungen nicht erforderliche Bekanntgabe personenbezogener Daten eines Beschuldigten an andere Beschuldigte nicht ersetzen. Im übrigen halte ich an meiner Auffassung fest, daß eine solche Bekanntgabe dem Verhältnismäßigkeitsgrundsatz widerspricht.

- Der gesetzlichen Vertreterin eines minderjährigen Angeklagten wurde eine Anklageschrift zugestellt, in der neben ihrem jetzigen Namen auch ihr Geburtsname und ihre früheren Namen mit dem Zusatz „geschiedene“ angegeben waren. Da es sich um ein Strafverfahren gegen mehrere Angeklagte handelte, erhielten alle Angeklagten bzw. deren gesetzliche Vertreter davon Kenntnis, daß sie zweimal geschieden war.

Nach § 200 Abs. 1 StPO hat die Anklageschrift den Angeschuldigten, die Tat, die ihm zur Last gelegt wird, Zeit und Ort ihrer Begehung, die gesetzlichen

Merkmale der Straftat und die anzuwendenden Strafvorschriften zu bezeichnen. Für die Bezeichnung des Angeschuldigten sind nach Nr. 110 Abs. 2 der Richtlinien für das Strafverfahren und das Bußgeldverfahren der Familienname und die Vornamen, Geburtstag und Geburtsort und seine Staatsangehörigkeit anzugeben, bei Minderjährigen Name und Anschrift des gesetzlichen Vertreters. Für die Angabe früherer Namen des gesetzlichen Vertreters ist eine gesetzliche Grundlage nicht vorhanden. Die Angabe früherer Namen ist nach meiner Auffassung auch nicht erforderlich. Für die Identifizierung des gesetzlichen Vertreters reichen dessen derzeitiger Familienname, Vorname und Anschrift in aller Regel aus.

#### **b) Ordnungswidrigkeitenverfahren**

In mehreren Fällen, in denen Autofahrern wegen einer Verkehrsordnungswidrigkeit ein Verwarnungsgeld auferlegt worden war, erhielten diese zusammen mit dem Vordruck für das Verwarnungsgeld eine vorbereitete Zahlkarte mit dem Aufdruck „Verwarnung Nummer“. Durch die Benutzung der Zahlkarte kann Postbediensteten bei der Einzahlung oder Überweisung des Betrages durch den Betroffenen bekannt werden, daß dieser ein Verwarnungsgeld zu zahlen hat. In einem Fall wurde sogar als Vordruck für das Verwarnungsgeld die Rückseite der Zahlkarte verwendet. Hierbei konnte der Postbedienstete während des Zahlungsvorgangs von dem Autokennzeichen, dem Fabrikat des Autos sowie Tag, Ort, Uhrzeit und Grund der Verkehrsordnungswidrigkeit Kenntnis nehmen.

Nach Artikel 4 Abs. 2 der Landesverfassung hat jeder Anspruch auf Schutz seiner personenbezogenen Daten. Dieses Grundrecht verbietet den Behörden nicht nur, personenbezogene Daten ohne gesetzliche Grundlage oder Einwilligung des Betroffenen selbst weiterzugeben. Es verpflichtet sie auch, die technischen und organisatorischen Maßnahmen zu treffen, die zum Schutz der Daten gegen unbefugte Kenntnisnahme durch Dritte erforderlich sind. Dazu gehören auch organisatorische und gegebenenfalls technische Maßnahmen zum Schutz des Bürgers vor Kenntnisnahme seiner personenbezogenen Daten durch Dritte, wie etwa Postbedienstete bei der Einzahlung oder Überweisung eines Verwarnungsgeldes. Erforderlich sind derartige Maßnahmen allerdings nur, wenn der Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Dieser ist wiederum abhängig von dem Grad der Geheimhaltungsbedürftigkeit der jeweiligen Daten.

Da zur Verbuchung überwiesener Beträge die Angabe der Verwarnungsnummer als solche ausreicht, habe ich empfohlen, auf den Aufdruck „Verwarnung Nummer“ zu verzichten. Ferner habe ich in dem einen Fall empfohlen, für die Verwarnung einen gesonderten Vordruck zu verwenden, der bei dem Betroffenen verbleibt. Hinsichtlich des Aufdrucks „Verwarnung Nummer“ wird meiner Empfehlung bereits gefolgt.

#### **c) Zivilsachen**

- In meinem fünften Tätigkeitsbericht (C.10.b) habe ich die Notwendigkeit einer alsbaldigen grundlegenden Überprüfung der **Anordnung über Mitteilungen in Zivilsachen (MIZI)** dargelegt. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine solche Überprüfung gefordert. Sie hat darauf hingewiesen, daß derartige Mitteilungen in aller Regel einen Eingriff in das Recht auf informationelle Selbstbestimmung darstellen und deshalb einer verfassungsgemäßen gesetzlichen Grundlage bedürfen, die den rechtsstaatlichen Geboten der Normenklarheit und Verhältnismäßigkeit entsprechen muß. Ein Teil der Mitteilungspflichten lasse sich auf Rechtsvorschriften zurückführen. Für andere Mitteilungspflichten sei eine Rechtsgrundlage nicht ersichtlich. Eine Überprüfung der Rechtsgrundlagen der Mitteilungspflichten müsse mit einer Überprüfung der Erforderlichkeit der Mitteilungen Hand in Hand gehen.

Die Konferenz der Datenschutzbeauftragten hat deshalb die von dem Bundesminister der Justiz im Zusammenwirken mit den Landesjustizverwaltungen eingeleitete umfassende Überprüfung der MiZi begrüßt. Sie hat parallel hierzu durch einen Arbeitskreis einzelne Abschnitte der MiZi unter datenschutzrechtlichen Gesichtspunkten prüfen lassen. Das Ergebnis dieser Prüfung wurde den Justizverwaltungen mitgeteilt mit der Empfehlung, es bei der Vorbereitung des Entwurfs einer gesetzlichen Regelung zu berücksichtigen.

Über die in meinem fünften Tätigkeitsbericht (C.10.b) dargelegten Grundsätze hinaus haben die Datenschutzbeauftragten folgendes hervorgehoben:

- Die Überprüfung sollte sich nicht nur auf die Erforderlichkeit und die Rechtsgrundlage der Mitteilungen beziehen, sondern auch deren Umfang, Inhalt und Form einschließen.
- Soweit für einzelne Mitteilungen von den Justizverwaltungen als „mittelbare Rechtsgrundlagen“ bezeichnete Rechtsgrundlagen bestehen, die sich auf die Aufgaben des Empfängers der Mitteilungen beziehen, so können diese zwar ein Indiz für die Erforderlichkeit der Übermittlung sein, jedoch notwendige bereichsspezifische Rechtsgrundlagen für die Zulässigkeit der Übermittlung nicht ersetzen.
- Die Übermittlungsvorgänge sollten transparenter gestaltet werden. Das Unbehagen vieler Bürger beim Umgang mit der öffentlichen Verwaltung rührt oftmals daher, daß diese über Kenntnisse verfügt, deren Herkunft den Betroffenen unbekannt ist. Wo es ohne unzumutbaren Aufwand möglich ist, sollte daher grundsätzlich vorgesehen werden, den Betroffenen von den Mitteilungen in geeigneter Weise zu unterrichten.
- Bei der Bestimmung der Empfängerbehörde sollte auf einen funktionalen Behördenbegriff abgestellt werden. Eine genaue Bezeichnung des Empfängers (z. B. Jugendamt, Straßenverkehrsamt) dient Anforderungen, die das Bundesverfassungsgericht an die präzise Bestimmung des Verwendungszwecks geknüpft hat.
- Der Eingriffscharakter von Mitteilungen tritt besonders bei solchen an die Finanzbehörde hervor. Die Notwendigkeit solcher nur im überwiegenden Allgemeininteresse zulässigen Eingriffe sollte unter Gesichtspunkten des in § 93 Abs. 1 Satz 3 der Abgabenordnung verankerten Subsidiaritätsprinzips geprüft werden, wonach andere Personen oder Stellen als die Betroffenen selbst erst dann zu einer Auskunft (bzw. Mitteilung) heranzuziehen sind, wenn die Sachverhaltsaufklärung durch die Betroffenen nicht zum Ziele führt oder keinen Erfolg verspricht.

Die Justizminister und -senatoren sind ebenfalls der Auffassung, daß die fehlenden gesetzlichen Grundlagen alsbald zu schaffen sind. Sie haben deshalb den Bundesminister der Justiz gebeten, noch im Jahr 1986 Vorschläge für eine solche gesetzliche Regelung vorzulegen.

Als Übergangsregelung ist am 1. Dezember 1985 eine geänderte Fassung der MiZi in Kraft getreten (Allgemeine Verfügung des Justizministers vom 24. Oktober 1985, JMBL. NW. S. 253). Wenngleich darin nur ein Teil der Forderungen der Datenschutzbeauftragten berücksichtigt wurde, ist diese Fassung als ein erster Schritt zur Einschränkung der Mitteilungspflichten zu begrüßen.

- Die Terminbestimmung in einem Zwangsversteigerungsverfahren muß nach § 39 Abs. 1 des Zwangsversteigerungsgesetzes (ZVG) durch einmalige Einrückung in das für Bekanntmachungen des Gerichts bestimmte Blatt öffentlich bekanntgemacht werden. Nach § 37 Nr. 1 ZVG muß die Terminbestimmung die Bezeichnung des Grundstücks enthalten. Außerdem soll sie die Bezeichnung des zur Zeit der Eintragung des Zwangsversteigerungsver-

merks eingetragenen Eigentümers sowie die Angabe des Grundbuchblattes und der Größe des Grundstücks enthalten (§ 38 Satz 1 ZVG). In einem Fall waren in einer solchen Bekanntmachung außer den genannten Angaben auch das Geburtsdatum des Eigentümers aufgeführt.

Die Namensnennung des Grundstückseigentümers soll zwar den Gläubigern erleichtern festzustellen, ob sie eine Forderung gegen den Schuldner haben. Dies gilt insbesondere für die Gläubiger, die keine dinglich gesicherte Forderung gegen den Schuldner haben und denen deshalb die bloße Grundstücksbezeichnung nicht helfen würde. Einige Gerichte verzichten aber gleichwohl auf den Namen des Eigentümers in der öffentlichen Bekanntmachung der Terminsbestimmung.

Mit Rücksicht auf das informationelle Selbstbestimmungsrecht der Betroffenen habe ich dem Direktor des Amtsgerichts empfohlen, das Geburtsdatum des Eigentümers in der öffentlichen Bekanntmachung der Terminsbestimmung wegzulassen und zu prüfen, ob nicht auch der Name des Eigentümers entfallen kann. Er hat mir mitgeteilt, daß künftig sowohl auf die Angabe des Geburtsdatums als auch auf den Namen des Eigentümers in der öffentlichen Bekanntmachung verzichtet werde, es sei denn, daß im Einzelfall der Name des Eigentümers erforderlich ist, um Verwechslungen zu vermeiden.

#### d) Strafvollzug

- Im Bereich des Strafvollzuges war die Zulässigkeit der Datenerhebung bei der **Behandlungsuntersuchung** sowie die weitere Verwendung dieser Daten zu prüfen. Eine solche Datenerhebung ist, sofern keine Einwilligung des Betroffenen vorliegt, ein Eingriff in sein aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes hergeleitetes Recht auf informationelle Selbstbestimmung und sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung, der einer gesetzlichen Grundlage bedarf.

Gesetzliche Grundlage für die Erhebung personenbezogener Daten bei der Behandlungsuntersuchung sowie für ihre Verwendung und Weitergabe für Zwecke des Strafvollzuges sind die Vorschriften der §§ 6 und 7 des Strafvollzugsgesetzes (StVollzG). Nach § 6 Abs. 1 StVollzG wird nach dem Aufnahmeverfahren damit begonnen, die Persönlichkeit und die Lebensverhältnisse des Gefangenen zu erforschen. Die Untersuchung erstreckt sich auf die Umstände, deren Kenntnis für eine planvolle Behandlung des Gefangenen im Vollzuge und für die Eingliederung nach seiner Entlassung notwendig ist (§ 6 Abs. 2 StVollzG). Nach § 7 Abs. 1 StVollzG wird auf Grund der Behandlungsuntersuchung ein Vollzugsplan erstellt. Soweit es für die Behandlungsuntersuchung und die Erstellung des Vollzugsplans erforderlich ist, dürfen personenbezogene Daten der Gefangenen erhoben und weitergegeben werden.

Der Justizminister hat mir hierzu mitgeteilt, daß die Behandlungsuntersuchung, die für Gefangene mit einer Vollzugsdauer von mehr als 18 Monaten in Nordrhein-Westfalen zentral in sogenannten Einweisungsanstalten durchgeführt wird, aus Erhebungen zur persönlichen, sozialen und kriminologischen Vorgeschichte durch einen Fragebogen, aus Verhaltensbeobachtungen, aus psychologischen und schulischen Prüfungsverfahren (Tests) und einer (oder mehrfacher) Exploration(en) bestehe. Die im Rahmen der Behandlungsuntersuchung erhobenen Informationen und Daten würden zusammen mit dem von dem Gefangenen selbst gefertigten Lebenslauf, dem Urteil und etwaigen weiteren diagnostischen oder anderen Erkenntnissen von den einzelnen Fachdiensten in ihren Stellungnahmen verarbeitet. Diese Stellungnahmen seien die Grundlage der Einweisungsentschließung und würden als Ergebnisse einer Persönlichkeitsdiagnose und Behandlungsprognose in die Empfehlungen zur Aufstellung eines Vollzugsplanes nach § 7

StVollzG einfließen. Auf Grund der Einweisungsentschließung werde der Gefangene sodann in eine bestimmte Vollzugsanstalt verlegt. Diese erstelle auf Grund der die Einweisung tragenden Gründe und der Behandlungsempfehlungen, die in der Gefangenenpersonalakte abgeheftet werden, den Vollzugsplan.

Ein Teil der Daten aus der psychologischen Untersuchung werde in verschlüsselter Form an den Psychologen der aufnehmenden Anstalt weitergegeben, um im Rahmen der Fortschreibung des Vollzugsplanes (§ 7 Abs. 3 StVollzG) Vergleiche zu früheren Befunden zu ermöglichen. Im übrigen würden die erhobenen Daten und Unterlagen in der Einweisungsanstalt aufbewahrt.

Wie der Justizminister weiter mitgeteilt hat, besteht ungeachtet der Notwendigkeit der Mitwirkung des Gefangenen im Hinblick auf die Erreichung des Vollzugsziels nach dem Strafvollzugsgesetz keine Pflicht des Gefangenen, an seiner Behandlungsuntersuchung und seiner Behandlung mitzuwirken. Der Gefangene habe es deshalb selbst in der Hand, ob und inwieweit er den an ihn gerichteten Anforderungen, wie seinen Lebenslauf frei niederzuschreiben oder einen Fragebogen über seine persönlichen Verhältnisse auszufüllen, entsprechen will. Komme er den Aufforderungen nach, stimme er der darin liegenden Datenerhebung zu.

Werden Daten beim Betroffenen erhoben, so ist er nach § 10 Abs. 2 Satz 1 DSGVO auf die der Datenerhebung zugrunde liegende Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hinzuweisen. 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, und bei fehlender Mitwirkungspflicht frei entscheiden kann, ob und in welchem Umfang er seine Daten offenbaren will.

Bei dem Hinweis ist zu beachten, daß Freiwilligkeit im Sinne des § 10 Abs. 2 Satz 1 DSGVO nur dann vorliegt, wenn weder eine Rechtspflicht noch eine Obliegenheit des Betroffenen derart, daß ohne seine Mitwirkung an der Datenerhebung eine ungünstige Entscheidung ergehen müßte, besteht (vgl. Dammann in Simitis/Dammann/Mallmann/Reh, Bundesdatenschutzgesetz, 3. Aufl., § 9 Rdnr. 41). Dementsprechend bestimmt § 10 Abs. 2 Satz 2 DSGVO NW, daß dem Betroffenen bei freiwilligen Angaben aus einer Verweigerung der Einwilligung keine Rechtsnachteile entstehen dürfen.

Der Justizminister hat mir hierzu mitgeteilt, daß er den Landesjustizverwaltungen vorschlagen werde, die bundeseinheitlichen Vordrucke durch einen Hinweis zu ergänzen, daß die Erstellung eines Lebenslaufs und die Ausfüllung des Fragebogens über die persönlichen Verhältnisse auf seiten des Gefangenen Freiwilligkeit voraussetzen, und daß eine Nichtbefolgung der Aufforderungen disziplinarische Folgen nicht nach sich zieht.

Soweit die Gefangenen in geeigneter Weise auf die Vorschrift des § 6 StVollzG und die Freiwilligkeit der Angaben hingewiesen werden, habe ich keine Bedenken gegen die Datenerhebung.

- Als gesetzliche Grundlage für die Verwendung der erhobenen Daten für die **kriminologische Forschung** kommt nur § 166 StVollzG in Betracht. Nach dieser Vorschrift obliegt es dem Kriminologischen Dienst, in Zusammenarbeit mit den Einrichtungen der Forschung den Vollzug, namentlich die Behandlungsmethoden, wissenschaftlich fortzuentwickeln und seine Ergebnisse für Zwecke der Strafrechtspflege nutzbar zu machen. Der Justizminister des Landes Nordrhein-Westfalen hat hierzu in der Allgemeinen Verfügung vom 27. Januar 1982 (JMBl. NW. S. 49) bestimmt, daß die kriminologisch relevanten Daten der Strafgefangenen, die am Einweisungsverfahren teilnehmen, in einer Kriminologischen Datei erfaßt werden.

Nach Auffassung des Justizministers kann bei kriminologischen Forschungsvorhaben zur Erfolgskontrolle des Behandlungsvollzugs eine Anonymisierung der Daten nicht in Betracht kommen. Es müsse in jedem Einzelfall möglich sein, nach Ablauf von mehrjährigen Fristen festzustellen, ob ein Strafgefangener, der ein bestimmtes Behandlungsprogramm im Vollzug durchlaufen habe, rückfällig geworden sei. Ebensowenig sei es möglich, die Speicherung der Daten auf diejenigen Gefangenen zu beschränken, die in eine entsprechende Befragung eingewilligt hätten (§ 3 Abs. 1 Nr. 2 DSGVO). Im Falle einer Beschränkung einschlägiger Untersuchungen auf die Strafgefangenen, die ihre Einwilligung erteilten, käme den Untersuchungsergebnissen keine objektive Aussagekraft zu.

Im Hinblick auf das Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 könnte es zweifelhaft sein, ob § 166 StVollzG als gesetzliche Grundlage für eine Verwendung der Daten für die kriminologische Forschung dem Gebot der Normenklarheit entspricht. Es obliegt dem Gesetzgeber, für eine derartige Verwendung der erhobenen Daten eine hinreichend präzise gesetzliche Grundlage zu schaffen. Bis dahin kann jedoch in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts für eine Übergangszeit zur Wahrung der Funktionsfähigkeit des Strafvollzugs die Verwendung der Daten für die kriminologische Forschung auf § 166 StVollzG gestützt werden.

Für nicht zulässig halte ich es dagegen, wenn nach Nr. 5 der Allgemeinen Verfügung des Justizministers vom 27. Januar 1982 eine Auskunftserteilung an Gefangene, die in der Kriminologischen Datei erfaßt sind, unter Berufung auf § 16 Abs. 3 Ziffer 1 DSGVO verweigert wird, weil

- die Daten ohne sachkundige Erläuterung nicht verständlich seien, ihre Mitteilung daher die Behandlung des Gefangenen gefährden könnte,
- die Ergebnisse der Behandlungsuntersuchung nach § 6 Abs. 3 StVollzG mit dem Gefangenen erörtert werden müßten,
- die Daten der Kriminologischen Datei bei der Behandlung der Gefangenen nicht verwertet würden.

Nach § 16 Abs. 1 Satz 1 DSGVO ist dem Betroffenen von der speichernden Stelle auf Antrag Auskunft über die zu seiner Person gespeicherten Daten und die Stellen, denen Daten regelmäßig übermittelt werden, zu erteilen. Eine Auskunftserteilung unterbleibt, soweit die Auskunft die rechtmäßige Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben gefährden würde (§ 16 Abs. 3 Nr. 1 DSGVO). Die hierfür vom Justizminister in der Allgemeinen Verfügung genannten Gründe vermögen nicht zu überzeugen.

- Zahlreiche Eingaben von Gefangenen betrafen die **Offenbarung ihres Gefangenenstatus** durch die Justizvollzugsanstalt an Dritte.

Durch das Anbringen des Namens eines Gefangenen an der Betreuertafel und an seiner Stubentür wurde der Name den anderen Gefangenen, gegebenenfalls auch Besuchern der Anstalt bekanntgegeben, die den Haftbereich betreten. Diese Bekanntgabe stellt einen Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch in sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung dar.

Der Justizminister hat die Auffassung vertreten, daß die Angaben des Namens von Gefangenen an den Stubentüren und den Betreuertafeln im Haftbereich keinen Verstoß gegen datenschutzrechtliche Vorschriften darstelle. Er bezieht sich auf einen Beschluß des Oberlandesgerichts Frankfurt vom 22. November 1984. Der in diesem Beschluß vertretenen Auffassung,

daß durch das Anbringen des Namensschildes eines Gefangenen am Haftraum dessen Rechtsstellung nicht berührt, namentlich sein Persönlichkeitsrecht nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes nicht beeinträchtigt werde, kann nicht gefolgt werden. Sie steht im Widerspruch zu dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz, wonach dieses Grundrecht die Befugnis des Einzelnen gewährleistet, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.

Auch wenn der Eingriff der in der Bekanntgabe der Namen der Gefangenen durch das Anbringen an der Betreuertafel und den Stubentüren liegt, von den Gefangenen im überwiegenden Allgemeininteresse hingenommen werden müßte, bedarf er einer hinreichend normenklaren gesetzlichen Grundlage. Eine solche ist nicht ersichtlich. Ich habe den Justizminister darauf hingewiesen, daß eine gesetzliche Grundlage geschaffen werden müsse, wenn an dem Anbringen der Namen an der Betreuertafel und an den Stubentüren festgehalten werden soll. Das praktizierte Verfahren kann ohne gesetzliche Grundlage allenfalls noch für eine Übergangszeit hingenommen werden.

Der Justizminister hat daraufhin meine Rechtsauffassung hinsichtlich der Schaffung einer gesetzlichen Grundlage für das Anbringen der Namen der Gefangenen an der Betreuertafel und an den Stubentüren dem Bundesminister der Justiz mitgeteilt und angeregt, diese in die Überlegungen zur Schaffung einer Ermächtigunggrundlage für die Erhebung, Verwendung und Übermittlung personenbezogener Daten im Strafvollzug miteinzubeziehen.

- Zu der Bekanntgabe personenbezogener Daten beim Einkauf der Gefangenen an den Vertragskaufmann habe ich in meinem dritten Tätigkeitsbericht (C.7.f) Stellung genommen. Inzwischen haben mir Gefangene mitgeteilt, daß der neue **Einkaufszettel** der Gefangenen wiederum dem Kaufmann vorgelegt werden mußte.

Die Gefangenen erhalten zur Vorbereitung des Einkaufs „Bestellzettel“ des Vertragskaufmanns, aus denen sich das Warenangebot ergibt, und von der Anstaltszahlstelle „Einkaufsscheine“. Auf dem Einkaufsschein kann der Gefangene die Höhe des ihm für den jeweiligen Einkauf zur Verfügung stehenden Betrages ersehen. Der Einkaufsschein verbleibt nach der geltenden Regelung beim Gefangenen.

Der Gefangene kennzeichnet die Bestelliste mit seinem Namen sowie seiner Abteilungs- und Haftraumnummer und trägt die gewünschten Waren ein. Die Bestelliste wird dem Vertragskaufmann zusammen mit einer von der Anstaltszahlstelle erstellten „Einkaufsliste“ zugeleitet. In der Einkaufsliste ist die Kontonummer, der Name, das Geburtsdatum sowie die Höhe des für den Einkauf zur Verfügung stehenden Betrages aufgeführt. Nach Auffassung des Justizministers bedarf es der Angaben in der Einkaufsliste, um den Gefangenen zu identifizieren, der Angabe des zur Verfügung stehenden Einkaufsbetrages, um zu verhindern, daß Gefangene mehr einkaufen, als es ihre Mittel zulassen. Die Einkaufsliste sei unverzichtbare organisatorische Grundlage für die Durchführung des Einkaufs.

Das praktizierte Verfahren für den Einkauf bei dem Vertragskaufmann greift in das Recht der Gefangenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch in ihr Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung dadurch ein, daß dabei mit der Bestelliste und der Einkaufsliste dem Vertragskaufmann Name und Geburtsdatum des Gefangenen offenbart werden. Für einen solchen Eingriff ist eine gesetzliche Grundlage erforderlich, die den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz beachten muß.

Als gesetzliche Grundlage kommt nur § 22 Abs. 1 Satz 1 StVollzG in Verbin-

dung mit § 81 Abs. 2 StVollzG in Betracht. Nach § 22 Abs. 1 Satz 1 StVollzG kann sich der Gefangene von seinem Hausgeld aus einem von der Anstalt vermittelten Angebot Nahrungs- und Genußmittel sowie Mittel zur Körperpflege kaufen. Nach § 81 Abs. 2 StVollzG sind die Beschränkungen, die dem Gefangenen zur Aufrechterhaltung der Ordnung der Anstalt auferlegt werden, so zu wählen, daß sie in einem angemessenen Verhältnis zu ihrem Zweck stehen und den Gefangenen nicht mehr als notwendig beeinträchtigen.

Zur Durchführung des Einkaufs nach § 22 Abs. 1 Satz 1 StVollzG können nur solche Datenflüsse als zulässig angesehen werden, die die Voraussetzungen des dem verfassungsrechtlichen Verhältnismäßigkeitsgebot entsprechenden § 81 Abs. 2 StVollzG erfüllen. Danach halte ich es für geboten, für den Einkauf nach § 22 Abs. 1 Satz 1 StVollzG ein Verfahren zu wählen, bei dem der Name des Gefangenen gegenüber dem Kaufmann nicht offenbart wird. Für die richtige Zuordnung der Lieferung könnte die Kontonummer statt des Namens verwendet werden.

Ich habe dem Justizminister empfohlen, für dieses Verfahren eine Regelung zu treffen, die den Datenschutzbelangen der Betroffenen Rechnung trägt. Das Ergebnis meiner Bemühungen bleibt abzuwarten.

- Ein Gefangener mußte für eine Bücherbestellung bei einem Verlag eine **Paketmarke** verwenden wie bei Paketen mit Nahrungs- und Genußmitteln. Das von der Vollzugsanstalt praktizierte Verfahren für den Bücherempfang durch Verwendung einer Paketmarke greift in das Recht der Gefangenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch in ihr Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung dadurch ein, daß durch die Verwendung der Paketmarke Außenstehenden der Status des Betroffenen als Gefangener bekannt wird.

Als gesetzliche Grundlage für derartige Eingriffe kommt nur § 33 Abs. 1 Satz 1 und 3 StVollzG in Verbindung mit § 81 Abs. 2 StVollzG in Betracht. Nach § 33 Abs. 1 Satz 1 StVollzG darf der Gefangene dreimal jährlich in angemessenen Abständen ein Paket mit Nahrungs- und Genußmitteln empfangen. Der Empfang weiterer Pakete oder solcher mit anderem Inhalt bedarf der Erlaubnis (§ 33 Abs. 1 Satz 3 StVollzG). Nach § 81 Abs. 2 StVollzG sind die Beschränkungen, die dem Gefangenen zur Aufrechterhaltung der Ordnung der Anstalt auferlegt werden, so zu wählen, daß sie in einem angemessenen Verhältnis zu ihrem Zweck stehen und den Gefangenen nicht mehr als notwendig beeinträchtigen.

Es mag notwendig sein, daß bei Paketen mit Nahrungs- und Genußmitteln, die zu bestimmten Zeiten alle Gefangenen der Anstalt erhalten, Paketmarken verwendet werden, um bei der Vielzahl der ankommenden Pakete sofort feststellen zu können, ob es sich um ein zugelassenes Paket handelt. Im übrigen erhalten die Gefangenen solche Pakete in der Regel von Personen, denen die Tatsache der Inhaftierung ohnehin bekannt ist. Bei dem Empfang von Paketen mit anderem Inhalt, wie zum Beispiel Buchbestellungen oder sonstigen Bestellungen bei Dritten, denen die Inhaftierung des Bestellers nicht bekannt ist, halte ich es aber für geboten, ein Verfahren zu wählen, bei dem die Tatsache der Inhaftierung den Dritten nicht offenbart wird. So könnte vorgesehen werden, daß der Absender des Bücherpakets bereits in der Erlaubnis für den Empfang festgelegt und bei Eingang eines Paketes von diesem Absender ohne Paketmarke die Annahme nicht verweigert, sondern lediglich bei der Durchsuchung geprüft wird, ob das Paket der erteilten Erlaubnis entspricht.

Ich habe dem Justizminister empfohlen, für den Empfang derartiger Pakete

eine Regelung zu treffen, die den Datenschutzbelangen der Betroffenen Rechnung trägt.

- Die Bundesversicherungsanstalt für Angestellte wurde über die Aufnahme eines Gefangenen in die Justizvollzugsanstalt gemäß Nr. 19 Abs. 1 der Vollzugsgeschäftsordnung (VGO) unterrichtet.

Nach § 19 Abs. 1 VGO ist zwar, wenn sich bei der Erstaufnahme eines Strafgefangenen mit mehr als einem Monat Vollzugsdauer oder eines Sicherungsverwahrten ergibt, daß er eine gesetzliche Rente oder eine dieser gleichzustellende Leistung erhält, die Aufnahme der zuständigen Behörde mitzuteilen. Diese Vorschrift kommt jedoch als Verwaltungsvorschrift für einen Eingriff in das Recht auf informationelle Selbstbestimmung und das Grundrecht auf Datenschutz nicht in Betracht. Nach Mitteilung des Justizministers fehlt es an einer entsprechenden gesetzlichen Ermächtigungsnorm als Rechtsgrundlage für die in Nr. 19 VGO geregelten **Mitteilungspflichten der Justizvollzugsanstalten**, worauf er den Bundesminister der Justiz hingewiesen habe.

- Nach Nr. 5 Abs. 2 VGO kann die Vollzugsgeschäftsstelle **Auskünfte** über einen Gefangenen **an Behörden oder andere öffentliche Stellen** erteilen. Eine Krankenkasse fragte bei einer Vollzugsanstalt an, in welchem Zeitraum einem inhaftierten Versicherungsmitglied Hafturlaub gewährt worden war und erhielt auf Grund Nr. 5 Abs. 2 VGO die gewünschte Auskunft. Wie bereits ausgeführt, kommen die Vorschriften der Vollzugsgeschäftsordnung als Rechtsgrundlage für einen Eingriff in die genannten Grundrechte nicht in Betracht. Bis zur Schaffung einer gesetzlichen Grundlage für Auskünfte über Gefangene sind derartige Mitteilungen nur mit Einwilligung des Betroffenen zulässig.

- Eine Gefangene stellte den schriftlichen Antrag auf **Gewährung von Ausgang** gemäß § 35 StVollzG, um einen Termin beim Vertrauensarzt der Landesversicherungsanstalt wahrzunehmen. Da nach § 35 Abs. 1 StVollzG für die Gewährung von Ausgang ein wichtiger Anlaß gefordert wird und Zweifel bestanden, ob diese Voraussetzung erfüllt war, wurde von der Vollzugsanstalt beim Vertrauensarzt die Notwendigkeit der Vorstellung abgeklärt. Eine gesetzliche Grundlage für die Offenbarung der Tatsache der Inhaftierung gegenüber dem Vertrauensarzt und dem darin liegenden Eingriff in die vorgenannten Grundrechte ist nicht vorhanden. Die Auskunft bei dem Vertrauensarzt hätte deshalb nur mit Einwilligung der Betroffenen eingeholt werden dürfen.

- Der Leiter einer Justizvollzugsanstalt lehnte einer Gefangenen den beantragten **Urlaub** ab und teilte dies ihren Rechtsanwälten mit. Zur Begründung der Ablehnung des Gesuchs wurde unter anderem angeführt, daß die Gefangene versucht habe, Schriftstücke an ihren Ehemann unter Umgehung der Briefkontrolle hinauszuschmuggeln. Zur weiteren Begründung wurde den Rechtsanwälten eine Ablichtung des gefundenen Briefes übersandt. In dem Brief der Gefangenen an ihren Ehemann waren auch kritische Äußerungen der Gefangenen über ihre Rechtsanwälte enthalten.

Die Tatsache des Schreibens der Gefangenen an ihren Ehemann und der Inhalt dieses Schreibens sind personenbezogene Daten, da es sich um Einzelangaben über persönliche und sachliche Verhältnisse einer natürlichen Person handelt (§ 2 Abs. 1 DSG NW). Eine gesetzliche Grundlage für die Weitergabe einer Kopie des Briefes an die Rechtsanwälte ist nicht ersichtlich. Selbst bei Vorliegen einer gesetzlichen Grundlage wäre an die Erforderlichkeit der Datenweitergabe ein strenger Maßstab anzulegen. Es genügt nicht, wenn die Kenntnis der Daten zur Aufgabenerfüllung nur dienlich ist, sie muß vielmehr hierfür unbedingt notwendig sein.

Zur Begründung des ablehnenden Bescheides über den Urlaubsantrag hätte es genügt, wenn gewonnene Erkenntnisse aus dem Brief, wie die Vermutung, daß eine Rückkehr aus dem Urlaub nicht beabsichtigt sei, oder sonstige Umstände, die zur Ablehnung des Urlaubsantrages geführt haben, den Rechtsanwälten mitgeteilt worden wären. Die Übersendung einer vollständigen Ablichtung des Schreibens mit Ausführungen, die nicht für die Rechtsanwälte bestimmt waren, war nicht erforderlich. Der Justizminister hat die Leiter der Justizvollzugsanstalten über meine Rechtsauffassung mit der Bitte um Beachtung unterrichtet.

- Nach § 24 Abs. 1 StVollzG darf ein Gefangener regelmäßig **Besuch** empfangen. Die Gesamtdauer beträgt mindestens eine Stunde im Monat. Das Weitere regelt die Hausordnung. In einem Fall trug ein Gefangener vor, seiner Ehefrau sei durch die Vollzugsanstalt telefonisch mitgeteilt worden, daß die Besuchszeit ihres Mannes bereits durch den Empfang anderen weiblichen Besuchs verbraucht sei. Es konnte nicht mehr festgestellt werden, ob diese Auskunft tatsächlich erteilt wurde. Der Leiter der Vollzugsanstalt nahm jedoch die Angelegenheit zum Anlaß, die Bediensteten daran zu erinnern, bei „verbrauchter“ Besuchszeit lediglich diese Tatsache mitzuteilen und keine näheren Auskünfte zu geben.
- Ein Justizvollzugsamt führte gegen eine Gefangene einen Zivilprozeß auf Zahlung eines Eigenanteils an einer ärztlichen Behandlung. In dem Verfahren legte das Vollzugsamt dem Gericht die Kopie einer Kassenanordnung mit einer Aufstellung über die Zusammensetzung des auszahlenden Betrages der Behandlungen von elf Gefangenen, darunter die der Beklagten, vor. Die Aufstellung enthielt neben der Zusammensetzung des auszahlenden Betrages aus Haushaltsmitteln, Eigengeld und Hausgeld auch die Namen und Geburtsdaten der Gefangenen, die an dem Zivilprozeß nicht beteiligt waren.

Nach § 130 ZPO sollen die vorbereitenden Schriftsätze die Angabe der zur Begründung der Anträge dienenden tatsächlichen Verhältnisse (Nr. 3) sowie die Bezeichnung der Beweismittel (Nr. 5) enthalten. Wenn eine öffentliche Stelle als Prozeßpartei dabei in das Recht Dritter auf informationelle Selbstbestimmung und in ihr Grundrecht auf Datenschutz eingreift, muß sie den Grundsatz der Erforderlichkeit beachten. Danach dürfen nur die Daten an das Gericht weitergegeben werden, die mit dem Streitgegenstand in Zusammenhang stehen und der sachgerechten Rechtswahrung dienen.

Die Bekanntgabe der Namen und Geburtsdaten der Gefangenen, die nicht an dem Zivilprozeß beteiligt waren, war nicht erforderlich. Ich habe empfohlen, in derartigen Fällen die personenbezogenen Daten Unbeteiligter unkenntlich zu machen. Meiner Empfehlung wird gefolgt.

- Ein Gefangener hatte mit einem „Zeitschriftenantrag“ in einer Justizvollzugsanstalt die **Genehmigung zur Bestellung einer Zeitschrift** beantragt. Diesem Antrag war eine von ihm mit Schreibmaschine ausgefüllte neutrale Zahlkarte beigelegt worden. Als Absender hatte er neben seinem Namen die Straße und den Ort der Vollzugsanstalt angegeben. Von der Zahlstelle der Vollzugsanstalt wurde ohne seine Erlaubnis eine neue Zahlkarte ausgefüllt mit dem Absender bzw. Kontoinhaber „Zahlstelle der Justizvollzugsanstalt“. Dadurch wurde dem Empfänger die Tatsache seiner Inhaftierung bekanntgegeben. Die spätere Zeitschriftensendung wurde von der Vollzugsanstalt mit dem Vermerk „Annahme verweigert“ an den Absender zurückgeschickt. Auf eine Anfrage des Zeitschriftenversenders nach dem Grund der Annahmeverweigerung hat der Leiter der Vollzugsanstalt geantwortet. In diesem Brief wurde als Betreff angegeben „Strafgefangener ..., geb. am ...“.

Eine Rechtsvorschrift, die in einem derartigen Fall die Bekanntgabe des

Gefangenenstatus an Dritte vorsieht, ist nicht ersichtlich. Im übrigen sind nach § 81 Abs. 2 StVollzG Beschränkungen, die dem Gefangenen zur Aufrechterhaltung der Ordnung der Anstalt auferlegt werden, so zu wählen, daß sie in einem angemessenen Verhältnis zu ihrem Zweck stehen und den Gefangenen nicht mehr als nötig beeinträchtigen.

Wenn ein Gefangener für den Bezug einer Zeitschrift schon die Genehmigung durch die Justizvollzugsanstalt einholen muß, sollte er nicht auch noch mit der Bekanntgabe seines Status als Gefangener gegenüber dem Zeitschriftenversand belastet werden. Kann die Genehmigung nicht erteilt werden, ist es zwar zulässig eine Zeitschrift mit dem Vermerk „Annahme verweigert“ zurückzusenden. Es sollte jedoch dem Gefangenen selbst überlassen werden, ob und in welcher Form er den Absender über den Grund der Annahmeverweigerung unterrichten will. Dabei lasse ich dahingestellt, ob es überhaupt zulässig ist, zunächst den Bezugspreis für die Zeitschrift aus Mitteln des Gefangenen zu überweisen und danach die Annahme der Zeitschrift zu verweigern.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich empfohlen, künftig in derartigen Fällen von der Bekanntgabe des Gefangenenstatus an Dritte abzusehen und für den Zeitschriftenbezug ein Verfahren vorzusehen, das auch den Gefangenen nicht in eine Lage bringt, in der er seinen Gefangenenstatus gegenüber dem Zeitschriftenversand offenbaren muß.

- Zu der **Überwachung des Schriftverkehrs** der Gefangenen mit dem Landesbeauftragten für den Datenschutz habe ich in meinem sechsten Tätigkeitsbericht (C.7.f) Stellung genommen. Inzwischen hat der Justizminister auch die Schreiben des Landesbeauftragten für den Datenschutz an Gefangene von der Überwachung des Schriftverkehrs nach § 29 Abs. 3 StVollzG ausgenommen.
- Der Leiter einer Vollzugsanstalt schrieb an einen Kollegen einen Brief, in dem er ihn über den Werdegang eines ehemaligen Strafgefangenen informierte, der nach seiner Entlassung aus der Haft im Rahmen seiner Aufgaben als Mitarbeiter einer Parlamentsfraktion in einem anderen Bundesland Gefangene besuchte, unter anderem auch in der Vollzugsanstalt, in der sein Kollege Leiter war. Dieses **Warnschreiben** enthielt zahlreiche zum Teil höchst sensible personenbezogene Daten des Betroffenen.

Die Weitergabe dieser Daten an eine andere Stelle ist ein Eingriff in das Grundrecht des Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung wie auch in sein Grundrecht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes. Eine gesetzliche Grundlage für einen solchen Eingriff ist nicht ersichtlich. Selbst wenn sie vorhanden wäre, würde die Weitergabe eines derart umfassenden Persönlichkeitsbildes gegen den Verhältnismäßigkeitsgrundsatz verstoßen.

Der Justizminister, den ich um Stellungnahme gebeten habe, hat mir mitgeteilt, daß auch er eine gesetzliche Grundlage für die Datenweitergabe nicht zu erkennen vermag. Wiederholungen seien indessen nicht zu befürchten.

## 11. Sozialwesen

### a) Sozialversicherung

- Ein Bürger wandte sich dagegen, daß er von einer Allgemeinen Ortskrankenkasse (AOK) bei der Beantragung einer **Haushaltshilfe** nach folgenden

Angaben zur Person der Ersatzkraft und zu den Kosten für die Haushaltshilfe befragt wurde: Name, Vorname, Geburtstag, Wohnung, Zahl der Kinder der Ersatzkraft unter 15 Jahren, Versorgung dieser Kinder außerhalb der Schulstunden, solange sich die Hilfskraft in der Wohnung des Antragstellers aufhält, Berufstätigkeit der Ersatzkraft, Art dieser Tätigkeit, Arbeitsstätte und tägliche Arbeitszeit, verwandt oder verschwägert mit Versicherten oder dessen Ehegatten, wenn ja, Verwandtschaftsgrad sowie Art und Höhe der Auslagen und Einbußen, die der Ersatzkraft durch die Übernahme der Haushaltshilfe entstehen, wenn nein, Höhe der Vergütung je Arbeitsstunde, Arbeitstag oder Woche, Gewährung kostenloser Verpflegung, Vorliegen einer Steuerkarte.

Das Verlangen dieser Angaben ist ein Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 2 des Grundgesetzes und in sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage.

Gesetzliche Grundlage für die Erhebung von Angaben im Rahmen eines Antrages auf Haushaltshilfe ist § 60 Abs. 1 Nr. 1 des Ersten Buches des Sozialgesetzbuchs (SGB I) in Verbindung mit § 185b der Reichsversicherungsordnung (RVO). Nach § 60 Abs. 1 Nr. 1 SGB I hat derjenige, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind.

Nach § 185b Abs. 1 Satz 1 RVO erhalten Versicherte Haushaltshilfe, wenn ihnen oder ihrem Ehegatten wegen Aufenthalts in einem Krankenhaus oder in einer Entbindungsanstalt oder wegen eines Kuraufenthalts, dessen Kosten von der Krankenkasse ganz oder teilweise getragen werden, die Weiterführung des Haushalts nicht möglich ist und eine andere im Haushalt lebende Person den Haushalt nicht weiterführen kann.

Nach § 185b Abs. 2 RVO ist als Haushaltshilfe eine Ersatzkraft zu stellen. Kann eine Ersatzkraft nicht gestellt werden oder besteht Grund, von der Gestellung einer Ersatzkraft abzusehen, so sind die Kosten für eine selbst beschaffte Ersatzkraft in angemessener Höhe zu erstatten. Für Verwandte und Verschwägte bis zum zweiten Grade werden keine Kosten erstattet; die Krankenkasse kann jedoch die erforderlichen Fahrkosten und den Verdienstaufschlag erstatten, wenn die Erstattung in einem angemessenen Verhältnis zu den sonst für eine Ersatzkraft entstehenden Kosten steht.

Zur Prüfung, ob die Kosten für eine selbst beschaffte Ersatzkraft in angemessener Höhe übernommen werden können, sind die von dem Versicherten verlangten Angaben über die Personalien der Ersatzkraft, das Verwandtschaftsverhältnis, das Entstehen von Art und Höhe von Auslagen und Einbußen sowie über Höhe der Kosten für die Haushaltshilfe, soweit diese mit dem Versicherten oder dessen Ehegatten nicht verwandt oder verschwägert ist, erforderlich. Hingegen ist für die anderen Angaben über die Ersatzkraft eine gesetzliche Grundlage nicht vorhanden. Wie mir die AOK inzwischen mitgeteilt hat, werden diese Angaben künftig nicht mehr verlangt.

- Durch eine Eingabe wurde ich auf das Verfahren bei der Erhebung von Daten für ein Forschungsvorhaben der Bundesanstalt für Arbeitsschutz und Unfallforschung über **Heim- und Freizeitunfälle** im Bereich einer AOK aufmerksam. Die AOK hatte den von der Bundesanstalt erstellten Erhebungsbogen, der zwar nicht den Namen des Versicherten, jedoch eine aufgedruckte Zählnummer enthielt, ihren Versicherten mit der Bitte um Ausfüllung und Rückgabe übersandt. Die AOK ging davon aus, daß es sich hier nicht um die Erhebung personenbezogener Daten, sondern um die Erhebung anonymisierter Daten handelte, da der Bundesanstalt die Erhebungsbogen ohne

jeden Hinweis auf die Person des Befragten weitergegeben wurden. Auch die hierauf angebrachten Zählnummern ermöglichten der Bundesanstalt keine Rückschlüsse auf bestimmte Personen, weil die verwendeten Anschriften des Versicherten nur der AOK bekannt waren. Eine Zusammenführung der Zählnummer mit den Angaben des Befragten durch die AOK war zwar nicht beabsichtigt, aber möglich.

Da für die AOK die Möglichkeit einer Zusammenführung der Zählnummer mit den Angaben des Befragten bestand, wobei unerheblich war, ob dies tatsächlich geschah, handelte es sich um eine Erhebung personenbezogener Daten. Eine nach Artikel 4 Abs. 2 der Landesverfassung erforderliche gesetzliche Grundlage für die Erhebung personenbezogener Daten durch die AOK im Rahmen der Befragung zu Unfällen in Heim und Freizeit ist nicht vorhanden. Die Erhebung der Angaben ist deshalb nur auf freiwilliger Grundlage zulässig.

Werden personenbezogene Daten beim Betroffenen erhoben, so ist dieser nach § 9 Abs. 2 des für Sozialleistungsträger geltenden Bundesdatenschutzgesetzes auf die der Datenerhebung zugrunde liegende Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hinzuweisen. 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. In dem mir vorgelegten Fragebogen fehlte ein solcher Hinweis. Ich habe daher der AOK empfohlen, künftig in vergleichbaren Fällen nach § 9 Abs. 2 BDSG auf die Freiwilligkeit der Ausfüllung des Fragebogens hinzuweisen. Die AOK wird entsprechend verfahren.

- Ein Arzt beschwerte sich darüber, daß eine AOK zum Zwecke der Prüfung der **Wirtschaftlichkeit der Verordnungsweise** des Betroffenen Krankenscheinoriginals und Kopien mit Diagnosen und persönlichen Daten seiner Patienten von anderen Krankenkassen angefordert und diese auch zur Auswertung erhalten habe. Die AOK teilte mir hierzu mit, daß sich die Krankenkassen, um die ihnen übertragenen Aufgaben wahrnehmen zu können, auf örtlicher Ebene zu Arbeitsgemeinschaften zusammengeschlossen hätten. Zu den Aufgaben dieser Arbeitsgemeinschaften gehörten die gesamten Vertragsbeziehungen zu den Leistungserbringern. So bestehe ein Gesamtvertrag-Ärzte mit Gemeinsamer Prüfvereinbarung, in die die Krankenkassen vor Ort durch die örtliche Arbeitsgemeinschaft fest eingebunden seien. Es sei Aufgabe der Krankenkasse, die Gesamttätigkeit des Arztes zu prüfen. Zur Erfüllung dieser Aufgabe sei die Zusammenführung der Abrechnungsunterlagen geboten.

Die Überlassung der in den Krankenscheinen festgehaltenen Angaben über die Patienten und den behandelnden Arzt durch die an der Arbeitsgemeinschaft beteiligten Krankenkassen an die AOK als federführende Stelle der Arbeitsgemeinschaft ist eine Offenbarung personenbezogener Daten im Sinne des § 35 SGB I. Diese Offenbarung wäre, soweit nicht der Betroffene im Einzelfall eingewilligt hat, nach § 67 Satz 1 des Zehnten Buches des Sozialgesetzbuchs (SGB X) nur zulässig, wenn eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt.

- Eine gesetzliche Offenbarungsbefugnis der anderen an der Arbeitsgemeinschaft beteiligten Krankenkassen gegenüber der AOK als federführender Stelle der Arbeitsgemeinschaft ergibt sich aus der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X nicht. Nach dieser Vorschrift ist eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch. Die Vorschrift des § 368n Abs. 5 RVO kommt hierfür nicht in Betracht. Nach § 368n Abs. 5 Satz 1 RVO errichten die Kassenärztlichen Vereinigungen zur Überwachung der Wirtschaftlichkeit der kassenärztlichen

Versorgung im einzelnen Prüfungs- und Beschwerdeausschüsse. Nach § 368n Abs. 5 Satz 2 RVO gehören den Ausschüssen Vertreter der Ärzte und Krankenkassen in gleicher Zahl an. Eine Übertragung der Aufgabe der Wirtschaftlichkeitsprüfung auf eine Arbeitsgemeinschaft der Krankenkassen sieht diese Vorschrift nicht vor. Ebenso wenig ist die Wahrnehmung dieser Aufgabe durch eine Arbeitsgemeinschaft der Krankenkassen nach den Vorschriften des Dritten Kapitels des Zehnten Buches des Sozialgesetzbuchs zulässig. Der Gesamtvertrag-Ärzte kann als gesetzliche Grundlage für einen derartigen Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung und in ihr Grundrecht auf Datenschutz schon deswegen nicht in Betracht kommen, weil dieser Vertrag keine Rechtsvorschrift ist und im übrigen die Versicherten nicht bindet. Da somit keine Offenbarungsbefugnis der anderen an der Arbeitsgemeinschaft beteiligten Krankenkassen bestand, war die AOK nicht befugt, die Krankenscheine von diesen Krankenkassen anzufordern.

Ich habe den beteiligten Krankenkassen empfohlen, künftig von einer derartigen Anforderung und Offenbarung abzusehen.

- In einem anderen Fall wies ein Arzt darauf hin, daß eine AOK zur **Kostenreduzierung** dazu übergegangen war, Anus-*praeter*-Patienten, die auf eine Versorgung mit Stomaartikeln angewiesen sind, dazu anzuhalten, diese Artikel nur von einem bestimmten Sanitätshaus zu beziehen. Zugleich wurden der betreffenden Firma zur Vorbereitung und Planung Name und Anschrift der Versicherten mitgeteilt, die diese Artikel benötigten.

Name und Anschrift der Versicherten unterliegen bei der AOK dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 Satz 1 SGB I). Soweit nicht der Betroffene eingewilligt hat (§ 67 Satz 1 SGB X), dürfen seine personenbezogenen Daten nur offenbart werden, wenn eine gesetzliche Offenbarungsbefugnis (§§ 68 bis 77 SGB X) vorliegt.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Nach § 376d RVO schließen zwar die Krankenkassen zur Sicherung einer wirtschaftlichen Versorgung der Versicherten mit Heil- und Hilfsmitteln Vereinbarungen mit den Leistungserbringern über die Erbringung von Leistungen und deren Preise. Zur Erfüllung dieser Aufgabe ist es jedoch nicht erforderlich, Name und Anschrift derjenigen Versicherten, die entsprechende Leistungen in Anspruch nehmen, den Leistungserbringern zu offenbaren, insbesondere nicht für Zwecke der Vorbereitung und Planung. Hierzu dürften Zahlenangaben ausreichen. Die Offenbarung von Namen und Anschriften der die entsprechenden Leistungen in Anspruch nehmenden Versicherten an das Sanitätshaus war daher nicht zulässig und verstieß gegen das Sozialgeheimnis.

Meiner Empfehlung, die dem Sanitätshaus zur Verfügung gestellten Unterlagen mit den Namen und Anschriften der Versicherten zurückzufordern und künftig in vergleichbaren Fällen derartige Daten nicht an Leistungserbringer zu offenbaren, ist die AOK gefolgt.

- Ein Bürger hat sich darüber beschwert, daß die für ihn zuständige AOK im Rahmen eines sozialgerichtlichen Verfahrens zum Zwecke der Erstellung eines Gegengutachtens zu dem vom Gericht eingeholten ärztlichen Gutachten unter Mißachtung seines ausdrücklichen Widerspruchs die über ihn geführten Akten an den von der AOK bestellten Gutachter weitergegeben habe.

Die in den Akten der AOK und in dem vom Gericht eingeholten **Gutachten** über den Betroffenen festgehaltenen Daten unterliegen bei der AOK dem

Schutz des Sozialgeheimnisses (§ 35 Abs. 1 SGB I). Diese Daten dürfen, soweit nicht der Betroffene im Einzelfall eingewilligt hat (§ 67 Satz 1 SGB X), nur offenbart werden, wenn eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch oder für die Durchführung eines damit zusammenhängenden gerichtlichen Verfahrens erforderlich ist. Hiernach ist die AOK zur Wahrung ihrer Rechtsposition im sozialgerichtlichen Verfahren befugt, das vom Gericht eingeholte Gutachten, wenn es dieses für nicht überzeugend hält, zur Unterstützung ihrer Stellungnahme gegenüber dem Gericht von einem Gutachter überprüfen zu lassen. Grundsätzlich ist es auch unbedenklich, daß hierfür dem Gutachter die Akten der AOK zur Verfügung gestellt werden, da er allein beurteilen kann, was zur Abgabe seiner sachgerechten Stellungnahme erforderlich ist. Dies gilt allerdings nicht für Teile der Akte, die für die Begutachtung erkennbar nicht erforderlich sind. Entweder sind diese Aktenteile zu entfernen, oder von der Akte sind Kopien zu fertigen, die die für den Gutachter irrelevanten Aktenteile nicht enthalten.

Einer Offenbarung der in den Akten festgehaltenen Daten steht jedoch, soweit sie der AOK von einem Arzt zugänglich gemacht worden sind, § 76 SGB X entgegen. Nach § 76 Abs. 1 SGB X ist die Offenbarung personenbezogener Daten, die einem Sozialleistungsträger von einem Arzt zugänglich gemacht worden sind, nur unter den Voraussetzungen zulässig, unter denen diese Person selbst offenbarungsbefugt wäre. Diese Vorschrift gilt zwar nach § 76 Abs. 2 Satz 1 SGB X im Rahmen des § 69 Abs. 1 Nr. 1 SGB X nicht für personenbezogene Daten, die im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistungen zugänglich gemacht worden sind. In diesem Fall kann aber der Betroffene nach § 76 Abs. 2 Satz 2 SGB X der Offenbarung widersprechen. Von diesem Recht hat der Betroffene Gebrauch gemacht, so daß die Aktenteile, die der AOK von einem Arzt zugänglich gemacht wurden (z. B. von ihr eingeholte Gutachten), nicht an den von ihr mit der Erstellung des Gegengutachtens beauftragten Gutachter weitergegeben werden durften. Sollten diese Aktenteile bereits vor dem Widerspruch des Betroffenen an den Gutachter weitergegeben worden sein, so unterliegen sie nach meiner Auffassung dort einem Verwertungsverbot, auf das die AOK den Gutachter hinweisen muß.

Ich habe der AOK empfohlen, in vergleichbaren Fällen den Widerspruch des Betroffenen nach § 76 Abs. 2 Satz 2 SGB X zu beachten und, soweit Aktenteile bereits vor dem Widerspruch des Betroffenen an den Gutachter weitergegeben worden sind, den Gutachter darauf hinzuweisen, daß er diese Aktenteile nicht verwerten darf.

- Ein Landesverband der Innenkrankenkassen erhob Bedenken gegen die Vorgehensweise der Finanzverwaltung im Rahmen von Lohnsteuer-Außenprüfungen. Die Innungskrankenkassen gewähren bei ihnen freiwillig Versicherten, also auch ihren bei der dienstgebenden Kasse freiwillig versicherten DO-Angestellten **Beitragsnachlässe**. Die Finanzämter vertreten die Auffassung, daß es sich bei diesen Beitragsnachlässen um steuerpflichtigen Arbeitslohn handelt, und verlangen die Bekanntgabe der Namen der freiwillig versicherten Mitglieder getrennt nach Arbeitnehmern und Nicht-Arbeitnehmern sowie der Höhe der einzelnen Beitragsnachlässe.

Da die Beitragsnachlässe für freiwillig Versicherte von den Innungskrankenkassen nicht in ihrer Eigenschaft als Arbeitgeber, sondern in ihrer Eigenschaft als Krankenversicherungsträger gewährt werden, unterliegt die Tatsache der Gewährung eines Beitragsnachlasses und dessen Höhe in Verbindung mit

dem Namen des Versicherten dem Sozialgeheimnis (§ 35 Abs. 1 SGB I). Sie darf, sofern keine Einwilligung des Betroffenen (§ 67 Satz 1 Nr. 1 SGB X) vorliegt, nur unter den Voraussetzungen der §§ 68 bis 77 SGB X offenbart werden. Die Befugnis zur Offenbarung dieser Tatsache könnte sich allein aus § 71 Abs. 1 Nr. 3 SGB X ergeben.

Nach dieser Vorschrift ist eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflichten zur Sicherung des Steueraufkommens nach den §§ 93, 97, 105, 111 Abs. 1 und 5 und § 116 der Abgabenordnung (AO), soweit diese Vorschriften unmittelbar anwendbar sind. Die Auskunftspflicht nach § 200 AO besteht für die Krankenkasse nur als Steuerpflichtiger (Arbeitgeber), nicht aber als Leistungsträger.

Für die Krankenkasse als Leistungsträger besteht jedoch eine Auskunftspflicht nach § 93 AO. Nach § 93 Abs. 1 Satz 1 AO haben die Beteiligten und andere Personen der Finanzbehörde die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte zu erteilen. Nach § 93 Abs. 1 Satz 2 AO gilt dies auch für Behörden der Körperschaften des öffentlichen Rechts. Nach § 93 Abs. 1 Satz 3 AO sollen andere Personen als die Beteiligten erst dann zur Auskunft angehalten werden, wenn die Sachverhaltsaufklärung durch die Beteiligten nicht zum Ziele führt oder keinen Erfolg verspricht. Dieser Subsidiaritätsgrundsatz wird im vorliegenden Fall bei Befragung der Innungskrankenkasse nach Beitragsnachlässen für ihre freiwillig versicherten Mitarbeiter nicht verletzt. Ich habe jedoch Zweifel, ob die von den Finanzämtern ebenfalls verlangten Angaben über Nichtarbeitnehmer (insbesondere Namen) zur Feststellung des für die Besteuerung erheblichen Sachverhalts erforderlich sind.

- Ein Bürger hat sich bei mir darüber beschwert, daß ihm von einer Innungskrankenkasse unter Verwendung seiner Versicherungsdaten ein **Werbeschreiben** übersandt worden war, obwohl er nicht Mitglied dieser Kasse war. Er hielt die Verwendung seiner Daten, die der Innungskrankenkasse durch den Einzug der Renten- und Arbeitslosenversicherungsbeiträge zur Kenntnis gelangt waren, zu Werbezwecken für unzulässig.

Der Zugriff auf die Sozialversicherungsdaten von Nichtmitgliedern ist der Innungskrankenkasse möglich, weil nach dem durch die Datenerfassungsverordnung (DEVO) und durch die Datenübermittlungsverordnung (DÜVO) bundeseinheitlich geregelten Meldeverfahren zur gesetzlichen Sozialversicherung die Krankenkassen Empfänger der vom Arbeitgeber zu erstattenden Meldungen über die Beitragspflicht des Arbeitnehmers zur Sozialversicherung sind.

Die bei den Krankenkassen im Zuge des DEVO/DÜVO-Datenflusses gespeicherten Sozialversicherungsdaten unterliegen dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 Satz 1 SGB I). Dieser Geheimhaltungsanspruch richtet sich zwar gegen den Leistungsträger, also gegen die jeweilige Körperschaft, Anstalt oder Behörde (§ 12 SGB I). Eine Offenbarung im Sinne dieser Vorschrift liegt jedoch auch dann vor, wenn personenbezogene Daten innerhalb eines Leistungsträgers weitergegeben werden. Dieser hat dafür zu sorgen, daß die ihm bekanntgewordenen Sozialdaten innerhalb des Leistungsträgers nicht ungefügt offenbart werden. Nach § 67 Satz 1 SGB X ist eine Offenbarung, sofern nicht der Betroffene eingewilligt hat, nur zulässig, soweit eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch

erforderlich ist. Eine gesetzliche Aufgabe der Innungskrankenkasse, Mitglieder zu werben, ist nicht vorhanden. Die im Zuge des DEVO/DÜVO-Datenflusses bei ihr gespeicherten Daten dürfen daher innerhalb der Innungskrankenkasse nicht zum Zweck der Mitgliederwerbung offenbart werden.

Darüber hinaus folgt nach dem Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 aus dem Recht auf informationelle Selbstbestimmung, daß diese Daten nur zu dem gesetzlich bestimmten Zweck verwendet werden dürfen (BVerfGE 65, 1, 46).

Die Nutzung der genannten Daten für die Mitgliederwerbung verstößt daher sowohl gegen das Recht der Betroffenen auf informationelle Selbstbestimmung (Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes) als auch gegen das Sozialgeheimnis (§ 35 Abs. 1 Satz 1 SGB I).

Der Auffassung der Innungskrankenkasse, ihre Aufklärungspflicht gegenüber den Versicherten rechtfertige die Verwendung der im Zuge des DEVO/DÜVO-Datenflusses bei ihr gespeicherten Daten zur Mitgliederwerbung, kann ich nicht folgen. Nach § 13 SGB I sind die Leistungsträger verpflichtet, im Rahmen ihrer Zuständigkeit die Bevölkerung über die Rechte und Pflichten nach dem Sozialgesetzbuch aufzuklären. Adressat dieser Aufklärung ist die Bevölkerung, also ein unbestimmter Personenkreis. Bei dieser Aufklärung kann es sich daher immer nur um eine allgemeine Aufklärung handeln. Hierfür kommen zum Beispiel Plakate, Zeitungsanzeigen, Broschüren, periodische Publikationen, Prospekte, Aufklärungskampagnen sowie Informationsstände in Betracht. Nicht zulässig ist hingegen eine gezielte Ansprache einzelner Personen unter Verwendung der Versicherungsdaten (Name, Anschrift).

Die Innungskrankenkasse wird meiner Empfehlung, die im Zuge des DEVO/DÜVO-Datenflusses bei ihr gespeicherten Daten nur für den gesetzlich bestimmten Zweck zu verwenden, folgen.

#### **b) Kriegersopferversorgung**

Ein Bürger fragte bei mir an, ob er verpflichtet sei, den ihm vom Versorgungsamt im Rahmen seines Antrags auf **Zahnersatz** übersandten umfangreichen Fragebogen auszufüllen.

Gesetzliche Grundlage für die Erhebung von Daten über die Einkommens- und Vermögensverhältnisse des Betroffenen im Rahmen seines Antrages auf Gewährung von Zahnersatz ist § 60 Abs. 1 Nr. 1 SGB I in Verbindung mit § 11 Abs. 1 Nr. 4 und § 10 Abs. 2 und 7 des Bundesversorgungsgesetzes (BVG). Nach § 60 Abs. 1 Nr. 1 SGB I hat, wer Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Nach § 11 Abs. 1 Nr. 4 in Verbindung mit § 10 Abs. 2 BVG wird Schwerbeschädigten Heilbehandlung (hier: Zahnersatz) auch für Gesundheitsstörungen gewährt, die nicht als Folge einer Schädigung anerkannt sind. Nach § 10 Abs. 7 Buchst. a BVG sind die Ansprüche nach § 10 Abs. 2 BVG ausgeschlossen, wenn der Berechtigte ein Einkommen hat, daß die Jahresarbeitsverdienstgrenze der gesetzlichen Krankenversicherung übersteigt, es sei denn, daß der Berechtigte Anspruch auf Pflegezulage hat oder die Heilbehandlung wegen der als Folge einer Schädigung anerkannten Gesundheitsstörung nicht durch eine Krankenversicherung sicherstellen kann. Zur Prüfung, ob die Anspruchsvoraussetzungen für die Versorgung mit Zahnersatz nach § 10 Abs. 2, § 11 Abs. 1 Nr. 4 BVG vorliegen, sind Angaben über die Einkommensverhältnisse des Betroffenen erforderlich. Hierzu gehören Art und Höhe der Einkünfte sowie Aufwendungen, die mit der Erzielung des Einkommens verbunden sind.

Der von dem Versorgungsamt verwendete Vordruck enthält jedoch auch Daten, die keine Angaben über Einkommensverhältnisse sind, wie Name und Anschrift

des Arbeitgebers, zuständiges Finanzamt und Steuernummer, Höhe des Einheitswertes des Hausbesitzes, die Angabe, ob es sich um ein Ein- oder Mehrfamilienhaus handelt, Art des benutzten Fahrzeuges einschließlich des Hubraums und die Angabe, seit wann der Betroffene verheiratet, verwitwet oder geschieden ist. Diese Angaben können allenfalls auf freiwilliger Grundlage erhoben werden. Dabei ist zu beachten, daß auch freiwillige Angaben nur erhoben werden dürfen, wenn sie der Aufgabenerfüllung zumindest dienlich sind. Zweifel an der Dienlichkeit bestehen insbesondere bei der Angabe, seit wann der Betroffene verheiratet, verwitwet oder geschieden ist, sowie bei der Angabe der Art und des Hubraums des benutzten Kraftfahrzeuges, außerdem bei der Angabe „Einfamilienhaus/Mehrfamilienhaus“ und „zuletzt festgestellter Einheitswert“.

Ich habe daher dem Versorgungsamt empfohlen,

- zu prüfen, inwieweit Angaben wie Namen und Anschrift des Arbeitgebers, zuständiges Finanzamt und Steuernummer, Einfamilienhaus/Mehrfamilienhaus, Höhe des zuletzt festgestellten Einheitswertes, Art des benutzten Fahrzeuges einschließlich des Hubraums und die Angabe, seit wann der Betroffene verheiratet, verwitwet oder geschieden ist, für die Aufgabenerfüllung dienlich sind;
- soweit diese Angaben hierfür dienlich sind, den Betroffenen auf die Freiwilligkeit dieser Angaben hinzuweisen;
- soweit die Angaben für die Aufgabenerfüllung nicht dienlich sind, von ihrer Erhebung abzusehen.

### c) Sozialhilfe

- Ein Bürger wandte sich dagegen, daß das Sozialamt seine Großmutter als Hilfesuchende zu seinen persönlichen Verhältnissen befragt hat.

Gesetzliche Grundlage für die Erhebung personenbezogener Daten **unterhaltspflichtiger Angehöriger** bei dem Hilfesuchenden ist § 60 Abs. 1 Nr. 1 SGB I in Verbindung mit § 2 Abs. 1 des Bundessozialhilfegesetzes (BSHG) und § 1601 BGB. Nach § 60 Abs. 1 Nr. 1 SGB I hat derjenige, der Sozialleistungen beantragt oder erhält, alle Tatsachen anzugeben, die für die Leistung erheblich sind. Nach § 2 Abs. 1 BSHG erhält ein Hilfesuchender Sozialhilfe nicht, soweit er sich selbst helfen kann oder soweit er die erforderliche Hilfe von anderen, besonders von Angehörigen erhält. Da nach § 1601 BGB Verwandte in gerader Linie einander, also auch Enkel ihren Großeltern unterhaltspflichtig sind, ist das Sozialamt zur Aufgabenerfüllung auf die Kenntnis des Namens, der Anschrift und des Verwandtschaftsverhältnisses dieser unterhaltspflichtigen Angehörigen des Hilfesuchenden angewiesen. Die Erhebung dieser Daten beim Hilfesuchenden ist daher zulässig. Soweit darüber hinaus die Kenntnis weiterer Angaben über die unterhaltspflichtigen Angehörigen zur Prüfung ihrer Leistungsfähigkeit erforderlich ist, dürfen diese Angaben nicht von dem Hilfesuchenden verlangt, sondern nur bei den Betroffenen selbst erhoben werden.

Ich habe daher dem Oberstadtdirektor empfohlen, bei dem Hilfesuchenden außer Name, Anschrift und Verwandtschaftsverhältnis keine Angaben über unterhaltspflichtige Angehörige zu erheben.

- Mehrere Eingaben richteten sich gegen die von Sozialämtern zur Überprüfung der **Einkommens- und Vermögensverhältnisse** unterhaltspflichtiger Angehöriger verwendeten Vordrucke „Prüfbogen zur Beurteilung der Zahlungsfähigkeit“ und „Anfrage über Arbeitsverdienst“ sowie gegen das Verfahren, Lohnauskünfte ohne Wissen der Betroffenen unmittelbar bei deren Arbeitgebern einzuholen.

Gesetzliche Grundlage für die Erhebung von personenbezogenen Daten bei unterhaltspflichtigen Angehörigen des Hilfesuchenden ist § 116 Abs. 1 BSHG. Nach dieser Vorschrift sind die Unterhaltspflichtigen verpflichtet, dem Träger der Sozialhilfe über ihre Einkommens- und Vermögensverhältnisse Auskunft zu geben, soweit die Durchführung des Bundessozialhilfegesetzes es erfordert. Nach § 1601 BGB sind Verwandte in gerader Linie einander unterhaltspflichtig. Da nach § 2 Abs. 1 BSHG ein Hilfesuchender Sozialhilfe nicht erhält, soweit er sich selbst helfen kann oder soweit er die erforderliche Hilfe von anderen, besonders von Angehörigen erhält, ist die Kenntnis der Einkommens- und Vermögensverhältnisse des Unterhaltspflichtigen und seines Ehegatten sowie der Einkommensverhältnisse seiner zu seinem Haushalt gehörenden sonstigen Familienangehörigen zur Durchführung des Bundessozialhilfegesetzes erforderlich. Hierzu gehören Art und Höhe der Einkünfte, Aufwendungen, die mit der Erzielung des Einkommens verbunden sind, Vermögen, Miete oder Belastung bei Eigenheim, Unterhaltspflichten sowie außergewöhnliche wirtschaftliche Belastungen.

Der von den Sozialämtern verwendete Vordruck enthält jedoch auch Daten, die keine Angaben über Einkommens- und Vermögensverhältnisse (§ 116 Abs. 1 BSHG) sind, wie Beruf, Krankenkasse, Name und Anschrift des Arbeitgebers des Unterhaltspflichtigen, Name und Anschrift des Arbeitgebers von Kindern oder sonstigen Angehörigen im Haushalt des Zahlungspflichtigen und deren Verwandtschaftsverhältnis zu ihm, deren Familienstand sowie Name, Anschrift, Familienstand und Nettoeinkommen von Kindern außerhalb des Haushalts und deren Verwandtschaftsverhältnis zum Zahlungspflichtigen sowie den Verwendungszweck von Schuldverpflichtungen des Unterhaltspflichtigen. Diese Angaben könnten allenfalls auf freiwilliger Grundlage erhoben werden. Dabei ist zu beachten, daß auch freiwillige Angaben nur erhoben werden dürfen, wenn sie für die Aufgabenerfüllung zumindest dienlich sind.

Zweifel an der Dienlichkeit habe ich insbesondere bei der Angabe von Namen und Anschrift des Arbeitgebers von Kindern und sonstigen Angehörigen im Haushalt des Zahlungspflichtigen, deren Verwandtschaftsverhältnis zu ihm und deren Familienstand sowie bei der Angabe des Namens, der Anschrift, des Familienstandes und des Nettoeinkommens von Kindern außerhalb des Haushalts, soweit diese vom Unterhaltspflichtigen nicht ganz oder teilweise unterhalten werden, deren Verwandtschaftsverhältnis zum Unterhaltspflichtigen und bei Angaben über den Verwendungszweck von Schuldverpflichtungen des Unterhaltspflichtigen.

Nach meiner Auffassung ist auch die Angabe der Krankenkasse nicht in allen Fällen dienlich. Nach § 205 Abs. 1 RVO erhalten Versicherte unter bestimmten Voraussetzungen für den unterhaltsberechtigten Ehegatten und die unterhaltsberechtigten Kinder Maßnahmen zur Früherkennung von Krankheiten, Krankenhilfe und sonstige Hilfen unter den gleichen Voraussetzungen und im gleichen Umfang wie Versicherte. Nach § 205 Abs. 3 Satz 2 bis 4 RVO besteht der Anspruch für Kinder grundsätzlich bis zur Vollendung des 18. Lebensjahres; er verlängert sich unter bestimmten Voraussetzungen. Für Kinder, die die Altersgrenze überschritten haben, sowie in den Fällen des § 205 Abs. 3 Satz 5 RVO und für vom Versicherten geschiedene Ehegatten besteht, auch wenn sie unterhaltsberechtigt sind, kein Anspruch auf Familienkrankenhilfe. In diesen Fällen wird die Angabe der Krankenkasse zur Aufgabenerfüllung des Sozialamtes nicht benötigt; insoweit ist daher von ihrer Erhebung abzusehen.

Gesetzliche Grundlage für die Erhebung von Daten über Arbeitsverdienst bei dem Arbeitgeber des Betroffenen ist § 116 Abs. 2 BSHG. Nach dieser Vorschrift ist der Arbeitgeber verpflichtet, dem Träger der Sozialhilfe über Art

und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst des bei ihm beschäftigten Unterhaltspflichtigen Auskunft zu geben, soweit die Durchführung des Bundessozialhilfegesetzes es erfordert.

In den von den Sozialämtern verwendeten Vordrucken „Anfrage über Arbeitsverdienst“ werden jedoch mehr Angaben verlangt als in § 116 Abs. 2 BSHG vorgesehen, wie „auf eigenen Wunsch entlassen“, Entlassungsgrund, Krankenkasse, Lohnsteuerermäßigung, Lohnpfändungen und Abtretungen, Ehegatte berufstätig, Ausstellung einer zweiten Lohnsteuerkarte. Für die Erhebung von Daten, die nicht in § 116 Abs. 2 BSHG genannt sind, besteht keine gesetzliche Grundlage. Von ihrer Erhebung ist daher abzu-  
sehen.

Nach § 116 Abs. 2 BSHG hat die Sozialbehörde zwar einen Auskunftsanspruch gegen den Arbeitgeber des Betroffenen. Jedoch ist bei Eingriffen in das Grundrecht des Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung wie auch in das durch Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 2 des Grundgesetzes gewährleistete allgemeine Persönlichkeitsrecht der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Danach muß der Eingriff zur Erreichung des vom Gesetzgeber angestrebten Zwecks erforderlich sein; unter mehreren für die Erreichung des Zwecks geeigneten Mitteln ist dasjenige zu wählen, das den Betroffenen am wenigsten belastet (BVerfGE 38, 202).

Der Verhältnismäßigkeitsgrundsatz gebietet mithin, soweit Angaben über Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst des Unterhaltspflichtigen benötigt werden, nicht den Namen und die Anschrift des Arbeitgebers zu erheben, um die benötigten Angaben unmittelbar von diesem zu verlangen, sondern stattdessen zunächst dem Betroffenen Gelegenheit zu geben, selbst beim Arbeitgeber eine Bescheinigung mit den benötigten Angaben einzuholen; hierfür sollte ihm ein neutral gehaltener Vordruck zur Verfügung gestellt werden, der die Sozialbehörde und den Verwendungszweck der Daten nicht erkennen läßt. Dementsprechend muß jede Angabe, die solche Rückschlüsse zuläßt, wie Absender, Geschäftszeichen, Hinweis auf § 116 Abs. 2 und 4 BSHG sowie auf die Gewährung von Sozialhilfe und die Angabe des Sozialamts als Empfänger unterbleiben.

Ich habe daher den zuständigen Stellen empfohlen,

- zu prüfen, inwieweit die Angaben über Beruf, Name und Anschrift des Arbeitgebers von Kindern und sonstigen Angehörigen im Haushalt des Zahlungspflichtigen und deren Verwandtschaftsverhältnis zu ihm, deren Familienstand sowie Name, Anschrift, Familienstand und Nettoeinkommen von Kindern außerhalb des Haushalts, soweit diese nicht ganz oder teilweise vom Unterhaltspflichtigen unterhalten werden, und deren Verwandtschaftsverhältnis zum Zahlungspflichtigen sowie Angaben über den Verwendungszweck von Schuldverpflichtungen des Unterhaltspflichtigen für die Aufgabenerfüllung dienlich sind;
- soweit diese Angaben dienlich sind, den Betroffenen nach § 9 Abs. 2 BDSG auf die Freiwilligkeit dieser Angaben hinzuweisen;
- soweit die Angaben für die Aufgabenerfüllung nicht dienlich sind, von ihrer Erhebung abzusehen;
- die Angabe über die Krankenkasse unter Hinweis auf § 205 RVO nur in den Fällen zu erheben, in denen sie benötigt wird;
- soweit Angaben über Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst benötigt werden, nicht Namen und Anschrift des Arbeitgebers des Betroffenen zu erheben, um die benötigten Angaben unmittelbar von diesem zu verlangen, sondern stattdessen zunächst dem

Betroffenen Gelegenheit zu geben, selbst beim Arbeitgeber mit einem von der Sozialbehörde zur Verfügung gestellten, neutral gehaltenen Vordruck die benötigten Angaben zu beschaffen;

- in dem Vordruck „Anfrage über Arbeitsverdienst“ Angaben, die durch § 116 Abs. 2 BSHG nicht gedeckt sind, wie insbesondere „auf eigenen Wunsch entlassen“, Entlassungsgrund, Krankenkasse, Lohnsteuerermäßigung, Lohnpfändungen und Abtretungen, Ehegatte berufstätig, Ausstellung einer zweiten Lohnsteuerkarte zu streichen.

- Ein Betroffener verlangte die **Löschung** der nicht benötigten Daten.

Da davon auszugehen ist, daß die mit dem Vordruck „Prüfbogen zur Beurteilung der Zahlungsfähigkeit“ erhobenen Daten nicht in einer Datei gespeichert, sondern lediglich in Akten festgehalten werden, findet die Vorschrift des § 84 SGB X, die unter bestimmten Voraussetzungen einen Anspruch auf Löschung von Daten vorsieht, keine Anwendung. Es gilt jedoch auch hier das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung, aus dem sich nach meiner Auffassung ein Anspruch auf Löschung der Daten ergibt, die zur Aufgabenerfüllung weder erforderlich noch dienlich sind und deshalb gar nicht hätten erhoben werden dürfen. Das gleiche muß für solche Angaben gelten, die zwar zur Aufgabenerfüllung dienlich sind, bei deren Erhebung aber nicht auf die Freiwilligkeit hingewiesen wurde (vgl. Dammann in Simitis/Dammann/Mallmann/Reh, BDSG, 3. Aufl., § 9 Rdnr. 50). In diesen Fällen müssen die Angaben unkenntlich gemacht werden.

Ich habe daher empfohlen, die mit dem Prüfbogen erhobenen Daten zu löschen, wenn sie zur Aufgabenerfüllung weder erforderlich noch dienlich sind oder wenn bei der Erhebung von dienlichen Angaben der Hinweis auf die Freiwilligkeit unterblieben ist.

- Ein Bürger machte mich auf die Verwaltungsrichtlinien zur Durchführung der Satzung des Landschaftsverbandes Westfalen-Lippe über die Heranziehung der örtlichen Träger der Sozialhilfe aufmerksam, die in Ziffer 5.2 Satz 1 vorsahen, daß „die **Anstalten, Heime oder gleichartigen Einrichtungen** gehalten sind, den kostenzusagenden Trägern der Sozialhilfe mitzuteilen, sobald das Eigengeldkonto bei Minderjährigen 1 200 DM und bei Volljährigen 4 000 DM erreicht hat“.

Eine nach Artikel 4 Abs. 2 der Landesverfassung erforderliche gesetzliche Grundlage für die dort vorgesehene Erhebung personenbezogener Daten der Betroffenen bei den Anstalten, Heimen und gleichartigen Einrichtungen ist nicht ersichtlich. Die Datenerhebung kann insbesondere nicht auf § 60 Abs. 1 Nr. 2 SGB I gestützt werden. Nach dieser Vorschrift hat, wer Sozialleistungen beantragt oder erhält, Änderungen in den Verhältnissen, die für die Leistung erheblich sind oder über die im Zusammenhang mit der Leistung Erklärungen abgegeben worden sind, unverzüglich mitzuteilen. § 60 Abs. 1 Nr. 2 SGB I verpflichtet also nur den Hilfeempfänger oder seinen gesetzlichen Vertreter zur Mitteilung der Änderungen. Eine Mitwirkungspflicht Dritter dergestalt, daß diese anstelle des Hilfeempfängers dem Leistungsträger die Änderung leistungserheblicher Verhältnisse des Betroffenen mitzuteilen haben, kann der Vorschrift nicht entnommen werden. Die in Nr. 5.2 Satz 1 der Richtlinien vorgesehenen Mitteilungen sind daher nur mit Einwilligung des Betroffenen oder seines gesetzlichen Vertreters zulässig. Im übrigen muß es dem Betroffenen oder seinem gesetzlichen Vertreter freistehen, selbst den Leistungsträger zu unterrichten, sobald das Eigengeldkonto bei Minderjährigen 1 200 DM und bei Volljährigen 4 000 DM erreicht hat.

Ich habe dem Landschaftsverband Westfalen-Lippe empfohlen, Nr. 5.2 Satz 1 der Richtlinien zu streichen und die Träger der Sozialhilfe darauf hinzuweisen, daß eine Erhebung der Daten bei den Anstalten, Heimen und gleicharti-

gen Einrichtungen ohne Einwilligung des Betroffenen oder seines gesetzlichen Vertreters nicht zulässig ist.

Der Landschaftsverband hat seine Richtlinien nunmehr wie folgt gefaßt:

„Die Hilfeempfänger bzw. die gesetzlichen Vertreter haben nach § 60 Abs. 1 Nr. 2 SGB I die hilfgewährenden (kostenzusagenden) Träger der Sozialhilfe zu unterrichten, sobald das Eigengeldkonto 4 000 DM (bei minderjährigen Hilfeempfängern 1 200 DM) erreicht hat.

Die Anstalten, Heime und gleichartigen Einrichtungen werden gebeten, mit vorheriger Einwilligung des Hilfeempfängers bzw. dessen gesetzlichen Vertreters diesem bei der Erfüllung seiner gesetzlichen Verpflichtung behilflich zu sein.“

Gegen den zweiten Satz bestehen Bedenken, weil die Formulierung „werden gebeten, behilflich zu sein“ die Gefahr in sich birgt, daß die Heimbewohner unter Druck gesetzt werden, die Einwilligung zu erteilen. Damit wäre die Einwilligung nicht mehr freiwillig.

- Ein Bürger hat mir mitgeteilt, daß ein Oberkreisdirektor die Sozialämter der kreisangehörigen Gemeinden angewiesen habe, bei der Beantragung von Hilfe zum Lebensunterhalt von den Betroffenen grundsätzlich eine Erklärung über die **Entbindung** ihrer Ärzte **von der Schweigepflicht** zu verlangen.

Nach § 60 Abs. 1 Nr. 1 SGB I hat, wer Sozialleistungen beantragt oder erhält, auf Verlangen des zuständigen Leistungsträgers der Erteilung der erforderlichen Auskünfte durch Dritte zuzustimmen. Diese Mitwirkungspflicht besteht jedoch nur, soweit Auskünfte Dritter für die Aufgabenerfüllung des Sozialleistungsträgers erforderlich sind. Die generelle Anforderung von Erklärungen über die Entbindung von der ärztlichen Schweigepflicht bei Anträgen auf Hilfe zum Lebensunterhalt ohne Rücksicht auf die Erforderlichkeit im Einzelfall erfüllt diese Voraussetzungen nicht.

Zudem ist in den erforderlichen Fällen die Erklärung über die Entbindung von der ärztlichen Schweigepflicht so zu fassen, daß für den Betroffenen eindeutig erkennbar ist, welchen Arzt er von der Schweigepflicht entbindet. Bei einer generellen Anforderung dieser Erklärung dürfte auch diese Voraussetzung nicht erfüllt sein.

Ich habe daher dem Oberkreisdirektor empfohlen,

- eine Erklärung über die Entbindung von der ärztlichen Schweigepflicht nur dann zu verlangen, wenn feststeht, daß sie zur Bearbeitung des Einzelfalles erforderlich ist;
  - in den erforderlichen Fällen die Erklärung über die Entbindung von der ärztlichen Schweigepflicht so zu fassen, daß für den Betroffenen eindeutig erkennbar ist, welchen Arzt er von der Schweigepflicht entbindet.
- Durch eine Eingabe wurde mir bekannt, daß Sozialhilfeträger für Alkoholabhängige, die sich in einer Alkoholentwöhnungsbehandlung befinden, zum Teil ohne Wissen der Betroffenen einen **Antrag auf Kindergeld** stellen. Hierzu bittet der Sozialhilfeträger den leitenden Arzt der Fachklinik um eine gutachtliche Stellungnahme, ob bei den Betroffenen eine körperliche, geistige oder seelische Behinderung vorliegt, und leitet diese Stellungnahme zur Prüfung der Voraussetzungen für die Gewährung von Kindergeld an das Arbeitsamt als Kindergeldkasse weiter.

Die in dem Kindergeldantrag wie auch in der Stellungnahme des leitenden Arztes enthaltenen Angaben über den Betroffenen unterliegen bei dem Sozialhilfeträger dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 SGB I). Sofern nicht der Betroffene eingewilligt hat (§ 67 Satz 1 SGB X), ist die

Offenbarung dieser Angaben nur zulässig, soweit eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist die Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Dabei sind an die Erforderlichkeit strenge Anforderungen zu stellen. Es genügt nicht, wenn die Offenbarung der Aufgabenerfüllung lediglich dienlich ist oder sie erleichtert; die Offenbarung muß vielmehr zur Aufgabenerfüllung notwendig sein.

Es kann dahinstehen, ob die Offenbarung der in dem Kindergeldantrag sowie in der Stellungnahme des leitenden Arztes der Fachklinik über den Betroffenen festgehaltenen Daten an das Arbeitsamt zur Erfüllung einer gesetzlichen Aufgabe des Sozialhilfeträgers nach dem Sozialgesetzbuch erforderlich ist. Zu denken wäre hier an die Aufgabe nach § 2 Abs. 1 BSHG, wonach demjenigen Hilfe nicht gewährt wird, der Hilfe von anderen, insbesondere auch von anderen Sozialleistungsträgern erhalten kann. Die Offenbarung der genannten Angaben gegenüber dem Arbeitsamt als der zuständigen Kindergeldkasse wäre jedoch geeignet, die nach § 1 Abs. 2 Satz 2 BSHG dem Sozialhilfeträger ebenfalls obliegende Aufgabe der Rehabilitation des Betroffenen zu vereiteln, mindestens aber zu gefährden.

Auf jeden Fall verstößt der mit der Offenbarung dieser Angaben verbundene Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch in sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung gegen den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz. Danach muß die mit dem Eingriff verbundene Belastung des Betroffenen in einem angemessenen Verhältnis zu dem zu erreichenden Zweck stehen. Die Offenbarung der Suchtkrankheit des Betroffenen an das Arbeitsamt zum Zwecke einer zeitlich begrenzten Kostenentlastung des Sozialhilfeträgers belastet den Betroffenen unverhältnismäßig, da sie seine Vermittlungschancen nachhaltig beeinträchtigen kann.

- In meinem sechsten Tätigkeitsbericht (C.8.c) habe ich auf die Praxis des Landeswohlfahrtsverbands Hessen hingewiesen, der an die Spitzenorganisationen aller Sozialhilfeträger der Bundesrepublik Listen versandt hat, in denen vor sogenannten **Unterstützungsschwindlern** gewarnt wurde. Der Minister für Arbeit, Gesundheit und Soziales teilt meine Auffassung, daß das vom Landeswohlfahrtsverband Hessen seinerzeit praktizierte Verfahren mit den datenschutzrechtlichen Bestimmungen nicht vereinbar war. Allerdings hielt er Warnmeldungen über Tuberkulosekranke und Mitteilungen der überörtlichen Träger an die örtlichen Träger für zulässig.

Der Auffassung, daß Warnmeldungen über Tuberkulosekranke zulässig seien, kann nicht gefolgt werden. Nach § 71 Abs. 1 Nr. 2 SGB X ist eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflichten zum Schutz der öffentlichen Gesundheit nach § 4 Abs. 1 Nr. 1 bis 4 und Abs. 2 des Bundesseuchengesetzes (BSeuchG). Diese Mitteilungspflicht besteht nach § 5 BSeuchG gegenüber dem für den Aufenthaltsort des Betroffenen zuständigen Gesundheitsamt. Daraus kann, selbst wenn der Aufenthaltsort des Betroffenen unbekannt ist, eine Berechtigung zur Offenbarung der Tatsache, daß der Betroffene an Tuberkulose erkrankt ist, im Rahmen eines Warndienstes nicht hergeleitet werden.

Auch auf § 69 Abs. 1 Nr. 1 SGB X in Verbindung mit § 48 Abs. 1 BSHG können derartige Warnmeldungen über Tuberkulosekranke nicht gestützt werden. Nach § 48 Abs. 1 BSHG ist es zwar Aufgabe des Trägers der

Sozialhilfe, im Rahmen der Gewährung von Tuberkulosehilfe die Umgebung der Kranken gegen die Übertragung der Tuberkulose zu schützen. Zur Umgebung des Kranken rechnen alle Personen, mit denen der Kranke in der Familie, der Wohnung und der Nachbarschaft, bei der Arbeit und während der Freizeit nicht nur ausnahmsweise Kontakt hat (vgl. Knopp/Fichtner, BSHG, 5. Aufl., § 48 Rdnr. 3). Diese Vorschrift rechtfertigt somit ein Tätigwerden nur im engeren Umkreis des Betroffenen. Zur Erfüllung dieser Aufgabe nach dem Sozialgesetzbuch ist es jedoch nicht erforderlich, die Tatsache der Erkrankung an Tuberkulose dem Landeswohlfahrtsverband Hessen und von dort allen anderen Trägern der Sozialhilfe im Bundesgebiet zu offenbaren.

Der vom Minister für Arbeit, Gesundheit und Soziales vertretenen Auffassung, daß es bei dem Datenaustausch zwischen dem überörtlichen und dem von ihm herangezogenen örtlichen Träger der Sozialhilfe nicht zu Offenbarungen nach § 35 SGB I kommt, muß nachdrücklich widersprochen werden. Alle in § 35 Abs. 1 SGB I genannten Stellen sind im Verhältnis zueinander Dritte, so daß die Weitergabe personenbezogener Daten vom überörtlichen an den örtlichen Sozialhilfeträger oder umgekehrt auch dann eine Offenbarung darstellt, wenn man entgegen meiner Auffassung der Ansicht ist, daß der Datenfluß innerhalb eines Leistungsträgers keine Offenbarung im Sinne von § 35 SGB I sei.

Die Zulässigkeit einer solchen Offenbarung richtet sich nach § 69 Abs. 1 Nr. 1 SGB X. Danach muß die Offenbarung zur Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich sein. Dabei sind an die Erforderlichkeit strenge Anforderungen zu stellen. Es genügt nicht, wenn die Offenbarung der Aufgabenerfüllung lediglich dienlich ist oder sie erleichtert. Die Offenbarung muß vielmehr zur Aufgabenerfüllung im Einzelfall notwendig sein. Darüber hinaus ist der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Ob danach eine Warnmeldung durch einen überörtlichen an einen örtlichen Träger oder umgekehrt zulässig ist, kann nur im Einzelfall beurteilt werden. Eine Warnmeldung über eine Person mit betrügerischen Absichten gezielt an eine andere Dienststelle könnte allenfalls dann zur Aufgabenerfüllung erforderlich sein, wenn mit einer gewissen Wahrscheinlichkeit davon ausgegangen werden kann, daß sich der Betroffene an diese Stelle wendet.

Die von einem Sozialhilfeträger vertretene Ansicht, daß sich die Zulässigkeit der Offenbarung personenbezogener Daten sogenannter Unterstützungsschwindler aus § 71 Abs. 1 Nr. 1 SGB X ergibt, ist unzutreffend. Nach dieser Vorschrift ist eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflichten zur Abwendung geplanter Straftaten nach § 138 StGB. Diese Voraussetzung liegt bei Warnmeldungen wegen der Erschleichung von Sozialhilfeleistungen nicht vor. Der Straftatbestand des Betruges (§ 263 StGB) ist in § 138 StGB nicht genannt.

Ich habe den beteiligten Trägern der Sozialhilfe empfohlen, künftig Warnmeldungen an den überörtlichen Träger der Sozialhilfe nur dann weiterzuleiten, wenn die Offenbarungsvoraussetzungen des § 69 Abs. 1 Nr. 1 SGB X eindeutig vorliegen.

- Ein Bürger beschwerte sich darüber, daß seine geschiedene Ehefrau Kenntnis über seine Einkommens- und Vermögensverhältnisse hatte, die er im Rahmen der Überprüfung seiner Unterhaltspflicht für seine Tochter dem Sozialamt dargelegt hatte. Die Überprüfung hatte ergeben, daß er in der Lage war, einen wesentlich höheren Unterhaltsbeitrag für seine Tochter zu leisten. Das Sozialamt hatte daraufhin die geschiedene Ehefrau des Betroffenen aufgefordert, eine **Unterhaltsabänderungsklage** zu erheben. Hierzu wurden ihr die vom Betroffenen eingereichten Lohnabrechnungen ausgehändigt.

Die im Rahmen der Überprüfung seiner Unterhaltsfähigkeit vom Betroffenen dem Sozialamt mitgeteilten Angaben über seine Einkommens- und Vermögensverhältnisse unterliegen dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 SGB I). Sofern nicht der Betroffene eingewilligt hat (§ 67 Satz 1 SGB X), dürfen diese Angaben nur unter den Voraussetzungen der §§ 68 bis 77 SGB X offenbart werden.

Die Offenbarung konnte im vorliegenden Fall nicht auf § 74 Nr. 2 Buchst. a SGB X gestützt werden. Danach ist eine Offenbarung personenbezogener Daten zulässig, soweit sie erforderlich ist für die Geltendmachung eines gesetzlichen Unterhaltsanspruchs außerhalb eines Verfahrens nach Nr. 1 Buchst. a, soweit der Betroffene nach den Vorschriften des bürgerlichen Rechts, insbesondere nach § 1605 BGB zur Auskunft verpflichtet ist und diese Pflicht innerhalb angemessener Frist, nachdem er unter Hinweis auf die in diesem Gesetzbuch enthaltene Offenbarungsbefugnis der in § 35 SGB I genannten Stellen gemahnt wurde, nicht oder nicht vollständig erfüllt hat. Diese Voraussetzung lag hier nicht vor.

In Betracht kam jedoch eine Offenbarung auf Grund des § 69 Abs. 1 Nr. 1 SGB X. Nach dieser Vorschrift ist eine Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch oder für die Durchführung eines damit zusammenhängenden gerichtlichen Verfahrens erforderlich ist. Nach § 11 BSHG ist Hilfe zum Lebensunterhalt dem zu gewähren, der seinen notwendigen Lebensunterhalt nicht oder nicht ausreichend aus eigenen Kräften und Mitteln beschaffen kann. Nach § 2 Abs. 2 Satz 1 BSHG werden Verpflichtungen anderer, besonders Unterhaltspflichtiger durch dieses Gesetz nicht berührt. Verwandte in gerader Linie sind verpflichtet, einander Unterhalt zu gewähren (§ 1601 BGB). Der Betroffene ist somit seiner Tochter unterhaltspflichtig. Durch eine Erhöhung der Unterhaltsleistungen verminderten sich die Sozialhilfeleistungen an seine Tochter. Die Weitergabe der Lohnabrechnungen an die sorgeberechtigte Mutter der Hilfeempfängerin diene somit der Erfüllung der Aufgaben nach § 11 BSHG.

Bei derartigen Eingriffen in das Recht des Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes sowie in sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung ist allerdings der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Danach muß die mit dem Eingriff verbundene Belastung des Betroffenen in einem angemessenen Verhältnis zu dem zu erreichenden Zweck stehen; unter mehreren zur Erreichung des Zwecks geeigneten Mitteln ist dasjenige zu wählen, das den Betroffenen am wenigsten belastet.

Die Weitergabe der Lohnabrechnungen an die sorgeberechtigte Mutter ist damit nicht vereinbar. Sie belastet den Betroffenen unverhältnismäßig, weil der Mutter durch die Weitergabe Daten offenbart wurden, die zur Geltendmachung von Unterhaltsansprüchen geeignet sind, die weit über die Sozialhilfeleistungen hinausgehen. Dies zu ermöglichen, gehört nicht zu den gesetzlichen Aufgaben des Trägers der Sozialhilfe. Dieser hätte eine Verminderung seiner finanziellen Belastung auch dadurch herbeiführen können, daß er den Unterhaltsanspruch in diesem Umfang nach §§ 90 und 91 BSHG auf sich überleitet und ihn selbst geltend macht. Er hätte die Sozialhilfeleistungen aber auch einstellen und die Mutter zur Geltendmachung eines höheren Unterhaltsanspruchs auf die Auskunftspflicht des Betroffenen nach § 1605 BGB und auf die Möglichkeit einer Offenbarung der Einkommensdaten nach § 74 Nr. 2 Buchst. a SGB X – nach Mahnung des Betroffenen unter Hinweis auf diese Offenbarungsbefugnis – verweisen können. Jedes dieser beiden Mittel hätte den Betroffenen weniger belastet als die Weitergabe der Lohnab-

rechnungen. Wegen Verstoßes gegen den Verhältnismäßigkeitsgrundsatz war daher diese Weitergabe nicht zulässig.

Meiner Empfehlung sicherzustellen, daß künftig in vergleichbaren Fällen personenbezogene Daten des Unterhaltspflichtigen nicht an den Unterhaltsberechtigten offenbart werden, wird der Oberstadtdirektor folgen.

- Mehrere Eingaben betrafen wiederum die Frage des Schutzes von **Gesprächen vertraulichen Inhalts** bei Sozialämtern. Wie ich bereits in meinem sechsten Tätigkeitsbericht (C.8.a) dargelegt habe, ergibt sich aus § 35 Abs. 1 Satz 1 SGB I der Anspruch des Betroffenen, daß Gespräche mit vertraulichem Inhalt so geführt werden, daß niemand mithören kann. Dies könnte zum Beispiel dadurch erreicht werden, daß für Beratungsgespräche beim Sozialamt ein Einzelzimmer oder ein Besprechungszimmer zur Verfügung gestellt wird und der Betroffene auf die Möglichkeit der Gesprächsführung in einem gesonderten Raum hingewiesen wird.

Die zuständigen Stadtdirektoren werden durch entsprechende organisatorische oder bauliche Maßnahmen sicherstellen, daß Gespräche vertraulichen Inhalts nicht von unbeteiligten Dritten mitgehört werden können.

#### d) Jugendhilfe

- Ein Bürger wandte sich dagegen, daß ein Jugendamt in seiner Eigenschaft als Amtspfleger eines nichtehelichen Kindes zum Zwecke der Neuregelung des **Kindesunterhalts** unmittelbar den Arbeitgeber des Kindesvaters nach dessen Einkommen befragt hat. Der Betroffene befürchtete, daß auf diese Weise dem Arbeitgeber bekanntgeworden sei, daß der Betroffene Unterhalt für ein nichteheliches Kind zu zahlen hat.

Die Amtspflegschaft des Jugendamts beruht auf § 40 Abs. 1 des Gesetzes für Jugendwohlfahrt (JWG), das nach Artikel II § 1 Nr. 16 SGB I als besonderer Teil des Sozialgesetzbuchs gilt. Die Wahrnehmung der Amtspflegschaft kann als Sozialleistung im Sinne des Sozialgesetzbuchs angesehen werden (Schellhorn in Burdinski/v. Maydell/Schellhorn, SGB-AT, 2. Aufl., § 27 Rdnr. 10). Die nach § 40 Abs. 1 JWG in Verbindung mit § 1706 Nr. 2 BGB dem Jugendamt als Amtspfleger obliegende Geltendmachung von Unterhaltsansprüchen des Kindes ist somit eine gesetzliche Aufgabe nach dem Sozialgesetzbuch.

Indem das Jugendamt unmittelbar den Arbeitgeber nach dem Verdienst des Betroffenen befragt hat, hat es dem Arbeitgeber zumindest die Tatsache offenbart, daß der Betroffene Kontakte zum Jugendamt hat. Diese Tatsache unterliegt dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 Satz 1 SGB I). Sie darf, sofern keine Einwilligung des Betroffenen (§ 67 Satz 1 Nr. 1 SGB X) vorliegt, nur unter den Voraussetzungen der §§ 68 bis 77 SGB X offenbart werden.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist die Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Dabei sind an die Erforderlichkeit strenge Anforderungen zu stellen. Es genügt nicht, wenn die Offenbarung der Aufgabenerfüllung lediglich dienlich ist oder sie erleichtert; die Offenbarung muß vielmehr zur Aufgabenerfüllung notwendig sein.

Zwar ist es zur Erfüllung der Aufgabe des Jugendamts als Amtspfleger im Rahmen der Geltendmachung von Unterhaltsansprüchen des von ihm vertretenen Kindes gegen den Kindesvater erforderlich, Auskünfte über dessen Einkommen einzuholen. Hierzu war es jedoch nicht erforderlich, dem Arbeitgeber des Betroffenen durch unmittelbare Anfrage über den Arbeitsverdienst

die Tatsache zu offenbaren, daß der Betroffene Kontakte zum Jugendamt hat. Nach § 1615a in Verbindung mit § 1605 Abs. 1 Satz 1 BGB ist der Betroffene als Kindesvater verpflichtet, seinem nichtehelichen Kind auf Verlangen Auskunft über seine Einkünfte und sein Vermögen zu erteilen, soweit dies zur Feststellung eines Unterhaltsanspruchs oder einer Unterhaltspflicht erforderlich ist. Nach § 1605 Abs. 1 Satz 2 BGB sind über die Höhe der Einkünfte auf Verlangen Belege, insbesondere Bescheinigungen des Arbeitgebers vorzulegen. Danach war eine unmittelbare Anfrage bei dem Arbeitgeber und damit die Offenbarung der Tatsache, daß der Betroffene Kontakte zum Jugendamt hat, nicht zulässig. Diese Offenbarung verstieß somit gegen das Sozialgeheimnis.

Ich habe dem Oberstadtdirektor empfohlen, künftig in vergleichbaren Fällen Anfragen über den Arbeitsverdienst nur an den nach § 1605 Abs. 1 Satz 1 BGB Auskunftspflichtigen zu richten.

- Ein Bürger, dessen Kind aus erster Ehe Freiwillige Erziehungshilfe erhält, wehrte sich dagegen, daß er bei der Heranziehung zu den **Kosten der Heimunterbringung** auch um Angaben über die Einkommens- und Vermögensverhältnisse seiner zweiten Ehefrau gebeten wurde, obwohl diese gegenüber seinem Kind aus erster Ehe nicht unterhaltspflichtig sei.

Gesetzliche Grundlage für die Erhebung von Angaben über die wirtschaftlichen Verhältnisse des Betroffenen ist § 85 Abs. 1 Satz 2 und 3 JWG in Verbindung mit § 47 Abs. 1 Satz 2 des Gesetzes zur Ausführung des Gesetzes für Jugendwohlfahrt (AG-JWG) und § 116 Abs. 1 BSHG. Nach § 85 Abs. 1 Satz 2 JWG haben der Minderjährige und seine Eltern zu den Kosten der Freiwilligen Erziehungshilfe beizutragen, soweit es ihnen zuzumuten ist. Nach § 47 Abs. 1 Satz 2 AG-JWG gilt für den Kostenbeitrag § 116 BSHG entsprechend. Nach § 116 Abs. 1 BSHG sind die Kostenersatzpflichtigen verpflichtet, dem Leistungsträger Auskunft über ihre Einkommens- und Vermögensverhältnisse zu geben. Hierzu gehören Art und Höhe der Einkünfte, Aufwendungen, die mit der Erzielung des Einkommens verbunden sind, Vermögen, Miete oder Belastung bei Eigenheim, Unterhaltspflichten sowie außergewöhnliche wirtschaftliche Belastungen. Nicht dazu gehören die Einkommens- und Vermögensverhältnisse der zweiten Ehefrau des Betroffenen, da diese nicht die leibliche Mutter des Kindes und deshalb nicht kostenersatzpflichtig ist. Die Erhebung von Angaben über die Einkommens- und Vermögensverhältnisse der zweiten Ehefrau bei dem Betroffenen ist daher nur mit deren Einwilligung zulässig.

Soweit Angaben der Ehefrau des Betroffenen über ihre Einkommens- und Vermögensverhältnisse für die Ermittlung des der Kostenersatzpflicht zugrundezulegenden Einkommens des Betroffenen erheblich sind (§ 76 Abs. 1 und 2, § 79 Abs. 1 Nr. 2 BSHG) und diese Angaben unterbleiben, muß der Betroffene allerdings damit rechnen, daß gemeinschaftliche Kosten wie zum Beispiel Kosten der Unterkunft bei der Berechnung des maßgeblichen Einkommens nicht in voller Höhe berücksichtigt werden.

Ich habe daher dem Landschaftsverband empfohlen, in vergleichbaren Fällen Daten über nicht kostenersatzpflichtige Dritte nur mit deren schriftlicher Einwilligung beim Kostenersatzpflichtigen zu erheben und in dem Vordruck auf die Folgen der Nichtabgabe dieser Daten hinzuweisen. Entsprechendes gilt für die Erhebung von Angaben über volljährige Kinder und sonstige Personen im Haushalt des Kostenersatzpflichtigen.

- Ein Bürger beschwerte sich darüber, daß ein über ihn im Zusammenhang mit der Vormundschaftsregelung für sein Kind aus erster Ehe erstelltes psychologisches Gutachten entgegen der ausdrücklichen **Zweckbindung** innerhalb des Jugendamtes von der für seine Familienrechtssache zuständigen Stelle

an die für die Pflegschaftssache der Kinder seiner zweiten Ehefrau zuständige Stelle weitergegeben worden ist.

Die für das Kind des Betroffenen zuständige Stelle des Jugendamtes hat in der Familienrechtssache Aufgaben der Vormundschaftsgerichtshilfe nach § 27 Abs. 1 Nr. 5 SGB I in Verbindung mit § 48a JWG wahrgenommen. Damit unterliegen die ihr in dieser Eigenschaft bekanntgewordenen personenbezogenen Daten, wozu auch der Inhalt des über den Betroffenen erstellten psychologischen Gutachtens gehört, dem Sozialgeheimnis (§ 35 Abs. 1 SGB I).

Nach § 35 Abs. 1 Satz 1 SGB I hat jeder Anspruch darauf, daß seine personenbezogenen Daten von den Leistungsträgern als Sozialgeheimnis gewahrt und nicht unbefugt offenbart werden. Der Geheimhaltungsanspruch richtet sich zwar gegen den Leistungsträger, also gegen die jeweilige Körperschaft, Anstalt oder Behörde (§ 12 SGB I). Eine Offenbarung im Sinne dieser Vorschrift liegt jedoch auch dann vor, wenn personenbezogene Daten innerhalb des Leistungsträgers weitergegeben werden. Dieser hat dafür zu sorgen, daß solche Daten auch innerhalb des Leistungsträgers nur offenbart werden, wenn eine Offenbarungsbefugnis besteht.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung nur zulässig, soweit sie zur rechtmäßigen Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Zwar sieht der Wortlaut des § 69 Abs. 1 Nr. 1 SGB X – anders als die Übermittlungsvorschriften der Datenschutzgesetze (§ 10 Abs. 1 Satz 1 BDSG; § 11 Abs. 1 Satz 1 DSG NW) – nicht ausdrücklich vor, daß die Aufgabenerfüllung rechtmäßig sein muß. Die Rechtmäßigkeit ist jedoch eine derart selbstverständliche Voraussetzung jedes Verwaltungshandelns, daß auch ohne ausdrückliche Festlegung im Gesetz eine Offenbarung nur unter dieser Voraussetzung als zulässig angesehen werden kann.

Zur Erfüllung ihrer gesetzlichen Aufgaben in der Pflegschaftssache eines der Kinder der zweiten Ehefrau des Betroffenen hatte sich die hierfür zuständige Stelle über die Persönlichkeit des Betroffenen zu informieren. Hierzu war es erforderlich, die Unterlagen, die bei der für das Kind aus erster Ehe des Betroffenen zuständigen Stelle des Jugendamts über den Betroffenen vorhanden sind, der für die Kinder der zweiten Ehefrau zuständigen Stelle zur Verfügung zu stellen.

Der Offenbarung der Daten, die in dem über den Betroffenen erstellten psychologischen Gutachten festgehalten sind, stand jedoch dessen ausdrückliche Zweckbindung entgegen. Dieses Gutachten war in der Familienrechtssache erstellt worden und mit dem Vermerk versehen: „Das Gutachten dient ausschließlich den im Gerichtsbeschuß genannten Zwecken in der Familienrechtssache. Außerhalb dieser Zwecke kann das Gutachten nicht verwendet werden.“ Wegen dieser Zweckbindung war die Verwendung der in dem Gutachten enthaltenen Daten zur Aufgabenerfüllung der für die Kinder der zweiten Ehefrau zuständigen Stelle des Jugendamts nicht rechtmäßig und die Offenbarung an diese Stelle deshalb nicht zulässig.

Ich habe dem Oberstadtdirektor empfohlen, soweit die Verwendung von Unterlagen einer ausdrücklichen Zweckbindung unterliegt, diese zu beachten. Er wird dieser Empfehlung folgen.

- Durch eine Eingabe erfuhr ich von einem schwerwiegenden Verstoß gegen das Sozialgeheimnis. Die Betroffene war Opfer einer Straftat. In dem Ermittlungsverfahren übersandte der zuständige Oberstadtdirektor die über die Betroffene geführte Jugendamtsakte mit dem darin enthaltenen Erziehungsbericht auf Anforderung an die Sonderkommission der **Kripo und Staatsanwaltschaft** sowie an die Staatsanwaltschaft. In dem Verfahren vor dem

Schwurgericht erhielten auch die Verteidiger Kenntnis von dem Inhalt der Jugendamtsakte.

Zu den Sozialleistungen nach § 27 SGB I gehören auch die Leistungen der Jugendhilfe nach den §§ 4 bis 8 JWG. Somit unterliegen alle im Rahmen der Wahrnehmung dieser Aufgaben vom Jugendamt erhobenen und festgehaltenen oder ihm bekanntgewordenen personenbezogenen Daten dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 Satz 1 SGB I). Die in der Jugendamtsakte enthaltenen Angaben über die Betroffene dürfen, soweit nicht die Betroffene im Einzelfall eingewilligt hat (§ 67 Satz 1 SGB X), nur offenbart werden, wenn eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt. Soweit eine Offenbarung nicht zulässig ist, besteht nach § 35 Abs. 3 SGB I keine Auskunftspflicht und keine Pflicht zur Vorlegung oder Auslieferung von Schriftstücken und Akten.

Eine gesetzliche Offenbarungsbefugnis war nicht gegeben. Die Offenbarung konnte insbesondere nicht auf § 69 Abs. 1 Nr. 1 SGB X gestützt werden, wonach eine Offenbarung personenbezogener Daten zulässig ist, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Zwar gehört zu den Aufgaben des Jugendamtes die Mitwirkung in der Jugendhilfe bei den Polizeibehörden, insbesondere bei der Unterbringung zur vorbeugenden Verwahrung, gemäß näherer landesrechtlicher Bestimmung (§ 4 Nr. 7 JWG). Nach der hierzu in § 31 AG-JWG getroffenen Regelung umfaßt die Jugendhilfe bei den Polizeibehörden jedoch eindeutig nicht die Aufklärung von Straftaten zum Nachteil Minderjähriger. Auch für die Erfüllung anderer Aufgaben nach den §§ 4 bis 8 JWG war die Offenbarung der in der Jugendamtsakte enthaltenen personenbezogenen Daten an die Sonderkommission der Kripo und Staatsanwaltschaft sowie an die Staatsanwaltschaft nicht erforderlich. Sie war im Gegenteil geeignet, das Wohl des Kindes zu gefährden und damit die Erfüllung der Aufgaben des Jugendamts zu beeinträchtigen.

Eine Offenbarung für die Durchführung eines Strafverfahrens nach § 73 SGB X schied aus, da die hierfür erforderliche richterliche Anordnung nicht vorlag. Es muß dem Richter überlassen bleiben zu entscheiden, ob das Sozialgeheimnis zur Aufklärung eines Verbrechens durchbrochen und damit die nach § 147 Abs. 1 und 2 StPO spätestens nach Abschluß der Ermittlungen gebotene Akteneinsicht des Verteidigers mit den sich daraus ergebenden Folgen in Kauf genommen werden soll.

Da somit eine gesetzliche Offenbarungsbefugnis nicht vorlag, war die Offenbarung der in der Jugendamtsakte enthaltenen personenbezogenen Daten der Betroffenen an die Sonderkommission der Kripo und Staatsanwaltschaft sowie an die Staatsanwaltschaft nicht zulässig.

Ich habe die Weitergabe der über die Betroffene geführten Jugendamtsakte an die Sonderkommission der Kripo und Staatsanwaltschaft sowie an die Staatsanwaltschaft als Verstoß gegen das Sozialgeheimnis (§ 35 Abs. 1 und 3 SGB I) gemäß § 30 Abs. 1 Satz 1 DSGVO beanstandet.

Der Staatsanwaltschaft habe ich empfohlen, künftig in vergleichbaren Fällen von der Anforderung von Schriftstücken und Akten des Jugendamts abzusehen, soweit nicht eine richterliche Anordnung nach § 73 SGB X vorliegt. Ich habe sie darauf hingewiesen, daß nach § 78 SGB X Stellen, denen personenbezogene Daten von einem Leistungsträger offenbart worden sind, diese nur zu dem Zweck verwenden dürfen, zu dem sie ihnen **befugt** offenbart worden sind. Für die Offenbarung der in der Jugendamtsakte enthaltenen personenbezogenen Daten der Betroffenen durch die Stadt an die Sonderkommission sowie an die Staatsanwaltschaft war jedoch, wie dargelegt, eine Offenbarungsbefugnis nicht gegeben.

- Ein Bürger teilte mir mit, daß die Leitung eines kommunalen **Kindergartens** den Mitarbeitern einer Semi-Emaile-Firma Namen und Anschriften der den Kindergarten besuchenden Kinder bekanntgegeben habe. Die Firma habe daraufhin den Eltern Photographien ihrer Kinder in einer Miniaturplatten-Einfassung angeboten.

Die Sozialleistungen nach § 27 SGB I in Verbindung mit §§ 4 bis 8 JWG umfassen auch die Förderung und gegebenenfalls Schaffung von Einrichtungen für die Pflege und Erziehung von Kleinkindern (§ 5 Abs. 1 Satz 1 Nr. 3 JWG). Dementsprechend ist das Kindergartengesetz als „Zweites Gesetz zur Ausführung des Gesetzes für Jugendwohlfahrt“ erlassen worden. Somit unterliegen die personenbezogenen Daten der den kommunalen Kindergarten besuchenden Kinder dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 Satz 1 SGB I). Personenbezogene Daten dürfen daher, sofern der Betroffene nicht eingewilligt hat (§ 67 Satz 1 SGB X) nur offenbart werden, soweit eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt.

Eine gesetzliche Offenbarungsbefugnis war im vorliegenden Fall nicht gegeben. Die Offenbarung konnte insbesondere nicht auf § 69 Abs. 1 Nr. 1 SGB X gestützt werden, da sie zur Erfüllung der gesetzlichen Aufgaben des Kindergartens nicht erforderlich war. Sie war daher ohne Einwilligung der Eltern unzulässig und verstieß gegen das Sozialgeheimnis.

Der Stadtdirektor wird meiner Empfehlung, dafür Sorge zu tragen, daß in vergleichbaren Fällen Name und Anschrift der den Kindergarten besuchenden Kinder ohne Einwilligung der Eltern nicht an Dritte offenbart werden, folgen.

#### e) Wohngeld

- Ein Bürger wandte sich dagegen, daß die Wohngeldstelle in einem Vordruck von ihm die Erklärung verlangte, ob, seit wann und mit wem (Name, Vorname, Anschrift) seine Tochter, die Wohngeld beantragt hatte, verlobt ist und wann voraussichtlich die Eheschließung erfolgt.

Wenn die Wohngeldstelle von den Eltern einer Antragstellerin zur Feststellung einer nicht nur vorübergehenden **Abwesenheit von dem elterlichen Haushalt** eine Erklärung verlangt, ob, seit wann und mit wem ihre Tochter verlobt ist und wann voraussichtlich die Eheschließung erfolgt, greift sie damit in das Recht der Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch in ihr Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung ein.

Zwar ist für die Datenerhebung zur Feststellung der Leistungsanspruchsvoraussetzungen eine gesetzliche Grundlage vorhanden. Hierbei ist jedoch der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit zu beachten. Dieser gebietet, unter mehreren für die Erreichung des Zwecks geeigneten Mitteln dasjenige zu wählen, das den Betroffenen am wenigsten belastet; darüber hinaus muß die mit dem Eingriff verbundene Belastung des Betroffenen in einem angemessenen Verhältnis zu dem zu erreichenden Zweck stehen.

Die Datenerhebung über das Verlöbniß bei einem – im Verhältnis zum Verlobten der Antragstellerin – Dritten belastet den betroffenen Verlobten wie auch die Antragstellerin unverhältnismäßig; sie ist nach meiner Auffassung mit dem Anspruch des Verlobten auf Schutz seiner Menschenwürde (Artikel 1 Abs. 2 des Grundgesetzes) nicht vereinbar. Vertretbar wäre allenfalls ein Verlangen der Bestätigung des Verlöbnisses durch den Verlobten selbst.

Meiner Empfehlung, davon abzusehen, die Eltern eines Antragstellers zu

befragen, ob, seit wann und mit wem dieser verlobt ist und wann voraussichtlich die Eheschließung erfolgt, ist der Oberstadtdirektor gefolgt.

- Ein Bürger, der sowohl in Nordrhein-Westfalen als auch in den Niederlanden eine Wohnung unterhält, hat für beide Wohnungen bei der jeweils zuständigen Gemeinde Wohngeld bzw. einen Mietzuschuß beantragt und auch erhalten.

Die **niederländische Gemeinde** hat die hiesige Gemeinde fernmündlich um Auskunft gebeten, ob die von dem Betroffenen hier genutzte Wohnung eine Eigentumswohnung sei. Die hiesige Gemeinde teilte daraufhin mit, daß es sich bei der fraglichen Wohnung um eine Mietwohnung handele, für die der Betroffene Wohngeld erhalte. Sie gab darüber hinaus den Namen des Vermieters sowie die Höhe der Miete bekannt.

Diese personenbezogenen Daten unterliegen dem Schutz des Sozialgeheimnisses (§ 35 Abs. 1 Satz 1 SGB I). Sie dürfen, sofern nicht der Betroffene eingewilligt hat, nur offenbart werden, wenn eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt.

Nach der hier allein in Betracht kommenden Vorschrift des § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung personenbezogener Daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Eine gesetzliche Aufgabe nach dem Sozialgesetzbuch, zu deren Erfüllung die Offenbarung der genannten Daten des Betroffenen gegenüber der niederländischen Gemeinde erforderlich gewesen sein könnte, ist nicht erkennbar. Die Offenbarung dieser Daten verstieß daher gegen das Sozialgeheimnis.

Ich habe dem Oberstadtdirektor empfohlen, in vergleichbaren Fällen von der Offenbarung personenbezogener Daten abzusehen. Der Oberstadtdirektor folgt meiner Empfehlung.

- Ein Bürger hat sich bei mir darüber beschwert, daß die in seiner Wohngeldakte festgehaltenen personenbezogenen Daten, wie der Hinweis auf eine Nervenkrankung durch die Wohngeldstelle an die für den **öffentlich geförderten Wohnungsbau** zuständige Stelle des Amtes für Wohnungswesen und von dort an den Regierungspräsidenten offenbart worden sind.

Die bei dem Amt für Wohnungswesen (Wohngeldstelle) in der Wohngeldakte des Betroffenen festgehaltenen personenbezogenen Daten unterliegen dem Schutz des Sozialgeheimnisses. Der Geheimhaltungsanspruch nach § 35 Abs. 1 Satz 1 SGB I richtet sich zwar gegen den Leistungsträger, also gegen die jeweilige Körperschaft, Anstalt oder Behörde (§ 12 SGB I). Eine Offenbarung im Sinne dieser Vorschrift liegt jedoch auch dann vor, wenn personenbezogene Daten innerhalb eines Leistungsträgers weitergegeben werden. Dieser hat dafür zu sorgen, daß die ihm bekanntgewordenen Sozialdaten auch innerhalb des Leistungsträgers nicht unbefugt offenbart werden. Danach darf das Amt für Wohnungswesen auch in seinem eigenen Bereich die Angaben nur dem für die Bearbeitung des Vorgangs zuständigen Personenkreis zugänglich machen. Weiterhin verbietet die Pflicht zur Wahrung des Sozialgeheimnisses den mit der Bearbeitung von Wohngeldangelegenheiten betrauten Bediensteten, sofern sie zugleich mit der Bearbeitung von öffentlich geförderten Wohnungsbauangelegenheiten betraut sind, hierfür die Wohngelddaten zu verwenden.

Die in der Wohngeldakte festgehaltenen Daten dürfen durch das Amt für Wohnungswesen nur offenbart werden, wenn der Betroffene im Einzelfall eingewilligt hat (§ 67 Satz 1 Nr. 1 SGB X) oder eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt (§ 67 Satz 1 Nr. 2 SGB X). Nach § 69 Abs. 1 Nr. 1 SGB X ist eine Offenbarung von Wohngeld-

daten zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch durch eine in § 35 SGB I genannte Stelle erforderlich ist.

Eine derartige Aufgabe der Wohngeldstelle (die für den öffentlich geförderten Wohnungsbau zuständige Stelle ist nicht Sozialleistungsträger) ist hier nicht ersichtlich. Die Offenbarung von in der Wohngeldakte festgehaltenen personenbezogenen Daten durch die Wohngeldstelle an die für den öffentlich geförderten Wohnungsbau zuständige Stelle des Amtes für Wohnungswesen und erst recht von dort an den Regierungspräsidenten war somit unzulässig und verstieß gegen das Sozialgeheimnis.

Ich habe dem Oberstadtdirektor empfohlen, künftig in vergleichbaren Fällen die in der Wohngeldakte festgehaltenen personenbezogenen Daten nicht an die für den öffentlich geförderten Wohnungsbau zuständige Stelle des Amtes für Wohnungswesen oder an den Regierungspräsidenten weiterzugeben. Der Oberstadtdirektor hat mir mitgeteilt, daß er meiner Empfehlung folgen werde.

#### **f) Ausbildungsförderung**

In meinem sechsten Tätigkeitsbericht (C.8.g) habe ich darauf hingewiesen, daß die Verwendung der dem Deutschen Studentenwerk (DSW) zu Zwecken der Darlehensverwaltung verfügbaren Daten von Hochschulabsolventen, die während ihrer Studienzeit eine Förderung nach dem Honnefer Modell erhalten haben, für **Spendenappelle** zugunsten eines Härtefonds datenschutzrechtlich unzulässig ist.

Meiner Empfehlung, bei derartigen Vorhaben künftig nicht mehr auf die für Verwaltungszwecke verfügbaren Daten von Darlehensempfängern zurückzugreifen, ist das DSW nicht gefolgt. Es hat zwar die für Spendenaufrufe bisher verwendeten Schreiben überarbeitet. Die Neufassung der Spendenaufrufe stellt jedoch aus der Sicht des Datenschutzes keine Verbesserung gegenüber dem bisher versandten Schreiben dar; vielmehr wird darin der Appellcharakter und somit der Druck auf die Betroffenen noch verstärkt.

Da das DSW die ihm für Verwaltungszwecke verfügbaren Daten von Hochschulabsolventen, die Ausbildungsförderung nach dem Honnefer Modell erhalten haben, auch künftig gezielt verwenden will, habe ich dieses Verfahren als Verletzung des Rechts auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes gemäß § 30 Abs. 1 Satz 1 DSGVO beanstandet.

## 12. Gesundheitswesen

### **a) Krankenhäuser**

- Die Datenschutzbeauftragten des Bundes und der Länder haben in ihrer EntschlieÙung vom 27./28. März 1984 über die Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts auf die Notwendigkeit hingewiesen, auch im Bereich des Gesundheitswesens bereichsspezifische gesetzliche Regelungen zu erlassen. Daran anknüpfend haben die Datenschutzbeauftragten in einem Beschluß vom 14. März 1986 zum Datenschutz im Krankenhaus folgendes festgestellt:

Die ärztliche Schweigepflicht und die allgemeinen Datenschutzgesetze reichen nicht aus, alle Fälle in denen im Bereich des Krankenhauses das Persönlichkeitsrecht des Patienten berührt wird, angemessen zu lösen. Konkrete Regelungen für diesen Bereich sind insbesondere deshalb notwen-

dig, weil automatisierte Datenverarbeitung in immer stärkerem Maße im Krankenhausbereich auch für die Verarbeitung medizinischer Daten eingesetzt wird. Die zunehmende Komplexität der Verarbeitung und Nutzung von Patientendaten führt dazu, daß für den einzelnen Patienten der Umfang und die Zwecke der Verwendung seiner Daten undurchschaubar werden. Der Bürger muß aber auch künftig die Gewähr haben, daß das Vertrauensverhältnis zwischen Arzt und Patient (Arzt-/Patientengeheimnis) und sein Persönlichkeitsrecht gewahrt bleiben.

Bisher wird die Datenverarbeitung in Krankenhäusern vielfach auf Grund sehr weit gefaßter formularmäßiger Einwilligungen gerechtfertigt. Die Einwilligung kann jedoch in vielen Fällen keine ausreichende Grundlage für die Verarbeitung von Patientendaten sein, da für den Patienten die Informationsmöglichkeit und die Entscheidungsfreiheit häufig eingeschränkt sind.

Maßstab für den Umfang der Erhebung, Verarbeitung und Nutzung von Patientendaten muß stets die Behandlung des Patienten sein. Eine zusätzliche vom Behandlungszweck nicht gedeckte Datenerhebung, -verarbeitung und -nutzung bedarf einer besonderen Legitimation.

Auch die für die Behandlung verwendeten Vordrucke und Aufnahmeverträge müssen diesen Grundsätzen angepaßt werden. Die zuständigen Stellen werden aufgefordert, ihre Vordrucke und Aufnahmeverträge entsprechend zu überarbeiten.

Zur Wahrung des Patientengeheimnisses ist es geboten, im Krankenhaus den ärztlichen Bereich von der Verwaltung informationell abzuschotten. Daraus folgt, daß z. B. die Akten der Krankenhausverwaltung getrennt von denjenigen des ärztlichen Bereichs zu führen sind. Daraus folgt weiter, daß auch im ärztlichen Bereich nur vom jeweils behandelnden Arzt auf die Daten zugegriffen werden kann.

Läßt das Krankenhaus Patientendaten bei anderen Stellen im Auftrag verarbeiten, wird das Arztgeheimnis durchbrochen. Auch besteht die Gefahr einer Grundrechtsbeeinträchtigung durch Verknüpfung von medizinischen Daten und solchen aus anderen Bereichen und durch überregionale Konzentration medizinischer Daten. Die Verarbeitung medizinischer Daten außerhalb des eigenen Krankenhauses sollte daher – in eingeschränktem Umfang – allenfalls bei einem anderen Krankenhaus zugelassen werden.

Das Krankenhaus steht im Zentrum vielfältiger Informationsanforderungen, nicht zuletzt von Sozialleistungsträgern und anderen öffentlichen Stellen. Diese Informationsanforderungen sind häufig nicht normenklar festgelegt. Ihre Notwendigkeit muß überprüft, die gesetzlichen Grundlagen müssen präzisiert werden. Dies gilt insbesondere dann, wenn die Übermittlung zu belastenden Konsequenzen für den Patienten im Verwaltungsvollzug (z. B. Führerscheinenzug) führen kann.

Der Patient darf ohne sein Wissen und sein Einverständnis grundsätzlich nicht zum Objekt der Forschung mit Daten gemacht werden, die zu seiner Behandlung erhoben werden. Die Verarbeitung von Daten zu Forschungszwecken ohne Beteiligung des Patienten sollte nur zugelassen werden, wenn dies im Interesse der wissenschaftlichen Forschung unabdingbar ist und die Rahmenbedingungen der Verarbeitung durch den Gesetzgeber näher festgelegt sind. Dies gilt auch für gemeinsame Dokumentationssysteme mehrerer behandelnder Einrichtungen.

Das informationelle Selbstbestimmungsrecht umfaßt auch das Recht des Patienten, Einsicht in Patientenakten und ärztliche Unterlagen zu nehmen und Auskunft zu erhalten, sofern nicht überwiegende Geheimhaltungsinteressen anderer entgegenstehen.

Eine undifferenzierte, zeitlich unbefristete Aufbewahrung von Patientenunterlagen darf es auch im Krankenhaus nicht geben. Deshalb müssen die Krankenhäuser prüfen, wann welche Patientenunterlagen ohne Beeinträchtigung schutzwürdiger Belange der Patienten vernichtet werden können.

Ich habe den Minister für Arbeit, Gesundheit und Soziales gebeten, diesen Beschluß bei der bevorstehenden Novellierung des Krankenhausgesetzes des Landes Nordrhein-Westfalen zu berücksichtigen. Dabei gehe ich davon aus, daß der Entwurf für die Novellierung entsprechend den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts auch bereichsspezifische Regelungen der Datenverarbeitung und des Datenschutzes im Krankenhaus enthalten wird.

- Ein Bürger hat mir den von dem Institut für Blutspendewesen eines städtischen Krankenhauses verwendeten Vordruck zur **Befragung von Blutspendern** vorgelegt, in dem von dem Betroffenen folgende Angaben über Veränderungen seit der letzten Blutspende verlangt werden: Erkrankungen, Unfall, Operation, regelmäßige Einnahme von Medikamenten, Impfungen, Schwangerschaft, Akupunktur, Tätowierung, größere Gewichtsabnahme, Lymphknotenschwellung, gehäufte fieberhafte Infekte, Infektionskrankheiten in der Umgebung (insbesondere Gelbsucht), außereuropäischer Aufenthalt. Gleichzeitig wird der Betroffene um seine Einwilligung für die Speicherung der die Blutspende betreffenden Daten gebeten.

Nach Artikel 4 Abs. 2 der Landesverfassung wie auch im Hinblick auf das Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes bedarf jeder Umgang öffentlicher Stellen mit personenbezogenen Daten, also auch jedes Erheben und Speichern solcher Daten einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen.

Zwar ist eine ausdrückliche gesetzliche Grundlage für die Erhebung der Daten bei den Blutspendern nicht vorhanden. Das Institut für Blutspendewesen kann jedoch im Rahmen der Erfüllung der Aufgaben des Krankenhauses nach § 3 Abs. 1 Satz 1 des Krankenhausgesetzes des Landes Nordrhein-Westfalen die Zulassung zur Blutspende davon abhängig machen, daß der Betroffene bereit ist, diejenigen personenbezogenen Daten bekanntzugeben, die zur Prüfung seiner Eignung als Blutspender erforderlich sind. Gegen die Erhebung der in dem Vordruck verlangten Angaben über Veränderungen seit der letzten Blutspende bestehen somit keine durchgreifenden datenschutzrechtlichen Bedenken. Jedoch müssen die Betroffenen bei der Erhebung auf die Obliegenheit, die verlangten Angaben zu machen, hingewiesen werden.

Gesetzliche Grundlage für die Speicherung der Daten in einer Blutspender-Datei ist § 10 Abs. 1 DSG NW. Danach ist das Speichern personenbezogener Daten zulässig, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist.

Das Institut für Blutspendewesen hat im einzelnen dargelegt, daß die Speicherung der in dem Vordruck verlangten Angaben zur Prüfung der Eignung als Blutspender erforderlich ist. Die Blutspender-Datei werde ähnlich wie eine Krankenakte geführt. Sie diene der Optimierung des Spender- wie auch insbesondere des Empfängerschutzes. Dazu sei, solange sich der Betroffene als Spender zur Verfügung stelle, eine ständige Verlaufsbeobachtung und der Rückgriff auch auf länger zurückliegende Ereignisse notwendig, die sich auf die Eignung als Blutspender auswirken können.

Da demnach die Datenspeicherung nach den Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen als zulässig anzusehen ist, bedarf es hierzu keiner Einwilligung des Betroffenen. Aus rechtsstaatlichen Gründen des

Vertrauensschutzes sollte eine Einwilligung in die Speicherung der Daten auch nicht eingeholt werden, damit nicht bei dem Betroffenen der Eindruck erweckt wird, die Einwilligung sei erforderlich und ohne sie würde die Speicherung unterbleiben.

Die in der Blutspender-Datei gespeicherten Daten werden nach Auskunft des Instituts – ähnlich wie Krankenunterlagen – 10 Jahre nach der letzten Spende gelöscht. Die Datei sei jetzt und künftig ausschließlich den Mitarbeitern des Instituts zugänglich.

Meinen Empfehlungen,

- die Betroffenen bei der Erhebung der in dem Vordruck verlangten Angaben auf die Obliegenheit, diese Angaben zu machen, hinzuweisen;
- die vorgedruckte Erklärung des Einverständnisses mit der Datenspeicherung zu streichen und stattdessen die Betroffenen darüber aufzuklären, daß und zu welchem Zweck ihre Daten gespeichert werden, wer Zugang zu ihnen hat und wann die Daten gelöscht werden;

wird das Institut für Blutspendewesen folgen.

- Ein Strafgefangener beschwerte sich darüber, daß die **Justizvollzugsanstalt (JVA)** bei der Überweisung von Strafgefangenen an externe Krankenhäuser und Ärzte die in der JVA geführte Gesundheitsakte, der aus einem ihr vorgehefteten Bogen die Art der Straftat und die Dauer der Strafzeit zu entnehmen ist, weitergegeben wird. Außerdem habe eine Universitätsklinik ihren Befundbericht über eine von dem Anstaltsarzt veranlaßte Untersuchung an diesen übersandt, obwohl der Betroffene die Klinikärzte ausdrücklich nicht von der Schweigepflicht entbunden habe.

Da die in der Gesundheitsakte des Betroffenen bei der JVA wie auch die in dem Befundbericht der Universitätsklinik festgehaltenen Daten nicht in einer Datei gespeichert werden, sind die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen hier nicht anwendbar. Jedoch gilt für in Akten und sonstigen Unterlagen festgehaltene personenbezogene Daten das Grundrecht des Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung wie auch das vom Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 aus Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes hergeleitete Recht auf informationelle Selbstbestimmung.

Als gesetzliche Grundlage für die Weitergabe von Krankenunterlagen bei Überweisungen an externe Ärzte oder Krankenhäuser wie auch für die Weitergabe des von der Universitätsklinik auf Veranlassung des Anstaltsarztes erstellten Befundberichts an diesen kommen § 56 Abs. 1 Satz 1, § 58 sowie § 65 Abs. 2 Satz 1 des Strafvollzugsgesetzes (StVollzG) in Betracht. Nach § 56 Abs. 1 Satz 1 StVollzG ist für die körperliche und geistige Gesundheit des Gefangenen zu sorgen. Nach § 58 StVollzG erhält der Gefangene Krankenpflege von Beginn der Krankheit an; hierzu wird in Nr. 2 Abs. 2 der Verwaltungsvorschriften zu § 58 StVollzG bestimmt, daß der Anstaltsarzt einen anderen Arzt oder Facharzt hinzuzieht, wenn er es nach Art und Schwere des Falles für erforderlich hält. Nach § 65 Abs. 2 Satz 1 StVollzG ist ein Gefangener in ein Krankenhaus außerhalb des Vollzuges zu bringen, wenn die Krankheit in einer Vollzugsanstalt oder einem Anstaltskrankenhaus nicht erkannt oder behandelt werden kann. Zur Erfüllung dieser Aufgaben ist es nach meiner Auffassung erforderlich, daß der Anstaltsarzt an Hand der bei ihm geführten Krankenunterlagen den externen (Krankenhaus-)Arzt über die Krankheit des Betroffenen unterrichtet. Dementsprechend sieht Nr. 51 Abs. 4 der Dienstordnung für das Gesundheitswesen in den Justizvollzugsanstalten vor, daß der Anstaltsarzt die erforderlichen ärztlichen Unterlagen dem behan-

deinden Arzt der Krankenanstalt außerhalb des Vollzuges verschlossen zuleitet.

Dabei ist jedoch der verfassungsmäßige Verhältnismäßigkeitsgrundsatz zu beachten. Dieser gebietet, dem externen Arzt nur die für die Untersuchung oder Behandlung notwendigen Krankenunterlagen zugänglich zu machen wie etwa ein Überweisungsschreiben mit den erforderlichen ärztlichen Informationen und gegebenenfalls Röntgenaufnahmen sowie Aufzeichnungen über bestimmte Untersuchungen. Dagegen war es nicht erforderlich, die ausschließlich für den dienstinternen anstaltsärztlichen Gebrauch bestimmte Gesundheitsakte, die auch Angaben über die Art der Straftat und die Strafdauer enthält, an externe Ärzte weiterzugeben. Somit war die Übersendung der vollständigen Gesundheitsakte des Betroffenen an die externen (Krankenhaus-)Ärzte durch die genannten Vorschriften nicht gedeckt und daher unzulässig.

Wie mir der Justizminister mitgeteilt hat, hat er den Präsidenten des zuständigen Justizvollzugsamtes gebeten, eine der Nr. 51 Abs. 4 der Dienstordnung für das Gesundheitswesen in den Justizvollzugsanstalten entsprechende Sachbehandlung durch den Leiter der JVA sicherzustellen.

Demgegenüber war es zur Erfüllung der dem Anstaltsarzt nach den genannten Vorschriften obliegenden Aufgaben nach meiner Auffassung erforderlich, daß dem Anstaltsarzt der Befundbericht der Universitätsklinik über die von ihm veranlaßte Untersuchung zugänglich gemacht wurde. Zu den Aufgaben des Anstaltsarztes gehört die Weiterbehandlung des Betroffenen nach Hinzuziehung der Universitätsklinik als Fachklinik. Zur Erfüllung dieser Aufgabe war er auf die Kenntnis des Befundberichts angewiesen.

Die in den Gesundheitsakten der JVA wie auch die in dem Befundbericht der Universitätsklinik festgehaltenen Daten unterliegen außerdem der ärztlichen Schweigepflicht (§ 203 Abs. 1 Nr. 1 StGB, § 2 Abs. 1 Satz 1 der Berufsordnung).

Wenn mehrere Ärzte gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, so sind sie nach § 2 Abs. 6 der Berufsordnung untereinander von der Schweigepflicht insoweit befreit, als der Patient nicht etwas anderes bestimmt. Nach § 3 Abs. 3 der Berufsordnung hat der Arzt, wenn er den Patienten an einen anderen Arzt überweist, ihm die erhobenen Befunde zu übermitteln und ihn über die bisherige Behandlung zu informieren, es sei denn, daß der Patient etwas anderes bestimmt. Nach dieser Vorschrift sind die für die Untersuchung oder Behandlung notwendigen Krankenunterlagen weiterzugeben. Hierzu gehört aber, wie oben dargelegt, keinesfalls die Weitergabe der vollständigen Gesundheitsakte.

Allerdings hat der Patient nach § 2 Abs. 6 und § 3 Abs. 3 Satz 1 letzter Halbsatz der Berufsordnung die Möglichkeit, die Weitergabe der notwendigen Krankenunterlagen dadurch zu verhindern, daß er etwas anderes bestimmt. Aus diesen Vorschriften ergibt sich jedoch nicht, daß der Patient auf diese Möglichkeit hingewiesen werden muß. Ginge man davon aus, daß es eines vorherigen Hinweises gegenüber dem Patienten bedarf, so käme dies der Einholung der Einwilligung und damit der Befreiung von der ärztlichen Schweigepflicht gleich. Dann hätte es aber der Regelung in § 3 Abs. 3 Satz 1 letzter Halbsatz der Berufsordnung nicht bedurft; die Weitergabe wäre in diesem Fall bereits nach § 2 Abs. 4 der Berufsordnung zulässig.

Die Weitergabe des Befundberichts der Universitätsklinik an den Anstaltsarzt verstieß nicht gegen die ärztliche Schweigepflicht. Zwar ist nach § 2 Abs. 5 der Berufsordnung der Klinikarzt auch dann zur Verschwiegenheit verpflichtet, wenn er wie hier im amtlichen Auftrag eines Dritten tätig wird. Dies gilt jedoch nicht, wenn dem Betroffenen vor der Untersuchung bekannt ist oder

eröffnet wurde, inwieweit die von dem Arzt getroffenen Feststellungen zur Mitteilung an Dritte bestimmt sind.

Nach den Umständen war davon auszugehen, daß dem Betroffenen vor der vom Anstaatsarzt veranlaßten Untersuchung deren Zweck bekannt war. Einer Entbindung des Klinikarztes von der Schweigepflicht bedurfte es daher nicht.

## b) Medizinische Forschung

- Durch einen Hinweis des Landesbeauftragten für den Datenschutz Baden-Württemberg wurde mir der „**Perinatologische Basis-Erhebungsbogen**“ bekannt, mit dem zahlreiche Einzelangaben über den sozialen Status sowie den Gesundheitszustand von Schwangeren, Drogen- oder Alkoholabhängigkeit, Zahl der Schwangerschaftsabbrüche, den Geburtsverlauf und den Gesundheitszustand des Neugeborenen erhoben werden. Auf Anfrage bestätigte mir der Minister für Arbeit, Gesundheit und Soziales, daß eine solche Erhebung auch in Nordrhein-Westfalen von einer Ärztekammer in Zusammenarbeit mit der Kassenärztlichen Vereinigung vorbereitet wird. Die mit diesen Erhebungen angestrebte Qualitätskontrolle auf Grundlage anonymisiert – von den Krankenhäusern – weitergegebener Daten solle dazu beitragen, Ansätze zur Senkung der Mütter- und Säuglingssterblichkeit zu finden.

Die Daten des aus drei Blättern bestehenden „Perinatologischen Basis-Erhebungsbogens“ werden in der geburtshilflichen Klinik im Rahmen der Patientenaufnahme und Behandlung erhoben und auf dem Beleg eingetragen. Das mit Namen und Anschrift der Patientin versehene Deckblatt verbleibt in der Klinik. Blatt 2 (Erfassungsbogen) wird dem Organisationsbüro und der Datenverarbeitungsstelle der Perinatologischen Arbeitsgemeinschaft zur Auswertung übersandt. Auf diesem Blatt fehlen die Angaben über Namen, Geburtsjahr, Wohnort und Krankenkasse der Entbundenen.

Die Erfassungsbogen enthalten zur Identifizierung der einsendenden Klinik eine dreistellige Kliniknummer sowie zur Reidentifizierung bei Ausfüllfehlern und zur Vollständigkeitskontrolle die Geburtsnummer. Diese Angaben werden auf dem Statistikband nach Erstellung der Gesamtstatistik im Rechenzentrum der Kassenärztlichen Vereinigung gelöscht. Eine Identifizierung ist dann nicht mehr möglich. Die Erfassungsbogen werden nach vollständiger Erfassung einer Klinik vernichtet.

Blatt 3 des Durchschreibesatzes wird nur benötigt, wenn das neugeborene Kind nach der Geburt in eine pädiatrische Klinik verlegt werden muß. Nur in diesen Fällen erhält die Kinderklinik den letzten Bogen, andernfalls wird er vernichtet.

Da auch der zur Übermittlung an die Perinatologische Arbeitsgemeinschaft bestimmte Erfassungsbogen weitere Daten enthält, aus denen die Betroffene bestimmbar bleibt, liegt hier keine vollständige Anonymisierung vor. Die Erhebung, Erfassung, Weitergabe und Auswertung ist bei diesem Verfahren daher nur mit Einwilligung der Betroffenen zulässig. Die Einholung der Einwilligung wirft nach Meinung der Forscher jedoch erhebliche Probleme auf (unzureichende Response-Quote und damit Beeinträchtigung der wissenschaftlichen Aussagen, Inhalt und Umfang der Einwilligung, besondere Notsituation), so daß ein anderes Verfahren gefunden werden mußte, das sowohl dem wissenschaftlichen Interesse als auch den schutzwürdigen Belangen der Betroffenen gerecht wird.

In einem Beschluß vom 10. Mai 1985 zum Datenschutz bei der Perinataldokumentation haben die Datenschutzbeauftragten des Bundes und der Länder folgendes Verfahren für notwendig gehalten:

1. Die Verarbeitung von Patientendaten für die Perinatalstudie erfolgt bei der Kassenärztlichen Vereinigung/Ärztchammer (je nach Land unterschiedlich) im Auftrag der beteiligten Klinik.

Sie geschieht nach Weisung der auftraggebenden Klinik. Die Daten dürfen nur im Rahmen der Zweckbestimmung der Perinatalstudie verwendet und verarbeitet werden. Eine Verknüpfung mit anderen Datenbeständen der auftragnehmenden Kassenärztlichen Vereinigung/Ärztchammer ist (vertraglich) auszuschließen. Die Auftragnehmerin hat in einem Datensicherungskonzept darzulegen, auf welche Weise die perinatologischen Daten von den übrigen Datenbeständen in technischer und organisatorischer Hinsicht getrennt gespeichert und verarbeitet werden.

2. Grundsätzlich dürfen an andere als die jeweils auftraggebende Klinik nur aggregierte Daten bzw. anonymisierte Mikrodatensätze weitergegeben werden. Die Regelauswertung ist die klinikspezifische Statistik und die Übersichtsstatistik ohne personenbezogene Einzelangaben von Patienten bzw. Kindern.
3. Im Hinblick auf die Gestaltung bzw. Ausfüllung des Erhebungsbogens wird empfohlen:
  - 3.1 Die Geburtsnummer nach Abschluß der maschinellen Plausibilitätsprüfung zu löschen,
  - 3.2 nur die beiden ersten Stellen der Postleitzahl zu erheben,
  - 3.3 für die Nationalität und für die Schulbildung Zusammenfassungen in größeren Gruppen vorzunehmen,
  - 3.4 auf die spezifizierte Benennung des Berufs des Ernährers zu verzichten und statt dessen eine Gruppenklassifikation vorzunehmen,
  - 3.5 die Entbindungseinrichtungen/Kliniken darauf hinzuweisen, daß Freitextangaben in den letzten Zeilen des Vordrucks nicht an die auftragnehmenden Stellen Kassenärztliche Vereinigung/Ärztchammer übermittelt werden dürfen.
4. Es bestehen grundsätzlich keine Bedenken gegen eine Weiterverwendung der bereits gedruckten Formulare, wenn die Ausfüllanleitung entsprechend Ziffer 3 verändert wird. Die Konferenz der Datenschutzbeauftragten behält sich vor, die Empfehlung nach konkreten Prüfungserfahrungen entsprechend zu modifizieren.

Die Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder hat sich am 8./9. Oktober 1985 mit diesem Beschluß befaßt und ihn als vertretbaren Kompromiß zwischen den Erfordernissen des Persönlichkeitsschutzes der Betroffenen und den Anforderungen einer fundierten wissenschaftlichen Untersuchung begrüßt. Allerdings bestehen noch Unstimmigkeiten hinsichtlich der Erhebung einzelner Daten. Darüber werden gegebenenfalls noch weitere Erörterungen stattfinden müssen.

- Durch eine Eingabe wurde mir das **Register der European Dialysis and Transplant Association (EDTA)** bekannt.

Hierbei handelt es sich um ein grenzüberschreitendes Register, das am St. Thomas-Hospital in London europaweit geführt wird. Jeder Patient, der an chronischer Niereninsuffizienz erkrankt und in einem Dialysezentrum behandelt wird, wird – bisher ohne seine Einwilligung – an das EDTA-Register gemeldet. Von dort erhält die Dialyseklinik einen Behandlungsbogen mit den Angaben des Patienten zurück. Jeder meldenden Einrichtung werden außerdem statistische Auswertungen zu ihren Behandlungsfällen zur Verfügung gestellt. Ferner erstellt das Register Gesamtauswertungen des Datenmate-

rials, die supranationale Vergleiche über Therapieerfolge, Inzidenz und Prävalenz der dort dokumentierten Erkrankungen erlauben. Das Register dient somit epidemiologischen und statistischen Zwecken. Für die Behandlung des einzelnen Patienten hat es allenfalls eine mittelbare Bedeutung.

Für die Übermittlung detaillierter Angaben über Diagnose, Krankheitsursache, Behandlungsmethode und Behandlungsverlauf der namentlich genannten Patienten ist weder eine gesetzliche Grundlage vorhanden, noch besteht eine Offenbarungsbefugnis, die eine Durchbrechung des Arztgeheimnisses rechtfertigt. Eine Offenbarung zum Zwecke der wissenschaftlichen Forschung ist nach § 2 Abs. 7 der ärztlichen Berufsordnung nur in anonymisierter Form oder mit Einwilligung des Patienten zulässig.

Die Übersendung der Fragebogen mit detaillierten Angaben über namentlich genannte Dialyse-Patienten ohne deren Einwilligung durch öffentliche Stellen an die EDTA verstößt gegen das informationelle Selbstbestimmungsrecht nach Artikel 2 Abs. 1 und Artikel 1 Abs. 1 des Grundgesetzes wie auch gegen das Grundrecht der Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung. Außerdem verbietet das Arztgeheimnis die Weitergabe der in den Fragebogen festgehaltenen Daten, da eine Offenbarungsbefugnis hier nicht vorliegt.

Da in Kürze eine erneute Meldung an die EDTA in London vorgesehen ist, hielt ich es für geboten, daß der Minister für Arbeit, Gesundheit und Soziales und der Minister für Wissenschaft und Forschung bei den ihrer Aufsicht unterliegenden Krankenhäusern sicherstellen, daß ohne ausdrückliche schriftliche Einwilligung des Patienten keine personenbezogenen Daten an das Register weitergegeben werden.

Der Minister für Arbeit, Gesundheit und Soziales hat mir inzwischen eine von der Arbeitsgemeinschaft für klinische Nephrologie e. V. entworfene Patienten-Einwilligungserklärung übersandt, die bereits für die nächste Meldung verwendet werden soll. Gegen diese Erklärung bestehen insofern Bedenken, als sie keinen ausdrücklichen Hinweis auf die Freiwilligkeit enthält. Die Einholung einer Einwilligung in die Weitergabe derartiger sensibler Daten an ein ausländisches Register erfordert nach meiner Auffassung einen unübersehbaren Hinweis auf die Freiwilligkeit. Außerdem sollte der Betroffene ausdrücklich darauf hingewiesen werden, daß ihm aus der Verweigerung seiner Einwilligung keine Rechtsnachteile entstehen.

- Eine Universitätsklinik erhob im Hinblick darauf, daß eine Meldepflicht für AIDS-Erkrankungen nicht besteht, Bedenken gegen den Vordruck „**AIDS-Fallbericht**“, mit dem das Bundesgesundheitsamt bei den behandelnden Ärzten zahlreiche detaillierte Angaben ihrer an AIDS erkrankten Patienten erhebt.

Ich habe hierzu die Auffassung vertreten, daß, solange eine Meldepflicht für AIDS-Erkrankungen nicht besteht, derartige Fallberichte nur mit Einwilligung des Patienten erstattet werden dürfen. Da in dem Vordruck auf diese Voraussetzung nicht hingewiesen wird, läßt sich nicht ausschließen, daß Ärzte im Hinblick auf den amtlichen Charakter des Vordrucks in Unkenntnis der Rechtslage die von ihnen verlangten Daten ihrer Patienten ohne deren Einwilligung an das Bundesgesundheitsamt weitergeben.

Der Bundesbeauftragte für den Datenschutz, den ich über meine Rechtsauffassung unterrichtet hatte, teilte mir hierzu mit, daß nach einem im November/Dezember 1983 mit dem Bundesgesundheitsamt geführten Schriftwechsel der AIDS-Fallberichtsbogen um den Hinweis ergänzt worden sei, daß der Name des Patienten nur angegeben werden dürfe, wenn hierfür das Einverständnis des Patienten vorliege. Dieser neue Fragebogen sei seither bei Anforderungen von Ärzten und Krankenhäusern verwendet worden. Der mir

von der Universitätsklinik übersandte Fragebogen sei vermutlich vom Bundesgesundheitsamt vor diesem Zeitpunkt zur Verfügung gestellt und offensichtlich von der betreffenden Klinik selbst vervielfältigt worden. Eine Möglichkeit der Einflußnahme durch das Bundesgesundheitsamt darauf, daß ausschließlich der neue Fallberichtsbogen zur Meldung benutzt werde, sehe er nicht. Letztlich liege es auch in der Verantwortung des meldenden Arztes, daß die Meldungen an das Bundesgesundheitsamt unter Wahrung der ärztlichen Schweigepflicht erfolgen.

### c) Gesundheitsämter

- Zu der in der Öffentlichkeit erörterten Frage einer **Meldepflicht** für die Erkrankung an **AIDS** habe ich darauf hingewiesen, daß eine solche Meldepflicht, mit der personenbezogene Daten des Betroffenen erhoben werden, in sein Recht auf informationelle Selbstbestimmung und sein Grundrecht auf Datenschutz eingreift und daher einer normenklaren und dem Verhältnismäßigkeitsgrundsatz entsprechenden gesetzlichen Grundlage bedarf.

Das Bundes-Seuchengesetz sieht eine Meldepflicht des behandelnden Arztes gegenüber dem zuständigen Gesundheitsamt für eine Vielzahl übertragbarer Krankheiten vor. AIDS gehört nicht zu dem Katalog dieser Krankheiten. Allerdings kann der Bundesminister für Jugend, Familie und Gesundheit durch Rechtsverordnung die Meldepflicht auf andere übertragbare Krankheiten ausdehnen, soweit die epidemische Lage dies erfordert (§ 7 Abs. 1). Solange der Minister von dieser Ermächtigung keinen Gebrauch macht, können auch die Landesregierungen eine entsprechende Rechtsverordnung erlassen (§ 7 Abs. 3).

Diese gesetzlichen Grundlagen sind nach meiner Auffassung hinreichend normenklar; sie lassen für den Betroffenen klar erkennen, daß nach Erlaß einer entsprechenden Rechtsverordnung die Tatsache seiner Erkrankung von dem behandelnden Arzt dem Gesundheitsamt gemeldet wird. Zweifelhafte erscheint jedoch, ob ein solcher Eingriff als verhältnismäßig angesehen werden kann. Nach Presseberichten haben die Professoren Koch und Steinbach gegenüber Mitgliedern des Gesundheitsausschusses des Bundestages Zweifel an der Eignung und der Erforderlichkeit einer solchen Maßnahme für die Bekämpfung der Krankheit geäußert. So sei es wegen der langen Inkubationszeit nicht möglich, auf dem Weg über Kontaktpersonen den Herd zu ermitteln. Auch könne eine Meldepflicht daran nichts ändern, daß es noch keine Mittel gebe, die Krankheit zu behandeln. Zudem könnte nach Ansicht dieser Experten eine Meldepflicht viele Gefährdete aus Angst vor Diskriminierung von einem Bluttest abhalten.

Wenn dies zutrifft, wäre eine Meldepflicht für die Bekämpfung der Krankheit nicht nur nicht geeignet, geschweige denn erforderlich, sondern hierfür sogar schädlich. Unter diesen Umständen könnte auch der Wunsch nach genauen statistischen Angaben über den Umfang der Erkrankungen eine Meldepflicht nicht rechtfertigen, zumal die Angaben wenig zuverlässig wären, wenn die Meldepflicht Gefährdete in größerem Umfange von Bluttests abhalten würde.

Nach dem derzeitigen Erkenntnisstand kann daher von einer personenbezogenen Meldepflicht nur abgeraten werden.

- Mehrere Bürger erhoben Bedenken gegen das von jugendzahnärztlichen Diensten praktizierte Verfahren, das Ergebnis der **schulzahnärztlichen Untersuchung** in einem offenen Vordruck über den Klassenlehrer den Eltern bekanntzugeben. Zudem wandten sie sich dagegen, daß die Untersuchung in Anwesenheit des Lehrers durchgeführt wurde.

Eine nach Artikel 4 Abs. 2 der Landesverfassung erforderliche gesetzliche Grundlage für die Unterrichtung des Klassenlehrers über das Ergebnis der

schulzahnärztlichen Untersuchung ist nicht vorhanden. Eine solche Unterrichtung ist im übrigen auch nicht erforderlich. Das Verfahren, das Untersuchungsergebnis offen über den Klassenlehrer an die Eltern bekanntzugeben, verstößt somit gegen das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung wie auch gegen das Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes.

Darüber hinaus verbietet auch die ärztliche Schweigepflicht, das Ergebnis der schulzahnärztlichen Untersuchung in einem offenen Vordruck über den Klassenlehrer an die Eltern bekanntzugeben. Eine Befugnis zur Offenbarung liegt nur dann vor, wenn der Arzt von der Schweigepflicht entbunden worden ist oder wenn der Schutz eines höherrangigen Rechtsguts dies erfordert. Diese Voraussetzungen sind hier nicht gegeben.

Ebenso verstößt die Durchführung der schulzahnärztlichen Untersuchung in Anwesenheit des Lehrers gegen Vorschriften über den Datenschutz. Eine nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch nach Artikel 4 Abs. 2 der Landesverfassung erforderliche gesetzliche Grundlage für die Durchführung der Untersuchung in Anwesenheit des Lehrers ist nicht vorhanden. Auch dieses Verfahren verstößt außerdem gegen das Arztgeheimnis.

Ich habe daher den zuständigen Stellen empfohlen, künftig ein Verfahren vorzusehen, daß die Offenbarung des Ergebnisses der schulzahnärztlichen Untersuchung gegenüber dem Klassenlehrer oder der Schule ausschließt, wie zum Beispiel unmittelbare Übersendung des Schreibens an die Wohnanschrift der Eltern, sowie dafür zu sorgen, daß die Lehrer nicht mehr bei der schulzahnärztlichen Untersuchung zugegen sind.

- Ein Oberstadtdirektor unterrichtete mich unter Hinweis auf § 12 DSGVO darüber, daß er dem Provinzialinstitut für Westfälische Landes- und Volksforschung, das als Einrichtung des Landschaftsverbandes Westfalen-Lippe unabhängige wissenschaftliche Forschung betreibt, für das Forschungsprojekt „Der Provinzialverband Westfalen in der Zeit des Nationalsozialismus – Psychiatrie im Dritten Reich“ die beim Gesundheitsamt vorhandenen **Erbgesundheitsakten** zur wissenschaftlichen Auswertung zur Verfügung gestellt hatte.

Die Vorschrift des § 12 DSGVO kann hier keine Anwendung finden, da die Daten nicht aus einer Datei übermittelt wurden. Alle in den Erbgesundheitsakten festgehaltenen personenbezogenen Daten unterliegen dem Grundrecht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch dem Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung.

Eine hiernach erforderliche gesetzliche Grundlage für die Weitergabe der in den Erbgesundheitsakten festgehaltenen Daten an das Provinzialinstitut ist derzeit nicht vorhanden. Eine bereichsspezifische Übermittlungsbefugnis (etwa in einem Archivgesetz) fehlt bisher. Somit ist die Weitergabe der Daten hier nur mit Einwilligung der Betroffenen, bei Verstorbenen mit Einwilligung der nächsten Angehörigen zulässig. Dabei ist nicht zu verkennen, daß die Einholung der Einwilligung in der Praxis auf erhebliche Schwierigkeiten stoßen wird. Diese Schwierigkeiten dürfen jedoch nicht durch einen unzulässigen Eingriff in die genannten Grundrechte der Betroffenen umgangen werden.

Darüber hinaus unterliegen die in den Erbgesundheitsakten festgehaltenen Daten – zumindest soweit es sich um ärztliche Unterlagen und Gutachten handelt – der ärztlichen Schweigepflicht nach § 203 Abs. 1 Nr. 1 StGB. Zum Zwecke der wissenschaftlichen Forschung dürfen der Schweigepflicht unter-

liegende Tatsachen und Befunde nur soweit mitgeteilt werden, als dabei die Anonymität des Patienten gesichert ist oder dieser ausdrücklich zustimmt (§ 2 Abs. 7 der Berufsordnung), den Arzt also von seiner Schweigepflicht entbindet. Die Übersendung der – nichtanonymisierten – Erbgesundheitsakten an das Provinzialinstitut erfordert somit die ausdrückliche Zustimmung des Betroffenen, also die Entbindung von der ärztlichen Schweigepflicht. Diese Einwilligung muß hier zwar nicht schriftlich erteilt werden; es muß aber eine Erklärung des Betroffenen vorliegen. Eine „mutmaßliche“ Einwilligung reicht nicht aus.

Der ärztlichen Schweigepflicht unterliegen auch die Daten verstorbener Betroffener (§ 203 Abs. 4 StGB). Eine Entbindung von der Schweigepflicht durch noch lebende Angehörige ist nicht möglich, da es sich insoweit um ein höchstpersönliches Recht des Betroffenen handelt, das nicht auf die Erben übergehen kann. Es besteht daher nach dem Tode des Betroffenen für den Arzt keine Möglichkeit einer Entbindung von der Schweigepflicht mehr, da es an einem Berechtigten dazu fehlt.

Allerdings besteht die Schweigepflicht nach dem Tode nicht mehr im gleichen Umfang wie vorher. Die Rücksichtnahme auf die Persönlichkeitsinteressen des Betroffenen verliert dann an Bedeutung. Daher kann ein Arzt ohne Verletzung der Schweigepflicht ihr unterliegende Tatsachen offenbaren, wenn eine Güterabwägung ergibt, daß das Interesse an einer wissenschaftlichen Auswertung der der Schweigepflicht unterliegenden Daten das Geheimhaltungsinteresse des Verstorbenen überwiegt (vgl. C.11.c meines vierten Tätigkeitsberichts).

Ob eine derartige Güterabwägung hier zu einer Offenbarungsbefugnis gegenüber dem Provinzialinstitut führen könnte, erscheint fraglich. Hingegen können die Weitergabe von Akten oder Aktenteilen in Kopie, wenn darin Namen und Anschriften der Betroffenen geschwärzt sind,

#### d) Berufskammern

- Wiederum wandten sich Ärzte gegen die **Beitragsordnung** der Ärztekammer Nordrhein, insbesondere gegen die Staffelung der Beiträge sowie dagegen, daß die Ärztekammer bei Vorlage des Einkommensteuerbescheides auch Einkünfte einsehen kann, die nicht die ärztliche Tätigkeit betreffen. Außerdem verletze das Verlangen nach Vorlage des Einkommensteuerbescheides das Steuergeheimnis.

Wie in meinem sechsten Tätigkeitsbericht (C.9.f) dargelegt, muß im Hinblick auf die Aufgaben der Kammer und unter Berücksichtigung der unterschiedlichen Leistungsfähigkeit der Ärzte davon ausgegangen werden, daß eine gestaffelte Beitragspflicht sowie die Überwachung ihrer Erfüllung durch die Kammer im überwiegenden Interesse der Allgemeinheit liegt. Da für die hierzu erforderliche Datenerhebung auch eine gesetzliche Grundlage vorhanden ist, ist sie grundsätzlich zulässig.

Bei derartigen Eingriffen ist der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Die Datenerhebung muß sich auf das zum Erreichen des Zwecks erforderliche Minimum beschränken. Daraus folgt, daß bei der Vorlage des Einkommensteuerbescheides alle Angaben, die nicht Einkünfte aus ärztlicher Tätigkeit betreffen, unkenntlich gemacht werden dürfen. Nach § 4 Abs. 2 der Beitragsordnung kann der Kammerangehörige seine Einkünfte aber auch auf andere geeignete Weise nachweisen. Die Ärztekammer ist bereit, anstelle der Vorlage von Einkommensteuerbescheiden eine Bestätigung des Steuerberaters über die Höhe der Einkünfte aus ärztlicher Tätigkeit zu akzeptieren.

Die Beitragsordnung verletzt auch nicht das Steuergeheimnis nach § 30 der Abgabenordnung. Dieses gilt nur für die Offenbarung von Daten durch Amtsträger, nicht aber für die Erhebung von Daten eines Steuerpflichtigen bei diesem selbst.

- Ein Arzt wandte sich dagegen, daß eine Ärztekammer die **Eingangsbestätigung** über die von ihm verlangte Selbsteinstufung, der die Nummer seiner Beitragsgruppe und der zu leistende Jahresbeitrag zu entnehmen war, nicht an seine Privatadresse sondern an seinen Arbeitsplatz übersandt hatte. Da der Betroffene zum Zeitpunkt des Eingangs des Schreibens nicht anwesend war, hatte seine Sekretärin das nicht mit dem Zusatz „persönlich“ gekennzeichnete Schreiben geöffnet. Auf diese Weise wurde ihr die Höhe des Einkommens des Betroffenen aus ärztlicher Tätigkeit bekannt.

Die Ärztekammer vertrat die Auffassung, der Betroffene hätte auf der Selbsteinstufung vermerken müssen, daß er eine Übersendung an seine Privatadresse wünsche. Ein solcher Vermerk war jedoch nicht erforderlich, zumal der Vordruck selbst an die Privatadresse gerichtet war. Nach Artikel 4 Abs. 2 der Landesverfassung wie auch nach § 6 Abs. 1 Satz 1 DSGVO ist die Ärztekammer verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, die zum Schutz der personenbezogenen Daten ihrer Kammerangehörigen gegen unbefugtes Nutzen, Kenntnisnehmen oder Weitergeben erforderlich sind. Sie muß sicherstellen, daß die auf Grund der Beitragsordnung erhobenen Daten nur dem für die Bearbeitung der Beiträge zuständigen Personenkreis bekanntwerden (§ 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSGVO). Zu den erforderlichen Maßnahmen der Datensicherung gehört auch, daß Briefe mit personenbezogenen Daten des Betroffenen, die an dessen Arbeitsplatz versandt werden, jedenfalls mit dem Zusatz „persönlich“ zu kennzeichnen sind, so daß klar erkennbar ist, daß es sich nicht um ein dienstliches Schreiben handelt.

Ich habe der Ärztekammer empfohlen, künftig Briefe mit personenbezogenen Daten ihrer Kammerangehörigen, die an deren Arbeitsplatz gesandt werden, mit dem Vermerk „persönlich“ zu versehen.

- Apotheker vermuteten auf Grund übereinstimmender Schreibfehler in der Anschrift auf Briefen ihrer Apothekerkammer und einer Wählerinitiative für die **Wahl der Kammerversammlung**, daß die Apothekerkammer der Wählerinitiative Adressenmaterial zur Verfügung gestellt habe. Sie baten um Prüfung des Vorgangs.

Nach Mitteilung der Apothekerkammer hat ihr Vorstand beschlossen, bis zum Ablauf der Wahl zur Kammerversammlung Anschriftenmaterial der Apothekerkammer an niemanden mehr auszuhändigen. Diesen Beschluß habe die Apothekerkammer auch uneingeschränkt befolgt. Sie habe seitdem keine Anschriften ihrer Kammerangehörigen an die Wählerinitiative oder an andere Stellen oder Personen weitergegeben. Vor diesem Beschluß habe sie jedoch an Kreisvertrauensapotheker auf deren Anforderung im Einzelfall eine Anschriftenliste der Kammerangehörigen für den jeweiligen Kreis gegeben. Dies sei erforderlich gewesen, wenn ein Kreisvertrauensapotheker die Angehörigen seines Kreises zu einer Versammlung habe einladen wollen. Außerdem habe die Apothekerkammer an ein Mitglied des Vorstandes der Kammer eine Auflistung der zu dieser Zeit gemeldeten WIV-Apotheker (Wissenschaft und Verwaltung) übersandt. Dieses Vorstandsmitglied vertrete im Vorstand der Kammer diese Berufsgruppe der Apotheker. Die Apothekerkammer habe ausdrücklich darauf hingewiesen, daß die Auflistung der zur Zeit gemeldeten WIV-Apotheker „zur persönlichen Verwendung“ bestimmt sei.

Nach dem Ergebnis meiner Ermittlungen ist dem für den Wohnort des Betroffenen zuständigen Kreisvertrauensapotheker eine Anschriftenliste der

Kammerangehörigen für seinen Kreis nicht übersandt worden. Allerdings war der Name und die Anschrift des Betroffenen in der dem Vertreter der Bezirksgruppe WIV – der auch der Betroffene angehörte – übersandten Liste aufgeführt. Nach den Feststellungen der Apothekerkammer hatte der Vertreter der Bezirksgruppe WIV die Liste zweckwidrig für die Wählerinitiative verwandt. Diese Zweckentfremdung verstieß gegen Vorschriften über den Datenschutz.

- Eine Zahnärztekammer bat um Auskunft, ob es zulässig sei, den **Gesundheitsämtern** Namen und Anschriften ihrer Kammerangehörigen zu übermitteln.

Ein solcher Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs.1 in Verbindung mit Artikel 1 Abs.1 des Grundgesetzes bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen muß; aus ihr müssen sich Voraussetzungen und Umfang der Einschränkung des Grundrechts klar und für den Bürger erkennbar ergeben. Es ist zweifelhaft, ob und gegebenenfalls inwieweit die Generalklauseln der Datenschutzgesetze für sich allein oder in Verbindung mit anderen Rechtsvorschriften als gesetzliche Grundlage für einen solchen Informationseingriff noch herangezogen werden können. Dies gilt insbesondere für Übermittlungsvorschriften, die – wie die hier in Betracht kommende 2. Alternative des § 11 Abs.1 Satz 1 DSG NW – an die rechtmäßige Aufgabenerfüllung des Empfängers anknüpfen, da sie den Verwendungszweck der Daten bei dem Empfänger nicht bestimmen und deshalb den Umfang des Eingriffs für den Bürger nicht erkennen lassen.

Nach meiner Auffassung können nur bei weniger schwerwiegenden Einschränkungen des Rechts auf informationelle Selbstbestimmung auch künftig als Generalklauseln ausgestaltete Auffangnormen in den Datenschutzgesetzen ausreichen. Dies gilt für Übermittlungen etwa dann, wenn die Daten von dem Empfänger für den gleichen Zweck benötigt werden, für den sie von der übermittelnden Stelle erhoben wurden oder gespeichert sind, oder wenn sie nicht personenbezogen verwendet werden sollen. Beide Voraussetzungen liegen hier jedoch nicht vor.

Bei einer stärkeren Belastung des Betroffenen kann eine Datenübermittlung jedoch nur noch dann als zulässig angesehen werden, wenn dafür eine bereichsspezifische gesetzliche Grundlage vorhanden ist. Dies gilt etwa dann, wenn – wie hier – die Daten von dem Empfänger personenbezogen für einen anderen Zweck verwendet werden sollen, insbesondere wenn sie für Maßnahmen bestimmt sind, die den Betroffenen belasten.

Da somit die Übermittlung von Namen und Anschriften der Kammerangehörigen an das Gesundheitsamt nicht auf § 11 Abs.1 Satz 1 DSG NW gestützt werden kann und eine bereichsspezifische gesetzliche Grundlage nicht ersichtlich ist, ist die Übermittlung nicht zulässig.

Auf einen „Übergangsbonus“, der nach der Rechtsprechung des Bundesverfassungsgerichts unter bestimmten Voraussetzungen die Übermittlung personenbezogener Daten bis zur Schaffung einer erforderlichen bereichsspezifischen gesetzlichen Grundlage rechtfertigen könnte, kann die Übermittlung im vorliegenden Fall schon deswegen nicht gestützt werden, weil das Gesundheitsamt die zur Erfüllung seiner Aufgaben benötigten Daten nach § 4 Abs. 2 der Ersten Verordnung über die Zulassung der regelmäßigen Datenübermittlung von Meldebehörden an andere Behörden oder sonstige öffentliche Stellen erhält.

Im Zusammenhang mit der Bearbeitung des Beratungersuchens dieser Zahnärztekammer wurde mir bekannt, daß auch eine Ärztekammer dem

Gesundheitsamt Name und Anschrift ihrer Kammerangehörigen übermittelt. Ich habe der Ärztekammer empfohlen, künftig von der Übermittlung personenbezogener Daten ihrer Kammerangehörigen abzusehen. Die Ärztekammer wird dieser Empfehlung folgen.

- Die Ehefrau eines Apothekers beschwerte sich darüber, daß eine Apothekerkammer dem **Kreiswehersatzamt** sie betreffende personenbezogene Daten übermittelt hat, die nur dem Personalmeldebogen entnommen sein konnten.

Nach Mitteilung der Apothekerkammer ist es eine ständige Übung der Kreiswehersatzämter, die Kammer um Stellungnahme zu Zurückstellungsanträgen von wehrpflichtigen Apothekern zu ersuchen. Diesen Ersuchen um Stellungnahme geht ein Antrag eines wehrpflichtigen Apothekers auf Freistellung oder Zurückstellung vom Wehrdienst an das zuständige Kreiswehersatzamt voraus. Der betreffende Apotheker trägt in der Regel vor, er sei in der von ihm geleiteten öffentlichen Apotheke nicht entbehrlich. Das zuständige Kreiswehersatzamt richtet daraufhin an die Apothekerkammer die Bitte um Stellungnahme, welche Hilfskräfte dem Antragsteller in der von ihm geleiteten Apotheke zur Verfügung stehen, wer den Antragsteller als Inhaber der Betriebserlaubnis im Krankheitsfalle vertrete und welche Maßnahmen der Antragsteller im Hinblick auf die bevorstehende Einberufung zur Aufrechterhaltung des Apothekenbetriebes unternommen habe.

Die Kammer nimmt zu einer derartigen Anfrage nach ihrem Kenntnisstand, insbesondere unter Auswertung des Personalmeldebogens des betreffenden Apothekenleiters Stellung. In ihrer Stellungnahme beschränkt sich die Kammer darauf, ausschließlich die Zahl der Mitarbeiter, nicht aber deren Namen zu nennen. Wird in der Anfrage eines Kreiswehersatzamtes nach der Ehefrau des Antragstellers gefragt, wird mitgeteilt, daß diese als Apothekerin im Mitarbeiterverhältnis gemeldet ist.

Die Weitergabe personenbezogener Daten durch die Apothekerkammer an die Kreiswehersatzämter ohne Einwilligung des Betroffenen stellt einen Eingriff in dessen Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes und in sein Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung dar. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen muß; aus ihr müssen sich Voraussetzungen und Umfang der Einschränkung des Grundrechts klar und für den Bürger erkennbar ergeben.

Soweit die Daten in einer Datei wie etwa der Sammlung der Personalmeldebogen gespeichert sind, kommt als gesetzliche Grundlage für die Weitergabe § 11 Abs. 1 Satz 1 DSGVO in Verbindung mit § 5 Abs. 1 Buchst. b des Heilberufsgesetzes (HeilBerG), soweit sie lediglich in Akten oder sonstigen Unterlagen festgehalten werden, allein die zuletzt genannte Vorschrift in Betracht. Nach der 1. Alternative des § 11 Abs. 1 Satz 1 DSGVO ist die Übermittlung an öffentliche Stellen zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist. Nach § 5 Abs. 1 Buchst. b HeilBerG ist es Aufgabe der Kammern, auf Verlangen der zuständigen Behörde Fachgutachten zu erstatten.

Die Abgabe einer Stellungnahme zu dem Zurückstellungsantrag eines wehrpflichtigen Apothekers kann als Erstattung eines Fachgutachtens angesehen werden. Soweit es zur Erfüllung dieser Aufgaben erforderlich ist, darf die Apothekerkammer in ihrer Stellungnahme personenbezogene Daten des Antragstellers an das Kreiswehersatzamt weitergeben. Insoweit sind die genannten Vorschriften hinreichend normenklar; der Apotheker kann ihnen entnehmen, daß sich die Kammer zu Fachfragen, die für die Entscheidung für

seinen Antrag erheblich sind, gegenüber dem Kreiswehrrersatzamt auf dessen Verlangen gutachtlich äußern und insoweit Daten zu seiner Person weitergeben muß.

Anders ist die Weitergabe personenbezogener Daten der Ehefrau des Apothekers zu beurteilen. Die Mitteilung, daß diese als Apothekerin im Mitarbeiterverhältnis gemeldet ist, ist durch die genannten Vorschriften nicht gedeckt. Die Ehefrau braucht nach diesen Vorschriften nicht damit zu rechnen, daß in einem Verfahren, das nicht sie betrifft, auch Daten zu ihrer Person an eine andere Stelle weitergegeben werden. Im übrigen ist eine derartige Mitteilung für die Stellungnahme auch nicht erforderlich. Um darzulegen, daß entgegen der Darstellung des Betroffenen gegenüber dem Kreiswehrrersatzamt eine ausreichende Vertretung gesichert ist, reicht es aus, dem Kreiswehrrersatzamt mitzuteilen, daß ein/e Apotheker/in im Mitarbeiterverhältnis gemeldet ist, ohne darauf hinzuweisen, daß es sich um die Ehefrau des Betroffenen handelt.

Da somit eine gesetzliche Grundlage nicht vorhanden ist, ist die Mitteilung personenbezogener Daten der Ehefrau ohne deren Einwilligung nicht zulässig. Dies gilt auch dann, wenn die Mitteilung ohne Namensangabe gemacht wird, da die Person der Betroffenen mit den bei dem Kreiswehrrersatzamt vorhandenen Unterlagen bestimmbar ist.

Die Apothekerkammer wird auf meine Empfehlung künftig bei gutachtlichen Stellungnahmen gegenüber dem Kreiswehrrersatzamt lediglich mitteilen, ob ein Apotheker im Mitarbeiterverhältnis gemeldet ist.

- Eine Ärztekammer fragte bei mir an, ob die Übermittlung von Namen und Anschriften der Ärzte mit der Teilgebietsbezeichnung „Rheumatologie“ an die **Deutsche Gesellschaft für Rheumatologie** zulässig sei.

Die Weitergabe personenbezogener Daten durch die Ärztekammer an die Deutsche Gesellschaft für Rheumatologie ohne Einwilligung der Betroffenen stellt einen Eingriff in deren Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes und in ihr Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung dar, der einer gesetzlichen Grundlage bedarf.

Eine bereichsspezifische Rechtsvorschrift, die die Übermittlung der vorgeannten Daten gestattet, ist nicht vorhanden. Insbesondere scheidet § 5 Abs. 1 HeilBerG als Rechtsgrundlage für die Übermittlung aus. In dieser Vorschrift sind die Aufgaben der Kammern geregelt; hierzu gehört die Übermittlung von Namen und Anschriften der Ärzte mit der Teilgebietsbezeichnung „Rheumatologie“ jedoch nicht.

Auf die Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen kann die Übermittlung der Namen und Anschriften der Ärzte ebenfalls nicht gestützt werden. Nach der hier in Betracht kommenden 2. Alternative des § 13 Abs. 1 Satz 1 DSGVO ist die Übermittlung personenbezogener Daten aus einer Datei an Dritte 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. Ein berechtigtes Interesse der Deutschen Gesellschaft für Rheumatologie an der Kenntnis der erbetenen Daten könnte zwar vorliegen. Durch die Übermittlung können jedoch schutzwürdige Belange der Betroffenen beeinträchtigt werden. Die nach dieser Vorschrift gebotene Interessenabwägung führt im vorliegenden Fall dazu, daß das Interesse der Deutschen Gesellschaft für Rheumatologie an der Kenntnis der Daten gegenüber dem Interesse der Kammermitglieder am Schutz ihrer personenbezogenen Daten zurücktreten muß.

Da die Beeinträchtigung schutzwürdiger Belange jedenfalls nicht auszuschließen ist, bedarf die Übermittlung der Namen und Anschriften der Ärzte mit der Teilgebietsbezeichnung „Rheumatologie“ der Einwilligung der Betroffenen (§ 3 Satz 1 Nr. 2 DSGVO).

## 13. Personalwesen

### a) Feststellung der Eignung

Praktikanten, die im Rahmen ihrer sozialpädagogischen Ausbildung ein kurzfristiges unentgeltliches **Praktikum** bei einer Stadt abgeleistet haben, haben mich gebeten, den Umfang der Erhebung ihrer personenbezogenen Daten anlässlich ihrer Einstellung datenschutzrechtlich zu überprüfen. Die Betroffenen wandten sich insbesondere gegen die ihnen abverlangten Erklärungen über Vorstrafen sowie zu ihren wirtschaftlichen Verhältnissen und zur Verfassungstreue wie auch gegen die Ausfüllung des vollständigen Personalblattes.

Nach Artikel 4 Abs. 2 der Landesverfassung wie auch nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes bedarf ein derartiges Verlangen einer gesetzlichen Grundlage. Hierfür kommt nur Artikel 33 Abs. 2 des Grundgesetzes in Verbindung mit den jeweiligen Ausbildungs- und Prüfungsordnungen in Betracht. Nach Artikel 33 Abs. 2 des Grundgesetzes hat jeder Deutsche nach seiner Eignung, Befähigung und fachlichen Leistung gleichen Zugang zu jedem öffentlichen Amt. Dabei ist es unerheblich, ob das öffentliche Amt im Beamtenverhältnis oder auf Grund eines privatrechtlichen Vertrages wahrgenommen wird. Es obliegt dem öffentlichen Arbeitgeber, das Vorliegen der erforderlichen Eigenschaften für den Zugang zu einem Ausbildungsplatz im öffentlichen Dienst zu prüfen. Hierbei wird sich der Arbeitgeber in der Regel auf die Prüfung der Eignung des Bewerbers beschränken müssen, da sich Befähigung und fachliche Leistung im allgemeinen erst nach entsprechender Unterweisung und praktischer Bewährung feststellen lassen. Der Begriff der Eignung ist als unbestimmter Rechtsbegriff gesetzlich nicht definiert. Er gewährt dem Arbeitgeber einen weiten Beurteilungsspielraum. Soweit dies zur Feststellung der Eignung erforderlich ist, dürfen auch personenbezogene Daten erhoben werden. Das bedeutet jedoch nicht, daß ein öffentlicher Arbeitgeber berechtigt wäre, beliebige Daten zu erfragen.

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. Das Fragerecht des öffentlichen Arbeitgebers wird auch durch den verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz eingeschränkt. Danach muß der in der Erhebung personenbezogener Daten liegende Eingriff nicht nur erforderlich sein, um den angestrebten Zweck zu erreichen; die damit verbundene Belastung muß auch in einem angemessenen Verhältnis zu den daraus erwachsenden Vorteilen stehen.

Gegen die Abgabe einer Erklärung über Vorstrafen sowie einer Erklärung zur freiheitlichen demokratischen Grundordnung bestehen bei einer Beschäftigung im Bereich der Erziehung keine durchgreifenden datenschutzrechtlichen Bedenken. Unverhältnismäßig erscheint jedoch das Verlangen nach Abgabe der Erklärung über wirtschaftliche Verhältnisse sowie nach Ausfüllung des vollständigen Personalblattes bei Praktikanten, die lediglich ein unentgeltliches sechswöchiges Praktikum ableisten. Derart umfangreiche Angaben waren für die Erfüllung der Aufgaben des Arbeitgebers jedenfalls im vorliegenden Falle weder erforderlich noch dienlich.

## b) Personalakten

- Ein Bürger hat sich an mich gewandt mit der Frage, ob seine in einer **automatisierten Datei** gespeicherten Personaldaten auch in seiner Personalakte festgehalten und ob in regelmäßigen Abständen Ausdrucke aus dieser Datei erstellt werden müssen.

Aus dem von der Rechtsprechung zu § 102 des Landesbeamtengesetzes (LBG) entwickelten Grundsatz der Vollständigkeit der Personalakten folgt, daß in einer Datei der Dienststelle keine Personaldaten gespeichert werden dürfen, die nicht zugleich auch in den Personalakten festgehalten werden. Wird aus einer automatisierten Datei ein Ausdruck gefertigt, so muß nach meiner Auffassung eine Kopie zu den Personalakten genommen werden.

Eine Regelung, die die Fertigung eines Ausdrucks in regelmäßigen Zeitabständen vorschreibt, besteht nicht. Der Bedienstete kann jedoch nach meiner Auffassung verlangen, daß ein Ausdruck gefertigt und zu den Personalakten genommen wird.

- Ein Kommunalbeamter hat mir mitgeteilt, daß der Vorgang, der seine **Eingabe** an seinen Dienstherrn wegen der Weitergabe von Daten zu seiner Person an die Presse betreffe, nicht zu seinen Personalakten genommen worden sei, sondern im Hauptamt der Stadt aufbewahrt werde. Er sieht darin einen Verstoß gegen Vorschriften über den Datenschutz.

Nach § 102 Abs. 1 Satz 1 LBG hat der Beamte ein Recht auf Einsicht in seine vollständigen Personalakten; dazu gehören alle ihn betreffenden Vorgänge mit Ausnahme der Prüfungsakten. Dieses Recht setzt voraus, daß alle den Beamten betreffenden Vorgänge in Personalakten gesammelt werden. Nach Nr. 1.1 VV zu § 102 LBG gehören zu den Personalakten alle Vorgänge über die dienstlichen und persönlichen Verhältnisse des Beamten, soweit sie seine Rechtsstellung oder seine dienstliche Verwendung betreffen oder im Zusammenhang mit seinen Rechten und Pflichten aus dem Beamtenverhältnis stehen.

Ich habe dem Oberstadtdirektor empfohlen, den die Eingabe wegen der Weitergabe der personenbezogenen Daten des Betroffenen an die Presse betreffenden Vorgang zu dessen Personalakten zu nehmen. Der Oberstadtdirektor ist meiner Empfehlung bisher nicht gefolgt.

- Ein Beamter wandte sich dagegen, daß zwei dienstliche **Beurteilungen**, die auf seine Gegenvorstellung hin geändert worden waren, zusammen mit dem zwischen ihm und seiner Dienststelle gewechselten Schriftverkehr nicht in seiner Personalakte, sondern in einer Sachakte festgehalten wurden.

Ich habe der Dienststelle empfohlen, sowohl die beiden beanstandeten Beurteilungen des Betroffenen wie auch den dazu entstandenen Schriftverkehr in einer Beiakte zur Personalakte aufzubewahren. Auf diese Weise wird vermieden, daß der Hauptordner der Personalakte mit überholten Vorgängen belastet wird und diese damit jedem, der Einsicht in die Personalakte erhält, zur Kenntnis gelangen. Der Leiter der Dienststelle wird meiner Empfehlung folgen.

- Ein Lehrer hat sich darüber beschwert, daß ihm das Protokoll über die im Rahmen eines Dienstgesprächs durch den Regierungspräsidenten ausgesprochene **Mißbilligung** offen auf dem Dienstwege vom Regierungspräsidenten über das zuständige Schulamt und von dort an seine Schule durch den Schulleiter, mit dessen Paraphe versehen, zugeleitet worden sei. Dadurch hätten mit Sicherheit die Schulsekretärin, wahrscheinlich aber auch Bedienstete des Schulamtes die Möglichkeit gehabt, Kenntnis von dem Inhalt des Protokolls zu nehmen.

Die in dem Protokoll festgehaltenen personenbezogenen Daten unterliegen dem Grundrecht des Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung wie auch dem Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes. Das Weitergeben solcher Daten bedarf einer gesetzlichen Grundlage oder der Einwilligung des Betroffenen.

Eine gesetzliche Grundlage für die Weitergabe einer mißbilligenden Äußerung des Dienstvorgesetzten (§ 6 Abs. 3 der Disziplinarordnung des Landes Nordrhein-Westfalen) über den Schulträger an den Schulleiter als Vorgesetzten des Bediensteten (§ 20 Abs. 2 Satz 3 des Schulverwaltungsgesetzes) ist nicht ersichtlich. Insbesondere kann sie weder der Disziplinarordnung noch dem Schulverwaltungsgesetz entnommen werden. Ist die Weitergabe personenbezogener Daten nicht in einer Rechtsvorschrift ausdrücklich vorgesehen, dürfen nur solche Angaben weitergegeben werden, deren Kenntnis zur Erfüllung einer gesetzlichen Aufgabe des Empfängers unbedingt notwendig ist. Darüber hinaus ist der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Danach muß die Weitergabe nicht nur notwendig sein, um den angestrebten Zweck der Verwaltung zu erreichen; die mit diesem Eingriff verbundene Belastung des Betroffenen muß auch in einem angemessenen Verhältnis zu den daraus erwachsenden Vorteilen stehen. Im vorliegenden Fall hätte es ausgereicht, nur dem Schulleiter für die Erfüllung seiner Aufgaben als Vorgesetzter mitzuteilen, daß der Dienstvorgesetzte ein bestimmtes Verhalten des Bediensteten mißbilligt habe.

Die offene Weitergabe des Protokolls als Bestandteil der Personalakte des Betroffenen ist in jedem Falle unzulässig. Die für die Bearbeitung von Personalakten geltenden Rechtsvorschriften setzen voraus, daß die mit der Bearbeitung beauftragten Bediensteten Zugang zu den Personalakten haben, soweit die Kenntnis der Vorgänge für die Bearbeitung erforderlich ist. Die Einsichtgewährung an andere Personen ist nicht zulässig. Um diese zu vermeiden, hätte dem Betroffenen das Protokoll im verschlossenen Umschlag mit der Aufschrift „Personalsache – Vertraulich“ übersandt werden müssen. Entsprechendes gilt für die Mitteilung des Dienstvorgesetzten an den Schulleiter.

- Einem Beamten einer Stadtparkasse wurden in einem anonymen Schreiben Einzelheiten aus einem gegen ihn durchgeführten **Disziplinarverfahren** in Nötigungsabsicht vorgehalten. Dem Schreiben, von dem sechs weitere Personen Durchschriften erhalten haben, waren Fotokopien von Vermerken über zwischen ihm und dem „Anzeigenerstatter“ des Disziplinarverfahrens geführte Telefongespräche beigelegt, die Bestandteile der Disziplinarakte beim Stadtdirektor waren.

Einen Hinweis dafür, aus welcher Quelle die mit den anonymen Briefen versandten Kopien der Gesprächsvermerke stammen, haben meine Ermittlungen nicht ergeben.

Auf meine Anregung haben der Stadtdirektor und der Vorsitzende des Vorstands der Stadtparkasse die Bediensteten, die in ihrem Bereich Zugang zu den Gesprächsvermerken hatten, um eine dienstliche Erklärung darüber gebeten, ob sie die Vermerke einem Dritten zugänglich gemacht hätten oder ob sie wüßten, wer der Verfasser des anonymen Schreibens sei. Alle in Betracht kommenden Bediensteten haben in einer entsprechenden Erklärung die gestellten Fragen verneint.

Darüber hinaus wurden Erklärungen von den Mitarbeitern der Stadtparkasse erbeten, die nach Auskunft des Vorstands zwar keinen Zugang zu den Vermerken hatten und auch nicht unterrichtet waren, jedoch im unmittelbaren Umfeld des Vorstands tätig sind oder als Mitarbeiter der Personalabteilung

die Sonderakte in einem verschlossenen Umschlag der Personalakte des Betroffenen verwahren. Diese Personen haben erklärt, sie hätten Schriftstücke der genannten Art, welche die Personalakte des Betroffenen betreffen, nicht gesehen und somit auch nicht an Dritte weitergegeben.

Nach diesem Ermittlungsergebnis konnte eine Verletzung der Verschwiegenheitspflicht (§ 64 Abs. 1 Satz 1 LBG, § 9 Abs. 1 BAT, § 203 Abs. 2 und § 353b Abs. 1 StGB) durch Bedienstete der Stadt oder der Stadtparkasse nicht mit der für eine Beanstandung nach § 30 DSGVO erforderlichen Sicherheit festgestellt werden.

Weitere Möglichkeiten, den Sachverhalt aufzuklären, hat der Landesbeauftragte für den Datenschutz nicht. Zwar kann er nach § 26 Abs. 3 DSGVO im Rahmen seiner Kontrollbefugnis von öffentlichen Stellen Auskunft zu Fragen sowie Einsicht in Unterlagen und Akten verlangen, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen; er kann ferner die Stellen jederzeit auch unangemeldet aufsuchen und ihre Diensträume betreten. Der Landesbeauftragte für den Datenschutz hat jedoch nicht die Befugnis, Bedienstete dieser Stellen zu vernehmen. Eine solche Möglichkeit hätte die Staatsanwaltschaft in einem strafrechtlichen Ermittlungsverfahren.

### **c) Beihilfen**

Bedienstete haben sich gegen das bei ihrer Behörde übliche Verfahren bei der Bearbeitung von Beihilfeanträgen gewandt. Sie rügten insbesondere, daß bei Anträgen auf Beteiligung zu den Aufwendungen für einen Kur- oder Sanatoriumsaufenthalt die amtsärztliche Stellungnahme geöffnet dem Behördenleiter vorgelegt und offen mit dem Beihilfeantrag auf dem Dienstweg der Beihilfestelle zugeleitet werde.

Beihilfeanträge, zu denen auch Anträge auf Beteiligung zu den Aufwendungen für einen Kur- oder Sanatoriumsaufenthalt gehören, sind vertraulich zu behandeln (§ 13 Abs. 2 Satz 4 der Beihilfenverordnung) und nur solchen Verwaltungsangehörigen vorzulegen, die mit der Bearbeitung von Personalangelegenheiten betraut sind. Beihilfeberechtigte, die ihren Antrag auf dem Dienstwege einreichen, sind berechtigt, die Belege und sonstigen ärztlichen Unterlagen in einem verschlossenen Umschlag beizufügen, der nur von den zuständigen Sachbearbeitern geöffnet werden darf (vgl. Köhnen/Mohr, Beihilfenrecht, § 13 Anm. 3 Abs. 4). Auch amtsärztliche Gutachten, die nicht von den Beihilfeberechtigten selbst vorgelegt, sondern von dem zuständigen Gesundheitsamt der Dienststelle übersandt werden, dürfen nur den zuständigen Sachbearbeitern im verschlossenen Umschlag zugeleitet und von diesen geöffnet werden.

### **d) Hausarbeitstag**

Bedienstete von Einrichtungen eines Sozialversicherungsträgers haben mich gebeten, den dort verwandten Antragsvordruck zur Bewilligung des monatlichen Hausarbeitstages datenschutzrechtlich zu überprüfen. In dem Vordruck wurde unter anderem nach Mitbewohnern der von der Antragstellerin genutzten Wohnung, nach Einzelheiten des Mietvertrages und nach der Mobiliarausstattung gefragt. Die Antragstellerin sollte weiterhin angeben, ob sie selbst die Wohnung sauber hält, ihre Wäsche ganz oder zum Teil selbst herrichtet und regelmäßig unter Benutzung der Kochstelle in ihrer Wohnung die Mahlzeiten zubereitet.

Das Verlangen der in dem Antragsvordruck vorgesehenen Angaben greift in das Recht der Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes wie auch in ihr Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung ein. Zwar ist für diese Datenerhebung eine gesetzliche Grundlage vorhanden (§ 1 des Gesetzes über Freizeitgewährung für Frauen mit eigenem Hausstand in

Verbindung mit § 26 Abs. 1 und 2 des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen). Bei der Datenerhebung ist jedoch der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Danach muß die Erhebung nicht nur notwendig sein, um den angestrebten Zweck der Verwaltung zu erreichen; die mit dem Eingriff verbundene Belastung des Betroffenen muß auch in einem angemessenen Verhältnis zu dem daraus erwachsenden Nutzen stehen.

Ich habe Zweifel, ob alle in dem Antrag auf Bewilligung des monatlichen Hausarbeitstages verlangten Angaben zur Feststellung der Notwendigkeit von Freizeitgewährung für die Haushaltsführung erforderlich sind. Dies gilt insbesondere für die oben genannten Fragen. Diese Fragen halte ich darüber hinaus wegen des mit der Menschenwürde (Artikel 1 Abs. 1 des Grundgesetzes) nicht vereinbaren Eindringens in den privaten Bereich für unzulässig. Sie dürfen nach meiner Auffassung auch dann nicht gestellt werden, wenn der Antragstellerin die Beantwortung freigestellt wird. Für die Feststellung des Anspruchs auf einen Hausarbeitstag reicht nach meiner Auffassung die Erklärung der Antragstellerin aus, daß sie einen eigenen Hausstand führt und ihr keine ausreichende Haushaltshilfe durch Eltern, Geschwister, Kinder oder andere Personen zur Verfügung steht.

#### **e) Telefongespräche**

- Auch in diesem Berichtszeitraum wandten sich Bedienstete gegen das Verfahren öffentlicher Stellen bei der Telefondatenerfassung.

Die Speicherung der vollständigen Rufnummer des angewählten Gesprächsteilnehmers bei privaten Gesprächen über dienstliche Fernmeldeeinrichtungen bei öffentlichen Stellen des Landes hatte ich als Verstoß gegen § 3 Satz 1 DSGVO sowie gegen Artikel 10 Abs. 1 des Grundgesetzes beanstandet (vgl. C.14.d meines zweiten, C.10.c meines dritten und C.12.d meines vierten Tätigkeitsberichts). Zwar betraf diese Beanstandung die Gesprächsdatenerfassung im automatisierten Verfahren. Entsprechendes muß aber auch dann gelten, wenn private Ferngespräche anhand von Gesprächszetteln oder anhand eines Gebührenbuches nachzuweisen sind oder wenn Bedienstete über ihre privaten Orts- und Nahgespräche selbst Anschreibungen zu führen haben, wie dies in der durch Runderlaß vom 18. Juni 1984 geänderten Fassung der Dienstanschlußvorschriften vorgesehen ist. Für die Zuordnung der privaten Gespräche zu dem gesprächführenden Bediensteten ist in diesen Fällen weder die Rufnummer noch der Ort des Gesprächsteilnehmers erforderlich, da bei Ferngesprächen der Anmelder sich gegenüber der Telefonvermittlung identifizieren muß und bei Orts- und Nahgesprächen jeder Bedienstete die von ihm geführten Gespräche selbst aufzeichnet. Nach meiner Auffassung sind daher die Bediensteten nicht verpflichtet, in den von ihnen zu führenden Nachweisungen die Telefonnummer des Gesprächsteilnehmers anzugeben.

Wie der Stellungnahme der Landesregierung zu meinem sechsten Tätigkeitsbericht (Drucksache 10/430, S. 10) zu entnehmen ist, werden bezüglich der Gesprächsdatenerfassung von Bediensteten in Landesbehörden seit längerem Überlegungen zu einer datenschutzfreundlicheren Verfahrensweise angestellt. Die Landesregierung hat in diesem Zusammenhang ihre grundsätzliche Bereitschaft betont, bei der Gesprächsdatenerfassung den Datenschutz zu verbessern. Im Hinblick auf diese Bemühungen habe ich von einer förmlichen Beanstandung des in den Dienstanschlußvorschriften vorgesehenen Verfahrens bei der Erfassung von privaten Telefongesprächen in Dienststellen, die nicht über eine automatische Gesprächsdatenerfassungsanlage verfügen, vorerst abgesehen.

- Der mir vorgelegte „Nachweis der Telefongespräche“, der von der Fernsprechgebührenerfassungsanlage einer Klinik erstellt wurde, unterscheidet nicht zwischen dienstlichen und privaten Telefongesprächen. Nach Auskunft des Verwaltungsleiters der Klinik sind in dem Ausdruck auch die privaten Gespräche erfaßt, ohne besonders gekennzeichnet zu sein. Die Privatgespräche würden über ihn angemeldet und dort auch abgerechnet. Trotzdem erscheinen sie – ohne Kennzeichnung – in dem monatlichen Nachweis der Telefongespräche. Wie mir der Verwaltungsleiter weiter mitteilte, erhält der leitende Arzt jeder Abteilung den Ausdruck über sämtliche in seiner Abteilung geführten Telefonate, aufgeschlüsselt nach den einzelnen Nebenstellen, zur Kenntnis. Er erhält damit auch Kenntnis von privaten Telefongesprächen seiner Mitarbeiter.

Nach § 5 Abs. 1 DSGVO ist es den bei der Datenverarbeitung beschäftigten Personen untersagt, geschützte personenbezogene Daten unbefugt zugänglich zu machen. Nach § 6 Abs. 1 Satz 1 DSGVO haben die datenverarbeitenden Stellen die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen zu gewährleisten. Dazu gehört insbesondere, die Daten vor unbefugter Kenntnisnahme durch Dritte zu schützen.

Durch die Weitergabe des Nachweises der Telefongespräche an den jeweils leitenden Arzt einer Abteilung werden diesen Angaben über private Gespräche – auch wenn sie nicht als solche gekennzeichnet sind – unbefugt zugänglich gemacht. Wenn die Klinik eine Kontrolle der dienstlichen Gespräche durch die leitenden Ärzte für erforderlich hält, müssen für dienstliche und private Gespräche getrennte Abrechnungen erstellt werden. Derartige Maßnahmen stehen auch in einem angemessenen Verhältnis zu ihrem Zweck, die Wahrung des Datengeheimnisses zu gewährleisten (§ 6 Abs. 1 Satz 2 DSGVO).

Ich habe der Klinik empfohlen,

- bei der Speicherung der Telefonnummer des Gesprächsteilnehmers bei privaten Gesprächen die beiden letzten Ziffern wegzulassen,
- den Ausdruck der Telefondaten, soweit deren Speicherung zulässig ist, dem Benutzer des jeweiligen Dienstanschlusses im verschlossenen Umschlag zuzuleiten und, sofern eine Kontrolle der dienstlichen Gespräche durch den leitenden Arzt der jeweiligen Abteilung erforderlich gehalten wird, für dienstliche und private Gespräche getrennte Abrechnungen zu erstellen.

Die Klinik ist meinen Empfehlungen gefolgt.

- In einem anderen Fall hatte das Rektorat einer Hochschule auf meine Empfehlung beschlossen, bei privaten Telefongesprächen von Mitarbeitern auf die Speicherung und den Ausdruck der letzten beiden Ziffern der angewählten Telefonnummer zu verzichten. Der Minister für Wissenschaft und Forschung hat diesen Beschluß des Rektorats mit der Begründung, der Beschluß verstoße gegen die Dienstanschlußvorschriften, im Wege der Fachaufsicht beanstandet.

Derartige Aufsichtsmaßnahmen in Fällen, in denen die technische Ausstattung der Gesprächsdatenerfassungsanlage einen Verzicht auf Speicherung und Ausdruck der letzten beiden Ziffern ermöglicht, sind geeignet, die Bereitschaft der Landesregierung zur Verbesserung des Datenschutzes in diesem Bereich in Zweifel zu ziehen. Es wäre daher zu begrüßen, wenn bis zur Einführung eines datenschutzgerechten Verfahrens derartige Aufsichtsmaßnahmen unterbleiben könnten.

Der Minister für Wissenschaft und Forschung hat mir hierzu mitgeteilt, er

habe sich um eine datenschutzrechtlich zulässige landeseinheitliche Regelung der privaten Nutzung dienstlicher Fernmeldeeinrichtungen bemüht. Der hierfür zuständige Finanzminister habe ihn darüber unterrichtet, daß er in Kürze den Entwurf einer Regelung zur Änderung der Dienstanschlußvorschriften mit wesentlichen Verbesserungen des Datenschutzes vorlegen werde.

#### **f) Lehrerdaten**

Eine Lehrerin wandte sich dagegen, daß ihr Schulleiter **Aufzeichnungen über das Verhalten** einzelner Lehrer anfertigte und in Form einer Kartei festhielt.

In meinem vierten Tätigkeitsbericht (C.12.e) habe ich datenschutzrechtliche Bedenken dagegen geäußert, daß in Schulen Durchschriften von schriftlichen Erinnerungen, Mahnungen und Zurechtweisungen, von denen Lehrer betroffen sind, aufbewahrt und bei Leistungsberichten herangezogen werden. Ich habe in diesem Zusammenhang auf die in dem Urteil des Bundesverwaltungsgerichts vom 26. Juni 1980 (BVerwGE 60, 245) dargelegten Grundsätze verwiesen.

Demgegenüber hatte der Kultusminister die Auffassung vertreten, daß die Aufbewahrung schriftlicher Aufzeichnungen über Lehrer durch den Schulleiter, die für die Vorbereitung von Leistungsberichten herangezogen werden sollen, nicht von vornherein unzulässig sei. Fraglich sei allerdings, und dies würde im wesentlichen nur im Einzelfall zu entscheiden sein, in welchem Umfang Aufzeichnungen überhaupt gemacht werden dürften und sollten, damit ein Mißbrauch vermieden wird. Das genannte Urteil des Bundesverwaltungsgerichts gehe zu Recht davon aus, daß Beurteilungen – in einem bestimmten Rahmen – gerichtlich nachprüfbar seien und daß zur Rechtfertigung der Beurteilung, insbesondere von Werturteilen, die Darlegung bestimmter Tatsachen gefordert werden könne. Nach dem Urteil liege es im pflichtgemäßen Ermessen des Dienstherrn, wie er die ihm aufgebene, für zukünftige Personalentscheidungen verwertbare Aussage zu den einzelnen Beurteilungsmerkmalen gestalten und begründen und worauf er im einzelnen sein Gesamturteil über den Beamten stützen wolle. So gingen die Beurteilungsrichtlinien des Landes Baden-Württemberg davon aus, daß schriftliche Aufzeichnungen zur Vorbereitung der Beurteilung gemacht werden dürften.

Der Kultusminister hatte mir mitgeteilt, daß geprüft werde, ob und in welchem Umfang Aufzeichnungen zulässig sind, ob eine generelle Regelung notwendig und möglich ist und wie eine solche Regelung ergehen soll. Das Ergebnis dieser Prüfung ist mir trotz wiederholter Nachfragen bis heute nicht zugegangen. Ich kann daraus nur den Schluß ziehen, daß das Sammeln und Aufbewahren von Aufzeichnungen über dienstliche Vorkommnisse, soweit nicht die Aufnahme in die Personalakte vorgeschrieben ist, nicht geeignet und deshalb nicht erforderlich ist, um den angestrebten Zweck – die Erstellung einer Beurteilung nach objektiven und unparteiischen Gesichtspunkten – zu erreichen. Gegen das genannte Verfahren bestehen deshalb datenschutzrechtliche Bedenken. Keinesfalls zulässig ist die Bekanntgabe des Inhalts der Aufzeichnungen gegenüber Dritten, auch nicht gegenüber anderen Lehrern.

Ich habe dem Schulleiter empfohlen,

- künftig davon abzusehen, Aufzeichnungen über dienstliche Vorkommnisse, soweit sie nicht in die Personalakten aufzunehmen sind, zu sammeln und aufzubewahren;
- die bereits vorhandenen Aufzeichnungen zu vernichten.

#### **g) Datenweitergabe innerhalb einer Stelle**

- Mir ist bekanntgeworden, daß die Verwaltung eines Landschaftsverbandes in

einer **Berichtsvorlage** für die Sitzung des Schulausschusses des Landschaftsverbandes personenbezogene Daten aller Lehrkräfte der zum Landschaftsverband gehörenden Schulen für Erziehungshilfe wie Namen, Geburtsdaten, Fächerkombinationen, Amtsbezeichnungen sowie persönliche Einschätzungen und charakterliche Bewertungen einzelner Lehrkräfte mitgeteilt hat.

Die Bekanntgabe der in der Berichtsvorlage enthaltenen personenbezogenen Daten der Lehrkräfte der Schulen für Erziehungshilfe durch die Verwaltung an den Schulausschuß des Landschaftsverbandes greift in das Grundrecht der Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung und in ihr Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes ein. Solche Eingriffe müssen zwar von den Betroffenen im überwiegenden Interesse der Allgemeinheit hingenommen werden; sie bedürfen jedoch einer gesetzlichen Grundlage.

Soweit die in der Berichtsvorlage enthaltenen Daten (wie Name, Geburtsdatum, Fächerkombination und Amtsbezeichnung) in einer Datei gespeichert sind, kommt als gesetzliche Grundlage für die Weitergabe nur § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSGVO und den Vorschriften der Landschaftsverbandsordnung über die Aufgaben der Fachausschüsse (insbesondere § 11 Abs. 1 Buchst. c, § 13 Abs. 1 und 2) in Betracht. Soweit die Daten (wie persönliche Einschätzungen und charakterliche Bewertungen) lediglich in Akten oder sonstigen Unterlagen festgehalten werden, kommen als gesetzliche Grundlage allein die zuletzt genannten Vorschriften der Landschaftsverbandsordnung in Betracht.

Nach § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSGVO ist die Weitergabe zulässig, wenn sie zur rechtmäßigen Erfüllung der Aufgaben der Verwaltung oder des Schulausschusses erforderlich ist. Nach den genannten Vorschriften der Landschaftsverbandsordnung hat der Landschaftsausschuß die Verwaltungsführung des Direktors des Landschaftsverbandes zu überwachen; zur Entlastung des Landschaftsausschusses kann als Fachausschuß auch ein Schulausschuß gebildet werden. Soweit es zur Erfüllung der Aufgaben dieses Ausschusses erforderlich ist, darf die Verwaltung an ihn personenbezogene Daten der Lehrer weitergeben.

Wie mir der Landschaftsverband mitgeteilt hat, hatte die Darstellung der besonderen Qualifikation der betroffenen Lehrkräfte den Zweck, den Schulausschuß davon zu überzeugen, daß diese Lehrkräfte auf Grund ihrer persönlichen und fachlichen Eignung für die Arbeit mit Heimschülern uneingeschränkt befähigt sind und daß deshalb ein Austausch gegen ausgebildete Sonderschullehrer nicht gerechtfertigt ist. Zu diesem Zweck war es jedoch nicht erforderlich, dem Schulausschuß die Namen und Geburtsdaten der Lehrkräfte bekanntzugeben. Eine Aufstellung über die Qualifikation der einzelnen Lehrkräfte ohne Angabe des Namens und des Geburtsdatums hätte genügt.

Darüber hinaus ist bei Eingriffen in die genannten Grundrechte der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz zu beachten. Danach muß die Belastung des Betroffenen in einem angemessenen Verhältnis zu dem zu erreichenden Zweck stehen. Hiermit ist es nach meiner Auffassung nicht vereinbar, dem Schulausschuß persönliche Einschätzungen und charakterliche Bewertungen namentlich bezeichneter Lehrkräfte mitzuteilen, es sei denn, dies wäre für eine konkrete die Lehrkraft betreffende Verwaltungsentscheidung des Schulausschusses erforderlich.

Da somit eine gesetzliche Grundlage für die Bekanntgabe der Namen und Geburtsdaten der betroffenen Lehrkräfte an den Schulausschuß nicht vor-

handen war und diese Bekanntgabe in Verbindung mit persönlichen Einschätzungen und charakterlichen Bewertungen darüber hinaus gegen den Verhältnismäßigkeitsgrundsatz verstieß, war die Bekanntgabe nicht zulässig.

Ich habe dem Landschaftsverband empfohlen, künftig in derartigen Vorlagen

- Namen und Geburtsdatum des Betroffenen wegzulassen,
- im Hinblick darauf, daß auch bei Weglassen von Namen und Geburtsdatum eine Identifizierung des Betroffenen nicht ausgeschlossen ist, auf subjektive Werturteile nach Möglichkeit zu verzichten.

Der Direktor des Landschaftsverbandes hat mir mitgeteilt, er werde meiner Empfehlung grundsätzlich folgen und künftig Namen und Geburtsdatum des Betroffenen weglassen und auf subjektive Werturteile verzichten.

- Ein Bürger, der sich um einen Ausbildungsplatz bei einer Stadtparkasse beworben hatte, hat mir mitgeteilt, daß ihm die Sparkasse kurz darauf ein Schreiben übersandt hat, in dem um die Eröffnung eines Girokontos geworben wird. Der Betroffene vermutet, daß die Sparkasse seine personenbezogenen Daten, die sie anlässlich seiner Bewerbung erhalten hat, zu **Werbezwecken** genutzt hat.

Die Zulässigkeit der Weitergabe innerhalb der Sparkasse ist nach § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSGVO zu beurteilen. Nach diesen Vorschriften dürfen personenbezogene Daten innerhalb der Sparkasse nur weitergegeben werden, wenn es zur rechtmäßigen Aufgabenerfüllung der weitergebenden oder der empfangenden Stelle innerhalb der Sparkasse erforderlich ist. Bei der Beurteilung der Rechtmäßigkeit der Aufgabenerfüllung ist die Zweckbestimmung zu berücksichtigen, mit der der Betroffene seine Daten der Sparkasse zur Verfügung gestellt hat. Danach kann die Verwendung von Personaldaten, die zu den ihrem Wesen nach geheimzuhaltenden Daten gehören, für Werbezwecke nicht als rechtmäßig angesehen werden. Die interne Weitergabe zu diesem Zweck ist daher unzulässig.

Demgegenüber vertritt die Stadtparkasse die Auffassung, daß für sie als der Aufsicht des Landes unterstehende juristische Person des öffentlichen Rechts, die am Wettbewerb teilnimmt, ausschließlich die Vorschriften des Dritten Abschnitts des Datenschutzgesetzes Nordrhein-Westfalen gelten. Dieser Auffassung kann jedoch nicht gefolgt werden. Die Weitergabe personenbezogener Daten innerhalb derselben öffentlichen Stelle ist im Ersten Abschnitt des Datenschutzgesetzes Nordrhein-Westfalen (§ 8 Satz 1 DSGVO) geregelt. Die Vorschriften des Ersten Abschnitts sind auch für die im Dritten Abschnitt (§ 18 DSGVO) genannten Stellen anzuwenden.

Im Hinblick auf die von der Stadtparkasse vertretene Auffassung habe ich die interne Weitergabe von Personaldaten zu Werbezwecken als Verstoß gegen § 8 Satz 1 DSGVO gemäß § 30 Abs. 1 Satz 1 DSGVO beanstandet.

#### **h) Datenweitergabe an öffentliche Stellen**

- Ein Polizeibeamter hat sich dagegen gewandt, daß bei seiner Versetzung seine von dem Polizeiarzt der bisherigen Dienststelle geführte **Krankenakte** auf Grund der mit Runderlaß des Innenministers vom 9. November 1960 getroffenen Regelung an den Polizeiarzt der neuen Dienststelle gegen seinen ausdrücklichen Widerspruch weitergegeben werden sollte. Er sieht darin eine Verletzung der ärztlichen Schweigepflicht.

Der Umgang mit personenbezogenen Daten der Bediensteten im Polizeivollzugsdienst, insbesondere auch die Weitergabe der Krankenakte mit den in ihr enthaltenen Daten der Bediensteten an andere Polizeiarzte ohne Einwilligung des Betroffenen ist ein Eingriff in das Grundrecht der Betroffenen auf

Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung und in ihr Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes, der einer gesetzlichen Grundlage bedarf. Diese muß dem rechtsstaatlichen Gebot der Normenklarheit entsprechen; aus ihr müssen sich die Voraussetzungen und der Umfang der Einschränkung des Grundrechts klar und für den Bürger erkennbar ergeben.

Eine diesen Anforderungen entsprechende gesetzliche Grundlage für die Weitergabe der Krankenakten, etwa in der Verordnung über die freie Heilfürsorge der Polizeivollzugsbeamten, ist nicht vorhanden. Die entsprechende Vorschrift des Runderlasses des Innenministers vom 9. November 1960 kommt als gesetzliche Grundlage nicht in Betracht, da sie keine Rechtsvorschrift ist.

Darüber hinaus verstößt im vorliegenden Fall die Weitergabe der Krankenakte des Polizeivollzugsbeamten durch den Polizeiarzt gegen die ärztliche Schweigepflicht, die auch zwischen den Polizeiarzten untereinander besteht. Zwar sind Ärzte, wenn sie gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, untereinander von der Schweigepflicht insoweit befreit, als der Patient nicht etwas anderes bestimmt (§ 2 Abs. 6 der Berufsordnung). Eine Befreiung nach dieser Vorschrift kommt jedoch nicht in Betracht, wenn der Betroffene der Weitergabe der Krankenakte ausdrücklich widersprochen hat. Hiervon abgesehen liegt eine Offenbarungsbefugnis nur dann vor, wenn der Schutz eines höherrangigen Rechtsguts die Offenbarung erfordert (§ 2 Abs. 4 der Berufsordnung). Im Fall der Weitergabe wegen Versetzung oder längerdauernder Abordnung vermag ich Anhaltspunkte hierfür nicht zu erkennen.

Ich habe deshalb dem Innenminister empfohlen, die Weitergabe der Krankenakten nur noch mit Einwilligung der Betroffenen zuzulassen oder eine normenklare gesetzliche Regelung zu schaffen, die den Anforderungen des Bundesverfassungsgerichts in seinem Urteil zum Volkszählungsgesetz 1983 entspricht. Das Ergebnis meiner Bemühungen bleibt abzuwarten.

- Ein anderer Polizeivollzugsbeamter hat mich gebeten, das Anfordern der von einem Privatarzt ausgestellten, die Diagnose enthaltenden **Arbeitsunfähigkeitsbescheinigung** durch den Polizeiarzt und das Ablegen dieser Bescheinigung in der von dem Polizeiarzt geführten Krankenakte datenschutzrechtlich zu überprüfen.

Auch für das Zuleiten der Arbeitsunfähigkeitsbescheinigung an den Polizeiarzt und das Ablegen in der Krankenakte ist eine den Anforderungen des Volkszählungsurteils entsprechende gesetzliche Grundlage, etwa in der Verordnung über die freie Heilfürsorge der Polizeivollzugsbeamten, nicht vorhanden. Die entsprechenden Regelungen in einem Runderlaß des Innenministers vom 9. Dezember 1983 kommen auch hier als gesetzliche Grundlage nicht in Betracht, da sie keine Rechtsvorschriften sind.

Selbst bei Vorliegen einer gesetzlichen Regelung bestünden jedoch dagegen rechtliche Bedenken. Sachliche Gründe für die datenschutzrechtliche Schlechterstellung der Polizeivollzugsbeamten gegenüber den übrigen Beamten und Angestellten des öffentlichen Dienstes, die dem Dienstherrn oder einem von ihm bestimmten Arzt nicht zusätzlich eine mit der Angabe der Diagnose versehene Dienstunfähigkeitsbescheinigung vorlegen müssen, sind nicht ersichtlich. Das Sammeln der Dienstunfähigkeitsbescheinigungen mit den Diagnosen in der Krankenakte des Polizeivollzugsbeamten ist eine unzulässige Datenspeicherung „auf Vorrat“.

Darüber hinaus verstößt die Weitergabe von Krankheitsdaten im Wege der Zusendung der Arbeitsunfähigkeitsbescheinigung durch den Hausarzt an den Polizeiarzt gegen die ärztliche Schweigepflicht. Zu den durch sie

geschützten Geheimnissen gehört auch die Angabe der Diagnose. Eine Offenbarungsbefugnis liegt nur dann vor, wenn der Betroffene den Arzt von der Schweigepflicht entbunden hat oder wenn der Schutz eines höherrangigen Rechtsguts die Offenbarung erfordert. Diese Voraussetzungen liegen hier nicht vor.

Die ärztliche Schweigepflicht besteht grundsätzlich auch zwischen Ärzten untereinander. Zwar sind Ärzte, wenn sie gleichzeitig oder nacheinander denselben Patienten untersuchen oder behandeln, untereinander von der Schweigepflicht insoweit befreit, als der Patient nicht etwas anderes bestimmt (§ 2 Abs. 6 der Berufsordnung). Eine Befreiung nach dieser Vorschrift kommt jedoch hier nicht in Betracht, weil der Polizeiarzt den arbeitsunfähigen Beamten nicht untersucht oder behandelt.

Ich habe daher dem Innenminister empfohlen, auf die Vorlage einer mit der Angabe der Diagnose versehenen Arbeitsunfähigkeitsbescheinigung des Hausarztes zur Krankenakte zu verzichten oder eine normenklare gesetzliche Regelung zu schaffen, die den Anforderungen des Bundesverfassungsgerichts in seinem Urteil zum Volkszählungsgesetz 1983 entspricht.

- Der Personalrat einer Polizeibehörde hat sich dagegen gewandt, daß dem Innenminister im Rahmen der **Krankenstatistik** für den Polizeivollzugsdienst die krankheitsbedingten Dienstauffälle der Polizeivollzugsbeamten mit zahlreichen Angaben zur Person, insbesondere unverschlüsselten Angaben über Art und Umfang der Erkrankung sowie über die Tatsache einer Aufnahme in ein Krankenhaus oder eine Heilstätte durch den jeweiligen Polizeiarzt gemeldet werden.

Eine bereichsspezifische Regelung der Krankenstatistik für Polizeivollzugsbeamte, etwa im Landesbeamtengesetz oder in der Verordnung über die freie Heilfürsorge der Polizeivollzugsbeamten, ist nicht vorhanden. Entsprechende Regelungen in einem Runderlaß des Innenministers vom 3. Februar 1969 kommen auch in diesem Fall als gesetzliche Grundlage nicht in Betracht, da sie keine Rechtsvorschriften sind.

Darüber hinaus verstößt die Weitergabe von Krankheitsdaten der Polizeibediensteten durch den jeweiligen Polizeiarzt gegen die ärztliche Schweigepflicht. Zu den hiernach geschützten Geheimnissen gehören auch die unverschlüsselten Angaben auf dem Krankenstammblatt über Art und Umfang der Erkrankung sowie die Angaben über die Tatsache einer Aufnahme in ein Krankenhaus oder in eine Heilstätte. Auch hier liegt eine Offenbarungsbefugnis nicht vor.

Ich habe dem Innenminister empfohlen, die Weitergabe der Krankenstammbblätter nach dem genannten Runderlaß nur noch mit Einwilligung des Betroffenen zuzulassen oder für die Durchführung der Krankenstatistik der Polizeivollzugsbeamten eine normenklare gesetzliche Regelung zu schaffen, die den Anforderungen des Bundesverfassungsgerichts in seinem Urteil zum Volkszählungsgesetz 1983 entspricht.

- Ärztinnen eines Gesundheitsamtes haben mich gebeten, die Erhebung ihrer personenbezogenen Daten im Rahmen eines Berichts über die Personalverhältnisse der **Gesundheitsämter** an den Regierungspräsidenten datenschutzrechtlich zu überprüfen. Im einzelnen werden von den Betroffenen folgende Angaben verlangt:
  - Name, Vorname, Dienstbezeichnung, Dienststellung, Besoldungs-/Vergütungsgruppe;
  - Gesundheitsamt der Stadt/des Kreises;
  - Geburtstag, Familienstand, Privatanschrift, Telefonnummer;

- Daten zu Staatsexamen, Approbation, Promotion, Facharztanerkennung, Fachgebiet und Amtsarztexamen;
- beruflicher Werdegang nach der Approbation.

Nach Mitteilung des Ministers für Arbeit, Gesundheit und Soziales wird die Erhebung zu den Personalverhältnissen der Gesundheitsämter auf der Grundlage des Runderlasses des Innenministers vom 28. April 1964 (MBl. NW. S. 748) durchgeführt. Über die Personalverhältnisse sollen danach zwei Vordrucke (A und B) Auskunft geben. Der Vordruck B, der mir zur datenschutzrechtlichen Überprüfung vorgelegt wurde, soll der Übersicht über die Person, die Ausbildung und den beruflichen Werdegang des einzelnen Arztes dienen. Beide Vordrucke sollen von den Beschäftigungsbehörden ausgefüllt werden. Eine Erhebung bei den Betroffenen selbst ist nicht vorgesehen.

Der Minister für Arbeit, Gesundheit und Soziales ist der Auffassung, daß die Weitergabe der in den Vordrucken festgehaltenen Daten an aufsichtsberechtigte Stellen (Regierungspräsidenten und Minister für Arbeit, Gesundheit und Soziales) auf § 106 der Gemeindeordnung (GO) und § 46 der Kreisordnung (KrO) in Verbindung mit § 4 des Gesetzes über die Vereinheitlichung des Gesundheitswesens gestützt werden könne. Die Angaben in Vordruck B würden in der Hauptsache anonymisiert für statistische Zwecke verwendet. Im übrigen werde der Vordruck für personelle Maßnahmen benötigt, um zum Beispiel bei vorgesehener Bestellung eines Arztes zum Amtsarzt oder zum stellvertretenden Amtsarzt die medizinalaufsichtliche Prüfung vornehmen zu können. Die Daten über die Ausbildung, Weiterbildung und den beruflichen Werdegang sowie die Angabe von Privatanschrift und privater Telefonnummer seien erforderlich, um gegebenenfalls den geeigneten Arzt ausfindig zu machen. Die beiden zuletzt genannten Daten müßten auch bekannt sein, um nach Dienstschluß im Seuchen- oder Alarmfall den Arzt oder die Ärztin zu erreichen. Der Vordruck B werde nach dem Ausscheiden des Bediensteten aus dem Dienst beim Gesundheitsamt vernichtet.

Eine nach dem Grundrecht auf Datenschutz wie auch nach dem Recht auf informationelle Selbstbestimmung erforderliche gesetzliche Grundlage für die Erhebung der mit Vordruck B verlangten Daten bei den Betroffenen wie auch für die Weitergabe dieser Daten aus deren Personalakten ist nicht vorhanden. § 106 GO und § 46 KrO enthalten Bestimmungen zur allgemeinen Aufsicht und zur Sonderaufsicht über Kreise und Gemeinden. § 4 des Gesetzes über die Vereinheitlichung des Gesundheitswesens regelt die Aufsicht insbesondere über Gesundheitsämter als Dienststellen der Kreise und kreisfreien Städte. Die genannten Vorschriften können als gesetzliche Grundlage nicht in Betracht kommen, da sie auch nicht andeutungsweise erkennen lassen, daß personenbezogene Daten aller in Gesundheitsämtern beschäftigten Ärzte weitergegeben werden sollen.

Zweifelhaft ist im übrigen auch die Erforderlichkeit der Erhebung und Weitergabe der Daten für die genannten Zwecke. Bei vorgesehener Bestellung zum Amtsarzt können die Daten des Betroffenen im Einzelfall weitergegeben werden. Es ist zudem nicht erkennbar, warum der Regierungspräsident und der Minister für Arbeit, Gesundheit und Soziales im gegebenen Falle den geeigneten Arzt ausfindig machen müssen; es dürfte genügen, wenn die notwendigen Angaben beim Gesundheitsamt verfügbar sind. Eine Datenerhebung „auf Vorrat“, wie sie durch den Vordruck B vorgenommen wird, ist datenschutzrechtlich nicht zulässig.

Ich habe mich gegenüber dem Minister für Arbeit, Gesundheit und Soziales dafür eingesetzt, daß auf die Erhebung der mit dem Vordruck B von allen in Gesundheitsämtern beschäftigten Ärzten verlangten Angaben und deren

Weitergabe verzichtet wird. Das Ergebnis meiner Bemühungen bleibt abzuwarten.

#### **1) Datenweitergabe an nicht-öffentliche Stellen**

- Im Rahmen einer **Organisationsuntersuchung** bei den Stadtwerken einer Stadt wurden von der mit der Untersuchung beauftragten Wirtschaftsprüfungsgesellschaft bei den Bediensteten der Stadtwerke personenbezogene Angaben für eine Stellenbeschreibung erhoben.

Gegen die Erhebung bestehen erhebliche datenschutzrechtliche Bedenken, soweit von den Betroffenen Angaben zur Ableistung des Wehrdienstes und des Ersatzdienstes verlangt wurden. Außerdem erscheint zweifelhaft, ob es für die Organisationsuntersuchung erforderlich war, Namen, Vornamen, Geburtsdatum und Wohnort der Stelleninhaber an die Wirtschaftsprüfungsgesellschaft weiterzugeben.

Ich habe dem Stadtdirektor empfohlen, künftig in vergleichbaren Fällen von der Erhebung der Angaben zur Ableistung des Wehr- und des Ersatzdienstes sowie von der Weitergabe des Namens, Vornamens, Geburtsdatums und Wohnorts der Stelleninhaber an die Wirtschaftsprüfungsgesellschaft abzusehen. Der Stadtdirektor wird der Empfehlung folgen.

- Ein Volkshochschulzweckverband beabsichtigte, den Arbeitsplan für das nächste Semester mit einem **Dozentenverzeichnis** als Zeitungsbeilage an die Bürger im Verbandsgebiet zu verteilen. Das Dozentenverzeichnis sollte auch Angaben über Anschriften und Telefonnummern der Betroffenen enthalten. Den Betroffenen wurde die Möglichkeit eingeräumt, dieser Veröffentlichung zu widersprechen.

Die Zulässigkeit einer Übermittlung der genannten, in einer Datei gespeicherten Daten ist nach § 13 Abs. 1 Satz 1 DSGVO zu beurteilen. Nach der hier allein in Betracht kommenden 2. Alternative dieser Vorschrift ist die Übermittlung personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs nur 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.

Es kann dahinstehen, ob die Presse und die Leser der Zeitungsbeilage ein berechtigtes Interesse nicht nur an dem Arbeitsplan der Volkshochschule, sondern auch an dem Dozentenverzeichnis mit Angaben über die Anschrift und die Telefonnummer haben. Auf jeden Fall können durch die Bekanntgabe dieser Daten schutzwürdige Belange der Betroffenen beeinträchtigt werden. Zwar mögen manche der Betroffenen nichts daran auszusetzen haben, daß auf diese Weise von ihren personenbezogenen Daten Notiz genommen wird; andere hingegen werden die dadurch ermöglichte Kontaktaufnahme als Belästigung empfinden. Bei einer Abwägung der Interessen überwiegt in diesem Fall das Interesse der Betroffenen an dem Schutz ihrer Privatsphäre gegenüber dem Informationsinteresse der Empfänger der Zeitungsbeilage.

Da die Verletzung schutzwürdiger Belange der Betroffenen jedenfalls nicht auszuschließen ist, bedarf die Veröffentlichung des Dozentenverzeichnisses der Einwilligung der Betroffenen (§ 3 Satz 1 Nr. 2 DSGVO). Die den Betroffenen eingeräumte Möglichkeit, einer Veröffentlichung zu widersprechen, reicht nicht aus. Die Einwilligung ist grundsätzlich schriftlich zu erteilen, nachdem die Betroffenen über ihre Bedeutung aufgeklärt worden sind (§ 3 Satz 2 und 3 DSGVO).

- Ein städtischer Beamter hat sich dagegen gewandt, daß in einem Zeitungsartikel über einen Rechtsstreit, den er gegen die Stadt führte und der starke Beachtung in der Öffentlichkeit gefunden hat, berichtet worden sei, er sei

infolge dieses Rechtsstreits versetzt worden und habe mit seinem Widerspruch gegen die Versetzung sowie mit seinem Antrag auf Erlaß einer einstweiligen Anordnung keinen Erfolg gehabt. Ferner sei in dem Artikel mitgeteilt worden, der Beamte habe seinen neuen Posten noch nicht angetreten und sich krank gemeldet.

Nach Auskunft des Oberstadtdirektors sind die genannten Sachverhalte der **Presse** auf Befragen mitgeteilt oder bestätigt worden. Im übrigen habe der Beamte selbst durch verschiedene Verlautbarungen gegenüber Presseorganen dazu beigetragen, daß sein Name, Beruf und Arbeitgeber in diesem Zusammenhang bekannt wurden.

Die Mitteilung oder Bestätigung dieser Sachverhalte gegenüber der Presse ohne Einwilligung des Betroffenen ist ein Eingriff in dessen Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung wie auch in sein Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes. Ein derartiger Eingriff bedarf einer gesetzlichen Grundlage. Hierfür kommt nur § 4 Abs. 1 in Verbindung mit Abs. 2 Nr. 2 und 3 des Landespressegesetzes (LPG) in Betracht.

Nach § 4 Abs. 1 LPG sind die Behörden verpflichtet, den Vertretern der Presse die zur Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. Nach § 4 Abs. 2 LPG besteht ein Anspruch auf Auskunft jedoch nicht, soweit Vorschriften über die Geheimhaltung entgegenstehen (Nr. 2) oder ein schutzwürdiges privates Interesse verletzt würde (Nr. 3). Mit dieser Regelung wird die Bekanntgabe personenbezogener Informationen zwar nicht ausgeschlossen, aber Einschränkungen unterworfen (vgl. hierzu C.20.d meines sechsten Tätigkeitsberichts).

Danach sind die Bestätigung gegenüber der Presse, daß, wann und wohin der Betroffene versetzt wurde, sowie die Mitteilung, daß er mit seinem Widerspruch gegen die Umsetzung und seinem Antrag auf Erlaß einer einstweiligen Anordnung auf Rückversetzung zu seiner früheren Dienststelle keinen Erfolg gehabt, seinen Dienst aber noch nicht angetreten habe, datenschutzrechtlich nicht zu beanstanden.

Vorschriften über die Geheimhaltung standen der Bekanntgabe dieser Angaben nicht entgegen (§ 4 Abs. 2 Nr. 2 LPG). Die Angaben unterliegen keinem Berufs- oder besonderen Amtsgeheimnis. Zwar werden sie auch in den Personalakten festgehalten. Gleichwohl mußten sie nach meiner Auffassung nicht ihrem Wesen nach geheimgehalten werden. Dabei ist auch zu berücksichtigen, daß nach den Ausführungen des Oberstadtdirektors der Betroffene selbst durch Verlautbarungen gegenüber der Presse dazu beigetragen hatte, daß das Interesse der Öffentlichkeit auf seinen Rechtsstreit mit der Stadt gelenkt wurde und in diesem Zusammenhang sein Name, sein beruflicher Status und sein Arbeitgeber bekannt wurden. Der Einsatz eines Beamten des gehobenen Dienstes bei einer bestimmten Dienststelle einer Kommunalverwaltung kann auch unabhängig von den Umständen des vorliegenden Falles nicht schlechthin als geheimhaltungsbedürftig angesehen werden.

Durch die Bekanntgabe der genannten Angaben an die Presse wurde auch kein schutzwürdiges privates Interesse verletzt (§ 4 Abs. 2 Nr. 3 LPG). Im Hinblick auf das auch von dem Betroffenen geförderte Interesse der Öffentlichkeit an seinem Rechtsstreit mit der Stadt überwog das Informationsinteresse der Öffentlichkeit an dem weiteren Verlauf des Verfahrens gegenüber seinem Geheimhaltungsinteresse.

Anders ist jedoch die Bekanntgabe der Tatsache seiner Erkrankung an die Presse zu beurteilen.

Dieser Bekanntgabe standen Vorschriften über die Geheimhaltung entgegen

(§ 4 Abs. 2 Nr. 2 LPG), da die Verpflichtung zur Geheimhaltung dieser zu den Personalakten gehörenden Information (VV 2.3 zu § 102 LBG) einer Veröffentlichung entgegensteht. Auch die besonderen Umstände des vorliegenden Falles können insoweit eine Ausnahme nicht rechtfertigen.

Auf jeden Fall wurde aber durch die Bekanntgabe das schutzwürdige Interesse des Betroffenen an der Geheimhaltung verletzt (§ 4 Abs. 2 Nr. 3 LPG). Es kann dahinstehen, ob unter den gegebenen Umständen überhaupt ein Interesse der Öffentlichkeit an der Kenntnis der Tatsache der Erkrankung bestand. Jedenfalls überwog ein solches nach meiner Auffassung nicht gegenüber dem Geheimhaltungsinteresse des Betroffenen.

Da insoweit nach § 4 Abs. 2 Nr. 2 und 3 LPG ein Auskunftsanspruch der Presse nach § 4 Abs. 1 LPG nicht bestand, fehlte für die Bekanntgabe der Tatsache der Erkrankung an die Presse eine nach Artikel 4 Abs. 2 der Landesverfassung sowie nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes erforderliche gesetzliche Grundlage. Meiner Empfehlung, in vergleichbaren Fällen künftig von der Bekanntgabe derartiger Angaben an die Presse abzusehen, sofern nicht der Betroffene eingewilligt hat, wird der Oberstadtdirektor folgen.

- Bewerber um die Stelle des Leiters eines städtischen Kunstmuseums haben sich bei mir darüber beschwert, daß in einem Zeitungsartikel ihr Name und ihr bisheriger Arbeitgeber genannt wurden.

Der Oberstadtdirektor hat mir mitgeteilt, daß die Veröffentlichung der **Namen der Bewerber** um die Stelle des Leiters des Städtischen Kunstmuseums nicht auf eine Bekanntgabe der Daten der Bewerber durch die Stadt an die Presse zurückzuführen sei. Dafür wäre das Presseamt zuständig gewesen, dem wiederum die Namen der Bewerber nicht bekannt gewesen seien.

Mit den Bewerbungen sei nur der Personenkreis befaßt worden, zu dessen Aufgabenbereich die Personalentscheidung oder deren Vorbereitung gehört. Das Personalamt habe die Zusammenstellung der Daten der Bewerber dem Oberstadtdirektor, dem Kulturdezernenten und dem Personaldezernenten zugeleitet. Vom Büro des Oberstadtdirektors sei der Oberbürgermeister gemäß § 47 Abs. 2 GO über die Bewerbungen mit der gleichen Zusammenstellung unterrichtet worden; dieser habe zur Vorbereitung der vom Rat zu beschließenden Personalmaßnahme die Fraktionen informiert. Der Oberstadtdirektor hat weiter mitgeteilt, er müsse davon ausgehen, daß der mit der Angelegenheit befaßte Personenkreis seiner Geheimhaltungspflicht genügt habe.

Ich habe leider keine Möglichkeit, selbst festzustellen, welche Person die Daten der Presse bekanntgegeben hat. Zwar kann der Landesbeauftragte für den Datenschutz nach § 26 Abs. 3 DSG NW im Rahmen seiner Kontrollbefugnis von öffentlichen Stellen Auskunft zu Fragen sowie Einsicht in Unterlagen und Akten verlangen, die im Zusammenhang mit der Verarbeitung personenbezogener Daten stehen; er kann ferner die Stellen jederzeit auch unangemeldet aufsuchen und ihre Diensträume betreten. Der Landesbeauftragte für den Datenschutz hat jedoch nicht die Befugnis, Bedienstete öffentlicher Stellen, ehrenamtlich Tätige oder sonstige Personen zu vernehmen.

- Im Berichtszeitraum sind wieder Beschwerden von Lehramtsanwärtern eingegangen, denen vor Einstellung in den Vorbereitungsdienst von privaten **Versicherungsunternehmen** unaufgefordert Werbematerial mit unmittelbarem Bezug auf die bevorstehende Einstellung in den öffentlichen Dienst zugesandt worden ist.

Erfahrungsgemäß bringen Ermittlungen bei den an den Einstellungen beteiligten Stellen keine Hinweise darauf, daß von dort Anschriften der Betroffene-

nen an private Unternehmen weitergegeben wurden. Da zu vermuten ist, daß von bei diesen Stellen beschäftigten Personen gleichwohl personenbezogene Daten weitergegeben wurden, habe ich dem Kultusminister nochmals empfohlen, die mit Personaldaten von Lehramtsanwärtern befaßten Dienststellen seines Geschäftsbereichs eindringlich auf die Unzulässigkeit dieser Datenweitergabe hinzuweisen und sie anzuweisen, ihre mit solchen Daten befaßten Mitarbeiter hierüber zu belehren.

Der Kultusminister ist meiner Empfehlung mit Runderlaß vom 7. November 1985 gefolgt.

#### **k) Dienstaussweis**

Ein Gemeindebediensteter hat mich gebeten, die Erforderlichkeit der Angabe des Geburtstags, Geburtsortes, der Anschrift und des Wohnortes in seinem Dienstaussweis datenschutzrechtlich zu überprüfen. Er befürchtete, daß zumindest bei schwierigen dienstlichen Verrichtungen die Offenbarung der Privatschrift Auswirkungen auf den häuslichen Bereich haben könnte.

Der Innenminister hat mir auf Anfrage mitgeteilt, daß er meine Zweifel, ob alle genannten Angaben in einem Dienstaussweis erforderlich sind, teile. Er hat die Behörden seines Geschäftsbereichs angewiesen, die persönlichen Angaben in den Dienstaussweisen künftig auf Vor- und Zunamen, das Geburtsdatum und die Amts- bzw. Dienstbezeichnung zu beschränken.

## 14. Statistik

### **a) Volkszählung**

Nach eingehender Beratung hat der Deutsche Bundestag das Gesetz über eine Volks-, Berufs-, Gebäude-, Wohn- und Arbeitsstättenzählung (Volkszählungsgesetz 1987) beschlossen. Über die bereits im Gesetzentwurf der Bundesregierung vorgesehenen Vorkehrungen (vgl. C.11.a meines sechsten Tätigkeitsberichts) hinaus hat er in das Gesetz weitere Regelungen zur Sicherung des Datenschutzes aufgenommen:

- Verbot für die in den Erhebungsstellen eingesetzten Personen wie auch für die Zähler, die ihnen bekanntgewordenen Erkenntnisse aus ihrer Tätigkeit für andere Zwecke zu verwenden; Verpflichtung, auch die gelegentlich ihrer Tätigkeit gewonnenen Erkenntnisse geheimzuhalten;
- strafbewehrtes Verbot der Zusammenführung von Merkmalen zum Zweck der Reidentifizierung des Betroffenen;
- Verzicht auf die Angabe des Geburtsmonats.

Zwar sieht das Gesetz eine Übermittlung von Einzelangaben an die Gemeinden vor. Die Angaben dürfen jedoch ausschließlich für statistische Aufgaben verwendet werden. Hilfsmerkmale (wie Name und Anschrift) dürfen nicht übermittelt werden. Eine Übermittlung ist nur an die zur Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden zulässig. Voraussetzung für die Übermittlung ist, daß durch Landesgesetz eine Trennung dieser Stellen von anderen kommunalen Verwaltungsstellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist. Inwieweit diese Voraussetzungen bei den Gemeinden erfüllt werden, bleibt abzuwarten.

Insgesamt entsprechen die Regelungen den Forderungen der Datenschutzbeauftragten. Nicht berücksichtigt wurden lediglich die Bedenken gegen die vorgesehene, allerdings auf wenige Angaben beschränkte Pflicht zur mündlichen

Auskunft gegenüber dem Zähler. Die Verfassungsmäßigkeit der Volkszählung wird dadurch jedoch nicht berührt.

#### **b) Mikrozensus**

Das vom Bundestag nach eingehender Beratung beschlossene Gesetz zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensusgesetz) enthält gegenüber dem Gesetzentwurf der Bundesregierung (vgl. C.11.b meines sechsten Tätigkeitsberichts) einige weitere Regelungen zur Verbesserung des Datenschutzes:

- Pflicht der Interviewer, auch die gelegentlich der Interviewertätigkeit gewonnenen Erkenntnisse geheimzuhalten;
- strafbewehrtes Verbot der Zusammenführung von Daten zum Zweck der Reidentifizierung des Betroffenen;
- Einschränkung der (freiwilligen) Angaben zu Urlaubs- und Erholungsreisen sowie zur Gesundheit;
- Freiwilligkeit der Angabe des Eheschließungsjahres;
- Verzicht auf Angaben zur Vertriebenen- und Flüchtlingseigenschaft;

Demgegenüber wird an der im Gesetzentwurf vorgesehenen – wenn auch begrenzten – Auskunftspflicht gegenüber dem Interviewer festgehalten. Außerdem enthält das Gesetz weder eine nähere Regelung des Auswahlverfahrens noch die Pflicht zur Unterrichtung der Auskunftspflichtigen über das Auswahlverfahren.

Insgesamt entsprechen die Regelungen jedoch den Forderungen der Datenschutzbeauftragten. Auch wird die Übermittlung von Einzelangaben an andere Stellen nicht zugelassen. Aus der Sicht des Datenschutzes bestehen daher gegen die Durchführung des Mikrozensus auf der Grundlage dieses Gesetzes keine durchgreifenden Bedenken.

#### **c) Handels- und Gaststättenzählung**

- Die Handels- und Gaststättenzählung 1985 war die erste Bundesstatistik, die nach dem Urteil des Bundesverfassungsgerichts zur Volkszählung als Totalerhebung stattfand. Sie war deshalb ein aufschlußreiches Beispiel dafür, wie Zählungen auf Grund bestehender Gesetze durchgeführt werden, die den Grundsätzen des Bundesverfassungsgerichts zu statistischen Erhebungen nicht mehr entsprechen. Die Konferenz der Datenschutzbeauftragten von Bund und Ländern hat dazu festgestellt:
  1. Die Gewährleistung des Rechts auf informationelle Selbstbestimmung setzt nach Auffassung des Bundesverfassungsgerichts eine frühzeitige Beteiligung der Datenschutzbeauftragten im Sinne eines effektiven Rechtsschutzes voraus. Dies ist bei der Vorbereitung der Handels- und Gaststättenzählung nicht geschehen. Den Datenschutzbeauftragten der für die Durchführung zuständigen Länder wurden bis zum Beginn der Erhebung weder die Fragebogen noch die Verwaltungsvorschriften vorgelegt, die zur Sicherung der Rechte der Betroffenen in der Übergangszeit bis zur Anpassung des Handelsstatistikgesetzes an die Anforderungen des Grundgesetzes erforderlich sind.
  2. Die Datenschutzbeauftragten wie auch das Statistische Bundesamt sind gleichermaßen der Ansicht, daß das Handelsstatistikgesetz in Teilen nicht den Anforderungen des Volkszählungsurteils entspricht und daher dringend einer Novellierung bedarf.
  3. Für verschiedene in den Erhebungsbogen enthaltene Fragen (z. B. über

gewerblichen Umsatz, unternehmensinterne Dienstleistungen, Zweigniederlassungen, Auszeichnung der Waren mit Brutto- oder Nettopreisen) ist die gesetzliche Grundlage zumindest zweifelhaft. Die Hilfsmerkmale werden in dem Gesetz überhaupt nicht bestimmt. Ferner fehlen präzise gesetzliche Regelungen über die Trennung der Hilfsmerkmale von den Erhebungsmerkmalen und ihre Löschung.

4. Die Datenschutzbeauftragten fordern, daß Namen und Anschriften sowie die weiteren Hilfsmerkmale unverzüglich nach Abschluß der maschinellen Plausibilitätskontrolle, spätestens bis zum Ablauf einer zu bestimmenden, möglichst kurzen Frist von den Erhebungsbogen abgetrennt und vernichtet werden. Bis zur Änderung des Handelsstatistikgesetzes müssen die Verpflichtung zur unverzüglichen Trennung und Löschung sowie die Frist, innerhalb deren die Löschung abgeschlossen sein muß, durch die zuständigen obersten Landesbehörden festgelegt werden. Eine Aufbewahrung bis zum Abschluß der folgenden Handels- und Gaststättenzählung ist auf keinen Fall vertretbar.
5. Bis zu einer anderweitigen gesetzlichen Regelung dürfen die von den Finanzbehörden für die Durchführung der Zählung im Handwerk und im Gaststättengewerbe gelieferten und mit Hilfe der Angaben der Unternehmen und Arbeitsstätten korrigierten und ergänzten Adreßdateien nach Auffassung der Datenschutzbeauftragten nur für Zählungen nach dem Handelsstatistikgesetz, nicht aber für andere statistische Zwecke verwendet werden.

Im übrigen vertreten die Datenschutzbeauftragten mit Nachdruck die Auffassung, daß die von dem Bundesverfassungsgericht in dem Volkszählungsurteil dargelegten Grundsätze nicht nur auf Bevölkerungsstatistiken, sondern auch auf Wirtschaftsstatistiken wie die Handels- und Gaststättenzählung anzuwenden sind. Soweit bei Wirtschaftsstatistiken Daten natürlicher Personen erhoben werden, haben die Betroffenen Anspruch auf den gleichen Schutz wie bei Bevölkerungsstatistiken.

- Erwartungsgemäß haben mich zahlreiche Betroffene gebeten, die **Durchführung** der Handels- und Gaststättenzählung 1985 durch das Landesamt für Datenverarbeitung und Statistik (LDS) datenschutzrechtlich zu überprüfen.

Nach den Ausführungen des Bundesverfassungsgerichts in seinem Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 muß davon ausgegangen werden, daß die Handels- und Gaststättenzählung im überwiegenden Allgemeininteresse liegt. Es werden nur Daten mit Sozialbezug (zu denen auch Angaben über Einkommensverhältnisse gehören), jedoch keine unzumutbar intimen Angaben erhoben und auch keine Selbstbezeichnungen verlangt. Bei der Durchführung der Handels- und Gaststättenzählung 1985 hat sich jedoch gezeigt, daß das Handelsstatistikgesetz in Teilen nicht den Anforderungen des genannten Urteils entspricht und daher dringend einer Novellierung bedarf.

Dementsprechend habe ich den Innenminister des Landes Nordrhein-Westfalen gebeten, sich mit Nachdruck für eine baldige Anpassung des Handelsstatistikgesetzes an die Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts einzusetzen. Für eine Übergangszeit bis zur Änderung des Handelsstatistikgesetzes habe ich empfohlen, das LDS anzuweisen, die Deckblätter mit den Hilfsangaben unverzüglich nach Abschluß der maschinellen Plausibilitätskontrolle von den Erhebungsbogen abzutrennen und zu vernichten sowie eine möglichst kurze Frist zu bestimmen, innerhalb deren die Vernichtung abgeschlossen sein muß.

Der Innenminister teilt die Auffassung, daß das Handelsstatistikgesetz in einigen Punkten nicht den Anforderungen des Volkszählungsurteils des

Bundesverfassungsgerichts entspricht. Diesem Umstand sei jedoch dadurch Rechnung getragen worden, daß das Erhebungsprogramm nach Absprache zwischen dem Bundeswirtschaftsminister, dem Statistischen Bundesamt, den Statistischen Landesämtern und den Verbänden der Wirtschaft auf die im Gesetz unmittelbar genannten bzw. zur Kennzeichnung der Unternehmen/Arbeitsstätten erforderlichen Merkmale reduziert worden sei. Darüber hinaus sei der Forderung nach Trennung von Namen und Anschrift nach Abschluß der maschinellen Plausibilitätskontrolle durch entsprechende Anweisungen in den Statistischen Landesämtern entsprochen worden. Der Erhebungsbogen sei so gestaltet, daß Namen, Anschrift und alle weiteren Hilfsmerkmale auf dem Deckblatt abtrennbar enthalten sind. Nach Abschluß der Plausibilitätskontrolle werde der Anschriftenteil vom Datenteil getrennt und umgehend vernichtet.

Hierzu habe ich den Innenminister darauf hingewiesen, daß es nach dem Beschluß der Datenschutzbeauftragten des Bundes und der Länder geboten ist, bis zur Änderung des Handelsstatistikgesetzes die Verpflichtung zur unverzüglichen Trennung der Hilfsmerkmale von den Erhebungsbogen und zu ihrer Löschung sowie die Frist, innerhalb deren die Löschung abgeschlossen sein muß, durch die obersten Landesbehörden festzulegen. Wenn der weitere Vollzug des in Teilen nicht den Grundsätzen des Volkszählungsurteils entsprechenden Handelsstatistikgesetzes für eine Übergangszeit bis zur Anpassung dieses Gesetzes an die Anforderungen des Grundgesetzes hingenommen werden soll, so müssen die obersten Landesbehörden für den Bürger erkennbar sicherstellen, daß die Rechte der Betroffenen in dieser Übergangszeit gewahrt sind. Interne Anweisungen in den Statistischen Landesämtern reichen nicht aus. Ich habe deshalb eine Weisung des Innenministers an das LDS (etwa wie in Nr. 4.3 des Runderlasses vom 25. März 1983 zur Volkszählung 1983) empfohlen.

Eine Weisung des Innenministers ist auch deswegen geboten, weil in dem Anschreiben des LDS an die Auskunftspflichtigen vom März 1985 darauf hingewiesen wurde, daß die Trennung der beiden Fragebogenteile nach Abschluß der Aufbereitungsarbeiten erfolgt und beide Fragebogenteile spätestens nach Abschluß der folgenden Handels- und Gaststättenzählung vernichtet werden. Daraus müssen die Betroffenen den Schluß ziehen, daß der Anschriftenteil nicht unmittelbar nach Abschluß der Aufbereitungsarbeiten, sondern erst später, unter Umständen erst nach Abschluß der nächsten Handels- und Gaststättenzählung vernichtet wird. Eine derartige Aufbewahrungsdauer ist auf keinen Fall vertretbar.

- Mehrere Eingaben betrafen die Rechtmäßigkeit der **Erhebung des Umsatzes** im Rahmen der Handels- und Gaststättenzählung.

Gesetzliche Grundlage für die Erhebung des Umsatzes bei Einzelhandelsunternehmen ist § 6 Abs. 1 Nr. 1 Buchst. c und d des Handelsstatistikgesetzes. Danach wird in den Zählungen im Handel und Gastgewerbe bei Unternehmen des Einzelhandels der Umsatz nach Art der ausgeübten wirtschaftlichen Tätigkeiten sowie der Umsatz nach Warengruppen erfaßt. Mit dieser gesetzlichen Regelung muß der Inhalt des Fragebogens übereinstimmen. Die einzelnen Fragen dürfen nicht weiter gehen, als die im Gesetz festgelegten Erhebungsmerkmale.

Soweit Angaben über handelsfremden Umsatz verlangt werden, sowie für die Frage nach der Auszeichnung der Waren mit Brutto- oder Nettopreisen und für die Frage nach Zweigniederlassungen und deren Anzahl ist eine gesetzliche Grundlage nach meiner Auffassung nicht vorhanden.

Ich habe dem LDS unter Hinweis auf meine Rechtsauffassung empfohlen,

bei Nichtbeantwortung dieser Fragen von der Durchführung von Verwaltungszwangs- oder Bußgeldverfahren abzusehen.

- Im Zusammenhang mit der Handels- und Gaststättenzählung 1985 haben die Finanzbehörden den mit der Durchführung der Zählungen im Handel und im Gastgewerbe betrauten statistischen Behörden auch die **Steuernummer** der auskunftspflichtigen Unternehmen weitergegeben.

Eine den Anforderungen des Volkszählungsurteils genügende Rechtsvorschrift, die im Zusammenhang mit der Durchführung des Gesetzes über die Statistik im Handel und Gastgewerbe die Weitergabe und Speicherung der Steuernummer der auskunftspflichtigen Unternehmen vorsieht, ist nicht ersichtlich. § 6 Abs. 2 des Handelsstatistikgesetzes bestimmt lediglich, daß die Finanzbehörden den mit der Durchführung der Zählungen im Handel und im Gastgewerbe betrauten statistischen Behörden die Anschriften und Gewerbekennziffern aller Unternehmen des Handels und des Gastgewerbes mitteilen. Eine darüber hinausgehende Weitergabe von Daten durch die Finanzbehörden ist nicht vorgesehen und daher datenschutzrechtlich unzulässig.

Zur Vermeidung von Verstößen gegen Vorschriften über den Datenschutz habe ich dem Finanzminister empfohlen, die seiner Aufsicht unterliegenden Finanzbehörden anzuweisen, im Zusammenhang mit der Durchführung der Handels- und Gaststättenzählung davon abzusehen, die Steuernummer der auskunftspflichtigen Unternehmen weiterzugeben. Der Finanzminister hat mir hierzu mitgeteilt, daß er den Umfang der weiterzugebenden Daten vor der nächsten Handels- und Gaststättenzählung mit mir abstimmen wird, sofern nicht bis dahin eine ausdrückliche gesetzliche Grundlage für die Verwendung und Weitergabe von Hilfsmerkmalen geschaffen worden ist.

#### d) Hochschulstatistik

- Mehrere Studenten haben gebeten, den Vordruck für die Erhebung personenbezogener Daten bei **Prüfungskandidaten** nach dem Hochschulstatistikgesetz datenschutzrechtlich zu überprüfen. Sie wandten sich ferner dagegen, daß die Ausstellung des Prüfungsergebnisses von der ordnungsgemäßen Ausfüllung des Erhebungsbogens abhängig gemacht wurde.

Gesetzliche Grundlage für die Erhebung personenbezogener Daten bei Prüfungskandidaten an Hochschulen ist § 9 Abs. 1 des Hochschulstatistikgesetzes (HStatG). Danach werden bei den Prüfungskandidaten folgende Tatbestände erhoben: Angaben zur Person, Staatsangehörigkeit, Wohnsitze, Studienverlauf, Art und Fachrichtung der abzulegenden Prüfung.

Ich habe Zweifel, ob sämtliche im Erhebungsbogen vorgesehenen Daten als „Angaben zur Person“ erforderlich sind. Die Erhebung zur Identifizierung bestimmter Angaben wäre nur dann erforderlich, wenn sie der Durchführung einer Verlaufsstatistik dienen soll. Bei anderen durch das Hochschulstatistikgesetz vorgesehenen Erhebungen, zum Beispiel bei Studenten, ist dies auch ausdrücklich gesetzlich vorgesehen. § 9 HStatG enthält eine solche Regelung nicht. Soweit die Rechtsgrundlage eine Verlaufsstatistik nicht nennt, ist davon auszugehen, daß der Gesetzgeber die Erhebung einer Bestandsstatistik für ausreichend erachtet hat. Für diese sind zumindest die Angaben zu Namen, Geburtsort und Familienstand nicht erforderlich. Auch für die Erhebung der Matrikelnummer fehlt die Rechtsgrundlage. Des weiteren gehören meines Erachtens die erhobenen Daten über die Berechtigung zum Hochschulstudium ebenfalls nicht zu den in § 9 Abs. 1 HStatG vorgesehenen Erhebungstatbeständen. § 9 Abs. 1 HStatG nennt lediglich den Erhebungstatbestand „Studienverlauf“.

Nach § 13 Abs. 1 Nr. 4 HStatG sind die Prüfungskandidaten für diese Erhe-

bung auskunftspflichtig. Hinsichtlich der allein für die Bundesstatistik bestimmten Angaben darf die Auskunftspflicht nur mit den nach dem Bundesstatistikgesetz zulässigen Mitteln durchgesetzt werden. Ein solches Mittel ist die Verweigerung des Prüfungszeugnisses nicht.

- Der inzwischen vorliegende Referentenentwurf für eine **Novellierung** des Hochschulstatistikgesetzes sieht neben einer erheblichen Einschränkung des Erhebungsprogramms vor, daß die Hochschulstatistik, allerdings mit Ausnahme der Statistik der Prüfungskandidaten, in ihren Erhebungsbereichen nur bei den Hochschulen und deren Einrichtungen auf Grund vorhandener Verwaltungsdatenbestände ohne Namen und Anschrift als Bestandsstatistik durchgeführt werden soll. Ich gehe davon aus, daß auch die Statistik der Prüfungskandidaten nicht personenbezogen erhoben werden muß. Die Datenschutzbeauftragten des Bundes und der Länder treten dafür ein, daß in der Hochschulstatistik in ihrer Gesamtheit auf die Erhebung unmittelbar beim Betroffenen verzichtet wird.

Demgegenüber hat die Ständige Konferenz der Kultusminister die Aufnahme einer Studienverlaufsstatistik gefordert. Der Bundesminister des Innern hat in einer Stellungnahme dazu überzeugend dargelegt, daß eine Studienverlaufsstatistik wegen mangelnder Eignung und Erforderlichkeit sowie wegen unzumutbarer Belastung der Betroffenen unverhältnismäßig und daher verfassungswidrig wäre. Diese Auffassung wird von mir geteilt. Ich habe daher dem Minister für Wissenschaft und Forschung empfohlen, die Absicht, in dem neuen Hochschulstatistikgesetz eine Studienverlaufsstatistik vorzusehen, nicht weiter zu verfolgen.

#### e) Kommunalstatistik

Auf Wunsch des Ausschusses für Innere Verwaltung des Landtags habe ich zu den Auswirkungen des Volkszählungsurteils des Bundesverfassungsgerichts auf die Kommunalstatistik Stellung genommen (Vorlage 10/132).

Die in dem genannten Urteil dargelegten Anforderungen an statistische Erhebungen gelten auch für die Kommunalstatistik sowie für die Beteiligung der Gemeinden bei der Durchführung von Bundes- und Landesstatistiken. Inwieweit hier für den Landesgesetzgeber ein Regelungsbedarf besteht, ist je nach der Art der statistischen Erhebung unterschiedlich zu beurteilen:

1. Soweit die Gemeinden **eigene statistische Erhebungen** durchführen wollen, ist hierfür eine hinreichend normenklare und den Verhältnismäßigkeitsgrundsatz beachtende gesetzliche Grundlage erforderlich. Eine allein auf Grund der Ermächtigung in § 4 Abs. 1 Satz 1 der Gemeindeordnung erlassene Satzung würde nach meiner Auffassung hierfür nicht ausreichen. Nach dem Gebot der Normenklarheit müßte der Landesgesetzgeber die Gemeinden zu statistischen Erhebungen ausdrücklich ermächtigen und Vorgaben für die notwendigen organisatorischen und verfahrensrechtlichen Vorkehrungen machen. Dies gilt jedenfalls für Erhebungen mit Auskunftspflicht, nach meiner Auffassung aber auch für solche auf freiwilliger Grundlage und für die statistische Auswertung von Verwaltungsdaten.

Nach dem Verhältnismäßigkeitsgrundsatz hat der Landesgesetzgeber zu prüfen, ob und inwieweit die Durchführung eigener statistischer Erhebungen zur Erfüllung der Aufgaben der Gemeinden geeignet und erforderlich ist sowie ob und inwieweit die Belastung der Betroffenen in einem angemessenen Verhältnis zu dem zu erreichenden Zweck steht (Zumutbarkeit).

Dabei wird zu berücksichtigen sein, daß sich der Gesetzgeber nach dem Volkszählungsurteil vor jeder Entscheidung für statistische Erhebungen erneut mit dem Stand der Methodendiskussion auseinandersetzen muß, um

festzustellen, ob alternative Methoden zur Totalerhebung und zum Auskunftszwang in Betracht kommen. Dies könnte den Gesetzgeber veranlassen, entweder auf eine Auskunftspflicht in der Kommunalstatistik zu verzichten oder aber (anders als bei der Regelung für die Bundesstatistik) vorzusehen, daß Erhebungen der Kommunalstatistik auf freiwilliger Grundlage durchgeführt werden, soweit nicht die Auskunftspflicht für die einzelne Erhebung ausdrücklich bestimmt ist.

Entscheidet sich der Gesetzgeber für eine Ermächtigung an die Gemeinden, so muß im Gesetz vorgeschrieben werden, daß die Durchführung einer Statistik der Anordnung durch Satzung bedarf. Die Satzung muß den gleichen Anforderungen entsprechen wie ein Gesetz, durch das eine Bundes- oder Landesstatistik angeordnet wird; sie muß die Erhebungsmerkmale, die Art der Erhebung, die Berichtszeit und den Kreis der zu Befragenden bestimmen.

Bei einer Entscheidung des Gesetzgebers für statistische Erhebungen der Gemeinden müssen den Gemeinden auch die organisatorischen und verfahrensrechtlichen Vorkehrungen durch den Gesetzgeber vorgegeben werden. Das Bundesverfassungsgericht fordert im Volkszählungsurteil:

- Aufklärungs- und Belehrungspflichten über die Art und Weise der Erhebung, insbesondere darüber, inwieweit die Angaben freiwillig sind oder eine Auskunftspflicht besteht, und darüber, welche Merkmale lediglich Hilfsmittel für die Durchführung der Erhebung sind;
- Löschung der zur Identifizierung dienenden Merkmale (insbesondere Namen und Anschriften) zum frühestmöglichen Zeitpunkt; bis dahin Aufbewahrung unter Verschuß getrennt von den übrigen Merkmalen;
- Maßnahme zur Vermeidung von Interessenkollisionen bei den Zählern; Recht des Bürgers, den ausgefüllten Erhebungsbogen unmittelbar der Zahldienststelle zuzuleiten;
- strikte Geheimhaltung der erhobenen Einzelangaben (auch schon während des Erhebungsverfahrens), solange ein Personenbezug noch besteht oder herstellbar ist;
- frühzeitige Anonymisierung; Vorkehrungen gegen eine Deanonymisierung;
- Trennung der Kommunalstatistik von anderen Aufgabenbereichen der Gemeinden („informationelle Gewaltenteilung“). Danach muß eine Vermengung von Statistik und Planung beim statistischen Amt der Gemeinde ausgeschlossen werden. Ihm dürfen neben der Durchführung der Statistik keine Verwaltungsaufgaben übertragen werden. Eine gewisse personelle Kontinuität ist erforderlich. Zwar kann kein absolutes Umsetzungsverbot verlangt werden. Die Fluktuation muß jedoch in Grenzen gehalten werden. Dies schließt kleinere Gemeinden von der Durchführung eigener statistischer Erhebungen aus.

Inwieweit diese Anforderungen in einer kommunalen Satzung konkretisiert werden müssen, hängt von der Regelungstiefe im Gesetz ab.

2. Nach § 14 Abs. 1 Satz 1 und 2 des Volkszählungsgesetzes 1987 (VZG) dürfen den zur Durchführung statistischer Aufgaben zuständigen Stellen der Gemeinden und Gemeindeverbänden für ausschließlich statistische Aufgaben **Einzelangaben der Volkszählung** ohne Hilfsmerkmale (insbesondere Namen und Anschriften), aber auf der Grundlage von Blockseiten (Straßenseite zwischen zwei Einmündungen) zur kleinräumigen Auswertung übermittelt werden. Diese Übermittlung ist nur zulässig, wenn durch Landesgesetz eine Trennung dieser Stellen von anderen kommunalen Verwaltungs-

stellen sichergestellt und das Statistikgeheimnis durch Organisation und Verfahren gewährleistet ist (§ 14 Abs. 1 Satz 3 VZG).

Soll von dieser Übermittlungsbefugnis Gebrauch gemacht werden, so muß zuvor der Landesgesetzgeber entsprechende Regelungen treffen. Diese müssen den oben genannten Forderungen des Bundesverfassungsgerichts Rechnung tragen.

Entsprechendes muß für eine Verwendung von Einzelangaben aus anderen Erhebungen der Bundes- oder Landesstatistik für Aufgaben der Kommunalstatistik gelten.

3. Nach § 9 Abs. 1 VZG werden zur **Durchführung der Volkszählung** Erhebungsstellen eingerichtet. Sie sind räumlich, organisatorisch und personell von anderen Verwaltungsstellen zu trennen. Es ist sicherzustellen, daß die Angaben in den Erhebungsvordrucken nicht für andere Aufgaben verwendet werden.

Nach § 9 Abs. 3 VZG obliegt die Bestimmung der Erhebungsstellen und das Nähere zur Ausführung des § 9 Abs. 1 VZG den Ländern. Sie können die Aufgaben der Erhebungsstellen auf die Gemeinden und Gemeindeverbände übertragen. Die Regelungen können durch Rechtsverordnung der Landesregierungen getroffen werden.

Sofern in Nordrhein-Westfalen wie bei der letzten Volkszählung die Gemeinden als Erhebungsstellen bestimmt werden, besteht hiernach eine Verpflichtung des Landes zur Konkretisierung des Trennungsgebots und der Sicherung der statistischen Zweckbindung. Ein Tätigwerden des Gesetzgebers ist hierzu nicht erforderlich; eine Rechtsverordnung der Landesregierung genügt.

## 15. Wissenschaft und Forschung

### a) Hochschulen

- Mehrere Studierende einer Universität haben sich dagegen gewandt, daß die von der Universität für das Sommersemester 1985 ausgegebenen **Studienbescheinigungen und Studentenausweise** außer der Angabe der Immatrikulation erstmalig auch Angaben enthalten über das Semester, in dem das Studium an der Universität aufgenommen wurde, über die Anzahl der Semester sowie über das Studienfach und die angestrebte Abschlußprüfung. Sie sähen nicht ein, daß auf diese Weise eine Vielzahl von Personen erfahre, im wievielten Semester sie bestimmte Fächer studierten.

Ich halte diese Bedenken für berechtigt. Zwar läßt sich ein Anspruch auf Erteilung eines Studentenausweises oder einer Studienbescheinigung, die die erwähnten Daten nicht enthält, nicht unmittelbar aus dem Datenschutzgesetz Nordrhein-Westfalen herleiten. Denn eine Übermittlung im Sinne dieses Gesetzes findet nicht statt, da der Ausweis und die Studienbescheinigung nicht einem Dritten, sondern dem Betroffenen selbst ausgehändigt werden (§ 2 Abs. 2 Nr. 2, Abs. 3 Nr. 2 DSG NW). Da der Betroffene jedoch in seiner Entscheidung, ob er von dem Studentenausweis oder der Studienbescheinigung Gebrauch macht und dadurch selbst die darin enthaltenen Daten offenbart, oft einem Zwang unterliegt, kann nach meiner Auffassung aus dem Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung die Verpflichtung der Universität hergeleitet werden, in den Ausweis oder die Studienbescheinigung nur solche Daten aufzunehmen, die für den Verwendungszweck dieser Unterlagen erforderlich sind.

Nach meiner Auffassung sollten daher die Hochschulen das Verfahren zur Ausgabe von Studentenausweisen und Studienbescheinigungen so organisieren, daß für die Studierenden die Möglichkeit besteht, einen Studentenausweis oder eine Studienbescheinigung ohne die genannten Angaben zu erhalten. Bei einer maschinellen Erstellung der Studienbescheinigungen bietet sich ein Verfahren an, bei dem bestimmte Teile der Bescheinigung vom Hauptteil abgetrennt werden können. Die Studierenden haben dann die Möglichkeit, die Angaben über das Studienfach, die Fachsemester und die angestrebte Abschlußprüfung sowie die Anzahl der Hochschulsemester vom Hauptteil der Bescheinigung abzutrennen.

Die Universität wird auf meine Einwendungen in Kürze mit der Einführung eines neuen Verfahrens für die Studentenverwaltung Studentenausweise ohne die von dem Betroffenen beanstandeten zusätzlichen Angaben ausgeben.

In die Studienbescheinigungen will die Universität dagegen weiterhin die Angaben über den Studiengang aufnehmen. Die Abtrennung von einzelnen Teilen der Bescheinigung hält sie für problematisch. Sie meint, eine mißbräuchliche Verwendung der einzelnen – jeweils unvollständigen – Bescheinigungsteile sei nicht auszuschließen. Auch könne eine gekürzte Bescheinigung bei Stellen, denen solche Bescheinigungen üblicherweise vorgelegt werden und die künftig gleichermaßen gekürzte wie ungekürzte Bescheinigungen erhielten, den Eindruck erwecken, daß der Studierende ihm mißliebig erscheinende Einträge verschweigen möchte, auch wenn dies gar nicht der Fall sei.

Die Hochschule hat sich jedoch bereit erklärt, im Einzelfall auf Wunsch den Studierenden eine auf herkömmliche Weise erstellte Studienbescheinigung auszuhändigen, die sich auf die Bestätigung der ordnungsgemäßen Einschreibung für das jeweilige Semester beschränkt. Solange mir nicht weitere Beschwerden bekannt werden, gehe ich mit davon aus, daß durch dieses Verfahren die Datenschutzbelange der Betroffenen gewahrt sind.

- Hauptamtliche wissenschaftliche Mitarbeiter von Universitäten haben mir mitgeteilt, sie hätten ein Schreiben der Personalverwaltung der Hochschule erhalten, in dem sie aufgefordert wurden, zu dem Umstand Stellung zu nehmen, daß sie noch für ein Studium an dieser Hochschule immatrikuliert seien. Sie äußerten die Vermutung, daß die Hochschule durch einen **Datenabgleich** zwischen der Personaldatei und der Studentendatei die Tatsache ihrer Immatrikulation in Erfahrung gebracht habe, und baten um datenschutzrechtliche Prüfung.

Zwei Hochschulen haben auf meine Anfrage bestätigt, daß ein solcher Datenabgleich stattgefunden hat. Anlässlich einer Prüfung durch den Landesrechnungshof habe dieser bei der Hochschule festgestellt, daß eine Reihe hauptberuflich an der Hochschule Beschäftigter neben ihrer Tätigkeit als ordentliche Studierende eingeschrieben waren. Gleichzeitig habe der Rechnungshof durch Einsichtnahme in Personalakten festgestellt, daß der Hochschulverwaltung die Aufnahme des Studiums nicht immer angezeigt worden war und demzufolge keine aktenkundigen Prüfungen vorgenommen worden sind, ob durch das Studium dienstliche Belange beeinträchtigt wurden. Der Rechnungshof habe gebeten, in allen Fällen zu prüfen, ob durch das Studium die ordnungsgemäße Erledigung der den Landesbediensteten übertragenen Dienstgeschäfte beeinträchtigt werde, die Ergebnisse aktenkundig zu machen und gegebenenfalls das Erforderliche zu veranlassen.

Zur rechtlichen Bewertung haben die Hochschulen die Auffassung vertreten, der Datenabgleich sei zu ihrer rechtmäßigen Aufgabenerfüllung nach § 11

Abs. 1 Satz 1 DSG NW zulässig gewesen. Dem vermag ich jedoch nicht zu folgen.

Die Weitergabe von Daten aus der Studentendatei an die Personalstelle der Universität ist ein Eingriff in das Grundrecht der Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung sowie in ihr Recht auf informationelle Selbstbestimmung. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen muß; aus ihr müssen sich Voraussetzungen und Umfang der Einschränkung des Grundrechts klar und für den Bürger erkennbar ergeben. Außerdem muß der Verhältnismäßigkeitsgrundsatz gewahrt werden.

Im vorliegenden Fall kommen als gesetzliche Grundlage für den Datenabgleich § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSG NW in Betracht. Nach diesen Vorschriften ist eine Datenweitergabe innerhalb der Hochschule zulässig, wenn sie zur rechtmäßigen Aufgabenerfüllung der abgebenden Stelle oder des Datenempfängers erforderlich ist. Es ist indes zweifelhaft, ob und gegebenenfalls inwieweit die Generalklauseln der Datenschutzgesetze als gesetzliche Grundlage für einen Informationseingriff noch herangezogen werden können. Dies gilt insbesondere für Übermittlungsvorschriften, die – wie die 2. Alternative des § 11 Abs. 1 Satz 1 DSG NW – an die rechtmäßige Aufgabenerfüllung des Empfängers anknüpfen, da sie den Verwendungszweck der Daten bei dem Empfänger nicht bestimmen und deshalb den Umfang des Eingriffs für den Bürger nicht erkennen lassen.

Nach meiner Auffassung können nur bei weniger schwerwiegenden Einschränkungen des Rechts auf informationelle Selbstbestimmung auch künftig als Generalklauseln ausgestaltete Auffangnormen in den Datenschutzgesetzen ausreichen. Dies gilt für Übermittlungen etwa dann, wenn die Daten von dem Empfänger für den gleichen Zweck benötigt werden, für den sie von der übermittelnden Stelle erhoben wurden oder gespeichert sind, oder wenn sie nicht personenbezogen verwendet werden sollen. Bei einer stärkeren Belastung des Betroffenen kann eine Datenübermittlung jedoch nur noch dann als zulässig angesehen werden, wenn dafür eine bereichsspezifische gesetzliche Grundlage vorhanden ist. Dies gilt etwa dann, wenn die Daten von dem Empfänger personenbezogen für einen anderen Zweck verwendet werden sollen, insbesondere wenn sie für Maßnahmen bestimmt sind, die den Betroffenen belasten.

In den an mich herangetragenen Fällen waren die Daten für eine Überprüfung bestimmt, ob durch die Aufnahme des Studiums etwa dienstliche Belange beeinträchtigt werden. Ein derartiger Vorgang stellt sich für die Betroffenen als Belastung dar. Hierbei muß außer Betracht bleiben, daß die Betroffenen nach § 57 Satz 1 des Landesbeamtengesetzes bzw. den entsprechenden Vorschriften des Bundes-Angestellten-Tarifvertrages verpflichtet sind, sich mit voller Hingabe ihrem Beruf zu widmen.

Die durch den Datenabgleich erfolgte Weitergabe der Studentendaten an die Personalstelle kann daher nicht auf § 8 Satz 1 in Verbindung mit § 11 Abs. 1 DSG NW gestützt werden. Da eine bereichsspezifische gesetzliche Grundlage für die Weitergabe dieser Daten nicht gegeben ist, war diese nicht zulässig.

Auf einem „Übergangsbonus“ bis zur Schaffung einer erforderlichen bereichsspezifischen gesetzlichen Grundlage könnte eine derartige Datenweitergabe nach der Rechtsprechung des Bundesverfassungsgerichts nur gestützt werden, wenn eine bisher schon geübte Verwaltungspraxis fortgesetzt werden soll, um eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen zu vermeiden, die der verfassungsmäßigen Ordnung noch

ferner stünde als der bisherige Zustand (BVerfGE 33, 12, 347; 41, 267). Diese Voraussetzung liegt hier nicht vor.

- Die Frage, inwieweit die Generalklauseln des Datenschutzgesetzes Nordrhein-Westfalen eine Rechtsgrundlage für den in der Übermittlung der Daten liegenden Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen noch sein können, stellte sich auch bei der Beurteilung der Anfrage des Rektors einer Fachhochschule. Dieser hatte mich um Stellungnahme gebeten, ob er das endgültige **Nichtbestehen einer Fachprüfung** durch einen an der Fachhochschule eingeschriebenen Zweithörer der anderen Hochschule, bei der der Studierende als Ersthörer eingeschrieben sei, mitteilen dürfe.

Es kann dabei davon ausgegangen werden, daß die Hochschule, bei der der Studierende als Ersthörer eingeschrieben ist, die Kenntnis der Tatsache des endgültigen Bestehens einer bestimmten Prüfung an der anderen Hochschule zur Erfüllung ihrer rechtmäßigen Aufgaben benötigt. Denn nach den Prüfungsordnungen ist die Zulassung zu einer Prüfung in der Regel nicht möglich, wenn der Kandidat entsprechende Prüfungen an anderen Hochschulen endgültig nicht bestanden hat.

Gleichwohl liegt in der Bekanntgabe des endgültigen Nichtbestehens der Prüfung an die andere Hochschule eine unzulässige Zweckentfremdung, die nach meiner Auffassung nicht auf § 11 Abs. 1 Satz 1 DSGVO gestützt werden kann. Übermittlungsvorschriften, die an die rechtmäßige Aufgabenerfüllung des Empfängers anknüpfen, können keinen ausreichenden Schutz gegen Zweckentfremdung bieten, da sie den Verwendungszweck der Daten nicht bestimmen und insoweit nicht dem Gebot der Normenklarheit entsprechen. Ich habe daher den Minister für Wissenschaft und Forschung des Landes Nordrhein-Westfalen darauf hingewiesen, daß für derartige Datenübermittlungen in Zukunft eine bereichsspezifische hochschulrechtliche Grundlage geschaffen werden muß.

#### **b) Studienplatzvergabe**

- Die Frage der Datenerhebung für die Begleituntersuchung zum Test für medizinische Studiengänge, mit der ich mich in meinem dritten Tätigkeitsbericht eingehend befaßt habe (C.12.c) war im Berichtsjahr wiederum Gegenstand einer Eingabe. Der Betroffene hatte aus den ihm zugeleiteten Unterlagen nicht ersehen können, ob die Beantwortung der Fragen Voraussetzung für die Testteilnahme ist. Auch bei der Testabnahme hatte er auf seine Fragen hierzu keine klare Antwort bekommen.

Die Begleituntersuchung zum Test wird vom Institut für Test- und Begabungsforschung im Auftrag der Zentralstelle für die Vergabe von Studienplätzen (ZVS) durchgeführt. Durch die Begleituntersuchung soll unter anderem die Frage möglicher Bevorzugungen oder Benachteiligungen bestimmter Bewerbergruppen geprüft werden. Hierfür werden von dem Bewerber auch Angaben zur Schulbildung und Berufsposition der Eltern erhoben.

Die Datenerhebung für die Begleituntersuchung bedarf als Eingriff in das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung sowie in das informationelle Selbstbestimmungsrecht der Betroffenen einer gesetzlichen Grundlage oder aber ihrer Einwilligung. Für das Feststellungsverfahren 1985 war die erforderliche gesetzliche Grundlage für die Erhebung der mit dem Fragebogen zur Begleituntersuchung erhobenen Daten in dem durch § 1 des Gesetzes über den Staatsvertrag über die Vergabe von Studienplätzen in Landesrecht transformierten § 16 Abs. 5 des Staatsvertrages sowie in § 23 Abs. 4 der auf Grund dieses Gesetzes erlassenen Vergabeverordnung enthalten.

Demgegenüber sieht Artikel 14 Abs. 8 der von den Ministerpräsidenten unterzeichneten, aber noch nicht in Kraft getretenen Neufassung des Staatsvertrags vor, daß von den Teilnehmern am Feststellungsverfahren mit deren Einverständnis die für die laufende Auswertung des Feststellungsverfahrens erforderlichen Angaben über ihren Bildungsgang und ihre persönlichen und sozialen Verhältnisse erhoben werden können. Die Angaben sind zu anonymisieren und dürfen nur zum Zweck der laufenden Auswertung des Feststellungsverfahrens verwertet werden. Die in dem Entwurf des neuen Staatsvertrages vorgesehene Verpflichtung zur Angabe der Daten (vgl. C.13.c meines sechsten Tätigkeitsberichts) ist somit durch eine Datenerhebung auf freiwilliger Grundlage ersetzt worden.

Dementsprechend bestimmt § 40 Abs. 1 der Vergabeverordnung ZVS 1985, die erstmalig für den Testtermin im Februar 1986 zur Anwendung kommt, daß die Zentralstelle von den Teilnehmern des Feststellungsverfahrens mit deren Einverständnis zusätzliche persönliche Angaben erhebt. Die Zentralstelle stellt die erhobenen Angaben, die Ergebnisse des Feststellungsverfahrens und die ihr vom Institut für medizinische und pharmazeutische Prüfungsfragen und den zuständigen Prüfungsämtern mitgeteilten Prüfungsergebnisse der Teilnehmer des Feststellungsverfahrens zusammen und übermittelt sie in anonymisierter Form der von den Ländern mit der laufenden Auswertung des Feststellungsverfahrens betrauten Einrichtung. Die Angaben dürfen nur zum Zweck der laufenden Auswertung des Feststellungsverfahrens verwertet werden.

Werden Daten beim Betroffenen erhoben, so ist er nach § 10 Abs. 2 Satz 1 DSGVO auf die der Datenerhebung zugrunde liegende Rechtsvorschrift oder auf die Freiwilligkeit seiner Angaben hinzuweisen. Im Test-Info 1986 ist nunmehr bei den Hinweisen zur Ausfüllung des Anmeldeformulars, mit dem auch die Fragen des Instituts für Test- und Begabungsforschung beantwortet werden, ausgeführt, daß die Antworten zu den Fragen des Instituts freiwillig sind.

## 16. Bildung und Kultur

### a) Schulwesen

- Im Schulverhältnis werden bei zahlreichen Anlässen personenbezogene Daten von Schülern und Eltern durch die Schule oder die Schulverwaltung erhoben. Dies beginnt mit der Schulaufnahme, bei der mit den Anmeldeformularen personenbezogene Daten der Schüler und Eltern verlangt werden. Während der Dauer des Schulverhältnisses werden personenbezogene Daten zum Beispiel zum Zweck der Leistungsbewertungen erhoben. Darüber hinaus werden aus vielfältigen anderen Anlässen (wie etwa zum Zweck der Schülerbeförderung, der Arbeit von Schülervertretungen und Schülerzeitschriften) personenbezogene Daten in der Schule erfragt und festgehalten.

Der Kultusminister hat durch die Verwaltungsvorschriften (VVzASchO) zu § 5 Abs. 4 ASchO – Richtlinien zum Schülerstammbuch und zum sonstigen Datenbestand in der Schule –, bei deren Vorbereitung ich beteiligt war (vgl. dritter Tätigkeitsbericht, C.13.a, und vierter Tätigkeitsbericht, C.15.a), Einzelheiten für die Erhebung, Speicherung und Übermittlung personenbezogener Daten an den Schulen geregelt. Diese Richtlinien haben sich nach meinem Eindruck in der Praxis im wesentlichen bewährt. Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 ist jedoch für Eingriffe in das Recht der Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes

eine gesetzliche Grundlage erforderlich, die dem Gebot der Normenklarheit entsprechen muß; aus ihr müssen sich die Voraussetzungen und der Umfang der Einschränkung klar und für den Bürger erkennbar ergeben. Soweit in den Schulgesetzen Rechtsgrundlagen für die Datenerhebung und Datenverarbeitung an Schulen enthalten sind, entsprechen sie häufig nicht dieser Anforderung. Dies hat in den Ländern Saarland und Rheinland-Pfalz im Jahre 1985 bereits zu gesetzlichen Neuregelungen geführt.

Ich habe daher den Kultusminister des Landes Nordrhein-Westfalen darauf hingewiesen, daß auch in Nordrhein-Westfalen eine **gesetzliche Regelung der Erhebung und Verarbeitung von Schüler- und Elterndaten** in den Schulen und im Schulgesundheitswesen erforderlich ist. Der Kultusminister hat mir hierzu mitgeteilt, er prüfe zur Zeit, welche konkreten gesetzgeberischen Konsequenzen aus dem Urteil des Bundesverfassungsgerichts für das Schulrecht des Landes Nordrhein-Westfalen zu ziehen sind. Die gesamte Problematik werde derzeit auch in den Gremien der Kultusministerkonferenz beraten.

Der Kultusminister hat eine grundlegende Überarbeitung der Schulgesetze während der derzeitigen Wahlperiode des Landtags in Aussicht gestellt. Ich gehe davon aus, daß im Zusammenhang damit die erforderliche gesetzliche Neuregelung der Erhebung und Verarbeitung von Schüler- und Elterndaten erfolgt.

- Von verschiedenen Gemeinden bin ich um Stellungnahme zu der Frage gebeten worden, welche Stelle für diejenigen in den Schulen geführten Dateien, die den sogenannten inneren Schulangelegenheiten zuzuordnen sind, als **speichernde Stelle** nach § 2 Abs. 3 Nr. 1 DSGVO anzusehen ist und hiernach die Anmeldung nach § 27 Abs. 3 DSGVO vorzunehmen sowie Auskunft nach § 16 DSGVO zu erteilen hat.

Öffentliche Schulen in kommunaler Trägerschaft sind nach § 6 des Schulverwaltungsgesetzes (SchVG) nichtrechtsfähige öffentliche Anstalten der Gemeinde. Für die Organisation und Verwaltungsführung in den Schulen ist der Schulträger unmittelbar rechtlich verantwortlich (§ 2 Abs. 1 SchVG). Für die in diesem Bereich geführten Dateien ist daher die Gemeinde speichernde Stelle. Dementsprechend bestimmt Nr. 3.4 VVzASchO, daß für das Einhalten der Datenschutzvorschriften als speichernde Stelle nach § 1 Abs. 2 Satz 1, § 2 Abs. 3 Nr. 1 DSGVO der Schulträger verantwortlich ist.

Allerdings könnte es zweifelhaft sein, ob zu dem Bereich der Organisation und Verwaltungsführung der Schulen auch diejenigen Angelegenheiten zu rechnen sind, die sich ausschließlich auf die Organisation und Gestaltung des Unterrichts sowie auf die Personalführung der Lehrer beziehen (z. B. Stundenplanprogramme/Dateien, Dateien über Vertretungen und Fehlzeiten der Lehrkräfte). Es ist nicht zu verkennen, daß die Organe der Gemeinden keinen maßgebenden Einfluß auf die Datenverarbeitung in derartigen Schuldateien haben.

Andererseits kann nach § 2 Abs. 3 Nr. 1 DSGVO speichernde Stelle nur eine der in § 1 Abs. 2 DSGVO genannten Stellen sein. Die Schulaufsichtsbehörden als Behörden des Landes kommen als speichernde Stelle für die in den einzelnen Schulen geführten Dateien nicht in Betracht. Die Schulen selbst gehören als nichtrechtsfähige Anstalten der Gemeinden nicht zu den in § 1 Abs. 2 DSGVO genannten Stellen.

Der Kultusminister, den ich um Mitteilung seiner Auffassung zu dieser Frage gebeten habe, hat im Einvernehmen mit dem Innenminister darauf hingewiesen, bei Schulen in kommunaler Trägerschaft trage die jeweilige Gemeinde oder der zuständige Gemeindeverband die rechtliche Verantwortung in den

Bereichen der Organisation und Verwaltungsführung. Mit den Rechtsvorschriften des Schulverwaltungsgesetzes korrespondierten die Kostentragungsvorschriften des Schulfinanzgesetzes (SchFG). So habe bei öffentlichen Schulen der Schulträger die Sachausgaben zu tragen (§§ 1 und 2 SchFG). Zu diesen Sachausgaben gehörten die Kosten der Organisation und Verwaltungsführung der einzelnen Schule. Bei dem so bestimmten Rechtscharakter der öffentlichen Schulen und der gesetzlich ausgewiesenen Regelung der Schulkosten/Sachausgaben sei für die im Bereich der Schule geführten Dateien die jeweilige Gemeinde/Gemeindeverband speichernde Stelle im Sinne von § 1 Abs. 2 Satz 1 und § 2 Abs. 3 Nr. 1 DSG NW.

Die Richtlinien zum Schülerstamblatt und zum sonstigen Datenbestand in der Schule postulierten ausdrücklich die Verantwortung für den kommunalen Schulträger für Daten, die ausschließlich den inneren Schulangelegenheiten dienen. Durch diese Richtlinien seien alle inneren Schulangelegenheiten erfaßt worden mit Ausnahme der die Organisation und Gestaltung des Unterrichts sowie die Personalführung der Lehrer betreffenden Dateien. Dieser wesentlich kleinere Teil der inneren Schulangelegenheiten könne aber grundsätzlich nicht anders behandelt werden als der weitaus umfassendere Teil der Datenbestände der inneren Schulangelegenheiten. Nach dem Zusammenhang der einschlägigen Vorschriften sei eine regelungsbedürftige Lücke nicht ersichtlich.

- Als gesetzliche Grundlage für Datenerhebungen im Zusammenhang mit schulischen Leistungsbewertungen können die Bestimmungen des V. Abschnitts der auf Grund des § 26 Abs. 1 Satz 1 SchVG erlassenen allgemeinen Schulordnung (ASchO) herangezogen werden. Dies gilt jedoch nicht für **Tests**, die an Schulen durchgeführt werden und die nicht unmittelbar der Leistungsbewertung dienen. Der Auffassung des Kultusministers, die Zulässigkeit derartiger Tests folge aus dem allgemeinen Bildungs- und Erziehungsauftrag der Schule, kann ich mich nicht anschließen. Zweifellos werden bei der Durchführung derartiger Tests personenbezogene Daten der betroffenen Schüler erhoben. Dabei ist die Eingriffsintensität bei solchen Tests erheblich höher als bei den sonst üblichen schulischen Leistungsprüfungen (etwa bei Klassenarbeiten). Eine gesetzliche Grundlage, die für einen derartigen Eingriff in das Grundrecht der Betroffenen auf Datenschutz sowie in ihr informationelles Selbstbestimmungsrecht erforderlich ist, ist zur Zeit nicht vorhanden.

Ich habe den Kultusminister darauf hingewiesen, daß im Zusammenhang mit einer gesetzlichen Neuregelung der Erhebung und Verarbeitung von Schüler- und Elterndaten in den Schulen auch die Frage der Datenerhebung durch Tests geregelt werden muß. Dabei wird der Gesetzgeber zu entscheiden haben, ob er die Schaffung einer solchen gesetzlichen Grundlage für erforderlich hält oder aber ob die Durchführung der Tests von der Einwilligung der Eltern abhängig gemacht werden soll. Bei der Durchführung von schulischen Tests muß nach meiner Auffassung insbesondere folgendes berücksichtigt werden:

- Die Schüler dürfen nicht über Angelegenheiten, die den unantastbaren Kernbereich der eigenen oder der elterlichen Persönlichkeitssphäre betreffen, befragt werden.
- Die Eltern sind, auch wenn die Durchführung der Tests in der Zukunft auf eine gesetzliche Grundlage gestützt wird, über das Testverfahren vorher eingehend zu unterrichten. Es ist ihnen auf Wunsch Gelegenheit zur Einsicht in die Testunterlagen oder zur Besprechung der Ergebnisse zu geben.
- Durch Einzelregelungen über den Zugang zu den Testergebnissen, die

Dauer und die Art der Aufbewahrung der Testunterlagen ist sicherzustellen, daß die bei den Tests erhobenen personenbezogenen Daten ausschließlich für den bestimmten Zweck verwendet werden.

- Immer wieder erhalte ich Eingaben zur Erhebung von Eltern- und **Familien-daten im Sachkundeunterricht** der Grundschule. In den dabei verwendeten Arbeitsunterlagen sind verschiedene Fragen zur Geburt, Heirat und Tod von Großeltern und Eltern sowie zahlreiche ins einzelne gehende Fragen zur eigenen Geburt und frühen Kindheit vorgesehen. Verschiedene Eltern haben in Zweifel gezogen, ob alle diese Fragen mit dem Daten- und Persönlichkeitsschutz vereinbar sind.

Der Kultusminister, den ich um Stellungnahme gebeten habe, hat darauf hingewiesen, daß die beanstandeten Arbeitsunterlagen im Zusammenhang stehen mit den in den Richtlinien und Lehrplänen für die Grundschule für den Sachunterricht festgelegten Aufgabenschwerpunkten „Zeiteinteilung und Zeitablauf“ und „Geburt und Aufwachsen“. Ziel der Unterrichtsarbeit in den beiden Aufgabenschwerpunkten sei es unter anderem, den Kindern zeitliche Abläufe sichtbar werden zu lassen und bei ihnen erste Kenntnisse über die Entstehung und Entwicklung menschlichen Lebens anzubahnen.

Dem Alter der Kinder entsprechend müßten die Lerninhalte des Sachunterrichts auf einfache, grundlegende, für Kinder durchschaubare Vorgänge, Beziehungen und Begriffe zurückgeführt werden. Deshalb werde bei der Vermittlung der Inhalte gern auf das Kind selbst oder auf den Bereich seiner Familie zurückgegriffen. Zeitliche Abläufe ließen sich zum Beispiel am Aufwachsen des Kindes und den dabei stattfindenden körperlichen und geistigen Veränderungen oder an den Generationsfolgen in der Familie, Entstehung und Entwicklung des Menschen durch Festmachen am jeweiligen Kinde selbst in den Verständnishorizont von Kindern bringen.

Natürlich müsse der Lehrer bei einem solchen Vorgehen darauf bedacht sein, die Persönlichkeitsrechte der Kinder und der Erziehungsberechtigten zu wahren. Bei einer vollständigen Beantwortung der Fragen könnten unter Umständen schutzwürdige Persönlichkeitsdaten (z. B. vor- oder uneheliche Geburt, Verzögerungen in der körperlichen und geistigen Entwicklung) offenbar werden. Deshalb werde ein verantwortungsbewußter Lehrer auch weder auf einer Beantwortung aller Fragen durch alle Kinder der Klasse bestehen noch einer solchen Datenermittlung eine Benotungsrelevanz zusprechen.

Wenn dies beachtet wird, habe ich keine durchgreifenden datenschutzrechtlichen Bedenken gegen die erwähnten Datenerhebungen. Sie können für die Übergangszeit bis zur erforderlichen Neuregelung der Datenerhebung und Datenverarbeitung im Schulwesen auf den in § 1 Abs. 3 des Schulordnungsgesetzes (SchOG) enthaltenen schulischen Bildungs- und Erziehungsauftrag sowie auf die Aufgabenzuweisung für die Grundschule in § 16 Abs. 1 SchOG gestützt werden.

- Eine Eingabe betraf die Datenerhebung durch einen **Jahrgangsstufen- und Schulpflegschaftsvorsitzenden** eines Gymnasiums. Dieser hatte zwei Schreiben an die Eltern einer Jahrgangsstufe sowie an die Eltern der Klassen 5 und 6 der Schule gerichtet, in denen zum Zweck der Erörterung von Möglichkeiten einer Verbesserung der Zusammenarbeit zwischen Schule und Elternhaus die Eltern gebeten wurden mitzuteilen, „was welcher Lehrer besonders gut und nachahmenswert gemacht habe und was der (aufbauenden) Kritik würdig erscheine“.

Die im Schulmitwirkungsgesetz (SchMG) vorgesehenen Mitwirkungsorgane sind als Organe der Schule ebenso wie diese selbst Teil einer öffentlichen Stelle gemäß § 1 Abs. 2 DSG NW. Ihre Datenerhebung bedarf daher einer dem Gebot der Normenklarheit entsprechenden gesetzlichen Grundlage

oder aber der Einwilligung der Betroffenen. Eine gesetzliche Grundlage für die Datenerhebung durch den Jahrgangsstufen- und Schulpflegschaftsvorsitzenden besteht nach meiner Auffassung nicht, insbesondere kann das Schulmitwirkungsgesetz dafür nicht herangezogen werden. Auch der Kultusminister vertritt die Auffassung, daß es nicht in die Zuständigkeit einer Elternpflegschaft fällt, durch eine Umfrage unter den Eltern das Verhalten von Lehrern im Unterricht zu beurteilen. Von der Datenerhebung ist daher an der Schule dann auch Abstand genommen worden.

- Immer wieder ergeben sich Fragen zum Inhalt von und zum Umgang mit **Klassenbüchern**. Dies wurde auch im Verlauf eines Kontrollbesuchs deutlich, der im Berichtsjahr bei einem Gymnasium durchgeführt wurde. Ich den an diesem Gymnasium verwendeten Klassenbüchern werden die Ergebnisse der schriftlichen Arbeiten des Schuljahres eingetragen. Diese Verfahrensweise entspricht der Regelung in den Verwaltungsvorschriften zu § 5 Abs. 4 ASchO. Dort ist vorgesehen, daß zum Inhalt des Klassenbuchs die Liste der schriftlichen Arbeiten und deren Ergebnisse gehört.

Das Klassenbuch ist der Obhut eines Klassenbuchführers anvertraut. Dieser holt das Klassenbuch morgens im Schulsekretariat ab und nimmt es zu dem jeweiligen Unterrichtsraum mit. Nach Unterrichtsschluß der Klasse legt er das Buch in einen vor dem Schulsekretariat bereitgestellten „Rollwagen“ in das dafür vorgesehene Fach. Der Wagen wird nach Schulschluß in das Schulsekretariat gerollt und ist dann dort unter Verschuß bis zum nächsten Schultag.

Durch das an diesem Gymnasium praktizierte Verfahren ist die Möglichkeit, daß einzelne Schüler sich über den Inhalt der Klassenbücher Kenntnis verschaffen, eingeschränkt. Es kann aber in der Praxis nicht ausgeschlossen werden, daß insbesondere die der Klasse angehörenden Schüler – etwa durch Einsichtnahme vor der Schulstunde –, in Einzelfällen auch andere Schüler durch Einsichtnahme in bereits im Rollwagen abgelegte Klassenbücher anderer Klassen vor allen oder einzelnen der im Klassenbuch eingetragenen Daten Kenntnis nehmen.

In meinem dritten Tätigkeitsbericht (C.13.a) habe ich auf datenschutzrechtliche Bedenken hingewiesen, wenn durch freien Zugang der Schüler zum Klassenbuch die Möglichkeit besteht, von allen eingetragenen, unter Umständen weit zurückliegenden Leistungsbewertungen der Mitschüler Kenntnis zu nehmen. Eine gesetzliche Grundlage für einen derartigen Eingriff in das Grundrecht der Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung und in ihr Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes ist nicht ersichtlich.

Der Kultusminister hat mir hierzu mitgeteilt, daß er zur Zeit die Erfahrungsberichte der oberen Schulaufsichtsbehörden zu den Verwaltungsvorschriften zu § 5 Abs. 4 ASchO auswertet und danach in Kürze zu der Frage Stellung nehmen wird, durch welche Maßnahmen der Inhalt der Klassenbücher besser geschützt werden kann. Dies könnte nach meiner Ansicht etwa dadurch geschehen, daß die Klassenbücher nur „von Lehrerhand“ weitergegeben werden. Ob ein solches Verfahren im Schulalltag in allen Fällen praktikabel ist, vermag ich jedoch nicht abschließend zu beurteilen. Mit Rücksicht auf die gegenwärtigen Überlegungen habe ich daher zunächst davon abgesehen, eine Empfehlung für den Inhalt des Klassenbuchs oder den Zugang zum Klassenbuch zu geben. Sollte sich jedoch mein bisher gewonnener Eindruck bestätigen, daß in der Schulpraxis gegenwärtig keine wirksamen Maßnahmen dagegen getroffen werden können, daß Klassenbücher zumindest von den jeweils der Klasse angehörenden Schülern eingesehen werden können, so können nach meiner Auffassung die Ergebnisse der schriftlichen Arbeiten in Zukunft nicht mehr in das Klassenbuch aufgenommen werden.

- An dem erwähnten Gymnasium wird die Kursbelegung den Schülern derzeit in der Weise bekanntgegeben, daß an bestimmten Orten, zum Beispiel in der Pausenhalle, ausgedruckte Listen über die Kursbelegung der einzelnen Jahrgangsstufen ausgehängt werden. Auf die gleiche Weise erfolgt eine Information der Schüler darüber, welche Schüler sich in welchen Fächern zu welchem Termin einer Nachprüfung unterziehen müssen und welcher Schüler in welchem Fach mündlich im Abitur geprüft wird. Bei diesem Verfahren erhalten sämtliche Schüler des Gymnasiums, aber auch andere Personen, die das Schulgebäude betreten, Gelegenheit, von diesen Daten Kenntnis zu nehmen.

Eine gesetzliche Grundlage für eine solche Datenübermittlung ist nicht ersichtlich. Ich habe daher empfohlen, die Schüler künftig nicht mehr durch allgemein zugängliche **Aushänge** über ihre Kursbelegung oder die Prüfungstermine zu informieren, sondern diese Informationen nur dem jeweils in Betracht kommenden Schüler zukommen zu lassen. Dies kann hinsichtlich der Kursbelegung etwa in der Weise erfolgen, daß dem einzelnen Schüler über den Beratungslehrer eine entsprechende Aufstellung zugeleitet wird.

Dementsprechend habe ich auch in anderen Fällen, in denen sich Betroffene gegen die Bekanntgabe personenbezogener Daten durch Aushänge gewandt hatten, die jeweilige Schule darauf hingewiesen, daß eine gesetzliche Grundlage für die Bekanntgabe der Daten an einen unbestimmten Personenkreis nicht vorhanden und diese Bekanntgabe somit unzulässig ist.

- Auf eine nicht den Vorschriften über den Datenschutz entsprechende **Nutzung der Schülerdaten** von Kreisberufsschulen **durch den Schulträger** wurde ich durch die örtliche Presse aufmerksam gemacht. Ein freier Träger wollte im Kreisgebiet ein Berufsbildungszentrum für arbeitslose Jugendliche unter Inanspruchnahme öffentlicher Mittel sowohl des Landes wie auch des Kreises errichten. Nach den für die Mittelvergabe geltenden Förderungsrichtlinien durften diese Jugendlichen unter anderem in dem betreffenden Schuljahr nicht einen vollzeitschulischen Unterricht begonnen haben. Bei der weiteren Planung des Projektes kam es hinsichtlich der Frage, ob alle angemeldeten Bewerber die Förderungsvoraussetzungen erfüllten, zu Unklarheiten. Um diese aufzuklären, begaben sich Mitarbeiter des Kreisjugendamtes, die vom Oberkreisdirektor mit der Bearbeitung des Projektes beauftragt worden waren, mit der Liste der angemeldeten Bewerber zu den Schulsekretariaten der vier berufsbildenden Schulen des Kreises. Dort wurde vom Schulpersonal geprüft, ob sich einzelne Bewerber in der Schulkartei befanden. Diese wurden den Mitarbeitern des Jugendamtes benannt.

Als gesetzliche Grundlage für die Datenübermittlung aus den Dateien der Kreisberufsschulen, die nichtrechtsfähige Anstalten des Kreises sind, an Bedienstete des Jugendamtes kommt nur § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSGVO in Betracht. Danach ist eine Datenweitergabe innerhalb des Kreises als speichernde Stelle zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Dabei ist an die Erforderlichkeit ein strenger Maßstab anzulegen.

Es mag sein, daß in dem zu beurteilenden Fall die Kenntnis der Daten über den Schulbesuch einzelner Bewerber zur Feststellung, ob die Förderungsvoraussetzungen nach Förderungsbestimmungen vorlagen, erforderlich gewesen ist. Gleichwohl kann nach meiner Auffassung die Datenweitergabe zwischen Schulsekretariat und Mitarbeitern des Kreisjugendamtes nicht auf § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSGVO gestützt werden. Wie das Bundesverfassungsgericht in dem Urteil zum Volkszählungsgesetz 1983 näher ausgeführt hat, muß die für einen Eingriff in das informationelle

Selbstbestimmungsrecht erforderliche gesetzliche Grundlage dem Gebot der Normenklarheit entsprechen. Es erscheint daher zweifelhaft, inwieweit die Generalklauseln der Datenschutzgesetze für sich allein oder in Verbindung mit anderen Rechtsvorschriften als gesetzliche Grundlage für einen Informationseingriff noch herangezogen werden können. Dies gilt insbesondere für Übermittlungsvorschriften, die – wie die 2. Alternative des § 11 Abs. 1 Satz 1 DSGVO – an die rechtmäßige Aufgabenerfüllung des Empfängers anknüpfen, da sie den Verwendungszweck der Daten bei dem Empfänger nicht bestimmen und deshalb den Umfang des Eingriffs für den Bürger nicht erkennen lassen. Die generalklauselartigen Übermittlungstatbestände der Datenschutzgesetze müssen daher unter Berücksichtigung der vom Bundesverfassungsgericht aufgestellten Grundsätze neu gefaßt werden. Für die Übergangszeit muß für die Anwendung der 2. Alternative des § 11 Abs. 1 Satz 1 DSGVO zumindest gefordert werden, daß die Aufgabe, zu deren rechtmäßiger Erfüllung die Übermittlung erforderlich sein muß, durch Gesetz festgelegt ist.

Diese Voraussetzung war in dem zu beurteilenden Fall nicht erfüllt.

Die Mitarbeiter des Jugendamtes sind bei dem Abgleich in den Karteien der Kreisberufsschulen nicht im Rahmen der dem Jugendamt nach dem Jugendwohlfahrtsgesetz zugewiesenen gesetzlichen Aufgaben tätig geworden. Denn die Schaffung von Einrichtungen und Veranstaltungen allein zur Berufsausbildung, also unabhängig davon, ob ein Erziehungshilfebedarf vorliegt, gehört nicht zu den Aufgaben der Jugendhilfe nach den §§ 8, 27 des Ersten Buches des Sozialgesetzbuchs in Verbindung mit den Vorschriften des Jugendwohlfahrtsgesetzes. Die Schaffung und Bereitstellung einer ausreichenden Zahl von Ausbildungsplätzen ist vielmehr eine gesamtgesellschaftliche Aufgabe, zu deren Erfüllung vorrangig die ausbildende Wirtschaft einschließlich der öffentlichen Hand sowie die Arbeitsverwaltung verpflichtet ist, zu deren Aufgaben nach dem Arbeitsförderungsgesetz die Schaffung von Einrichtungen zur Berufsausbildung einschließlich überbetrieblicher Lehrwerkstätten gehört. Darüber hinaus sind aber auch Bund, Länder, Gemeinden und Gemeindeverbände verpflichtet, zur Lösung dieses Problems im Rahmen ihrer generellen Zuständigkeit beizutragen.

Nach § 16 Abs. 1 der Kreisordnung schaffen die Kreise innerhalb der Grenzen ihrer Leistungsfähigkeit die für die wirtschaftliche, soziale und kulturelle Betreuung ihrer Einwohner erforderlichen öffentlichen Einrichtungen. Entsprechend dieser allgemeinen Aufgabenzuweisung hatte sich der Kreis des hier in Rede stehenden Anliegens angenommen. Dabei hatte er wegen der sachlichen Nähe zu den gesetzlichen Aufgaben der Verwaltung des Jugendamtes im Rahmen seiner Organisationsgewalt bestimmt, daß dieses Amt die federführende Bearbeitung des Projektes übernehmen sollte.

Die Daten über den Schulbesuch einzelner Bewerber sind den Mitarbeitern des Jugendamtes somit nicht bei der Erfüllung einer durch Gesetz festgelegten Aufgabe bekanntgegeben worden. Da nach den vorhergehenden Ausführungen in diesen Fällen für eine Datenübermittlung § 11 Abs. 1 Satz 1 DSGVO oder für eine Datenweitergabe innerhalb der speichernden Stelle § 8 Satz 1 in Verbindung mit § 11 Abs. 1 Satz 1 DSGVO nicht herangezogen werden kann, war die Bekanntgabe der Daten von den Mitarbeitern der Schulen an die Mitarbeiter des Kreisjugendamtes datenschutzrechtlich nicht zulässig.

In diesem Zusammenhang ist auch auf Nr. 4.22 VVzASchO hinzuweisen. Nach dieser Vorschrift kann eine Schule bei einer Datenanforderung im Wege der Amtshilfe von der Übermittlung absehen, wenn erkennbar ist, daß diese unter Berücksichtigung der Aufgaben der ersuchenden Behörde mit

dem besonderen Vertrauensverhältnis zwischen der Schule und dem Schüler nicht vereinbar ist. Bei dem im vorliegenden Fall ohne Einwilligung und Wissen der Betroffenen durchgeführten Datenaustausch zwischen den Mitarbeitern der Schule und Mitarbeitern des Kreisjugendamtes mußte aber befürchtet werden, daß diese Maßnahme geeignet war, das Vertrauensverhältnis zwischen den Schülern der Kreisberufsschule und der Schule zu belasten. Trotz eines anzuerkennenden Bedarfs nach genauem Zahlenmaterial konnte daher die zur Feststellung der Förderungsvoraussetzungen getroffene Maßnahme des Abgleichs in den Karteien der Kreisberufsschulen datenschutzrechtlich nicht gebilligt werden. Da es im Zweifel dem Träger obliegen sollte, das Vorliegen der Förderungsvoraussetzungen nachzuweisen, hätte er entweder einen solchen Nachweis führen müssen, oder aber es hätte die Einwilligung der Betroffenen zu derartigen Ermittlungsmaßnahmen bei den Schulen eingeholt werden müssen.

- Von den Schulen des Landes Nordrhein-Westfalen werden einmal jährlich die **Erhebungsbogen SCD 021, LID 121, UVD 221 und KLD 321** ausgefüllt und sodann an die vorgesehenen Empfänger übermittelt. Die Erstschrift erhält das Landesamt für Datenverarbeitung und Statistik für den Kultusminister des Landes Nordrhein-Westfalen. Die Schulaufsichtsbehörde erhält eine Zweitschrift, ein drittes Exemplar ist für den Schulträger bestimmt, und die vierte Ausfertigung verbleibt bei der Schule. Von diesen Erhebungsbogen enthalten insbesondere die Bogen LID 121 und UVD 221, aber auch der Bogen KLD 321 personenbezogene Lehrerdaten.

Die Weitergabe dieser Daten an das Landesamt für Datenverarbeitung und Statistik, die Schulaufsichtsbehörde und den Schulträger stellt einen Eingriff in das Recht der Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung und in ihr Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes dar. Ein solcher Eingriff bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen muß; aus ihr müssen sich die Voraussetzungen und der Umfang der Einschränkung des Grundrechts klar und für den Bürger erkennbar ergeben.

Eine diesen Anforderungen entsprechende gesetzliche Grundlage für die Weitergabe der Daten ist nicht ersichtlich. Soweit die in die Erhebungsbogen einzutragenden Daten einer Datei entnommen werden, kommt zwar als gesetzliche Grundlage § 11 Abs. 1 Satz 1 DSGVO in Betracht. Nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 ist jedoch zweifelhaft, inwieweit die Generalklauseln der Datenschutzgesetze für sich allein oder in Verbindung mit anderen Rechtsvorschriften als gesetzliche Grundlage für eine Datenübermittlung noch herangezogen werden können. Der in dem Urteil geforderten Normenklarheit entbehren insbesondere Übermittlungsvorschriften, die wie die 2. Alternative des § 11 Abs. 1 Satz 1 DSGVO an die rechtmäßige Aufgabenerfüllung des Empfängers anknüpfen, da sie den Verwendungszweck der Daten bei dem Empfänger nicht bestimmen und deshalb den Umfang des Eingriffs für den Betroffenen nicht erkennen lassen.

Nach meiner Auffassung können daher die Generalklauseln der Datenschutzgesetze als gesetzliche Grundlage für Datenübermittlungen künftig nur noch dann herangezogen werden, wenn es sich um weniger schwerwiegende Einschränkungen des Rechts auf informationelle Selbstbestimmung handelt. Darüber hinaus muß zumindest die Aufgabe, zu deren Erfüllung die Übermittlung erfolgt, durch Gesetz festgelegt sein. Ob diese Voraussetzungen bei den Datenübermittlungen gegeben sind, die mittels der Erhebungsbogen LID 121, UVD 221 und KLD 321 erfolgen, erscheint fraglich.

Die Überprüfungen sind noch nicht abgeschlossen.

- Von Eltern wurde ich darauf aufmerksam gemacht, daß von einer Fotofirma in der Schule neben einem Klassenfoto auch **Porträtfotos** der einzelnen Kinder angefertigt wurden. Die Anfertigung von Porträtfotos einzelner Schüler ist ohne ausdrückliche Einwilligung der Erziehungsberechtigten datenschutzrechtlich nicht zulässig. Dies war auch die Ansicht der zuständigen Schulaufsichtsbehörde. Sie glaubte jedoch, die Einwilligung daraus entnehmen zu können, daß Eltern auf ein Schreiben des Fördervereins der Schule, in dem die Eltern auf den Fototermin in der Schule hingewiesen worden waren, keinen Widerspruch erhoben hätten. Das Unterlassen eines Widerspruchs kann jedoch auch in diesem Fall die erforderliche ausdrückliche Einwilligung der Erziehungsberechtigten, die für die Anfertigung der Porträtfotos erforderlich ist, nicht ersetzen. Von den Betroffenen kann nicht erwartet werden, daß sie in einem solchen Fall selbst tätig werden, wenn sie eine Aufnahme ihres Kindes nicht wünschen.
- Eine Vielzahl von Eingaben im Berichtsjahr betraf die Weitergabe von Elternadressen an politische Parteien und örtliche Initiativen im Zusammenhang mit einer **Elternbefragung** zur Feststellung des Bedürfnisses für eine Gesamtschule nach § 10 Abs. 2 und 4 SchVG.

Wie in meinem dritten Tätigkeitsbericht (C.13.a) dargelegt, bestehen gegen eine Übermittlung der Elternadressen auf der Grundlage des § 13 Abs. 1 Satz 1 DSGVO keine durchgreifenden datenschutzrechtlichen Bedenken, wenn zu dem Zeitpunkt vom Schulträger eine Elternbefragung durchgeführt wird, um den Willen der Erziehungsberechtigten festzustellen, den er bei der Entscheidung über die Errichtung einer Gesamtschule zu berücksichtigen hat. Entsprechendes muß, wenn die Daten dem Melderegister entnommen werden, für eine Übermittlung auf der Grundlage des § 34 Abs. 3 Satz 1 MG NW gelten.

Bei einer solchen Sachlage überwiegt nach meiner Auffassung bei einer Abwägung der Interessen des Datenempfängers mit denen der Betroffenen das Interesse der Parteien an einer gezielten Unterrichtung der Erziehungsberechtigten, das zugleich ein öffentliches Interesse ist, gegenüber dem Interesse der Eltern an dem Schutz vor einer Mitteilung ihrer Namen und Anschriften. Da bei der Mitgestaltung des politischen Willens in der Gemeinde Initiativen auf örtlicher Ebene eine den politischen Parteien gleichwertige Funktion erfüllen, ist unter den entsprechenden Voraussetzungen die Übermittlung der Adreßdaten auch an solche örtlichen Initiativen zulässig.

Diese Erwägungen gelten jedoch nur, solange die Elternbefragung noch nicht abgeschlossen ist. Eine erneute Verwendung der Adressen, etwa während des Anmeldeverfahrens, ist nach meiner Auffassung nicht zulässig, weil das Anmeldeverfahren mit einer Elternbefragung zur Bedürfnisfeststellung nicht vergleichbar ist und in diesem Stadium die schutzwürdigen Belange der Erziehungsberechtigten überwiegen. Die Anschriften dürfen daher nach Abschluß der Elternbefragung nicht weiter verwendet werden und sind, wenn sie nicht zurückgegeben werden, zu vernichten.

Nach § 13 Abs. 2 DSGVO und § 34 Abs. 4 MG NW darf der Empfänger die übermittelten Daten nur für den Zweck verwenden, zu dessen Erfüllung sie ihm übermittelt worden sind. Die Adressen dürfen daher nur von der politischen Partei oder der örtlichen Initiative selbst für die Unterrichtung der Erziehungsberechtigten über ihren Standpunkt zur Frage der Errichtung einer Gesamtschule verwendet werden. Daraus folgt, daß die Weitergabe an andere Organisationen oder sonstige Dritte unzulässig ist. Eine unzulässige Zweckentfremdung wäre aber auch der Vergleich mit dem Mitgliederverzeichnis der Partei.

Aus dem Recht auf informationelle Selbstbestimmung und dem Grundrecht auf Datenschutz ergibt sich nach meiner Auffassung eine Verpflichtung der übermittelnden Stelle, auf die Zweckbindung hinzuweisen und auch die Verwendung der Adressen für Hausbesuche auszuschließen, weil ein solcher Eingriff nicht mehr dem Grundsatz der Verhältnismäßigkeit entsprechen würde. Wer vorsätzlich oder fahrlässig entgegen § 13 Abs. 2 DSG NW oder § 34 Abs. 4 MG NW die Daten für einen anderen Zweck verwendet, begeht eine Ordnungswidrigkeit (§ 34 Abs. 1 DSG NW, § 37 Abs. 2 Nr. 2 MG NW), die mit einer Geldbuße bis zu 50 000 Deutsche Mark geahndet werden kann (§ 34 Abs. 2 DSG NW/§ 37 Abs. 3 MG NW). Auch hierauf sollte bei der Datenübermittlung hingewiesen werden.

- Mehrere Schulpflegschaften einer Stadt wandten sich dagegen, daß die **Fragebogen einer Projektgruppe** vom Schulträger zur Bedürfnisfeststellung für eine Gesamtschule zweckentfremdet wurden. Der Rat der Stadt hatte beschlossen, die Projektgruppe mit der Ausarbeitung eines Gutachtens zur Schulentwicklungsplanung zu beauftragen. Dazu war ein umfangreicher Fragebogen erarbeitet worden, der insgesamt zwanzig ins einzelne gehende Antworten darüber vorsah, welche Wünsche die Eltern für die Schulausbildung ihrer Kinder haben und wie sie die weiterführenden Schulangebote in der Stadt beurteilen. Eine der Fragen lautete: „Würden Sie Ihr Kind auf eine Gesamtschule schicken, wenn es in unserer Stadt eine Gesamtschule geben würde?“ In einem Anschreiben hatte die Projektgruppe bei der Versendung der Fragebogen die volle Anonymität der Antworten zugesichert; außerdem wurde zugesichert, daß weder die Schulen noch die Stadt Einblick in die Fragebogen erhalten würden. Entgegen der ursprünglichen Absicht, nach der die Befragung der Aufstellung eines Schulentwicklungsplanes dienen sollte, wurden dann jedoch kurzfristig die Antworten auf die genannte Frage gesondert zum Zweck der Bedürfnisfeststellung nach § 10 Abs. 2 und 4 SchVG durch die Mitglieder der Arbeitsgruppe ausgezählt. An dieser Auszählung nahmen entgegen der Zusicherung in dem Anschreiben Vertreter der Verwaltung und der Schulaufsichtsbeamte teil.

Zwar sah der Fragebogen die Angabe des Namens und der Anschrift der betroffenen Eltern nicht vor. Es war jedoch nicht auszuschließen, daß auf Grund der Antworten zu den zahlreichen Fragen die Person eines Betroffenen mit Hilfe von Zusatzwissen bestimmt werden konnte, etwa durch die Mitarbeiter der Verwaltung, die an der Auszählung teilnahmen.

Die Verwendung der Angaben, soweit sie personenbezogen sind, für einen anderen als den dem Anschreiben der Projektgruppe zu entnehmenden Zweck greift in das Recht der Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes und in ihr Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung ein und bedarf deshalb einer gesetzlichen Grundlage. Auch bei nicht personenbezogenen Angaben kann jedenfalls dann, wenn sie wie hier von erheblicher Tragweite sind, aus dem Recht auf informationelle Selbstbestimmung hergeleitet werden, daß sie nur für den angegebenen Zweck verwendet werden dürfen, soweit nicht die Verwendung für einen anderen Zweck ausdrücklich gesetzlich zugelassen ist.

Eine gesetzliche Grundlage für die Verwendung der Angaben für die Ermittlung des Willens der Erziehungsberechtigten bei der Bedürfnisfeststellung für eine Gesamtschule war nicht vorhanden. Auf § 10 Abs. 4 SchVG konnte diese Zweckentfremdung nicht gestützt werden. Nach dem Urteil des Verfassungsgerichtshofs vom 23. Dezember 1983 (NVwZ 1984, 781) hat die Befragung der Eltern in einem förmlichen Verfahren zu erfolgen. Grundlegende Elemente eines solchen förmlichen Verfahrens sind nach dem Runderlaß des Kultusministers vom 11. November 1982, geändert durch Runderlaß vom

27. Juli 1984 (SMBl. NW. 223), unter anderem eine eindeutige und sachgerechte Fragestellung sowie ein geordneter Verfahrensablauf.

Diese Voraussetzungen sind nach meiner Auffassung nur erfüllt, wenn das Verfahren von dem Schulträger selbst durchgeführt wird, wobei unmißverständlich deutlich zu machen ist, daß es sich um eine Befragung der Erziehungsberechtigten zur Feststellung des Bedürfnisses für eine bestimmte Schulform handelt. Gemäß § 10 Abs. 2 Satz 1 DSGVO ist dabei auf die Rechtsgrundlage der Erhebung (§ 10 Abs. 2 und 4 SchVG) hinzuweisen. Ein derartiger Hinweis erscheint nach meiner Auffassung auch dann geboten, wenn die Angaben in einer Form erhoben werden, bei der ein Personenbezug nicht hergestellt werden kann.

Von einem förmlichen Verfahren unter Beachtung der genannten Anforderungen konnte im vorliegenden Fall keine Rede sein. Die Befragung war nicht von der Stadt, sondern von einer externen Arbeitsgruppe durchgeführt worden. Auch die Fragestellung war nach meiner Auffassung nicht sachgerecht, da die entscheidende Frage „Würden Sie Ihr Kind auf eine Gesamtschule schicken, wenn es in unserer Stadt eine Gesamtschule geben würde?“ in einem umfangreichen Fragebogen an versteckter Stelle inmitten von zahlreichen anderen Fragen gestellt wurde. Ein Hinweis auf die Rechtsgrundlage der Erhebung fehlte. Unter diesen Umständen durften die Angaben nach meiner Auffassung nicht für die Ermittlung des Willens der Erziehungsberechtigten bei der Bedürfnisfeststellung für eine Gesamtschule nach § 10 Abs. 2 und 4 SchVG verwendet werden.

#### b) Bibliotheken

Bei einem Kontrollbesuch in einer Stadtbücherei wurde die Datenerhebung für die Anmeldung zur Benutzung geprüft. Hierbei hat der künftige Benutzer eine **Anmeldekarte** auszufüllen, die folgende Angaben vorsah: Name, Vorname, Beruf/Schule, Geburtstag, Geburtsort, Wohnort, Straße.

Als Rechtsgrundlage für die Datenerhebung bei der Anmeldung zur Stadtbücherei kam im vorliegenden Fall eine Vorschrift der Benutzungsordnung in Betracht, die als Satzung nach den §§ 4 Abs. 1 Satz 1 und 28 Abs. 1 Satz 2 Buchst. g der Gemeindeordnung erlassen worden war. Nach dieser Vorschrift muß sich jeder Benutzer persönlich unter Vorlage eines Personalausweises anmelden. In der Vorschrift wird jedoch nicht angegeben, welche einzelnen Daten für das Benutzungsverhältnis und für die Aufgabenerfüllung der Bücherei benötigt werden und daher von dem Betroffenen anzugeben sind. Dies ist jedoch erforderlich. Denn eine Rechtsvorschrift kann nur dann als gesetzliche Grundlage für einen Eingriff in das Grundrecht der Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung sowie in ihr Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes dienen, wenn sie dem Gebot der Normenklarheit entspricht; aus ihr müssen sich die Voraussetzungen und der Umfang der Einschränkung des Grundrechts klar und für den Bürger erkennbar ergeben. Daraus folgt, daß der Betroffene aus der Vorschrift ersehen können muß, welche personenbezogenen Daten von ihm zur Verfügung zu stellen sind. Daher muß die Benutzungsordnung entsprechend ergänzt werden.

Dabei gebietet es der Verhältnismäßigkeitsgrundsatz, nur solche Daten zu verlangen, die für die Aufgabenerfüllung der Bücherei tatsächlich erforderlich sind. Hierzu hatte die Bücherei erklärt, daß die Angaben zum Geburtsort und zum Beruf oder zur Schule von ihr nicht benötigt würden. Soweit derartige Angaben für die Aufgabenerfüllung einer Bücherei zwar nicht notwendig sind, aber nützlich erscheinen, können sie nur auf freiwilliger Grundlage erhoben werden. Nach § 10 Abs. 2 Satz 1 DSGVO NW muß der Betroffene (zweckmäßiger-

weise auf der Anmeldekarte) darauf hingewiesen werden, welche Angaben für die Anmeldung notwendig und welche Angaben freiwillig sind.

In der kontrollierten Stadtbücherei werden die Daten über **Ausleihvorgänge** in einer ADV-Anlage gespeichert. Bei der Rückgabe entliehener Bücher oder anderer Medien werden die über den Ausleihvorgang gespeicherten Daten gelöscht. Bei einer solchen Verfahrensweise erscheint es ausgeschlossen, daß Leserprofile entstehen. Sie ist daher datenschutzrechtlich zu begrüßen.

Von Mitarbeitern der Bücherei wurde jedoch darauf hingewiesen, daß es für die Aufgabenerfüllung der Stadtbücherei erforderlich sei, in bestimmten Fällen noch innerhalb eines gewissen Zeitraums nach der Rückgabe entliehener Medien feststellen zu können, wer der Entleiher eines Buches oder eines anderen Gegenstandes gewesen sei. Denn nur dann könne wegen Beschädigungen etwas unternommen werden, die in der Eile bei der Rückgabe nicht sofort bemerkt werden, sondern erst später, etwa bei dem Zurückstellen eines Buches, auffallen.

Dieses Ziel kann bei der genannten Stadtbücherei unter Beibehaltung der jetzigen Verfahrensweise, bei der bei der Rückgabe eine sofortige Löschung der Daten über den Ausleihvorgang in der Leser- und in der Buchdatei erfolgt, dadurch erreicht werden, daß die über die täglichen Ausleih- und Rückgabevorgänge zusätzlich geführten Protokolldateien nicht wie bisher am folgenden Tag durch Überschreiben gelöscht, sondern noch für einen Zeitraum von etwa vier Wochen zur Verfügung gehalten werden. Gegen eine solche Änderung der Verfahrensweise habe ich keine durchgreifenden datenschutzrechtlichen Bedenken erhoben.

### c) Archive

Mehrere Städte und Gemeinden baten mich um eine datenschutzrechtliche Beurteilung von Vorhaben mit den Themenbereichen „Verfolgung und Widerstand“, bei denen Material aus der NS-Zeit gesammelt, vervollständigt, aufgearbeitet und zum Teil auch veröffentlicht werden sollte. Ich habe dazu darauf hingewiesen, daß ich keine datenschutzrechtlichen Bedenken dagegen habe, wenn das Archiv der Stadt eigenes Material aus der NS-Zeit prüft, katalogisiert und in chronologischer Reihenfolge ablegt. Eine Bekanntgabe daraus entnommener Informationen, bei denen ein Personenbezug gegeben ist, wäre jedoch, sofern keine Einwilligung des Betroffenen vorliegt, ein Eingriff in dessen Grundrecht auf Datenschutz wie auch in sein Recht auf informationelle Selbstbestimmung. Auch die Weitergabe von Unterlagen mit personenbezogenen Informationen durch andere öffentliche Stellen an die Stadt wäre ein solcher Eingriff. Derartige Eingriffe bedürften einer gesetzlichen Grundlage, die derzeit nicht vorhanden ist. Die Städte und Gemeinden können solche Grundlagen allerdings durch eine entsprechende Satzung nach § 4 Abs. 1 Satz 1 der Gemeindeordnung schaffen (vgl. C.13.b meines dritten Tätigkeitsberichts).

Auf die Notwendigkeit, durch den Erlass eines Landesarchivgesetzes die für die Arbeit der staatlichen wie der kommunalen Archive notwendige gesetzliche Grundlage zu schaffen, habe ich in meinen Tätigkeitsberichten mehrfach hingewiesen, zuletzt in meinem sechsten Tätigkeitsbericht (C.14.c). Die Landesregierung hat in ihrer Stellungnahme zu diesem Bericht (Drucksache 10/430, S. 39) ausgeführt, daß sie ebenfalls eine landesgesetzliche Regelung des Archivwesens für notwendig hält. Der Kultusminister des Landes Nordrhein-Westfalen prüft derzeit die Voraussetzungen einer landesrechtlichen Regelung des Archivwesens. Hierzu hat im November 1985 beim Kultusminister eine Erörterung der mit dem Gesetzesvorhaben zusammenhängenden Grundsatzfragen und der vorgesehenen Eckdaten eines solchen Gesetzes stattgefunden. Dabei wurde die Notwendigkeit einer Regelung der persönlichkeits- und datenschutzrechtlichen Fragen im Bereich der Archive von allen Beteiligten anerkannt.

## 17. Finanzwesen

### a) Steuerverwaltung

- Mehrere Eingaben betrafen den Umfang der Datenerhebung von Finanzämtern bei der Aufklärung steuerlicher Sachverhalte.

Ein Bürger teilte mir mit, das Finanzamt fordere abweichend von der bisherigen Verfahrensweise zu seiner Steuererklärung eine Auflistung von Angaben nicht nur über seine dienstlichen und beruflichen, sondern auch über alle **privaten Telefongespräche**. Entsprechend seien auch Angaben zu allen seinen **privaten Pkw-Fahrten** gefordert worden. Im einzelnen handelte es sich um folgende Angaben: Datum, Uhrzeit, Dauer, Telefonnummer, Ort, Gesprächspartner, Kosten; Zeitangaben über Beginn und Ende der Fahrt, Ort der Abfahrt und des Zieles, Grund der Fahrt (z. B. Name des Besuchten).

Das Anfordern solcher Angaben ist ein Eingriff in das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung und das Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes, der einer gesetzlichen Grundlage bedarf. Für die Ermittlungen des Finanzamtes gelten im vorliegenden Fall die §§ 88, 92, 93 der Abgabenordnung (AO). Nach § 88 AO ermittelt die Finanzbehörde den Sachverhalt von Amts wegen und bestimmt Art und Umfang der Ermittlungen. Nach § 92 AO bedient sich die Finanzbehörde der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält. Insbesondere kann sie Auskünfte jeder Art von den Beteiligten und anderen Personen einholen.

Bei der Aufklärung eines steuerlichen Sachverhalts dürfen von den möglichen Beweismitteln des § 92 AO jedoch nur diejenigen angewendet werden, die verhältnismäßig, insbesondere erfüllbar und zumutbar sind. Soweit in den Kernbereich des Grundrechts auf informationelle Selbstbestimmung eingegriffen wird, wie etwa durch die Aufforderung, bei allen privat geführten Telefongesprächen genaue Angaben über den Gesprächspartner und die Zeitdauer zu machen oder bei Privatfahrten den Grund und den Namen des Besuchten anzugeben, sind solche Eingriffe nach meiner Auffassung überhaupt unzulässig.

Das Finanzamt ist meiner Rechtsauffassung gefolgt und hat auf die Angaben zu privaten Telefongesprächen sowie auf die Angabe des Reiseweges und Reisezieles bei den Privatfahrten verzichtet.

- In einem anderen Fall verlangte das Finanzamt von einem Bürger zum Nachweis für die von ihm geltend gemachten Schuldzinsen eines Dispositionskredites die Vorlage von Ablichtungen seiner **Kontoauszüge**, um daraus den jeweiligen Negativsaldo ersehen zu können. Der Dispositionskredit war als Kontokorrentkredit über das Privatgirokonto des Bürgers bei einer Sparkasse abgewickelt worden, über das auch alle Buchungen seiner privaten Lebenshaltung erfolgten. Durch die Vorlage der geforderten Kopien der Kontoauszüge hätte das Finanzamt daher über die entsprechenden Zahlungen einen umfassenden Einblick in die persönlichen Lebensumstände des Bürgers erhalten.

Ich habe das Finanzamt auch in diesem Fall darauf hingewiesen, daß bei der Aufklärung eines steuerlichen Sachverhaltes von den möglichen Beweismitteln des § 92 AO nur diejenigen angewendet werden dürfen, die verhältnismäßig, insbesondere erfüllbar und zumutbar sind. Da nach dem konkreten Sachverhalt zweifelhaft war, ob die Forderung des Finanzamtes zur Vorlage der Kontoauszüge mit dem Grundsatz der Verhältnismäßigkeit zu vereinbaren war, habe ich empfohlen, dem Bürger für die geltend gemachten steuerli-

chen Aufwendungen eine andere, datenschutzrechtlich unbedenkliche Form des Nachweises einzuräumen.

- Durch das Steuerbereinigungsgesetz 1986 vom 19. Dezember 1985 (BGBl. I S. 2436) ist nunmehr in die Abgabenordnung eine Regelung über **Kontrollmitteilungen** aufgenommen worden (§ 93a AO). Entgegen früheren Entwürfen sind nach der nunmehr geltenden gesetzlichen Regelung die zuständigen Finanzbehörden nur über die Tatsache, nicht aber über die Höhe geleisteter Zahlungen zu unterrichten. Die Finanzbehörde muß sich insoweit, falls sie dazu Fragen hat, an den Betroffenen selbst wenden. Der Gesetzgeber hat damit die vorrangige Bedeutung berücksichtigt, die den Erklärungen der Beteiligten zur Ermittlung steuerlicher Sachverhalte zukommt (§ 90 Abs. 1 Satz 2, § 93 Abs. 1 Satz 3 AO). Wegen der näheren Einzelheiten des künftigen Verfahrens der Kontrollmitteilungen muß die Regelung durch die vorgesehene Rechtsverordnung abgewartet werden, die zur Zeit von den Finanzbehörden erarbeitet wird. Darin ist auch die Verpflichtung zur Unterrichtung des Betroffenen näher zu bestimmen. In der Rechtsverordnung können Ausnahmen von der Mitteilungspflicht, insbesondere für Fälle geringer steuerlicher Bedeutung, zugelassen werden. Ich gehe davon aus, daß entsprechend dem Verhältnismäßigkeitsgrundsatz eine Mitteilungspflicht an die Finanzbehörden nur im notwendigen Umfang und nur in den Fällen begründet wird, in denen tatsächlich ein steuerliches Bedürfnis für die Unterrichtung der Finanzbehörden besteht (vgl. sechster Tätigkeitsbericht, C.15.). Jedenfalls sind erhebliche Änderungen in dem Verfahren der Kontrollmitteilungen zu erwarten.

Gegen die jetzige Fassung des § 93a AO ist eingewandt worden, sie trage, bedingt durch die Einschränkung des Umfangs der Kontrollmitteilungen und die Nichtmitteilung geleisteter Zahlungen, den Bedürfnissen der Verwaltung keinerlei Rechnung, sondern führe nur zu einer unvermeidbaren Verwaltungserschwerung (Antrag der Länder Bremen, Hamburg, Nordrhein-Westfalen und Saarland; BR-Drucksache 568/3/85). Ich will dies nicht bewerten. Aus der Sicht des Persönlichkeitsschutzes der Betroffenen ist jedenfalls die vom Gesetzgeber getroffene Regelung, die der Forderung der Datenschutzbeauftragten nach einer eindeutigen Rechtsgrundlage für Kontrollmitteilungen entspricht, zu begrüßen.

- Immer häufiger beschweren sich Bürger darüber, daß in den Drittschuldnern zugestellten **Pfändungs- und Einziehungsverfügungen** des Finanzamtes der Schuldgrund angegeben ist und die Steuerschulden des Vollstreckungsschuldners im einzelnen aufgezählt werden. Ich habe hierzu in meinem fünften Tätigkeitsbericht (C.17.) und meinem sechsten Tätigkeitsbericht (C.15.) Stellung genommen. Die von den Bürgern vorgetragene Bedenken werden von mir geteilt. Die Datenschutzbeauftragten des Bundes und der Länder wenden sich seit Jahren gegen eine derartige Unterrichtung des Drittschuldners über Einzelheiten der zu vollstreckenden Forderung. Der Bundesminister der Finanzen und die Bundesregierung haben sich diesen Bedenken angeschlossen. Entsprechend der im Entwurf des Steuerbereinigungsgesetzes 1985 (Bundestagsdrucksache 10/1636) vorgesehenen, aber aus Zeitgründen nicht mehr in dieses Gesetz aufgenommenen Regelung ist nunmehr durch das Steuerbereinigungsgesetz 1986 nach § 309 Abs. 2 Satz 1 AO folgender Satz angefügt worden: „Die an den Drittschuldner zuzustellende Pfändungsverfügung soll den beizutreibenden Geldbetrag nur in einer Summe, ohne Angabe der Steuerarten und der Zeiträume, für die er geschuldet wird, bezeichnen.“ Allerdings tritt diese Ergänzung erst am 1. Januar 1987 in Kraft. Einen Grund für die Entscheidung des Gesetzgebers, den oft und zu Recht bemängelten datenschutzrechtlichen Mißstand bis dahin fortbestehen zu lassen, vermag ich nicht zu erkennen.

Bereits im Sommer 1985 habe ich mich an den Finanzminister des Landes Nordrhein-Westfalen gewandt und ihm empfohlen, er solle bereits vor Inkrafttreten einer gesetzlichen Neuregelung die Finanzämter des Landesbereichs anweisen, in der für den Drittschuldner bestimmten Ausfertigung der Pfändungsverfügung eine detaillierte Angabe der einzelnen Steuerrückstände wegzulassen und lediglich die Gesamthöhe der Steuerschuld anzugeben. Nach meiner Auffassung würde eine derartige Verfahrensweise dem verfassungsrechtlichen Verhältnismäßigkeitsgrundsatz entsprechen, wonach ein Eingriff zur Erreichung des vom Gesetzgeber angestrebten Zwecks erforderlich sein muß und unter mehreren für die Erreichung des Zwecks geeigneten Mitteln dasjenige zu wählen ist, das den Betroffenen am wenigsten belastet.

Der Finanzminister hat mir jedoch hierzu mitgeteilt, er sehe sich bei der derzeitigen Fassung des § 309 AO durch die Rechtsprechung der Finanzgerichte, insbesondere des Bundesfinanzhofs, gehindert, entsprechend meiner Empfehlung die Finanzämter anzuweisen, schon vor dem Inkrafttreten der gesetzlichen Neuregelung nach dieser zu verfahren. Um so mehr ist das späte Inkrafttreten der Änderung des § 309 AO zu bedauern.

#### **b) Kommunales Finanzwesen**

- Von einem Stadtdirektor wurde ich um Stellungnahme zu der Frage gebeten, ob er in dem Verfahren der **Niederschlagung** von Gewerbesteuern verpflichtet ist, dem für diese Entscheidung zuständigen Finanzausschuß des Rates auch den Namen des Steuerpflichtigen mitzuteilen, wenn er dem Ausschuß einen entsprechenden Vorschlag unter detaillierter Angabe der Umstände und Gründe für die beabsichtigte Niederschlagung unterbreitet. Der Stadtdirektor vertrat die Auffassung, er sei darüber hinaus zur Bekanntgabe des Namens des Steuerpflichtigen nicht befugt, da die Mitglieder des Ausschusses nicht berechtigt seien, eigene Nachforschungen vorzunehmen, und damit durch die Mitteilung des Namens nicht zu weiteren Erkenntnissen gelangen könnten.

Nach § 30 Abs. 1 und 2 AO haben Amtsträger das Steuergeheimnis zu wahren. Diese Vorschrift gilt nach § 1 Abs. 2 Nr. 1 AO auch für die Gemeinden im Bereich der Realsteuern. Auch im Verhältnis zwischen der Gemeindeverwaltung und dem zur Entscheidung berufenen Ausschuß ist das Steuergeheimnis zu beachten. Ob eine Offenbarung des Namens des Steuerpflichtigen zulässig ist, richtet sich im vorliegenden Fall allein nach § 30 Abs. 4 Nr. 1 AO. Danach ist eine Offenbarung zulässig, soweit sie der Durchführung eines Verwaltungsverfahrens in Steuersachen dient. Dabei ist dieser Begriff des „Dienens“ der Bedeutung des Steuergeheimnisses entsprechend auszulegen; die Offenbarung darf nicht über den zur Erreichung des steuerlichen Zwecks erforderlichen Umfang hinausgehen.

Nach § 32 Abs. 2 der Gemeindehaushaltsverordnung dürfen Ansprüche niedergeschlagen werden, wenn feststeht, daß die Einziehung keinen Erfolg haben wird. Um diese Entscheidung treffen zu können, benötigt der Ausschuß die notwendigen Informationen zum Entstehen und zu dem bisherigen Schicksal der Forderung. Darüber hinaus ist für die Entscheidung die Kenntnis der wirtschaftlichen Verhältnisse und auch der persönlichen Lebensumstände des Zahlungspflichtigen erforderlich. Zur Vorbereitung der Entscheidung des Ausschusses hat die Verwaltung hierzu die einzelnen ihr bekannten Gesichtspunkte zusammenzustellen.

Nach meiner Auffassung verlangt die Entscheidungsbefugnis des Ausschusses jedoch auch, daß seine Mitglieder in den Stand gesetzt werden, den ihnen dargelegten Sachverhalt vor dem Hintergrund ihres eigenen präsenten Wissens zu würdigen. Die Niederschlagung von Gewerbesteuern ist kein ausschließlich objektbezogener Verwaltungsakt, bei dem die Person des

Steuerpflichtigen grundsätzlich ohne Bedeutung wäre. Da für die Niederschlagung von Forderungen die wirtschaftlichen und persönlichen Verhältnisse des Zahlungspflichtigen von besonderer Bedeutung sind, ist nach meiner Auffassung im Regelfall auch der Name des Betroffenen den Ausschußmitgliedern mitzuteilen. Zwar sind die Ausschußmitglieder nicht befugt, eigene Nachforschungen anzustellen. Sie sind jedoch berechtigt und verpflichtet, die ihnen bekannten Umstände der Verwaltung mitzuteilen und dadurch gegebenenfalls weitere Darlegungen oder Ermittlungen der Verwaltung zu veranlassen. Nach meiner Auffassung bestehen daher im Regelfall keine durchgreifenden datenschutzrechtlichen Bedenken dagegen, daß im Zusammenhang mit der Niederschlagung von Forderungen dem Finanzausschuß der Name des Zahlungspflichtigen bekanntgegeben wird.

Die Ausschußmitglieder sind verpflichtet, das Steuergeheimnis zu wahren (§ 30 Abs. 2 AO). Für sie gilt ferner die Verschwiegenheitspflicht nach § 22 Abs. 1 Satz 1 der Gemeindeordnung (GO) und das Verwertungsverbot nach § 22 Abs. 1 Satz 2 GO. Sie müssen außerdem nach § 5 Abs. 2 Satz 1 DSGVO auf das Datengeheimnis verpflichtet sein.

In Ausnahmefällen kann allerdings der verfassungsrechtliche Verhältnismäßigkeitsgrundsatz eine von dem Vorstehenden abweichende Beurteilung rechtfertigen. Nach diesem Grundsatz müßte die Bekanntgabe des Namens unterbleiben, wenn sie auf Grund besonderer Umstände des Einzelfalles, gemessen an ihrer Erforderlichkeit zu dem vorgesehenen Zweck der Berücksichtigung eigenen Wissens der Ausschußmitglieder trotz der genannten Geheimhaltungspflichten den Betroffenen unverhältnismäßig belastet.

- Ein Bürger beschwerte sich darüber, daß seine **Bankverbindung**, die er seiner Wohnsitzgemeinde zum Einzug der Grundsteuer angegeben hatte, von dieser an eine **Gerichtskasse** weitergegeben worden war. Die Gerichtskasse hatte sich im Wege der Amtshilfe zwecks Beitreibung eines gegen den Bürger wegen einer Verkehrsordnungswidrigkeit verhängten Bußgeldes an die Gemeindekasse gewandt. Diese hatte die Bankverbindung des Bürgers mitgeteilt. Daraufhin war von der Gerichtskasse das Konto gepfändet worden.

Das Steuergeheimnis erstreckt sich auf alles, was über eine Person bekanntwerden kann, also die gesamten persönlichen, wirtschaftlichen, rechtlichen, öffentlichen und privaten Verhältnisse einer Person. Unter das Steuergeheimnis fällt damit auch die Bankverbindung eines Grundstückseigentümers, die beim Einzug der gemeindlichen Grundsteuer bekanntgeworden ist. Eine Offenbarung dieser Tatsache ist daher nur unter den Voraussetzungen des § 30 Abs. 4 AO zulässig. Die Voraussetzungen dieser Vorschrift waren jedoch in dem vorliegenden Fall nicht gegeben. Insbesondere bestand keine gesetzliche Offenbarungsbefugnis nach § 30 Abs. 4 Nr. 2 AO.

Die Gemeinde hat in ihrer Stellungnahme die Auffassung vertreten, die Bekanntgabe der Kontonummer an die ersuchende Gerichtskasse sei nach § 11 Abs. 1 Satz 1 DSGVO zulässig gewesen. Auf § 11 Abs. 1 Satz 1 DSGVO kann jedoch im Rahmen des § 30 Abs. 4 Nr. 2 AO schon deshalb nicht zurückgegriffen werden, weil diese Vorschrift die Übermittlung von Daten, die dem Steuergeheimnis unterliegen, nicht ausdrücklich zuläßt. Ich habe daher der Gemeinde empfohlen, künftig in vergleichbaren Fällen von der Mitteilung von Bankverbindungen, die im Steuereinzugsverfahren bekanntgeworden sind, abzusehen. Die Gemeinde wird dieser Empfehlung folgen.

Der Bürger hat auf Grund des geschilderten Vorgangs die der Gemeindekasse erteilte Einzugsermächtigung widerrufen. Da infolgedessen die Kenntnis der Kontodaten für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich war, waren diese Daten auf Verlangen des Betroffenen zu löschen.

### a) Bezirksschornsteinfegermeister

- Ein Oberkreisdirektor verlangte von den Bezirksschornsteinfegermeistern seines Kreises Angaben über die Betreiber von **Flüssiggas-Heizungsanlagen**. Nach § 23 Abs. 2 der Feuerungsverordnung haben Betreiber von Heizungsanlagen, die durch Flüssiggas gespeist werden, Feuerstätten und Leitungsanlagen in Räumen unter Erdgleiche diese in bestimmten Abständen von einem Fachunternehmer auf ordnungsgemäßen Zustand und Dichtheit prüfen zu lassen. Für die Überwachung dieser Prüfungen ist die untere Bauaufsichtsbehörde zuständig. Bei dem zuständigen Oberkreisdirektor waren die Betreiber solcher prüfpflichtigen Anlagen bisher nicht besonders erfaßt. Da er davon ausging, daß die entsprechenden Daten den zuständigen Bezirksschornsteinfegermeistern bekannt sind, hat er diese ersucht, ihm die Daten zu übermitteln.

Der Minister für Wirtschaft, Mittelstand und Technologie hat zu dieser Frage gegenüber dem Landesinnungsverband des Schornsteinfegerhandwerks die Auffassung vertreten, die von dem Oberkreisdirektor verlangte Bekanntgabe der Betreiber von Flüssiggasanlagen verstoße nicht gegen datenschutzrechtliche Vorschriften. Zur Begründung seiner Auffassung verwies er auf die Ausführungen in meinem sechsten Tätigkeitsbericht (C.16.b), in denen ich die Übermittlung von adressenbezogenen Angaben über Feuerungsanlagen durch die Bezirksschornsteinfegermeister zum Zweck der Erstellung eines Hausbrandemissionskatasters nach der 2. Alternative des § 11 Abs. 1 Satz 1 DSGVO für zulässig angesehen habe. Für die hier von den Bezirksschornsteinfegermeistern verlangte Datenübermittlung kann der Auffassung des Ministers jedoch nicht gefolgt werden.

Jeder Eingriff in das Recht auf informationelle Selbstbestimmung bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen muß; aus ihr müssen sich Voraussetzungen und Umfang der Einschränkung des Grundrechts klar und für den Bürger erkennbar ergeben. Es ist zweifelhaft, inwieweit die Generalklauseln der Datenschutzgesetze für sich allein oder in Verbindung mit anderen Rechtsvorschriften als gesetzliche Grundlage für einen Informationseingriff noch herangezogen werden können. Dies gilt insbesondere für Übermittlungsvorschriften, die – wie die 2. Alternative des § 11 Abs. 1 Satz 1 DSGVO – an die rechtmäßige Aufgabenerfüllung des Empfängers anknüpfen, da sie den Verwendungszweck der Daten bei dem Empfänger nicht bestimmen und deshalb den Umfang des Eingriffs für den Bürger nicht erkennen lassen.

Nach meiner Auffassung können nur bei weniger schwerwiegenden Einschränkungen des Rechts auf informationelle Selbstbestimmung auch künftig als Generalklauseln ausgestaltete Auffangnormen in den Datenschutzgesetzen ausreichen. Dies gilt für Übermittlungen etwa dann, wenn die Daten von dem Empfänger für den gleichen Zweck benötigt werden, für den sie von der übermittelnden Stelle erhoben wurden oder gespeichert sind, oder wenn sie nicht personenbezogen verwendet werden sollen. Voraussetzung muß allerdings auch hier sein, daß die Aufgabe, zu deren Erfüllung die Übermittlung erfolgt, durch Gesetz festgelegt ist.

Bei einer stärkeren Belastung des Betroffenen kann eine Datenübermittlung jedoch nur noch dann als zulässig angesehen werden, wenn dafür eine bereichsspezifische gesetzliche Grundlage vorhanden ist. Dies gilt etwa dann, wenn die Daten von dem Empfänger personenbezogen für einen anderen Zweck verwendet werden sollen, insbesondere wenn sie für Maßnahmen

bestimmt sind, die den Betroffenen belasten, oder wenn zwischen der speichernden Stelle und dem Betroffenen ein Vertrauensverhältnis besteht.

Anders als bei der in meinem sechsten Tätigkeitsbericht behandelten Datenübermittlung können die im vorliegenden Fall von den Bezirksschornsteinfegermeistern erbetenen Daten unmittelbar zu belastenden behördlichen Maßnahmen gegen die Betroffenen führen. Die Erstellung eines Hausbrandemissionskatasters ist demgegenüber keine Maßnahme, die den Betroffenen unmittelbar belastet. Im übrigen sprechen das zweckgebundene Zutrittsrecht des Bezirksschornsteinfegermeisters nach § 1 Abs. 3 des Schornsteinfegergesetzes (SchfG) und die insoweit erfolgte Einschränkung des Grundrechts der Unverletzlichkeit der Wohnung für die Annahme eines besonderen Vertrauensverhältnisses.

Eine Übermittlung der von den Bezirksschornsteinfegermeistern erbetenen Angaben über die Betreiber von Flüssiggas-Heizungsanlagen kann daher nicht auf § 11 Abs. 1 Satz 1 DSGVO gestützt werden. Da eine bereichsspezifische gesetzliche Grundlage für die Übermittlung dieser Daten weder im Schornsteinfegergesetz, noch in anderen Rechtsvorschriften enthalten ist, ist diese nicht zulässig.

Auf einen „Übergangsbonus“ bis zur Schaffung einer erforderlichen bereichsspezifischen gesetzlichen Grundlage könnte eine derartige Datenübermittlung nach der Rechtsprechung des Bundesverfassungsgerichts nur gestützt werden, wenn eine bisher schon geübte Verwaltungspraxis fortgesetzt werden soll, um eine sonst eintretende Funktionsunfähigkeit staatlicher Einrichtungen zu vermeiden, die der verfassungsmäßigen Ordnung noch ferner stünde als der bisherige Zustand (BVerfGE 33, 12, 347; 41, 267). Diese Voraussetzung liegt hier nicht vor.

- Gemäß § 23 Abs. 1 Satz 3 SchfG haben in Nordrhein-Westfalen die Regierungspräsidenten in jedem Jahr, dessen Jahreszahl durch fünf teilbar ist, nachzuprüfen, ob die Kehrbezirkseinteilung im Interesse der Feuersicherheit oder der Gleichwertigkeit der Kehrbezirke zu ändern ist. Die Nachprüfung ist ferner in einem kürzeren Zeitraum als fünf Jahre vorzunehmen, wenn besondere Gründe dafür vorliegen. Vor einer Neueinteilung der Kehrbezirke sind der Vorstand und der Gesellenausschuß der Schornsteinfegerinnung zu hören.

Art und Umfang der Einschaltung des **Gesellenausschusses** wird in Nordrhein-Westfalen von den Regierungspräsidenten unterschiedlich gehandhabt. Der Gesellenausschuß einer Schornsteinfegerinnung hat hierzu verlangt, daß ihm vor Einteilungsmaßnahmen in den Kehrbezirken für jeden Kehrbezirk die Kehrbücher oder deren wesentlicher Inhalt zugänglich gemacht werden müßten. Diesem Begehren ist der zuständige Regierungspräsident nicht nachgekommen; er hat dem Gesellenausschuß nur die festgestellten Arbeitswerte in jedem Kehrbezirk mitgeteilt und ansonsten lediglich stichprobenweise Überprüfungen zugelassen.

Diese Verfahrensweise halte ich für richtig. Mit dem Zugänglichmachen von Unterlagen über einen Kehrbezirk werden, soweit dies die Gebühren und Erträge betrifft, personenbezogene Daten des Kehrbezirkseinhabers übermittelt. Es erscheint zweifelhaft, ob und inwieweit § 23 Abs. 1 Satz 3 SchfG als gesetzliche Grundlage für einen derartigen Eingriff herangezogen werden kann. In jedem Fall wird zu fordern sein, daß der Umfang der bekanntgegebenen Daten nach einem strengen Maßstab der Erforderlichkeit beschränkt wird. Das Zugänglichmachen der Kehrbücher oder deren wesentlichen Inhalts kann der Gesellenausschuß nach § 23 Abs. 1 Satz 3 SchfG nicht verlangen, denn für einen derart weitgehenden Eingriff in das informationelle

Selbstbestimmungsrecht des Kehrbezirkseinhabers genügt die Vorschrift nicht dem Gebot der Normenklarheit.

#### b) Industrie- und Handelskammern

- Verschiedene Beratungsersuchen betrafen die Frage, ob die von anderen Behörden erbetene Übermittlung von Daten der **Kammermitglieder** nach den Übermittlungsvorschriften des Datenschutzgesetzes Nordrhein-Westfalen zulässig ist.

In einem Fall war die Vereinigung der Industrie- und Handelskammern des Landes Nordrhein-Westfalen der Auffassung, ihre Mitgliedskammern dürften einem Ersuchen der Gemeinden in ihren Bezirken, ihnen die nach der **Ernährungswirtschaftsmeldeverordnung** meldepflichtigen Betriebe zu benennen, auf der Grundlage des § 11 DSGVO nachkommen. Nach der Verordnung haben die Inhaber bestimmter ernährungswirtschaftlicher Betriebe den Gemeinden verschiedene Angaben über ihren Betrieb zu machen. Die meldepflichtigen Betriebe können im Verteidigungsfall und bei Versorgungskrisen durch Rechtsverordnung angewiesen werden, lebenswichtige Erzeugnisse herzustellen.

In das Grundrecht auf informationelle Selbstbestimmung darf nur auf Grund einer Rechtsvorschrift eingegriffen werden, die dem Gebot der Normenklarheit entspricht. Wie oben (C.18.a) ausgeführt, können nur bei weniger schwerwiegenden Einschränkungen des Rechts auf informationelle Selbstbestimmung die Generalklauseln der Datenschutzgesetze als gesetzliche Grundlage ausreichen. Dies gilt für Übermittlungen etwa dann, wenn die Daten von dem Empfänger für den gleichen Zweck benötigt werden, für den sie von der übermittelnden Stelle erhoben wurden oder gespeichert sind, oder wenn sie nicht personenbezogen verwendet werden sollen. Voraussetzung muß allerdings auch hier sein, daß die Aufgabe, zu deren Erfüllung die Übermittlung erfolgt, durch Gesetz festgelegt ist.

Bei einer stärkeren Belastung des Betroffenen kann eine Datenübermittlung jedoch nur dann als zulässig angesehen werden, wenn dafür eine bereichsspezifische gesetzliche Grundlage vorhanden ist. Dies gilt etwa dann, wenn die Daten von dem Empfänger personenbezogen für einen anderen Zweck verwendet werden sollen, insbesondere wenn sie wie hier für Maßnahmen bestimmt sind, die den Betroffenen belasten.

Da eine bereichsspezifische gesetzliche Grundlage für die Übermittlung der Daten der nach der Ernährungswirtschaftsmeldeverordnung meldepflichtigen Betriebe durch die Industrie- und Handelskammern nicht gegeben ist, bestehen gegen eine solche Datenübermittlung daher datenschutzrechtliche Bedenken, wenn der Inhaber des Betriebes eine natürliche Person ist (§ 2 Abs. 1 DSGVO). Die Voraussetzungen für die Inanspruchnahme eines „Übergangsbonus“ liegen auch in diesem Fall nicht vor.

- In einer weiteren Anfrage bat mich die Vereinigung der Industrie- und Handelskammern um Auskunft, ob sie der Staatskanzlei die Daten der Unternehmen mitteilen dürfe, für die in nächster Zeit ein wichtiges **Firmenjubiläum** heranstünde. Die Staatskanzlei beabsichtigte, diese Firmen besonders zu ehren, und hatte daher um entsprechende Angaben gebeten.

Als gesetzliche Grundlage für die Übermittlung der Daten der Unternehmen, die in nächster Zeit Firmenjubiläen feiern, aus der Datei der Vereinigung der Industrie- und Handelskammern an die Staatskanzlei kommt nur § 11 Abs. 1 Satz 1 DSGVO in Betracht. Danach ist die Übermittlung an öffentliche Stellen zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle (1. Alternative) oder des Empfängers liegenden Aufgaben (2. Alternative) erforderlich ist.

Wie oben dargelegt, können nach meiner Auffassung zwar die Generalklauseln der Datenschutzgesetze bei weniger schwerwiegenden Eingriffen in das Recht auf informationelle Selbstbestimmung als gesetzliche Grundlage auch künftig herangezogen werden. Dabei muß aber zumindest die Aufgabe, zu deren Erfüllung die Übermittlung erfolgt, durch Gesetz normenklar festgelegt sein.

Diese Voraussetzung ist hier nicht erfüllt. Ich halte daher die Übermittlung der Unternehmensdaten, soweit es sich um personenbezogene Daten und nicht um Daten einer juristischen Person handelt, nur mit Einwilligung der Betroffenen für zulässig. Es kann durchaus Betroffene geben, die eine Ehrung nicht wünschen.

- Eine Industrie- und Handelskammer hatte mich gebeten, ihr meine Auffassung zur datenschutzrechtlichen Zulässigkeit der Bitte einer Stadtverwaltung um Überlassung der Anschriften aller der Kammer angehörenden Unternehmen in dieser Stadt mitzuteilen. Die Firmenanschriften sollten für eine Information der Firmen über die Angebote der **städtischen Wirtschaftsförderung** für die heimische Wirtschaft verwendet werden.

Auch hier habe ich die Auffassung vertreten, daß die von der Stadtverwaltung erbetene Datenübermittlung, soweit es sich um personenbezogene Daten handelt, nur mit Einwilligung der Betroffenen zulässig ist.

Die Übermittlung der Unternehmensanschriften kann auch in diesem Fall nicht auf § 11 Abs. 1 Satz 1 DSGVO gestützt werden. Zwar handelt es sich um einen weniger schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung. Die weitere Voraussetzung für eine Anwendung dieser Vorschrift, daß die Aufgabe, zu deren Erfüllung die Übermittlung erfolgt, durch Gesetz normenklar festgelegt sein muß, ist jedoch nicht erfüllt.

Wirtschaftsförderung ist zwar heute ein fester Bestandteil der kommunalen Aufgabenerfüllung. Sie ist aber als Aufgabe im Gesetz nicht ausdrücklich festgelegt und kann nur auf die §§ 1 und 2 der Gemeindeordnung gestützt werden, wonach die Gemeinden das Wohl der Einwohner in freier Selbstverwaltung fördern und in ihrem Gebiet, soweit die Gesetze nicht ausdrücklich etwas anderes bestimmen, ausschließliche und eigenverantwortliche Träger der öffentlichen Verwaltung sind. Diese Umschreibung der Aufgaben der kommunalen Selbstverwaltung ist zu unbestimmt, als daß sie eine Übermittlung personenbezogener Daten auf Grund der Generalklauseln der Datenschutzgesetze noch rechtfertigen könnte.

- Auf Wunsch der Vereinigung der Industrie- und Handelskammern des Landes Nordrhein-Westfalen haben bei mir mehrere Gespräche über datenschutzrechtliche Fragen des neuen **Wirtschafts-Informationssystems** der Industrie- und Handelskammern stattgefunden. Für das Informationssystem sollen Produktdaten und Export/Import-Informationen der den Kammern angehörenden Unternehmen in einer Datenbank gespeichert werden. Die Datenbank soll ab Frühjahr 1986 über Btx bundesweit und über internationale Informationsvermittler (Hosts) weltweit zugänglich gemacht werden.

Zum Aufbau des Informationssystems erhalten die Unternehmen von ihren Kammern einen Erhebungsvordruck, in dem nach den Produkten des Unternehmens gefragt wird. Der Vordruck wird mit einem Begleitschreiben versandt, in dem das Informationssystem näher beschrieben wird.

Ich habe darauf hingewiesen, daß es nach § 10 Abs. 2 Satz 1 DSGVO erforderlich ist, in dem Begleitschreiben einen ausdrücklichen Hinweis auf die Freiwilligkeit der Datenerhebung zu geben. Darüber hinaus habe ich empfohlen, auch in den Kopf des Fragebogens einen Hinweis auf die Freiwilligkeit der Datenerhebung aufzunehmen und die Einwilligungserklä-

rung am Schluß des Fragebogens dahin zu erweitern, daß sie sich nicht nur auf die Datenübermittlung, sondern auch auf die Speicherung der Daten erstreckt.

- Ein Bürger hat sich dagegen gewandt, daß eine Industrie- und Handelskammer Angaben aus seiner **Gewerbeanzeige** unter anderem an Versicherungsgesellschaften weitergegeben hat, obwohl er in die Weitergabe seiner Daten nicht eingewilligt hatte.

Die Kammer hat mir zu dem Vorfall mitgeteilt, daß sie Anschriften und die Art der wirtschaftlichen Tätigkeit von Gewerbetreibenden an andere Gewerbetreibende, die ein berechtigtes Interesse darlegten, zur Anbahnung von Geschäftskontakten weitergebe. Bevor entsprechend verfahren werde, würden alle Gewerbetreibenden nach Eingang der Gewerbeanmeldung angeschrieben und über die beabsichtigte Datenweitergabe informiert. Die Gewerbetreibenden, die die Weitergabe ihrer Daten nicht wünschten, erhielten nach Eingang einer entsprechenden Mitteilung ein Sperrkennzeichen im Datenbestand, durch das eine Datenweitergabe ausgeschlossen sei. Ein solcher Sperrvermerk habe im gegebenen Fall nicht vorgelegen.

Nach dieser Stellungnahme sieht die Kammer eine Weitergabe der Gewerbedaten in den Fällen für zulässig an, in denen die Betroffenen dieser Datenweitergabe nicht widersprochen haben. Dem kann ich jedoch nicht folgen.

Nach § 3 Satz 1 DSGVO ist die Übermittlung personenbezogener Daten an Dritte, soweit sie nicht gesetzlich erlaubt ist, nur zulässig, wenn der Betroffene eingewilligt hat. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist; wird die Einwilligung zusammen mit anderen Erklärungen schriftlich erteilt, ist der Betroffene hierauf schriftlich besonders hinzuweisen (§ 3 Satz 2 DSGVO).

Die von der Kammer angewendete „Widerspruchslösung“ bietet für den Betroffenen keinen gleichwertigen Schutz wie eine nach den genannten Vorschriften eingeholte Einwilligungserklärung. Die Schutzwirkung dieser Vorschriften besteht darin, daß die Zulässigkeit der Datenübermittlung im Gegensatz zur Widerspruchslösung von einem Tätigwerden des Betroffenen abhängig gemacht wird. Aus diesem Grunde halte ich die Übermittlung von Angaben aus der Gewerbeanmeldung zum Zwecke der Geschäftsanbahnung nur mit ausdrücklicher Einwilligung des Betroffenen für zulässig.

### c) Handwerkskammern und Innungen

- Von einer Handwerkskammer bin ich um Stellungnahme zu der Frage gebeten worden, ob es zulässig ist, daß der Deutsche Handwerkskammertag (DHKT) die bei den Handwerkskammern vorliegenden Anmeldungen zur **Zahntechniker-Meisterprüfung** zentral erfaßt, um zu einer besseren Koordinierung der Anmeldungen zu gelangen. Mit dieser Maßnahme soll herausgefunden werden, wie die ungewöhnlich hohe Zahl der Anmeldungen, die bei einigen Handwerkskammern ganz erhebliche Wartezeiten verursacht, zustande kommt. Es wird vermutet, daß die Zahl der Anmeldungen künstlich aufgebläht ist. Viele Bewerber würden sich für die Ablegung der Meisterprüfung bei verschiedenen Handwerkskammern gleichzeitig anmelden oder nach Ablegung der Prüfung die mehrfach vorgenommenen Anmeldungen nicht rückgängig machen. Die Untersuchung hätte keinerlei belastende Folgen für die Bewerber. Vielmehr könne ihre Prüfungssituation verbessert werden.

Der DHKT ist eine Vereinigung der Handwerkskammern im Bundesgebiet. Nach dem Sitzlandprinzip finden auf seine Datenverarbeitung die für Vereini-

gungen der Aufsicht des Landes unterstehender juristischer Personen des öffentlichen Rechts geltenden Vorschriften des Datenschutzgesetzes Nordrhein-Westfalen Anwendung (§ 1 Abs. 2 Satz 1 DSGVO).

Nach § 10 Abs. 1 DSGVO dürfen personenbezogene Daten gespeichert werden, wenn es zur rechtmäßigen Erfüllung der in der Zuständigkeit der speichernden Stelle liegenden Aufgaben erforderlich ist. Der DHKT hat nach § 2 Satz 1 seiner Satzung die Aufgabe, die gemeinsamen Angelegenheiten der ihm angehörenden Kammern zu vertreten und alle gemeinsamen Aufgaben wahrzunehmen, die den Kammern übertragen sind. Die zuständigen Handwerkskammern haben nach § 91 Abs. 1 Nr. 6 in Verbindung mit § 47 der Handwerksordnung (HwO) die Aufgabe, die Geschäfte der Meisterprüfungsausschüsse zu führen. Zur Geschäftsführung eines Prüfungsausschusses gehört es auch, durch geeignete organisatorische Maßnahmen einen zügigen Prüfungsablauf zu gewährleisten. Soweit dafür eine über den Zuständigkeitsbereich der einzelnen Kammer hinausgehende Koordinierung erforderlich ist, kann die zentrale Erfassung der Anmeldungen zur Meisterprüfung als eine Aufgabe des DHKT im Sinne des § 2 Satz 1 der Satzung angesehen werden. Zur Durchführung der beabsichtigten Untersuchung erscheint es erforderlich, die bei den Handwerkskammern vorliegenden Anmeldungen zur Zahntechniker-Meisterprüfung zentral zu erfassen.

Die Übermittlung der Daten aus den Anmeldungen zur Meisterprüfung durch die meiner Kontrolle unterliegenden Handwerkskammern an den DHKT kann auf § 11 Abs. 1 Satz 1 DSGVO gestützt werden; aus den vorstehenden Erwägungen kann sie als zur rechtmäßigen Erfüllung der Aufgaben der Handwerkskammern wie auch des DHKT erforderlich angesehen werden. Eine Zweckentfremdung der Daten ist mit dieser Maßnahme, die der Verbesserung des Prüfungsverfahrens dienen soll, nicht verbunden. Sie führt auch nicht zu einer Belastung der Betroffenen.

Nach dem derzeitigen Erkenntnisstand habe ich daher gegen die zentrale Erfassung der Anmeldungen zur Meisterprüfung im Zahntechniker-Handwerk keine durchgreifenden datenschutzrechtlichen Bedenken.

- Eine Innung für das Gebäudereiniger-Handwerk hat bei mir angefragt, ob bei der Innung eine zentrale Datei der bei den Innungsmitgliedern **sozialversicherungsfrei beschäftigten Mitarbeiter** angelegt werden darf. Mit Hilfe dieser Datei sollen Erkenntnisse darüber gewonnen werden, ob solche Mitarbeiter bereits in einer anderen Reinigungsfirma einer versicherungsfreien Beschäftigung nachgehen. Nach dem Sozialversicherungsrecht hängt die Versicherungsfreiheit eines Beschäftigungsverhältnisses von der Höhe des Monatseinkommens aus allen Beschäftigungsverhältnissen und den insgesamt geleisteten Arbeitsstunden ab. In der Vergangenheit sei bei Firmenprüfungen durch Sozialversicherungsträger verschiedentlich festgestellt worden, daß versicherungsfrei geführte Arbeitnehmer auch bei anderen Reinigungsfirmen beschäftigt waren, obwohl die Betroffenen bei ihrer Einstellung schriftlich erklärt hätten, keiner weiteren Beschäftigung nachzugehen. In solchen Fällen hätten die Arbeitgeber zum Teil erhebliche Beträge an die Sozialversicherungsträger nachentrichten müssen.

Für die Errichtung einer zentralen Datei der bei den Innungsmitgliedern sozialversicherungsfrei geführten Mitarbeiter durch die Innung ist eine dem Gebot der Normenklarheit entsprechende gesetzliche Grundlage nicht ersichtlich. Die Vorschriften des § 54 Abs. 1 Satz 1 HwO und des § 3 Abs. 2 Nr. 1 Abs. 4 der Satzung der Innung des Gebäudereiniger-Handwerks können hierfür nicht herangezogen werden. Darin wird der Innung insbesondere die Aufgabe zugewiesen, die gemeinsamen gewerblichen Interessen ihrer Mitglieder zu fördern. Diese allgemein gehaltenen Aufgabenzuweisungen

lassen nicht mit genügender Deutlichkeit erkennen, daß das geplante Vorhaben zu den gesetzlichen oder satzungsmäßigen Aufgaben der Innung gehört und zu seiner Durchführung personenbezogene Daten von Mitarbeitern durch die Innung erhoben und gespeichert werden dürfen.

Ich habe daher die Innung darauf hingewiesen, daß gegen das geplante Vorhaben nach dem derzeitigen Erkenntnisstand datenschutzrechtliche Bedenken bestehen, sofern nicht von den betroffenen Mitarbeitern eine wirksame Einwilligung zur Speicherung ihrer Daten bei der Innung eingeholt wird. Es wäre nach meiner Ansicht keine unangemessene Benachteiligung, wenn der Abschluß eines Arbeitsvertrages von der Erteilung einer solchen Einwilligung abhängig gemacht würde.

## 19. Verkehrswesen

### a) Fahrerlaubnis

- Mehrere Eingaben betrafen die Erhebung von Angaben über den **Gesundheitszustand** des Antragstellers für eine Fahrerlaubnis.

Ein Bürger trug vor, er habe bei der örtlich zuständigen Behörde die Erweiterung seiner Fahrerlaubnis von Klasse 2 und 3 auf Klasse 1 beantragt. Die in dem Antrag auf Erweiterung der Fahrerlaubnis enthaltenen Fragen über den Gesundheitszustand habe er nicht beantwortet, da er diese Fragen nicht für zulässig hielt. Abgesehen davon sah er sich zur Verweigerung der Auskünfte berechtigt, da im Kopf des Fragebogens folgender Hinweis enthalten ist: „Zur Beantwortung der nachstehenden Fragen bin ich nicht verpflichtet. Von Amts wegen können jedoch im Rahmen des Untersuchungsgrundsatzes (§ 26 Abs. 1 VwVfG NW) weitere Ermittlungen durchgeführt werden.“ Wegen seiner Weigerung, die Gesundheitsfragen zu beantworten, habe ihm die Führerscheinstelle mitgeteilt, er habe ein amtsärztliches Gutachten vorzulegen. Andernfalls müsse er als ungeeignet angesehen und ihm die beantragte Fahrerlaubnis versagt werden. Der Bürger bat mich um datenschutzrechtliche Prüfung dieses Vorgehens der Behörde.

Das Recht auf informationelle Selbstbestimmung gewährleistet die Befugnis des einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts bedürfen einer gesetzlichen Grundlage. Das gleiche gilt für das Grundrecht auf Schutz der personenbezogenen Daten nach Artikel 4 Abs. 2 der Landesverfassung.

Gesetzliche Grundlage für die Datenerhebung bei der Erteilung von Fahrerlaubnissen ist § 2 Abs. 1 Satz 2 des Straßenverkehrsgesetzes (StVG) und § 9 Satz 1 der Straßenverkehrs-Zulassungs-Ordnung (StVZO) in Verbindung mit §§ 24 und 26 des Verwaltungsverfahrensgesetzes für das Land Nordrhein-Westfalen (VwVfG NW).

Nach § 2 Abs. 1 Satz 2 StVG setzt die Erteilung der Fahrerlaubnis voraus, daß keine Tatsachen vorliegen, die die Annahme rechtfertigen, daß der Antragsteller zum Führen von Kraftfahrzeugen ungeeignet ist. Die Eignung kann unter anderem wegen Neigung zum Trunk oder zur Rauschgiftsucht sowie durch körperliche oder geistige Mängel beschränkt oder ausgeschlossen sein (§ 9 Satz 1 StVZO).

Nach § 24 Abs. 1 VwVfG NW ermittelt die Behörde den Sachverhalt von Amts wegen; sie bestimmt Art und Umfang der Ermittlungen. Nach § 26 Abs. 1 VwVfG NW bedient sich die Behörde der Beweismittel, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält; sie

kann unter anderem Auskünfte jeder Art und die schriftliche Äußerung von Beteiligten einholen. Nach § 26 Abs. 2 VwVfG NW sollen die Beteiligten bei der Ermittlung des Sachverhalts mitwirken. Sie sollen insbesondere ihnen bekannte Tatsachen angeben. Eine weitergehende Pflicht, bei der Ermittlung des Sachverhalts mitzuwirken, insbesondere eine Pflicht zur Aussage, besteht nur, wenn sie durch Rechtsvorschrift besonders vorgesehen ist; dies ist bei der Erteilung der Fahrerlaubnis nicht der Fall.

Nach den genannten Vorschriften darf die Behörde Ermittlungen über den Gesundheitszustand des Antragstellers durchführen. Hierzu darf sie dem Antragsteller in dem Antragsvordruck Fragen zu seinem Gesundheitszustand stellen, soweit diese für die Eignung zum Führen von Kraftfahrzeugen erheblich und für den Betroffenen nicht unzumutbar sind. Dabei ist zu berücksichtigen, daß die Prüfung der Eignung zum Führen von Kraftfahrzeugen dem Schutz hochrangiger Rechtsgüter wie des Lebens und der Gesundheit anderer Verkehrsteilnehmer dient.

Eine Verpflichtung des Antragstellers zur Beantwortung der Fragen über seinen Gesundheitszustand besteht nach § 26 Abs. 2 VwVfG NW nicht. Allerdings muß er bei Nichtbeantwortung damit rechnen, daß die Behörde weitere Ermittlungen durchführen wird.

Soweit durch die Beantwortung der Fragen zum Gesundheitszustand 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 Gutachtens fordern (§ 12 Abs. 1 Satz 1 StVZO). Allein die Weigerung des Antragstellers, die Fragen zu beantworten, läßt nach meiner Auffassung allerdings nicht den Schluß zu, daß Bedenken gegen seine Eignung bestehen. Die Nichtbeantwortung allein kann daher nicht Anlaß für das Verlangen der Behörde zur Vorlage eines amts- oder fachärztlichen Gutachtens sein. Eine derartige Maßnahme wäre nur bei konkreten Anhaltspunkten, die Bedenken gegen die Eignung begründen, gerechtfertigt.

Allerdings könnte erwogen werden, ob die Behörde im Rahmen ihrer Ermittlungen dem Antragsteller anbieten sollte, daß er an Stelle der Beantwortung der Fragen zum Gesundheitszustand auch ein ärztliches (oder nach Wahl des Betroffenen ein amtsärztliches) Zeugnis vorlegen kann. Ein solches ärztliches Zeugnis hätte sich im Gegensatz zu einem amtsärztlichen oder fachärztlichen Gutachten auf die Aussage zu beschränken, daß der Antragsteller geistig und körperlich uneingeschränkt oder nur eingeschränkt zum Führen von Kraftfahrzeugen geeignet ist und gegebenenfalls welche Einschränkung vorliegt. Wird eine derartige Einschränkung festgestellt, kann es geboten sein, in dem Zeugnis die der Einschränkung zugrunde liegenden ärztlichen Befunde aufzuführen.

Sofern die Behörde diesen Weg der Prüfung der Eignung wählt, bleibt aber die Frage, ob die Weigerung der Vorlage des Zeugnisses für die Behörde der alleinige Anlaß sein darf, den Bewerber als ungeeignet zum Führen von Kraftfahrzeugen anzusehen und ihm deshalb die beantragte Fahrerlaubnis zu versagen.

Ich habe hierzu den Minister für Stadtentwicklung, Wohnen und Verkehr um Stellungnahme gebeten. Dieser hat mir mitgeteilt, daß er keine Bedenken habe, wenn der Führerscheinbewerber seine Kraftfahrtauglichkeit durch Vorlage einer ärztlichen Bescheinigung nachweist. Im übrigen bereite der Bundesminister für Verkehr eine gesetzliche Regelung unter Berücksichtigung datenschutzrechtlicher Belange vor, die auch die Frage nach dem Gesundheitszustand des Fahrerlaubnisbewerbers einschließe.

- Ein Vormundschaftsgericht hat sich an mich gewandt, weil es die derzeitige Praxis der Straßenverkehrsämter, zur Beurteilung der Eignung zum Führen von Kraftfahrzeugen die **Vormundschafts- und Pflegschaftsakten** der Gerichte anzufordern, für datenschutzrechtlich bedenklich hält. Die Straßenverkehrsämter würden die Aktenanforderung nicht näher begründen, so daß der zuständige Richter nicht prüfen könne, welche Gesichtspunkte für diesen Schritt maßgeblich seien. Die Folge wäre, daß die angeforderten Akten in der Regel ohne eine Prüfung der schutzwürdigen Belange der Betroffenen durch die Gerichte übersandt würden.

In meinem dritten (C.16.a), vierten (C.18.a) und fünften Tätigkeitsbericht (C.19.a) habe ich meine datenschutzrechtliche Beurteilung zur Übermittlung von Erkenntnissen und Unterlagen an die zuständige Verwaltungsbehörde zur Beurteilung der Eignung zum Führen von Kraftfahrzeugen dargelegt. In den dort behandelten Fällen ist als gesetzliche Grundlage, die für den Eingriff in das Grundrecht des Betroffenen auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung erforderlich ist, § 4 Abs. 1 StVG und § 15b Abs. 1 StVZO herangezogen worden. Nach diesen Vorschriften hat die Straßenverkehrsbehörde die Fahrerlaubnis zu entziehen, wenn sich der Inhaber der Fahrerlaubnis zum Führen von Kraftfahrzeugen als ungeeignet erweist. Um eine solche Entscheidung treffen zu können, ist das Straßenverkehrsamt auf die Kenntnis derartiger Sachverhalte angewiesen.

Die Anfrage des Vormundschaftsgerichts sowie mehrere Beschwerden von Bürgern über die Weitergabe von Verfahrensakten durch die Justiz an die Straßenverkehrsämter geben jedoch Veranlassung, die bisherige datenschutzrechtliche Beurteilung solcher Datenweitergaben unter Berücksichtigung des Urteils des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 zu überprüfen.

Das Bundesverfassungsgericht hat in diesem Urteil dargelegt, das Grundrecht auf informationelle Selbstbestimmung dürfe nur im überwiegenden Allgemeininteresse durch eine verfassungsgemäße gesetzliche Grundlage eingeschränkt werden, die dem rechtsstaatlichen Gebot der Normenklarheit entsprechen muß. Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten. Auch hat er organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken.

Nach diesen Grundsätzen können bei der Beurteilung der Eignung zum Führen von Kraftfahrzeugen die Vorschriften des § 4 Abs. 1 StVG, § 15b Abs. 1 StVZO nach meiner Auffassung nicht mehr als ausreichende gesetzliche Grundlage für eine zweckentfremdete Verwendung der personenbezogenen Daten, die in anderen Bereichen staatlichen Handelns über den Betroffenen gesammelt worden sind, angesehen werden. Hierfür ermangelt es § 4 Abs. 1 StVG und § 15b Abs. 1 StVZO bereits an der erforderlichen Normenklarheit. Das Gebot der Normenklarheit verlangt, daß sich aus der Gesetzesvorschrift die Voraussetzungen und der Umfang der Einschränkung klar und für den Bürger erkennbar ergeben (BVerfGE 65, 1, 44). In den hier angesprochenen Fällen geht es meist um sehr sensible Daten, zum Beispiel aus Unterbringungsverfahren nach dem Psychischkrankengesetz, aus Verfahren wegen Anordnung einer Pflegschaft oder Entmündigung oder aus Strafverfahren. Der Eingriff in das Recht des Betroffenen auf informationelle Selbstbestimmung, der sich aus einer Verwertung dieser Erkenntnisse für andere Verwaltungszwecke ergibt, ist daher besonders einschneidend. Vorschriften, die lediglich Aufgabenzuweisungen ohne Regelung der für die Erfüllung der Aufgabe erforderlichen Befugnisse zu Informationseingriffen enthalten, wie § 4 Abs. 1 StVG und § 15b Abs. 1 StVZO, können als gesetzliche Grundlage für solche Eingriffe nicht mehr ausreichen. Auch Vorschriften

über ein Akteneinsichtsrecht wie § 34 Abs. 1 FGG und § 299 Abs. 2 ZPO, soweit sie in entsprechender Anwendung für Datenübermittlungen an öffentliche Stellen herangezogen werden, entsprechen nach meiner Auffassung nicht den vom Bundesverfassungsgericht aufgestellten Anforderungen.

Bereits die fehlende Normenklarheit der Vorschriften erfordert hier nach meiner Auffassung ein Tätigwerden des Gesetzgebers. Aber auch unabhängig hiervon erscheint es mit Rücksicht auf die Erheblichkeit des Eingriffs in das Recht auf informationelle Selbstbestimmung bei einer Übermittlung von personenbezogenen Daten etwa aus Unterbringungsverfahren nach dem Psychischkrankengesetz oder aus Pflegschafts- und Entmündigungsverfahren geboten, daß der Gesetzgeber diesen Komplex neu regelt.

Für eine begrenzte Übergangszeit könnten nach der Rechtsprechung des Bundesverfassungsgerichts (BVerfGE 33, 12, 347; 41, 267) § 4 Abs. 1 StVG und § 15b Abs. 1 StVZO in bestimmten Fällen weiterhin als gesetzliche Grundlage für die Übermittlung von Erkenntnissen und Unterlagen an die zuständige Verwaltungsbehörde zur Beurteilung der Eignung zum Führen von Kraftfahrzeugen herangezogen werden. Hierzu muß jedoch nach meiner Auffassung zumindest durch entsprechende Verwaltungsvorschriften sichergestellt sein, daß eine Berücksichtigung des Persönlichkeitsrechts des Betroffenen soweit wie möglich gewährleistet und dieses nur nach sorgfältiger Abwägung mit dem Allgemeininteresse zugunsten eines höherrangigen Rechtsguts zurückgestellt wird.

Eine solche vorläufige Regelung durch Verwaltungsvorschriften erscheint mir insbesondere vordringlich für Ersuchen der für die Entziehung der Fahrerlaubnis zuständigen Behörde auf Gewährung von Einsicht in Verfahrensakten im Wege der Amtshilfe. Dabei müßte nach meiner Auffassung auch vorgesehen sein, daß dem Betroffenen in der Regel zuvor Gelegenheit gegeben wird, sich zur beabsichtigten Akteneinsicht zum Zweck der Beurteilung seiner Eignung zur Führung von Kraftfahrzeugen zu äußern. Auf jeden Fall ist sicherzustellen, daß die erlangten Daten unter strikter Beachtung des Erforderlichkeitsgrundsatzes nur bei Vorliegen besonders gewichtiger Gründe zum Zwecke der Beurteilung der Eignung zum Führen von Kraftfahrzeugen übermittelt werden.

- Die Bundesregierung hat einen Gesetzentwurf zur Änderung des Straßenverkehrsgesetzes (Bundestagsdrucksache 10/4490) zur Beratung vorgelegt, der die Rechtsgrundlage für die Einführung eines **Führerscheins auf Probe** für Fahranfänger schaffen soll. Darin ist vorgesehen, daß sich jeder Fahranfänger in den ersten zwei Jahren nach Erwerb der Fahrerlaubnis besonders zu bewähren hat. Diese Zeit soll deshalb als Probezeit gelten. Von mangelnder Bewährung eines Fahranfängers wird ausgegangen, wenn dieser während der Probezeit erhebliche oder wiederholte Verkehrsverstöße begeht. Die Verkehrsverstöße werden zu diesem Zweck nach ihrer Schwere gewichtet. Bei Nichtbewährung innerhalb der Probezeit sind – je nach Häufigkeit der begangenen Verkehrsverstöße – als Maßnahmen die Teilnahme an einem Nachschulungskurs, die Wiederholung der theoretischen Fahrerlaubnisprüfung oder die Beibringung eines medizinisch-psychologischen Eignungsgutachtens vorgesehen. Zur Teilnahme an einem Nachschulungskurs soll beispielsweise bereits derjenige verpflichtet sein, der innerhalb der Probezeit eine gewichtige oder zwei einfachere Verkehrsverstöße begangen hat. Die Maßnahmen sollen von den örtlichen Straßenverkehrsbehörden veranlaßt und über das Verkehrszentralregister des Kraftfahrt-Bundesamtes (KBA) gesteuert werden. Zu diesem Zweck ist vorgesehen, beim KBA ein Register der Fahranfänger für die Dauer der Probezeit zu führen. Durch Abgleich mit diesem Register wird bei der Eintragung eines Verkehrsverstoßes in das Verkehrszentralregister festgestellt, ob die einzutragende Straftat oder Ver-

kehrordnungswidrigkeit von einem Fahranfänger innerhalb der Probezeit begangen wurde. In diesen Fällen erfolgt von Amts wegen eine Unterrichtung der zuständigen Straßenverkehrsbehörde.

Die Speicherung der Daten der Führerscheineulinge beim KBA ist ein Eingriff in das Grundrecht der Betroffenen auf Datenschutz und in ihr Recht auf informationelle Selbstbestimmung. Der Gesetzgeber muß entscheiden, ob er einen solchen Eingriff im überwiegenden Interesse der Allgemeinheit für geboten hält. Hierbei ist zu prüfen, ob der Zweck – nämlich frühzeitig das Fahrverhalten noch nicht geeigneter Führerscheininhaber durch abgestufte Maßnahmen zu verbessern – gegenüber dem Datenschutzinteresse des Betroffenen überwiegt.

Die mit dem Gesetzentwurf beabsichtigte Wirkung hängt wesentlich davon ab, daß die Nachschulung wie auch die weiteren Maßnahmen möglichst „der Tat auf dem Fuße folgend“ angeordnet werden, weil erfahrungsgemäß dann die Motivation für eine Änderung der Einstellung und des Verhaltens zu einer unauffälligen, risikolosen Verkehrsteilnahme am stärksten ist. Diese Grundsätze können nur verwirklicht werden, wenn das Kraftfahrt-Bundesamt eindeutig und in jedem Fall einer Eintragung in das Verkehrszentralregister feststellen kann, ob die Zuwiderhandlung von einem Fahranfänger während der Probezeit begangen wurde, und wenn die für die Anordnung der Nachschulung oder der weiteren Maßnahmen zuständige Behörde schnell unterrichtet wird. Dies setzt voraus, daß das Kraftfahrt-Bundesamt Angaben über alle Fahranfänger speichert.

Ein besseres Verfahren, um die frühzeitige Nachschulung zu erreichen, ist bisher nicht bekannt. Es wurden zwar andere Verfahren vorgeschlagen, bei denen auf die Speicherung von Daten aller Fahranfänger verzichtet werden kann. Diese Verfahren haben jedoch Nachteile. Wenn nach dem einen Vorschlag die Eignung des Fahranfängers erst nach Ablauf der Probezeit überprüft wird, wird die Wirkung einer frühzeitigen Nachschulung bereits nach den ersten Verstößen nicht erreicht. Nach dem anderen Vorschlag sind umfangreiche Nachermittlungen über den Zeitpunkt der Erteilung des Führerscheins notwendig, wenn bei einem Verstoß der Führerschein nicht vorgelegt wird. Der erste Vorschlag ist mit dem Zweck des Gesetzesvorhabens nicht vereinbar, und gegen die Nachermittlungen bestehen datenschutzrechtliche Bedenken. Denn diese Ermittlungen können für die Betroffenen belastender sein, als eine Speicherung aller Führerscheininhaber auf Probe in einer Datei.

#### **b) Kraftfahrzeugzulassung**

Der von den Fraktionen der CDU/CSU und der FDP im Deutschen Bundestag eingebrachte Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes, des Verwaltungsverfahrensgesetzes, des Bundesverfassungsschutzgesetzes und des Straßenverkehrsgesetzes (Bundestagsdrucksache 10/4737) enthält Regelungen über die Verarbeitung der bei der Kraftfahrzeugzulassung erhobenen Daten in den örtlichen Fahrzeugregistern und in dem beim KBA in Flensburg geführten Zentralen Fahrzeugregister einschließlich der Nutzung dieser Daten im Rahmen des von dem KBA entwickelten „Zentralen Verkehrs-Information-Systems (ZEVIS)“. Zu einem früheren Entwurf für solche Regelungen habe ich in meinem sechsten Tätigkeitsbereich (C.17.a) Stellung genommen.

Die Schaffung gesetzlicher Grundlagen für die Register beim KBA und bei den örtlichen Zulassungsstellen ist grundsätzlich zu begrüßen; sie entspricht langjährigen Forderungen der Datenschutzbeauftragten und ist nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 unab-

weisbar geworden. Gegen die in dem Gesetzentwurf vorgesehenen Regelungen bestehen jedoch in einigen wesentlichen Punkten Bedenken.

Wie im sechsten Tätigkeitsbericht dargelegt, ist insbesondere bedenklich, daß der Gesetzentwurf die automatisierte Erschließung der im Zentralen Fahrzeugregister gespeicherten Daten über die Personalien der Kraftfahrzeughalter durch Polizeidienststellen ohne sachliche und regionale Beschränkung zuläßt (P-Anfrage). Ebenso müssen die aufgeführten Bedenken gegen den vorgesehenen Fahndungsabgleich sowie gegen die Übermittlung der Daten zur Durchsetzung beliebiger, nicht verkehrsbezogener Ansprüche öffentlich-rechtlicher Natur (nunmehr allerdings oberhalb einer Bagatellgrenze von 1 000 Deutsche Mark) aufrechterhalten werden.

Die vorgesehene Einsichtnahme der Polizei in die örtlichen Fahrzeugregister („Schlüssellösung“) ist als Dauerregelung nicht vertretbar, da der Umfang der Einsichtnahme praktisch nicht kontrollierbar ist. Außerhalb der Dienststunden der örtlichen Zulassungsstelle kann die Polizei die für ihre Aufgabenerfüllung notwendigen Informationen in eilbedürftigen Fällen beim KBA einholen. Erforderlichenfalls sind die dafür notwendigen Voraussetzungen beim KBA zu schaffen.

### c) Personenbeförderung

- Ein Taxiunternehmer hat mich um datenschutzrechtliche Prüfung der Praxis des Genehmigungsverfahrens für die Ausübung des Gelegenheitsverkehrs mit Taxen (Kraftdroschken) nach dem Personenbeförderungsgesetz (PBefG) gebeten. Er wendet sich dagegen, daß durch die vor der Entscheidung über den Antrag zu hörende **Industrie- und Handelskammer** eine unzulässige Ausforschung der Verhältnisse des Antragstellers erfolge. Insbesondere dürfe sie anläßlich der Anhörung die Antragsteller nicht routinemäßig zu einem Gespräch einladen. Falls ein Erscheinen des Antragstellers gewünscht werde, müsse die Kammer auf die Freiwilligkeit seiner Teilnahme an dem Gespräch hinweisen.

Nach § 14 Abs. 1 Nr. 5 PBefG ist vor der Entscheidung über den Antrag auf Erteilung der Genehmigung zum Gelegenheitsverkehr mit Personenkraftwagen nach den §§ 47, 48, 49 Abs. 4 PBefG unter anderem die für den Betriebssitz des Unternehmers zuständige Industrie- und Handelskammer gutachtlich zu hören.

Obwohl die Voraussetzungen für die Genehmigung in erster Linie vom Antragsteller gegenüber der Genehmigungsbehörde darzulegen sind (vgl. auch § 12 Abs. 2 PBefG), muß davon ausgegangen werden, daß sich die Stellungnahme der Industrie- und Handelskammer auf alle Tatsachen und rechtlichen Gesichtspunkte erstrecken kann, die für die Erteilung oder Versagung der beantragten Genehmigung wesentlich sind oder wesentlich sein können, insbesondere also auf die für die Beurteilung der Voraussetzungen des § 13 Abs. 1 Satz 1 PBefG einschlägigen Gesichtspunkte (vgl. Bidinger, Personenbeförderungsgesetz, 2. Aufl., § 14 Anm. 3). Denn der Zweck des Anhörungsverfahrens ist es, der Genehmigungsbehörde eine verbreiterte sachliche Grundlage für die Beurteilung des Antrags im Hinblick auf die personellen und betrieblichen Voraussetzungen sowie die öffentlichen Verkehrsinteressen zu geben.

Dabei ist davon auszugehen, daß die Industrie- und Handelskammer im Anhörungsverfahren in erster Linie gehalten ist, ihr bekannte Tatsachen über den Antragsteller der Genehmigungsbehörde mitzuteilen. Inwieweit darüber hinaus die Industrie- und Handelskammer im Anhörungsverfahren eigene Ermittlungen vornehmen und dabei den Antragsteller zu einem Gespräch bitten darf, richtet sich nach dem Verhältnismäßigkeitsgrundsatz. Jedenfalls

darf die Teilnahme an einem solchen Gespräch und die Beantwortung dabei gestellter Fragen durch den Antragsteller nur auf freiwilliger Grundlage erfolgen. Hierauf muß von der Industrie- und Handelskammer bei der Einladung zu dem Gespräch nach § 10 Abs. 2 Satz 1 DSG NW unmißverständlich hingewiesen werden.

Im übrigen sind nach dem Verhältnismäßigkeitsgrundsatz eigene Ermittlungen der Industrie- und Handelskammer dann unzulässig, wenn sie zu einer unter den gegebenen Umständen unzumutbaren Belastung des Antragstellers führen. Danach wird die Einladung zu einem Anhörungsgespräch bei der Wiedererteilung von Genehmigungen nicht regelmäßig in Frage kommen.

- In der gleichen Beschwerde wurde die Zulässigkeit der Erhebung von **Angaben über das Vermögen** des Antragstellers in einer Beilage zum Antrag auf Erteilung der Genehmigung für einen Verkehr nach dem Personenbeförderungsgesetz bezweifelt.

Der von der Genehmigungsbehörde verwendete Vordruck entspricht im wesentlichen dem Formular, das vom Bundesminister für Verkehr zusammen mit den zuständigen obersten Landesbehörden für den entgeltlichen oder geschäftsmäßigen Straßenpersonenverkehr entwickelt worden ist (Verkehrsblatt 1981 S. 299). Dieser als Empfehlung gefaßte Erlaß des Bundesministers für Verkehr ist selbst keine Rechtsgrundlage für die Datenerhebung. Als gesetzliche Grundlage der in dem Vordruck vorgesehenen Datenerhebung kommen die Vorschriften des Personenbeförderungsgesetzes in Betracht.

Nach § 13 Abs. 1 Nr. 1 PBefG darf die Genehmigung für einen Verkehr nach dem Personenbeförderungsgesetz nur erteilt werden, wenn die Sicherheit und die Leistungsfähigkeit des Betriebs gewährleistet sind. Der Grund dafür, daß der Gesetzgeber in § 13 Abs. 1 Nr. 1 PBefG die Sicherheit und Leistungsfähigkeit des Betriebs zur Genehmigungsvoraussetzung macht, ist auch darin zu sehen, daß bei Nichtvorliegen dieser Voraussetzungen Nachteile bei der Ausübung des Gewerbes, etwa durch einen mangelhaften Wartungs- und Sicherheitszustand der Fahrzeuge zu befürchten sind.

Zur Prüfung dieser Voraussetzungen sind dem Genehmigungsantrag Unterlagen beizufügen, die ein Urteil über die Sicherheit und Leistungsfähigkeit des Betriebs ermöglichen (§ 12 Abs. 2 PBefG). Zu der Erhebung von Angaben über die Sicherheit und Leistungsfähigkeit des Betriebs hat das Oberverwaltungsgericht Münster in seiner Entscheidung (OVG Münster in Verkehrsrecht-Sammlung 29, 388) klargestellt, daß der Bewerber um eine Verkehrsgenehmigung darzutun und zu belegen hat, daß ihm das für die Betriebseinrichtung und Betriebsfortführung erforderliche Kapital auch tatsächlich zur Verfügung steht.

Es besteht jedoch keine gesetzliche Verpflichtung eines Antragstellers, die Beilage auszufüllen. Denn eine solche Verpflichtung des Bürgers zur Angabe bestimmter personenbezogener Daten kann nach dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 nur dann aus einer gesetzlichen Vorschrift hergeleitet werden, wenn diese dem Gebot der Normenklarheit entspricht. Danach muß der Bürger aus der Vorschrift selbst ersehen können, welche Daten von ihm anzugeben sind. Diese Voraussetzung erfüllen die §§ 12 Abs. 2 und 13 Abs. 1 Nr. 1 PBefG im Hinblick auf die Daten der Beilage nicht. Durch § 12 Abs. 2 PBefG wird lediglich festgelegt, daß es dem Antragsteller obliegt, über die allgemeine Mitwirkungspflicht nach § 26 Abs. 2 VwVG NW hinaus solche Unterlagen beizubringen, die ein Urteil über die Sicherheit und Leistungsfähigkeit des Betriebs ermöglichen. Will er dafür nicht die Beilage ausfüllen, so hat er andere Unterlagen vorzulegen, die ein Urteil der Genehmigungsbehörde über die Sicherheit und Leistungsfähigkeit seines Betriebs ermöglichen. Die Genehmigungsbehörde, die nach dem

Verwaltungsverfahrensgesetz den Sachverhalt von Amts wegen ermittelt (§ 24 Abs. 1 VwVfG NW) und sich dabei der Beweismittel bedient, die sie nach pflichtgemäßem Ermessen zur Ermittlung des Sachverhalts für erforderlich hält (§ 26 Abs. 1 VwVfG NW), hat den Antragsteller gegebenenfalls darauf hinzuweisen, durch welche andere Unterlagen dies erfolgen kann.

Wie auch durch die Eingabe deutlich geworden ist, bestehen über die Rechtslage für das Ausfüllen der Beilage zum Antrag auf Erteilung der Genehmigung für einen Verkehr nach dem Personenbeförderungsgesetz Unklarheiten. Ich habe daher dem Minister für Stadtentwicklung, Wohnen und Verkehr empfohlen, gemäß § 10 Abs. 2 Satz 1 DSGVO in der Beilage auf die Rechtsgrundlage der Datenerhebung sowie darauf hinzuweisen, daß die Beilage nur eine von der Behörde angebotene Form für die Ermittlung der gesetzlichen Voraussetzungen für die Erteilung eines Verkehrs nach dem Personenbeförderungsgesetz ist, daß aber eine gesetzliche Verpflichtung zur Eintragung der Angaben in die Beilage nicht besteht.

Ein solcher Hinweis könnte wie folgt lauten:

„Nach § 12 Abs. 2 PBefG sind dem Genehmigungsantrag Unterlagen beizufügen, die ein Urteil über die Sicherheit und Leistungsfähigkeit des Betriebs ermöglichen. Dies kann durch die in der Beilage zum Antrag vorgesehene Vermögensübersicht erfolgen. Falls Sie nicht bereit sind, diese Angaben zu machen, müssen Sie durch andere geeignete Unterlagen belegen, daß Ihnen das für die Betriebseinrichtung und Betriebsfortführung erforderliche Kapital tatsächlich zur Verfügung steht.“

- In einem anderen Fall hat mir ein Taxifahrer eine Ablichtung der von einem Gesundheitsamt ausgestellten **amtsärztlichen Zeugnisse** über die Eignung zur Führung von Kraftfahrzeugen für sich und seine Ehefrau zugeleitet. In seiner Eingabe wendet sich der Bürger dagegen, daß in diesen für das Straßenverkehrsamt bestimmten amtsärztlichen Zeugnissen detaillierte Angaben über die Gesundheitsverhältnisse enthalten sind. Insbesondere wird von ihm bezweifelt, daß die in den amtsärztlichen Zeugnissen im einzelnen aufgeführten Angaben zu seinen Kriegsverletzungen und den Geburten seiner Ehefrau, die dem untersuchenden Amtsarzt im Vertrauen auf die ärztliche Schweigepflicht gemacht worden seien, zum Nachweis der geistigen und körperlichen Eignung erforderlich sind.

Nach Artikel 4 Abs. 2 der Landesverfassung wie auch nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes bedarf die Weitergabe personenbezogener Daten durch öffentliche Stellen, sofern keine Einwilligung des Betroffenen vorliegt, einer gesetzlichen Grundlage; dabei ist der Verhältnismäßigkeitsgrundsatz zu beachten.

Zwar findet bei der Erteilung einer behördlichen Bescheinigung mit personenbezogenen Daten an den Betroffenen zum Zweck der Vorlage bei einer anderen Behörde keine Weitergabe durch die öffentliche Stelle statt. Da der Betroffene in seiner Entscheidung, ob er von der Bescheinigung Gebrauch macht und dadurch selbst Daten offenbart, einem Zwang unterliegt, kommt dieser Vorgang einer Weitergabe personenbezogener Daten durch eine öffentliche Stelle gleich.

Nach § 15f Abs. 2 Nr. 2 Buchst. a StVZO wird die Geltungsdauer der Fahrerlaubnis zur Fahrgastbeförderung auf Antrag des Inhabers jeweils bis zu drei Jahren verlängert, wenn der Antragsteller unter anderem seine geistige und körperliche Eignung durch das Zeugnis eines Arztes nachweist. Nach dem Verhältnismäßigkeitsgrundsatz darf das amtsärztliche Zeugnis nur solche Angaben enthalten, die die Behörde für ihre Entscheidung über die Verlängerung der Geltungsdauer der Fahrerlaubnis zur Fahrgastbeförderung unbedingt benötigt. Hierfür reicht es nach meiner Auffassung aus, wenn das

Zeugnis lediglich die Aussage enthält, daß der Inhaber der Fahrerlaubnis zur Fahrgastbeförderung geistig und körperlich uneingeschränkt oder nur eingeschränkt geeignet ist und gegebenenfalls welche Einschränkung vorliegt. Wird eine derartige Einschränkung festgestellt, kann es geboten sein, in dem Zeugnis die der Einschränkung zugrunde liegenden ärztlichen Befunde aufzuführen.

Ich habe dem Gesundheitsamt empfohlen, die Angaben in einem zur Vorlage bei einem Straßenverkehrsamt bestimmten amtsärztlichen Zeugnis auf solche Daten zu beschränken, die das Straßenverkehrsamt für seine Entscheidung über die Verlängerung der Geltungsdauer einer Fahrerlaubnis wissen muß.

## 20. Umweltschutz

- Durch Gesetz vom 19. März 1985 (GV. NW. S. 255) wurde in die Verfassung des Landes Nordrhein-Westfalen ein neuer **Artikel 29a** eingefügt, der die natürlichen Lebensgrundlagen und die Umwelt unter den Schutz des Landes, der Gemeinden und Gemeindeverbände stellt. Diese Verfassungsvorschrift enthält eine Staatszielbestimmung und ist insbesondere bei der Ermessensausübung von Gesetzgebung und Verwaltung von Bedeutung. Subjektiv-öffentliche Rechte des einzelnen werden durch die Vorschrift nicht begründet.

Auch Eingriffe in das Grundrecht auf Datenschutz nach Artikel 4 Abs. 2 der Landesverfassung sowie in das Recht auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes können nicht unmittelbar auf die Vorschrift gestützt werden. Das Staatsziel Umweltschutz kann jedoch ein überwiegendes Allgemeininteresse begründen, das Voraussetzung für die Zulassung von Eingriffen in diese Grundrechte durch den Gesetzgeber ist.

Von Umweltschützern ist verschiedentlich geltend gemacht worden, daß es sich bei der Durchsetzung von Maßnahmen im Bereich des Umweltschutzes als hinderlich erweise, wenn die zuständigen Stellen es unter Berufung auf die Vorschriften des Datenschutzes ablehnten, bestimmte „Umweltdaten“ bekannt zu geben (vgl. sechster Tätigkeitsbericht, C.18; Kleine Anfrage 109, Drucksache 10/197).

Die genannten Grundrechte verbürgen natürlichen Personen ein unmittelbares Recht auf Schutz der Daten, die ihnen zugeordnet werden können. Ein Eingriff in diese Grundrechte bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen und den Verhältnismäßigkeitsgrundsatz beachten muß.

Wie die Landesregierung in ihrer Antwort auf die erwähnte Kleine Anfrage (Drucksache 10/574) ausgeführt hat, muß der Ausgleich im Spannungsverhältnis zwischen dem Informationsinteresse der Öffentlichkeit und dem informationellen Selbstbestimmungsrecht des Einzelnen durch den Bundes- und Landesgesetzgeber getroffen werden. Soweit sich herausstellen sollte, daß die bestehende Rechtslage den notwendigen Umweltschutz behindere, werde die Landesregierung entsprechende Initiativen ergreifen. Diese Initiativen könnten sich sowohl auf die Änderung landesrechtlicher Vorschriften als auch auf entsprechende Schritte im Bundesrat beziehen.

Soweit hierbei die Verhältnismäßigkeit der Mittel gewahrt, der Eingriff also zur Erreichung des Ziels geeignet und erforderlich sowie für den Betroffenen zumutbar ist, werden hiergegen aus der Sicht des Datenschutzes keine Einwendungen zu erheben sein.

- Die Eingabe eines Bürgers betraf den Schutz personenbezogener Daten in einem immissionsschutzrechtlichen **Genehmigungsverfahren**. Die Genehmigungsbehörde hatte in einem auf die Erteilung eines Vorbescheides nach § 9 des Bundes-Immissionsschutzgesetzes (BImSchG) gerichteten Verfahren dem Antragsteller den Inhalt der erhobenen Einwendungen dadurch bekanntgegeben, daß sie ihm Ablichtungen der Schreiben und der Unterschriftenlisten der Einwender übersandt hatte. Hierdurch erhielt der Antragsteller Kenntnis von Namen und Anschriften der Einwender. Unter diesen befanden sich Betriebsangehörige des antragstellenden Betriebes. Der Bürger teilte mit, der Antragsteller habe die Einwendungen unter anderem auch daraufhin ausgewertet, welcher Einwender Betriebsangehöriger sei. Der Bürger befürchtete ein erhebliches Arbeitsplatzrisiko für diese Einwender.

Das immissionsschutzrechtliche Genehmigungsverfahren richtet sich nach den Vorschriften des § 10 Abs. 1 bis 8 BImSchG. Diese gelten nach § 10 Abs. 9 BImSchG entsprechend für die Erteilung eines Vorbescheides. Die Grundsätze des Genehmigungsverfahrens sind in der Neunten Verordnung zur Durchführung des Bundes-Immissionsschutzgesetzes – 9. BImSchV – geregelt.

Nach § 12 Abs. 2 Satz 1 der 9. BImSchV ist der Inhalt der Einwendungen dem Antragsteller bekanntzugeben. In der Verwaltungspraxis der Genehmigungsbehörden wird diese Vorschrift so angewendet, daß dem Antragsteller in aller Regel Abschriften oder Ablichtungen der Einwendungen übersandt werden.

Ich habe gegen diese Verfahrensweise datenschutzrechtliche Bedenken erhoben. Die Weitergabe der Namen und Anschriften von Personen, die Einwendungen gegen die Erteilung eines Vorbescheides nach § 9 BImSchG erhoben haben, ist ein Eingriff in das Grundrecht auf Datenschutz und das Recht auf informationelle Selbstbestimmung der Betroffenen. Er bedarf einer gesetzlichen Grundlage, die dem Gebot der Normenklarheit entsprechen und den Verhältnismäßigkeitsgrundsatz beachten muß. Eine generelle Weitergabe von Namen und Anschriften der Einwender könnte nur dann auf die Vorschrift des § 12 Abs. 2 Satz 1 der 9. BImSchV gestützt werden, wenn sie für den Bürger klar und erkennbar die Zulässigkeit der Weitergabe dieser Daten vorsehen würde. Das ist aber nicht der Fall.

Darüber hinaus würde eine generelle Weitergabe der Namen und Anschriften aller Einwender auch gegen den Verhältnismäßigkeitsgrundsatz verstoßen. Dieser gebietet, die Weitergabe auf die Fälle zu beschränken, in denen die Kenntnis der Daten zur Erfüllung des Zwecks des § 12 Abs. 2 Satz 1 der 9. BImSchV erforderlich ist.

Der Minister für Umwelt, Raumordnung und Landwirtschaft hat in diesem Zusammenhang darauf hingewiesen, in der Praxis ließe sich häufig erst aus der Anschrift auf die Lage eines Nachbargrundstücks, die mögliche Betroffenheit und damit den Aussagegehalt der Einwendung zurückschließen. In derartigen Fällen sei die Übersendung einer vollständigen Ablichtung des Einwendungsschreibens erforderlich, wenn nicht die Berücksichtigung als Einwendung unterbleiben solle.

Für die Fälle, in denen dies zutrifft, mag es zur sachgerechten Vorbereitung des Erörterungstermins erforderlich sein, dem Antragsteller bekanntzugeben, wo und bei wem schädliche Auswirkungen seiner Anlage befürchtet werden. Die Bekanntgabe muß jedoch auf solche Fälle beschränkt bleiben, in denen es nach dem Zweck der Vorschrift zweifelsfrei ist, daß der Antragsteller bereits zu diesem Zeitpunkt die Daten zu einer sachgerechten Vorbereitung des Erörterungstermins benötigt.

Nur in diesen Fällen kann davon ausgegangen werden, daß die in § 12 Abs. 2

Satz 1 der 9. BImSchG vorgesehene Bekanntgabe des „Inhalts“ der Einwendungen auch die Anschrift und, soweit erforderlich, des Namens eines Einwenders umfaßt. Denn bei der Auslegung von Rechtsvorschriften ist nach der Rechtsprechung des Bundesverfassungsgerichts derjenigen Interpretation der Vorzug zu geben, die den Grundrechten – hier dem Recht auf informationelle Selbstbestimmung – zu einer größtmöglichen Wirksamkeit verhilft. Gerade bei Einwendungen, die von Betriebsangehörigen eines Antragstellers erhoben werden, sind deren besonders schutzwürdige Belange im Einwendungsverfahren zu beachten. Eine Verfahrensweise, wonach generell dem Antragsteller Ablichtungen der Einwendungen sowie der Unterschriftenlisten übersandt werden, ist damit nicht vereinbar.

Darüber hinaus vertritt der Minister für Umwelt, Raumordnung und Umweltschutz die Auffassung, aus § 29 des Verwaltungsverfahrensgesetzes Nordrhein-Westfalen (VwVfG NW) und aus den §§ 99 und 100 der Verwaltungsgerichtsordnung (VwGO) könne der allgemeine Rechtsgrundsatz abgeleitet werden, in einem rechtsförmlichen Verfahren hätten Beteiligte keinen Anspruch darauf, daß ihre Identität gegenüber anderen am Verfahren Beteiligten verborgen bleibt.

Ein solcher allgemeiner Rechtsgrundsatz würde jedoch den Anforderungen des Volkszählungsurteils an die erforderliche gesetzliche Grundlage für einen Eingriff in das Recht auf informationelle Selbstbestimmung nicht entsprechen. Die an dem Verfahren Beteiligten können den genannten Rechtsvorschriften einen derartigen Umfang der Einschränkung ihres Grundrechts nicht entnehmen. Darüber hinaus würde der verfassungsrechtliche Grundsatz der Verhältnismäßigkeit (Eignung und Erforderlichkeit zur Erreichung des Zwecks, Zumutbarkeit für den Betroffenen) nicht beachtet.

Weder die Verpflichtung, den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist (§ 29 VwVfG NW), noch das Recht der Beteiligten auf Einsicht in die dem Gericht vorgelegten Akten (§ 100 VwGO) rechtfertigt es, dem Antragsteller bereits bei der Bekanntgabe des Inhalts der Einwendungen nach § 12 Abs. 2 Satz 1 der 9. BImSchV die Namen und Anschriften der Einwender von Amts wegen mitzuteilen. Soweit die Mitteilung dieser Angaben nicht im Einzelfall für eine sachgerechte Vorbereitung des Erörterungstermins erforderlich ist, muß den Einwendern die Möglichkeit erhalten bleiben, bis zum Erörterungstermin ihre Einwendungen zurückzunehmen, ohne daß die Behörde ihre Identität gegenüber dem Antragsteller aufdeckt.

## 21. Öffentliche Unternehmen

### a) Kreditinstitute

- In meinem sechsten Tätigkeitsbericht (C.19.a) hatte ich im Zusammenhang mit der Neuregelung für das Bankauskunftsverfahren darauf hingewiesen, daß auch die bisherige **Schufa-Klausel** geändert werden müsse. Der Bundesgerichtshof hat inzwischen in dem Urteil vom 19. September 1985 (NJW 1986, 46) entschieden, daß die bisher allgemein von den Kreditinstituten verwendete Schufa-Klausel gegen § 9 des Gesetzes zur Regelung des Rechts der Allgemeinen Geschäftsbedingungen verstößt und daher unzulässig ist. In dem Urteil weist der Bundesgerichtshof jedoch zugleich darauf hin, daß sich die Berechtigung der einem Kreditinformationssystem angeschlossenen Bank, gespeicherte Daten über Rechtsnatur, Anzahl und Höhe eingegangener Verpflichtungen wie auch über Art und Zeitraum ihrer Tilgung zu

übermitteln, aus § 24 Abs. 1 BDSG (gleichlautend mit § 20 Abs. 1 DSG NW) ergeben kann, weil das Ziel eines solchen Informationssystems, potentiellen Kreditgebern die Beurteilung der Kreditwürdigkeit eines Kreditbewerbers zu erleichtern, im Interesse sämtlicher Beteiligten liegt.

Bereits vor diesem Urteil hatten die Vertreter der obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich und der Datenschutzbeauftragten des Bundes und der Länder zusammen mit der Kreditwirtschaft Beratungen über eine Neugestaltung des Schufa-Verfahrens und der Schufa-Klausel aufgenommen. Diese Verhandlungen konnten im März 1986 abgeschlossen werden.

Mit der neuen Schufa-Klausel wird dem Kunden nunmehr eine umfangreiche Information über die Speicherung und Übermittlung seiner Daten in dem Schufa-System gegeben. So lautet die von den Sparkassen verwendete Schufa-Klausel auf Kontoeröffnungsanträgen künftig wie folgt:

Ich/Wir willige(n) ein, daß das Kreditinstitut der für meinen/unseren Wohnsitz zuständigen SCHUFA-Gesellschaft (Schutzgemeinschaft für allgemeine Kreditsicherung) Daten über die Beantragung, die Aufnahme und Beendigung dieser Kontoverbindung übermittelt.

Unabhängig davon wird das Kreditinstitut der SCHUFA auch Daten aufgrund nicht vertragsgemäßen Verhaltens (z. B. Scheckkartenmißbrauch durch den rechtmäßigen Karteninhaber, Scheckrückgabe mangels Deckung, Wechselprotest, beantragter Mahnbescheid bei unbestrittener Forderung sowie Zwangsvollstreckungsmaßnahmen) melden. Diese Meldungen dürfen nach dem Datenschutzgesetz Nordrhein-Westfalen nur erfolgen, soweit dies zur Wahrung berechtigter Interessen des Kreditinstituts, eines Vertragspartners der SCHUFA oder der Allgemeinheit erforderlich ist und dadurch meine/unsere schutzwürdigen Belange nicht beeinträchtigt werden.

Soweit hiernach eine Übermittlung erfolgen kann, befreie(n) ich/wir das Kreditinstitut zugleich vom Bankgeheimnis.

Die SCHUFA speichert die Daten, um den ihr angeschlossenen Kreditinstituten, Leasinggesellschaften, Einzelhandels-, Versandhandels- und sonstige Unternehmen, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben, Informationen zur Beurteilung der Kreditwürdigkeit von Kunden geben zu können. Sie stellt diese Daten ihren Vertragspartnern nur zur Verfügung, wenn diese ein berechtigtes Interesse an der Datenübermittlung glaubhaft darlegen. Die SCHUFA übermittelt nur objektive Daten ohne Angabe des kontoführenden Instituts; subjektive Werturteile, persönliche Einkommens- und Vermögensverhältnisse sind in SCHUFA-Auskünften nicht enthalten.

Ich kann/Wir können Auskunft bei der SCHUFA über die mich/uns betreffenden gespeicherten Daten erhalten. Die Adresse der SCHUFA lautet:

.....  
Ich/Wir willige(n) ein, daß im Falle eines Wohnsitzwechsels die vorgenannte SCHUFA die Daten an die dann zuständige SCHUFA übermittelt.

Weitere Informationen über das SCHUFA-Verfahren enthält ein Merkblatt, das auf Wunsch zur Verfügung gestellt wird.

.....  
Unterschrift(en)

Darüber hinaus haben die Kreditinstitute zusammen mit den Vertretern der Datenschutzbehörden und der Datenschutzbeauftragten ein umfangreiches Schufa-Merkblatt erarbeitet, das die Kreditinstitute den Kunden auf Wunsch aushändigen.

Mit seiner Unterschrift unter die Schufa-Klausel erteilt der Kunde seine Einwilligung (§ 3 Satz 1 Nr. 2 DSG NW) dazu, daß das Kreditinstitut Daten über die Beantragung, die Aufnahme und Beendigung einer Kontoverbindung (Positivmerkmale) an die Schufa übermittelt. Unabhängig von dieser Einwilligung dürfen Daten einer nicht vertragsgemäßen Abwicklung (Negativmerkmale) nach § 20 Abs. 1 Satz 1 DSG NW an die Schufa nur übermittelt werden, soweit dies zur Wahrung berechtigter Interessen des Kreditinstituts, der Vertragspartner der Schufa oder der Allgemeinheit erforderlich ist und dadurch schutzwürdige Belange des Kunden nicht beeinträchtigt werden. Vor jeder Übermittlung von Negativmerkmalen an die Schufa ist also eine Interessenabwägung erforderlich.

Das neue Schufa-Verfahren stellt daher nicht geringe Anforderungen an die Mitarbeiter der Kreditinstitute, die in der täglichen Praxis diese Abwägung vor der Übermittlung von Negativmerkmalen an die Schufa vorzunehmen haben. Die damit verbundenen Fragen werden deshalb in Ausbildung und Schulung der Mitarbeiter besonders berücksichtigt werden müssen. Für den Beginn des neuen Verfahrens haben die Spitzenverbände des Kreditwesens eine schriftliche Mitarbeiterinformation erarbeitet, in der diesen die Gesichtspunkte des neuen Verfahrens erläutert und praktische Hinweise für dessen Durchführung gegeben werden.

Nach allem muß nunmehr zunächst die weitere Entwicklung abgewartet und daraufhin beobachtet werden, ob sich die neue Schufa-Klausel und das neue Schufa-Verfahren bewähren oder ob weitere Verbesserungen vorgenommen werden müssen.

- Ebenfalls in meinem sechsten Tätigkeitsbericht (C.20.c) habe ich auf eine Vereinbarung zwischen den Spitzenverbänden der Kreditwirtschaft und der von dem Westdeutschen Rundfunk Köln betriebenen **Gebühreneinzugszentrale** der öffentlich-rechtlichen Rundfunkanstalten in der Bundesrepublik Deutschland (GEZ) hingewiesen, nach der die Kreditinstitute der GEZ Änderungen der Anschriften ihrer Kunden mitteilen, die am Lastschriftverfahren teilnehmen.

Nach meiner Auffassung ist die Mitteilung solcher Anschriftenänderungen durch die meiner Kontrolle unterliegenden Sparkassen an die GEZ ohne Einwilligung der Betroffenen nicht zulässig, da eine solche Datenübermittlung nicht auf § 20 Abs. 1 Satz 1 DSG NW gestützt werden kann. Nach dieser Vorschrift 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. Zwar kann davon ausgegangen werden, daß ein berechtigtes Interesse der GEZ daran besteht, die Änderung der Anschrift von Rundfunkteilnehmern zu erfahren, und daß dies auch im Interesse der Allgemeinheit liegt. Auch die Anschriften ihrer Kunden unterliegen jedoch dem besonderen Verschwiegenheitsgebot, das die Sparkassen als Vertragspflicht gegenüber ihren Kunden zu wahren haben (Bankgeheimnis). Da durch die Mitteilung von Anschriftenänderungen dieses Verschwiegenheitsgebot verletzt wird, werden durch die Datenübermittlung schutzwürdige Belange der Betroffenen beeinträchtigt.

Ich habe den Sparkassen- und Giroverbänden in Nordrhein-Westfalen meine Auffassung zu der Rechtslage mitgeteilt. Sie folgen meiner Rechtsauffassung jedoch nicht und weisen in ihrer Antwort darauf hin, daß die Vertreter der für

den Datenschutz im nicht-öffentlichen Bereich zuständigen obersten Aufsichtsbehörden („Düsseldorfer Kreis“) mit einer Ausnahme die von mir für unzulässig angesehene Datenübermittlung datenschutzrechtlich für unbedenklich halten. Nach nochmaliger Überprüfung bin ich zu dem Ergebnis gekommen, daß kein Grund besteht, meine Rechtsauffassung zu ändern. Ich habe daher dem Rheinischen Sparkassen- und Giroverband und dem Westfälisch-Lippischen Sparkassen- und Giroverband mitgeteilt, daß ich derartige Datenübermittlungen nach § 30 Abs. 1 Satz 1 DSG NW beanstanden müßte, sofern nicht der Kunde hierzu seine Einwilligung erteilt hat.

- Mehrere Bürger haben sich mit der Frage an mich gewandt, ob der von manchen Sparkassen angebotene **„Vereinservice“** datenschutzrechtlich unbedenklich ist. Mit diesem Vereinservice bieten die Sparkassen den Vereinen in ihrem Einzugsbereich eine Dienstleistung an, mit der den Vereinen eine Hilfe zur rationellen und wirtschaftlichen Finanzverwaltung, insbesondere durch den Einzug von Mitgliederbeiträgen, geleistet werden soll.

Bei dieser Dienstleistung handelt es sich nach meiner Auffassung nicht um eine Datenverarbeitung im Auftrag (§ 7 DSG NW), da der Auftrag, den das Kreditinstitut übernimmt, insgesamt eine Geschäftsbesorgung, nämlich den Einzug von Mitgliederbeiträgen, und nicht nur die Verarbeitung von Daten zum Gegenstand hat. Die Weitergabe von Mitgliederdaten durch die Vereine an das Kreditinstitut stellt daher eine Übermittlung im Sinne von § 2 Abs. 2 Nr. 2 BDSG dar. Die datenschutzrechtliche Zulässigkeit der Speicherung von Mitgliederdaten durch die Sparkasse im Rahmen des Vereinservice hängt deshalb in erster Linie von der Zulässigkeit der Übermittlung durch den Verein ab. Ist diese zu bejahen, so bestehen gegen die Speicherung und Verwendung der Daten für Zwecke des Vereinservice keine grundsätzlichen Bedenken.

Da der Vereinservice jedoch außerhalb der eigentlichen Aufgaben der Sparkasse nach dem Sparkassengesetz und ihrer Satzung liegt, muß in Anlehnung an die Vorschriften für die Datenverarbeitung im Auftrag verlangt werden, daß der Verein die Verarbeitung seiner Mitgliederdaten ausschließlich nach seinen Weisungen sicherstellt, gegebenenfalls auch durch Kontrollen. Die Verwendung der Daten für andere Zwecke der Sparkasse ist auszuschließen.

Die Frage, ob Vereine ihre Mitgliederdaten an Sparkassen für Zwecke eines Vereinservice übermitteln dürfen, unterliegt nicht meiner Kontrollzuständigkeit, sondern ist durch die nach § 30 BDSG örtlich zuständige Aufsichtsbehörde zu beurteilen. Ich habe daher die mir vorliegenden Eingaben zur Prüfung dieser Frage zunächst an den zuständigen Regierungspräsidenten abgegeben.

## **b) Versicherungsunternehmen**

- Immer wieder beschwerten sich Bürger über die von der Versicherungswirtschaft allgemein verwendete „Datenschutzklausel“ in den Versicherungsanträgen und die zusätzlich in den Anträgen für Lebensversicherung enthaltenen **„Ermächtigungs- und Schweigepflichtentbindungsklausel“**.

Mit der Datenschutzklausel soll der Versicherte in die Übermittlung seiner personenbezogenen Daten an andere Versicherungen (Versicherungsauskunft) sowie an die Verbände der Versicherungswirtschaft einwilligen.

Durch die Ermächtigungs- und Schweigepflichtentbindungsklausel soll die Versicherung zur Nachprüfung und Verwertung der vom Versicherten über seine Gesundheitsverhältnisse gemachten Angaben ermächtigt werden, alle Ärzte, Krankenhäuser und sonstige Krankenanstalten, bei denen der Versi-

cherte in Behandlung war oder sein wird, sowie andere Personenversicherer und Behörden über seine Gesundheitsverhältnisse zu befragen. Dies gilt für die Zeit nach der Antragsannahme. Die Versicherung darf auch die Ärzte, die den Versicherten im letzten Jahr vor seinem Tod untersuchen oder behandeln werden, über die Todesursachen oder die Krankheiten, die zum Tode geführt haben, befragen. Insoweit entbindet der Versicherte alle, die hiernach befragt werden, von der Schweigepflicht auch über seinen Tod hinaus.

Für die meiner Kontrolle unterliegenden öffentlich-rechtlichen Versicherungsunternehmen habe ich in meinem vierten Tätigkeitsbericht (C.19.c) zur Zulässigkeit der Datenübermittlungen auf der Grundlage der verwendeten Klauseln Stellung genommen. Insbesondere habe ich zur Ermächtigungs- und Schweigepflichtentbindungsklausel dargelegt, daß eine so weit gefaßte Erklärung den Anforderungen nicht genügt, die an eine Einwilligung nach § 3 Satz 1 Nr. 2, Satz 2 DSGVO zu stellen sind. Danach muß eine Einwilligung hinreichend bestimmt sein. Die Anforderungen an die Bestimmtheit müssen um so strenger gefaßt werden, je sensibler die Daten sind, auf die sich die Erklärung bezieht. Die Wirksamkeit einer Einwilligung setzt deshalb voraus, daß der Betroffene weiß, worauf er sich einläßt. Dieser Voraussetzung kann die Klausel jedenfalls insoweit nicht entsprechen, als sie auf in der Zukunft liegende und daher nicht vorhersehbare ärztliche Behandlungen abstellt.

Weitere Bedenken gegen die Ermächtigungs- und Schweigepflichtentbindungsklausel bestehen, soweit sie das Versicherungsunternehmen zu Fragen über die Gesundheitsverhältnisse des Versicherten auch gegenüber Behörden ermächtigt. Mit Behörden sind hier vor allem die Sozialversicherungsträger gemeint. Für diese bestimmt jedoch § 67 Satz 1 SGB X ausdrücklich, daß der Betroffene „im Einzelfall“ in eine Offenbarung eingewilligt haben muß, soweit nicht eine gesetzliche Offenbarungsbefugnis nach den §§ 68 bis 77 SGB X vorliegt.

Meine datenschutzrechtlichen Bedenken gegen die Ermächtigungs- und Schweigepflichtentbindungsklausel werden von den für den Datenschutz im nicht-öffentlichen Bereich zuständigen obersten Aufsichtsbehörden geteilt. Aus diesem Grund wie auch zur Behebung anderer datenschutzrechtlicher Defizite haben sie Gespräche mit Vertretern der Versicherungswirtschaft geführt, an denen der Landesbeauftragte für den Datenschutz beteiligt war. Von den Datenschutzbehörden ist dabei darauf hingewiesen worden, daß die derzeit verwendete Klausel viel zu weit geht und daß eine Konkretisierung sowie eine Beschränkung auf die für den Abschluß und Durchführung des Versicherungsvertrages wirklich benötigten Daten dringend erforderlich ist.

Die Vertreter der Versicherungswirtschaft haben sich grundsätzlich zu einer Neufassung der Klausel bereit erklärt. Diese muß mit dem Bundesaufsichtsamt für das Versicherungswesen abgestimmt werden. Die Vorarbeiten für eine Neufassung der Klausel sind aufgenommen worden. Ein konkreter Formulierungsvorschlag liegt für die in der Lebensversicherung verwendete Klausel jedoch bisher nicht vor.

## 22. Ordensangelegenheiten

Der Landtag hat ein Gesetz über den Verdienstorden des Landes Nordrhein-Westfalen beschlossen. Für die Verleihung des Ordens ist die Erhebung personenbezogener Daten des zu Ehrenden erforderlich. Das Gesetz sieht deshalb vor, daß die Vorschlagsberechtigten personenbezogene Daten erheben können, soweit dies zur Begründung ihres Vorschlags erforderlich ist (§ 5 Abs. 1). Der Ministerpräsident kann personenbezogene Daten des Vorgesetzten erheben, soweit dies zur Prüfung der Ordenswürdigkeit erforderlich ist (§ 5 Abs. 2).

Die Aufnahme einer solchen Regelung, an deren Vorbereitung ich beteiligt war, war nach dem Volkszählungsurteil des Bundesverfassungsgerichts notwendig. Eine derartige Datenerhebung, die auch Anfragen bei dem Verfassungsschutz einschließt, greift in das Recht der Betroffenen auf informationelle Selbstbestimmung nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 des Grundgesetzes ein. Sie bedarf daher einer normenklaren gesetzlichen Grundlage, in der der Verwendungszweck der Daten bereichsspezifisch und präzise bestimmt wird (BVerfGE 65, 1, 44, 46).

Der Grundsatz der informationellen Selbstbestimmung verlangt in derartigen Fällen aber auch, daß der Betroffene die Möglichkeit haben muß, der Datenerhebung zu widersprechen. Eine Erhebung ohne sein Wissen oder Wollen kann für ihn eine unverhältnismäßige Belastung darstellen. So könnte es für ihn unangenehm sein, wenn die an dem Verleihungsverfahren beteiligten Stellen von Informationen Kenntnis erhalten, die der Verfassungsschutz über ihn hat. Möglicherweise wird er lieber auf eine Ehrung verzichten.

Dementsprechend sieht der von der SPD-Fraktion des Deutschen Bundestages eingebrachte Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes (Bundestagsdrucksache 10/1180) vor, daß eine Datenübermittlung für Zwecke einer öffentlichen Auszeichnung nur zulässig ist, wenn der Betroffene nicht widersprochen hat; nach dem Entwurf muß die Absicht der Übermittlung so angekündigt werden, daß der Betroffene Gelegenheit zur Kenntnisnahme und zum Widerspruch hat. Die Verwendung der übermittelten Daten zu anderen Zwecken soll unzulässig sein.

Unter Berücksichtigung der in dem Gesetzentwurf dieser Fraktion vorgesehenen Regelung habe ich dem Landtag (in der Vorlage 10/279) vorgeschlagen, in dem Gesetz zu bestimmen, daß die Absicht der Datenerhebung dem Betroffenen so angekündigt werden muß, daß er Gelegenheit zur Kenntnisnahme und zum Widerspruch hat; dabei sollten dem Betroffenen diejenigen Stellen benannt werden, bei denen beabsichtigt ist, Auskünfte einzuholen. Ferner habe ich vorgeschlagen, die Verwendung der erhobenen Daten zu anderen als den im Gesetz genannten Zwecken auszuschließen. Der Landtag hat diese Vorschläge jedoch nicht aufgegriffen.

## 23. Medien

### **a) Entwurf eines Landesrundfunkgesetzes**

Die Fraktion der FDP hat im Landtag den Entwurf eines Gesetzes über die Veranstaltung von Rundfunkprogrammen und deren kabelgebundene oder drahtlose Verbreitung in Nordrhein-Westfalen (Landesrundfunkgesetz) eingebracht (Drucksache 10/610). Der Entwurf enthält auch bereichsspezifische Datenschutzregelungen (§ 11).

Vergleichbar mit entsprechenden Regelungen des Kabelversuchsgesetzes NW ist vorgesehen, daß die Speicherung der Abrechnungsdaten Zeitpunkt, Dauer, Art, Inhalt und Häufigkeit bestimmter von einzelnen Teilnehmern empfangener Sendungen nicht erkennen lassen darf, es sei denn, der Teilnehmer beantragt eine andere Art und Weise der Speicherung. Damit wird der Gefahr einer Bildung von Interessenprofilen begegnet.

Einer solchen Gefahr soll offenbar auch mit der Regelung über Akzeptanzuntersuchungen entgegengewirkt werden. So dürfen personenbezogene Daten über die Inanspruchnahme technischer Einrichtungen und den Empfang einzelner Programme oder Sendungen nur erhoben oder gespeichert werden, soweit und solange dies erforderlich ist, um die Akzeptanz einzelner Sendungen zu ermit-

tein. Allerdings sieht der Entwurf als Voraussetzung für derartige Ermittlungen eine Einwilligung der Betroffenen nicht vor.

Außerdem ist weder ein Recht des durch eine Sendung Betroffenen auf Einsicht in die Ton- und Bildaufzeichnungen (vgl. § 12 Abs. 2 des WDR-Gesetzes) noch ein Recht auf Speicherung seiner Gegendarstellung, Auskunft über die der Berichterstattung zugrunde liegenden Daten und gegebenenfalls Berichtigung oder Hinzufügung einer eigenen Darstellung (vgl. § 50 Abs. 2 und 3 des WDR-Gesetzes) vorgesehen.

#### **b) Fernwirken**

In meinem sechsten Tätigkeitsbericht (C.20.b) habe ich auf die beabsichtigte Einrichtung eines Fernwirkinformationssystems unter der Bezeichnung „Temex“ durch die Deutsche Bundespost im Rahmen eines Betriebsversuchs in einer kreisfreien Stadt und meine Auffassung hierzu hingewiesen. Die Stadt hat nunmehr mitgeteilt, daß im Rahmen des Betriebsversuchs folgende Datenschutzanforderungen verwirklicht werden sollen:

- Der Temex-Anschluß erfolgt nur mit schriftlicher Einwilligung des Teilnehmers und auf Grund schriftlicher, für alle Beteiligten verbindlicher Festlegung des Verfahrens nach geeigneter Unterrichtung der Teilnehmer über die jeweils vorgesehenen Anwendungen und die zur Verfügung stehenden Einflußmöglichkeiten.
- Jeder Ablesebefehl löst ein Signal aus, das dem Teilnehmer anzeigt, daß eine Ablesung erfolgt. Zählerstand, Datum und Uhrzeit der Ablesung können vom Teilnehmer jederzeit am Anzeigegerät kontrolliert werden. Auf Wunsch des Teilnehmers kann das Ablesen durch Aktivieren der Datenauslesesperre verhindert werden.
- Das System wird so eingerichtet, daß die von der Zentrale ausgehenden Daten vom Teilnehmer jederzeit abgeschaltet werden können.
- Anfallende Verbrauchsdaten werden durch geeignete technische Vorkehrungen nur zu dem vereinbarten Zweck verarbeitet. Die Daten werden gelöscht, wenn sie zur Erfüllung dieses Zwecks nicht mehr erforderlich sind.

Die genannten Anforderungen sollen zwischen allen am Temex-Betriebsversuch Beteiligten durch einzelvertragliche Regelungen festgeschrieben werden.

Im Interesse der betroffenen Bürger halte ich es nach wie vor für geboten, bei Einrichtungen von Fernwirkinformationssystemen eine gesetzliche Grundlage zu schaffen, die den vom Bundesverfassungsgericht in seinem Urteil zum Volkszählungsgesetz 1983 aufgestellten Grundsätzen entspricht. Dies erscheint im Hinblick auf die gesetzliche Regelung des Feldversuchs mit Bildschirmtext (Bildschirmtextversuchsgesetz NW) und des Modellversuchs mit Breitbandkabel (Kabelversuchsgesetz NW) auch konsequent.

Demgegenüber sieht es die Landesregierung in ihrer Stellungnahme zu meinem sechsten Tätigkeitsbericht (Drucksache 10/430, S. 43) in Anbetracht des Erprobungscharakters der Temex-Betriebsversuche der Deutschen Bundespost und mit Blick darauf, daß sich im Laufe der Versuche weitere Erkenntnisse über den Regelungsbedarf ergeben werden, zum gegenwärtigen Zeitpunkt als vertretbar an, von einer bereichsspezifischen gesetzlichen Regelung abzusehen.

## D. Organisatorische und technische Maßnahmen

Obgleich bei öffentlichen Stellen zahlreiche kleinere Datenverarbeitungsanlagen aufgestellt sind, besteht bei deren Einsatz hinsichtlich der Anforderungen und Möglichkeiten der Datensicherung eine große Unsicherheit. Kleinere Datenverarbeitungsanlagen wurden deshalb in den letzten Jahren bevorzugt in die Kontrolltätigkeit einbezogen. Die Datensicherung bei Einsatz kleinerer Datenverarbeitungsanlagen bildete Schwerpunkte in meinem vierten und sechsten Tätigkeitsbericht (D.5.).

Im vorliegenden Bericht wird erneut auf die besonderen Schwierigkeiten der Datensicherung bei der Abwicklung von Verwaltungsaufgaben auf kleineren Datenverarbeitungsanlagen eingegangen (unten D.5.). Prüfungen ergaben, daß öffentliche Stellen, die kleinere Datenverarbeitungsanlagen einsetzen, mit den heute zur Verfügung stehenden Mitteln im allgemeinen nicht in der Lage sind, die Datensicherung hinreichend zu gewährleisten. Wesentlich verbessert werden könnten die Möglichkeiten zur Datensicherung durch ein Versiegeln der Programme. Ein Hersteller hat sich auf meine Empfehlung bereit erklärt, für die bei einer Stadtverwaltung eingesetzten Programme eine Programmsicherung durch Versiegeln zu verwirklichen (unten D.5.c). Der Stadtdirektor und der Hersteller sehen darin ein Pilotprojekt für eine wesentliche Verbesserung der Datensicherung.

Zu einer Beeinträchtigung der Datensicherheit in Datennetzen führt der Einsatz des Schnittstellenvervielfachers SK 12 der Deutschen Bundespost (SK 12). Eine auf meine Empfehlung durchgeführte Untersuchung des Innenministers hat entsprechende Befürchtungen bestätigt (unten D.4.a). Nunmehr sollten bestehende Datennetze daraufhin untersucht werden, ob der SK 12 eingesetzt wird und welche Maßnahmen der Datensicherung zusätzlich erforderlich sind. Die Deutsche Bundespost sollte eine technische Alternative zu dem SK 12 in ihr Angebot aufnehmen, bei der die Datensicherung nicht beeinträchtigt ist.

Erneut hatte ich Veranlassung, auf unzureichende Datensicherung bei Zugriffsmöglichkeiten über Datenendgeräte hinzuweisen (unten D.4.b). Damit wurde der Hinweis in meinem sechsten Tätigkeitsbericht (D.4.a), daß ein Paßwortschutz nur selten die erforderliche Authentifizierung mit hinreichender Sicherheit gewährleistet, durch Beobachtungen im Berichtsjahr leider bestätigt.

### 1. Maßnahmen der Strukturorganisation

#### a) Zuordnen und Abgrenzen von Funktionen

##### – Beauftragter für den Datenschutz

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. Der darin enthaltenen Verpflichtung, einen Beauftragten für den Datenschutz schriftlich zu bestellen, ist eine kontrollierte Stadt bisher nicht nachgekommen.

Ein kontrollierter Krankenkassenverband, der für seine Mitgliedskassen die automatisierte Datenverarbeitung in einem eigenen Rechenzentrum durchführt, hat zwar einen Beauftragten für den Datenschutz bestellt. Über die Aufgabenzuweisung des § 29 BDSG hinaus wurden aber keine Einzelheiten der Aufgaben des Beauftragten für den Datenschutz festgelegt.

Nach dem Organisationsplan des Krankenkassenverbandes (Stand: Juli 1979) war der Datenschutzbeauftragte in Personalunion für die Innenrevision zuständig. Nach dem Geschäftsverteilungsplan (Stand: April 1981) liegt die Zuständigkeit für die Innenrevision nicht mehr in Personalunion beim Datenschutzbeauftragten, der der Abteilung Allgemeine Verwaltung angehört. Für die Innenrevision ist vielmehr der Abschnitt Innenrevision, Beitragsrecht der Abteilung Versicherungsrecht zuständig.

In einem Diskussionspapier zum Geschäftsverteilungsplan der Abteilung EDV vom Juni 1985 ist innerhalb dieser Abteilung die Aufgabe EDV-Revision vorgesehen. Für diese Aufgabe soll der Abschnitt EDV-Organisation, Anwendungsberatung, EDV-Revision zuständig sein.

Im allgemeinen ist es organisatorisch angemessen und für die effektive Wahrnehmung aller Kontrollaufgaben günstig, die mit dem Datenschutz verbundenen zentralen Zuständigkeiten bei einer Person zusammenzufassen. Die Zuordnung der Aufgabe der EDV-Revision zum Beauftragten für den Datenschutz wäre für die Wahrnehmung der Kontrollaufgabe günstig. Eine Zuordnung der EDV-Revision zur EDV-Abteilung führt dagegen zu einer Interessenkollision, da Kontrollen der EDV-Revision vor allem der Arbeit der EDV-Abteilung gelten. Die EDV-Revision sollte daher nicht von einem Mitarbeiter der EDV-Abteilung wahrgenommen werden. Die Verpflichtung der EDV-Abteilung, die eigene Arbeit selbst zu kontrollieren, bleibt hiervon unberührt.

Auch eine Zuordnung der Innenrevision zum Beauftragten für den Datenschutz kann organisatorisch sinnvoll sein, da beide Aufgaben in enger Zusammenarbeit wahrgenommen werden sollten. Eine Personalunion in der Zuständigkeit ist aber nicht Voraussetzung für diese Zusammenarbeit. Gegen eine Zuordnung der Innenrevision zu einer anderen Organisationseinheit bestehen daher aus der Sicht des Datenschutzes keine Bedenken.

#### **- Interne Kontrolle**

Nach der Satzung eines Zweckverbandes, der eine kommunale Datenzentrale betreibt, obliegt die Prüfung der Geschäftsführung, der Wirtschaftsführung und der Betriebsabrechnung dem Rechnungsprüfungsamt des Kreises. Dies gilt auch für die fachbezogenen Prüfungen nach § 102 Abs. 1 Nr. 4 GO NW. Die Rechnungsprüfungsämter der übrigen Verbandsmitglieder sind nach Möglichkeit zu beteiligen.

Durch diese Regelungen wird dem Rechnungsprüfungsamt des Kreises unter anderem ein Teil der Aufgabe der internen Kontrolle des Datenschutzes übertragen. Eine darüber hinausgehende Regelung der internen Kontrolle gibt es bei der Datenzentrale nicht. Während des Kontrollbesuchs wurde die Möglichkeit besprochen, das Rechnungsprüfungsamt des Kreises mit der internen Kontrolle der Datensicherung insgesamt zu beauftragen.

Eine derartige Regelung würde von mir grundsätzlich begrüßt. In diesem Zusammenhang habe ich allerdings auf die Aufgaben des Rechnungsprüfungsamtes nach § 102 Abs. 1 Nr. 4 GO NW hingewiesen. Danach gehört zu den Aufgaben des Rechnungsprüfungsamtes bei Automation im Bereich der Haushaltswirtschaft die Prüfung der Programme vor ihrer Anwendung. Ich gehe davon aus, daß das Rechnungsprüfungsamt im Rahmen seiner Prüfung der Programme nicht in solchem Umfang eine Verantwortung für deren

Ordnungsmäßigkeit übernimmt, daß dadurch die Unbefangenheit bei der späteren Kontrolle beeinträchtigt werden könnte.

– **Zuständigkeit für Änderungen der Datei der freigegebenen Fassungen der Quellprogramme**

Vor ihrer Freigabe befinden sich Programme üblicherweise in maschinell geführten Testbibliotheken. Nach der Freigabe werden sie in die Bibliotheken der freigegebenen Programme übernommen. Für die Übernahme in die Bibliotheken der freigegebenen Programme ist die Arbeitsvorbereitung zuständig.

Wenn Programme ohne Beteiligung der Arbeitsvorbereitung in den Bibliotheken der freigegebenen Programme gespeichert werden können, ist die Datensicherheit deutlich beeinträchtigt. Aus Gründen der Datensicherheit sollte daher ausschließlich die Arbeitsvorbereitung für die Bibliotheken der freigegebenen Programme verantwortlich sein.

Bei einer kontrollierten kommunalen Datenzentrale ist die Arbeitsvorbereitung für die Bibliothek der freigegebenen Fassungen der ablauffähigen Programme zuständig. Änderungen in der Datei der ablauffähigen Fassungen der freigegebenen Programme können nur durch die Arbeitsvorbereitung vorgenommen werden.

Änderungen an freigegebenen Fassungen der Quellprogramme werden dagegen bei der Datenzentrale durch die Programmierer vorgenommen. Jeder Programmierer hat von seinem Datenendgerät Zugriff zu den freigegebenen Fassungen der Quellprogramme. Von den Datenendgeräten der Programmierer können auch unbemerkte Änderungen an den freigegebenen Fassungen der Quellprogramme vorgenommen werden. Über Datenendgeräte mit gleicher Berechtigung verfügen die bei der Datenzentrale tätigen Mitarbeiter des Rechnungsprüfungsamtes des Kreises. Auch von deren Datenendgeräten sind Änderungen an den freigegebenen Fassungen der Quellprogramme möglich.

Die Zuständigkeit der Programmierer für Änderungen an den freigegebenen Fassungen der Quellprogramme und die Möglichkeit unbemerkter Änderungen von den Datenendgeräten der Programmierer und der Mitarbeiter des Rechnungsprüfungsamtes sind sehr bedenklich. Für das Ändern von Programmen in der Bibliothek der freigegebenen Fassungen auch der Quellprogramme sollte ausschließlich die Arbeitsvorbereitung zuständig sein. Vor einer Änderung dieser Bibliothek sollte die Arbeitsvorbereitung in jedem Fall die Vollständigkeit und Ordnungsmäßigkeit des Freigabevorgangs überprüfen. Andere Stellen sollten keine Möglichkeit haben, Programme in den Bibliotheken der freigegebenen Programme zu speichern. Ich habe empfohlen, die Zuständigkeit für das Ändern der freigegebenen Fassungen der Quellprogramme und die Möglichkeiten des ändernden Zugriffs zu diesen Programmen entsprechend neu zu regeln.

– **Funktionstrennung zwischen der Systemprogrammierung und der Leitung der technischen Abwicklung**

Bei einer kontrollierten öffentlichen Stelle ist einer der Systemprogrammierer in Personalunion Leiter der technischen Abwicklung. Zu der technischen Abwicklung gehören neben der Systemprogrammierung die Bereiche Arbeitsvorbereitung, Maschinenbedienung, Archivverwaltung, Nachbereitung und Datenerfassung. Diese organisatorische Regelung ist unter dem Gesichtspunkt der Datensicherheit sehr bedenklich.

Es sollte eine Lösung gesucht werden, bei der die Verantwortung für die technische Abwicklung nicht in Personalunion bei einem Systemprogrammierer liegt. Bei der neuen organisatorischen Regelung könnte die System-

programmierung aus der technischen Abwicklung ausgegliedert werden. Es wäre aber auch unbedenklich, wenn die Systemprogrammierung weiterhin der technischen Abwicklung zugeordnet bliebe. In diesem Fall sollte die Leitung der technischen Abwicklung einem Mitarbeiter übertragen werden, der nicht in Personalunion Aufgaben der Systemprogrammierung durchführt.

## **b) Freigabe von Anwendungsprogrammen**

### **– Zuständigkeit des Anwenders**

Nach der Dienstanweisung eines kontrollierten Krankenkassenverbandes, der für seine Mitglieds-kassen die automatisierte Datenverarbeitung in einem eigenen Rechenzentrum durchführt, werden die Programme aus eigener Entwicklung durch den ADV-Abteilungsleiter freigegeben. Während des Kontrollbesuchs wurde ergänzend berichtet, daß Voraussetzung für die Freigabe ein Programmtest durch Mitarbeiter der ADV-Abteilung ist.

Die Erklärung der ADV-Abteilung, ein Programm sei fertiggestellt und fehlerfrei, ist als Freigabe von Anwendungsprogrammen nicht ausreichend. Als Voraussetzung der Freigabe muß vielmehr eine Bestätigung der Fehlerfreiheit des Programms durch den Anwender vorliegen. Erforderlich ist daher ein zusätzlicher Test durch den Anwender. Dieser Test könnte von einem Anwender des Krankenkassenverbandes oder einer Mitglieds-kasse durchgeführt werden. Die Freigabe des Programms könnte dann durch den Geschäftsführer des Krankenkassenverbandes erfolgen.

Der Entwurf der Dienstanweisung über die Organisation der ADV und des Datenschutzes bei einer kontrollierten Stadt enthält Vorschriften über die Freigabe von Programmen, die auf der eigenen Datenverarbeitungsanlage ablaufen sollen. Danach werden Programme für den Produktionseinsatz durch den Stadtdirektor oder durch den für die Organisation zuständigen Beigeordneten freigegeben.

In dem Entwurf der Dienstanweisung ist außerdem vorgeschrieben, daß die insbesondere für das Finanzwesen einzusetzenden Programme vom Rechnungsprüfungsamt für unbedenklich zu erklären sind. Ich habe darauf hingewiesen, daß es bedenklich wäre, die Unbedenklichkeitserklärung des Rechnungsprüfungsamtes als verbindliche Bestätigung der Richtigkeit des Programms anzusehen. Durch eine derartige Regelung würde möglicherweise die Unbefangenheit des Rechnungsprüfungsamtes bei der späteren Prüfung beeinträchtigt.

Für die übrigen Programme ist zwar vorgesehen, daß die Fachämter insbesondere bei der Entwicklung und Einführung von Verfahren für ihren Bereich mitwirken, Anregungen für einen möglichen DV-Einsatz geben und die fachlichen Grundlagen und Vorgaben für die DV-Verfahren zusammenstellen. Ein Programmtest durch den Anwender als Voraussetzung der Programmfreigabe ist in dem Entwurf der Dienstanweisung jedoch nicht vorgeschrieben. Nach Fertigstellung eines Programms reicht ein Testat der für die Programmierung verantwortlichen Stelle im allgemeinen für die Freigabe zum Produktionslauf nicht aus. Eine abschließende Überprüfung durch den Anwender (Anwendertest) ist sowohl bei neuentwickelten Programmen als auch dann erforderlich, wenn von einer Programmänderung der fachliche Programminhalt betroffen ist. In der Dienstanweisung sollte daher vorgeschrieben werden, daß ein Anwendertest die Voraussetzung für die Programmfreigabe darstellen muß.

Ein Teil der automatisierten Datenverarbeitung für diese Stadt wird bei einer kommunalen Datenzentrale abgewickelt. Vorschriften über die Freigabe der dabei eingesetzten Programme enthält das ADV-Organisationshandbuch der Datenzentrale. Danach gibt der Leiter der Datenzentrale ein Programm durch

schriftliche Verfügung zur Produktion frei. Für Programme im Bereich der Haushaltswirtschaft ist dazu die Unbedenklichkeitsbescheinigung des Rechnungsprüfungsamtes erforderlich. Darüber hinaus ist lediglich vorgeschrieben, daß die betroffenen Fachbereiche nach Möglichkeit und Notwendigkeit an dem Freigabeverfahren zu beteiligen sind. Zuständig für die Beteiligung der Fachbereiche ist der Organisator. Der Organisator ist grundsätzlich verpflichtet, im Rahmen von periodisch durchzuführenden Facharbeitskreisen über Programmneuerstellungen und Programmänderungen zu unterrichten.

Die Zuständigkeit des Anwenders für die Programmfreigabe kommt in diesen Regelungen nicht zum Ausdruck. Eine Freigabe durch den Anwender muß aber bei allen neuentwickelten Programmen und auch dann erfolgen, wenn von einer Programmänderung der fachliche Programminhalt betroffen ist. In diesen Fällen ist eine Freigabe durch den Leiter der Datenzentrale nicht ausreichend.

Wenn danach der Anwender für die Programmfreigabe zuständig ist, muß er sich durch eine abschließende Überprüfung des Programms (Anwendertest) von der Richtigkeit des Programms überzeugen. Es wurde bereits darauf hingewiesen, daß die Unbedenklichkeitsbescheinigung des Rechnungsprüfungsamtes einen Anwendertest nicht entbehrlich macht.

Ich habe empfohlen, bei der Datenzentrale nur solche Programme für die Verarbeitung personenbezogener Daten der kontrollierten Stadt einzusetzen, die durch den Anwender getestet und freigegeben wurden. Ferner habe ich empfohlen zu veranlassen, daß das ADV-Organisationshandbuch der Datenzentrale entsprechend überarbeitet wird.

#### **- Einzelregelungen**

Bei einer kontrollierten kommunalen Datenzentrale wird das Verfahren der Programmfreigabe durch eine Verwaltungsvereinbarung über das Freigabeverfahren bei gemeinsamen ADV-Programmen zwischen den Kreisen, für die diese Datenzentrale arbeitet, den diesen Kreisen angehörigen Städten und Gemeinden und der Datenzentrale geregelt. In der Verwaltungsvereinbarung ist festgelegt, daß die von der Datenzentrale für die automatisierte Bearbeitung von Verwaltungsaufgaben der Beteiligten eingesetzten Programme der Freigabe durch die Beteiligten bedürfen. In diesem Zusammenhang sollte zum Ausdruck gebracht werden, daß eine solche Freigabe durch den Anwender nicht nur bei neuentwickelten Programmen, sondern auch dann erfolgen muß, wenn von einer Programmänderung der fachliche Programminhalt betroffen ist. Lediglich bei systembedingten Programmänderungen, die ohne Einfluß auf den fachlichen Programminhalt sind, kann die Datenzentrale selbst über die Freigabe entscheiden.

Ergänzend ist in der Verwaltungsvereinbarung festgelegt, daß auf eine besondere Freigabe durch die Beteiligten verzichtet wird, soweit bei Einsatz eines überregionalen Gemeinschaftsverfahrens in einer Projektvereinbarung der Anwender die fachliche Freigabe der Programme geregelt ist. Diese Ausnahmeregelung sollte insoweit eingeschränkt werden, daß auf erneute Freigabe nur dann verzichtet wird, wenn bei der durch die Projektvereinbarung geregelten Freigabe die Verantwortung des Anwenders gewahrt ist. Die Freigaberegeln in der Projektvereinbarung muß daher sinngemäß dem in der Verwaltungsvereinbarung festgelegten Freigabeverfahren entsprechen.

Werden Programme von zwei oder mehr Beteiligten angewendet (gemeinsame Programme), wird die Freigabe dieser Programme durch die Verwaltungsvereinbarung dem Hauptverwaltungsbeamten des federführenden Fachamtes mit Wirkung für alle Beteiligten übertragen. Ergänzend zu dieser

Regelung sollte festgelegt werden, daß jeder einzelne der Auftraggeber im Hinblick auf seine Verantwortung als speichernde Stelle die von ihm erteilte Ermächtigung zur Programmfreigabe jederzeit widerrufen kann.

Nach der Verwaltungsvereinbarung beantragt die Datenzentrale rechtzeitig vor dem festgelegten Einführungstermin die Freigabe. Einen derartigen Antrag sollte die Datenzentrale nur dann stellen dürfen, wenn sie bestätigen kann, daß das Programm von der entwickelnden Stelle ordnungsgemäß getestet ist und erkannte Fehler beseitigt wurden. Daher sollte vorgeschrieben werden, daß die Datenzentrale dem Antrag auf Freigabe eine Erklärung über den erfolgreich abgeschlossenen Programmierertest beizufügen hat.

Bezüglich der für die Freigabe erforderlichen Programmtests regelt die Verwaltungsvereinbarung, daß die Kontrolle durch einen zeitlich begrenzten Parallelauf vorgenommen werden kann, wenn es notwendig und wirtschaftlich vertretbar ist. Nicht in jedem Fall ist sichergestellt, daß ein Programm durch einen Parallelauf ausreichend getestet werden kann. Es sollte daher vorgesehen werden, daß die Beschränkung auf den zeitlich begrenzten Parallelauf nur dann zulässig ist, wenn damit das Programm ausreichend getestet wird.

Nach der Verwaltungsvereinbarung kann der zuständige Arbeitsgruppenleiter die vorläufige Programmfreigabe erklären, wenn aus dringenden Termingründen der Programmeinsatz vor Abschluß der Programmfreigabe erfolgen muß. Es sollte vorgesehen werden, daß die vorläufige Programmfreigabe der Schriftform bedarf und die Freigabe durch den Anwender unverzüglich nachzuholen ist.

## 2. Maßnahmen der Ablauforganisation

### a) Sicherheit der Daten

#### - Weitergabe personenbezogener Daten an das Rechnungsprüfungsamt

In einem Beratungsgespräch des Rechnungsprüfungsamtes einer Stadt wurde die Frage vorgelegt, ob es zulässig sei, dem Rechnungsprüfungsamt über Datenendgeräte den ständigen Zugriff zu allen Dateien zu ermöglichen, zu deren Prüfung das Rechnungsprüfungsamt berechtigt ist.

Zwar ist die Weitergabe personenbezogener Daten durch ein Amt der Gemeinde an das Rechnungsprüfungsamt derselben Gemeinde keine Übermittlung im Sinne des Datenschutzgesetzes Nordrhein-Westfalen, weil das Rechnungsprüfungsamt kein Dritter ist (§ 2 Abs. 2 Nr. 2, Abs. 3 Nr. 2 DSGVO NW). Die Gemeinden haben jedoch für die Beachtung der Grundsätze über die Zulässigkeit der Übermittlung (§ 11 Abs. 1 DSGVO NW) auch dann zu sorgen, wenn personenbezogene Daten innerhalb der Gemeinde von einer Stelle an eine andere weitergegeben oder zur Einsichtnahme, namentlich zum Abruf, bereitgehalten werden (§ 8 Satz 1 DSGVO NW).

Nach § 11 Abs. 1 DSGVO NW ist die Übermittlung personenbezogener Daten an Behörden und sonstige öffentliche Stelle zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Empfängers liegenden Aufgaben erforderlich ist. Unterliegen die personenbezogenen Daten einem Berufs- oder besonderen Amtsgeheimnis und sind sie der übermittelnden Stelle von der zur Verschwiegenheit verpflichteten Person in Ausübung ihrer Berufs- oder Amtspflicht übermittelt worden, ist für die Zulässigkeit der Übermittlung ferner erforderlich, daß der Empfänger die Daten zur Erfüllung des gleichen Zwecks benötigt, zu dem sie die übermittelnde Stelle erhalten hat.

Jede der Dateien, zu deren Prüfung das Rechnungsprüfungsamt berechtigt ist, ist daher im Hinblick auf die dem Rechnungsprüfungsamt übertragenen Aufgaben einschließlich der internen Kontrolle im Sinne des Datenschutzgesetzes Nordrhein-Westfalen (oben D.1.a) daraufhin zu überprüfen, ob es nach § 8 Satz 1 in Verbindung mit § 11 Abs. 1 DSGVO zulässig ist, die Datei oder Teile der Datei zum Abruf bereitzuhalten. Dabei muß für jede Datei geprüft werden, ob es zulässig ist,

- die gesamte Datei ständig,
- Teile der Datei ständig,
- die gesamte Datei auf besondere Anforderung oder
- Teile der Datei auf besondere Anforderung

zum Abruf bereitzuhalten. Nur soweit und solange eine dieser Voraussetzungen erfüllt ist, darf dem Rechnungsprüfungsamt ein Zugriff in dem jeweiligen Umfang über Datenendgeräte ermöglicht werden. Nur in seltenen Ausnahmefällen wird es zulässig sein, eine gesamte Datei oder Teile einer Datei ständig zum Abruf bereitzuhalten. Die Möglichkeit, dem Rechnungsprüfungsamt über Datenendgeräte den ständigen Zugriff zu allen Dateien zu ermöglichen, zu deren Prüfung es berechtigt ist, scheidet dabei aus. Ich habe angeregt, zur Erleichterung der Arbeit des Rechnungsprüfungsamtes programmtechnische Voraussetzungen zu schaffen, die es dem jeweils zuständigen Fachamt ermöglichen, zukünftigen Anforderungen des Rechnungsprüfungsamtes in angemessener Frist zu entsprechen.

#### – **Maßnahmen zur Sicherung maschinenlesbar gespeicherter Daten**

Die Benutzer der Datenendgeräte einer kontrollierten Stadt haben je nach ihrem Aufgabengebiet unterschiedliche Befugnisse des Zugriffs zu den gespeicherten Daten. Die auf den Benutzer bezogenen Zugriffsbefugnisse sind in der Datenverarbeitungsanlage gespeichert. Die Zugriffsbefugnisse werden durch den ADV-Leiter in die Datenverarbeitungsanlage eingegeben und geändert.

Es ist allerdings nicht schriftlich geregelt, wer über den Umfang der Zugriffsbefugnisse der einzelnen Mitarbeiter entscheidet. Diese Festlegung sollte verbindlich getroffen werden. Es muß festgelegt sein, wer den ADV-Leiter anweisen darf, Zugriffsbefugnisse für die einzelnen Mitarbeiter in die Datenverarbeitungsanlage einzugeben oder bestehende Zugriffsbefugnisse zu ändern. Ich habe empfohlen, eine entsprechende Regelung in die Dienstanweisung aufzunehmen.

Bei einer kontrollierten kommunalen Datenzentrale wird fast ausschließlich mit Daten getestet, die nicht personenbezogen sind. In Sonderfällen wird allerdings auch mit personenbezogenen Daten getestet. In der Dienstanweisung sind diese Sonderfälle bisher nicht geregelt.

Bei einem kontrollierten Krankenkassenverband entscheidet der Leiter der EDV-Abteilung, ob ein Anonymisieren personenbezogener Daten, die bei Tests verwandt werden, erfolgen soll. Eine Regelung, unter welchen Voraussetzungen ein Test mit personenbezogenen Daten zulässig ist, besteht nicht.

Jedenfalls sollte in der Dienstanweisung festgelegt werden, daß ein Test mit personenbezogenen Daten nur mit Zustimmung des für diese Daten zuständigen Anwenders erfolgen darf. Diese Zustimmung sollte nur in begründeten Ausnahmefällen erteilt werden dürfen. Darüber hinaus sollte festgelegt werden, wer entscheidet, daß ein derartiger Ausnahmefall vorliegt. Ich habe jeweils empfohlen, die Verwendung nicht personenbezogener Daten als Regelfall in der Dienstanweisung vorzuschreiben und die Verwendung per-

sonenbezogener Testdaten für begründete Ausnahmefälle in der Dienstanweisung zu regeln.

Bei der oben erwähnten kommunalen Datenzentrale werden den Programmierern freigegebene Magnetbänder als Testbänder zugeordnet. Freigegebene Magnetbänder werden bei dieser Datenzentrale im allgemeinen nicht gelöscht. Es ist auch nicht vorgeschrieben, Magnetbänder, die einem Programmierer als Testbänder zur Verfügung gestellt werden, vorher zu löschen. Ein dem Programmierer zur Verfügung gestelltes freigegebenes Magnetband enthält daher den gesamten früheren Datenbestand.

Der einzelne Programmierer kann frei verfügen, welche Arbeiten mit einem ihm zugeordneten Testband ausgeführt werden. Er kann daher auch beliebige Verarbeitungen eventuell auf dem Testband stehender Daten veranlassen. Diese Beeinträchtigung der Datensicherheit läßt sich beseitigen, indem sichergestellt wird, daß den Programmierern für Testzwecke nur gelöschte Magnetbänder zur Verfügung gestellt werden. Ich habe empfohlen, eine entsprechende Regelung durch Dienstanweisung zu treffen.

## **b) Sicherung der Arbeitsdurchführung**

### **- Sicherheit der Programme**

Für jeden einzelnen Einsatz eines Programms, mit dem personenbezogene Daten verarbeitet werden, ist derjenige Anwender verantwortlich, der Herr dieser Daten ist. Die Verantwortlichkeit sollte dadurch zum Ausdruck kommen, daß der Anwender mit einem schriftlichen Auftrag den Programmlauf veranlaßt. Der Entwurf der Dienstanweisung über die Organisation der ADV und des Datenschutzes bei einer kontrollierten Stadt enthält Regelungen für die Arbeitsdurchführung. Dabei ist allerdings nicht vorgeschrieben, daß jeder Einsatz eines Programms, mit dem personenbezogene Daten verarbeitet werden, eines schriftlichen Auftrages des Anwenders bedarf. Ich habe daher empfohlen, die Dienstanweisung insoweit zu ergänzen. Darüber hinaus sollte vorgeschrieben werden, daß derartige Aufträge für eventuelle spätere Kontrollen hinreichend lange aufbewahrt werden. Ebenfalls aufbewahrt werden sollten maschinelle Aufzeichnungen der Datenverarbeitungsanlagen, die im einzelnen Auskunft über die zum Ablauf gekommenen Programme geben. Eine Aufbewahrungsdauer von wenigstens fünf Jahren ist im allgemeinen angemessen.

Moderne Verfahren der maschinellen Archivierung von Quellprogrammen machen es möglich, von den eingesetzten Programmen auch alle früher zum Einsatz gekommenen Fassungen automatisch zu archivieren. Auf dieser Grundlage ist für jeden Zeitpunkt der Vergangenheit rekonstruierbar, mit welcher Verarbeitungslogik ein Programm zum Einsatz gekommen ist.

Nach Einsatz einer neuen Programmversion wird bei einer kontrollierten kommunalen Datenzentrale das gesamte alte Programm archiviert. Alte Programme werden allerdings nur während etwa drei Monaten aufbewahrt und anschließend gelöscht. Sehr wünschenswert wäre es, die alten Fassungen der in der Vergangenheit zum Einsatz gekommenen Programme für einen wesentlich längeren Zeitraum zu archivieren. Angestrebt werden sollte ein Zeitraum von fünf Jahren. Hierzu könnte geprüft werden, ob ein auf dem Markt erhältliches Programm zur Verwaltung von Programmbibliotheken eine Möglichkeit der Archivierung aller Programmänderungen bietet. Andernfalls sollte geklärt werden, ob ein Archivieren der alten Fassungen der Gesamtprogramme, wie es bei der Datenzentrale für jeweils drei Monate verwirklicht ist, auf einen Zeitraum von fünf Jahren ausgedehnt werden kann. Mir ist bekannt, daß bei einem großen Rechenzentrum in Nordrhein-Westfalen so

verfahren wird. Ich habe empfohlen, eine Möglichkeit zu schaffen, daß frühere Programmstände über einen längeren Zeitraum rekonstruierbar sind.

#### **- Dienstanweisung für den technischen Betrieb**

Die Arbeit des technischen Betriebs einer kontrollierten Datenzentrale ist durch eine Dienstanweisung geregelt. In dieser Dienstanweisung ist vorgeschrieben, daß alle Meldungen, die vom Betriebssystem, der Systemsoftware und den übrigen Programmen auf dem Bedienungsplatz ausgegeben werden, täglich auf Magnetband zu sichern sind. In regelmäßigen Zeitabständen (etwa alle 3 Monate) sind diese Bedienungsplatzmeldungen auf Mikrofilme zu übertragen und 10 Jahre lang aufzubewahren.

Aufgezeichnete Systemnachrichten können unter anderem genutzt werden, um eventuelle Unregelmäßigkeiten nachträglich aufzuklären. Falls für eine derartige Aufklärung die Systemnachrichten eines längeren Zeitraums ausgewertet werden müssen, ist es sehr vorteilhaft, wenn die Systemnachrichten maschinenlesbar aufgezeichnet sind. Systemnachrichten werden daher üblicherweise auf Magnetband aufgezeichnet und archiviert. Eine Aufklärung von Unregelmäßigkeiten durch Auswerten der Systemnachrichten ist allerdings nur dann möglich, wenn die aufgezeichneten Systemnachrichten eine hinreichende Aussagekraft haben. Zur Erhöhung der Datensicherheit sollten daher hinreichend ausführliche Systemnachrichten über einen längeren Zeitraum maschinenlesbar archiviert werden.

In derselben Dienstanweisung ist festgelegt, daß ein Verlust von Datenträgern unverzüglich dem Leiter des technischen Betriebes, bei Datenträgern mit geschütztem Inhalt auch dem Leiter der Datenverarbeitungszentrale mitzuteilen ist. Ein Verlust von Datenträgern ist immer ein Hinweis auf eine ernste Beeinträchtigung der Datensicherheit. Ein derartiger Verlust sollte ausnahmslos dem Leiter der Datenverarbeitungszentrale gemeldet werden. Derartige Meldungen sollten nicht auf Fälle beschränkt werden, bei denen der Inhalt des Datenträgers zu schützen war.

Nach der Dienstanweisung ist der Verkauf des Altpapiers zur Zerkleinerung und Wiederaufbereitung als Rohstoff für die Papierindustrie zulässig, wenn der Käufer sich schriftlich zur Einhaltung der Datenschutzbestimmungen verpflichtet hat. Eine Vernichtung von Altpapier mit personenbezogenen Daten im Fremdauftrag ist aber nicht schon dann datenschutzrechtlich unbedenklich, wenn eine Firma sich verpflichtet, die Datenschutzvorschriften zu beachten. Die in der Dienstanweisung genannte Voraussetzung ist daher im allgemeinen nicht ausreichend. Die Anforderungen, die sich aus dem Datenschutzgesetz Nordrhein-Westfalen und aus dem Sozialgesetzbuch ergeben, werden in meinem zweiten (D.3.e) und fünften Tätigkeitsbericht (D.2.b) genannt. Ich habe empfohlen, die Regelung der Dienstanweisung unter Berücksichtigung dieser Anforderungen zu ergänzen.

### **3. Technische Maßnahmen**

#### **a) Schutz der Vertraulichkeit am Kassenschalter**

Bereits in meinem vierten (D.3.b) und meinem sechsten Tätigkeitsbericht (D.3.a) wurde darauf hingewiesen, daß es notwendig ist, die Vertraulichkeit von Gesprächen durch geeignete Maßnahmen sicherzustellen. Um die Vertraulichkeit am Kassenschalter zu gewährleisten, hat die Stadt-Sparkasse Düsseldorf ein Konzept entwickelt, das sie nach einer ersten Erprobung in ihrer Hauptstelle inzwischen auch bei einigen Zweigstellen verwirklicht hat. Der Raum vor dem Kassenschalter wird dabei in solchem Umfang von der Umgebung abgegrenzt,

daß der gerade bediente Kunde durch eine hinter ihm stehende Warteschlange nur noch wenig beeinträchtigt wird.

Der am Kassenschalter stehende Kunde hat hinter sich eine Holzwand, an deren linker und rechter Seite je ein Schwingelement für den Zu- und Abgang befestigt ist. Holzwand und Schwingelemente grenzen den Kunden, der gerade bedient wird, gegen die Umgebung und eine eventuelle Warteschlange ab. Die Schwingelemente wirken ähnlich wie Türen. Sie haben allerdings nur etwa die halbe Höhe.

In der Maßnahme der Stadt-Sparkasse Düsseldorf sehe ich eine wirksame Möglichkeit, mit relativ geringem Aufwand die Vertraulichkeit beim Kundenkontakt am Schalter weitgehend sicherzustellen. Eine Befragung der Kunden zeigte, daß die Maßnahme fast ausnahmslos begrüßt wird. Etwa 95 Prozent der Besucher gaben ein positives Urteil ab.

## **b) Sicherheitsbereich**

### **- Umfang des Sicherheitsbereichs**

Neben dem Rechenzentrum eines kontrollierten Krankenkassenverbandes befindet sich das Papierlager, das vom Rechenzentrum durch eine Wand aus Einbauschränken abgeteilt ist. Das Papierlager wird zusätzlich als Datenarchiv genutzt. Dazu ist im Papierlager ein offenes Regal aufgestellt, in das die archivierten Magnetbänder eingehängt sind. Rechenzentrum und Papierlager bilden den Sicherheitsbereich.

Rechenzentrum und Papierlager haben je eine Außentür mit zwei Türflügeln. Die Außentüren werden bei der Anlieferung von Material oder Geräten genutzt. In der übrigen Zeit sind die Außentüren verschlossen und über eine Türsicherung an die Alarmanlage angeschlossen. Ein Türflügel beider Außentüren wird jeweils durch einen Hebel festgestellt. Durch Betätigung des Hebels oder bei unzureichendem Feststellen dieses Hebels können auch verschlossene Außentüren grundsätzlich geöffnet werden.

Die Raumsituation des Sicherheitsbereichs ist sehr unbefriedigend. Das Papierlager ist ein Bereich, zu dem in gewissen Zeitabständen anliefernde Firmen Zugang haben müssen. Während der Anlieferungen ist eine Sicherung erfahrungsgemäß nur schwer durchführbar. Keinesfalls darf daher in dem Papierlager ein offenes Regal mit archivierten Magnetbändern aufgestellt sein. Die Abgrenzung zum Rechenzentrum sollte durch eine feste Wand erfolgen.

Während des Kontrollbesuchs wurden verschiedene Möglichkeiten für ein neues Raumkonzept erörtert. Im Rahmen dieses neuen Raumkonzeptes sollte jedenfalls das Datenarchiv vom Papierlager getrennt und das Papierlager möglichst aus dem Sicherheitsbereich herausgenommen werden. Es sollte darüber hinaus überprüft werden, welche der Außentüren notwendig sind. Bei einer eventuell noch notwendigen Außentür sollte sichergestellt werden, daß bei verschlossener Tür kein unsicherer Zustand bestehen kann.

Eine kontrollierte kommunale Datenzentrale verfügt über einen abgeschlossenen Sicherheitsbereich. Die Nachbereitung ist außerhalb dieses Sicherheitsbereichs untergebracht. Dadurch ist die Datensicherheit beeinträchtigt. Während des Kontrollbesuchs wurde besprochen, welche Möglichkeiten bestehen, die Nachbereitung im Sicherheitsbereich unterzubringen. Eine entsprechende räumliche Lösung sollte jedenfalls langfristig angestrebt werden.

### **- Sicherungsmaßnahmen für den Sicherheitsbereich**

Es ist eine übliche Sicherungsmaßnahme bei Rechenzentren, durch Bewegungsmelder oder sonstige Geräte eine Raumsicherung zu verwirklichen.

Der Sicherheitsbereich einer kontrollierten kommunalen Datenzentrale verfügt über keine Raumsicherung. Dadurch ist die Sicherheit beeinträchtigt.

Unbefugter Zugang zu dem Sicherheitsbereich der Datenzentrale ist außerhalb der Dienstzeit über die ungesicherten Fenster des unter dem Sicherheitsbereich liegenden Kellers möglich. Zusätzlich sind dazu zwar noch die Türen des Sicherheitsbereichs zu überwinden. Diese liegen aber sämtlich innerhalb des Gebäudes. Arbeiten an den Türen könnten daher unbeobachtet erfolgen. Während des Kontrollbesuchs wurde diese Unsicherheit besprochen. Eine Raumsicherung im Maschinenraum und im Datenträgerarchiv könnte die bestehende Unsicherheit beseitigen. Ich habe empfohlen, für den Maschinenraum und für das Datenträgerarchiv eine Raumsicherung vorzusehen.

Die Fenster des Sicherheitsbereichs der Datenzentrale sind in Panzerglas ausgeführt. Die Fensterflügel können allerdings geöffnet werden. Es muß daher damit gerechnet werden, daß ein Fensterflügel außerhalb der Dienstzeit nicht geschlossen ist. Dadurch ist die Datensicherheit beeinträchtigt. Ich habe empfohlen, die Fenster des Sicherheitsbereichs durch eine Alarmanlage zu sichern, die anspricht, wenn ein Fensterflügel nicht geschlossen ist.

Von dem wenig gesicherten Keller unter dem Sicherheitsbereich der Datenzentrale führt ein Lastenaufzug in den Maschinenraum. In dem Lastenaufzug könnte auch eine Person befördert werden. Während des Kontrollbesuchs wurde besprochen, daß ein Vorhängeschloß an der Aufzugtür im Maschinenraum die Sicherheit wesentlich erhöhen würde. Die zusätzlich erforderlichen Vorrichtungen sind leicht anzubringen.

Duplikate der wichtigsten Dateien eines kontrollierten Krankenkassenverbandes werden regelmäßig ausgelagert. Als Auslagerungsarchiv dient ein verschlossener Keller einer Mitgliedskasse, zu dem ein größerer Personenkreis Zugang hat. In diesem Keller verfügt der Krankenkassenverband über einen verschließbaren Schrank. Bei einer Begehung wurde festgestellt, daß die Schlüsselnummer von außen sichtbar in das Schloß dieses Schanks eingeprägt war.

Die Datensicherheit der in dem Schrank verschlossen aufbewahrten Datenträger ist beeinträchtigt, solange die Schlüsselnummer von außen sichtbar in das Schloß eingeprägt ist. Auf einen entsprechenden Hinweis hat der Krankenkassenverband noch während des Kontrollbesuchs die Schlüsselnummer entfernt. Ich habe empfohlen, darüber hinaus auch den Schließzylinder des als Auslagerungsarchiv dienenden Schanks baldmöglichst auszuwechseln. Auf dem neuen Schließzylinder sollte die Schlüsselnummer nicht von außen sichtbar angegeben sein.

Zur Datensicherung werden die Dateien einer kontrollierten Stadt auf Magnetplatten ausgelagert. Als Auslagerungsarchiv dient ein Tresorraum, zu dem verschiedene Ämter der Stadt Zugang haben. In dem Tresorraum sind die Magnetplatten ungeschützt abgelegt. Eine Nutzung der Magnetplatten durch Dritte wäre nicht erkennbar. Eine zusätzliche Sicherung der Magnetplatten in dem als Auslagerungsarchiv dienenden Tresorraum sollte jedenfalls in solchem Umfang erfolgen, daß eine unbefugte Nutzung der Magnetplatten durch Dritte nicht unerkannt bleiben könnte. Die Stadt hat bereits während des Kontrollbesuchs einen verschließbaren Schrank in dem Auslagerungsarchiv aufgestellt, in dem die Magnetplatten jetzt unter Verschluss aufbewahrt werden.

In zwei Fällen wurde bei dem Kontrollbesuch in einer Schule festgestellt, daß geeignete verschließbare Schränke fehlen. Wechselplatten und Disketten mit personenbezogenen Daten werden innerhalb eines verschlossenen Raums in einem nicht verschließbaren Schrank aufbewahrt. Für diese Datenträger

sollte ein verschließbarer Schrank zu Verfügung gestellt werden. Die Beratungsunterlagen des Oberstufenkoordinators sind innerhalb eines verschlossenen Raums in einem einfachen Schrank mit Rolltür untergebracht, der nur eine geringe Sicherung bietet. Dieser Schrank sollte durch einen besser gesicherten Schrank ersetzt werden. Ich habe empfohlen, in diesen Fällen jeweils einen geeigneten verschließbaren Schrank zur Verfügung zu stellen.

- **Zugangsmöglichkeit der Feuerwehr außerhalb der Dienstzeit**

Der Maschinensaal einer kontrollierten kommunalen Datenzentrale ist durch eine Feuermeldeanlage gesichert. Bei einem Brand wird durch diese Anlage die Feuerwehr automatisch alarmiert. Um der Feuerwehr ein Betreten des Gebäudes und des Sicherheitsbereichs zu ermöglichen, ist in die Außenwand des Gebäudes der Datenzentrale ein Notschlüsselkasten eingelassen. In diesem Notschlüsselkasten befinden sich die Schlüssel für das Gebäude der Datenzentrale und den Sicherheitsbereich.

Der Notschlüsselkasten ist durch eine äußere und eine innere Tür gesichert. Die äußere Tür kann von außen normalerweise nicht geöffnet werden. Sie wird aber automatisch freigegeben, sobald die Feuermeldeanlage anspricht. Durch das Öffnen der äußeren Tür wird die innere Tür zugänglich. Die innere Tür ist verschlossen. Über den Schlüssel für die innere Tür verfügt die Feuerwehr. Im Brandfall kann die Feuerwehr daher die innere Tür mit ihrem Schlüssel öffnen und hat dann Zugriff zu den Schlüsseln für das Gebäude und den Sicherheitsbereich.

Durch die geschilderte Technik ist zwar sichergestellt, daß die Feuerwehr nur dann den Sicherheitsbereich betreten kann, wenn die Alarmanlage angesprochen hat. Es ist aber nicht sichergestellt, daß ein Betreten des Sicherheitsbereichs durch die Feuerwehr in jedem Fall für die Datenzentrale nachträglich erkennbar wird. Insofern ist die Datensicherheit beeinträchtigt. Es sollte daher durch eine geeignete Maßnahme sichergestellt werden, daß ein Betreten des Sicherheitsbereichs durch die Feuerwehr nachträglich für die Datenzentrale erkennbar ist.

Zum Schutz des Notschlüsselkastens ist es wünschenswert, dessen äußere Tür an eine Alarmanlage anzuschließen. Die Technik des Notschlüsselkastens sieht einen solchen Anschluß vor. Von dieser Möglichkeit sollte jedenfalls dann Gebrauch gemacht werden, wenn für den Sicherheitsbereich eine Alarmanlage eingebaut wird.

#### 4. Organisatorisch-technische Maßnahmen

**a) Beeinträchtigung der Datensicherheit bei Einsatz des Schnittstellenvervielfachers SK 12 der Deutschen Bundespost**

Durch den Hessischen Datenschutzbeauftragten bin ich darauf hingewiesen worden, daß der Datenschutz in Datennetzen bei Verwendung des Schnittstellenvervielfachers SK 12 der Deutschen Bundespost (SK 12) nicht gewährleistet sei. Ein Teilnehmer könne nicht nur die für ihn bestimmten Daten empfangen, sondern nach Manipulation an der Datenendeinrichtung oder durch Aufschalten eines Leitungsmonitors auch alle Daten, die für irgendwelche anderen Teilnehmer bestimmt sind, die hinter dem SK 12 angeschlossen sind. Die Gefährdung der Datensicherheit sei für die Benutzer nicht ohne weiteres ersichtlich. Ich habe daraufhin dem Innenminister empfohlen untersuchen zu lassen, ob und in welchem Umfang die aufgezeigte Gefährdung der Datensicherheit besteht.

Die inzwischen abgeschlossene Untersuchung hat bestätigt, daß bei Einsatz des SK 12 die Datensicherheit beeinträchtigt ist. Die Beeinträchtigung der Datensicherheit

cherheit liegt darin, daß der SK 12 Daten, die von einer Datenverarbeitungsanlage an eine hinter dem SK 12 angeschlossene Dateneneinrichtung gesendet werden, in alle hinter dem SK 12 angeschlossenen Leitungen überträgt.

– **Unbefugte Kenntnisnahme von Daten durch Mitarbeiter oder Dritte (mit Ausnahme der Wartungstechniker)**

Die Möglichkeiten, bei Einsatz des SK 12 die Datensicherung gegen unbefugte Kenntnisnahme von Daten durch Mitarbeiter oder Dritte zu gewährleisten, sind von der Gestaltung des Datennetzes abhängig. Dabei ist unter anderem zu unterscheiden, ob sämtliche Anschlüsse für Dateneneinrichtungen hinter dem SK 12 bei derselben öffentlichen Stelle oder bei verschiedenen öffentlichen Stellen liegen.

- Falls sämtliche Anschlüsse für Dateneneinrichtungen hinter dem SK 12 bei derselben öffentlichen Stelle liegen, muß diese sicherstellen, daß eine unbefugte Kenntnisnahme der Daten, die der SK 12 in die Leitungen überträgt, ausgeschlossen ist. Dazu muß der öffentlichen Stelle die durch die Arbeitsweise des SK 12 bedingte Gefährdung der Datensicherheit bekannt sein; die öffentliche Stelle muß daher auf diese Gefährdung ausdrücklich hingewiesen werden.

Eine allgemeine Aussage, ob und wie die Datensicherheit durch die öffentliche Stelle gewährleistet werden kann, ist nicht möglich. Für jedes Datennetz muß daher geprüft werden, welche Maßnahmen zur Datensicherung erforderlich sind und ob mit diesen Maßnahmen die Datensicherheit gewährleistet werden kann.

An die zu treffenden Maßnahmen sind nur geringe Anforderungen zu stellen, wenn alle Mitarbeiter, die an den hinter dem SK 12 angeschlossenen Dateneneinrichtungen tätig sind, gleiche Zugriffsbefugnisse haben. In diesem Fall kann die Datensicherung im allgemeinen angemessen gewährleistet werden; gegen den Einsatz des SK 12 bestehen dann keine durchgreifenden Bedenken.

- Falls an ein Rechenzentrum verschiedene öffentliche Stellen hinter demselben SK 12 angeschlossen sind, werden Daten, die das Rechenzentrum an eine der öffentlichen Stellen (Adressat) sendet, zusätzlich in die zu den anderen öffentlichen Stellen führenden Leitungen übertragen. Der Adressat kann Maßnahmen zur Datensicherung im eigenen Bereich durchsetzen. Er kann darüber hinaus Maßnahmen zur Datensicherung bei dem Rechenzentrum durchsetzen, soweit dieses Datenverarbeitung im Auftrag des Adressaten durchführt. Das Rechenzentrum kann Maßnahmen der Datensicherung im eigenen Bereich durchsetzen.

Die Durchführung von Maßnahmen zur Datensicherung bei den übrigen angeschlossenen öffentlichen Stellen kann im allgemeinen weder der Adressat noch das Rechenzentrum sicherstellen. Beide können daher bei dieser Netzkonfiguration nicht sicherstellen, daß eine unbefugte Kenntnisnahme der von dem Rechenzentrum an den Adressaten gesendeten Daten im Bereich der anderen angeschlossenen öffentlichen Stellen ausgeschlossen ist.

Die Datensicherheit kann deshalb im allgemeinen nicht gewährleistet werden, wenn Anschlüsse für Dateneneinrichtungen hinter demselben SK 12 bei verschiedenen öffentlichen Stellen liegen. Diese Netzkonfiguration ist in einem solchen Fall unzulässig.

– **Unbefugte Kenntnisnahme von Daten durch Wartungstechniker**

Ein Wartungstechniker, der die Wartung einer Dateneneinrichtung oder eines sonstigen an eine Datenleitung angeschlossenen Geräts durchzuführen

ren hat, kann im allgemeinen von der öffentlichen Stelle, bei der die Dateneinrichtung oder das sonstige Gerät aufgestellt ist, nicht fachlich beaufsichtigt werden. Es ist davon auszugehen, daß der Wartungstechniker Daten, die über eine Leitung übertragen werden, auch dann zur Kenntnis nehmen kann, wenn die zu wartende Dateneinrichtung oder das zu wartende Gerät außer Betrieb oder defekt ist. Der Wartungstechniker kann daher über alle Daten verfügen, die auf einer Leitung, zu der er Zugriff hat, übertragen werden. Derartige Daten werden somit für den Wartungstechniker zum Abruf bereitgehalten. Da Wartung keine Datenverarbeitung im Auftrag ist, gelten daher alle Daten als übermittelt, die während des Wartungsvorgangs über eine Leitung übertragen werden, zu der der Wartungstechniker Zugriff hat.

Grundsätzlich könnte die Datensicherheit dadurch gewährleistet werden, daß über eine Leitung solange keine personenbezogenen Daten übertragen werden, wie der Wartungstechniker Zugriff zu dieser Leitung hat. Die Tätigkeit des Wartungstechnikers wäre in diesem Fall zulässig. Soweit der Wartungstechniker eine Datenübertragung als Voraussetzung des Wartungsvorganges benötigt, könnte die Übertragung von Testdaten, die nicht personenbezogen sind, vorgesehen werden.

Falls personenbezogene Daten über eine Leitung übertragen werden, während der Wartungstechniker Zugriff zu dieser Leitung hat, ist die in diesem Fall erfolgende Übermittlung personenbezogener Daten an den Wartungstechniker nur unter den Voraussetzungen des § 13 Abs. 1 Satz 1 DSGVO bzw. des § 69 Abs. 1 Nr. 1 SGB X zulässig. Es ist davon auszugehen, daß diese Voraussetzungen nur in seltenen Fällen erfüllt sind. Darüber hinaus ist eine mögliche zusätzliche Einschränkung der Übermittlung nach § 13 Abs. 1 Satz 2 DSGVO und § 76 SGB X zu beachten.

Bedingt durch die Arbeitsweise des SK 12 werden möglicherweise während des Wartungsvorgangs personenbezogene Daten übermittelt, die das Rechenzentrum an eine andere als die zu wartende Dateneinrichtung gesandt hat. Für deren Übermittlung ist die Zustimmung des für diese Daten zuständigen Anwenders erforderlich. Die Übermittlung derartiger Daten wird darüber hinaus nicht als zulässig angesehen werden können, falls es technisch möglich ist, mit angemessenem Aufwand ein gleichwertiges Datennetz zu errichten, in dem diese durch die Arbeitsweise des SK 12 bedingte Übermittlung vermieden wird.

#### **- Schlußfolgerungen**

Bei Einsatz des Schnittstellenvervielfachers SK 12 ist die Datensicherheit beeinträchtigt. Der Umfang der Beeinträchtigung der Datensicherheit hängt stark von den Umständen des Einzelfalls und insbesondere von dem Netzkonzept ab. Um die erforderliche Datensicherheit zu gewährleisten, habe ich dem Innenminister folgende Maßnahmen empfohlen:

- Die obersten Landesbehörden werden über die Beeinträchtigung der Datensicherheit bei Einsatz des Schnittstellenvervielfachers SK 12 informiert.
- Die obersten Landesbehörden untersuchen alle Datennetze innerhalb ihres eigenen Geschäftsbereichs im Hinblick auf die Gefährdung der Datensicherheit durch den SK 12. In diese Untersuchung sind auch alle Datennetze nachgeordneter Behörden einzubeziehen. Soweit sich dabei herausstellt, daß die Datensicherheit nicht gewährleistet ist, sind geeignete Maßnahmen zu treffen.

Darüber hinaus habe ich den Innenminister darauf hingewiesen, daß ich folgende zusätzliche Maßnahmen begrüßen würde:

- Es sollten die technischen Möglichkeiten für den Ersatz des SK 12 ermittelt und bewertet werden.
- Der Kooperationsausschuß ADV Bund/Länder/Kommunaler Bereich (KoopA ADV) sollte veranlaßt werden, bei der Deutschen Bundespost anzuregen, eine Alternative für den SK 12 in das Angebot aufzunehmen, bei deren Einsatz die durch die Arbeitsweise des SK 12 bedingte Beeinträchtigung der Datensicherheit vermieden wird.

## **b) Datensicherung bei On-line-Zugriff**

### **- Paßwortschutz**

In fast jedem meiner Tätigkeitsberichte hatte ich Veranlassung, auf Schwächen des Paßwortschutzes einzugehen, die ich bei Kontrollbesuchen festgestellt hatte. Maßnahmen, die dazu dienen, einen Paßwortschutz sicher zu gestalten, werden insbesondere in meinem vierten (D.4.a), fünften (D.4.c) und sechsten Tätigkeitsbericht (D.4.a) dargestellt. Trotz der Möglichkeit, mit einem gut organisierten Paßwortschutz Datenbestände außerordentlich wirksam zu schützen, mußte ich in meinem sechsten Tätigkeitsbericht feststellen, daß ich inzwischen davon ausgehe, daß ein Paßwortschutz nur selten die erforderliche Authentifizierung mit hinreichender Sicherheit gewährleistet. Feststellungen im Berichtsjahr haben diese Ansicht leider bestätigt.

Über die in den Räumen einer kontrollierten kommunalen Datenzentrale aufgestellten Datenendgeräte verkehren die Mitarbeiter als Teilnehmer mit dem Datenverarbeitungssystem. Die Datenendgeräte sind durch Paßworte gesichert, die von den einzelnen Mitarbeitern selbst vergeben werden. Die Länge der Paßworte reicht von 0 bis 21 Zeichen. Dabei bedeutet die Möglichkeit der Vergabe eines Paßwortes von 0 Zeichen, daß der Mitarbeiter sogar auf die Vergabe des Paßwortes verzichten kann. Ein Änderungsintervall für die Paßworte ist nicht vorgeschrieben. Es wird nicht durch die Datenverarbeitungsanlage überwacht, ob Paßworte jemals geändert werden. Die Datenverarbeitungsanlage überprüft auch nicht, ob Versuche gemacht werden, gültige Paßworte durch Probieren zu finden. Bei Eingabe eines ungültigen Paßwortes wird zwar kein Zugriff zu den Anwendungsprogrammen eröffnet. Der Benutzer kann aber beliebig viele weitere Zugriffsversuche mit anderen Paßworten unternehmen. Ein Abschalten des Datenendgeräts nach einigen Fehlversuchen mit einem ungültigen Paßwort ist nicht vorgesehen. Durch die Datenverarbeitungsanlage wird auch keine Statistik erstellt, die einen Überblick über den Umfang derartiger Fehlversuche geben könnte.

Die Mitarbeiter sind nicht durch Dienstanweisung verpflichtet, ihre Paßworte geheimzuhalten. Es besteht auch keine Verpflichtung, Paßworte nur dann einzugeben, wenn kein Dritter die Eingabe beobachten kann.

Dieser Paßwortschutz muß als fast unwirksam bezeichnet werden. Es ist mit der Möglichkeit zu rechnen, daß die Mitarbeiter sich sehr kurze oder gar keine Paßworte vergeben. Da darüber hinaus weder Änderungsintervalle noch sonstige Sicherungsmaßnahmen für die Paßworte vorgeschrieben sind, ist davon auszugehen, daß Paßworte auch interessierten Dritten bekannt sein können. Der mit dem Paßwortverfahren angestrebte Schutz ist daher kaum vorhanden.

Durch den bei einem kontrollierten Krankenkassenverband eingesetzten Paßwortschutz werden nur Benutzerbereiche der Programmierer und der Arbeitsvorbereiter, aber weder personenbezogene Daten noch freigegebene Programme geschützt. Der bestehende Paßwortschutz hat daher im Rahmen der Maßnahmen zur Datensicherung nur eine geringe Bedeutung. Dennoch wurde der Paßwortschutz während des Kontrollbesuchs auf seine Schutzwirkung überprüft.

Eingesetzt werden Paßworte von maximal sechs Stellen. Eine minimale Stellenzahl, die zur Datensicherung zu fordern wäre, ist nicht vorgegeben. Die Paßworte werden durch die einzelnen Mitarbeiter selbst vergeben. Änderungsintervalle sind für die Paßworte nicht vorgeschrieben. Eine Anweisung, Paßworte geheimzuhalten, besteht nicht. Durch das Datenverarbeitungssystem werden keine Maßnahmen ergriffen, wenn nacheinander mehrere Versuche der Benutzung des Systems mit falschen Paßworten unternommen werden. Die Paßworte sind unverschlüsselt gespeichert. Wegen eines fehlenden Schutzes der gespeicherten Dateien ist es Unbefugten mit gewissen Systemkenntnissen daher möglich, die gültigen Paßworte der Datenverarbeitungsanlage zu entnehmen.

Dieser Paßwortschutz ist fast unwirksam. Bedenklich sind insbesondere das Fehlen einer Mindestlänge der Paßworte, eines vorgeschriebenen Änderungsintervalls, einer Verpflichtung zur Geheimhaltung der Paßworte und einer angemessenen Reaktion des Datenverarbeitungssystems auf mehrfache Benutzung unzulässiger Paßworte. Im Hinblick darauf, daß die Datei der gespeicherten Paßworte nicht geschützt ist, erscheint darüber hinaus eine verschlüsselte Speicherung der Paßworte erforderlich. In meinem zweiten Tätigkeitsbericht (D.5.a) habe ich das Verfahren der Einwegverschlüsselung zur Sicherung gespeicherter Paßworte geschildert.

Ich habe jeweils empfohlen, geeignete Maßnahmen zur Verbesserung des Paßwortschutzes zu treffen. Dem Krankenkassenverband habe ich darüber hinaus empfohlen, den Hersteller der Datenverarbeitungsanlage auf die Erforderlichkeit einer Verschlüsselung von ungeschützt gespeicherten Paßworten hinzuweisen.

Bei einer kontrollierten Stadt, deren Programme die Lieferfirma der Datenverarbeitungsanlage entwickelt hat, werden die Paßworte von den einzelnen Mitarbeitern vergeben. Eine Änderung der Paßworte wird weder vom Programm erzwungen noch durch Dienstanweisung vorgeschrieben.

Die Wirkung des Paßwortschutzes bei der Stadt ist deutlich dadurch beeinträchtigt, daß die Paßworte über einen langen Zeitraum unverändert bleiben können. Günstig wäre es, wenn die eingesetzten Programme eine Änderung der Paßworte nach einer gewissen Zeit erzwingen würden. Dazu könnte jedem Paßwort eine maximale Gültigkeitsdauer zugeteilt werden, nach deren Ablauf das Paßwort von den Programmen nicht mehr als gültig anerkannt würde. Diese maximale Gültigkeitsdauer sollte nicht länger als einen Monat betragen. Zusätzlich sollte durch Dienstanweisung die Änderung der Paßworte vorgeschrieben werden. Ich habe darüber hinaus empfohlen, bei der Lieferfirma eine Programmänderung anzuregen, die ein automatisches Überwachen der Änderung von Paßworten möglich macht.

Bei derselben Stadt werden die Datenendgeräte nach 10 nacheinander erfolgenden Eingaben ungültiger Paßworte durch die Datenverarbeitungsanlage automatisch abgeschaltet. Dadurch wird bereits ein gewisser Schutz gegen unzulässige Versuche, Paßworte in Erfahrung zu bringen, erreicht. Ein Abschalten der Datenendgeräte sollte allerdings nicht erst nach 10 derartigen Versuchen erfolgen. Üblich ist es, Datenendgeräte bereits nach 3 nacheinander erfolgenden Eingaben ungültiger Paßworte automatisch abzuschalten. Ich habe empfohlen, durch die Lieferfirma das eingesetzte Programm entsprechend ändern zu lassen.

Jeder einzelne zum Zugriff berechtigte Mitarbeiter dieser Stadt vergibt sich sein Paßwort selbst. Er teilt dieses Paßwort dem ADV-Leiter mit. Das Paßwort wird dann durch den ADV-Leiter in die Datenverarbeitungsanlage eingegeben.

Durch dieses Verfahren werden sämtliche Paßworte dem ADV-Leiter bekannt. Zur Verbesserung der Datensicherheit wäre es zweckmäßig, wenn jeder Mitarbeiter sein Paßwort selbst in die Datenverarbeitungsanlage eingeben könnte. Der ADV-Leiter würde in diesem Fall keine Kenntnis der vergebenen Paßworte erhalten. Ich habe empfohlen vorzuschreiben, daß die Mitarbeiter ihre Paßworte selbst in die Datenverarbeitungsanlage eingeben, und erforderlichenfalls die Lieferfirma zu einer entsprechenden Programmänderung zu veranlassen.

- **Beschränken von Möglichkeiten des Zugriffs**

Anwendungsprogramme werden bei einem kontrollierten Krankenkassenverband nach ihrer Freigabe in die Produktionsbibliothek übernommen. Für die Übernahme ist die Arbeitsvorbereitung zuständig. Aus Gründen der Datensicherheit sollte ausschließlich die Arbeitsvorbereitung eine Möglichkeit zum Ändern der Produktionsbibliothek haben.

Bei dem Krankenkassenverband ist die Produktionsbibliothek nicht geschützt. Ein Zugriff zur Produktionsbibliothek ist den Programmierern und den Maschinenbedienern von ihren Datenendgeräten möglich. Unbemerkte Änderungen an Programmen der Produktionsbibliothek können daher nicht ausgeschlossen werden. Die Datensicherheit ist dadurch deutlich beeinträchtigt.

Änderungen an Systemprogrammen des Krankenkassenverbandes werden ausschließlich in Absprache mit dem Bundesverband durchgeführt. Der Krankenkassenverband sollte daher mit dem Bundesverband und der Lieferfirma seiner Datenverarbeitungsanlage klären, auf welche Weise ein Schutz der Produktionsbibliothek verwirklicht werden kann. Ein derartiger Schutz sollte baldmöglichst eingeführt werden. Ich habe empfohlen, baldmöglichst geeignete Maßnahmen zum Schutz der Produktionsbibliothek zu treffen.

Die Verarbeitung personenbezogener Daten erfolgt bei dem Krankenkassenverband ausschließlich durch Stapelverarbeitung. Die vorhandenen Anwendungsprogramme ermöglichen keinen direkten Zugriff von den Datenendgeräten des Krankenkassenverbandes zu den auf Magnetplatten aufgezeichneten Daten. Wegen des Fehlens dieser Möglichkeit wurde darauf verzichtet, die auf Magnetplatten gespeicherten Dateien gegen unbefugten Zugriff zu schützen.

Grundsätzlich ist es möglich, von jedem Datenendgerät des Krankenkassenverbandes ein Programm zu entwickeln und zum Ablauf zu bringen, das einen Zugriff zu den auf Magnetplatten gespeicherten Dateien ermöglicht. Mit entsprechenden Kenntnissen können Mitarbeiter des Krankenkassenverbandes von allen Datenendgeräten zu allen auf Magnetplatten gespeicherten Dateien zugreifen und dabei die gespeicherten Daten lesen oder auch ändern.

Durch diese Möglichkeit ist die Datensicherheit stark beeinträchtigt. Während des Kontrollbesuchs konnte nicht geklärt werden, ob sich die bestehende Unsicherheit kurzfristig beseitigen läßt. Es wurde besprochen, daß diese Klärung umgehend erfolgen und die Möglichkeit des unkontrollierten Zugriffs zu gespeicherten Daten schnellstmöglich beseitigt werden sollte. Ich habe empfohlen, möglichst umgehend Maßnahmen zum Schutz der auf Magnetplatten gespeicherten Dateien mit personenbezogenen Daten gegen unbefugten Zugriff zu treffen.

- **Beschränken der Befugnisse von Datenendgeräten**

Es ist nicht leicht sicherzustellen, daß ein Datenendgerät, das zur interaktiven Programmierung eingesetzt werden kann, nicht für unzulässige Zugriffe zu

Dateien und Programmen genutzt werden kann. Die interaktive Programmierung kann gerade dem fachlich qualifizierten Mitarbeiter Wege zu unzulässigen Transaktionen ermöglichen. Daher sollte jedenfalls sichergestellt sein, daß interaktive Programmierung nur mit solchen Datenendgeräten möglich ist, bei denen dafür eine dienstliche Notwendigkeit besteht.

Bei einem kontrollierten Krankenkassenverband wird für die interaktive Programmierung ein Programm eingesetzt, das eine Trennung der Möglichkeit des interaktiven Programmierens von Funktionen, die im Maschinenraum und bei der Arbeitsvorbereitung verfügbar sein müssen, nicht zuläßt. Interaktive Programmierung ist daher auch an den Datenendgeräten des Maschinenraums und der Arbeitsvorbereitung möglich. Es sollte angestrebt werden, diese Datenendgeräte in ihrer Funktion so einzuschränken, daß ein interaktives Programmieren nicht mehr möglich ist.

Dazu sollte mit der Lieferfirma des Programms geklärt werden, ob es eine Programmversion gibt, die diese Einschränkung ermöglicht. Falls keine derartige Programmversion verfügbar ist, sollte spätestens bei einem Wechsel der eingesetzten Datenverarbeitungsanlage sichergestellt werden, daß die Datenendgeräte des Maschinenraums und der Arbeitsvorbereitung keine interaktive Programmierung ermöglichen. Ich habe empfohlen, Maßnahmen zu treffen, damit ein interaktives Programmieren an den Datenendgeräten des Maschinenraums und der Arbeitsvorbereitung baldmöglichst ausgeschlossen wird.

Die Arbeitsvorbereiter einer kontrollierten kommunalen Datenzentrale verkehren als Teilnehmer mit der Datenverarbeitungsanlage. Bei der Arbeit als Teilnehmer bietet das verwendete Betriebssystem nicht die Möglichkeit, das interaktive Programmieren auszuschließen. Dazu wäre vielmehr ein Verkehr mit der Datenverarbeitungsanlage als Teilhaber erforderlich.

Die Datenzentrale entwickelt zur Zeit ein Programm für die Abwicklung der Arbeitsvorbereitung. Nach Fertigstellung dieses Programms können die Arbeitsvorbereiter als Teilhaber des Systems auf die Möglichkeiten dieses Programms beschränkt werden. Ein interaktives Programmieren von den Datenendgeräten der Arbeitsvorbereitung kann dann unterbunden werden.

### **c) Datensicherung bei Dateien**

#### **- Dateien zur Datensicherung**

Nach der Dienstanweisung eines kontrollierten Krankenkassenverbandes sind Systemnachrichten täglich auszudrucken. Der Inhalt wird monatlich fortgeschrieben und verfilmt. Nach der Verfilmung sind die Ausdrücke zu vernichten. Die Microfiche sind sechs Jahre aufzubewahren.

Aufgezeichnete Systemnachrichten können unter anderem genutzt werden, um eventuelle Unregelmäßigkeiten nachträglich aufzuklären. Falls für eine derartige Aufklärung die Systemnachrichten eines längeren Zeitraums ausgewertet werden müssen, ist es sehr vorteilhaft, wenn die Systemnachrichten maschinenlesbar aufgezeichnet sind. Systemnachrichten werden daher im allgemeinen auf Magnetband aufgezeichnet und archiviert. Ich habe empfohlen, die Systemnachrichten maschinenlesbar aufzuzeichnen und zu archivieren.

Der Krankenkassenverband, der die Daten seiner Mitgliedskassen in deren Auftrag verarbeitet, berichtete während des Kontrollbesuchs, daß bei den Mitgliedskassen die Eingabekontrolle in Form von schriftlichen Protokollierungen vorgenommen werde. Protokolliert werde chronologisch. Die Ablage erfolge in der Reihenfolge der Aufzeichnungen.

Nach § 6 Abs. 1 Satz 1 BDSG/DSG NW in Verbindung mit Nr. 7 der Anlage zu dieser Vorschrift haben die Mitgliedskassen und der Krankenkassenverband die technischen und organisatorischen Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle). Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 6 Abs. 1 Satz 2 BDSG/DSG NW).

Die Eingabekontrolle soll eine nachträgliche Überprüfung von Inhalt, Zeitpunkt und Verursacher einer Dateiänderung ermöglichen. Diese Überprüfung sollte über längere Zeiträume rückwirkend möglich sein. Jedenfalls muß eine Überprüfung solange möglich sein, wie die eingegebenen Daten unverändert in der Datei gespeichert sind. Chronologische Aufzeichnungen, die zeitlich geordnet abgelegt werden, sind für eine Eingabekontrolle nur mit erheblichem Arbeitsaufwand verwendbar.

Für Zwecke der Eingabekontrolle ist daher eine Protokollierung auf maschinenlesbaren Datenträgern üblich. Durch maschinelle Umsortierung kann daraus eine Historie jedes gespeicherten Datensatzes erzeugt werden. Diese Historien der Datensätze werden ständig fortgeschrieben und dienen der Eingabekontrolle. Der Krankenkassenverband, der seine Programme von dem Bundesverband erhält, sollte klären, ob es für die bei ihm eingesetzten Programme entsprechende Ergänzungen gibt, die eine Protokollierung auf maschinenlesbaren Datenträgern für Zwecke der Eingabekontrolle ermöglichen. Ich habe um Unterrichtung gebeten, ob eine solche Programmergänzung möglich ist und erfolgen wird.

#### **- Löschen von Daten**

Während des Kontrollbesuchs bei einer kommunalen Datenzentrale wurde die Frage erörtert, unter welchen Umständen Daten als gelöscht angesehen werden können.

Daten sind bei einer speichernden Stelle erst dann im Sinne des § 2 Abs. 2 Nr. 4 DSG NW gelöscht, wenn diese Stelle an keinem Ort mehr über die Daten oder über Aufzeichnungen verfügt, die es gestatten, die Daten zu rekonstruieren. Bei der Datenzentrale sind Daten nicht nur in den jeweils aktuellen Dateien, sondern zusätzlich auf Sicherungsbändern gespeichert. Für das Löschen der Daten ist es daher nicht ausreichend, wenn diese nur in der aktuellen Datei gelöscht werden. Daten, die in einer aktuellen Datei gelöscht wurden, können vielmehr erst dann als gelöscht bezeichnet werden, wenn sichergestellt ist, daß weder auf einem Sicherungsband noch in einem sonstigen Datenbestand die zu löschende Angabe gespeichert ist.

## **5. Datensicherung bei Einsatz kleinerer Datenverarbeitungsanlagen**

### **a) Abgrenzung des Themas**

Kleinere Datenverarbeitungsanlagen können heute zu niedrigen Preisen angeschafft werden. Ein weiteres Sinken der Preise ist zu erwarten. Dennoch ist die Leistungsfähigkeit der kleineren Anlagen sehr groß und gestattet es, umfangreiche Datenverarbeitungsaufgaben abzuwickeln. Als Folge der Marktsituation wurden in den vergangenen Jahren zahlreiche kleinere Datenverarbeitungsanlagen bei öffentlichen Stellen aufgestellt. Mit einer starken Zunahme kann gerechnet werden.

Bezüglich der Anforderungen und Möglichkeiten zur Datensicherung bei kleineren Datenverarbeitungsanlagen besteht große Unsicherheit. Manche Anforderungen, die bei großen Rechenzentren selbstverständlich sind, können bei Einsatz kleinerer Datenverarbeitungsanlagen nicht verwirklicht werden. Angemessene Alternativen wurden bisher nicht angeboten.

Um zu einem eigenen Urteil und nach Möglichkeit zu Empfehlungen für die Lösung der bestehenden Schwierigkeiten zu kommen, habe ich öffentliche Stellen mit kleineren Datenverarbeitungsanlagen seit einigen Jahren bevorzugt in meine Kontrolltätigkeit einbezogen. In zahlreichen Besprechungen mit den öffentlichen Stellen und teilweise auch mit den jeweiligen Herstellerfirmen der Datenverarbeitungsanlagen wurden die Möglichkeiten und die heute bestehenden Grenzen der Datensicherung erörtert. Über Beobachtungen und Empfehlungen habe ich in meinem vierten und sechsten Tätigkeitsbericht (D.5.) informiert.

Zwei Arten des Einsatzes kleinerer Datenverarbeitungsanlagen lassen sich unterscheiden. Bei der einen Art soll die Verarbeitung der Daten mit einer verbindlichen Verarbeitungslogik erfolgen. Verarbeitung mit verbindlicher Verarbeitungslogik soll bedeuten, daß es eine Verarbeitungslogik gibt, die verbindlich durch eine Person oder Stelle vorgeschrieben oder gegenüber einer Person oder Stelle zugesagt ist. Bei der anderen Art des Einsatzes ist die Verarbeitungslogik nicht verbindlich.

Verbindlich ist die Verarbeitungslogik im allgemeinen, wenn eine kleinere Datenverarbeitungsanlage durch eine öffentliche Stelle für Verwaltungsaufgaben eingesetzt wird. Meist ergibt sich die Verarbeitungslogik aus den geltenden Rechtsvorschriften. Beispiele dafür sind die Datenverarbeitung bei einem Versicherungsträger oder bei einem Einwohnermeldeamt. Auch außerhalb des öffentlichen Bereichs werden kleinere Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik eingesetzt. So setzt der Einsatz einer kleineren Datenverarbeitungsanlage im Rahmen des Rechnungswesens im allgemeinen eine verbindliche Verarbeitungslogik voraus.

Meist ist der Einsatz kleinerer Datenverarbeitungsanlagen öffentlicher Stellen, bei denen die Verarbeitungslogik verbindlich vorgeschrieben ist, durch folgende Eigenarten gekennzeichnet:

- Es gibt einen Mitarbeiter, der als Maschinenbediener für den Betrieb der Datenverarbeitungsanlage zuständig ist. Dieser Mitarbeiter übt eine Art Rechenzentrumsfunktion aus.
- Die zum Einsatz kommenden Programme werden dem Maschinenbediener vorgegeben. Bei einigen Einsatzfällen hat der Maschinenbediener die Aufgabe, diese Programme in bestimmten Situationen selbständig zu ändern. Es gibt auch Einsatzfälle, in denen der Maschinenbediener die Aufgabe hat, einzelne Programme selbst zu entwickeln.
- Eine Möglichkeit der fachlichen Kontrolle des Maschinenbedieners durch seinen Vorgesetzten besteht nicht, weil die dazu notwendigen Fachkenntnisse der automatisierten Datenverarbeitung bei dem Vorgesetzten nicht vorhanden sind und auch nicht erwartet werden können.
- Eine gegenseitige Kontrolle von Mitarbeitern kann nicht durch Funktionstrennung verwirklicht werden, weil für die Bedienung der Datenverarbeitungsanlage nur ein Mitarbeiter tätig ist.

Datenverarbeitung auf kleineren Anlagen ohne verbindliche Verarbeitungslogik findet man vor allem bei wissenschaftlichen und technischen Anwendungen. Derartige Einsatzfälle sind im allgemeinen durch folgende Eigenarten gekennzeichnet:

- Vom Anwender wird schöpferische Arbeit erwartet, in die er die Datenverarbeitung einbezieht.
- Die Verantwortung des Anwenders umfaßt auch den logischen Weg zu dem Ergebnis seiner Arbeit.
- Anwender und Bediener der Datenverarbeitungsanlage sind dieselbe Person.
- Der Anwender entwickelt seine Programme teilweise selbst.

Im Zusammenhang mit dieser Einsatzart kleinerer Datenverarbeitungsanlagen entstanden die Begriffe persönlicher Computer (PC), Arbeitsplatzcomputer und individuelle Datenverarbeitung (IDV). Der Begriff IDV ist vor allem in der Industrie verbreitet. Gemeint ist damit eine Einsatzform, bei der der einzelne Bearbeiter über eine kleinere Datenverarbeitungsanlage verfügt, diese Anlage selbst programmiert und auch selbst bedient. In Industrieunternehmen hat sich herausgestellt, daß die IDV einer gewissen Koordination und Unterstützung bedarf. Dazu wird eine Stelle mit der Bezeichnung Information Center gebildet, die dem ADV-Bereich angegliedert wird und organisatorisch gleichrangig neben Anwendungsentwicklung und Rechenzentrum steht.

Aufgaben des Information Center sind etwa

- Beratung zu Fragen der Hardware und Software,
- Kontakt zu Lieferanten von Hardware und Software,
- Aus- und Weiterbildung,
- Koordination von Anwendungen, soweit erforderlich.

Auch bei dem Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik ist eine Aufgabe ähnlich derjenigen des Information Center wahrzunehmen. Die organisatorische Lösung wird aber anders geartet sein (unten D.5.f).

Öffentliche Stellen setzen kleinere Datenverarbeitungsanlagen für Verwaltungsaufgaben im allgemeinen mit verbindlicher Verarbeitungslogik ein. Über einen organisatorischen Ausnahmefall bei einer Schule wird unten (D.5.c) berichtet. Die folgenden Ausführungen gelten daher fast ausnahmslos, wenn öffentliche Stellen für Verwaltungsaufgaben personenbezogene Daten auf kleineren Datenverarbeitungsanlagen verarbeiten.

Falls die Verarbeitungslogik verbindlich ist, gibt es eine Person oder Stelle, die darauf angewiesen ist, daß die Daten mit dieser Verarbeitungslogik verarbeitet werden. In diesem Fall ist es Aufgabe des Vorgesetzten des Maschinenbedieners sicherzustellen, daß Daten ausschließlich mit dieser Verarbeitungslogik verarbeitet werden. Der Vorgesetzte muß dazu über geeignete organisatorische oder technische Hilfsmittel verfügen.

Das Vorhandensein derartiger Hilfsmittel ist Voraussetzung einer ausreichenden Datensicherung. Im folgenden wird dargestellt, inwieweit die Datensicherung heute Hilfsmittel in dem erforderlichen Umfang bereitstellt. Dabei werden Lücken der Datensicherung erkennbar, und es werden Vorschläge gemacht, wie diese Lücken geschlossen werden können.

#### **b) Besonderheiten der Datensicherung beim Einsatz kleinerer Datenverarbeitungsanlagen**

Organisatorisch und räumlich entspricht die Einbettung kleinerer Datenverarbeitungsanlagen, die mit verbindlicher Verarbeitungslogik arbeiten, häufig folgendem Modell:

- Organisatorisch gehört die Datenverarbeitungsanlage zum Anwenderbereich.
- Es gibt nur einen Maschinenbediener.
- Der Vorgesetzte des Maschinenbedieners verfügt nicht über Fachwissen der automatisierten Datenverarbeitung.
- An die Datenverarbeitungsanlage ist eine Anzahl von Datenendgeräten angeschlossen, zu denen die Anwender Zugriff haben.
- Die eingesetzten Programme werden von einer anderen Stelle bezogen.
- Die Datenverarbeitungsanlage ist in den Arbeitsräumen der Anwender untergebracht oder von diesen nur unzureichend abgetrennt.

Durch diese organisatorischen und räumlichen Bedingungen wird die Datensicherung sehr erschwert. Zur Datensicherung in größeren Rechenzentren wurden in den vergangenen Jahrzehnten zahlreiche Maßnahmen entwickelt, die heute für ordnungsgemäß arbeitende Rechenzentren zu den Selbstverständlichkeiten gehören. Eine Anzahl dieser Maßnahmen ist bei Einsatz kleinerer Datenverarbeitungsanlagen nicht praktikabel. Diese Situation soll an einigen Beispielen erläutert werden:

- Bei größeren Rechenzentren ist eine Funktionstrennung zu verwirklichen. Die Aufgaben Anwendungsprogrammierung, Systemprogrammierung, Arbeitsvorbereitung, Maschinenbedienung und Arbeitskontrolle sind unterschiedlichen Mitarbeitern zuzuordnen. Wenn bei Einsatz einer kleineren Datenverarbeitungsanlage nur ein Mitarbeiter oder nur wenige Mitarbeiter mit diesen Aufgaben betraut sind, scheiden die Möglichkeiten für derartige Funktionstrennungen weitgehend aus. Die Aufgabe der Anwendungsprogrammierung wird allerdings getrennt wahrgenommen, soweit Fremdprogramme eingesetzt werden.
- In größeren Rechenzentren werden neue Produktionsprogramme ausschließlich auf Veranlassung der Arbeitsvorbereitung durch die Maschinenbediener übernommen. Bei Einsatz kleinerer Datenverarbeitungsanlagen gibt es keine Arbeitsvorbereitung als getrennte Organisationseinheit.
- Bei größeren Rechenzentren darf nicht ein Maschinenbediener allein die Datenverarbeitungsanlage bedienen. Es gilt vielmehr das Vier-Augen-Prinzip. Diese Regelung setzt voraus, daß die Stelle über wenigstens zwei Maschinenbediener verfügt.
- In größeren Rechenzentren wird die Arbeit der Maschinenbediener durch eine Arbeitskontrolle nachträglich geprüft. Bei Einsatz kleinerer Datenverarbeitungsanlagen gibt es keine zur Kontrolle der Abwicklung der automatisierten Datenverarbeitung befähigte Arbeitskontrolle als getrennte Organisationseinheit.

Die beispielhaft aufgeführten Maßnahmen sollen in größeren Rechenzentren sicherstellen, daß die Vorschriften der Dienstanweisung eingehalten werden. Wenn sie bei Einsatz kleinerer Datenverarbeitungsanlagen nicht verwirklicht werden, ist insoweit die Möglichkeit zur Kontrolle der Einhaltung der Dienstanweisung eingeschränkt. Diese Aussage läßt sich verallgemeinern. Alle bei größeren Rechenzentren für erforderlich gehaltenen Maßnahmen, die bei Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik nicht oder nur mit großen Schwierigkeiten verwirklicht werden können, dienen in irgendeiner Weise dazu sicherzustellen, daß die zur Gewährleistung der Datensicherheit erforderliche Dienstanweisung eingehalten wird. Die beim Übergang von größeren auf kleinere Datenverarbeitungsanlagen auftretenden besonderen Schwierigkeiten lassen sich daher zu einer einfachen Aussage zusammenfassen: Es ist im allgemeinen möglich, eine Dienstanweisung für den Betrieb einer

kleineren Datenverarbeitungsanlage aufzustellen, bei deren Einhaltung eine ordnungsgemäße Datenverarbeitung sichergestellt wäre. Besonderen Schwierigkeiten begegnet aber die Kontrolle der Einhaltung der Dienstanweisung. Die Datensicherheit ist beim Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik vor allem dadurch eingeschränkt, daß die Einhaltung einer Dienstanweisung nur beschränkt sichergestellt werden kann.

Die Einhaltung der Dienstanweisung läßt sich insbesondere bei demjenigen, der über die Anlage verfügt, nicht sicherstellen. Gelegentlich kommt diese Tatsache auch bei Kontrollbesuchen zum Ausdruck. Wenn meine Mitarbeiter eine Empfehlung aussprechen, die eine zusätzliche Möglichkeit der Kontrolle schaffen soll, kommt in Einzelfällen vom Maschinenbediener die Frage, was denn diese Empfehlung solle. Meinen Mitarbeitern als Fachleuten sei doch bekannt, daß er als Bediener der Datenverarbeitungsanlage an alle Daten kommen und alle von ihm gewünschten Änderungen durchführen könne. Daran ändere auch die empfohlene neue Maßnahme nichts.

Ein derartiger Hinweis des Maschinenbedieners ist meist zutreffend. In einer Fachdiskussion wurde kürzlich eine entsprechende These aufgestellt: „Die Überwachung der Befugten stellt das schwierigste und bis heute nicht gelöste PC-Problem dar.“ (Datenschutz-Berater 4/1985 S. 16). Bezogen auf die Anlage zu § 6 Abs. 1 Satz 1 DSGVO bedeutet diese Situation, daß sich die Speicherkontrolle, die Zugriffskontrolle und die Eingabekontrolle bei Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik zur Zeit nur beschränkt sicherstellen lassen.

Die heute allgemein anerkannten Vorstellungen, welche Maßnahmen zur Datensicherung bei größeren Rechenzentren als notwendig anzusehen sind, wurden in den letzten Jahrzehnten entwickelt. In der Anfangszeit der automatisierten Datenverarbeitung waren die heute als selbstverständlich geltenden Vorschriften weitgehend unbekannt. Heute befinden wir uns in einer vergleichbaren Situation bezüglich des Einsatzes kleinerer Datenverarbeitungsanlagen. Allerdings werden die bei Einsatz der kleineren Datenverarbeitungsanlagen bestehenden Sicherheitsmängel durch die Möglichkeit des Vergleichs mit den weit entwickelten Vorstellungen zur Datensicherung bei größeren Rechenzentren schneller offenbar.

Es ist davon auszugehen, daß die mit dem Einsatz kleinerer Datenverarbeitungsanlagen verbundenen Schwierigkeiten der Datensicherung bei verbindlicher Verarbeitungslogik besonders hervortreten. Die für andere Einsatzformen angemessenen Maßnahmen können daher im Einzelfall aus den Ergebnissen der folgenden Untersuchung abgeleitet werden. Das gilt auch für Fragen der Datensicherung bei der individuellen Datenverarbeitung, das heißt bei Einsatz kleinerer Datenverarbeitungsanlagen, bei denen die Verarbeitungslogik nicht verbindlich ist.

### **c) Sicherheit der Programme**

#### **– Bereitstellen einwandfreier Programme**

Eine Stelle, die ihre Programme nicht selbst entwickelt, ist darauf angewiesen, einwandfreie Programme von einer anderen Stelle zu erhalten. Es sind heute unterschiedliche Wege üblich, derartige Fremdprogramme zu beschaffen. Häufig werden die Programme vom Lieferanten der Hardware oder von einer Softwarefirma geliefert. Auch Datenzentralen oder Anwendergemeinschaften treten als Lieferanten von Anwendungsprogrammen auf.

Fremdprogramme werden im allgemeinen eingesetzt, um die Kosten der eigenen Programmentwicklung zu sparen oder weil das für die Programmierung notwendige Fachwissen auf dem Gebiet der automatisierten Datenver-

arbeitung in der eigenen Stelle nicht vorhanden ist. Gegen den Einsatz von Fremdprogrammen bestehen aus der Sicht des Datenschutzes keine grundsätzlichen Bedenken. Die Funktionstrennung zwischen Programmierung und Anwendung ist dabei sogar besonders weitgehend verwirklicht. Bei Einsatz kleinerer Datenverarbeitungsanlagen wird die Datensicherung durch den Einsatz von Fremdprogrammen daher fast immer verbessert.

Programme müssen im Rahmen der bestehenden Möglichkeiten einwandfrei sein. Zur Prüfung, ob ein Programm einwandfrei ist, sind heute zwei Stufen des Programmtests selbstverständlich. Zunächst testen die entwickelnden Programmierer das Programm, beseitigen dabei erkannte Fehler und erklären anschließend das Programm als fehlerfrei. Anschließend führt der Anwender einen unabhängigen Test durch. Erweist sich das Programm auch bei diesem Anwendertest als fehlerfrei, so wird es anschließend durch den Anwender für Produktionsläufe freigegeben.

Entsprechend ist bei der Freigabe von Fremdprogrammen vorzugehen. An die Stelle der Erklärung des Programmierers über die Fehlerfreiheit des Programms hat eine Erklärung des Lieferanten des Programms zu treten. Zusätzlich ist der Programmtest durch den Anwender erforderlich. Der als Voraussetzung der Programmfreigabe durch den Anwender notwendige Programmtest erfordert allerdings einen beträchtlichen Arbeitsaufwand. Falls sich mehrere Auftraggeber desselben Programms bedienen, empfiehlt sich daher im allgemeinen eine Vereinbarung, nach der ein Auftraggeber oder einzelne Auftraggeber den Programmtest für alle übrigen durchführen und eventuell auch ermächtigt sind, das Programm im Namen der übrigen Auftraggeber freizugeben. Hier sind sehr unterschiedliche Organisationsformen denkbar, die sich jeweils an der speziellen Situation zu orientieren haben. In jedem einzelnen Fall muß allerdings die Verantwortung jedes einzelnen Auftraggebers für die Freigabe des Programms zum Ausdruck kommen. Meine bisherigen Tätigkeitsberichte enthalten zahlreiche Empfehlungen zu Programmtest und Programmfreigabe.

Eine kontrollierte Stadt führt die automatisierte Datenverarbeitung mit eigenen kleineren Datenverarbeitungsanlagen durch. Die dabei eingesetzten Programme erhält die Stadt von der Lieferfirma ihrer Datenverarbeitungsanlagen. Die Programme werden ohne jede Änderung übernommen.

Anwendungsprogramme unterliegen im allgemeinen einer laufenden Änderung. Auch bei der kontrollierten Stadt zeigte die Erfahrung, daß die eingesetzten Programme in gewissen Zeitabständen gewartet und durch neue Programmversionen ersetzt werden mußten. Ursachen für derartige Änderungen liegen sowohl in Änderungen der fachlichen Vorgaben, wie sie etwa aus Gesetzesänderungen folgen können, als auch in seit dem ersten Einsatz erkannten Programmfehlern.

Die Programmwartung und der darauf folgende Ersatz des bisherigen Programms durch eine neue Programmversion sind übliche Maßnahmen der automatisierten Datenverarbeitung. Bei eigenen Programmentwicklungen großer datenverarbeitender Stellen ist es selbstverständlich, daß der Programmierer nach Abschluß seiner Arbeiten das geänderte Programm testet. Das Programm wird dann dem Anwender mit einer Erklärung des Programmierers übergeben, daß sich das Programm bei dem Programmierertest als fehlerfrei erwiesen habe. Die als Voraussetzung der Programmfreigabe erforderlichen Anwendertests werden erst anschließend durchgeführt. Eine entsprechende Bestätigung der Fehlerfreiheit der Programme durch die Lieferfirma ist erforderlich, bevor die Stadt die geänderten Programme übernehmen und durch eigene Tests die Freigabe vorbereiten kann. Es ist daher wichtig, nicht nur bei der ersten Programmversion, sondern auch bei allen

folgenden Versionen von der Lieferfirma eine Bestätigung der Fehlerfreiheit der Programme zu erhalten.

Während des Kontrollbesuchs konnte nicht geklärt werden, ob Bestätigungen der Fehlerfreiheit der Programme durch die Lieferfirma vorliegen. Derartige Bestätigungen sollten ausnahmslos vorliegen, bevor mit eigenen Programmtests begonnen und damit die abschließende Programmfreigabe vorbereitet wird. Ich habe daher der Stadt empfohlen festzulegen, daß für die erste und für jede neue Programmversion eine schriftliche Bestätigung der Fehlerfreiheit durch die Lieferfirma vorzuliegen hat.

Bei dem Kontrollbesuch bei einem Gymnasium wurde unter anderem die Datensicherung der eingesetzten kleineren Datenverarbeitungsanlage geprüft. Auf der Datenverarbeitungsanlage werden personenbezogene Daten verarbeitet. Dennoch ergaben sehr eingehende Erörterungen, daß die eingesetzten Programme keiner unabhängigen Freigabe bedürfen. Bei dem Gymnasium ist die bei Verwaltungsaufgaben ungewöhnliche Organisationsform einer Datenverarbeitung ohne verbindliche Verarbeitungslogik (oben D.5.a) verwirklicht. Gegen die gewählte Verantwortungszuordnung bestehen dennoch aus der Sicht des Datenschutzes keine durchgreifenden Bedenken.

Nach Nr. 5.4 Satz 3 Buchst. d der Verwaltungsvorschriften zur Verordnung über den Bildungsgang und die Abiturprüfung in der Oberstufe des Gymnasiums (VVzAPO-GOST) gehört die Vorbereitung der Unterlagen für die Abiturprüfung zu den Aufgaben der Beratungslehrer. Zur Vorbereitung von Entscheidungen des Zentralen Abiturausschusses werten die Beratungslehrer des kontrollierten Gymnasiums unter anderem die Leistungen der ihnen zugeordneten Schüler aus.

Die Kontrolle der Arbeit der Beratungslehrer wurde dem Oberstufenkoordinator übertragen. Diese Kontrollaufgabe nimmt der Oberstufenkoordinator eigenverantwortlich wahr. Inhalt der ihm erteilten Weisung ist nur die Gesamtaufgabe; Einzelheiten der Durchführung der Kontrollaufgabe sind nicht vorgeschrieben.

Der Oberstufenkoordinator setzt die Datenverarbeitungsanlage des Gymnasiums für folgende Auswertungen im Rahmen seiner Kontrollaufgabe ein:

- Notenauswertung für die Zulassung zum Abitur,
- Feststellen der Prüfungsteilnehmer im ersten bis dritten Abiturfach.

Die dafür erforderlichen Programme schreibt und testet der Oberstufenkoordinator selbst. Die durch die Programme auszuwertenden Daten werden von ihm erfaßt. Er bedient die Datenverarbeitungsanlage selbst. Die Ergebnisse der automatisierten Verarbeitung werden von ihm anschließend für seine Kontrollaufgabe verwendet.

Die Datenverarbeitung durch den Oberstufenkoordinator erfolgt im Rahmen einer dienstlichen Aufgabe. Für die hierbei gespeicherten personenbezogenen Daten ist die Stadt, die Trägerin des Gymnasiums ist, speichernde Stelle. Dateien, die der Oberstufenkoordinator im Rahmen seiner Arbeit führt, sind Dateien dieser Stadt.

Vorschriften oder Weisungen gibt es allerdings weder bezüglich der von dem Oberstufenkoordinator entwickelten Programme noch bezüglich des Erfassens der Daten, deren Speicherung auf maschinenlesbaren Datenträgern sowie deren automatisierter Verarbeitung. Eine verbindliche Verarbeitungslogik ist dem Oberstufenkoordinator daher nicht vorgeschrieben und wird von ihm auch nicht zugesagt. Die Programme, die Speicherung der Daten, deren automatisierte Verarbeitung und das Auswerten der Ergebnisse der automatisierten Verarbeitung liegen in diesem Fall in der Verantwortung des Oberstu-

fenkoordinators. Gegen den Verzicht auf Regelung von Einzelheiten der Aufgabenerfüllung bestehen keine durchgreifenden Bedenken. Die Art der Aufgabenübertragung entspricht vielmehr der dem Oberstufenkoordinator übertragenen Verantwortung. Auch besteht keine Abhängigkeit von der Arbeit der automatisierten Datenverarbeitung. Während des Kontrollbesuchs wurde berichtet, eine ernste Beeinträchtigung der Arbeit des Gymnasiums durch einen eventuellen Ausfall der Möglichkeit zur automatisierten Verarbeitung der Daten sei nicht möglich, da jederzeit zur bisherigen manuellen Bearbeitung übergegangen werden könne.

Da der Oberstufenkoordinator seine Programme selbst entwickelt hat und die Ergebnisse ihres Einsatzes eigenverantwortlich verwertet, scheiden ein unabhängiger Test und eine unabhängige Freigabe dieser Programme durch einen geeigneten anderen Mitarbeiter aus. Anders wäre die Situation zu beurteilen, wenn die Ergebnisse der automatisierten Verarbeitung von den Beratungslehrern ganz oder teilweise übernommen würden, indem diese insoweit auf eigene Berechnungen verzichteten. Die Beratungslehrer wären in diesem Fall Anwender der automatisierten Datenverarbeitung. Die eingesetzten Programme müßten durch einen dieser Anwender oder einen anderen geeigneten Mitarbeiter getestet und durch die speichernde Stelle freigegeben werden; der Träger des Gymnasiums könnte dieses zu derartigen Freigaben ermächtigen.

Das Gymnasium erklärte ausdrücklich, die Beratungslehrer würden in jedem Fall sämtliche erforderlichen Berechnungen selbst durchführen. Zwar erhielten die Beratungslehrer Listen mit den Ergebnissen der automatisierten Verarbeitung zur Kenntnis. Diese Listen sollen es den Beratungslehrern aber nur ermöglichen, von ihnen vorher errechnete Werte zu überprüfen. Die Beratungslehrer sind nicht berechtigt, die Angaben der Listen ohne vorherige eigene Berechnungen zu verwenden und als Grundlage für die von ihnen zu erstellende Auswertung zu nehmen.

Auf den Anwendertest und auf die Freigabe der Programme kann nur verzichtet werden, wenn sichergestellt ist, daß jeder Beratungslehrer die zur Auswertung der Leistungen der Schüler erforderlichen Berechnungen zunächst selbst durchführt und die Listen der automatisierten Datenverarbeitung nur zur Kontrolle seiner eigenen Berechnungen verwendet. Das könnte dadurch sichergestellt werden, daß der Beratungslehrer die Ergebnisse der automatisierten Datenverarbeitung erst erhält, wenn er seine Berechnungen abgeschlossen hat. Besser wäre es, auf die Weitergabe dieser Ergebnisse an den Beratungslehrer zu verzichten. Der Beratungslehrer sollte in diesem Fall die Ergebnisse seiner Berechnungen dem Oberstufenkoordinator zuleiten, der den Vergleich mit den Ergebnissen der automatisierten Datenverarbeitung durchführen würde.

Unbedenklich wäre auch eine andere Zuordnung der Verantwortungen. Es könnte festgelegt werden, daß die Programme mit ihren Ergebnissen verbindlich sind und daß der Beratungslehrer die Ergebnisse der automatisierten Datenverarbeitung als Grundlage seines Berichts für den Zentralen Abiturausschuß verwendet. In diesem Fall wird die Verarbeitungslogik verbindlich, und die Programme müssen vor ihrem ersten Einsatz und nach jeder Änderung, die den fachlichen Programminhalt betrifft, durch den Anwender oder im Namen des Anwenders getestet und durch die speichernde Stelle freigegeben werden.

Ich habe empfohlen, eine Regelung einzuführen, durch die sichergestellt wird, daß keine Ergebnisse einer Verarbeitung mit einem nicht freigegebenen Programm von den Beratungslehrern als verbindlich übernommen werden.

#### - Einsatz unveränderter Programme

Selbstverständlich ist es nicht ausreichend, nach der ersten Entwicklung und nach jeder Programmwartung einwandfreie Programme für die Verarbeitung bereitzustellen. Es muß darüber hinaus auch sichergestellt werden, daß diese Programme unverändert eingesetzt werden. Dazu bestehen grundsätzlich die beiden Möglichkeiten, die Änderung unmöglich zu machen oder die Änderung zu untersagen. Wenn die Änderung möglich ist, aber untersagt wird, muß es eine Kontrollmöglichkeit geben, die erkennen läßt, ob ein Programm gegenüber der bereitgestellten Fassung verändert wurde.

Einen praktikablen Weg, die Änderung von Programmen unmöglich zu machen, gibt es nicht. Allerdings ist die Änderung erschwert, wenn die Quellprogramme und eine der Wartung dienende Dokumentation nicht verfügbar sind. Um unzulässige Programmänderungen zu erschweren, sollte die datenverarbeitende Stelle bei Einsatz von Fremdprogrammen daher auf eine Auslieferung der Quellprogramme und derjenigen Teile der Dokumentation verzichten, die nur der Programmwartung dienen. Es gibt allerdings Situationen, in denen ein Rückgriff auf die Quellprogramme und die vollständige Dokumentation möglich sein muß. In meinem sechsten Tätigkeitsbericht (D.5.a) habe ich einen dafür geeigneten Weg genannt.

In jedem Fall sollte die Änderung freigegebener und bereitgestellter Programme untersagt werden. Ein entsprechendes Verbot sollte Bestandteil der Dienstanweisung sein. Darauf habe ich eine Stadt bei einem Kontrollbesuch hingewiesen.

Die auf ihren eigenen kleineren Datenverarbeitungsanlagen eingesetzten Anwendungsprogramme erhält die Stadt von der Lieferfirma ihrer Datenverarbeitungsanlagen. Die Programme werden ohne jede Änderung eingesetzt. Der unveränderte Einsatz von Programmen, deren Entwicklung bei einer anderen Stelle lag, ist unter dem Gesichtspunkt der Datensicherheit zu begrüßen. Die notwendige Funktionstrennung zwischen Programmierung und Durchführung ist hier besonders weitgehend verwirklicht. Eine Verpflichtung, die übernommenen Anwendungsprogramme unverändert einzusetzen, ist in einem von der Stadt vorgelegten Entwurf einer Dienstanweisung über die Organisation der ADV und des Datenschutzes allerdings nicht enthalten. Ich habe daher empfohlen, den unveränderten Einsatz der Programme ausdrücklich vorzuschreiben und die Dienstanweisung insoweit zu ergänzen.

Die Regelung in der Dienstanweisung kann nur durchgesetzt werden, wenn es möglich ist zu kontrollieren, ob ein Programm in der freigegebenen Fassung vorliegt oder inzwischen unzulässig verändert wurde. Das Systemprotokoll bietet dazu nach aller Erfahrung bei kleineren Datenverarbeitungsanlagen eine nur wenig geeignete Grundlage. Es ist nicht hinreichend aussagekräftig, der erfahrene Maschinenbediener kennt Möglichkeiten der Umgehung, und eine Auswertung aussagekräftiger Protokolle würde an einem Fehlen des dazu erforderlichen Fachwissens bei den für die Kontrolle des Maschinenbedieners zuständigen Mitarbeitern scheitern.

Systemprotokolle enthalten Aussagen darüber, welche Handlungen von wem an der Datenverarbeitungsanlage vorgenommen wurden. Mit ihrer Hilfe würde im allgemeinen nur indirekt kontrolliert, ob ein Programm geändert wurde. Einen wesentlichen Fortschritt in den Möglichkeiten der Kontrolle würde es bedeuten, wenn ein Programm direkt auf Übereinstimmung mit der ursprünglichen Fassung geprüft werden könnte.

Grundsätzlich ist es möglich, daß eine Stelle mit der Aufgabe der Innenrevision oder des Rechnungsprüfungsamtes über Kopien freigegebener Programme verfügt und diese Kopien von Zeit zu Zeit maschinell mit den für

Produktionsläufe gespeicherten Fassungen der Programme vergleicht. Ein solches Vorgehen ist allerdings wegen des hohen Aufwandes wenig praktikabel. Von dieser Möglichkeit kann daher nur in Sonderfällen Gebrauch gemacht werden.

Um eine für die Praxis geeignete Kontrollmöglichkeit zu schaffen, habe ich in meinem fünften Tätigkeitsbericht (D.4.d) ein Verfahren vorgeschlagen, bei dem jedem einzelnen Programm eine Prüfinformation zugeordnet wird. Der Informationsgehalt der Prüfinformation und die Logik ihrer Zuordnung sollen es praktisch unmöglich machen, ein Programm so zu ändern, daß auch dem geänderten Programm dieselbe Prüfinformation entspricht. Man könnte bei einer Maßnahme dieser Art von einem Versiegeln der Programme sprechen.

Nach meinem damaligen Vorschlag sollte für die Zuordnung der Prüfinformation die Verschlüsselungsmethode des DES (Data Encryption Standard) eingesetzt werden. Aus einer Veröffentlichung ist zu entnehmen, daß ein Hersteller die in seinen Geldausgabeautomaten eingesetzten Programme in entsprechender Weise versiegelt. Um die Datensicherung darüber hinaus zu verbessern, könnte man an Stelle des DES ein Verfahren der Einwegverschlüsselung einsetzen. Dadurch würde es zusätzlich erschwert, auf systematische Weise zu einer Programmänderung eine zweite zusätzliche Änderung zu finden, die so geartet ist, daß nach Einbau beider Änderungen die Prüfinformation des Programms unverändert ist.

Auf dem Markt sind Verfahren zum Versiegeln von Programmen allerdings nicht erhältlich. Auch sonstige Verfahren, die es dem Anwender einer kleineren Datenverarbeitungsanlage ohne Fachkenntnisse der automatisierten Datenverarbeitung ermöglichen könnten zu prüfen, ob ein Programm unzulässig verändert wurde, werden nicht angeboten. Der für den Einsatz einer kleineren Datenverarbeitungsanlage zuständige Vorgesetzte hat daher heute keine praktikable Möglichkeit sicherzustellen, daß die ursprünglich bereitgestellten Programme unverändert zum Einsatz kommen.

In jedem großen Rechenzentrum ist es eine Selbstverständlichkeit, sich durch eine Summe von Maßnahmen gegen unzulässige Programmänderungen abzusichern und damit das Risiko für denjenigen, der eine Manipulation beabsichtigt, wesentlich zu erhöhen. Gegenüber dem Bediener einer kleineren Datenverarbeitungsanlage bleiben dagegen im wesentlichen die Möglichkeiten, die Quellprogramme und die der Wartung dienende Dokumentation nicht verfügbar zu halten und in der Dienstanweisung jegliche Programmänderung zu untersagen.

Diese Unsicherheit bei Einsatz kleinerer Datenverarbeitungsanlagen sollte nur für eine Übergangszeit hingenommen werden.

Die Hersteller kleinerer Datenverarbeitungsanlagen sollten die bestehende Unsicherheit unverzüglich beseitigen. Sie könnten dazu Verfahren zum Versiegeln von Programmen entwickeln und anbieten. Damit wäre die Möglichkeit verbunden, daß eine Innenrevision, ein Rechnungsprüfungsamt, ein Datenschutzbeauftragter oder eine sonstige Stelle mit der Aufgabe der Kontrolle (unten D.5.f) überprüfen könnte, ob ein zum Einsatz kommendes Programm gegenüber der ursprünglichen Fassung geändert ist. Günstig wäre es, wenn darüber hinaus sichergestellt wäre, daß Programme bei der ersten Benutzung an einem Tag oder aus einem sonstigen noch festzulegenden Anlaß automatisch auf Übereinstimmung mit der freigegebenen Fassung überprüft würden. Eine Empfehlung zur Häufigkeit derartiger Überprüfungen ist erst möglich, wenn der Zeitaufwand für die Ermittlung der Prüfinformationen der Programme bekannt ist.

In diesem Zusammenhang ist eine weitere These aus der oben (D.5.b) erwähnten Fachdiskussion von Interesse: „Ob die Hersteller Sicherheit

anbieten, hängt von der Nachfrage ab. Nur wenn die Anwender massiv und breit danach verlangen, entsteht ein Markt und ein Preis dafür. Sie alle sind Anwender, helfen Sie mit, die angesprochenen Forderungen zu konkretisieren und zu unterstützen – und nutzen sie dann auch die Angebote!" (Datenschutz-Berater 4/1985 S. 17).

Inzwischen ist es nach sehr intensiven Bemühungen gelungen, einen Hersteller zu veranlassen, für die von einer Stadt eingesetzten Programme eine derartige Programmsicherung durch Versiegeln zu verwirklichen. Der Stadtdirektor und der Hersteller der Datenverarbeitungsanlage sehen darin einen Pilotfall für eine wesentliche Verbesserung der Datensicherheit bei Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik. Bei Bewährung will der Hersteller sein Verfahren für das Versiegeln von Programmen für weitere Anwendungsfälle einsetzen.

Jeder Anwender, der eine kleinere Datenverarbeitungsanlage mit verbindlicher Verarbeitungslogik einsetzt, sollte den Hersteller seiner Datenverarbeitungsanlage auf die bestehende Lücke der Datensicherheit hinweisen und Maßnahmen fordern, diese Lücke zu schließen. Die Hersteller sollten den Anwendern eine Möglichkeit bereitstellen, den unveränderten Einsatz von Programmen sicherzustellen und zu überprüfen.

#### – **Versiegeln von Programmen als Maßnahme gegen Programmviren**

Auf einen weiteren Vorteil des Versiegelns von Programmen soll noch hingewiesen werden. In den letzten Monaten wird in der Fachwelt über „Programmaviren“ diskutiert. Darunter sind Programmteile zu verstehen, die sich selbsttätig von einem gerade aufgerufenen Programm in andere Programme kopieren. Sie werden damit Teile dieser anderen Programme. Programmaviren sollen Programme sein, die unter bestimmten Umständen jedes Programm, in das sie eingebaut sind, schädigen oder in seinem Ablauf blockieren. Man hat sich zwei Phasen der Wirkung des Virus vorzustellen. In der ersten Phase breitet sich das Virus lediglich aus, ohne darüber hinaus schädigend wirksam zu werden. Die zweite Phase wird durch einen Auslöser, der etwa ein Tagesdatum sein kann, eingeleitet. In dieser zweiten Phase würde kein mit dem Virus behaftetes Programm ordnungsgemäß ablaufen.

Selbstverständlich wäre es als Maßnahme gegen Programmaviren hilfreich, laufend kontrollieren zu können, ob Programme modifiziert wurden. Eine derartige Möglichkeit könnte das Versiegeln der Programme bieten. Bei einem versiegelten Programm wäre erkennbar, ob eine „Infektion“ erfolgt ist. Geeignete Gegenmaßnahmen könnten im allgemeinen so bald eingeleitet werden, daß eine nennenswerte Beeinträchtigung der Arbeit der Datenverarbeitungsanlage durch das Programmavirus vermieden wird.

Das Versiegeln hat noch eine weitere günstige Wirkung. Das Einbringen eines Programmavirus ist für denjenigen, der das Programmavirus von außen in das erste Programm einbringt, dann mit einem besonderen Risiko verbunden, wenn damit zu rechnen ist, daß die Manipulation schon nach kurzer Zeit aufgedeckt wird. In einem solchen Fall muß der Verursacher mit hoher Wahrscheinlichkeit seine Entdeckung befürchten.

#### – **Sichern der Programmwartung**

Programme bedürfen im allgemeinen der laufenden Wartung. Ursachen für die Notwendigkeit der Programmwartung sind Änderungen der sachlichen oder rechtlichen Grundlagen des Programms, Programmfehler oder Änderungen der Umgebung des Programms, das heißt Änderungen des Betriebssystems oder der Hardware.

Wer eine Datenverarbeitungsanlage einsetzt, wird vom einwandfreien Ablauf

der darauf abzuwickelnden Arbeiten mehr oder weniger abhängig. Da die Programmwartung eine Voraussetzung der einwandfreien Arbeit ist, muß sichergestellt werden, daß sie immer sachgerecht und rechtzeitig erfolgt. Programmwartung ist im allgemeinen eine Aufgabe der Stelle, die das Programm entwickelt hat. Sichern der Programmwartung bedeutet daher, daß diese Stelle entsprechende Verpflichtungen übernehmen muß. Auf einzelne Sachverhalte, die in diesem Zusammenhang geregelt werden sollten, habe ich in meinem sechsten Tätigkeitsbericht (D.5.a) hingewiesen.

Bei einer kontrollierten Stadt hat die Lieferfirma der Datenverarbeitungsanlage auch die Anwendungsprogramme geliefert. Die Lieferfirma hat gegenüber der Stadt keine Verpflichtung zur Programmwartung übernommen. Zur Sicherung der zukünftigen Datenverarbeitung halte ich es für erforderlich, daß die Lieferfirma ihre Bereitschaft zur Programmwartung erklärt. Die Lieferfirma sollte wenigstens ihre Bereitschaft zur Programmwartung für einen zu vereinbarenden Zeitraum verbindlich zusagen. Angemessen wäre es, wenn die Lieferfirma darüber hinaus verbindlich zusagen würde, daß sie die Programmwartung nicht aufgeben wird, ohne die Stadt wenigstens zwei Jahre vorher schriftlich darüber zu unterrichten. Ich habe empfohlen, mit der Lieferfirma wegen entsprechender Zusagen zur Programmwartung zu verhandeln.

#### **- Schwierigkeiten bei der Eigenentwicklung von Programmen**

Auf kleineren Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik werden im allgemeinen Fremdprogramme eingesetzt. Naheliegend ist die Frage, ob es möglich und zweckmäßig ist, einzelne Programme selbst zu entwickeln oder die Fremdprogramme selbst so zu ändern, daß sie den eigenen Anforderungen besser angepaßt sind.

Es ist zwar davon auszugehen, daß die Fremdprogramme der verbindlichen Verarbeitungslogik entsprechen. Dennoch gibt es im allgemeinen viele Programmeigenschaften, die trotz der verbindlichen Verarbeitungslogik nicht vorgegeben sind. Derartige Programmeigenschaften betreffen etwa Form und Anordnung der Eingabe und Ausgabe oder die Anpassung an organisatorische Gegebenheiten wie bestehende Nummernsysteme.

Bei den Plänen und Entscheidungen, Programme selbst zu entwickeln oder zu ändern, werden oft die eigenen Möglichkeiten überschätzt und die bestehenden Schwierigkeiten unterschätzt. Zwar sind die Kosten der Datenverarbeitungsanlagen in den letzten Jahren stark gesunken; mit einem weiteren Sinken ist auch in der Zukunft zu rechnen. Nicht entsprechend gesunken sind aber Schwierigkeit und Kosten der Entwicklung von Programmen. Gerade deshalb werden kleinere Datenverarbeitungsanlagen im allgemeinen mit Fremdprogrammen betrieben.

In manchen Fällen hat der Hersteller des Programms bereits gewisse Möglichkeiten zur Anpassung an den jeweiligen Einsatzfall vorgesehen. Ein solches Programm kann dann durch Eingabe von Parametern den Wünschen des Anwenders angepaßt werden. Jedes darüber hinausgehende Eingreifen des Anwenders in die Programmlogik sollte aber unterbleiben. Schon die geringste zusätzliche Änderung führt dazu, daß das Programm neu getestet und freigegeben werden muß. Die ändernde Stelle übernimmt mit einer solchen Änderung eine Verantwortung, die sie nur selten tragen kann. Dem Bearbeiter fehlen die für die Änderung notwendigen Kenntnisse des Gesamtprogramms. Der zuständige Vorgesetzte ist im allgemeinen weder in der Lage, Schwierigkeitsgrad und Verantwortbarkeit der Änderung zu beurteilen, noch kann er die durchzuführenden Arbeiten fachlich beaufsichtigen.

Die Entwicklung eigener Programme ist dann ähnlich zu beurteilen, wenn

durch die Programme wesentliche Dateien geändert werden können. Auch in diesem Fall kann der zuständige Vorgesetzte das damit verbundene Risiko im allgemeinen nicht überblicken und die Entwicklung nicht fachlich beaufsichtigen. Insbesondere sollten Dateien, die von Fremdprogrammen verwaltet werden, keinesfalls von eigenen Programmen geändert werden dürfen.

In Einzelfällen wird der Wunsch geäußert, eigene Programme zu entwickeln, um bestehende Dateien statistisch auswerten zu können. Die Bedenken gegen den Einsatz derartiger Programme sind zwar geringer. Es besteht allerdings auch in diesem Fall das schon mehrfach genannte Problem der Überwachung des Befugten. Falls zum Beispiel nur ein Mitarbeiter für Bedienung und Programmierung der Datenverarbeitungsanlage zuständig ist, erscheint es ausgeschlossen, diesen Mitarbeiter bei Einsatz eigener Programme daran zu hindern, von ihm gewünschte Dateiänderungen vorzunehmen.

#### **d) Sicherheit der Daten**

##### **- Zuführen nach ordnungsgemäßem Erfassen**

Selbstverständlich muß sichergestellt sein, daß dem Datenverarbeitungssystem nur ordnungsgemäß erfaßte Daten zugeführt werden. Bezüglich dieser Anforderung unterscheidet sich die Situation bei Einsatz einer kleineren Datenverarbeitungsanlage nicht wesentlich von derjenigen bei der Arbeit mit einem großen Rechenzentrum. Das Zuführen der Daten liegt im allgemeinen in der Verantwortung des Anwenders. Das Sicherstellen des ordnungsgemäßen Erfassens ist daher weniger ein Problem der automatisierten Datenverarbeitung als eine Frage der konventionellen Organisation.

Bei Kontrollbesuchen zeigte sich allerdings, daß häufig die in den kleineren Datenverarbeitungsanlagen eingesetzten Programme weniger Unterstützung für Kontrollen liefern. Die Ursache dafür sehe ich nur zum Teil in der geringeren Größe der Datenverarbeitungsanlage. Ursächlich scheint mir vor allem zu sein, daß bei Programmentwicklungen für eine kleinere Datenverarbeitungsanlage nur ein geringerer Aufwand als angemessen angesehen wird.

Als Beispiel dafür kann die Eingabekontrolle dienen, die bei Einsatz kleinerer Datenverarbeitungsanlagen nur selten hinreichend verwirklicht ist. Nach § 6 Abs. 1 Satz 1 DSGVO in Verbindung mit Nr. 7 der Anlage zu dieser Vorschrift hat die speichernde Stelle die technischen und organisatorischen Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten geeignet sind zu gewährleisten, daß nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind (Eingabekontrolle). Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht (§ 6 Abs. 1 Satz 2 DSGVO).

Zur Eingabekontrolle bei der kleineren Datenverarbeitungsanlage einer kontrollierten Stadt, deren Programme die Lieferfirma der Datenverarbeitungsanlage bereitstellt, werden die einzelnen Eingaben ausgedruckt und aufbewahrt. Derartige Ausdrucke werden allerdings schon nach einigen Wochen vernichtet. Eine Eingabekontrolle ist daher nur über den Zeitraum einiger Wochen möglich. Für weiter zurückliegende Eingaben ist eine Eingabekontrolle bei diesem Verfahren ausgeschlossen.

Die auf einige Wochen beschränkte Archivierung von Inhalt, Zeitpunkt und Verursacher einer Dateiänderung ist im allgemeinen für Zwecke der Eingabekontrolle nicht ausreichend. Die Eingabekontrolle sollte eine nachträgliche Überprüfung über wesentlich längere Zeiträume ermöglichen. Jedenfalls

muß eine Überprüfung solange möglich sein, wie die eingegebenen Daten unverändert in der Datei gespeichert sind.

Für Zwecke der Eingabekontrolle ist daher eine Protokollierung auf einem maschinenlesbaren Datenträger üblich. Durch maschinelle Umsortierung kann daraus eine Historie jedes gespeicherten Datensatzes erzeugt werden. Diese Historien der Datensätze dienen dann der Eingabekontrolle. Ich habe der Stadt empfohlen zu klären, ob es für die bei ihr eingesetzten Programme entsprechende Ergänzungen bei der Lieferfirma gibt, die eine maschinelle Protokollierung für Zwecke der Eingabekontrolle ermöglichen. Andernfalls sollte die Lieferfirma zu Programmergänzungen veranlaßt werden, die eine Eingabekontrolle über hinreichend lange Zeiträume ermöglichen.

Bei den Dateien einer kontrollierten Stadtbücherei ist keine Eingabekontrolle im Sinne des Datenschutzgesetzes Nordrhein-Westfalen verwirklicht. Eine Eingabekontrolle würde allerdings voraussetzen, daß sich der einzelne Mitarbeiter bei der Bedienung eines Datenendgeräts gegenüber der Datenverarbeitungsanlage identifiziert. Eine solche Identifizierung ist bei den Programmen der Stadtbücherei nicht vorgesehen, weil eine Benutzung der Datenendgeräte durch Unbefugte durch die räumliche Anordnung ausgeschlossen ist.

Auch bei der beschränkten Speicherkapazität einer solchen kleinen Datenverarbeitungsanlage ist es möglich, für die wichtigsten Datenarten eine Eingabekontrolle im Sinne des Datenschutzgesetzes Nordrhein-Westfalen zu verwirklichen. Ich habe darauf hingewiesen, daß die Eingabekontrolle programmiert werden kann, sobald vom Programmkonzept sichergestellt ist, daß sich der einzelne Bediener eines Datenendgeräts gegenüber der Datenverarbeitungsanlage identifiziert. Falls im Rahmen einer zukünftigen Änderung des Programmkonzepts eine Identifizierung der Benutzer der Datenendgeräte gegenüber der Datenverarbeitungsanlage eingeführt wird, sollte daher wenigstens für die wichtigsten Datenarten eine Eingabekontrolle verwirklicht werden.

#### **- Verarbeiten im Rahmen ordnungsgemäßer Programmläufe**

Die Forderung, das Verarbeiten der Daten im Rahmen ordnungsgemäßer Programmläufe sicherzustellen, ist nur schwer erfüllbar. Diese Aufgabe gleicht derjenigen sicherzustellen, daß Programme nicht in unzulässiger Weise verändert werden. Oben (D.5.c) wurde erörtert, warum es bei kleineren Datenverarbeitungsanlagen mit den heute verfügbaren Hilfsmitteln fast unmöglich ist, unzulässige Programmänderungen mit hinreichender Sicherheit auszuschließen. Die Schwierigkeit liegt vor allem darin, daß der Maschinenbediener kaum überwacht werden kann. Ähnlich ist die Situation bezüglich des ordnungsgemäßen Einsatzes von Programmen. Die Nutzung der Programme kann zwar in der Dienstanweisung geregelt werden. Das Einhalten der Dienstanweisung ist bei einer kleineren Datenverarbeitungsanlage aber im allgemeinen schwer zu kontrollieren.

Eine konzeptionelle Möglichkeit, die in der Zukunft vielleicht einen Ausweg aus dieser Schwierigkeit bieten könnte, wird unten erörtert.

#### **- Verhindern von Verlust, unzulässiger Verarbeitung, Nutzung oder Kenntnisnahme**

Das Sichern von Daten gegen Verlust ist bei Einsatz kleinerer Datenverarbeitungsanlagen in ähnlicher Weise wie in großen Rechenzentren möglich. Insbesondere können Daten dupliziert und durch Auslagern an einen anderen Ort zusätzlich gesichert werden. Bei Daten, die in besonderer Weise gegen Verlust zu sichern sind, kann eine Auslagerung in zwei unabhängige Auslagerungsarchive vorgesehen werden.

Weitere Maßnahmen sind möglich, um unzulässige Zugriffe zu den Daten zu verhindern. Datenträger sind verschlossen aufzubewahren. Auch sollte sichergestellt werden, daß nur der Bediener der Datenverarbeitungsanlage Zugang zu den Datenträgern hat. Darüber hinaus können Regelungen getroffen werden, die der speziellen Situation angemessen sind, wie Kontrollbesuche immer wieder zeigen.

Die Datenverarbeitungsanlage eines kontrollierten Gymnasiums wird sowohl zur Verarbeitung von personenbezogenen Daten als auch für den Unterricht im Fach Informatik genutzt. Es ist erforderlich, durch geeignete organisatorische und technische Maßnahmen sicherzustellen, daß den Schülern während ihrer Übungsarbeiten im Fach Informatik keine personenbezogenen Daten bekannt werden.

Während des Kontrollbesuchs wurde berichtet, daß Arbeiten mit personenbezogenen Daten nur zu Zeiten erfolgen, in denen keine Übungsarbeiten an der Datenverarbeitungsanlage ausgeführt werden. Auch seien Dateien mit personenbezogenen Daten ausschließlich auf Wechselplatten und Disketten gespeichert. Während der Übungsarbeiten von Schülern sei keiner dieser Datenträger mit personenbezogenen Daten in ein Gerät der Datenverarbeitungsanlage eingelegt. Ein Zugriff von Schülern zu personenbezogenen Daten sei daher ausgeschlossen. Eine Anweisung, so zu verfahren, bestehe allerdings nicht. Ich habe empfohlen, eine entsprechende Regelung durch Dienstanweisung zu treffen.

Ich gehe davon aus, daß während der Übungsarbeiten von Schülern dieses Gymnasiums keine Möglichkeit des Zugriffs zu den Datenträgern besteht, auf denen die Dateien mit personenbezogenen Daten gespeichert sind. Dennoch könnten während der Übungsarbeiten in der Datenverarbeitungsanlage personenbezogene Daten verfügbar sein. Personenbezogene Daten könnten in einem Speicherbereich, der während einer früheren Verarbeitung dieser Daten als Zwischenspeicher benutzt wurde, aufgezeichnet sein. Eine solche Aufzeichnung könnte im Arbeitsspeicher oder im Arbeitsbereich eines im Zugriff befindlichen sonstigen Datenspeichers erfolgt sein. Es ist nicht auszuschließen, daß die Daten den Schülern im Rahmen ihrer Übungsarbeiten zugänglich werden.

Durch eine geeignete Maßnahme sollte daher ausgeschlossen werden, daß personenbezogene Daten aus einer früheren Verarbeitung nach Abschluß dieser Verarbeitung noch in der Datenverarbeitungsanlage verfügbar sind. Als Zwischenspeicher benutzte Speicherbereiche sollten nach Abschluß von Arbeiten mit personenbezogenen Daten gelöscht oder mit anderen Informationen beschrieben werden. Eine unbefugte Kenntnisnahme von personenbezogenen Daten aus früherer Verarbeitung während nachfolgender Übungsarbeiten wäre damit ausgeschlossen. Ich habe empfohlen vorzuschreiben, daß als Zwischenspeicher benutzte Speicherbereiche nach Abschluß von Arbeiten mit personenbezogenen Daten zu löschen oder mit anderen Informationen zu beschreiben sind.

Zur Sicherung gegen Datenverlust bei einem plötzlich auftretenden Schaden an der Festplatte werden bei einer kontrollierten Stadtbücherei die Ausleihe und Rückgabe von Büchern und die Zahlung von Gebühren zusätzlich in einer Protokolldatei gespeichert. Die aufgezeichneten Protokolldaten stehen nur für die Dauer eines Tages zur Verfügung. Am folgenden Tag werden die neuen Protokolldaten in den für die Protokolldatei vorgesehenen Bereich eingetragen, indem jeweils vom Anfang des Bereichs beginnend fortlaufend aufgezeichnet wird. Die Daten des Vortages werden durch Überschreiben gelöscht.

Allerdings werden jeweils nur so viele Daten gelöscht, wie an dem betreffen-

den Tag neu eingetragen werden. Es ist daher nicht ausgeschlossen, daß Reste alter Protokoll Daten über längere Zeit ungelöscht erhalten bleiben. Während des Kontrollbesuchs wurde besprochen, daß durch eine einfache Programmänderung sichergestellt werden kann, daß die Protokolldatei vor dem erneuten Beschreiben vollständig gelöscht wird. Ich habe empfohlen, eine Programmänderung zu veranlassen, die sicherstellt, daß die gesamte Protokolldatei nach Ablauf der vorgegebenen Löschrfrist gelöscht wird.

Bei Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik gibt es zweifellos eine große Zahl möglicher Einzelmaßnahmen zur Sicherung von Daten gegen unzulässige Verarbeitung, Nutzung oder Kenntnisnahme. Dennoch ist eine hinreichende Sicherung im allgemeinen kaum zu verwirklichen. Die Eigenart der Situation ist vergleichbar mit der Schwierigkeit sicherzustellen, daß unveränderte Programme eingesetzt werden (oben D.5.c). Es ist möglich, entsprechende Regelungen in der Dienst-anweisung vorzuschreiben. Praktisch nicht möglich ist es aber sicherzustellen, daß der Bediener der Datenverarbeitungsanlage entsprechend diesen Vorschriften verfährt, da die Möglichkeiten zur Kontrolle nur gering sind. Die Schwierigkeit liegt auch hier wieder in der Überwachung des Befugten.

Langfristig sehe ich eine Möglichkeit, ausreichende Maßnahmen zur Datensicherung zu verwirklichen. Gesichert werden könnten kleinere Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik, auf denen ausschließlich Fremdprogramme eingesetzt werden. Diese Fremdprogramme sollten durch Versiegeln (oben D.5.c) gegen unzulässige Veränderungen gesichert werden. Darüber hinaus sollten die versiegelten Anwendungsprogramme in den zugelassenen Anwender- und Bedienerfunktionen so beschränkt sein, daß eine unzulässige Verarbeitung, Nutzung oder Kenntnisnahme der in der Anlage gespeicherten Daten bereits durch die Programme nach Möglichkeit ausgeschlossen wird.

Eine derartige Beschränkung von Anwender- und Bedienerfunktionen kann jeweils nur bei speziellen Anwendungen verwirklicht werden. Zusätzlich sollte die Datensicherung durch eine aussagekräftige und nicht unterdrückbare Protokollierung sämtlicher Bedieneraktivitäten gestützt werden.

#### **e) Sicherheit bei Ausnahmesituationen**

Als Ausnahmesituation in einem Rechenzentrum, die besondere Maßnahmen erfordert, kommt etwa eine Extremsituation wie ein Brand in Betracht, bei dem die Zerstörung des Rechenzentrums droht. Die für die Datensicherung wichtigste Vorsorgemaßnahme für eine solche Ausnahmesituation ist das Auslagern der Daten. Das Auslagern muß in der Dienst-anweisung geregelt sein. Dabei ist unter anderem festzulegen, welche Dateien wann auszulagern sind. Darüber hinaus sollte durch geeignete Kontrollen (unten D.5.f) sichergestellt werden, daß auch tatsächlich entsprechend der Dienst-anweisung verfahren wird.

Eine Besonderheit beim Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik liegt darin, daß es Ausnahmesituationen ganz anderer Art geben kann, die wie der Brand des Rechenzentrums dazu führen können, daß die datenverarbeitende Stelle an der Durchführung von Arbeiten auf ihrer Datenverarbeitungsanlage gehindert wird. Falls ein zeitweiliger Ausfall der Möglichkeit, die Datenverarbeitungsanlage zu betreiben, die Arbeitsfähigkeit der datenverarbeitenden Stelle in untragbarer Weise beeinträchtigt, ist der Einsatz einer eigenen kleineren Datenverarbeitungsanlage nur dann verantwortbar, wenn auch für derartige Ausnahmesituationen Vorsorge getroffen ist. Einige Beispiele sollen die bestehenden Gefahren erläutern.

Es wurde bereits darauf hingewiesen (oben D.5.c), daß Anwendungsprogramme in gewissen Zeitabständen gewartet werden müssen. Möglicherweise muß ein

bisher einwandfreies Programm von einem bestimmten Zeitpunkt an in seiner Programmlogik geändert sein und darf danach in der bisherigen Logik nicht mehr eingesetzt werden. Eine derartige Situation kann als Folge einer Gesetzesänderung eintreten. Dann ist es wichtig, daß die Wartung des Programms gesichert ist. Sollte bei Einsatz von Fremdprogrammen die für die Wartung zuständige Stelle oder Firma nicht oder nicht rechtzeitig zu den Wartungsarbeiten in der Lage sein, muß eine andere Stelle mit diesen Arbeiten beauftragt werden können. Dazu muß die datenverarbeitende Stelle über die Quellprogramme und über eine für die Wartung geeignete Dokumentation der Programme verfügen.

Auf weitere mögliche Ausnahmesituationen und entsprechende Maßnahmen zur Vorsorge habe ich in meinem vierten Tätigkeitsbericht (D.5.c) hingewiesen. Bei einer kleineren datenverarbeitenden Stelle, die selbst programmiert, aber nur über zwei Programmierer verfügt, kann nicht ausgeschlossen werden, daß beide Programmierer durch Krankheit oder Unglücksfall gleichzeitig ausfallen. Es ist daher Vorsorge für den Fall zu treffen, daß in einer solchen Situation die Notwendigkeit der Programmwartung eintritt.

Eine ähnliche Situation besteht bezüglich der Bedienung der Datenverarbeitungsanlage. Falls nur ein Mitarbeiter die für die Bedienung der Datenverarbeitungsanlage erforderlichen Kenntnisse besitzt, ist es notwendig vorzusorgen, daß der Betrieb der Datenverarbeitungsanlage bei Ausfall dieses Mitarbeiters ohne Beeinträchtigung weiterläuft. Welche Dokumentation und welche Aufzeichnungen dafür vorhanden sein müssen, kann nur im Einzelfall entschieden werden. Möglicherweise ist es sogar angemessen, durch Absprache mit einer fachlich qualifizierten anderen Stelle frühzeitig für eine derartige Notlage vorzusorgen.

Die Anforderungen möglicher Ausnahmesituationen sollten rechtzeitig durchdacht werden. Dabei sollte vor allem geklärt werden, wie stark die Abhängigkeit von der termingerechten Abwicklung der Arbeiten auf der Datenverarbeitungsanlage ist. Vorsorgemaßnahmen sind jedenfalls insoweit erforderlich, als eine Unterbrechung als nicht tragbar angesehen werden muß.

#### **f) Organisation und Kontrolle**

##### **– Sicherstellen, daß angemessene Maßnahmen getroffen werden**

Es ist Aufgabe der öffentlichen Stelle, bei der eine kleinere Datenverarbeitungsanlage mit verbindlicher Verarbeitungslogik eingesetzt ist, und es gehört insbesondere auch zur Verantwortung des für die kleinere Datenverarbeitungsanlage zuständigen Vorgesetzten sicherzustellen, daß angemessene Maßnahmen zur Sicherheit der Programme, zur Sicherheit der Daten und zur Sicherheit bei Ausnahmesituationen (oben D.5.c–e) getroffen werden. Die Auswahl der zweckmäßigen Maßnahmen und die Entscheidung darüber, welche Maßnahmen angemessen sind, setzt Fachwissen der automatisierten Datenverarbeitung voraus. Über ein gewisses Fachwissen der automatisierten Datenverarbeitung verfügen die für die Bedienung der Datenverarbeitungsanlage eingesetzten Mitarbeiter. Innerhalb der öffentlichen Stelle ist derartiges Fachwissen darüber hinaus häufig nicht vorhanden. Auch der für die automatisierte Datenverarbeitung zuständige Vorgesetzte verfügt nur in seltenen Fällen über Fachwissen der automatisierten Datenverarbeitung.

Um die erforderlichen Entscheidungen zu Fragen der Datensicherheit treffen zu können, sollte sich die öffentliche Stelle daher beraten lassen. Eine solche Beratung ist nicht nur vor der Erstinstallation einer kleineren Datenverarbeitungsanlage zweckmäßig. Vielmehr sollte eine kontinuierliche Beratung sichergestellt werden, da sich die Anforderungen und Möglichkeiten der

Datensicherung wegen der Weiterentwicklung der Anwendungen und der Technik der automatisierten Datenverarbeitung ständig ändern.

Häufig will die öffentliche Stelle nicht nur zu Fragen der Datensicherung beraten werden. Es besteht vielmehr Interesse an einer umfassenden Beratung zu sämtlichen Fragen der automatisierten Datenverarbeitung. Einige Stichworte sollen den Umfang möglicher Beratungsthemen aufzeigen:

- Organisation und Technik der Datensicherung
- Marktsituation
- Untersuchung und Vorschläge zur Auswahl der Hardware
- Untersuchung und Vorschläge zur Auswahl der einzusetzenden Programme
- Aufstellen einer Konzeption zur Programmentwicklung (Fremdentwicklung, gemeinsame zentrale Entwicklung mehrerer Anwender, eigene Entwicklung)
- Zentrale Beschaffung (Stärken der Stellung gegenüber Herstellern durch gemeinsame Beschaffung)
- Projektmanagement
- Ausbildung, Schulung
- Aufstellung, Inbetriebnahme

Beratung zu einigen der angeschnittenen Fragen bieten im allgemeinen die Lieferanten der Hardware oder der Software an. Ziel der Beratung ist es dabei allerdings, den Vertrieb der eigenen Produkte zu unterstützen. Diese Art der Beratung ist wertvoll und notwendig. Sie sollte im allgemeinen aber durch eine herstellerunabhängige Beratung ergänzt werden. Eine solche herstellerunabhängige Beratung können Stellen mit den entsprechenden Kenntnissen der automatisierten Datenverarbeitung und der Probleme des Anwenders übernehmen. Zu denken ist in diesem Zusammenhang an bestehende größere Rechenzentren oder Datenzentralen, die auch eine zentrale Funktion bei einer eventuellen Gemeinschaftsentwicklung von Programmen übernehmen könnten.

Es wurde bereits darauf hingewiesen, daß Industrieunternehmen dazu übergehen, ihrem für die automatisierte Datenverarbeitung zuständigen Bereich ein Information Center anzugliedern (oben D.5.a). Die Aufgaben des Information Center sind dem bei der Industrie vorherrschenden Organisationskonzept der individuellen Datenverarbeitung angepaßt. Dagegen berücksichtigen die oben genannten Beratungsthemen und das Organisationskonzept die besonderen Anforderungen bei verbindlicher Verarbeitungslogik und die organisatorischen Gegebenheiten öffentlicher Stellen.

**- Zusammenfassen aller Regelungen zu einer schriftlichen Dienstanweisung**

Oben (ab D.5.c) wurde dargelegt, welche Voraussetzungen verwirklicht sein sollten, damit eine öffentliche Stelle die Datensicherheit bei Einsatz einer eigenen kleineren Datenverarbeitungsanlage mit verbindlicher Verarbeitungslogik gewährleisten kann. Darüber hinaus hat die öffentliche Stelle sicherzustellen, daß sich alle Mitarbeiter entsprechend den entwickelten Vorstellungen für die Datensicherheit verhalten. Als Voraussetzung ist es dazu erforderlich, daß dieses erwartete Verhalten verbindlich vorgeschrieben wird. Bei der großen Bedeutung der Datensicherheit sollten alle Anweisungen schriftlich erfolgen. Mündliche Anweisungen werden häufig mißverstanden oder als weniger verbindlich angesehen.

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

Bei einem Kontrollbesuch wurde besprochen, daß die von mir herausgegebene „Organisationshilfe zur Datensicherung“ (unten D.6.) Hinweise für den Inhalt der Dienstanweisung geben kann. Die Organisationshilfe enthält einen Katalog regelungsbedürftiger Sachverhalte für eine Dienstanweisung.

Die Organisationshilfe kann zunächst genutzt werden, um zu überprüfen, ob in der Dienstanweisung sämtliche im Rahmen der Datensicherung regelungsbedürftigen Sachverhalte geregelt werden. Durch Verweise auf Empfehlungen in meinen Tätigkeitsberichten gibt die Organisationshilfe darüber hinaus auch Hinweise für den Inhalt der zu treffenden Regelungen. In meinem sechsten Tätigkeitsbericht (D.5.c) habe ich darauf hingewiesen, daß zusätzliche Maßnahmen, die sich auf die eingesetzte Datenverarbeitungsanlage und die Anwendungsprogramme beziehen, von der jeweils liefernden Stelle vorgeschlagen werden sollten.

#### – **Institutionalisierung der Kontrolle**

Aufgabe der öffentlichen Stelle ist es nicht nur, ihren Mitarbeitern Anweisungen zur Datensicherung zu erteilen. Sie hat auch dafür zu sorgen, daß entsprechend den Anweisungen verfahren wird. Erst dadurch wird die erforderliche Datensicherheit gewährleistet. Dazu ist es notwendig zu kontrollieren, ob entsprechend der Dienstanweisung verfahren wird. Für derartige Kontrollen gibt es grundsätzlich die Möglichkeiten der Kontrolle durch den Vorgesetzten, der gegenseitigen Kontrolle der Mitarbeiter und der institutionalisierten Kontrolle.

Bei Einsatz kleinerer Datenverarbeitungsanlagen ist die Möglichkeit einer Kontrolle durch den Vorgesetzten insoweit eingeschränkt, als sie Fachwissen der automatisierten Datenverarbeitung erfordert. Derartiges Fachwissen kann bei dem Vorgesetzten häufig nicht vorausgesetzt werden. Eine Kontrolle der Durchführung der Arbeiten der automatisierten Datenverarbeitung durch den Vorgesetzten scheidet daher in vielen Fällen aus.

Die gegenseitige Kontrolle der Mitarbeiter setzt Funktionstrennung voraus. Funktionstrennungen sind nur möglich bei hinreichend großer Mitarbeiterzahl. Bei großen Rechenzentren gehört eine Reihe von Funktionstrennungen zu den selbstverständlichen organisatorischen Maßnahmen der Datensicherung. Ihre Bedeutung für die Datensicherung ist sehr groß.

Falls bei einer kleineren Datenverarbeitungsanlage nur ein einziger Mitarbeiter Aufgaben der automatisierten Datenverarbeitung wahrnimmt, besteht keine Möglichkeit zur Funktionstrennung. Bei nur wenigen Mitarbeitern sind die Möglichkeiten entsprechend eingeschränkt. Eine Organisation, die zu einer wirksamen gegenseitigen Kontrolle der Mitarbeiter führt, wird im allgemeinen erst bei einer größeren Zahl von Mitarbeitern möglich.

Gerade bei Einsatz kleinerer Datenverarbeitungsanlagen ist es daher wichtig, die Kontrolle in geeigneter Weise zu institutionalisieren. Notwendig ist vor allem eine Kontrolle des Befugten. Es wurde bereits darauf hingewiesen (oben D.5.b), daß die Überwachung des Befugten das schwierigste und bis heute nicht gelöste Problem darstellt. Durch die bisher erörterten Maßnahmen zur Datensicherung soll es zusammen mit einer institutionalisierten Kontrolle in Zukunft möglich sein, eine Überwachung des Befugten in ähnlich

befriedigender Weise zu erreichen, wie sie bei größeren Rechenzentren verwirklicht ist. Erst wenn dieses Ziel erreicht ist, kann das Problem der Datensicherung bei Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik als gelöst angesehen werden.

Bei einer öffentlichen Stelle, die eine kleinere Datenverarbeitungsanlage mit verbindlicher Verarbeitungslogik einsetzt, ist der Maschinenbediener möglicherweise der einzige Mitarbeiter, der über ein gewisses Fachwissen der automatisierten Datenverarbeitung verfügt. Zu der Kontrolle der automatisierten Datenverarbeitung ist derartiges Fachwissen erforderlich. Während verschiedener Kontrollbesuche wurde daher die Frage eingehend erörtert, wie eine solche Kontrolle verwirklicht werden kann. Dabei wurde jeweils besprochen, ob und wie eine andere fachlich qualifizierte Stelle mit der Durchführung der Kontrolle beauftragt werden könne.

Von einer Stadt, die eine kleinere Datenverarbeitungsanlage mit verbindlicher Verarbeitungslogik einsetzt, wurde die Frage gestellt, ob Bedenken dagegen beständen, die kommunale Datenverarbeitungszentrale (KDZ) mit der internen Kontrolle zu beauftragen.

Gegenstand der internen Kontrolle soll die Kontrolle der Einhaltung organisatorischer Regelungen im Zusammenhang mit dem Einsatz der automatisierten Datenverarbeitung bei der Stadt sein. Es ist davon auszugehen, daß die KDZ über Mitarbeiter verfügt, die zur Durchführung einer derartigen Kontrolle besonders qualifiziert sind. Auch ist die KDZ in der Lage, die fachliche Verantwortung für den Einsatz dieser Mitarbeiter zu übernehmen. Die KDZ bietet daher die fachlichen Voraussetzungen für diese Aufgabe.

Bedenken könnten wegen einer eventuellen Interessenkollision entstehen, soweit die interne Kontrolle sich auf Sachverhalte bezieht, bei deren Gestaltung die KDZ wesentliche Entscheidungshilfe geleistet hat. Innerhalb der KDZ sollten daher nach Möglichkeit eventuelle Aufgaben der internen Kontrolle und der Entscheidungshilfe unterschiedlichen Mitarbeitern zugeordnet werden.

Der Auftrag an die KDZ, Kontrollen bei der Stadt durchzuführen, darf die Verantwortung der Stadt als speichernde Stelle nicht beeinträchtigen. Die KDZ ist der Stadt für eine fachlich qualifizierte Durchführung der Kontrollen verantwortlich. Der konkrete Kontrollauftrag muß aber von der Stadt erteilt werden, die Berichte über die Kontrollen erhält die Stadt, und die Stadt verfolgt die Erledigung der in den Berichten vorgeschlagenen Maßnahmen.

Ein eventueller Vertrag der Stadt mit der KDZ würde die Kontrolle der Einhaltung organisatorischer Regelungen im Zusammenhang mit dem Einsatz der automatisierten Datenverarbeitung bei der Stadt betreffen. Zu den Aufgaben dieser Kontrolle gehört in keinem Fall eine der Phasen der Datenverarbeitung. Die im Auftrag durchgeführte Kontrolle ist daher keine Datenverarbeitung im Auftrag.

Die Weitergabe personenbezogener Daten an Mitarbeiter der mit der Kontrolle beauftragten öffentlichen Stelle ist daher Übermittlung. Zulässig ist eine derartige Übermittlung unter den Voraussetzungen des § 11 Abs. 1 Satz 1 DSG NW bzw. des § 69 Abs. 1 Nr. 1 SGB X. Darüber hinaus ist eine mögliche zusätzliche Einschränkung der Übermittlung nach § 76 SGB X zu beachten.

Über die Zulässigkeit einer Übermittlung personenbezogener Daten an den Auftragnehmer wäre in jedem Einzelfall zu entscheiden. Bei dieser Entscheidung ist zu berücksichtigen, daß die §§ 6 und 8 DSG NW bzw. §§ 6 und 15 BDSG die öffentliche Stelle zur datenschutzrechtlichen Selbstkontrolle verpflichten. Soweit eine öffentliche Stelle zur Selbstkontrolle durch eigene Mitarbeiter nicht oder nur unzureichend in der Lage ist, läßt sich daher die

Notwendigkeit einer im Auftrag durch einen Dritten durchgeführten Kontrolle aus den Vorschriften der Datenschutzgesetze ableiten. Zu dieser Kontrolle kann eine Übermittlung personenbezogener Daten erforderlich sein.

Im allgemeinen ist es organisatorisch angemessen und für die effektive Wahrnehmung aller Kontrollaufgaben günstig, die mit dem Datenschutz verbundenen zentralen Zuständigkeiten bei einer Person zusammenzufassen. Als Verantwortlicher bei der Stadt und Kontaktperson zur KDZ für die Kontrolle könnte daher der Beauftragte für den Datenschutz bestimmt werden. Ich habe der Stadt empfohlen, eine interne Kontrollinstanz für Fragen der Datensicherheit unter Berücksichtigung der oben genannten Gesichtspunkte zu schaffen.

Eine entsprechende Frage wurde von einem Krankenkassenverband gestellt. Dieser erledigt die Arbeiten der angeschlossenen Mitgliedskassen auf seiner Datenverarbeitungsanlage. Er berichtete, daß einzelne Mitgliedskassen erwägen, kleinere Datenverarbeitungsanlagen anzuschaffen, um die eigenen Arbeiten selbständig abwickeln zu können.

Während eines Kontrollbesuchs wies der Krankenkassenverband darauf hin, daß man von der einzelnen Mitgliedskasse nicht fordern könne, sie müsse einen Mitarbeiter haben, der über das für Kontrollen zu Fragen der Datensicherheit erforderliche Fachwissen verfüge. Bei dem weitgehenden Einsatz der automatisierten Datenverarbeitung setzten Kontrollen zur Datensicherheit das entsprechende Fachwissen der automatisierten Datenverarbeitung voraus. Dieses Fachwissen sei im allgemeinen bei einer Mitgliedskasse nicht vorhanden.

Vorhanden ist das für Kontrollen erforderliche Fachwissen der automatisierten Datenverarbeitung aber bei Mitarbeitern des Krankenkassenverbandes. Daher wurde besprochen, daß eine Mitgliedskasse ihrer Verpflichtung zu Kontrollen auf dem Gebiet der Datensicherheit auch entsprechen könnte, indem sie den Krankenkassenverband mit der Kontrolle der Datensicherheit beauftragt. Die Hinweise zu der entsprechenden Zusammenarbeit zwischen einer KDZ und einer Stadt gelten dabei in gleicher Weise.

Der einer anderen Stelle erteilte Kontrollauftrag ist als „Notlösung“ anzusehen. Langfristig sollte eine andere organisatorische Lösung angestrebt werden. Falls Programme versiegelt werden (oben D.5.c) und die versiegelten Programme so konzipiert sind, daß nur sehr wenige Aktivitäten von der Datenverarbeitungsanlage zugelassen werden (oben D.5.d), kann aus der universell einsetzbaren Datenverarbeitungsanlage eine Anlage für eine Anwendung oder für wenige Anwendungen werden. Dadurch könnte das Ziel erreicht werden, daß die Handhabung dieser Anlage kein Fachwissen der automatisierten Datenverarbeitung erfordert. Dann würde auch die Kontrolle der Arbeiten ohne Fachwissen der automatisierten Datenverarbeitung möglich sein. Die öffentliche Stelle würde wieder in die Lage versetzt, ihre eigenen Arbeiten ohne Einschränkung selbst zu kontrollieren.

Sicher wäre es für viele öffentliche Stellen von großem Interesse, wenn dieses Fernziel erreicht werden könnte. Auf einer in dieser Weise in ihren Funktionen beschränkten Anlage würde allerdings wahrscheinlich kein einziges zusätzliches Programm ablaufen können. Weder sonstige Fremdprogramme noch Programme aus eigener Entwicklung würde die Anlage annehmen. Falls weitere Programme zum Ablauf kommen sollen, müßte dafür eine unabhängige zweite Anlage eingesetzt werden. Im Hinblick auf die voraussichtliche Preisentwicklung der Hardware und auf den großen Vorteil an Sicherheit bei dem vorgeschlagenen Organisationsmodell sehe ich darin aber kein wesentliches Hindernis.

### **g) Zusammenfassung**

Eine öffentliche Stelle, die eine kleinere Datenverarbeitungsanlage einsetzt, ist mit den ihr heute zur Verfügung gestellten Hilfsmitteln im allgemeinen nicht in der Lage, die Datensicherung bei Verarbeitung mit verbindlicher Verarbeitungslogik sicherzustellen. Ungelöst ist vor allem das Problem einer Kontrolle des Befugten. Unzulässige Handlungen des Maschinenbedieners lassen sich zwar erschweren; sie können aber nicht mit hinreichender Sicherheit ausgeschlossen werden. Schwierigkeiten bestehen dabei im Sicherstellen des Einsatzes unveränderter Programme, des Verarbeitens im Rahmen ordnungsgemäßer Programmläufe und des Verhinderns von unzulässiger Verarbeitung, Nutzung oder Kenntnisnahme der Daten.

Es gibt Möglichkeiten, die bestehenden Schwächen der Datensicherung bei Einsatz kleinerer Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik zu beseitigen. Dazu müssen allerdings die Hersteller der Datenverarbeitungsanlagen und die Lieferanten eventueller Fremdprogramme die notwendigen Voraussetzungen schaffen. Vorgeschlagen wird, die Programme durch Versiegeln gegen unzulässige Veränderung zu sichern. Das Versiegeln wäre auch gegen die in der Diskussion befindlichen Programmviren wirksam. Als zusätzliche Sicherung wird vorgeschlagen, Ablaufbeschränkungen der versiegelten Programme zu verwirklichen. Als Folge davon wäre die einzelne Datenverarbeitungsanlage allerdings voraussichtlich nur für eine Anwendung oder für eine beschränkte Zahl von Anwendungen verwendbar.

Eine öffentliche Stelle, die eine eigene kleinere Datenverarbeitungsanlage einsetzt oder einzusetzen beabsichtigt, sollte sich im allgemeinen in geeigneter Weise in Fachfragen der automatisierten Datenverarbeitung beraten lassen. Dazu sollte es im öffentlichen Bereich Stellen geben, die ähnlich dem Information Center der Industrie tätig werden.

Die Anweisungen zur Datensicherung sind in einer Dienstanweisung zusammenzufassen. Die Einhaltung der Dienstanweisung bedarf der Kontrolle. Das zur Kontrolle notwendige Fachwissen der automatisierten Datenverarbeitung ist allerdings bei den Stellen, die kleinere Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik einsetzen, häufig nicht vorhanden. Mit der Durchführung von Kontrollen sollte in dieser Situation eine fachlich qualifizierte andere Stelle beauftragt werden.

Langfristig könnte es erreichbar sein, daß durch Versiegeln und Ablaufbeschränkung der Programme eine Kontrolle ohne Fachwissen der automatisierten Datenverarbeitung möglich wird. Die Vergabe des Kontrollauftrags an eine andere Stelle wäre dann unnötig.

Ich gehe davon aus, daß es mit den genannten Maßnahmen möglich gemacht werden kann, kleinere Datenverarbeitungsanlagen mit verbindlicher Verarbeitungslogik so zu betreiben, daß die Datensicherheit dem heute erreichten hohen Standard bei großen Rechenzentren entspricht.

## **6. Organisationshilfe zur Datensicherung**

Die von mir jährlich herausgegebene Organisationshilfe zur Datensicherung soll als Hilfsmittel beim Gestalten der Datensicherung dienen. Sie stellt regelungsbedürftige Sachverhalte heraus und gibt durch Verweise auf Empfehlungen in meinen Tätigkeitsberichten Hinweise für den Inhalt ihrer Regelung. Die Organisationshilfe soll damit helfen, Schwachstellen der Datensicherung zu erkennen und zu beseitigen.

Verteilt wurde die Organisationshilfe bisher an öffentliche Stellen in Nordrhein-Westfalen mit großen Rechenzentren. Heute werden Geräte zur automatisierten Datenverarbeitung zunehmend auch außerhalb der großen Rechenzentren aufgestellt. Zahlreiche Anwender untersuchen die Frage, ob und wie bei ihnen kleinere Datenverarbeitungsanlagen eingesetzt werden können. In einer Reihe von Fällen wurden bereits entsprechende Entscheidungen getroffen. Dieser Situation wurde der bisherige Verteiler der Organisationshilfe nicht gerecht. Auf mehrfachen Wunsch wurde deshalb der Verteiler durch Aufnahme zahlreicher weiterer öffentlicher Stellen im Lande Nordrhein-Westfalen wesentlich erweitert.

## E. Weiterentwicklung des Datenschutzrechts

### 1. Novellierung des Bundesdatenschutzgesetzes

In einer Anhörung vor dem Innenausschuß des Deutschen Bundestages zu dem von der Fraktion der SPD bereits kurz nach dem Volkszählungsurteil des Bundesverfassungsgerichts eingebrachten Gesetzentwurf (Bundestagsdrucksache 10/1180) habe ich zu Fragen der Novellierung des Bundesdatenschutzgesetzes Stellung genommen. Nach längeren Verhandlungen haben inzwischen auch die Fraktionen der CDU/CSU und der FDP einen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes, des Verwaltungsverfahrensgesetzes, des Bundesverfassungsschutzgesetzes und des Straßenverkehrsgesetzes (Bundestagsdrucksache 10/4737) eingebracht.

Der Gesetzentwurf der Koalitionsfraktionen enthält zwar Verbesserungen gegenüber dem geltenden Recht. Die Datenschutzbeauftragten des Bundes und der Länder haben jedoch feststellen müssen, daß die vorgeschlagenen Regelungen den von ihnen erhobenen Forderungen nur unzureichend Rechnung tragen und den Vorgaben des Bundesverfassungsgerichts nur teilweise entsprechen. Zum Bundesdatenschutzgesetz haben sie in einer ersten Bewertung auf folgende Mängel hingewiesen:

- Das Recht auf informationelle Selbstbestimmung gilt für jeglichen Umgang mit personenbezogenen Daten. Daher ist es nicht gerechtfertigt, die Beschränkung des Bundesdatenschutzgesetzes auf Dateien festzuschreiben und die Datenerhebung auszugrenzen. Die vorgeschlagenen Regelungen im Verwaltungsverfahrensgesetz sind kein ausreichender Ersatz, weil wichtige Verwaltungsbereiche, wie zum Beispiel die Finanzbehörden, ausgenommen sind und die Datenverarbeitung in Akten und anderen Unterlagen der Datenschutzkontrolle weitgehend entzogen wird.
- Eine wirksame Kontrolle durch die Datenschutzbeauftragten in Bund und Ländern ist nach wie vor nicht sichergestellt.
- Das Auskunftsrecht des Bürgers bleibt stark eingeschränkt.
- Unbefriedigend ist auch, daß der Datenschutz im nicht-öffentlichen Bereich insgesamt nicht verbessert wird.

Die Länder Bremen, Hamburg, Hessen, Nordrhein-Westfalen und Saarland haben dem Bundesrat einen Gesetzentwurf zugeleitet, der eine Neufassung des Bundesdatenschutzgesetzes enthält (Bundesratsdrucksache 121/86). Der Entwurf, der die Datenverarbeitung in Akten sowie die Datenerhebung einbezieht, entspricht in der Konzeption und in vielen Einzelfragen auch meinen Vorstellungen.

### 2. Novellierung des Datenschutzgesetzes Nordrhein-Westfalen

Der von der Landesregierung im März 1985 eingebrachte Entwurf eines Gesetzes zur Fortentwicklung des Datenschutzes (Drucksache 9/4075) konnte bis zum Ende der 9. Wahlperiode des Landtags nicht mehr verabschiedet werden.

Wie die Landesregierung in ihrer Stellungnahme zu meinem sechsten Tätigkeitsbericht (Drucksache 10/430, S. 3) dargelegt hat, wird sie ihre Vorschläge zur Fortentwicklung des Datenschutzes sobald wie möglich erneut in den Landtag einbringen und dabei auch diejenigen datenschutzrechtlichen Überlegungen mit einbeziehen, die zwischenzeitlich in Bund und Ländern angestellt worden sind. Hierzu hat der Innenminister im Plenum des Landtags die Absicht bekundet, sehr bald einen neuen Referentenentwurf vorzulegen, der auf den Eckpunkten des früheren Gesetzentwurfs aufbaut (Plenarprotokoll 10/13, S. 886). Gerade auch vor dem Hintergrund der Vorschläge der Koalitionsfraktionen im Deutschen Bundestag zur Novellierung des Bundesdatenschutzgesetzes bietet sich hier der Landesregierung und dem Landtag die Chance, bei der Novellierung des Datenschutzgesetzes Nordrhein-Westfalen das bürgerfreundlichste Datenschutzgesetz der Bundesrepublik zu schaffen.

Düsseldorf, den 8. April 1986

Dr. Weyer