13. Wahlperiode

Drucksache **13/7165**

HESSISCHER LANDTAG

21. 02. 95

Dreiundzwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 1994
nach § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 21. Februar 1995 · Ausgegeben am 16. März 1995

Herstellung: Wiesbadener Graphische Betriebe GmbH, 65199 Wiesbaden · Auslieferung: Kanzlei des Hessischen Landtags · Postf. 3240 · 65022 Wiesbaden

INHALTSVERZEICHNIS

		Seite
1.	**Vorwort**	11
2.	**Europa**	11
2.1	Schengener Durchführungsübereinkommen	11
2.1.1	Zum Inhalt des Schengener Durchführungsübereinkommens	12
2.1.2	Schengener Informationssystem	12
2.2	Europol	12
3.	**Justiz**	13
3.1	Länderübergreifendes staatsanwaltschaftliches Verfahrensregister	13
3.2	Benachrichtigung gemeinnütziger Einrichtungen bei Verfahrenseinstellungen nach § 153a StPO	14
3.3	Datenschutz bei den Grundbuchämtern	14
3.4	Schuldnerverzeichnisse	15
4.	**Finanzen**	16
4.1	Datenschutz bei der Versendung von Lohnsteuerkarten	16
4.2	Steuernummer im Adreßfeld	17
5.	**Gesundheit**	17
5.1	Prüfung des Medizinischen Dienstes der Krankenversicherung Hessen	17
5.1.1	Aufgaben und Befugnisse des Medizinischen Dienstes der Krankenversicherung	18
5.1.2	Funktionelle Trennung zwischen Medizinischem Dienst und Krankenkassen	18
5.1.3	Speicherung von Versichertendaten in Dateien	19
5.1.4	Verpflichtung zur Datenlöschung nach fünf Jahren	20
5.1.5	Hinweis auf das Widerspruchsrecht der Versicherten	20
5.1.6	Speicherung medizinischer Daten bei externen Gutachtern	20
5.1.7	Überprüfung der Notwendigkeit und Dauer der Krankenhausbehandlung durch den Medizinischen Dienst	21
5.1.8	Datensicherheit in den Leit- und Beratungsstellen	21
5.1.9	Dienstanweisung des Medizinischen Dienstes zum Datenschutz	21
5.1.10	Einführung von ISmed beim Medizinischen Dienst	22
5.1.10.1	Technische Rahmenbedingungen	22
5.1.10.2	Anwendungspezifische Datensicherungsmaßnahmen	22
5.1.10.2.1	Benutzerkontrolle/Aufruf von ISmed	22
5.1.10.2.2	Zugriffskontrolle	22
5.1.10.2.3	Protokollierung	23
5.1.10.2.4	Verschlüsselung	23
5.1.10.3	Installationsspezifische Defizite	23
5.1.10.3.1	Zugriffsrechte	23
5.1.10.3.2	Fernbetreuung	23
5.1.10.3.3	Organisatorische Maßnahmen	23
5.2	Verarbeitung von Beihilfedaten	24
5.2.1	Trennung der Beihilfeakten von den Personalakten	24
5.2.2	Abschottung der Beihilfebearbeitung von der allgemeinen Personalverwaltung	24
5.2.3	Aufbewahrungsfristen von Beihilfeunterlagen	25
5.2.4	Vorprüfung von Beihilfeanträgen	25
5.2.5	Datensicherungsmaßnahmen	25
5.3	Maschinenlesbare Patientenkarten – Stand der Entwicklung und Diskussion	26

5.4 Behinderung der Einsicht in eine Patientenakte im Universitätsklinikum Frankfurt 27
5.5 Umsetzung des Hessischen Archivgesetzes im Universitätsklinikum Frankfurt 28
5.6 Einsichtsrecht in die Krankenakte bei stationärer Psychotherapie 29
6. Personalverwaltung 30
6.1 Prüfung der Personalaktenführung 30
6.1.1 Durchführung der Prüfungen 30
6.1.2 Organisation der Personalverwaltungen 30
6.1.3 Inhalt der Personalakten 32
6.1.4 Konsequenzen der Prüfungen 33
6.2 Weitergabe von Mitarbeiterdaten 33
7. Soziales 34
7.1 Neuordnung des Sozialdatenschutzes 34
7.1.1 Die neuen gesetzlichen Regelungen 34
7.1.1.1 Gesetzgebungsverfahren 34
7.1.1.2 Erhebung beim Betroffenen und Zweckbindung 34
7.1.1.3 Übermittlung von Sozialdaten an Polizei und Geheimdienste 35
7.1.1.4 Kontrollbefugnisse der Landesdatenschutzbeauftragten 35
7.1.2 Erste Anwendungserfahrungen im Bereich der Jugendämter 35
7.2 Datenverarbeitung beim Hessischen Amt für Versorgung und Soziales in Wiesbaden 36
7.3 Verwendungsnachweise für private Kinderbetreuungseinrichtungen 37
8. Schulen 38
8.1 Datenschutz in Schulen 38
8.1.1 Einsatz privater PC für schulische Zwecke 39
8.1.2 Fehlende Datensicherheit bei dienstlichen PC 39
8.1.3 Aufbewahrungsfristen und Archivierung bei schulischen Unterlagen 39
8.1.4 Unzulässige Klassenbucheintragungen 40
8.2 Klassenbücher im Müll 40
9. Forschung: Akteneinsicht in Strafakten zu Forschungszwecken 41
10. Archive 42
10.1 Aufbewahrung und Archivierung von Personalakten des Justizministeriums 42
10.2 Neue Benutzungsordnung für Hessische Staatsarchive 42
11. Kommunen 43
11.1 Prüfungen 43
11.1.1 Zugang und Sicherheit der Dienstgebäude und Diensträume 43
11.1.2 Führung der Melde- und Wahlunterlagen sowie der Personalakten 43
11.1.3 Archive 44
11.1.4 Probleme beim Einsatz von Novell-Netzen 44
11.2 Aufzeichnung von Vermittlungsgesprächen in Telefonzentralen 45
11.3 Information über Grundstückskauf 45
11.4 Was macht die Ehefrau, wenn ihr Mann an der Sitzung der Stadtverordnetenversammlung teilnimmt? 46
11.5 Behörde bringt Nachbarn gegeneinander auf 46
11.6 Weitergabe einer Namensliste über gewährte Zuschüsse zum Musikunterricht an einen städtischen Ausschuß 46
11.7 Anwesenheitslisten über Bürgerversammlungen 46
11.8 Fehlbelegungsabgabe 47

12.	**Melderecht**	47
12.1	Online-Verbindung zwischen Polizei und Meldebehörde – Programmfehler	47
12.2	Mangelhafte Aufklärung der Bürger bei der Beantragung von Führungszeugnissen	48
12.3	Adreßlisten an Ausländerbeiträte	49
12.4	Bekanntgabe der Anschrift des Frauenhauses durch ein Meldeamt	49
12.5	Auskünfte an Pächter eines Bürgerhauses	50
13.	**Umwelt**	50
13.1	Prüfungen bei Umweltämtern	50
13.2	Umweltinformationsgesetz des Bundes	53
14.	**Landwirtschaft**	54
14.1	Datenübermittlung aus der Weinbaukartei an eine private Firma im Rahmen einer EG-Prüfung	54
14.2	Datenübermittlung aus der Weinbaukartei an das Amt für Regionalentwicklung, Landschaftspflege und Landwirtschaft	55
14.3	Ernährungssicherstellung und Datenschutz	56
15.	**Behördliche Datenschutzbeauftragte**	56
16.	**Ausländerrecht**	56
16.1	Einbürgerung von Ausländern	56
16.1.1	Zum Ablauf des Verfahrens	57
16.1.2	Mängel des Verfahrens	57
16.2	Ausländerzentralregistergesetz	58
16.2.1	Das Ausländerzentralregister beim Bundesverwaltungsamt	58
16.2.2	Aufgaben und Inhalt des Registers	58
16.2.3	Kommunikation mit dem Register	58
16.2.4	Rechte des Betroffenen	59
16.3	Aufenthaltsgestattung mit Polizeivermerk	59
17.	**Verfassungsschutz**	60
17.1	Verbrechensbekämpfungsgesetz	60
17.2	Einbeziehung des Ehegatten in die Sicherheitsüberprüfung	61
18.	**Polizei**	61
18.1	Datenerhebung durch den Einsatz von V-Personen, Verdeckten Ermittlern sowie technischer Mittel	61
18.1.1	V-Personen und Verdeckte Ermittler	61
18.1.2	Technische Mittel	62
18.1.3	Umgang der Ermittlungsbehörden mit den neuen Befugnissen	62
18.2	Unterrichtung über polizeiliche Datenspeicherung	62
18.3	Verwechslungsfälle	63
18.3.1	Der Zuhälter	63
18.3.2	Der Mörder	64
18.3.3	Maßnahmen	64
18.4	Fahndung nach Ausbrechern aus psychiatrischen Krankenhäusern	64
18.5	Rahmendienstanweisung zum Datenschutz bei Arbeitsplatzrechnern und anderen IT-Geräten für die Hessische Vollzugspolizei	65
19.	**Ordnungswidrigkeiten**	65
19.1	Lichtbildvergleich in Ordnungswidrigkeitenverfahren	65
19.2	Weitere Ermittlungsmaßnahmen in Ordnungswidrigkeitenverfahren	66
20.	**Straßenverkehr: Inhalt einer Führerscheinakte für Zwecke der medizinisch-psychologischen Untersuchung**	67

21. Sparkassen kopierten rechtswidrig Pässe und Personalausweise ihrer Kunden 68
22. Telekommunikation 68
22.1 Postreform II 68
22.1.1 Folgen der Privatisierung für den Grundrechtsschutz und die Datenschutzkontrolle 69
22.1.2 Auskunft an Strafverfolgungsbehörden über den Fernmeldeverkehr 69
22.1.3 Anrufe bei Beratungseinrichtungen und Einzelgebührennachweis 69
22.2 EU-Richtlinie zum Datenschutz in Telekommunikationsnetzen (ISDN-Richtlinie) 70
23. Statistik: Novellierung des Landesstatistikgesetzes 70
24. Presseerklärungen der Regierung 71
25. Datensicherheitskonzepte 72
25.1 Allgemeine Anmerkungen 72
25.1.1 Überblick 72
25.1.2 Sicherheit am PC-Arbeitsplatz 73
25.2 Einzelne Projekte 73
25.2.1 Das Hessische Ministerium für Umwelt und Bundesangelegenheiten 73
25.2.2 Polizei 73
25.2.3 Staatskanzlei 74
26. Einsatz von Verschlüsselungsverfahren 74
26.1 Datenübertragung zwischen der AOK Hessen und Arbeitgebern 74
26.2 Umsetzung der Pflegeversicherung; Einbeziehung externer Gutachter 74
27. Workshop Kryptografie 75
27.1 Verschlüsselungsverfahren 75
27.1.1 Sicherheit von Verschlüsselungsverfahren 75
27.1.2 DES 76
27.1.3 RSA 76
27.1.4 Neue Entwicklungen 76
27.2 Offenlegung von Verschlüsselungsverfahren 77
27.3 Neue Entwicklungen in der elektronischen Kommunikation 77
27.3.1 Überwachung elektronischer Kommunikation 77
27.3.1.1 Situation in den USA 77
27.3.1.2 Situation in Deutschland 78
27.3.1.3 Situation in Frankreich 78
27.3.1.4 Weitere Ansätze 78
27.3.2 Neue Mechanismen 79
27.3.3 Ausblick auf soziale und politische Implikationen von Sicherheitsinfrastrukturen 79
27.3.4 Problem der Offenlegung geheimer Schlüssel 79
27.4 Probleme aus der Nutzung von Verschlüsselungsverfahren 80
28. Viren in der Datenverarbeitung 80
29. Autobahnmaut 81
29.1 Feldversuch auf der A555 82
29.1.1 Gebührenerhebung 82
29.1.2 Kontrolle 82
29.2 Datenschutzrechtliche Anforderungen 82
29.3 Präsentation des Feldversuchs 84
29.4 Weiteres Vorgehen 84

30. Bilanz 84
30.1 EU-Richtlinie zum Datenschutz 84
30.2 Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Hessen 85
30.3 Datenschutz bei den Staatsanwaltschaften 85
30.4 Reform der Strafprozeßordnung 85
30.5 Einsicht in Vereinsregisterakten 86
30.6 Arbeitsgruppe Korruptionsbekämpfung 86
30.7 Neuer landeseinheitlicher Personalbogen 87
31. Materialien 87
31.1 Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam zur Informationsverarbeitung im Strafverfahren 87
31.2 Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam zu Chipkarten im Gesundheitswesen 88
31.3 Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam zum Abbau des Sozialdatenschutzes. 89
31.4 Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam zum Ausländerzentralregistergesetz 90
31.5 Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 9./10. März 1994 in Potsdam zum Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz) und zu der dafür erforderlichen Änderung des Grundgesetzes 91
31.6 Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam zu den datenschutzrechtlichen Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL) 91
31.7 Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Postdam zu fehlenden bereichsspezifischen gesetzlichen Regelungen bei der Justiz 92
31.8 Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Postdam zu Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten 92
31.9 Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam über Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen 92
31.10 Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 in Potsdam zum geänderten Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen 93
31.11 Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1994 (Potsdam) zum Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik . 94

KERNPUNKTE

1. Die Strafprozeßordnung enthält jetzt Regelungen, nach denen bundesweit sämtliche Ermittlungsverfahren in ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister einzutragen sind. Aufzunehmen und damit bundesweit abrufbar sind u.a. die Personendaten und Identifikationsmerkmale eines jeden Beschuldigten (Ziff. 3.1).

2. Der Umstand, daß in Hessen im Gegensatz zu anderen Bundesländern eine Einsichtnahme in Grundbücher und Grundakten nicht protokolliert wird, macht eine datenschutzrechtliche Prüfung der Grundbuchämter nahezu unmöglich (Ziff. 3.3).

3. Der Einsatz von maschinenlesbaren Patientenkarten darf nicht zu einem Zwang zur pauschalen Angabe von Patientendaten führen. Die Karten sind so zu gestalten, daß der Betroffene von Fall zu Fall den Zugriff auf bestimmte Daten beschränken kann (Ziff. 5.3).

4. Will ein Patient sein Recht auf Einsicht in seine Krankenakte wahrnehmen, so braucht er kein berechtigtes Interesse an der Einsicht darlegen. Das Krankenhaus hat dem Patienten die Akte unverzüglich und vollständig zur Verfügung zu stellen (Ziff. 5.4).

5. Die neuen Vorschriften des Hessischen Beamtengesetzes über die Führung und Aufbewahrung von Personalakten wurden von den Verwaltungen bislang nur teilweise umgesetzt (Ziff. 6).

6. Beim Datenschutz an den hessischen Schulen gibt es erhebliche Defizite. Datenschutzrechtliche Vorschriften werden nicht beachtet beim Einsatz privater PC für schulische Zwecke, beim Einsatz dienstlicher PC und auch bei der Aufbewahrung und Archivierung schulischer Unterlagen (Ziff. 8).

7. Eine hessische Kommune zeichnete in ihrer zentralen Telefonvermittlungsstelle den Inhalt sämtlicher ankommender Telefongespräche automatisch und deshalb rechtswidrig auf (Ziff. 11.2).

8. Führungszeugnisse zur Vorlage bei Behörden werden nicht den Antragstellern ausgehändigt, sondern den jeweiligen Behörden unmittelbar übersandt. Enthält das Führungszeugnis Eintragungen, so hat der Betroffene das Recht, das Führungszeugnis vorher einzusehen. Häufig versäumen es die Meldebehörden, die Antragsteller auf diese Möglichkeit hinzuweisen (Ziff. 12.2).

9. Mit dem neuen Umweltinformationsgesetz des Bundes hat jeder Anspruch auf freien Zugang zu Informationen über die Umwelt, die bei einer Behörde vorhanden sind. Allerdings bestehen bei der Anwendung dieses Gesetzes vielfach Unsicherheiten bei den Behörden, da durch die Herausgabe der geforderten Umweltinformationen Vorschriften des Datenschutzes oder des Schutzes von Geschäftsgeheimnissen verletzt werden können (Ziff. 13.2).

10. Die hessische Polizei hält beim Einsatz von V-Personen, verdeckten Ermittlern sowie technischen Mitteln die gesetzlichen Vorgaben strikt ein. Allerdings bestehen Zweifel an der Effektivität der neuen Methoden (Ziff. 18.1).

11. Sparkassen kopierten rechtswidrig Pässe und Personalausweise ihrer Kunden unter Berufung auf das Geldwäschegesetz (Ziff. 21.).

12. Zur Berechnung einer Autobahnmaut werden z.Zt. verschiedene Systeme erprobt. Bei der Entscheidung für ein bestimmtes Verfahren wird darauf zu achten sein, daß erhobene personenbezogene Daten zur Erstellung von Bewegungsprofilen einzelner oder beliebig vieler Bürger oder zur Fahrtroutenverfolgung nicht genutzt werden können (Ziff. 29).

1. Vorwort

Im Jahre 1995 ist die gesetzliche Einrichtung des Datenschutzes ein viertel Jahrhundert alt; 1970 ist das Hessische Datenschutzgesetz in Kraft getreten – weltweit das erste. Das Jahr 1995 wird deshalb Anlaß geben, sich der Entwicklung des Datenschutzes, seiner Gegenwart und seiner Perspektiven zu vergewissern. Nicht nur die Symbolik der Zeit legt solche Vergewisserung nahe; auch die technologischen und die gesellschaftlichen Entwicklungen, die für den Datenschutz bedeutsam sind, fordern neue Konzeptionen.

Diese Entwicklungen zeichnen sich auch in meinem Tätigkeitsbericht über das Jahr 1994 ab.

Das "Forum Datenschutz" hat sich im Jahr 1994 wiederum mit einem allgemeinen und aktuellen Problem befaßt, welches mit dem Recht auf informationelle Selbstbestimmung in Zusammenhang steht. Es ging diesmal um den Datenschutz für Ausländer. Die konzentrierten Auseinandersetzungen auf dem Podium und mit dem Publikum haben vor allem dies gezeigt: Die Garantie von Menschenrechten für Ausländer ist um so besser, je grundsätzlicher die gesetzlichen Verbürgungen sind; sie ist um so schlechter, je konkreter sich diese Verbürgungen in Gesetze, Verordnungen und in den Alltag des Rechts auf Datenschutz verlängern. Und es geht nicht nur um rechtliche Ausstattung: Die Ausländer selbst sind viel weniger als die Deutschen bereit oder imstande, Verletzungen ihrer Rechte im Einzelfall auch zu rügen. Das Forum Datenschutz 1994 hatte also nicht nur das Datenschutzrecht und seine Anwendung im Visier; es ging ebenfalls darum, auf dieses Recht, seine Bedeutung für die betroffenen Menschen und seine Anwendung in der Alltagspraxis öffentlich aufmerksam zu machen.

Auch sonst scheinen mir Kampf und Werben um gesetzliche Einrichtungen des Datenschutzes nicht mehr im Zentrum der Aufmerksamkeit stehen zu müssen. Es wird zwar natürlich auch weiterhin darum gehen, bereichsspezifische Regelungen zu finden, welche dem Recht auf informationelle Selbstbestimmung konkret und sensibel für spezifische Handlungsfelder der öffentlichen Verwaltung Rechnung tragen. Daneben aber werden zwei Dinge immer wichtiger: die Überprüfung der Alltagspraxis und die Beobachtung neuer Entwicklungen.

Wir haben im Jahre 1994 große Anstrengungen unternommen, um ein verläßliches Bild von der konkreten Umsetzung datenschutzrechtlicher Regelungen im Alltag zu gewinnen. Wir haben – teilweise recht umfangreiche – Prüfungen veranstaltet, etwa bei Einbürgerungsbehörden, in der Personalverwaltung, bei Kommunen, bei der Polizei und in Kliniken. Natürlich haben wir dabei Fehler und Mißstände entdeckt; sie sind in diesem Tätigkeitsbericht aufgeführt. Im großen und ganzen aber kann man mit den Entwicklungen der Alltagspraxis zufrieden sein. Wir werden diese Prüfungen vor allem dort, wo neue rechtliche Regelungen ergangen sind, fortsetzen.

Anlaß zu besonderer Aufmerksamkeit gibt es in Bereichen, für die ich nicht oder nur zu einem Teil zuständig bin. Es ist nicht mehr nur der Staat mit seinen Behörden, welcher als der bedrohliche Leviathan gegenüber den bürgerlichen Freiheitsrechten auftritt. Es ist sogar bisweilen eher so, daß sich die Hoffnungen auf Sicherung solcher Freiheitsrechte an den Staat richten. In diese Situation kommen wir vor allem durch die rasanten Entwicklungen der Informations- und Kommunikationstechnologie, durch die Tendenzen zu einer Privatisierung und Deregulierung und durch die Perspektiven einer wirtschaftlich erschwinglichen und gleichwohl hochkomplexen Datenverarbeitung.

Der Tätigkeitsbericht 1994 belegt diese Entwicklungen vor allem an drei Bereichen: der Gesundheitskarte (Ziff. 5.3), der Entwicklung der Telekom (Ziff. 21) sowie den Bestrebungen, intelligente Überwachungssysteme im Straßenverkehr einzurichten (Ziff. 29). Das ist natürlich nur ein Ausschnitt, welcher mit denjenigen Feldern in Berührung steht, auf denen ich zu arbeiten habe: der behördlichen Datenverarbeitung.

Nach 25 Jahren Datenschutz müssen wir an neuen Konzeptionen arbeiten, welche diesen Entwicklungen in Technologie und Wirtschaft Rechnung tragen können. Am 9. Juni wird sich das "Forum Datenschutz 1995" deshalb mit Bestandsaufnahme und Perspektiven des Datenschutzes öffentlich auseinandersetzen.

W.H.

2. Europa

2.1
Schengener Durchführungsübereinkommen

In dem nach dem luxemburgischen Ort des Vertragschlusses benannten "Schengener Abkommen" vom 14. Juni 1985 (GMBl. 1986 S. 79) hatten die Regierungen der Benelux-Staaten, von Frankreich und der Bundesrepublik Deutschland vereinbart, die Kontrollen an den gemeinsamen Landesgrenzen schrittweise abzubauen. Auf der Grundlage dieser Vereinbarung wurde am 19. Juni 1990 ein Staatsvertrag, das sog. "Schengener Durchführungsübereinkommen" ausgehandelt, in dem eine engere Zusammenarbeit zwischen den Behörden der beteiligten Staaten vorgesehen ist. Zu dem Entwurf des Schengener Durchführungsübereinkommens hatte ich mich im 18. Tätigkeitsbericht, Ziff. 3.1 geäußert (vgl. auch die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sowie der Datenschutzkommission Rheinland-Pfalz vom 26. und 27. Oktober 1989 zum Entwurf eines Schengener Zusatzübereinkommens über den schrittweisen Abbau der Grenzkontrollen, ebenda Ziff. 19.1.8). Zwischenzeitlich sind dem Schengener Durchführungsübereinkommen über die fünf Vertragsstaaten hinaus Italien, Portugal, Spanien und Griechenland beigetreten.

Das Schengener Durchführungsübereinkommen wurde am 15. Juli 1993 vom Deutschen Bundestag ratifiziert. Wesentliche Passagen sind – anders als es der Wortlaut vermuten läßt – noch nicht in Kraft getreten, sondern bedürfen eines Beschlusses der zuständigen Minister der Vertragsstaaten. Dieser Beschluß vom 22. Dezember 1994

sieht vor, daß das gesamte Schengener Durchführungsübereinkommen für die Vertragsstaaten – mit Ausnahme von Griechenland und Italien – zum 26. März 1995 in Kraft gesetzt wird. Zu diesem Zeitpunkt soll auch das sog. "Schengener Informationssystem" funktionsfähig sein.

2.1.1
Zum Inhalt des Schengener Durchführungsübereinkommens

Als Ausgleich für den mit dem Wegfall der Kontrollen an den gemeinsamen Grenzen befürchteten Sicherheitsverlust hielten die Vertragsparteien kompensierende Maßnahmen für erforderlich. Diese bilden den wesentlichen Gegenstand des Schengener Durchführungsübereinkommens. Vorgesehen sind unter anderem verstärkte Kontrollen an den Außengrenzen, gemeinsame Bedingungen für die Visaerteilung, Bestimmungen über die Behandlung von Asylanträgen. Ein Schwerpunkt liegt bei der Zusammenarbeit der Polizeibehörden bei Vorbeugung und Bekämpfung von Verbrechen. Weitere Bestimmungen betreffen die Vollstreckungszusammenarbeit in Strafsachen und die Bekämpfung des Handels mit Betäubungsmitteln und Feuerwaffen.

2.1.2
Schengener Informationssystem

Als Kernstück betrachten die Vertragsparteien das im Schengener Durchführungsübereinkommen vorgesehene "Schengener Informationssystem" (SIS). Es handelt sich dabei um ein polizeiliches Fahndungssystem, mittels dessen in allen Schengen-Vertragsstaaten gleichzeitig nach bestimmten Personen oder Gegenständen gesucht werden kann. Technisch gesehen besteht das Schengener Informationssystem aus einem zentralen System (CSIS) in Straßburg und den nationalen Teilen (NSIS) der einzelnen Vertragsstaaten. In der Bundesrepublik Deutschland befindet sich das NSIS beim Bundeskriminalamt. Die Identität der Datenbestände von CSIS und der NSIS wird durch ständigen Abgleich gewährleistet. Die NSIS können nicht untereinander, sondern nur über CSIS Informationen austauschen. Der Umfang der im Schengener Informationssystem gespeicherten Daten ist abschließend festgelegt; gespeichert werden hauptsächlich Identifizierungsmerkmale (u.a. Name, Geburtsort, Geschlecht, Staatsangehörigkeit, besondere physische Merkmale und der Hinweis, ob die Person bewaffnet oder gewalttätig ist).

Bei folgenden Sachverhalten kommt eine Speicherung im Schengener Informationssystem in Betracht:

- Personen, die zur Festnahme oder Auslieferung ausgeschrieben werden,
- Personen, die nicht Staatsangehörige der Schengen-Vertragsstaaten sind (Drittausländer) und zur Einreiseverweigerung ausgeschrieben werden,
- vermißte Personen, Zeugen und Verurteilte, die eine Haftstrafe antreten sollen,
- Personen oder Fahrzeuge, die der polizeilichen Beobachtung oder gezielten Kontrolle unterliegen,
- Gegenstände, die beschlagnahmt werden oder als Beweismittel im Strafverfahren dienen.

Die Ausschreibung richtet sich grundsätzlich nach dem Recht der ausschreibenden Vertragspartei. Da die entsprechenden Gesetze in den Schengen-Vertragsstaaten unterschiedlich sind, kann es durchaus dazu kommen, daß ein Ersuchen an ein Land gerichtet wird, für das nach seinem nationalen Recht die materiellen Voraussetzungen für das Ersuchen nicht vorliegen. Das Schengener Durchführungsübereinkommen sieht Verfahrensregeln vor, nach denen in einem derartigen Fall dem nationalen Recht Geltung verschafft werden kann. Bei der Ausschreibung zur Einreiseverweigerung von Drittausländern ist eine Abweichung allerdings nur in beschränktem Umfang möglich. Bleiben auch noch eine Reihe von Fragen im Zusammenhang mit dem Schengener Informationssystem offen, so sind einige Datenschutzregelungen doch als positiv hervorzuheben:

- Die Vertragsparteien verpflichten sich, bis zum Inkrafttreten des Vertrags, einen Datenschutzstandard zu verwirklichen, der zumindest dem Übereinkommen des Europarats über den Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten vom 28. Januar 1981 entspricht.
- Jede Vertragspartei muß eine unabhängige Kontrollinstanz besitzen – in der Bundesrepublik Deutschland der Bundesbeauftragte für den Datenschutz –, deren Aufgabe darin besteht, den nationalen Datenbestand (NSIS) zu überwachen.
- Zur Kontrolle des zentralen Datenbestands (CSIS) in Straßburg und zur Behandlung übergreifender datenschutzrechtlicher Fragen wurde eine gemeinsame – bisher provisorische – Kontrollinstanz eingerichtet. Für die Bundesrepublik Deutschland nehmen der Bundesbeauftragte für den Datenschutz und bis auf weiteres der Hessische Datenschutzbeauftragte als Vertreter der Landesdatenschutzbeauftragten an den Sitzungen teil.
- Jeder Bürger kann in jedem Schengen-Vertragsstaat sein Auskunftsrecht geltend machen. Das Gleiche gilt für die Rechte auf Berichtigung unrichtiger, die Löschung unrechtmäßig gespeicherter Daten und die Geltendmachung von Schadensersatz. Diese Rechte können auch im Wege der Klage im Hoheitsgebiet jeder Vertragspartei durchgesetzt werden.

2.2
Europol

In dem Vertrag über die Europäische Union vom 7. Februar 1992 wurde die Schaffung eines Europäischen Polizeiamts (Europol) vereinbart. Der Entwurf eines Übereinkommens der Mitgliedstaaten der Europäischen Union über die Errichtung eines Europäischen Polizeiamts (Rats-Dok. 8074/1/94) weist Europol folgende Aufgaben zu:

- Informationen und Kenntnisse zu sammeln, zusammenzustellen, zu analysieren und auszuwerten
- über die nationalen Stellen die zuständigen Behörden der Mitgliedstaaten hinsichtlich der sie betreffenden Informationen und der in Erfahrung gebrachten Zusammenhänge von Straftaten unverzüglich zu unterrichten
- Ermittlungen in den Mitgliedstaaten durch die Übermittlung aller sachdienlichen Informationen an die nationalen Stellen zu unterstützen
- eine automatisiert geführte Sammlung von Informationsbeständen zu unterhalten, die nationale und neue Daten enthalten.

Aus der Aufgabenbeschreibung ergibt sich bereits, daß Europol in jedem Mitgliedstaat mit einer nationalen Stelle – in Deutschland dem Bundeskriminalamt – verbunden werden soll. Die nationale Stelle soll die einzige Verbindungsstelle zwischen Europol und den zuständigen Behörden der Mitgliedstaaten sein. Die Beziehungen zwischen der nationalen Stelle und den zuständigen Behörden unterliegen dem jeweiligen nationalen Recht. Jede nationale Stelle entsendet einen Verbindungsbeamten zu Europol, der ebenfalls dem nationalen Recht unterliegt.

Zur Erfüllung seiner Aufgaben errichtet und unterhält Europol ein automatisiert geführtes Informationssystem. Dieses Informationssystem besteht aus einer zentralen Datenbank, in welche die Mitgliedstaaten und Europol Daten unmittelbar eingeben und aus der sie Daten unmittelbar abrufen können. Daneben sollen sonstige Dateien für Zwecke der Analyse und Auswertung eingerichtet werden. Eine nationale und eine unabhängige internationale Kontrollinstanz sollen die Einhaltung des Datenschutzes bei Europol und den Mitgliedstaaten kontrollieren können.

In diesem Zusammenhang ist wesentlich, daß das Übereinkommen mit der verfassungsrechtlichen Kompetenzverteilung zwischen Bund und Ländern für die Polizei in Einklang steht. Soweit die Länderpolizeibehörden Daten erheben, muß auch die Verantwortung für die Datenverarbeitung weiterhin bei den Ländern liegen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in diesem Sinne auf ihrer 48. Sitzung einen Beschluß zu den datenschutzrechtlichen Anforderungen an das Übereinkommen gefaßt (vgl. Ziff. 31.6).

3. Justiz

3.1
Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Mit dem Verbrechensbekämpfungsgesetz vom 28. Oktober 1994 (BGBl. I S. 3186) hat der Gesetzgeber die Strafprozeßordnung um ein "Achtes Buch" erweitert, das Regelungen für ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister enthält, in das bundesweit sämtliche Ermittlungsverfahren einzutragen sind. Das Register wird beim Bundeszentralregister geführt; aufzunehmen sind neben Personendaten und Identifikationsmerkmalen des Betroffenen Angaben über die zuständige Stelle und das Aktenzeichen, die Tatzeiten, Tatvorwürfe, die Einleitung des Verfahrens sowie die Verfahrenserledigung bei der Staatsanwaltschaft und bei Gericht.

Die Staatsanwaltschaften teilen der Registerbehörde die einzutragenden Daten mit. Die Daten sind laufend zu aktualisieren, wofür die zuständige Staatsanwaltschaft die Verantwortung trägt. Auskünfte dürfen nur an Strafverfolgungsbehörden für Zwecke eines Strafverfahrens erteilt werden. Statt der Erteilung von Einzelauskünften ist auch die Einrichtung eines automatisierten Verfahrens zulässig, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, wenn diese Form der Datenübermittlung unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen wegen der Vielzahl der Übermittlungen oder wegen ihrer besonderen Eilbedürftigkeit angemessen ist und wenn gewährleistet ist, daß die Daten gegenüber unbefugten Dritten bei der Übermittlung wirksam geschützt werden.

Mit dem Verfahrensregister soll die Ermittlung überörtlich agierender Täter und Mehrfachtäter erleichtert und die Prüfung der Haftvoraussetzungen, insbesondere wegen Wiederholungsgefahr, auf eine gesicherte Grundlage gestellt werden. Auch soll das Register dazu beitragen, Doppelverfahren zu vermeiden, Sammelverfahren zu bilden, unwesentliche Taten oder Tatteile frühzeitig auszuscheiden und zuverlässige Grundlagen für Verfahrenseinstellungen nach den §§ 153ff. StPO zu schaffen.

Dies sind sicher verständliche Anliegen, fraglich ist jedoch, ob ihnen mit dem vorgesehenen Register tatsächlich ausreichend gedient ist.

Das Verfahrensregister verursacht auf Dauer einen erheblichen Aufwand für die Staatsanwaltschaften. Die Frage drängt sich auf, wie die Justiz mit ihrem "notleidenden mittleren Dienst" (so die Stellungnahme der Landesregierung betreffend den 22. Tätigkeitsbericht, LTDrucks. 13/8513, S. 14) die laufende Aktualisierung der Daten gewährleisten will. Die Folge verzögerter Mitteilungen wäre zum Beispiel, daß unzulässige Speicherungen nicht unverzüglich berichtigt bzw. gelöscht und folglich zum Nachteil des Betroffenen weiterverwertet würden.

Der Aufwand für die Staatsanwaltschaften wäre um einiges geringer, hätte der Gesetzgeber sich bei der gesetzlichen Regelung auf den Zweck des Registers besonnen und den Umfang der einzutragenen Verfahren entsprechend beschränkt. Ich vermag nicht nachzuvollziehen, weshalb beispielsweise Verfahren, die aufgrund gänzlich unbegründeter Strafanzeigen eingeleitet und alsbald wieder eingestellt wurden, oder etwa Fahrlässigkeitsdelikte und Bagatelldelikte in einem bundesweiten System verfügbar sein müssen. Hier wären gesetzliche Kriterien festzulegen, die eine Abgrenzung der relevanten von den übrigen Verfahren ermöglichen.

(Zur Informationsverarbeitung im Strafverfahren vgl. auch den Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994, hier Ziff. 31.1.)

3.2
Benachrichtigung gemeinnütziger Einrichtungen bei Verfahrenseinstellungen nach § 153a StPO

Wird ein Strafverfahren nach § 153a StPO eingestellt, erfolgt dies oft mit der Auflage, daß der Beschuldigte einen Geldbetrag zugunsten einer gemeinnützigen Einrichtung zahlt. Damit die gemeinnützige Einrichtung den Eingang der Zahlung überwachen kann, muß sie über die Auflage informiert werden. Auch muß sie als Empfängerin der Geldbuße darüber informiert werden, daß dem Einzahler keine Spendenbescheinigung ausgestellt werden darf, denn die Erfüllung einer Geldauflage ist keine steuerbegünstigte Ausgabe i. S. v. § 10b EStG.

Es ist gängige Praxis, daß die Staatsanwaltschaften und Gerichte dazu den gemeinnützigen Einrichtungen personenbezogene Daten der Beschuldigten übermitteln. Diese Praxis ist datenschutzrechtlich bedenklich. Eine einfache Lösung, die Übermittlung personenbezogener Daten zu vermeiden, wäre, die Geldbeträge auf Konten der Justizkasse zu vereinnahmen, um sie von dort an die gemeinnützigen Empfänger entsprechend weiterzuleiten. Alternativ wäre es möglich, Überweisungsträger zu verwenden, bei denen der Beleg für die empfangende gemeinnützige Organisation keine personenbezogenen Daten, sondern z. B. nur ein Codewort enthält. Die Überwachung des Zahlungseingangs durch die gemeinnützige Organisation wäre dann anhand von anonymisierten Listen möglich. Auch bei dieser Lösung müßten dem privaten Empfänger der Geldbuße keine personenbezogenen Daten der Beschuldigten übermittelt werden, denn auf dem Überweisungsträger kann auf deren Angabe verzichtet werden.

§ 153a StPO regelt zwar die Einstellung von Strafverfahren nach der Erfüllung von Geldauflagen, die Vorschrift ist jedoch keine ausreichende bereichsspezifische Regelung für die Übermittlung personenbezogener Daten an nichtöffentliche Stellen. Rechtsgrundlage hierfür sind die §§ 11 und 16 HDSG. § 16 HDSG erlaubt die Übermittlung personenbezogener Daten an Personen oder Stellen außerhalb des öffentlichen Bereichs, wenn der Empfänger ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft macht und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können. Letzteres ist hier der Fall. Mit der Datenübermittlung erfährt die gemeinnützige Organisation, daß gegen die Beschuldigten ein Verfahren anhängig ist und wenigstens "zureichende tatsächliche Anhaltspunkte" für seine Schuld vorliegen. Die Datenübermittlung kann daher nur unter den Voraussetzungen des § 11 HDSG getätigt werden, d. h., sie muß zur rechtmäßigen Erfüllung der Aufgaben von Staatsanwaltschaft oder Gericht und für den jeweils damit verbundenen Zweck – also der Überwachung des Zahlungseingangs – erforderlich sein. Da es aber die dargestellten anderen Möglichkeiten gibt, den Zweck zu erfüllen, fehlt es an der Erforderlichkeit.

Das Bundesministerium der Justiz hat vorgeschlagen, mit einer Änderung der Strafprozeßordnung eine gesetzliche Grundlage für die Übermittlung personenbezogener Daten an gemeinnützige Einrichtungen zu schaffen. Es hat folgenden Formulierungsvorschlag zur Diskussion gestellt:

"An gemeinnützige Einrichtungen dürfen personenbezogene Informationen aus Strafverfahren übermittelt werden, soweit dies zum Nachweis der Erfüllung von Auflagen oder Weisungen erforderlich ist. Informationen zu der zugrunde liegenden Straftat dürfen nicht mitgeteilt werden. Die personenbezogenen Informationen dürfen nur zum Zweck des Nachweises der Erfüllung von Auflagen oder Weisungen verwendet werden; hierauf ist die gemeinnützige Einrichtung hinzuweisen. Die personenbezogenen Informationen sind gegen unbefugte Kenntnisnahme zu schützen und nach Erfüllung der Auflage oder Weisung oder nach Ablauf der Frist zur Erfüllung der Auflage oder Weisung unverzüglich zu vernichten."

Das Problem auf diese Weise, sozusagen "auf dem Rücken der Betroffenen", zu lösen, halte ich für problematisch. Immerhin sind die anderen aufgezeichneten Lösungsmöglichkeiten nicht unpraktikabel. So wurde beispielsweise in Bremen in Abstimmung mit dem Landesbeauftragten für den Datenschutz die Regelung getroffen, daß die Zahlungen an die Gerichte bzw. an die Stadtkasse erfolgen und von dort die summenmäßig zusammengefaßten Beträge an die gemeinnützigen Organisationen abfließen. Es darf auch nicht außer acht gelassen werden, daß die Datenübermittlung von den Betroffenen als zusätzliche Sanktion empfunden werden muß, die über das eigentliche vom Gesetzgeber verfolgte Ziel, den Betroffenen ein finanzielles Opfer aufzuerlegen, hinausgeht, die Zahlungsauflage soll nicht gleichzeitig eine "Prangerfunktion" haben.

Auch in Hessen werden die gemeinnützigen Einrichtungen von Name und Anschrift des Beschuldigten, sowie Aktenzeichen, Höhe und Fälligkeit der Geldauflage informiert. Ein Betroffener hatte deshalb bei der Staatsanwaltschaft Darmstadt Dienstaufsichtsbeschwerde eingelegt. Die Staatsanwaltschaft wies die Beschwerde ab. Sie war der Ansicht, daß die Übermittlung personenbezogener Daten an die gemeinnützige Organisation erforderlich sei. Bei ihrer Prüfung wurde sie aber darauf aufmerksam, daß die Information an den Empfänger mittels einer Durchschrift der Einstellungsverfügung erfolgte. Der verwendete Vordruck enthält neben den bereits genannten personenbezogenen Daten des Betroffenen auch noch die Angabe des strafrechtlichen Vorwurfs. Dazu sah allerdings auch sie kein Erfordernis und regte bei der Generalstaatsanwaltschaft die Änderung der landesweit gebräuchlichen Formulare an. Unabhängig von der danach noch verbleibenden problematischen Datenübermittlung habe ich diesen Vorschlag gegenüber dem Justizministerium unterstützt. Eine Umsetzung ist noch nicht erfolgt. Vorab hat die Dienststellenleitung der Staatsanwaltschaft Darmstadt die Dezernate aufgefordert, bei künftigen Datenübermittlungen an gemeinnützige Einrichtungen keine Angaben mehr über den strafrechtlichen Vorwurf zu übermitteln.

3.3
Datenschutz bei den Grundbuchämtern

Im Lauf des Berichtszeitraums habe ich verschiedene Grundbuchämter aufgesucht, um zu überprüfen, unter welchen Voraussetzungen die Ämter Einsicht in das Grundbuch bzw. die Grundakten gewähren und Grundbuchauszüge erteilen.

Nach § 12 GBO ist die Einsicht des Grundbuchs jedem gestattet, der ein berechtigtes Interesse darlegt. Das gleiche gilt für die Urkunden, auf die im Grundbuch zur Ergänzung einer Eintragung Bezug genommen ist, sowie für die noch nicht erledigten Eintragungsanträge. Soweit die Einsicht des Grundbuchs gestattet ist, kann eine Abschrift gefordert werden, die auf Verlangen zu beglaubigen ist.

In § 43 GBVerf. ist weiterhin vorgesehen, daß Beauftragte inländischer öffentlicher Behörden befugt sind, das Grundbuch einzusehen und eine Abschrift zu verlangen, ohne daß es der Darlegung eines berechtigten Interesses bedarf. Dasselbe gilt für Notare sowie Rechtsanwälte, die im nachgewiesenen Auftrag eines Notars das Grundbuch einsehen wollen.

Nach § 46 GBVerf. ist bei der Darlegung eines berechtigten Interesses – bei Einsicht durch öffentliche Behörden und Notare auch ohne eine solche Darlegung – die Einsicht in Grundakten auch insoweit gestattet, als es sich nicht um die oben erwähnten Urkunden handelt. Unter entsprechenden Voraussetzungen kann auch eine Abschrift gefordert werden.

Das Grundbuchamt muß sich also zunächst die Frage stellen, ob der Antragsteller ein berechtigtes Interesse an der Einsichtnahme hat. Ein berechtigtes Interesse ist ein nach vernünftiger Erwägung durch die Sachlage gerechtfertigtes Interesse, das rechtlicher, wirtschaftlicher oder ideeller Natur sein kann. Für die Einsicht des Grundbuchs und der Grundakten sind also sachliche Gründe darzulegen, eine Einsichtnahme aus bloßer Neugier soll ausgeschlossen sein; datenschutzrechtlich gesehen wäre dies ein unverhältnismäßiger Eingriff in das Persönlichkeitsrecht des Betroffenen. Das Grundbuchamt ist daher verpflichtet, die Darlegung des berechtigten Interesses in jedem Einzelfall genau zu prüfen. Hierdurch sollen Einsichtnahmen verhindert werden, die das Recht auf informationelle Selbstbestimmung des Betroffenen verletzen, weil sie unbefugten Dritten einen Einblick in seine Rechts- und Vermögensverhältnisse gewähren. Denn der Antragsteller kann sehr persönliche Informationen über den Betroffenen erlangen, angefangen von Belastungen des Grundstücks über Ehescheidungsurteile, Testamente, Erbverträge usw.

Das Einsichtsrecht bei Darlegung eines berechtigten Interesses geht nicht weiter als das Interesse sachlich reicht. Es sind folglich Fälle denkbar, in denen beispielsweise ein Interesse nur an der Einsicht in einzelne Abteilungen des Grundbuchs besteht. So wird es häufig vorkommen, daß der Antragsteller nur darauf angewiesen ist, die Eintragungen über den Eigentümer zur Kenntnis zu nehmen, während die Kenntnis der Eintragungen in Abteilung II und III für ihn nicht notwendig ist.

Nun hatte ich bei meiner Prüfung folgendes Problem: In Hessen wird – im Gegensatz zu Berlin und Schleswig-Holstein – weder protokolliert, wer wann Einsicht genommen hat, noch was der Grund für die Einsichtnahme war. Eine solche Dokumentation wäre jedoch zum Zweck der Nachprüfung durch den Grundstückseigentümer und durch mich unverzichtbar. Ich hatte mich daher bereits im Jahr 1992 an das Hessische Ministerium der Justiz gewandt und angeregt, mittels Erlaß die Grundbuchämter zu verpflichten, Einsichtnahmen in Grundbücher und Grundakten zu protokollieren und zumindest Name, Vorname und Anschrift des Antragstellers sowie Datum und Grund der Einsichtnahme festzuhalten. Das Justizministerium sah allerdings keine Notwendigkeit für eine solche Protokollierung, u.a. mit der fast zynisch anmutenden Begründung, der Grundstückseigentümer habe ohnehin kein Beschwerderecht gegen die Einsichtnahme.

Also blieb mir nur die Möglichkeit, in Gesprächen mit den Urkundsbeamten der Geschäftsstelle und den Rechtspflegern zu ermitteln, wie die Praxis in den einzelnen Ämtern aussieht. Dabei konnte ich feststellen, daß an die Darlegung eines berechtigten Interesses i.d.R. überall dieselben Anforderungen gestellt werden, die Beschränkung des Einsichtsrechts auf Teile des Grundbuchs bzw. der Grundakte in der Handhabung allerdings schon unterschiedlich ist. Das kann sich dann so auswirken, daß ein Rechtsanwalt, der für eine Mietrechtsstreitigkeit Grundbucheinsicht begehrt, bei dem einen Grundbuchamt nur in das Bestandsverzeichnis und Abteilung I einsehen darf, bei dem anderen Grundbuchamt aber ohne weiteres Einsicht in das gesamte Grundbuch erhält.

Ich habe daher beim Hessischen Ministerium der Justiz angeregt, durch eine gesetzesinterpretierende Verwaltungsvorschrift auf eine gleichmäßige Behandlung der Fälle i. S. d. von der Rechtsprechung entwickelten Grundsätze hinzuwirken.

3.4
Schuldnerverzeichnisse

Hat eine Pfändung nicht zur vollständigen Befriedigung des Gläubigers geführt, ist der Schuldner auf Antrag des Gläubigers verpflichtet, ein Verzeichnis seines Vermögens vorzulegen. Zu Protokoll des Gerichts hat er an Eides Statt zu versichern, daß er die von ihm verlangten Angaben nach bestem Wissen und Gewissen richtig und vollständig gemacht hat. Verweigert der Schuldner die Abgabe der eidesstattlichen Versicherung oder erscheint er nicht zu dem zur Abgabe der eidesstattlichen Versicherung anberaumten Termin vor Gericht, kann das Gericht die Haft anordnen.

Die Gerichte führen ein Verzeichnis der Personen (Schuldnerverzeichnis), welche die eidesstattliche Versicherung abgegeben haben oder gegen welche die Haft angeordnet wurde. Über das Bestehen oder Nichtbestehen einer Eintragung im Schuldnerverzeichnis ist jedermann auf Antrag Auskunft zu erteilen (§ 915 Abs. 3 ZPO alt).

Nach Ablauf bestimmter Fristen wird ein Eintrag im Schuldnerverzeichnis gelöscht. Weist der Schuldner nach, daß der Gläubiger befriedigt ist, wird der Eintrag auch vorzeitig gelöscht.

Nachdem sein Eintrag im Schuldnerverzeichnis über die Abgabe der eidesstattlichen Versicherung gelöscht war, versicherte sich ein Betroffner darüber, daß auch die Schutzgemeinschaft für allgemeine Kreditsicherung (Schufa) – eine Gemeinschaftseinrichtung der kreditgebenden deutschen Wirtschaft – die Information getilgt hatte. Trotzdem

wurde er bei Verhandlungen über einen Vertragsabschluß von seinem Geschäftspartner damit konfrontiert, daß er schon einmal eine eidesstattliche Versicherung habe abgeben müssen. Sein Geschäftspartner, so erklärte ihm dieser, habe die Information von einer Auskunftei erlangt. Nun fragte er selbst bei mehreren Wirtschaftsauskunfteien nach und erhielt von drei Institutionen die Auskunft, daß sie über die Information, er habe eine eidesstattliche Versicherung abgegeben, verfügen. Offensichtlich hatten die Auskunfteien zwar von der Abgabe der eidesstattlichen Versicherung erfahren, aber nicht von der Löschung des Eintrags.

Meine Einsichtnahme in die Unterlagen des Amtsgerichts ergab, daß Dritte über Eintragungen in der Schuldnerkartei mittels Übersendung von monatlichen Sammellisten Nachricht erhalten. Dies ist zwar mit § 915 Abs. 4 ZPO (alt) i.V.m. der aufgrund dieser Vorschrift ergangenen Bestimmung (Allgemeine Vorschriften über die Erteilung und die Einsichtnahme von Abschriften oder Auszügen aus den Schuldnerverzeichnissen vom 1. August 1955, BAnz. 156) unter bestimmten Voraussetzungen zulässig. Die förmlichen Voraussetzungen – u.a. muß der Präsident des Amts- bzw. Landgerichts die Erteilung von Abschriften förmlich genehmigen, die Empfänger der Abschriften müssen sich verpflichten, vorzeitige Löschungen zu berücksichtigen usw. – waren erfüllt. Eine Genehmigung zum Empfang von Nachrichten über Eintragungen im Schuldnerverzeichnis war beispielsweise der örtlichen Industrie- und Handelskammer erteilt. Außerdem erhielt das örtlich zuständige Finanzamt regelmäßig Nachrichten.

Im konkreten Fall konnte ich auch feststellen, daß sowohl dem Finanzamt als auch der Industrie- und Handelskammer eine Nachricht über die vorzeitige Löschung übersandt worden war. Wie die Auskunfteien Kenntnis von der Eintragung erhalten hatten, war nicht festzustellen. Dazu mußte ich den Vorgang an die für die Kontrolle der Einhaltung datenschutzrechtlicher Bestimmungen im nicht-öffentlichen Bereich zuständige Stelle, also das zuständige Regierungspräsidium, abgeben.

Auch wenn die Vorschrift aus dem Jahre 1955 eine Reihe datenschutzrechtlicher Aspekte berücksichtigt, wird sie den neueren Anforderungen an die Bedürfnisse des Datenschutzes und des Rechts auf informationelle Selbstbestimmung nicht gerecht. § 915 Abs. 4 ZPO (alt) schuf lediglich einen Erlaubnistatbestand für das Gericht, Dritten durch Erteilung von Abschriften Daten aus dem Schuldnerverzeichnis zu übermitteln. Im übrigen ließen die Vorschriften eine ausreichend präzise gesetzliche Regelung über die Befugnis zur Erteilung von Abschriften und deren Verarbeitung sowie über Zweckbindung, Löschungspflicht und Kontrollbefugnis vermissen.

Dieses Defizit scheint jetzt weitgehend beseitigt. Durch das Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis vom 15. Juli 1994 (BGBl. I, S. 1566) trat am 1. Januar 1995 eine neue Fassung des § 915 ZPO in Kraft. Außerdem erfährt der gesamte Komplex durch die neuen Vorschriften §§ 915a bis h eine gesetzliche Regelung. Weiterhin wurde durch die "Verordnung über das Schuldnerverzeichnis" vom 15. Dezember 1994 (BGBl. I S. 3822ff.) die aus dem Jahre 1955 stammende Allgemeine Verwaltungsvorschrift abgelöst.

Die neuen Vorschriften enthalten beispielsweise in § 915 Abs. 2 ZPO eine Aufzählung der Zwecke, zu denen personenbezogene Daten aus dem Schuldnerverzeichnis verwendet werden dürfen. Anfrager müssen darlegen, für welchen Zweck sie eine Auskunft benötigen. Unabhängig von einer vorzeitigen Löschung konnten die Betroffenen bisher nach Ablauf von drei Jahren seit dem Ende des Jahres, in dem der Eintrag erfolgte, einen Antrag auf Löschung im Schuldnerverzeichnis stellen, ansonsten erfolgte die Löschung erst nach fünf Jahren. Jetzt erfolgt die Löschung nach drei Jahren, auch ohne besonderen Antrag. Ausführlich regelt die Verordnung das Verfahren der Bewilligung zum Bezug von Abdrucken und Listen aus dem Schuldnerverzeichnis. Auch der letzte Empfänger von Abdrucken und Listen muß Nachricht über vorzeitige Löschungen erhalten. Zur Durchsetzung der Vernichtungs- und Löschungspflichten können Zwangsgelder bis zu einem Betrag von 50.000 DM festgesetzt werden. Daneben kann die Ersatzvornahme angeordnet werden. Detailliert sind die Bedingungen für die Einrichtung automatisierter Abrufverfahren geregelt. Es gibt Protokollpflichten. Werden Tatsachen bekannt, die erkennen lassen, daß abgerufene Daten zweckwidrig verwendet oder in unzulässiger Weise weitergegeben wurden, ist die für die Einhaltung datenschutzrechtlicher Bestimmungen zuständige Aufsichtsbehörde einzuschalten.

Insgesamt wird damit der Umgang mit Daten aus dem Schuldnerverzeichnis auf eine Rechtsgrundlage gestellt, welche den Anforderungen des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz genügt.

4. Finanzen

4.1
Datenschutz bei der Versendung von Lohnsteuerkarten

Das Adressieren, Kuvertieren und Versenden der Lohnsteuerkarten hat seit einiger Zeit eine private Firma für die Stadt Oberursel zum Preis von insgesamt 700,00 DM übernommen. Die Stadt erhielt einen Hinweis, daß nach einer Rundverfügung der Oberfinanzdirektion Frankfurt am Main über die Ausstellung und Übermittlung der Lohnsteuerkarten vom 6. September 1993 für die Finanzämter, Gemeinden und Kommunalen Gebietsrechenzentren in Hessen diese Praxis nicht weitergeführt werden könne. Die Verfügung bestimmt: "Es ist nicht zulässig, die Lohnsteuerkarten durch private Dienstleistungsunternehmen einkuvertieren bzw. versenden zu lassen, da deren Bedienstete nicht verpflichtet sind, das Steuergeheimnis zu wahren".

Das Kommunale Gebietsrechenzentrum Frankfurt am Main erklärte sich gegenüber der Stadt Oberursel bereit, diese Aufgabe künftig zu übernehmen, allerdings zum Preise von insgesamt 2.700,00 DM. Die Stadt Oberursel hatte hinsichtlich der Mehrkosten von 2.000,00 DM für die gleiche Aufgabe Bedenken und bat mich um Prüfung, ob die Änderung der Beauftragung aus der Sicht des Datenschutzes gerechtfertigt und notwendig sei. Auch der Hessische Städtetag unterstützte den Wunsch seiner Mitgliedsstadt.

Nach § 4 Abs. 2 HDSG, der die Datenverarbeitung im Auftrag regelt, würde es ausreichen, wenn sich die beauftragte Firma gegenüber der Stadt vertraglich verpflichtete, die Bestimmungen des Hessischen Datenschutzgesetzes (insbesondere die Geheimnisverpflichtung nach § 9 HDSG) zu beachten und sich der Kontrolle des Hessischen Datenschutzbeauftragen zu unterwerfen. Im vorliegenden Fall gehen jedoch die Vorschriften der Abgabenordnung als sog. "bereichsspezifische Rechtsvorschriften" nach § 3 Abs. 3 HDSG denen des Hessischen Datenschutzgesetzes vor. Danach kommt es darauf an, ob durch die Beauftragung der privaten Firma eine unzulässige "Offenbarung" personenbezogener Daten i.S.d. § 30 AO bewirkt würde.

In mehreren Gesprächen mit dem Hessischen Ministerium der Finanzen konnte eine unbürokratische Lösung gefunden werden, die es ermöglicht, daß die Stadt Oberursel ihre kostensparende Praxis unter bestimmten Voraussetzungen weiterführen kann:

Das Finanzministerium verlangt, daß die Mitarbeiter der beauftragten Firma auf die Einhaltung des Steuergeheimnisses nach der Abgabenordnung verpflichtet werden. Außerdem dürfen von den Firmen keine Freistempler verwendet werden, aus denen der Absender der Firma hervorgeht. Auf Anordnung des Ministeriums wird die Oberfinanzdirektion diese Voraussetzungen in die gegenwärtig überarbeitete Rundverfügung einarbeiten. Das Ministerium betonte, daß auch in verschiedenen anderen Bundesländern bereits so verfahren werde.

In diesem Zusammenhang ist zu beachten, daß bei Beauftragung einer privaten Firma nach § 4 Abs. 2 HDSG diese Beauftragung, die Verpflichtung auf das Datengeheimnis nach § 9 HDSG sowie die Verpflichtung auf das Steuergeheimnis dem Hessischen Datenschutzbeauftragten anzuzeigen ist, damit er seine Kontrollaufgaben wahrnehmen kann.

4.2
Steuernummer im Adreßfeld

Zur Durchführung einer Aktion zur Abfall- und Abwassergebühr verschickte die Stadt Nidderau Fragebögen an Grund- und Hauseigentümer. Die Kuverts waren mit Adressenaufklebern versehen, auf denen über der jeweiligen Anschrift auch die dazugehörige Steuernummer aufgeführt war.

Dies führte zu massiven Beschwerden einzelner Bürger. Es wurde unsorgfältiges Verhalten der Behörden im Umgang mit Daten gerügt und befürchtet, daß nach außen erkennbar werde, wie viele und welche Häuser der jeweilige Adressat besitzt.

Eine Rückfrage bei der Stadt Nidderau ergab, daß die Adressenaufkleber vom Kommunalen Gebietsrechenzentrum Frankfurt erstellt wurden und eine Unterdrückung der Steuernummer datenverarbeitungstechnisch zunächst nicht vorgesehen war. Die Stadtverwaltung benutzte die gelieferten Aufkleber, ohne zu erkennen, daß die Verwendung der Steuernummer im Adreßfeld nicht erforderlich und deshalb datenschutzrechtlich unzulässig war. Daß es sich bei der Steuernummer in Verbindung mit der jeweiligen Anschrift um ein personenbezogenes Datum handelt, ist unbestritten und unbestreitbar.

Entgegen den Befürchtungen einzelner Betroffener gibt die Steuernummer zwar keinen Aufschluß darüber, welchen konkreten Grundbesitz der Adressat hat. Allerdings ist aus der Zahlenreihe zu erkennen, daß der Adressat überhaupt Grundbesitz hat und ggf., daß weiterer Grundbesitz vorhanden ist bzw. sein kann.

Den Datenschutzverstoß hat die Stadt umgehend eingesehen und sichergestellt, daß zukünftig derartige Adreßausdrucke beim Kommunalen Gebietsrechenzentrum nicht mehr vorkommen. Auch ist es allen Mitarbeitern des Steueramts der Stadt Nidderau untersagt, aufgrund der telefonischen Angabe einer Steuernummer Auskünfte zu erteilen.

Ich habe von einer förmlichen Beanstandung abgesehen, da keine weiteren Maßnahmen mehr zu veranlassen waren, als die Stadt Nidderau sie bereits freiwillig durchgeführt hatte.

5. Gesundheit

5.1
Prüfung des Medizinischen Dienstes der Krankenversicherung Hessen

Mit dem Gesundheitsreformgesetz von 1988 (BGBl. I S. 2477) und dem Gesundheitsstrukturgesetz von 1992 (BGBl. I S. 2266) hat der Gesetzgeber eine weitgehende Automatisierung der Datenverarbeitung im Bereich der gesetzlichen Krankenversicherung vorgeschrieben, mit der insbesondere "Transparenz des Leistungsgeschehens" und Kostenbegrenzung im Gesundheitswesen erreicht werden sollen (vgl. auch 21. Tätigkeitsbericht, Ziff. 9.2).

In der Diskussion um die Gesetzentwürfe haben die Datenschutzbeauftragten auf die Gefahr des "gläsernen Patienten" hingewiesen und u.a. auch für die Verarbeitung der umfangreichen sensitiven Daten durch den Medizinischen Dienst konkrete Regelungen gefordert, die Art, Umfang und Zweck der Datenverarbeitung festlegen und die Entstehung einer umfassenden medizinischen Zentraldatei über die Versicherten verhindern (Entschließung der Konferenz der Datenschutzbeauftragten vom 6. Juni 1988 zum Entwurf eines Gesetzes zur Strukturreform im Gesundheitswesen, abgedruckt im 17. Tätigkeitsbericht, Ziff. 16.4).

Aufgrund der datenschutzrechtlichen Diskussionen wurde in das Sozialgesetzbuch V eine Vorschrift über die Erhebung, Erfassung und Löschung personenbezogener Daten beim Medizinischen Dienst aufgenommen. Von zentraler

Bedeutung ist insbesondere, daß eine Löschung personenbezogener Angaben nach fünf Jahren zu erfolgen hat (§ 276 Abs. 2 Satz 3 SGB V) und daß der Medizinische Dienst in Dateien nur Angaben zur Person und Hinweise auf bei ihm vorhandene Akten aufnehmen darf (§ 276 Abs. 2 Satz 5 SGB V), damit keine umfassenden personenbezogenen medizinischen Dateien aufgebaut werden (vgl. BTDrucks. 11/3480 S. 66/67).

Diese neuen Regelungen und auch die zahlreichen Anfragen, die ich in den letzten Jahren zu diesem Thema erhalten habe, waren für mich Anlaß, die Datenverarbeitung durch den Medizinischen Dienst in Hessen zu einem Schwerpunktthema für 1994 zu machen. Ich habe mich sowohl in der Hauptverwaltung des Medizinischen Dienstes als auch in einer Reihe regionaler Leit- bzw. Beratungsstellen über die Praxis der Datenübermittlung zwischen den Leistungsträgern (z. B. Ärzten und Krankenhäusern), den Krankenkassen und dem Medizinischen Dienst sowie über die interne Datenverarbeitung durch den Medizinischen Dienst informiert.

Bei der Durchführung meiner Prüfungen hat mich der Medizinische Dienst umfassend unterstützt. Positiv ist zu vermerken, daß zum Zeitpunkt meiner Prüfung bereits eine eingehende Dienstanweisung für den Datenschutz sowohl in der Hauptverwaltung als auch in den Leit- und Beratungsstellen vorhanden war.

5.1.1
Aufgaben und Befugnisse des Medizinischen Dienstes der Krankenversicherung

Der Medizinische Dienst ist der sozialmedizinische Beratungs- und Begutachtungsdienst der gesetzlichen Krankenversicherung. Er ist auf Landesebene als eigenständige, von den Krankenkassen gemeinsam getragene Arbeitsgemeinschaft organisiert. Im Sozialgesetzbuch V ist eine klare funktionelle Trennung zwischen den Krankenkassen einerseits und dem Medizinischem Dienst andererseits festgelegt. Die Aufgaben des Medizinischen Dienstes sind in den §§ 275 – 277 SGB V geregelt. Danach sind die Krankenkassen in den gesetzlich bestimmten Fällen oder wenn es nach Art, Schwere, Dauer oder Häufigkeit der Erkrankung oder nach dem Krankheitsverlauf erforderlich ist, unter bestimmten Voraussetzungen bei der Erbringung von Leistungen, zur Einleitung von Maßnahmen zur Rehabilitation und bei Arbeitsunfähigkeit verpflichtet, eine gutachtliche Stellungnahme des Medizinischen Dienstes einzuholen (§ 275 Abs. 1 SGB V). Darüber hinaus können die Krankenkassen bei bestimmten Fallkonstellationen – z. B. bei kieferorthopädischer Behandlung und bei Dialysebehandlung – eine Prüfung des Medizinischen Dienstes veranlassen, in bestimmten Fällen – z. B. bei stationärer Krankenhausbehandlung, Schwerpflegebedürftigkeit und Kostenübernahme einer Behandlung im Ausland – sind sie hierzu sogar verpflichtet (§ 275 Abs. 2 und 3 SGB V).

Darüber hinaus müssen die Krankenkassen in jedem Bundesland die Notwendigkeit der Krankenhausaufnahme durch den Medizinischen Dienst im Rahmen eines Modellvorhabens prüfen lassen (§ 275a SGB V). Im übrigen sollen die Krankenkassen und ihre Verbände den Medizinischen Dienst generell zu Rate ziehen, insbesondere für allgemeine medizinische Fragen der gesundheitlichen Versorgung und Beratung der Versicherten, für Fragen der Qualitätssicherung, für Vertragsverhandlungen mit den Leistungserbringern und Beratungen der gemeinsamen Ausschüsse von Ärzten und Krankenkassen, insbesondere der Prüfungsausschüsse (§ 275 Abs. 4 SGB V). Zur Erfüllung dieser Aufgaben benötigt der Medizinische Dienst allerdings grundsätzlich keine personenbezogenen Daten, sondern nur fallbezogene oder statistische Daten.

Die Krankenkassen sind verpflichtet, dem Medizinischen Dienst die bei ihnen vorhandenen, für die Beratung und Begutachtung erforderlichen Unterlagen vorzulegen und Auskünfte zu erteilen (§ 276 Abs. 1 Satz 1 SGB V). Der Medizinische Dienst darf personenbezogene Daten nur erheben und erfassen, soweit dies für die Prüfungen, Beratungen und gutachtlichen Stellungnahmen nach § 275 SGB V und für die Modellvorhaben nach § 275a SGB V erforderlich ist (§ 276 Abs. 2 Satz 1 SGB V).

5.1.2
Funktionelle Trennung zwischen Medizinischem Dienst und Krankenkassen

Krankenkassen und Medizinischer Dienst arbeiten zwar eng zusammen, sie haben jedoch jeweils unterschiedliche Aufgaben und Befugnisse. Detaillierte medizinische Stellungnahmen oder Prüfungen obliegen nach der gesetzlichen Regelung ausschließlich dem Medizinischen Dienst, der hierfür auch über das erforderliche medizinische Fachwissen verfügt. Konsequenterweise darf auch nur der Medizinische Dienst detaillierte medizinische Unterlagen der behandelnden Ärzte bzw. Krankenhäuser, die er für die Begutachtung und Prüfung benötigt, zur Kenntnis erhalten. Für die Aufgabenerfüllung der Krankenkassen ist eine Kenntnisnahme dieser Unterlagen nicht erforderlich und damit auch nicht zulässig.

In der Praxis bestanden in den letzten Jahren Unklarheiten hinsichtlich der Frage, wer welche Unterlagen anfordert und an wen die Leistungserbringer die Unterlagen übersenden. Vielfach haben die Krankenkassen die Unterlagen zunächst für sich selbst angefordert und dann dem Medizinischen Dienst zur Verfügung gestellt. Dies war aus datenschutzrechtlicher Sicht nicht akzeptabel.

Das Zweite Gesetz zur Änderung des Sozialgesetzbuchs von 1994 (BGBl. I S. 1229) hat nunmehr eine Verpflichtung der Leistungserbringer, ihre Unterlagen direkt dem Medizinischen Dienst zur Verfügung zu stellen, ausdrücklich vorgeschrieben:

"...; haben die Krankenkassen nach § 275 Abs. 1 – 3 eine gutachtliche Stellungnahme oder Prüfung durch den Medizinischen Dienst veranlaßt, sind die Leistungserbringer verpflichtet, Sozialdaten auf Anforderung des Medizinischen Dienstes unmittelbar an diesen zu übermitteln, soweit dies für die gutachtliche Stellungnahme und Prüfung erforderlich ist."

Damit hat der Gesetzgeber – insbesondere auch aufgrund der datenschutzrechtlichen Diskussionen und Forderungen – eindeutig bestätigt, daß eine funktionelle Trennung zwischen Medizinischem Dienst und Krankenkassen vorzunehmen ist. Die Leistungserbringer sind verpflichtet, die medizinischen Daten an den Medizinischen Dienst direkt zu übersenden. Die medizinischen Daten sind für die Krankenkassen nicht erforderlich und dürfen nicht an diese übersandt und von diesen auch nicht für sich selbst angefordert werden.

Bei meinen Prüfungen habe ich festgesellt, daß diese rechtlichen Vorgaben jetzt in Hessen überwiegend korrekt umgesetzt werden. Zum Teil fordern jedoch die Krankenkassen nach wie vor die medizinischen Unterlagen für sich an und fügen sie dem Auftrag an den Medizinischen Dienst bei. Der Medizinische Dienst schickt dann zum Teil die von den Krankenkassen angeforderten Unterlagen zusammen mit seinem Gutachten an die Krankenkassen zurück. Dort werden die detaillierten medizinischen Daten dann gespeichert.

Bei meinen Prüfungen wurde ich in diesem Zusammenhang auf die bundesweiten Richtlinien über die Zusammenarbeit der Krankenkassen mit dem Medizinischen Dienst der Krankenversicherung von 1990 hingewiesen. Diese Richtlinien wurden von den Spitzenverbänden der Krankenkassen beschlossen und sind für jeden Landesverband verbindlich (§§ 213 Abs. 2, 210 Abs. 2 SGB V). In den Richtlinien ist vorgesehen, daß die Krankenkassen ihre Unterlagen vor der Begutachtung durch den Medizinischen Dienst vervollständigen und die angeforderten Unterlagen dem Auftrag an den Medizinischen Dienst beifügen. Diese Bestimmungen in den Richtlinien entsprechen jedoch nicht den – vorrangigen – gesetzlichen Vorgaben im Sozialgesetzbuch V.

Der Medizinische Dienst hat mir zugesagt, in einem Rundschreiben an die Leit- und Beratungsstellen darauf hinzuweisen, daß nur der Medizinische Dienst die medizinischen Unterlagen zur Kenntnis erhalten darf und daß diese Unterlagen auch nach der Begutachtung bei dem Medizinischen Dienst verbleiben müssen. Ferner hat er zugesagt, auf eine entsprechende Änderung der bundesweiten Richtlinien hinzuwirken.

Parallel zur Besprechung mit dem Medizinischen Dienst habe ich die Krankenkassen auf die Notwendigkeit einer Änderung des Verfahrens hingewiesen.

Der funktionellen Trennung zwischen dem Medizinischen Dienst und Krankenkassen entsprechend darf auch der Medizinische Dienst nicht alle medizinischen Informationen, die ihm vorliegen, im Rahmen seiner Stellungnahme oder Prüfung an die Krankenkassen übermitteln. § 277 Abs. 1 Satz 1 SGB V schreibt vor, daß der Medizinische Dienst der Krankenkassen "das Ergebnis der Begutachtung und die erforderlichen Angaben über den Befund" mitzuteilen hat. Damit ist einerseits klar festgelegt, daß die Krankenkassen nicht lediglich das Ergebnis der Begutachtung erhalten. Die Krankenkassen, die aufgrund der Begutachtung durch den Medizinischen Dienst eine Entscheidung über die Leistungsgewährung bzw. die Ablehnung der Kostenübernahme zu treffen haben, müssen das Ergebnis der Begutachtung nachvollziehen können. Das Gutachten dient als Hilfsmittel zur Entscheidungsfindung für die Krankenkassen.

Gerade auch im Fall eines negativen Ergebnisses des Medizinischen Dienstes ist für die Krankenkassen ein Gutachten erforderlich, weil im Fall einer Ablehnung einer Leistungsgewährung durch die Krankenkasse die Ablehnungsgründe für den Antragsteller nachvollziehbar im Ablehnungsbescheid aufzuführen sind. Die Begründung der Ablehnung der beantragten Leistung ist gerichtlich überprüfbar. Andererseits ist durch die Formulierung des § 277 Abs. 1 Satz 1 SGB V auch eindeutig vorgegeben, daß der Medizinische Dienst nur die jeweils im Einzelfall erforderlichen Angaben an die Krankenkassen übermitteln darf.

Bei meinen Prüfungen habe ich festgestellt, daß der Medizinische Dienst in Einzelfällen sehr ausführliche Gutachten mit eingehenden Angaben über Anamnese, Diagnose und Befund an die Krankenkassen übermittelt, zum Teil auch mit Informationen über mehrere Familienmitglieder des Versicherten.

Gegen diese Praxis habe ich Bedenken. Bei der Beurteilung der Frage, welches die "erforderlichen" Angaben sind, die der Medizinische Dienst den Krankenkassen mitzuteilen hat, muß die funktionelle Trennung zwischen dem Medizinischen Dienst und den Krankenkassen stärker berücksichtigt werden. Der Medizinische Dienst darf den Krankenkassen nur die zum Verständnis des jeweiligen Gesamtzusammenhangs unerläßlichen Einzelangaben übermitteln. Umfassende Angaben zur gesamten Krankengeschichte des Versicherten oder auch Informationen über Krankengeschichten von Familienmitgliedern benötigen die Krankenkassen im Regelfall zur Erfüllung ihrer Aufgaben nicht.

Der Medizinische Dienst hat in erster Linie auf die Schwierigkeit hingewiesen, ein praktikables Verfahren für eine differenzierte Übermittlungspraxis zu finden. Er hat mir zugesagt, dieses Problem mit den Leit- und Beratungsstellen zu besprechen und anschließend zur künftigen Verfahrensweise noch einmal Stellung zu nehmen. In jedem Fall wird in die Dienstanweisung zum Datenschutz ein Hinweis darauf aufgenommen, daß im Rahmen einer Begutachtung nur die jeweils erforderlichen Daten an die Krankenkassen übermittelt werden dürfen.

5.1.3
Speicherung von Versichertendaten in Dateien

Nach § 276 Abs. 2 Satz 5 SGB V darf der Medizinische Dienst in Dateien nur Angaben zu Personen und Hinweise auf bei ihm vorhandene Akten aufnehmen. Medizinische Einzelangaben dürfen grundsätzlich nicht automatisiert gespeichert werden. Durch diese Regelung will der Gesetzgeber den Risiken einer pauschalen maschinellen Auswertung umfangreicher medizinischer Datenbestände begegnen.

Bei meinen Prüfungen habe ich festgestellt, daß die von den Krankenkassen erbetenen Gutachten in den Leit- und Beratungsstellen mit Hilfe der EDV erstellt und anschließend gelöscht werden. Gegen diese Verfahrensweise habe ich

keine grundsätzlichen Bedenken. Ich sehe es als zulässig an, die für die Gutachtenerstellung erforderlichen medizinischen Daten (z. B. Diagnosen, Befunde usw.) automatisiert zu speichern und die Daten mit Hilfe eines Textverarbeitungssystems zu verarbeiten, wenn die gespeicherten Daten ausschließlich für die Erstellung dieses konkreten Gutachtens verwertet und nach Fertigstellung des Gutachtens umgehend gelöscht werden. Der Medizinische Dienst hat mir dargelegt, daß die Hauptverwaltung diese Voraussetzungen durch eine entsprechende Parametrisierung von ISmed (vgl. dazu unten 9.1.10) sicherstellt. Die Einzelheiten des Verfahrens werden in die Dienstanweisung zum Datenschutz aufgenommen.

5.1.4
Verpflichtung zur Datenlöschung nach fünf Jahren

Der Medizinische Dienst darf bei der Erstellung eines Gutachtens auf ein bereits zuvor erstelltes Gutachten zurückgreifen, soweit dies im Einzelfall erforderlich ist. Nach § 276 Abs. 2 Satz 3 SGB V ist der Medizinische Dienst aber verpflichtet, die von ihm erhobenen und gespeicherten personenbezogenen Daten nach fünf Jahren zu löschen.

Bei meinen Prüfungen habe ich registriert, daß zum Teil bereits erhebliche Anstrengungen unternommen wurden, diese rechtlichen Vorgaben umzusetzen, zum Teil habe ich aber auch Schwierigkeiten hinsichtlich der Umsetzung der Vorschrift festgestellt; z. B. habe ich in einem Einzelfall noch Unterlagen im Keller vorgefunden, die bis zum Jahre 1956 zurückgehen und längst hätten vernichtet werden müssen. Aufgrund meiner Feststellungen habe ich den Medizinischen Dienst gebeten, mir eine vollständige Übersicht über den Stand der Umsetzung der Löschungsverpflichtung in allen Leit- und Beratungsstellen zu erstellen und mir einen konkreten Zeitplan für die vollständige Umsetzung der rechtlichen Vorgaben in allen Leit- und Beratungsstellen zu nennen. Dies hat der Medizinische Dienst zugesagt.

5.1.5
Hinweis auf das Widerspruchsrecht der Versicherten

Nach § 277 Abs. 1 SGB V hat der Medizinische Dienst auch dem behandelnden Arzt und den sonstigen Leistungserbringern, über deren Leistungen er eine gutachterliche Stellungnahme abgegeben hat, Mitteilung zu machen. In diesem Fall kann jedoch der Versicherte der Mitteilung über den Befund widersprechen, so daß der Medizinische Dienst dann nur das Ergebnis seiner Begutachtung mitteilen darf. Damit der Versicherte auch in der Lage ist, über die Wahrnehmung seines Widerspruchsrechts zu entscheiden, bedarf es allerdings einer vorherigen Information über die gesetzlich eingeräumte Widerspruchsmöglichkeit; sonst besteht die Gefahr, daß das Widerspruchsrecht des Versicherten faktisch funktionslos bleibt.

Die Richtlinien über die Zusammenarbeit der Krankenkassen mit dem Medizinischen Dienst der Krankenversicherung (vgl. oben 9.1.2) sehen vor, daß der Versicherte auf sein Widerspruchsrecht in der Einladung zur sozialmedizinischen Begutachtung hinzuweisen ist. Wenn ein solcher Hinweis erkennbar unterblieben ist, soll der Versicherte durch den Arzt des Medizinischen Dienstes auf sein Widerspruchsrecht hingewiesen werden.

Bei meinen Prüfungen habe ich festgestellt, daß in den Leit- und Beratungsstellen unterschiedlich verfahren wird. Zum Teil erfolgt im Einladungsschreiben ein Hinweis auf das Widerspruchsrecht, zum Teil wird der Versicherte bei der Untersuchung vom Arzt, von der Geschäftsstelle oder durch einen Aushang im Wartezimmer darauf hingewiesen. Der Medizinische Dienst wird künftig ein einheitliches Verfahren einführen. Die Versicherten sollen ein Informationsschreiben zu ihrem Widerspruchsrecht erhalten. Der Inhalt des Informationsschreibens wird mit mir abgestimmt.

5.1.6
Speicherung medizinischer Daten bei externen Gutachtern

Im Sozialgesetzbuch V ist festgelegt, daß die Fachaufgaben des Medizinischen Dienstes von Ärzten und Angehörigen anderer Heilberufe wahrgenommen werden; der Medizinische Dienst hat vorrangig externe Gutachter zu beauftragen.

Bei meinen Prüfungen hat sich die Frage ergeben, wie sichergestellt wird, daß bei den externen Gutachtern keine umfassenden Dateien mit medizinischen Daten über die Versicherten entstehen und damit die Verpflichtung des Medizinischen Dienstes zur Datenlöschung nach fünf Jahren (vgl. oben 5.1.4) praktisch ins Leere läuft. Der Medizinische Dienst stimmt mit mir darin überein, daß es nicht akzeptiert werden kann, daß externe Gutachter in größerem Umfang personenbezogene Daten von Versicherten verarbeiten dürfen als er es selbst darf. Er hat mir zugesagt, künftig in die vertraglichen Einzelvereinbarungen mit den externen Gutachtern die folgenden Verpflichtungen aufzunehmen:

- Die dem Gutachter zur Verfügung gestellten Befunde (Arztbriefe, Krankenhausentlassungsbriefe usw.) sind an den Medizinischen Dienst zurückzugeben.
- Das Gutachten ist beim Gutachter nach Abwicklung des Auftrags zu löschen. Beim Gutachter dürfen nur Daten über die verwaltungsmäßige Auftragsdurchführung gespeichert bleiben.

Der vollständige Inhalt des externen Gutachtens bleibt beim Medizinischen Dienst gespeichert und wird – wie andere Gutachten auch – nach fünf Jahren gelöscht.

5.1.7
Überprüfung der Notwendigkeit und Dauer der Krankenhausbehandlung durch den Medizinischen Dienst

Durch das Gesundheitsstrukturgesetz ist der Katalog derjenigen Daten, welche die Krankenhäuser routinemäßig in jedem Einzelfall einer Krankenhausbehandlung den Krankenkassen übermitteln müssen, wesentlich erweitert worden (§ 301 Abs. 1 SGB V). Der neuen Regelung zufolge müssen die Krankenhäuser über die Abrechnungsdaten hinaus die folgenden medizinischen Daten der Versicherten – maschinenlesbar – übermitteln:

- den Tag, die Uhrzeit und den Grund der Aufnahme sowie die Einweisungsdiagnose, die Aufnahmediagnose, bei einer Änderung der Aufnahmediagnose die nachfolgenden Diagnosen, die voraussichtliche Dauer der Krankenhausbehandlung sowie, falls diese überschritten wird, auf Verlangen der Krankenkasse die medizinische Begründung,
- bei ärztlicher Verordnung von Krankenhausbehandlung die Arztnummer des einweisenden Arztes, bei Verlegung das Institutionskennzeichen des veranlassenden Krankenhauses, bei Notfallaufnahme die die Aufnahme veranlassende Stelle,
- die Bezeichnung der aufnehmenden Fachabteilung, bei Verlegung die der weiterbehandelnden Fachabteilungen,
- Datum und Art der im jeweiligen Krankenhaus durchgeführten Operationen,
- den Tag, die Uhrzeit und den Grund der Entlassung oder der externen Verlegung sowie die Entlassungsdiagnose; bei externer Verlegung das Institutionskennzeichen der aufnehmenden Institution,
- Angaben über die im jeweiligen Krankenhaus durchgeführten Rehabilitationsmaßnahmen sowie Vorschläge für die Art der weiteren Behandlung mit Angabe geeigneter Einrichtungen.

Soweit die Krankenkassen darüber hinaus eine Überprüfung der Notwendigkeit und Dauer der stationären Behandlung des Versicherten veranlassen, sind die Ärzte des Medizinischen Dienstes befugt, die Krankenhäuser zu betreten, die Krankenunterlagen einzusehen und ggf. den Versicherten zu untersuchen, soweit dies im Einzelfall zu einer gutachterlichen Stellungnahme erforderlich ist (§ 276 Abs. 4 SGB V).

Im Zusammenhang mit dieser Regelung habe ich zahlreiche Anfragen erhalten, ob der Medizinische Dienst vom Krankenhaus eine Übersendung von Krankenunterlagen verlangen kann.

Grundsätzlich bestehen gegen eine solche Verfahrensweise keine datenschutzrechtlichen Bedenken. Das in § 276 Abs. 4 SGB V vorgesehene Recht auf Akteneinsicht schließt das Recht zur Erstellung von Kopien in dem erforderlichen Umfang ein. Statt der Erstellung von Kopien kann auch eine Übersendung von Krankenunterlagen an den Medizinischen Dienst erfolgen; es liegt insoweit kein weitergehender, nicht von der gesetzlichen Regelung gedeckter Eingriff in die Rechte der Versicherten vor. Selbstverständlich darf der Medizinische Dienst aber nur in dem Umfang Unterlagen anfordern bzw. dürfen ihm nur in dem Umfang Unterlagen übersandt werden, in dem er sie für den konkreten Auftrag tatsächlich benötigt.

Ich habe keine Anhaltspunkte dafür festgestellt, daß Daten über den jeweils im Einzelfall erforderlichen Umfang hinaus angefordert bzw. übermittelt wurden.

5.1.8
Datensicherheit in den Leit- und Beratungsstellen

Bei meinen Prüfungen habe ich nur in Einzelfällen Probleme hinsichtlich der Datensicherheit in den Leit- und Beratungsstellen festgestellt. Diese betrafen z.B. eine mangelhafte Sicherung von im Keller gelagerten Akten, eine unzureichende Sicherung eines Briefkastens, aus dem Post leicht entwendet werden konnte, und die Sicherung eines Serverraums. Der Medizinische Dienst hat zugesagt, diese Mängel zu beseitigen. Im übrigen hat er darauf hingewiesen, daß die Anzahl der Leit- und Beratungsstellen in der nächsten Zeit reduziert wird und in diesem Zusammenhang auch die technisch-organisatorischen Datensicherheitsmaßnahmen überprüft werden.

5.1.9
Dienstanweisung des Medizinischen Dienstes zum Datenschutz

Zum Zeitpunkt meiner Prüfung hatte der Medizinische Dienst bereits eine umfangreiche Dienstanweisung zum Datenschutz erarbeitet. Diese Dienstanweisung wurde mit mir erörtert und soll insbesondere in folgenden Punkten überarbeitet werden:

- Einbeziehung der neuesten Gesetzesänderungen im Sozialgesetzbuch V und X
- Konkretisierung der Anforderungen an die Ausgestaltung von Schweigepflichtentbindungserklärungen, die dem Medizinischen Dienst vorgelegt werden
- Regelung der Verantwortlichkeiten bezüglich der DV-Konzeption und deren Umsetzung
- Beschaffung von Hardware und Beschaffung bzw. Erstellung von Software.

Hinsichtlich der technisch-organisatorischen Datensicherungsmaßnahmen habe ich vorgeschlagen, die Passagen der Dienstanweisung aufbauend auf ein Datenschutz-/Datensicherungskonzept (vgl. auch Ziff. 25) anzupassen.

5.1.10
Einführung von ISmed beim Medizinischen Dienst

ISmed ist ein Verfahren, das in der Mehrzahl der Bundesländer in den Geschäftsstellen des Medizinischen Dienstes der Krankenkassen eingesetzt werden soll. In Hessen gibt es erste Installationen. Im wesentlichen unterstützt ISmed die Geschäftsstellen bei der Erstellung von medizinischen Gutachten. Dazu werden u.a. verschiedene Verwaltungsinformationen vorgehalten, die automatisiert den Gutachten hinzugefügt werden. Ferner werden in einer Verweiskartei Stammdaten von Patienten gespeichert, durch die ein schneller Zugriff auf vorhandene Akten möglich ist. Einige Teilanwendungen stehen nur der Anwendungsbetreuung offen oder wurden nicht genutzt.

In einer Geschäftsstelle habe ich die Anwendung geprüft. Das Ergebnis zeigt einerseits Defizite, die anwendungsspezifisch sind, und andererseits Defizite, die sich aus der Installation ergaben.

5.1.10.1
Technische Rahmenbedingungen

ISmed wurde auf einem PC unter dem Betriebssystem SINIX-Z betrieben, welches UNIX System V.41 entspricht. An den Rechner waren 10 PC mit einer Terminalemulation angeschlossen. Es waren keine weiteren Anwendungen für die PC vorgesehen.

Das Verfahren wurde nur zur Erstellung von Gutachten verwendet. Weitere Anwendungsteile, wie z.B. der Terminplaner, wurden nicht genutzt. Durch die Grundeinstellung war gewährleistet, daß die Gutachten nach dem Ausdruck umgehend physisch gelöscht wurden. Die Verweisdatei blieb davon unberührt.

5.1.10.2
Anwendungsspezifische Datensicherungsmaßnahmen

Der Medizinische Dienst der Krankenkassen Hessen kann Defizite, die anwendungsspezifisch sind, nur mittelbar beheben. Er setzt ISmed als Software ein, ist aber nicht für die Entwicklung zuständig. Zwar kann er Änderungen fordern, diese müssen aber in Abstimmung mit anderen Stellen vorgenommen werden.

5.1.10.2.1
Benutzerkontrolle/Aufruf von ISmed

Nach dem Start der Terminalemulation mußte die Anmeldeprozedur von SINIX mit der Eingabe von User-ID und Paßwort durchlaufen werden.

Die Benutzer von ISmed wurden sofort in ihre Anwendung weitergeleitet. Anschließend erfolgte die Anmeldung unter ISmed mit Kennung und Paßwort. Das Paßwort mußte mindestens eine Stelle lang sein, es gab keine Historie, keine Alterung, und es wurde nicht nach mehrmaliger Fehleingabe die Kennung gesperrt. Auch wurde die unter SINIX eingegebene User-ID nicht gegengecheckt; ein Identitätswechsel wäre möglich gewesen. Die Paßwortverwaltung von ISmed entspricht insofern nicht dem Stand der Technik und erfüllt nicht die Anforderungen, wie ich sie z.B. im 19. Tätigkeitsbericht, Ziff. 15 formuliert habe. Ich habe daher gefordert, ISmed oder die Einbettung in SINIX entsprechend anzupassen.

5.1.10.2.2
Zugriffskontrolle

– Zugriffe auf Systemebene

  Die Sicherheitsmechanismen von SINIX müssen für die Benutzer von ISmed auf der Betriebssystemebene identische, umfassende Zugriffsrechte auf die Daten von ISmed vorsehen.

  Anwendungsspezifische Zugriffseinschränkungen machen folglich nur Sinn, wenn die Anwender nicht auf die Systemebene gelangen. Der Versuch, die Anmeldeprozedur abzubrechen oder aus der Anwendung auf die Betriebssystemebene zu gelangen, führte zur Abmeldung unter SINIX. Ein "normaler" Benutzer konnte daher nur mit ISmed arbeiten.

– Zugriffskontrolle von ISmed

  ISmed kennt fünf verschiedene Anwendergruppen, so z.B. die Anwendungsbetreuung, Ärzte oder Sekretärinnen. Abhängig von der Anwendergruppe stehen die Programme mit unterschiedlichen Verarbeitungsmöglichkeiten zur Verfügung. Die Zugriffsmöglichkeiten auf die Gutachten selbst werden über ein Feld im Datensatz und eine Tabelle gesteuert. In dem Datenfeld wird die Kennung des zuständigen Arztes gespeichert, und in der Tabelle befinden sich zu jeder Arztkennung die Benutzerkennungen, denen ein Zugriff auf die Gutachten des Arztes eingeräumt wird. Ein Arzt "Meier", dessen Name im Feld des zuständigen Arztes gespeichert ist, kann auf das Gutachten zurückgreifen. Will ein anderer Benutzer auf das Gutachten zugreifen, so wird geprüft, ob dessen Kennung dem Arzt "Meier" zugeordnet ist. Ist das der Fall, wird der Zugriff erlaubt.

  Die Patientendaten können, nachdem das Gutachten angelegt wurde, außer durch die Anwendungsbetreuung, nicht mehr geändert werden. Die Anwendungsbetreuung kann allerdings auch bei begonnenem Gutachten den zuständigen Arzt ändern. Damit ergeben sich entsprechend andere Zugriffsrechte.

  Insgesamt können die erforderlichen Zugriffseinschränkungen in der Anwendung umgesetzt werden.

5.1.10.2.3
Protokollierung

Es existieren nur die Standard-UNIX-Protokolle. In der Anwendung sind keine Protokollierungen vorgesehen.

Hier sind Verbesserungen unbedingt erforderlich. Es sind insbesondere die Protokollierungen auf System- und Anwendungsebene vorzunehmen bzw. zu programmieren, mit denen die Tätigkeit der System- und Anwendungsbetreuer nachvollzogen werden kann.

5.1.10.2.4
Verschlüsselung

Eine Verschlüsselung von Daten findet zur Zeit wegen technischer Probleme noch nicht statt.

Trotz einiger Bedenken habe ich den Zustand für eine Übergangszeit akzeptiert. Die Zugriffe der Mitarbeiter der Geschäftsstelle werden über ISmed kontrolliert. Sie gelangen nicht auf die Betriebssystemebene. Personen mit weitergehenden Zugriffsrechten werden nur im Fehlerfall tätig. Sie gehören nicht zur Geschäftsstelle und arbeiten nur unter Aufsicht an dem Rechner. Da die medizinischen Gutachten umgehend gelöscht werden, ist das Risiko einer unberechtigten Kenntnisnahme sensibler Daten gering. Dennoch ist eine Verschlüsselung der Daten so schnell wie möglich vorzunehmen.

5.1.10.3
Installationsspezifische Defizite

Die installationsspezifischen Defizite konnten bzw. können durch den Medizinischen Dienst selbst abgestellt werden.

5.1.10.3.1
Zugriffsrechte

In der Zugriffskontrolltabelle waren zu einem Arzt alle Sekretärinnen als zugriffsberechtigt eingetragen. Zugriffsrechte der Ärzte untereinander waren nicht vorgesehen. In Anbetracht der Aufgabenverteilung der wenigen Sekretärinnen hatte ich keine Bedenken.

Als Anwendungsbetreuung arbeiteten mehrere Benutzer mit einer Kennung. Mit dieser Kennung wurde die Anwendung administriert; so wurden die Zugriffsrechte mit dieser Kennung gepflegt. Ein direkter Zugriff auf den Inhalt der Gutachten ist mit der Kennung jedoch nicht möglich.

In der Schulung zu ISmed wurden alle Sekretärinnen über die Kennung informiert, und das Paßwort wurde genannt. Die Zugriffe und Zugriffsmöglichkeiten waren dadurch nicht kontrollierbar. Dieser Zustand wurde dadurch beseitigt, daß jede Person, die als Anwendungsbetreuer tätig wird, eine eigene Kennung erhält, deren Paßwort nur ihr bekannt ist.

5.1.10.3.2
Fernbetreuung

Die Fernbetreuung der Anwendung wurde durch die Hauptverwaltung vorgenommen. Durch organisatorische Regelungen und die Sicherheitsvorkehrungen des eingesetzten Produkts kann die Fernbetreuung abgesichert werden. Bei einem Zugriff über die Software müssen die für SINIX üblichen Sicherheitsmaßnahmen durchlaufen werden. Ferner gelten u.a. die folgenden zusätzlichen Maßnahmen:

- Das Modem ist deaktiviert, wenn keine Unterstützung angefordert wird.
- Es muß ein gesondertes Paßwort für die Software eingegeben werden. Die Anzahl der maximal zulässigen Fehlversuche ist auf drei festgelegt.
- Abhängig vom Einzelfall wird ein Rückruf vorgesehen.
- Die Abläufe bei der Fernwartung werden protokolliert.
- Auf dem PC in der Geschäftsstelle können die Eingaben am externen Arbeitsplatz direkt verfolgt werden.
- Wird über 20 Minuten keine Eingabe vorgenommen, erfolgt der Abbruch der Verbindung.
- Nach dem Verlassen der Software erfolgt ein Warmstart des PC.
- Es wird eine Verschlüsselungsoption für die Kommunikation aktiviert.

Insgesamt ist dadurch ein adäquates Sicherheitsniveau erreicht.

5.1.10.3.3
Organisatorische Maßnahmen

ISmed und die Fernbetreuungssoftware waren korrekt implementiert. Die Vorgaben waren jedoch nicht schriftlich fixiert. Gleiches gilt für das Sicherheitskonzept. Ich habe daher gefordert, die Regelungen schriftlich vorzunehmen.

5.2
Verarbeitung von Beihilfedaten

Beihilfeakten im öffentlichen Dienst enthalten sehr sensible Daten von Bediensteten, ggf. auch von ihren Familienangehörigen. Bereits im Jahr 1982 hatte ich auf das Problem hingewiesen, daß im öffentlichen Dienst – im Unterschied zur Privatwirtschaft – keine strikte Trennung erfolgt zwischen den Angaben, die der Bedienstete zur Deckung seiner Krankheitskosten offenbaren muß, und solchen Daten, die der Arbeitgeber oder Dienstherr für Zwecke der Personalverwaltung verarbeitet. Ich hatte damals eine strikte Zweckbindung der Beihilfedaten im öffentlichen Dienst gefordert.

Nachdem die damalige Landesregierung meine Forderungen zunächst abgelehnt hatte – u.a. mit der Begründung, in der Praxis zeige sich immer wieder, "daß auch aus Beihilfeakten wichtige Erkenntnisse für die schwerwiegenden Personalentscheidungen gewonnen ... werden könn(t)en" – forderte der Hessische Landtag im Jahr 1984 die Landesregierung auf, "umgehend Regelungsvorschläge vorzulegen, die die strikte Zweckbindung bei der Verwendung von für die Gewährung von Beihilfen gemachten Angaben unter Berücksichtigung der vom Datenschutzbeauftragten gemachten Anmerkungen gewährleisten" (vgl. 11. Tätigkeitsbericht, Ziff. 5.2.2, 12. Tätigkeitsbericht, Ziff. 2.1.6.2, 13. Tätigkeitsbericht, Ziff. 4.2.2.2). Aufgrund des Landtagsbeschlusses änderte das Hessische Ministerium des Innern die Verwaltungsvorschriften zu § 107 HBG (Erlaß vom 16. September 1985, StAnz. 1985, S. 1810). Mit der Einfügung eines neuen Abschnitts Va wurde nach jahrelangen Diskussionen endlich klargestellt, daß Beihilfeunterlagen strikt zweckgebunden für die Prüfung und Berechnung der Beihilfe zu verwenden sind. Die Beihilfeakten sind getrennt von den übrigen Personalakten zu führen und dürfen ohne Zustimmung des Bediensteten von Mitarbeitern der Personalabteilung nicht eingesehen werden.

Inzwischen wurde eine entsprechende Regelung auch in § 90a BBG aufgenommen, und mit Wirkung vom 1. November 1993 wurden die Verwaltungsvorschriften zu § 107 HBG durch die Einfügung des § 107a HBG im "Gesetz zur Änderung dienstrechtlicher Vorschriften" vom 28. Oktober 1993 (GVBl. I S. 470) abgelöst. Die neue detaillierte gesetzliche Regelung habe ich zum Anlaß genommen, die Praxis der Verarbeitung der Beihilfedaten in mehreren Behörden zu prüfen. Um mir einen möglichst genauen Überblick zu verschaffen, habe ich Behörden unterschiedlicher Größe und Struktur, nämlich den Hessischen Rechnungshof, das Hessische Landesamt für Versorgung und Soziales, den Landeswohlfahrtsverband Hessen und die Kommunalverwaltung Kriftel geprüft. Die Zahl der Beihilfeakten der Behörden, die ich geprüft habe, bewegte sich zwischen weniger als 100 Beihilfeakten und weit über 1000.

5.2.1
Trennung der Beihilfeakten von den Personalakten

§ 107a HBG schreibt vor, daß Unterlagen über Beihilfen stets als Teilakten zu führen sind, die von der übrigen Personalakte getrennt aufzubewahren sind.

Meine Prüfungen ergaben, daß alle vier Behörden die Beihilfeunterlagen als Teilakten führen. Nur bei der Kommunalverwaltung wurden die Beihilfeakten und die Personalakten zusammen aufbewahrt. Meine Anregung, die Aktenbestände getrennt zu führen, hat der Gemeindevorstand kurzfristig umgesetzt.

Im Landesamt für Versorgung und Soziales befanden sich im Büro der Beihilfesachbearbeiter zum Zeitpunkt der Prüfung auch die Personalnebenakten "Fahrtkosten" und "Trennungsgeld", die allerdings von einer Mitarbeiterin der Personalverwaltung bearbeitet wurden. Da sich die Akten im Zugriff der Beihilfesachbearbeiter befanden, habe ich empfohlen, sie aus dem Büro zu entfernen; sie wurden bereits am Tag nach meiner Prüfung in die Registratur der Personalabteilung verlagert.

5.2.2
Abschottung der Beihilfebearbeitung von der allgemeinen Personalverwaltung

Jeder, der im Einzelfall berechtigt auf die Personalhaupt- oder Teilakten zugreifen kann, darf nicht mit Beihilfeakten bzw. -vorgängen befaßt werden. Nach § 107a Abs. 1 Satz 3 HBG "soll" die Beihilfebearbeitung in einer von der übrigen Personalverwaltung getrennten Organisationseinheit vorgenommen werden. Zugang "sollen" nur Beteiligte dieser Organisationseinheit haben. Die Sollvorschrift in § 107a Abs. 1 Satz 3 HBG berücksichtigt die Schwierigkeiten kleinerer Behörden, eine getrennte Bearbeitung von Personalangelegenheiten einerseits und Beihilfeangelegenheiten andererseits durchzuführen. Soweit jedoch in einer Behörde die getrennte Bearbeitung möglich ist – und dies ist der Regelfall –, muß die Beihilfebearbeitung von der übrigen Personalverwaltung getrennt werden.

Ich habe bei meinen Prüfungen festgestellt, daß die Trennung der Beihilfebearbeitung von der übrigen Personalverwaltung nicht immer im erforderlichen Umfang gewährleistet war. So wurden in der Kommunalverwaltung die Beihilfeanträge von der Personalsachbearbeiterin bearbeitet. Mit der Auslagerung der Beihilfeakten aus der Personalsachbearbeitung wurde hier auch die Beihilfebearbeitung auf einen Mitarbeiter übertragen, der keine sonstigen Aufgaben innerhalb der Personalverwaltung wahrnimmt. Das Landesamt für Versorgung und Soziales, von dem auch die Beihilfeakten eines Ministeriums bearbeitet werden, hatte die erforderliche Abschottung der Beihilfestelle von der übrigen Personalverwaltung bereits vorbildlich vollzogen. Es bestanden hier keinerlei Berührungspunkte zwischen Beihilfebearbeitung und sonstiger Personalverwaltung.

Die vom Gesetz geforderte Abschottung der Beihilfestelle ist dann nicht vollzogen, wenn der Leiter der Personalabteilung die Beihilfebescheide unterschreibt. Dies ist beim Rechnungshof der Fall. Die Beihilfeanträge werden zwar in vollem Umfang von Beihilfesachbearbeitern bearbeitet, die Bescheide jedoch vom Leiter der Personalabteilung

unterschrieben. Zu diesem Zweck erhält der Personalleiter auch jeweils die kompletten Beihilfeunterlagen, wie Arztrechnungen, Rezepte usw. Ich habe dem Rechnungshof mitgeteilt, daß das Verfahren nicht im Einklang mit § 107a HBG steht.

Beim Landeswohlfahrtsverband ist das Personaldezernat in mehrere Referate unterteilt. Die Referate wiederum sind unterteilt in Hauptsachgebiete und Sachgebiete. Zwar werden die Beihilfeanträge in einem eigenen Sachgebiet "Beihilfe nach den hessischen Beihilfevorschriften" bearbeitet, jedoch sind die Beihilfesachbearbeiter nicht befugt, die Anträge abschließend zu bearbeiten. Sie berechnen die Beihilfe, setzen sie fest, bestätigen die sachliche Richtigkeit und leiten sie einschließlich aller Unterlagen an die Hauptsachgebietsleiterin weiter. Diese unterschreibt die Bescheide bis zu einer bestimmten Ausgabenhöhe. Bescheide mit darüber hinausgehenden Zahlungen werden von der Referatsleiterin unterschrieben.

Der Referatsleiterin obliegt neben der Bearbeitung von Beihilfeanträgen u.a. auch noch die Bearbeitung anderer Personalangelegenheiten wie beispielsweise Disziplinarverfahren. Für diese Tätigkeiten hat die Referatsleiterin auch Zugriff auf die entsprechenden Personalakten. Es besteht somit eine Vermischung von Beihilfebearbeitung und Bearbeitung sonstiger Personalangelegenheiten des Personaldezernats. Auch die Hauptsachgebietsleiterin hat im Rahmen ihrer sonstigen Tätigkeit Zugriff auf die Personalhauptakten. Der Landeswohlfahrtsverband hat mir mitgeteilt, daß die notwendigen organisatorischen Vorbereitungen getroffen werden, um die Beihilfesachbearbeitung von sonstiger Sachbearbeitung zu trennen.

5.2.3
Aufbewahrungsfristen von Beihilfeunterlagen

Nach § 107f Abs. 2 HBG sind Unterlagen über Beihilfen fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren.

Meine Prüfung des Inhalts von Beihilfeakten der vier Behörden hatte zum Ergebnis, daß bis auf eine Ausnahme die Unterlagen in den Beihilfeakten nicht älter als fünf Jahre waren. Lediglich beim Rechnungshof hatte eine von zwei Beihilfesachbearbeiterinnen bisher keine Bereinigung der Beihilfeakten vorgenommen.

Vereinzelt habe ich in den Personalakten Beihilfeunterlagen gefunden, die älter als fünf Jahre waren. Ich habe die betreffenden Behörden aufgefordert, noch in den Personalakten vorhandene Beihilfeunterlagen zu vernichten.

Den Vollzug der Bereinigung werde ich 1995 überprüfen.

5.2.4
Vorprüfung von Beihilfeanträgen

Der Landeswohlfahrtsverband hat im Zusammenhang mit der Beihilfebeantragung ein besonderes Verfahren entwikkelt, das allerdings nicht den rechtlichen Anforderungen genügt.

Auf der Rückseite des Vordrucksatzes "Antrag auf Beihilfe" kann ein Antragsteller mit seiner Unterschrift erklären, daß er mit einer Vorprüfung seines Antrags durch seine Dienststelle (hier der Personalabteilung) einverstanden ist oder die Vorprüfung ablehnt. Ist ein Antragsteller mit der Vorprüfung einverstanden, bestätigt die Dienststelle, daß der Antrag auf Richtigkeit und Vollständigkeit überprüft worden ist, und leitet ihn zusammen mit den Rechnungen an die Beihilfefestsetzungsstelle weiter. Diese Verfahrensweise hat für die Bediensteten der einzelnen Zweigverwaltungen und Einrichtungen des Landeswohlfahrtsverbandes den Vorteil, daß unvollständige Anträge ohne größere Verzögerung ergänzt werden können.

Eine – wenn auch freiwillige – Vorprüfung von Beihilfeanträgen durch die Personalabteilung einer Dienststelle widerspricht dem gesetzlich vorgesehenen Trennungsgebot von Personalabteilung und Beihilfebearbeitung. Die Regelungen in § 107a HBG lassen auch für die beschriebene Einwilligungslösung keinen Spielraum. Dies ist sachgerecht, da die Gefahr einer Zweckvermengung auch bei einer Einwilligungslösung nicht ausgeschlossen werden kann. Ich habe die Behörde darauf hingewiesen, daß das Antragsformular in der vorliegenden Form nicht mehr zu benutzen ist. Der Landeswohlfahrtsverband hat daraufhin alle Dienststellen angewiesen, die Vorprüfung von Beihilfeanträgen ab sofort zu unterlassen.

5.2.5
Datensicherungsmaßnahmen

Als durchweg erfreulich ist festzustellen, daß die Teilakten mit Beihilfeunterlagen von den jeweiligen Dienststellen so aufbewahrt werden, daß ein Zugriff durch Unbefugte nicht möglich ist. In allen von mir geprüften Stellen werden die Beihilfeakten in verschließbaren Schränken aufbewahrt. Die postalische Bearbeitung der Beihilfeunterlagen ist ohne Ausnahme vorbildlich geregelt. So wurde in allen Behörden die eingehende Post, soweit als Post mit Beihilfeunterlagen erkennbar, ungeöffnet der jeweiligen Beihilfestelle zugeleitet. Ausgehende Post wird ausnahmslos von den zuständigen Beihilfesachbearbeitern kuvertiert und verschlossen an die Poststellen zur Absendung weitergeleitet.

5.3
Maschinenlesbare Patientenkarten – Stand der Entwicklung und Diskussion

1993/94 ist in Hessen die Krankenversichertenkarte in Chipkartenform als Krankenscheinersatz eingeführt worden (vgl. 21. Tätigkeitsbericht, Ziff. 9.2). Die Krankenversichertenkarte enthält keine medizinischen Daten. Der Umfang der auf der Krankenversichertenkarte gespeicherten Daten ist in § 291 SGB V abschließend geregelt (ausstellende Krankenkasse, Name, Geburtsdatum und Anschrift des Versicherten, Krankenversichertennummer, Versichertenstatus, Zeit des Versicherungsschutzes), ebenso der Zweck der Karte: Die Krankenversichertenkarte darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen sowie für die Abrechnung mit den Leistungsträgern verwendet werden.

Bereits im 22. Tätigkeitsbericht habe ich berichtet, daß in zunehmendem Maße darüber hinausgehende Möglichkeiten und Ziele des Einsatzes von maschinenlesbaren Patientenkarten mit medizinischen Daten (z. B. Notfallkarten, Karten für besondere Patientengruppen wie etwa Dialysepatienten und Krebskranke, Röntgenkarten, Apothekenkarten etc.) diskutiert und teilweise auch bereits erprobt werden (22. Tätigkeitsbericht, Ziff. 9.1). Dabei besteht derzeit in der Bundesrepublik grundsätzlich ein Konsens darüber, daß die Verwendung einer Patientenkarte mit medizinischen Daten nur auf freiwilliger Basis in Betracht kommt. Mit dem Stichwort "Freiwilligkeit" der Patientenentscheidung sind allerdings keineswegs alle sich aus datenschutzrechtlicher Sicht ergebenden kritischen Fragen hinreichend beantwortet.

Im Frühjahr 1994 hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder intensiv die Frage des Einsatzes maschinenlesbarer Patientenkarten mit medizinischen Daten diskutiert und einen Beschluß zu "Chipkarten im Gesundheitswesen" gefaßt (abgedruckt unter 31.). In dem Beschluß wird zunächst klargestellt, daß eine einmalige pauschale Entscheidung des Patienten für die Verwendung einer Patientenkarte mit medizinischen Daten datenschutzrechtlichen Standards nicht genügt, sondern sich die Entscheidungsfreiheit des Patienten auf jede Verwendung der Karte im Einzelfall beziehen muß. Die Freiwilligkeit der Entscheidung des Patienten für oder gegen eine Verwendung einer Patientenkarte muß gewährleistet sein. Ein faktischer Zwang widerspricht dem Prinzip der Freiwilligkeit. Eine Entscheidungsfreiheit des Betroffenen ist – darüber hinausgehend – nur dann tatsächlich gegeben, wenn die technische Ausgestaltung der Patientenkarte auch eine differenzierte Offenlegung der medizinischen Daten zuläßt, so daß der Patient die Möglichkeit hat, einem bestimmten Arzt bestimmte Daten zu offenbaren, die für den konkreten Behandlungskontext relevant sind, und er nicht zur pauschalen Offenlegung seiner Gesundheitsdaten gezwungen ist. Von diesem Ausgangspunkt aus haben die Datenschutzbeauftragten in ihrem Beschluß u.a. die folgenden Forderungen aufgestellt:

- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken.

Im Beschluß der Datenschutzbeauftragten des Bundes und der Länder werden zentrale Forderungen aufgestellt, die allerdings entsprechend der Weiterentwicklung der Kartenmodelle und ihrer jeweiligen Ziele und Funktionen der Differenzierung und Weiterentwicklung bedürfen werden. Grundsätzlich ist aus datenschutzrechtlicher Sicht zu fordern, daß der Patient bei Verwendung einer Patientenkarte zumindest nicht schlechter hinsichtlich seiner Rechte und Entscheidungsmöglichkeiten gestellt werden darf als ohne Verwendung einer Patientenkarte.

Von den Befürwortern der Einführung medizinischer Patientenkarten wird vielfach hervorgehoben, daß der Einsatz von Patientenkarten eine umfassendere Verwirklichung des Rechts des Patienten auf informationelle Selbstbestimmung mit sich bringt. Der Patient mit Patientenkarte wird als "Herr seiner Gesundheitsdaten" bezeichnet und die Patientenkarten als Beitrag zu einer "Demokratisierung des Gesundheitswesens" angesehen. Durch die bisher entwickelten Kartenmodelle ist eine solche Bewertung jedoch bisher keineswegs belegt. Es gibt vielmehr bereits Beispiele dafür, daß der Einsatz einer Patientenkarte zu einem Zugang zur pauschalen Offenlegung von Patientendaten führen kann. Dies hat etwa auch ein Beispiel einer Röntgenkarte gezeigt, die 1994 in einer hessischen Klinik im Bereich Unfallchirurgie/Orthopädie im Testbetrieb erprobt wurde. Auf dieser Röntgenkarte, die den Patienten zum Kauf angeboten wurde, wurden die persönlichen Daten des Patienten, die Röntgenbilder sowie Befundtexte dokumentiert. Die Patienten erhielten ein Merkblatt, in dem u.a. empfohlen wurde, Röntgenaufnahmen, die von anderen Kliniken bzw. niedergelassenen Ärzten – z. B. auch von Internisten, Gynäkologen etc. angefertigt wurden –, in die Klinik zu bringen, damit auch diese Daten auf der Röntgenkarte gespeichert werden. Unterschiedliche Zugriffsbereiche waren auf der Karte nicht vorhanden, so daß ein Patient, wenn er eine Röntgenkarte verwenden wollte, jedem Arzt alle Röntgendaten pauschal zur Verfügung stellen mußte, auch wenn diese zur konkreten Behandlung nicht erforderlich waren.

Der betroffenen Klinik habe ich mitgeteilt, daß ich gegen eine derartige pauschale Verwendung einer Röntgenkarte bei allen Fachärzten Bedenken habe. Inzwischen hat der Hersteller der Röntgenkarte mitgeteilt, daß er in diesem Punkt eine Veränderung seines Konzepts plant.

Die Erfahrungen der Datenschutzbeauftragten mit individuellen Einwilligungen der Bürger in die Verarbeitung personenbezogener Daten geben auch grundsätzlich Anlaß zur Skepsis. Vielfach hat der Bürger bei sog. "freiwilligen" Einwilligungen keine echte Alternative und kann auch als Einzelner die Modalitäten der Verarbeitung seiner Daten nicht selbst effektiv steuern. Als Beispiele seien hier die sog. "Schufa-Klausel" der Banken und die Schweigepflichtentbindungserklärung in den Aufnahmeverträgen privater Krankenversicherungen genannt. In beiden Fällen führte erst eine Intervention der Datenschutzbeauftragten zu einer für die betroffenen Bürger angemessenen Begrenzung der

Verarbeitung der personenbezogenen Daten. Es besteht kein Anlaß dazu, das Prinzip der Freiwilligkeit bei dem Einsatz von Patientenkarten als weniger problematisch anzusehen. Vielmehr ist davon auszugehen, daß sich der Patient, gerade auch der schwerwiegender erkrankte Patient, in einer schwierigen Situation befindet, die auch eine psychologische Abhängigkeit vom Arzt mit sich bringen kann. Die Frage der Freiwilligkeit der Patientenentscheidung wird daher der kritischen Aufmerksamkeit der Datenschutzbeauftragten bedürfen.

Insgesamt ist hervorzuheben, daß die Einführung von Patientenkarten vielfach mit Stichworten befürwortet wird, die einer genaueren Analyse nicht standhalten. Mit der Entwicklung von Patientenkarten werden unterschiedliche Ziele verfolgt, neben der Verbesserung der medizinischen Betreuung z.B. auch eine Kostenreduktion im Gesundheitsbereich, Wettbewerbsvorteile für einzelne Krankenkassen etc. Es bedarf daher künftig einer konkreteren Auseinandersetzung mit den Zielen, Funktionen, Einsatzmodalitäten und Vor- und Nachteilen für die informationelle Selbstbestimmung des Patienten hinsichtlich der verschiedenen Kartenmodelle, an denen ich mich auch weiterhin intensiv beteiligen werde.

5.4
Behinderung der Einsicht in eine Patientenakte im Universitätsklinikum Frankfurt

Im vergangenen Jahr hat sich eine Patientin an mich gewandt, nachdem sie vergeblich versucht hatte, Einsicht in ihre Krankenakte im Universitätsklinikum Frankfurt zu nehmen. Weder ihre persönliche Vorsprache noch mehrfache Telefongespräche in dieser Angelegenheit, bei denen sie vom Klinikum auch nach dem Grund für die gewünschte Akteneinsicht gefragt wurde, führten zum Erfolg. Zuletzt war ihr – fast drei Wochen nach der persönlichen Vorsprache im Universitätsklinikum – telefonisch mitgeteilt worden, die Akte müsse aus dem Archiv geholt werden, dies würde "jedoch seine Zeit dauern". In den Gesprächen hatte die Stationsärztin der Station, in der die Patientin behandelt worden war, ihr mitgeteilt, sie sei zu dem Behandlungszeitraum in einer anderen Station gewesen und deshalb für diesen Fall nicht zuständig.

Eine solche Verfahrensweise steht nicht im Einklang mit den gesetzlichen Vorschriften. Nach § 12 Abs. 5 HKG in Verbindung mit § 18 Abs. 1 HDSG steht jedem Patienten ein Recht auf Einsicht in seine Krankenakte zu. Der Angabe eines Grundes für die Akteneinsicht bedarf es nicht. Das Krankenhaus kann die Auskunft sowie die Einsichtnahme in die Krankenakte durch einen Arzt vermitteln lassen, soweit dies mit Rücksicht auf den Gesundheitszustand des Patienten dringend geboten ist. Auskunfts- und Einsichtsrecht des Patienten dürfen durch diese Vermittlung nicht beschränkt werden.

Für den Patienten ist die interne Organisation des Krankenhauses, insbesondere auch die Organisation der Archivierung der Krankenakten und der Entscheidungsbefugnisse der einzelnen Ärzte, im Regelfall nicht durchsichtig. Es muß für die Wahrnehmung des Rechts auf Akteneinsicht ausreichen, wenn er in einer der Abteilungen, in denen er behandelt wird bzw. wurde, mitteilt, daß er seine Krankenakte einsehen möchte. Diese Abteilung muß dann – soweit notwendig – die weitere Verfahrensweise abklären. Die Gewährung der Akteneinsicht muß auf jeden Fall alsbald erfolgen. Dies liegt zweifelsohne auch im Interesse des Krankenhauses selbst, da das Vertrauen des Patienten in die ordnungsgemäße Dokumentation sonst möglicherweise in Frage gestellt sein könnte. Falls im Einzelfall ausnahmsweise ein zwingender Grund für eine Verzögerung der Gewährung der Akteneinsicht vorliegen sollte, muß dem Patienten auf jeden Fall dieser Grund mitgeteilt werden.

Aufgrund der Eingabe habe ich dem Universitätsklinikum Frankfurt mitgeteilt, daß der Patientin nunmehr schnellstmöglich Einsicht in ihre Krankenakte gewährt werden muß. Darüber hinaus habe ich das Universitätsklinikum um Stellungnahme zu der geschilderten Verfahrensweise im konkreten Fall gebeten, ferner auch dazu, wie künftig das Verfahren bei der Einsichtnahme in Krankenakten durch Patienten so organisiert werden kann, daß Akteneinsicht komplikationslos und zeitnah gewährleistet ist.

Einige Tage nach meiner Anfrage beim Universitätsklinikum erhielt die Patientin Einsicht in die Krankenakte. Hierbei ergab sich allerdings ein weiteres Problem: Die Patientin hatte wegen der zuvor aufgetretenen Probleme nachgefragt, ob ihr die vollständigen Krankenunterlagen vorgelegt worden seien. Diese Frage wurde zwar bejaht, es wurde jedoch vom Universitätsklinikum abgelehnt, eine entsprechende schriftliche Bestätigung auszuhändigen. Als Begründung dieser Ablehnung wurde u.a. angeführt, daß

- die Krankenhausverwaltung die Unterlagen selbst nur von der zuständigen medizinischen Station erhalten habe, wo sie geführt und von dort aus auch archiviert würden und
- eine Rechtspflicht zu einer Unterzeichnung einer derartigen Bestätigung weder aus dem Hessischen Krankenhausgesetz noch aus dem Behandlungsvertrag hergeleitet werden könne.

Grundsätzlich verstehe ich, daß von einem Klinikum, in dem bei einer Reihe von Stellen personenbezogene Daten über Patienten gespeichert sind (z. B. auch im Labor, in der Krankenhausverwaltung etc.) nicht ohne weiteres bestätigt werden kann, daß außer den vorgelegten Krankenakten keine personenbezogenen Unterlagen existieren. In den meisten Fällen von Einsichtnahmen, mit denen meine Dienststelle befaßt war, war die Angelegenheit mit der Einsichtnahme in die Krankenakte ohnehin erledigt.

In diesem Fall wollte sich die Patientin jedoch ausdrücklich – aufgrund der vorher aufgetretenen und in der Verantwortung des Klinikums liegenden Umstände – über die vollständigen Krankenunterlagen informieren. Dann muß das Klinikum auch entsprechende Informationen zur Verfügung stellen, denn die Patientin hat ein Recht auf Einsichtnahme in sämtliche im Klinikum zu ihrer Person vorhandenen personenbezogenen Unterlagen. Das Vorgehen

des Klinikums ist mit Wortlaut und Zweck der genannten Regelungen zur Einsicht und Auskunft nicht vereinbar, die darauf abzielen, daß für die Patienten Transparenz hinsichtlich der Verarbeitung ihrer personenbezogenen Daten hergestellt wird. Dieses Ziel wird aber gerade nicht erreicht, wenn einer Patientin zwar Unterlagen vorgelegt werden, sie aber im unklaren darüber gelassen wird, ob und ggf. welche weiteren Unterlagen außerdem im Klinikum vorhanden sind. Ich hielt es daher für geboten, daß das Universitätsklinikum der Patientin eine Liste der vollständigen personenbezogenen Unterlagen im Klinikum erstellt.

Wie schon erwähnt, bin ich mir darüber im klaren, daß die Erstellung einer derartigen vollständigen Liste der personenbezogenen Unterlagen etwas Aufwand erfordert. Daß sich jedoch in diesem Fall die Frage der Vollständigkeit der Unterlagen in dieser Weise ergeben hat, ist eine Folge der Unklarheiten, die über Wochen im Klinikum verursacht wurden, und es ist durchaus nachvollziehbar, daß die Betroffene eine vollständige Aufklärung wünscht.

Ich habe das Klinikum außerdem darauf hingewiesen, daß es für die Gewährung der Akteneinsicht verantwortlich ist und klären muß, welche Unterlagen innerhalb des Klinikums vorhanden sind und wer im Auftrag des Klinikums der Betroffenen Einsicht gewährt. Es kann nicht akzeptiert werden, daß eine Stelle innerhalb des Klinikums die Unterlagen vorlegt und, da sie diese Unterlagen von einer anderen Stelle erhalten hat, keine Verantwortung für die Vollständigkeit der Akten übernehmen will.

5.5
Umsetzung des Hessischen Archivgesetzes im Universitätsklinikum Frankfurt

Im vergangenen Jahr erhielt ich eine Anfrage der Psychiatrischen Klinik des Universitätsklinikums Frankfurt. Die im Klinikum archivierte Krankenakte von Friedrich Edinger, die Informationen über Behandlungen in den Jahren 1937 und 1941 enthielt, sollte für wissenschaftliche Zwecke, u.a. auch für eine Ausstellung der Ludwig-Edinger-Stiftung in der Paulskirche vom 4. bis 18. September 1994 ausgewertet werden.

Es stellte sich heraus, daß die Krankenakte bereits zu Forschungszwecken zur Verfügung gestellt worden war, allerdings ohne daß ein formalisiertes und dokumentiertes Verfahren eingehalten worden war, so daß für mich nicht mehr nachvollziehbar war, wer nach welchen Kriterien aufgrund welcher Rechtsvorschriften eine solche Entscheidung getroffen hatte.

Daraufhin habe ich dem Universitätsklinikum mitgeteilt, daß ich zwar davon ausgehe, daß ein erhebliches öffentliches Interesse an den hier angesprochenen Forschungsarbeiten bestehe, ich jedoch gegen die derzeitige Verfahrensweise mit Archivgut im Universitätsklinikum rechtliche Bedenken hätte. Denn es handelt sich hier um sehr sensible Daten; die Unterlagen unterliegen der ärztlichen Schweigepflicht im Sinne von § 203 StGB, die grundsätzlich auch nach dem Tod der Betroffenen weiter gilt.

Die Verwendung der Patientenunterlagen zu Forschungszwecken einschließlich der Veröffentlichung der Forschungsergebnisse richtet sich nach dem neuen Hessischen Archivgesetz (HArchivG). Im einzelnen gilt folgendes:

§ 10 Abs. 1 HArchivG verpflichtet die öffentlichen Stellen, Unterlagen, die zur Aufgabenerfüllung nicht mehr erforderlich sind, unverzüglich auszusondern und dem zuständigen Archiv zur Übernahme anzubieten. Dies soll im Regelfall dreißig Jahre nach Entstehung der Unterlagen erfolgen. Für die der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts und ihre Vereinigungen bestimmt § 5 HArchivG, daß diejenigen Unterlagen, die nicht mehr benötigt werden, dem jeweils zuständigen Staatsarchiv zur Verwahrung anzubieten sind. Die Anbietungspflicht entfällt, wenn sie ein eigenes öffentliches Archiv unterhalten, das archivfachlichen Ansprüchen genügt und Zugang zu dem Archivgut entsprechend den gesetzlichen Bestimmungen ermöglicht, oder wenn die Unterlagen bei einer dazu geschaffenen Gemeinschaftseinrichtung archiviert werden. Für die Benutzung des öffentlichen Archivguts enthalten die §§ 14 ff. HArchivG Regelungen, die sicherstellen sollen, daß sowohl der Persönlichkeitsschutz als auch die Forschungsfreiheit möglichst weitgehend realisiert werden.

Nach diesen Bestimmungen hätten die Patientenunterlagen im konkreten Fall bereits an ein – universitätseigenes oder an ein anderes – öffentliches Archiv i. S. d. Archivgesetzes abgegeben werden müssen, weil sie für die Aufgabenerfüllung des Klinikums nicht mehr erforderlich waren. Die Universität Frankfurt hat jedoch bisher die archivrechtlichen Bestimmungen nicht umgesetzt, worauf ich bereits anläßlich einer Prüfung der Datenverarbeitung des Dekanats Fachbereich Wirtschaftswissenschaften im Jahr 1990 hingewiesen hatte.

Nach dem Hessischen Archivgesetz dürfen personenbezogene Unterlagen, die besonderen Geheimhaltungsvorschriften (hier: § 203 StGB) unterliegen, erst sechzig Jahre nach ihrer Entstehung genutzt werden (§ 15 Abs. 1 HArchivG). Beziehen sie sich auf eine natürliche Person, dürfen sie erst dreißig Jahre nach dem Tod der betroffenen Person durch Dritte benutzt werden. Ist der Todestag nicht festzustellen, endet die Schutzfrist 120 Jahre nach der Geburt der betroffenen Person (§ 15 Abs. 1 Satz 2 und 3 HArchivG).

Diese Schutzfristen können im Einzelfall verkürzt werden, wenn dies im öffentlichen Interesse liegt (§ 15 Abs. 4 Satz 1 HArchivG). Bei personenbezogenem Archivgut ist eine Verkürzung nur zulässig, wenn die Benutzung für ein bestimmtes Forschungsvorhaben erfolgt und schutzwürdige Belange der betroffenen Personen oder Dritter nicht beeinträchtigt werden oder wenn das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange erheblich überwiegt; soweit der Forschungszweck dies zuläßt, sind die Forschungsergebnisse ohne personenbezogene Angaben aus dem Archivgut zu veröffentlichen. Die Entscheidung über eine Verkürzung der Fristen trifft die archivführende Stelle nach Prüfung dieser Voraussetzungen.

Solange die archivrechtlichen Vorschriften von der Universität nicht umgesetzt sind, sind die im Archivgesetz enthaltenen Vorschriften über die Benutzung von öffentlichem Archivgut (§ 14ff.) entsprechend anzuwenden, denn die Tatsache, daß eine Umsetzung der Bestimmungen noch nicht erfolgt ist, darf weder zu Lasten derjenigen Personen gehen, deren personenbezogene Daten in den Unterlagen enthalten sind und deren Persönlichkeitsschutz durch die Vorschriften über die Benutzung von öffentlichem Archivgut sichergestellt wird, noch zu Lasten der Forschung. Eine solche konkrete Prüfung und Entscheidung ist jedoch hier nicht erfolgt. Ich sehe es als dringend notwendig an, daß nunmehr – fast fünf Jahre nach Verabschiedung des Hessischen Archivgesetzes – diese Bestimmungen umgesetzt werden. Insbesondere müssen Regelungen für die Benutzung des Archivguts festgelegt und sichergestellt werden, daß die gesetzlichen Voraussetzungen für die Benutzung des Archivguts in einem formalisierten und dokumentierten Verfahren von einer zuständigen Stelle geprüft werden. Ich habe vom Universitätsklinikum eine Stellungnahme zur weiteren Verfahrensweise angefordert.

5.6
Einsichtsrecht in die Krankenakte bei stationärer Psychotherapie

Im Krankenhaus wird eine Fülle sensibler Patientendaten verarbeitet, die besonders schutzwürdig sind.

Der Hessische Gesetzgeber hat daher auf meine Anregungen hin (vgl. 17. Tätigkeitsbericht, Ziff. 5.1) im Hessischen Krankenhausgesetz (HKHG) vom 18. Dezember 1989 (GVBl. I S. 452) bereichsspezifische Bestimmungen für die Verarbeitung von Patientendaten in Krankenhäusern verabschiedet. Die gesetzlichen Regelungen zum Datenschutz im Krankenhaus entsprechen den Vorgaben der Rechtsprechung des Bundesverfassungsgerichts im Volkszählungsurteil 1983.

Einer der zentralen datenschutzrechtlichen Forderungen zum Auskunftsrecht der Patienten hat der Gesetzgeber in § 12 Abs. 5 HKHG, entsprochen. Nach § 12 Abs. 1 HKHG gelten für Krankenhäuser grundsätzlich die Bestimmungen des Hessischen Datenschutzgesetzes. Über das Auskunftsrecht nach § 18 Abs. 1 HDSG hinaus bestimmt § 12 Abs. 5 HKHG aber, daß sich das Auskunftsrecht des Patienten auch auf die Empfänger von im Einzelfall oder gelegentlich übermittelten Daten erstreckt.

Neben dem Auskunftsanspruch hat der Patient ein Einsichtsrecht in die Krankenakte.

Einschränkungen des Auskunfts- und Einsichtsrechts enthalten § 18 Abs. 4 und 5 HDSG. Nach § 18 Abs. 4 HDSG ist die Einsichtnahme in Akten dann unzulässig, wenn die Daten des Betroffenen mit Daten Dritter derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist. In diesem Fall ist dem Betroffenen Auskunft nach § 18 Abs. 1 HDSG zu erteilen. Im übrigen kann ihm statt Einsicht Auskunft gewährt werden.

In § 18 Abs. 5 HDSG ist geregelt, daß die Rechte des Betroffenen auf Auskunft und Einsicht hinter dem öffentlichen Interesse an der Geheimhaltung oder an einem überwiegenden Geheimhaltungsinteresse Dritter zurücktreten müssen. Die Entscheidung darüber trifft der Leiter der speichernden Stelle. Werden Auskunft oder Einsicht nicht gewährt, ist der Betroffene unter Mitteilung der wesentlichen Gründe darauf hinzuweisen, daß er sich an den Hessischen Datenschutzbeauftragten wenden kann.

Die Frage, ob und in welchem Umfang ein überwiegendes Geheimhaltungsinteresse Dritter der Akteneinsicht des (ehemaligen) Patienten entgegensteht, führte in der Vergangenheit immer wieder zu Konflikten zwischen Ärzten und Patienten vor allem im Bereich der psychiatrischen bzw. psychotherapeutischen Behandlung.

In einem Fall teilte mir ein ehemaliger Patient, der eine freiwillige stationäre Psychotherapie in einem Psychiatrischen Krankenhaus durchgeführt hatte, in einer Eingabe mit, daß ihm bei Einsichtnahme in seine Krankenakte die komplette psychologische Anamnese des Arztes und Therapeuten sowie weitere anamnestische Aufzeichnungen nicht vorgelegt wurden. Das von mir zu der Problematik angeschriebene Psychiatrische Krankenhaus hat in einer ausführlichen Stellungnahme, die ich nachfolgend auszugsweise wiedergebe, seinen Standpunkt zur Verweigerung der Vorlage der vorgenannten Aktenteile an den ehemaligen Patienten überzeugend dargelegt.

Die Stellungnahme lautet:

"Wir verweigerten Herrn ... die Einsicht in die von ihm aufgeführten Aktenteile mit der Begründung, daß sie persönliche Ausführungen zu den sogenannten Gegenübertragungsgefühlen der Behandler enthalten, die wegen ihres subjektiven Charakters ausdrücklich als persönliche Aufzeichnungen der Behandler anzusehen und daher vor der Kenntnisnahme durch den Patienten zu schützen sind. Ohne einen derartigen Schutz betreffs der sich auf Gegenübertragungsgefühle beziehenden persönlichen Notizen der Behandler ist uns die Arbeit in unserem Fach der Psychotherapie nicht denkbar. Eine solche Haltung liegt daher in der Natur der Sache, d.h. sie ist eine conditio sine qua non für die Behandlungssituation an sich.

Zu dem bei uns angewandten psychoanalytisch orientierten Therapieverfahren gehört essentiell, die persönlichen Gefühle und Phantasien der Therapeuten, die sich aus der therapeutischen Beziehung zum Patienten in ihnen abbilden, gewissermaßen als Ausdruck der Übertragung des Patienten auf sie zu ergründen, zu benennen und in Bezug auf ihre Aussage zur Psychodynamik der therapeutischen Beziehung zu analysieren. Die sich aus diesem Prozeß der Analyse ergebende Sichtweise läßt sich nicht quasi naturwissenschaftlich distanziert objektivistisch beschreiben, sondern wird nur vollständig sein, wenn die subjektive Seite des Beziehungsverlaufes in ihr auch ihren Niederschlag findet. Eine fachgerechte Verlaufsbeschreibung wird deshalb immer eine Skizzierung der therapeutischen Beziehung sein müssen als zum Standard einer Psychotherapie gehörend. Anders als in der alten Psychiatrie,

in der scheinbar Behandler und Behandelte keine persönliche Behandlungsbeziehung haben, sondern sich durch unterschiedliche Rollen sehr strikt voneinander abheben.

Konflikte zwischen dem Recht des Patienten auf Akteneinsicht einerseits und dem Recht des Therapeuten auf Schutz seines persönlichen Anteils an der Behandlungsbeziehung andererseits, ist daher ohne Schaden an der Qualität der Behandlung und ihrer Dokumentation nicht einfach dadurch zu lösen, daß etwa verfügt würde, nur noch ojektivierende, d.h. justiziable Angaben gehörten in die Akten, was eine tendenzielle Rückkehr in die Zeiten der alten Verwahrpsychiatrie nahekäme, in der der aktenmäßig erfaßte ‚Krankheitsverlauf' fast ausschließlich vom äußeren, beobachtbaren Verhalten und der Beschreibung von auffälligen Symptomen handelte. Ein derartiges Zurückgehen in eine unpersönliche, distanzierte, ‚objektivistische' Beschreibung des Behandlungsprozesses kann nach dem Stand der Wissenschaft weder im Interesse des Patienten noch des Datenschutzes liegen. Es liegt daher in der Natur des psychotherapeutischen Arbeitens, daß auch der Behandler einen juristisch gesicherten Raum, seinen persönlichen Beziehungsanteil an der Therapie betreffend (vergleichbar dem Intimraum eines jeden in einer Partnerbeziehung) braucht, um fachgerecht arbeiten zu können."

Ich habe mich der Auffassung des Psychiatrischen Krankenhauses angeschlossen und den Betroffenen entsprechend unterrichtet.

6. Personalverwaltung

6.1
Prüfung der Personalaktenführung

6.1.1
Durchführung der Prüfungen

Im Laufe des letzten Jahres habe ich die Praxis der Personalaktenführung verschiedener Behörden geprüft. Gleichzeitig gaben auch mehrere Anfragen und Eingaben Anlaß, einzelne Personalakten unter datenschutzrechtlichen Gesichtspunkten durchzusehen.

Die Auswahl der zu prüfenden Behörden war zufällig. Geprüft habe ich die Personalverwaltungen unterschiedlich großer Behörden. Dazu gehörten der Hessische Rechnungshof, das Hessische Landesamt für Versorgung und Soziales, der Landeswohlfahrtsverband sowie die Kommunen Mühltal und Kriftel.

Im wesentlichen bezogen sich meine Prüfungen auf die folgenden Punkte:

a) Organisation der Personalverwaltungen
b) Inhalt der Personal- und Sachakten
c) Aufbewahrungsfristen.

6.1.2
Organisation der Personalverwaltungen

Die vertrauliche Behandlung von Personalakten und die Befolgung der Pflicht, Personalakten vor unbefugter Einsicht zu schützen, waren in der Vergangenheit bereits selbstverständliche Übung der personalverwaltenden Stellen. Mit dem "Gesetz zur Änderung dienstrechtlicher Vorschriften" vom 28. Oktober 1993 (GVBl. I S. 470) wurden diese Verpflichtungen in § 107 HBG aufgenommen. Neu ist auch die gesetzliche Festschreibung der strikten Zweckbindung der Personalaktendaten für Zwecke der Personalverwaltung oder der Personalwirtschaft in § 107 HBG.

Bei allen geprüften Stellen habe ich festgestellt, daß die erforderliche Abschottung der personalverwaltenden Stellen von der übrigen Verwaltung durchgehend vollzogen ist. Dies betrifft sowohl die Bearbeitung und die Aufbewahrung der laufenden und archivierten Akten wie die Behandlung der entsprechenden Unterlagen im Postgang. Die laufenden und archivierten Personalakten sind überall von den Aktenbeständen der übrigen Verwaltung getrennt. Zugang zu archivierten Personalakten haben grundsätzlich nur die hierfür zuständigen und autorisierten Mitarbeiter der jeweiligen Personalverwaltung.

Auch die aktuellen Personalaktenbestände der geprüften Behörden sind dem Zugriff und der Einsichtnahme durch Unbefugte entzogen. Die Personalakten werden ausnahmslos in verschließbaren Schränken aufbewahrt, die bei Dienstschluß verschlossen werden. Die Büros, in denen Personalakten aufbewahrt und bearbeitet werden, werden auch bei nur kurzer Abwesenheit verschlossen.

Bei allen Stellen wird die eingehende Post in Personalangelegenheiten (soweit dies auf dem Umschlag erkennbar ist) von den zentralen Poststellen ungeöffnet an die Personalabteilungen weitergeleitet. Die zu versendende Post in Personalangelegenheiten wird von den Personalsachbearbeitern kuvertiert und geht den Poststellen verschlossen zur Weiterleitung zu.

— Inhalt der Personal- und Sachakten

Entsprechend § 107 Abs. 2 HBG kann die Personalakte nach sachlichen Gesichtspunkten in Grundakte und Teilakten gegliedert werden. Bei den von mir geprüften Behörden werden zu folgenden Bereichen Teilakten geführt:

a) Unfall
b) Ausbildung
c) Vergütung und Besoldung
d) Nebentätigkeit
e) Abgeschlossene Arbeitsgerichtsverfahren
f) Disziplinarverfahren
g) Disziplinarvorgänge und solche Zurechtweisungen, Mahnungen oder Rügen, die nicht ausdrücklich als Disziplinarstrafen bezeichnet sind
h) Trennungsgeld und Fahrtkosten
i) Verwaltungshilfe Thüringen
j) Beihilfe
k) Versorgung
l) Krankheit, Urlaub, Sozialversicherung und sonstige Versicherungen.

Nicht immer werden die Unterlagen entsprechend diesen – von den Behörden selbst vorgenommenen – Unterteilungen abgelegt: Beim Rechnungshof war die Personalakte in mehrere Beihefte unterteilt. Die Gründe für das System der schon lange genutzten Unterteilung waren den jetzigen Mitarbeitern nicht bekannt. Sie wurden auch nicht immer konsequent durchgehalten.

Nicht überall gibt es schriftlich festgelegte, organisatorische Regelungen zur Bearbeitung und Führung von Personalakten. Soweit vorhanden, sind diese jedoch noch nicht an die neue Rechtslage angepaßt. Beim Landeswohlfahrtsverband bestehen zwar die ausführlichsten Regelungen, was jedoch nicht zwingend zu einer besseren Handhabung der Verwaltungsabläufe führt.

Gerade bei dieser Stelle werden neben den als Personalakten bezeichneten Unterlagen eine Fülle von als Sachakten bezeichneten Vorgängen geführt. Dies sind z. B.:

a) Mietzuschüsse an Mitarbeiter
b) Ausgabebelege für Geschenke aus Anlaß von Dienstjubiläen, Geburtstagen und Verabschiedungen
c) Aussagegenehmigungen
d) Beschäftigung von ausländischen Arbeitskräften
e) Befreiungsgesetze vom 5. März 1946
f) Büchergeld für Anwärter und Auszubildende
g) Amtsärztliche Untersuchung des Küchenpersonals
h) Schutzimpfungen der Mitarbeiter
i) Dienstaufsichtsbeschwerden.

Bei der Durchsicht verschiedener Sachakten ergab sich, daß hierin auch personenbezogene Mitarbeiterdaten verarbeitet wurden. So fanden sich z. B. in der Sachakte Aus- und Fortbildung Listen von Teilnehmern der Hessischen Verwaltungsseminare mit Name, Geburtsdatum, Art des Lehrgangs zurückgehend bis zum Jahre 1971. Es fand sich weiter ein Ordner mit Reisekostenabrechnungen aus den Jahren 1975 und 1976. Die Sachakte "Ausschreibungen und Eignungsprüfungen" enthielt für den Zeitraum von 1979 bis 1981 Prüfungsunterlagen von Bewerbern mit Name, Alter, Schulbildung und den Prüfungsnoten. Ein Ordner enthielt Schriftwechsel mit personenbezogenen Mitarbeiterdaten der Jahre 1942 bis 1993.

Beim Landeswohlfahrtsverband ist der Bestand, auch von an sich abgeschlossenen Akten, sehr groß. Auch die zuständigen Mitarbeiter hatten keinen vollständigen Überblick, was warum in welchen Vorgängen abgelegt war. In meinem Prüfbericht habe ich darauf hingewiesen, daß der Bestand an Sachakten entsprechend den gesetzlichen Vorgaben u.a. auf Einhaltung der Aufbewahrungsfristen zu überprüfen und zu bereinigen ist. Der Bestand an Sachakten ist jedoch nicht nur daraufhin durchzusehen, ob personenbezogene Unterlagen zu vernichten sind. Ich habe auch festgestellt, daß sich in einer Reihe von Sachakten Unterlagen befanden, die in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis liegen und in die laufenden Personalakten zu übernehmen sind.

– Aufbewahrungsfristen

Zu weitreichenden Konsequenzen und teilweise auch zu erheblichem Arbeitsaufwand führen die Vorschriften der §§ 107e und 107f HBG. Die Vorschriften regeln die Entfernung unbegründeter oder ungünstiger Inhalte sowie die Aufbewahrung von Personalakten.

Zum Zeitpunkt meiner Prüfungen im Mai und Juni 1994 hatten die personalverwaltenden Stellen noch keine Überlegungen angestellt, wie die gesetzlichen Vorgaben in die Praxis umzusetzen sind. Demzufolge befanden sich in den von mir stichprobenweise durchgesehenen Personalakten ohne Ausnahme Unterlagen, die nach den gesetzlichen Regelungen aus den Personalakten zu entfernen und zu vernichten sind. Dies betraf insbesondere Urlaubskarteien und Unterlagen über Krankmeldungen in den Personalakten, die weitaus älter als fünf Jahre waren. Zudem war an einer Stelle die Dienstanweisung "Aufbewahrungsfristen für Schriftgut im Personalwesen" der neuen Rechtslage nicht angepaßt.

– Unterlagen über Erkrankungen

Verschiedentlich habe ich festgestellt, daß bei Schwerbehinderten als Nachweis der Schwerbehinderteneigenschaft die Anerkennungsbescheide in die Personalakten aufgenommen wurden. Die Anerkennungsbescheide enthalten jedoch

auch Daten, die für eine Personalakte nicht relevant sind, u.a. Aussagen über Erkrankungen – auch solcher, die bei der Feststellung des Grades der Schwerbehinderung nicht berücksichtigt werden konnten.

Entsprechend § 107f Abs. 2 Satz 2 HBG sind Unterlagen, aus denen die Art einer Erkrankung ersichtlich ist, unverzüglich zurückzugeben, wenn sie für den Zweck, zu dem sie vorgelegt worden sind, nicht mehr benötigt werden. Diese Vorschrift bedeutet für die personalverwaltenden Stellen, daß der Bestand an Personalakten daraufhin durchzusehen ist, ob sich Unterlagen in den Personalakten befinden, aus denen die Art einer Erkrankung ersichtlich ist. Diese Unterlagen sind nicht aus den Personalakten zu entfernen und zu vernichten, sondern den Betroffenen zurückzugeben.

Beim Landesamt für Versorgung und Soziales befand sich in den Personalakten älterer Bediensteter, vor allem im Zusammenhang mit Einstellungsuntersuchungen, eine Fülle von ärztlichen Unterlagen. Hier habe ich empfohlen, die Akten entsprechend zu bereinigen, so daß der Inhalt der Personalakten in diesen Fällen denen der Beschäftigten entspricht, für die aufgrund der jetzigen Rechtslage bei der Einstellungsuntersuchung nur noch das Ergebnis ("geeignet" oder "nicht geeignet") enthalten ist. Auch hier sollte darauf geachtet werden, daß Gutachten und ähnliche Unterlagen in verschlossenen Umschlägen aufbewahrt werden.

– Akteneinsicht

Unterschiedliche Regelungen habe ich zur Handhabung des Rechts auf Akteneinsicht festgestellt. Bei drei der geprüften Behörden mußte die Akteneinsicht schriftlich beantragt werden. Die Bitte der Bediensteten auf Gewährung von Akteneinsicht (bei einer Stelle wird ein Vordruck benutzt) wurde in die Personalakte abgeheftet.

Diese Praxis ist nicht zulässig; die Tatsache, daß ein Bediensteter seine Personalakte eingesehen hat, ist für zukünftige Entscheidungen nicht relevant. Nach den Vorschriften des Hessischen Beamtengesetzes ist zudem nicht zwingend ein schriftlicher Antrag erforderlich. Auf keinen Fall ist ein solcher Antrag Bestandteil der Personalakte.

Die Behörden habe ich in meinen Prüfberichten auf die Rechtslage hingewiesen. Bisher hat mir allerdings erst eine Stelle mitgeteilt, daß zukünftig die Anträge auf Akteneinsicht zurückgegeben und in den Personalakten vorhandene Unterlagen zur Akteneinsicht im Zuge der Bereinigung der Personalakten entfernt werden.

6.1.3
Inhalt der Personalakten

Personalverwaltung ist in vielen Bereichen ein sehr umfangreiches Gebiet mit großem, gleichartigem Arbeitsanfall bzw. mit geregelten Abläufen. Andererseits ist zu bedenken, daß Personalakten über einen langen Zeitraum geführt werden und daß sie die Betroffenen ggf. auch durch mehrere Dienststellen begleiten. Dabei ist der Einfluß der Betroffenen auf den Inhalt ihrer eigenen Personalakten eher gering. Bei meiner Prüfung habe ich unter anderem folgendes festgestellt:

– Häufig befanden sich Vorgänge in den Personalakten, die – etwa bei Beförderungsentscheidungen, aber auch bei Mitteilungen über eine Erweiterung der Zeichnungsberechtigung – die Namen weiterer Bediensteter enthielten. Beim Landeswohlfahrtsverband beispielsweise wurde bei einem Mitarbeiter, der früher in einer Klinik beschäftigt war, eine Personalliste mit 40 weiteren Beschäftigten dieser Klinik in der Personalakte aufbewahrt. Hier ist es dringend erforderlich, die entsprechenden Unterlagen so zu bereinigen, daß die Namen der anderen Beschäftigten nicht mehr kenntlich sind.

– Beim Rechnungshof wurde eine Teilakte – Unfallakte – gefunden, die sich auf einen Unfall mit einem Dienstwagen bezog. In dieser Akte war ein Strafurteil aus dem Jahre 1986 gegen den Bediensteten enthalten. Die Dienststelle hatte entschieden, von einem Schadenersatzanspruch abzusehen. Nach § 107e Abs. 2 HBG sind Mitteilungen in Strafsachen – soweit sie nicht Bestandteil einer Disziplinarakte sind – mit Zustimmung des Bediensteten nach drei Jahren zu vernichten.

– Beim Rechnungshof befanden sich außerdem teilweise Unterlagen in den Akten, die nicht Gegenstand einer Personalakte sein können, etwa die Kopie eines Tagungsbeitrags, den ein Mitarbeiter auf einem Kongreß gehalten hatte; oder ein Anschreiben der Frauenbeauftragten an alle Kolleginnen, in dem sie sich wegen Antritts des Erziehungsurlaubs verabschiedet hatte.

– Personalakten können sehr alt werden. Die besondere Brisanz zeigt sich in einem Fall des Landeswohlfahrtsverbands: Es handelte sich um eine Akte, die noch bis Ende des Jahres 1994 aufzubewahren war. Die Akte des ehemaligen Bediensteten, der im Jahre 1905 geboren wurde, begann im Jahre 1926, dem Zeitpunkt der Einstellung des Bediensteten bei der damaligen Nassauischen Brandkasse in Wiesbaden. In der Akte befanden sich u.a. ein Lebenslauf vom Mai 1926, ein Fragebogen zur Durchführung des Gesetzes zur Wiederherstellung des Berufsbeamtentums vom April 1933, eine Erklärung wegen der Zugehörigkeit zur SPD vom August 1933 sowie ein Meldebogen nach dem Gesetz zur Befreiung von Nationalsozialismus und Militarismus aus dem Jahre 1946. In der Akte befand sich auch ein Schreiben des Bediensteten aus dem Jahre 1932, in dem er seinen Dienststellenleiter handschriftlich und untertänigst um Gewährung von einem Tag unbezahltem Sonderurlaub bat.

– Von einer Lehrerin wurde ich gebeten, ihre beim Regierungspräsidium Darmstadt geführte Personalakte einzusehen. Die Durchsicht der Akten fand im Juli 1994 statt. Auch hier habe ich festgestellt, daß die Neuregelungen des Hessischen Beamtengesetzes nicht zu Konsequenzen geführt hatten. In den Akten befanden sich Belege über Erkrankungen der Lehrerin zurückgehend bis auf das Jahr 1976. Die Akte enthielt weiter eine Reihe von Unterlagen mit für die Betroffene ungünstigen Inhalten i. S. v. § 107e HBG. Aufgenommen in die Personalakte

wurde auch ein "Merkblatt über psychische Behinderungen im Zusammenhang mit Arbeitsbedingungen". Es war aus der Akte nicht ersichtlich, in welchem Zusammenhang dieses Merkblatt aufgenommen wurde. In meinem Brief an das Regierungspräsidium habe ich gebeten, diese Unterlage sofort aus der Akte zu entfernen.

Auch eine weitere Reihe von Unterlagen, die sich in der Personalakte befanden, standen nicht in einem unmittelbaren Zusammenhang mit dem Dienstverhältnis und sollten in einer Sachakte abgelegt werden. Dies betraf insbesondere den Schriftwechsel des Regierungspräsidiums mit dem Rechtsanwalt der Beamtin zur Akteneinsicht sowie Kopien des von mir mit dem Staatlichen Schulamt geführten Schriftwechsel zu datenschutzrechtlichen Fragen. Auch die Rechnung zur Erstellung eines Gutachtens zur Frage der Dienstfähigkeit der Beamtin gehört nicht in die Personalakte. Zu den vorgenannten und weiteren Punkten habe ich empfohlen, eine Bereinigung der Personalakte durchzuführen Das Regierungspräsidium hat mir allerdings mitgeteilt, daß die Akte an ein Verwaltungsgericht abgegeben wurde und aus diesem Grund eine Bereinigung nicht möglich war. Ich hatte erwartet, daß die Bereinigung der Akte vor der Weitergabe an Dritte erfolgt. Ich habe das Regierungspräsidium daher nochmals um Stellungnahme zu dem Sachverhalt gebeten.

- Beim Landeswohlfahrtsverband habe ich auch Akten von Mitarbeitern, die bei der Dienststelle ausgeschieden und zu anderen Dienststellen gewechselt waren, gefunden. Vor Abgabe der Originalpersonalakten an die neuen Dienststellen wurden jeweils die kompletten Personalakten fotokopiert. Nach dem Hessischen Beamtengesetz darf aber jeweils nur eine Personalakte zu einem Mitarbeiter geführt werden. Bei den fotokopierten und abgegebenen Personalakten handelt es sich um weitere Personalakten, über deren Existenz die Betroffenen nicht informiert sind und deren Führung nicht zulässig ist. Ich habe die Dienststelle aufgefordert, die fotokopierten Personalakten auszusondern und zu vernichten.

6.1.4
Konsequenzen der Prüfungen

In meinen Prüfberichten habe ich die betroffenen Behörden über meine Feststellungen unterrichtet und um Stellungnahme gebeten. Gleichzeitig wurden sie aufgefordert, mir die Konzepte zur Umsetzung der Aktenbereinigung bzw. Änderung der Verwaltungspraxis und den dafür vorgesehenen Zeitrahmen mitzuteilen. Die Bereinigung kann während der laufenden Bearbeitung erledigt werden. Die vollständige Bereinigung hat hierbei jedoch in einem angemessenen Zeitraum zu erfolgen. Bevor eine Akte an eine andere Stelle weitergegeben wird, sollte auf jeden Fall eine Kontrolle durchgeführt werden.

Der Rechnungshof hat angekündigt, er wolle mit seiner Stellungnahme zu meinem Prüfbericht auf die Neufassung der Verwaltungsvorschriften zum Hessischen Beamtengesetz warten. Die anderen Behörden haben inzwischen die entsprechenden Konzepte erarbeitet bzw. sind dabei, die Ergebnisse der Prüfung umzusetzen.

Als allgemeines Ergebnis ist festzustellen, daß anscheinend die Neuregelungen nur sehr begrenzt die personalaktenführenden Behörden dazu angeregt haben, ihre Verfahrensweise zu überprüfen. Zum Teil ist die Verwaltung offensichtlich gar nicht über die Änderungen informiert. So wurde meinen Mitarbeitern bei einer Behörde, wo sie eine einzelne Akte einsehen wollten, als aktuelles Gesetz ein Text mit Stand 1989 vorgelegt. Teilweise wollen Behörden auch Verwaltungsvorschriften oder andere Anweisungen des Hessischen Ministeriums des Inneren abwarten. Dazu liegt inzwischen ein Entwurf vor. In diesem werden sowohl zum Inhalt der Personalakten als auch zu den organisatorischen Fragen Erläuterungen gegeben. Der Entwurf enthält auch eine Regelung zu Art und Frist für die durch die gesetzlichen Änderungen notwendigen Bereinigungen von Personalakten. Wann dieser Erlaß in Kraft tritt, ist freilich derzeit noch nicht abzusehen.

6.2
Weitergabe von Mitarbeiterdaten

Eine Anfrage des Personalrates eines nordhessischen Kreises gab erneut Anlaß klarzustellen, daß auch gegenüber anderen Behörden nicht unbegrenzt Daten der Mitarbeiter weitergegeben werden können. Der Anlaß war ein organisatorisches Problem innerhalb der Verwaltung.

Das Jugendamt ist nach den Vorgaben des SGB VIII verpflichtet, Kinder und Jugendliche, die von der Polizei aufgegriffen werden, in seine Obhut zu nehmen und für eine geeignete Unterbringung zu sorgen (§ 42 SGB VIII). Um dies auch außerhalb der normalen Dienstzeiten des Jugendamts zu ermöglichen, stellte das Amt der Polizeidirektion eine Liste aller Sachbearbeiter mit den privaten Telefonnummern der Ansprechpartner zur Verfügung. Es begründete sein Verhalten damit, daß es nur offenkundige Daten und diese auch nur zum Behördengebrauch weitergegeben habe. Im Anschreiben an die Polizei war der Satz enthalten: "Diese Daten dürfen nicht an Dritte weitergegeben werden".

Diese Vorgehensweise entsprach nicht den Vorgaben der Datenschutzregelungen. Daten der Beschäftigten dürfen nur dann an andere Behörden weitergegeben werden, wenn eine Rechtsvorschrift dies vorsieht oder der Dienstverkehr diese Übermittlung erfordert. An den Begriff der Erforderlichkeit sind strenge Maßstäbe anzulegen. Es reicht nicht aus, daß die Übermittlung nützlich ist, sondern sie ist nur zulässig, wenn es ansonsten für die Verwaltung unmöglich ist, ihre Aufgaben zu erfüllen. In unserem Fall sind jedoch andere Lösungen denkbar. Ganz abgesehen davon, daß ich keine Informationen darüber erhalten habe, wie häufig ein solches Eingreifen des Jugendamts außerhalb der üblichen Bürozeiten überhaupt notwendig ist: Auch für andere Bereiche gibt es Notfallisten und Regelungen, wann und wo auf sie zugegriffen werden kann. Dann fände die Übermittlung nur in dem Einzelfall statt, in dem die Information durch die Polizei wirklich benötigt wird.

– § 67c Abs. 3 SGB X stellt klar, daß es keine Zweckänderung ist, wenn Sozialdaten für Aufsichts- und Kontrollzwecke oder auch zur Durchführung von Rechnungsprüfungen verwandt werden.

– § 81 Abs. 4 S. 4 SGB X legt fest, daß für die Registerführung sowie die Bestellung eines Datenschutzbeauftragten die Regelungen des jeweiligen Landesrechts entscheidend sind. Das Hessische Datenschutzgesetz schreibt vor, daß jede datenverarbeitende Stelle einen Datenschutzbeauftragten zu bestellen hat (§ 5 Abs. 2 HDSG). Da die hessischen Kommunen ohnehin einen Datenschutzbeauftragten bestellt haben, halte ich eine besondere Bestellung für den Bereich des Sozialdatenschutzes nicht für erforderlich. Hier besteht ein Unterschied zur bisherigen Rechtslage, nach der die Bestellung einmal nach dem Hessischen Datenschutzgesetz und einmal nach den Vorschriften des Bundesdatenschutzgesetzes (für den privaten Bereich) erfolgen mußte. Das Hessische Datenschutzgesetz schließt die Möglichkeit, zwei Datenschutzbeauftragte zu bestellen, aber auch nicht aus.

§ 67d Abs. 3 SGB X enthält eine Regelung zur Übermittlung von Sozialdaten aus Akten. Sind mit den Daten, die übermittelt werden dürfen, weitere personenbezogene Daten des Betroffenen in Akten so verbunden, daß eine Trennung nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, darf eine Übermittlung nur erfolgen, wenn schutzwürdige Interessen des Betroffenen nicht verletzt werden; die Veränderung und Nutzung dieser Daten ist unzulässig. Dies sollte zur Konsequenz haben, daß in Zukunft, etwa nach einem Wohnortwechsel, noch sorgfältiger überlegt wird, welche Daten wirklich von anderen Sozialleistungsträgern benötigt werden. Diese Regelung kann nicht damit umgangen werden, daß vom Betroffenen verlangt wird, er solle in die Übersendung der vollständigen Akte einwilligen; eine Einwilligung im Rahmen der Mitwirkungspflicht muß er nur für "erforderliche" Daten abgeben.

§ 68 SGB X, die Amtshilferegelung, hat erhebliche Änderungen erfahren. Der Kreis der Behörden, die im Rahmen der Amtshilfe Daten erhalten können, wurde eingeschränkt. Amtshilfe kann noch gewährt werden zur Durchsetzung öffentlich-rechtlicher Ansprüche von mindestens 1.000,– DM. Aus anderen Gründen können jetzt nur noch Strafverfolgungsbehörden, Gerichte, Justizvollzugsanstalten und Gefahrenabwehrbehörden Daten entsprechend dem bisherigen Datenkatalog erhalten. Dabeiist zu berücksichtigen, daß § 78 Abs. 1 S. 4 SGB X die Zweckbindung im Rahmen der Strafverfolgung und Gefahrenabwehr aufhebt bzw. einschränkt. Es ist nicht ausgeschlossen, daß sich dadurch gerade im Bereich der Jugendhilfe Probleme ergeben könnten. Die Arbeit der Jugendhilfe ist in weiten Bereichen auf das Vertrauen der Jugendlichen zu den Mitarbeitern, die sie betreuen, angewiesen. Nicht immer unterliegen aber deren Informationen dem besonderen Schutz des § 65 SGB VIII. Hier gilt es, die Auswirkungen aufmerksam zu beobachten.

Mit § 78 Abs. 1 SGB X wurde die Zweckbindung im Bereich des Sozialdatenschutzes endlich auch auf gerichtliche Entscheidungen ausgedehnt. Sind Sozialdaten an Gerichte oder Staatsanwaltschaften übermittelt worden, dürfen diese gerichtliche Entscheidungen, die Sozialdaten enthalten, weiter übermitteln, wenn ein Sozialleistungsträger zur Übermittlung an den weiteren Empfänger befugt wäre. Auch hier wird es für die Praxis, gerade auch der Gerichte, erhebliche Auswirkungen geben.

§ 73 SGB X, der die Übermittlung von Sozialdaten für die Durchführung eines Strafverfahrens regelt, trifft keine Unterscheidung mehr nach Verbrechen und Vergehen. Die Übermittlung ist jetzt auch zulässig, wenn kein Verbrechen, sondern eine "Straftat von erheblicher Bedeutung" verfolgt werden soll. Dies kann vor allem im Bereich von Kindesmißhandlungen usw. eine Rolle spielen, da aufgrund dieser Regelung die Vorlage der gesamten Akte des Beschuldigten verlangt werden kann.

Die Regelung der Amtspflegschaft in § 68 SGB VIII wurde ebenfalls geändert. Sie verdeutlicht jetzt die Rechte und Pflichten des Amtspflegers: Er darf Sozialdaten erheben, soweit dies zur Erfüllung seiner Aufgaben erforderlich ist. Damit erhalten aber andere Stellen, die an das Sozialgeheimnis gebunden sind, keine Übermittlungsbefugnis.

§ 56 Abs. 1 S. 1 SGB VIII legt ausdrücklich fest, daß – soweit das SGB VIII keine Sonderregelungen enthält – der Amtsvormund auf Grundlage des Bürgerlichen Gesetzbuchs handelt, also nicht in Ausübung eines öffentlichen Amts.

§ 65 SGB VIII stellt jetzt klar, daß in den Fällen, in denen ein Sozialarbeiter befugt Daten (innerhalb) des Amts weitergibt, der Empfänger an den Übermittlungszweck gebunden ist. Dies könnte eine Hilfestellung für die Praxis sein.

Außerdem ergibt sich durch den Verweis auf § 35 Abs. 3 SGB I, daß auch die Weitergabe von Unterlagen usw. eingeschränkt ist, mit der Folge, daß beispielsweise kein Einsichtsrecht durch Vorgesetzte besteht, wenn der Sozialarbeiter nicht zur Weitergabe befugt ist.

Ich werde die Auswirkungen dieser Änderungen auf die Praxis weiter beobachten.

7.2
Datenverarbeitung beim Hessischen Amt für Versorgung und Soziales in Wiesbaden

In der hessischen Versorgungsverwaltung werden ganz überwiegend Akten mit medizinischen Inhalten geführt und bearbeitet, da zu den Aufgaben der Versorgungsverwaltung u.a. die Durchführung des Bundesversorgungsgesetzes und die Feststellung von Behinderungen nach dem Schwerbehindertengesetz gehören.

Mit diesen Aufgabenbereichen zählen die Hessischen Ämter für Versorgung und Soziales zu den Sozialleistungsträgern, für welche die Vorschriften des Sozialgesetzbuches zum Sozialgeheimnis (§ 35 SGB I) und den Übermittlungsbe-

fugnissen (§ 67 ff. SGB X) gelten. Die Wahrung des Sozialgeheimnisses hat auch zur Voraussetzung, daß technische und organisatorische Maßnahmen von den jeweiligen Sozialleistungsträgern getroffen werden müssen, die einen größtmöglichen Schutz der Sozialdaten gewährleisten.

§ 38 Abs. 4 "Allgemeine Geschäftsordnung für die Versorgungsverwaltung des Landes Hessen" vom 8. Juni 1993 (StAnz S. 1723) bestimmt daher:

> "Akten sind in allen Bereichen der Dienststelle grundsätzlich so aufzubewahren, daß sie Unbefugten nicht zugänglich sind und auch während der Dienstzeit der Datenschutz gewährleistet ist."

Ob diese Vorgabe auch vom Amt für Versorgung und Soziales in Wiesbaden eingehalten wird, davon wollte ich mich im Juli 1994 überzeugen.

Das Amt für Versorgung und Soziales ist auf mehrere Halbstockwerke eines Gebäudes, in dem sich außerdem noch mehrere Firmen befinden, verteilt. Die Haupteingangstür ist bis 15.00 Uhr geöffnet, aber auch später ist das Betreten des Gebäudes noch möglich, indem man abwartet, bis jemand das Haus verläßt. Im Erdgeschoß befindet sich die Anmeldung. Die weiteren Etagen der Dienststelle können unter Umgehung der Anmeldung über das Treppenhaus oder den Fahrstuhl erreicht werden.

Bei meinem Rundgang mußte ich feststellen, daß einige Bürotüren geöffnet und die Zimmer nicht besetzt waren. In den Büros lagerten stapelweise Versorgungsakten offen auf den Schreibtischen, dem Boden und in einfachen offenen Holzregalen. Auch in nicht mehr besetzten Arztzimmern, deren Türen ebenfalls offen standen, lagerten Versorgungsakten in offenen Holzregalen und auf den Schreibtischen.

Ich habe weiter festgestellt, daß zwar das Geschäftszimmer der Verwaltungsabteilung der Dienststelle bzw. das Vorzimmer des Dienststellenleiters mit modernen abschließbaren Schränken ausgestattet sind, keiner der Schränke jedoch abgeschlossen war.

In meinem Prüfbericht habe ich aufgrund der festgestellten gravierenden Mängel gefordert, daß umgehend Maßnahmen getroffen werden, die den Zugriff Unbefugter auf Akten und sonstige Unterlagen verhindern. Als sofortige Sicherungsmaßnahmen habe ich empfohlen, in einer Dienstanweisung zu regeln, daß die Bediensteten nach Verlassen der Büros diese zu verschließen haben. Außerdem ist der Einsatz des Reinigungspersonals zu regeln, so daß die Reinigungskräfte keinen Zugriff auf die Akten bekommen.

Das Amt für Versorgung und Soziales hat sehr schnell reagiert. Zu den getroffenen Sofortmaßnahmen gehört, daß in einer Hausmitteilung der Dienststelle alle Bediensteten auf die Beachtung des Datenschutzes hingewiesen wurden. Die Bediensteten wurden aufgefordert, ihre Zimmer auch bei nur kurzfristigem Verlassen abzuschließen. Zur Aufbewahrung der Büroschlüssel wurden Regelungen getroffen, die die Benutzung durch Unbefugte verhindern. In diesem Zusammenhang ist darauf hinzuweisen, daß zu den Unbefugten auch die Mitarbeiter gehören, die nicht in den jeweiligen Dienstzimmern beschäftigt sind. Die Reinigungskräfte dürfen grundsätzlich nur dann in die Büros gehen, wenn sich noch Bedienstete darin aufhalten.

Für weitergehende Maßnahmen, insbesondere Regelungen der Zugangssicherung, wurde ein Konzept erarbeitet, das wegen fehlender Haushaltsmittel jedoch nicht sofort umgesetzt werden kann.

Ob und in welchem Umfang die vom Amt für Versorgung und Soziales in seiner Stellungnahme beschriebenen Sofortmaßnahmen Wirkung zeigten, habe ich in einem weiteren unangekündigten Besuch überprüft. Es war erfreulich festzustellen, daß die bei meinem ersten Besuch vorhandenen Mängel beseitigt waren. Die in der Hausmitteilung festgelegten Datensicherungsmaßnahmen wurden beachtet.

7.3
Verwendungsnachweise für private Kinderbetreuungseinrichtungen

Eine privat geführte Krabbelstube in Frankfurt hatte sich mit der Frage an mich gewandt, welche Daten vom städtischen Jugendamt im Zusammenhang mit der Gewährung von "Betriebskostenzuschüssen" erhoben werden dürfen. Der Eingabe lag folgender Sachverhalt zugrunde:

Die Stadt Frankfurt unterstützt die selbstorganisierte Förderung von Kindern in Tageseinrichtungen – Krabbelstuben, Kinderläden und Schülerläden – durch Zahlung von "Betriebskostenzuschüssen" einerseits und durch Übernahme von Elternbeiträgen aus Jugendhilfemitteln im Rahmen der Einzelfallhilfe andererseits.

Für die Beantragung der Gewährung einer städtischen Zuwendung durch eine Einrichtung ist von der Einrichtung ein Vordrucksatz auszufüllen und dem Jugendamt zur Prüfung und Entscheidung vorzulegen. Bestandteile des Vordrucksatzes sind unter anderem eine Liste der in der Einrichtung angemeldeten Kinder sowie eine Liste zu den Personalausgaben.

Auf der Liste der angemeldeten Kinder erscheinen der Name der Kinder, ihr Wohnort und das Geburtsdatum. Die Liste der Personalausgaben enthält Name, Vorname, Tätigkeit und Tarifgruppe, Vergütung monatlich und die Jahresvergütung aller hauptamtlich Beschäftigten einer Einrichtung. Zusätzlich verlangt die Stadt die Vorlage der mit den Beschäftigten abgeschlossenen Arbeitsverträge.

Die Datenerhebungen basieren auf den "Grundsätzen für die Verwendung der Zuwendungen sowie für den Nachweis und die Prüfung der Verwendung (allgemeine Bewirtschaftungsgrundsätze – ABewGr)". Die Stadt Frankfurt hat die listenmäßige Erhebung von Daten von Kindern in Betreuungseinrichtungen zunächst damit begründet, daß Grundlage für die Berechnung und Bewilligung der Betriebskostenzuschüsse an die Einrichtungen die Anzahl der

angemeldeten Kinder mit Wohnsitz Frankfurt am Main darstelle. Daß die Zuwendungen an Einrichtungen von dem Kriterium "Wohnort Frankfurt" abhängig gemacht werden, ist selbstverständlich zulässig und muß auch im Rahmen der Rechnungsprüfung nachprüfbar sein.

Anders zu beurteilen ist die Argumentation der Stadt Frankfurt im Hinblick auf die Rechtsgrundlagen der Datenerhebungen. Das städtische Jugendamt hat mir hierzu mitgeteilt, daß die Datenerhebung im Rahmen der Aufgabenerfüllung nach dem Sozialgesetzbuch VIII beim Trägerverein beziehungsweise bei einzelnen Einrichtungen erfolgt, weil die Erhebung bei den Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden (§ 62 Abs. 3 Nr. 3 SGB VIII). Dieser Argumentation habe ich widersprochen.

Die Betroffenen, über die hier Daten erhoben werden, sind nicht zugleich Leistungsberechtigte oder sonst an der Leistung Beteiligte i. S. v. § 62 Abs. 4 SGB VIII. Bei dem von der Stadt Frankfurt gewählten Weg wird die einzelne Einrichtung durch städtische Zuschüsse gefördert und nicht das jeweils in der Einrichtung befindliche Kind. Daher dürften die Daten unmittelbar bei den leistungsberechtigten Einrichtungen erhoben werden, wenn sie für die Gewährung der Fördermittel notwendig sind (§ 62 Abs. 4 SGB VIII). Eine regelmäßige listenmäßige Überlassung der Angaben über alle Kinder, die eine entsprechende Einrichtung besuchen, ist für diesen Zweck aber gerade nicht notwendig. Ausreichend ist, wenn eine Prüfung des Merkmals "Wohnort Frankfurt" bei Bedarf durch Einsicht in die Unterlagen erfolgen kann.

Auch der von der Stadt Frankfurt angeführte § 62 Abs. 3 Nr. 3 SGB VIII führt hier zu keinem anderen Ergebnis. Nach dieser Vorschrift können personenbezogene Daten ohne Mitwirkung des Betroffenen erhoben werden, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern würde und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden. Aber auch in diesem Fall gilt der Grundsatz, daß ausschließlich die zur Aufgabenerfüllung erforderlichen Daten übermittelt werden dürfen.

Das Jugendamt hat zwar seine Bedenken gegen eine Veränderung des bisher von ihm praktizierten Verfahrens aufrecht erhalten, sich aber dennoch entschlossen, künftig auf die Vorlage von Listen aller Kinder, welche die jeweilige Einrichtung besuchen, zu verzichten. Stattdessen läßt sich das Jugendamt von den Trägern der Einrichtungen schriftlich bestätigen, daß Betriebskostenzuschüsse nur für Frankfurter Kinder beantragt werden. Das Jugendamt prüft diese Angaben stichprobenhaft durch Einsichtnahme in die Unterlagen bei den einzelnen Trägern. Gegen diese Verfahrensweise bestehen keine datenschutzrechtlichen Bedenken.

Etwas anders zu beurteilen ist die Rechtslage für die Beschäftigten in den geförderten Einrichtungen. Rechtsgrundlage für eine Übermittlung der angeforderten Daten durch die Träger der Einrichtungen als Arbeitgeber an die Stadt Frankfurt ist hier § 28 BDSG (beziehungsweise entsprechende andere datenschutzrechtliche Regelungen, soweit sie auf die Träger – etwa kirchliche Einrichtungen – anwendbar sind). Die Übermittlung von Beschäftigtendaten ist zulässig, da die Arbeitsverhältnisse davon abhängig sind, daß eine Förderung durch die Stadt erfolgt. Die Förderung der Stadt kann nur gewährt werden, wenn die entsprechende Qualifikation des Betreuungspersonals nachgewiesen wird. Ein Qualifikationsnachweis – etwa durch die Vorlage entsprechender Zeugnisse – erscheint mir notwendig. Die Höhe der Vergütung für die einzelnen Beschäftigten ist jedoch nur dann relevant, wenn die Förderrichtlinien eine entsprechende Förderung bezogen auf die tatsächliche Leistung an den einzelnen Stelleninhaber vorsehen.

Diese Rechtsauffassung hat sich das Jugendamt insoweit zueigen gemacht, als künftig auf die Vorlage von Arbeitsverträgen der Beschäftigten verzichtet wird. Es werden jedoch weiterhin neben der Qualifikation Angaben zur Vergütung verlangt, weil diese in den Fällen, in denen das Jugendamt den Elternbeitrag für die Kinderbetreuungseinrichtung ganz oder teilweise übernimmt, als ein Kostenfaktor in die Berechnungen des Jugendamts einfließen.

Auch dieses Verfahren ist unter datenschutzrechtlichen Gesichtspunkten akzeptabel.

8. Schulen

8.1
Datenschutz in Schulen

Im 22. Tätigkeitsbericht, Ziff. 12.1 hatte ich mich zu dem Entwurf einer "Rechtsverordnung über die Verarbeitung personenbezogener Daten in Schulen", den das Hessische Kultusministerium auf der Grundlage des § 83 Abs. 7 SchulG erarbeitet hatte, geäußert. Die Rechtsverordnung wurde nach einem längeren Abstimmungsverfahren verkündet (ABl. 1994 S. 114) und ist am 15. Februar 1994 in Kraft getreten. Meine Änderungsvorschläge wurden ganz überwiegend berücksichtigt. Auf wesentliche Neuerungen hatte ich ebenfalls im 22. Tätigkeitsbericht, Ziff. 12.1 bis 12.14 hingewiesen.

Mit der Rechtsverordnung sollten vor allem zahlreiche datenschutzrechtliche Zweifelsfragen im täglichen Schulbetrieb geklärt werden. Der Zwang für die Schulleitungen, sich der Durchführung der einzelnen, teils sehr konkreten Regelungen zu stellen, nahm damit erheblich zu. Sicherlich ist jeder Verwaltung, die mit neuen Vorschriften konfrontiert wird, ein "Übergangsbonus" bei der Umsetzung einzuräumen. Dies gilt auch für die Schulverwaltung, die inzwischen geprägt ist von einem hohen Grad der Verrechtlichung. Meine Prüfungen bei mehreren Schulen im Herbst letzten Jahres ergaben deutliche Anhaltspunkte für verbreitete Verwaltungsmängel im datenschutzrechtlichen Bereich, auch unter dem Aspekt der neuen Rechtslage. Hier gibt es noch einiges zu tun.

8.1.1
Einsatz privater PC für schulische Zwecke

Zahlreiche Lehrkräfte benutzen ihren privaten PC – neben der automatisierten Erstellung von Unterrichtsunterlagen – für die Verwaltung von Schüler- und Elterndaten. Dieser Trend nimmt deutlich zu, zwei Drittel aller Haushalte mit Kindern verfügen bereits über ein solches Gerät, dessen technische Möglichkeiten meist umfassend genutzt werden. Im Gegensatz zu verschiedenen anderen Bundesländern (z. B. Schleswig-Holstein) hat Hessen die schulische Nutzung des privaten PC nicht generell untersagt, sondern an eine formale Genehmigung der Schulleitung gebunden (§ 83 Abs. 7 SchulG i.V.m., § 2 Abs. 2 der o.g. Rechtsverordnung). Der Antrag auf Genehmigung muß Angaben enthalten zum Zweck der Verarbeitung, zu den eingesetzten Programmen, vorgesehenen Dateien und notwendigen Datensicherungsmaßnahmen.

Dieses Verfahren wird, so haben meine Prüfbesuche gezeigt, nicht beachtet. Keine der geprüften Schulen hat eine solche Genehmigung bisher erteilt, trotz verhältnimäßig großer Lehrerschaften. Nicht verläßlich zu klären war die Frage, ob die Lehrer keine Informationen über das Verfahren erhalten haben oder ob es an der notwendigen Akzeptanz fehlt. Hier besteht jedenfalls ein unübersehbarer Nachholbedarf. Inzwischen hat das Hessische Kultusministerium ein Antragsformular als Muster entwickelt, auf das bei Unsicherheiten zurückgegriffen werden kann.

8.1.2
Fehlende Datensicherheit bei dienstlichen PC

Das Fehlen notwendiger Datensicherheitsmaßnahmen bei der Verarbeitung personenbezogener Daten auf schulischen PC ist mir bei meinen Prüfbesuchen mehrfach aufgefallen. Obwohl in der "Rechtsverordnung über die Verarbeitung personenbezogener Daten in Schulen" (SchulVO) in § 6 eindeutig geregelt ist, daß die Schule bei der automatisierten Verarbeitung alle technischen und organisatorischen Maßnahmen i. S. v. § 10 HDSG durchzuführen hat und die Einzelheiten hierzu in der Anlage 5 zur SchulVO geregelt sind, mußte ich gravierende Defizite feststellen.

In einem Fall verarbeitete der stellvertretende Schulleiter auf dem dienstlichen PC, der über eine Festplatte sowie ein 5 1/4 Zoll Disketten-Laufwerk verfügt, ein Statistikprogramm, das vom Hessischen Institut für Bildungsplanung und Schulentwicklung den Schulen zur Verfügung gestellt wird. Zusätzlich hatte er sich ein Hilfsprogramm erstellt, mit dem er Lehrerdaten verarbeitete. Es handelte sich hierbei um die Erfassung von Fehlzeiten der Lehrkräfte, wobei teilweise auch konkrete Gründe (z. B. Beurlaubung zur Betreuung eines Kindes wegen Krankheit des Ehegatten und anderes mehr) gespeichert waren.

Es gab weder mechanische (z. B. Schloß) noch systembedingte (z. B. Paßwortschutz) Schutzmechanismen, die einen unbefugten Zugriff Dritter hätten verhindern können. Die auf dem PC gespeicherten personenbezogenen Daten waren sowohl für das Reinigungspersonal als auch für andere dritte, unberechtigte Personen frei zugänglich.

Auch der PC des Förderstufenleiters, auf dem umfangreiche Programme installiert und Schülerdaten gespeichert waren, verfügte über keine Schutzsoftware.

Die genannte Rechtsverordnung sieht bei der automatisierten Verarbeitung von personenbezogenen Daten eine Fülle von Datensicherungsmaßnahmen vor, die sich auf räumliche, organisatorische und systembezogene Komponenten (z. B. Einsatz einer Schutzsoftware) beziehen. So ist in der Anlage 5 Nr. 2 explizit geregelt, daß das DV-System mit einer Sicherheitssoftware (Zugriffsschutzprogramm) abzusichern ist. Auch ist der Kreis der Systembenutzer (berechtigte Personen) schriftlich festzulegen (vgl. Anlage 5 Nr. 2, 4. Spiegelstrich). Diese sind anzuweisen, ihre Paßwörter geheimzuhalten und regelmäßig zu wechseln.

Hinzu kommt, daß die Verarbeitung personenbezogener Daten nur mit Programmen durchgeführt werden darf, die ausreichend getestet und dokumentiert worden sind. Auch in diesem Bereich gab es Mängel: Für die von dem stellvertretenden Schulleiter selbst angelegte Datei hätte sowohl eine Dateibeschreibung nach § 6 Abs. 1 HDSG erstellt als auch eine Registermeldung nach § 26 HDSG zu dem bei mir geführten Dateienregister abgegeben werden müssen. Es fehlte auch die vorgeschriebene Verschlüsselung der Festplattenspeicherung (vgl. Anlage 5, Nr. 2, 10. Spiegelstrich).

Ich habe die Schulleitung aufgefordert, die festgestellten Datenschutzmängel unverzüglich zu beseitigen.

Im übrigen waren auch keine Schutzmaßnahmen gegen Computerviren getroffen, ein Thema, das mittlerweile mehr und mehr an Bedeutung gewinnt und im Fall der "Verseuchung" der Festplatte unvorhersehbare Konsequenzen im Hinblick auf die vorhandenen Dateninhalte haben kann. Aus diesem Grund muß ich erneut darauf hinweisen, daß der Einsatz eines Virenscanners in der jeweils aktuellsten verfügbaren Version mittlerweile ebenso unabdingbar ist wie eine Regelung zum Einsatz von "Fremddisketten".

8.1.3
Aufbewahrungsfristen und Archivierung bei schulischen Unterlagen

Maßgebend für die Aufbewahrung von Schriftgut in Schulen sind die "Aufbewahrungsbestimmungen für Schriftgut in Schulen und bei den Wissenschaftlichen Prüfungsämtern für die Lehrämter", die in einem Erlaß des Hessischen Kultusministeriums vom 24. Mai 1985 (ABl. S. 409) geregelt sind. Er bezeichnet insbesondere die Unterlagen und ihre Aufbewahrungszeit, die regelmäßig im Laufe des Schulbetriebs anfallen. Für die dort nicht genannten sonstigen schulischen Unterlagen gelten die "Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen" vom 20. Oktober 1986 (StAnz. S. 2107ff.).

Bei meinen Prüfungen habe ich festgestellt, daß die in den Erlassen genannten Speicherfristen regelmäßig um ein Vielfaches überschritten werden. So sind z. B. Klassenbücher, Lehrerberichte, Zeugnisentwürfe u. a. zwei Jahre nach dem Ausscheiden des Schülers oder der Jahrgangsstufe aus der Schule auszusondern. Diese – zugegebenermaßen kurzen – Fristen waren in Einzelfällen um mehr als zehn Jahre überschritten. Auch Versäumnislisten sind frühzeitig, d.h. ein Jahr nach dem Ausscheiden des Schülers auszusortieren.

Selbstverständlich gibt es auch Unterlagen, die einer längerfristigen Aufbewahrung bedürfen. So ist beispielsweise die Schulchronik aus nachvollziehbaren Gründen dauernd aufzubewahren. Schülerakten oder Schülerverzeichnisse sind für einen Zeitraum von 40 Jahren aufzuheben. Selbst Konferenzprotokolle bzw. die Schulstatistik sind über einen Zeitraum von zehn Jahren im "Schularchiv" zu führen. Aber was geschieht mit den schulischen Unterlagen nach Ablauf der Aufbewahrungsfrist?

Nach § 10 Abs. 1 HArchivG vom 18. Oktober 1989 (GVBl. I S. 270ff.) sind die Unterlagen auszusondern und dem zuständigen Staatsarchiv zur Übernahme und Archivierung anzubieten. Nach § 10 Abs. 2 HArchivG dürfen Unterlagen nur vernichtet bzw. Daten gelöscht werden, wenn das Staatsarchiv die Übernahme ablehnt oder nicht binnen eines Jahres über die Archivwürdigkeit angebotener Unterlagen entschieden hat. Sinnvoll erscheint es, daß sich die Schulen mit dem für ihren Bereich zuständigen Hauptstaatsarchiv auf ein Verfahren verständigen, das einerseits den Erfordernissen des Archivgesetzes Rechnung trägt, andererseits aber die Schulen auch von der Verpflichtung entbindet, Unterlagen von geringer Bedeutung, wie etwa Notenbücher oder Versäumnislisten, den Archiven formell anbieten zu müssen. Ich habe das Hessische Kultusministerium gebeten, diese Fragen durch einen Erlaß grundsätzlich zu klären.

In den oben zitierten Erlassen sind Art und Weise, wie die Vernichtung von Unterlagen vorgenommen werden soll, detailliert geschildert. Grundsätzlich bleibt die Behörde selbst, also die Schule, verantwortlich für die ordnungsgemäße Vernichtung von Unterlagen, deren Archivwürdigkeit verneint worden ist. Sollte die Vernichtung nicht von der Schule selbst vorgenommen werden können, dürfen die Akten bzw. Unterlagen nur an zuverlässige Unternehmer zur Entsorgung gegeben werden, soweit dies nicht im Wege der Amtshilfe durch andere Behörden erfolgen kann. Die Unternehmen sind vertraglich zu verpflichten, die Akten im Inland zu vernichten, niemandem Einsicht zu gestatten und die Vernichtung innerhalb einer bestimmten Frist nachzuweisen.

Meine bisherigen Prüferfahrungen offenbarten in diesem Punkt deutliche Schwachstellen. So sind die Schulen in der Regel nicht in der Lage, die Unterlagen selbst zu vernichten. Die Beauftragung von geeigneten Firmen scheitert oftmals an fehlenden finanziellen Ressourcen und geschieht letztlich (wie der unter Ziff. 8.2 beschriebene Fall des Fundes von Klassenbüchern auf dem Müll in Darmstadt gezeigt hat) völlig unzureichend. Soweit der Schulträger die entsprechenden Kosten zu tragen hat, kann er sich dieser Pflicht nicht entziehen.

An diesem Punkt gilt es anzusetzen und die verantwortlichen Stellen auf ihre Pflichten nachdrücklich hinzuweisen. Schließlich handelt es sich auch und gerade bei Unterlagen von Schülern um oftmals sensible personenbezogene Daten. Wieder sei an den "Darmstädter Fall" erinnert, denn in den aufgefundenen Klassenbüchern befanden sich neben Name und Anschrift der Schüler sowie deren Eltern auch ärztliche Atteste und anderer Schriftverkehr. Solche Unterlagen gehören jedenfalls nicht auf irgendeinen Papierberg, wo sie dem potentiellen Zugriff Dritter ausgesetzt sind.

8.1.4
Unzulässige Klassenbucheintragungen

In ihrer Anlage 3 enthält die o.g. Rechtsverordnung einen abschließenden Katalog von Eintragungen, die im Klassenbuch erfolgen dürfen (vgl. auch 22. Tätigkeitsbericht, Ziff. 12.1.2). Das heißt, alle dort nicht genannten Daten dürfen nicht eingetragen werden. Meine Prüfbesuche zeigten, daß auch diese Regelung nicht immer beachtet wird, obwohl sie überschaubar ist. Aufgefallen waren mir beispielsweise Eintragungen zu Adressen, Staatsangehörigkeit usw. Offensichtlich führt auch die Tatsache, daß zahlreiche Schulen immer noch Klassenbücher verwenden, die in ihren Strukturen und Rubriken veraltet sind, also der neuen Rechtslage noch nicht angepaßt wurden, zu solchen unzulässigen Datenspeicherungen. Wie ich durch eine Umfrage feststellen konnte, berücksichtigen die Druckereien bei Neuaufträgen die neue Rechtslage und gestalten die Klassenbücher entsprechend. Sofern die Schulverwaltung jedoch noch alte Klassenbuchbestände verwendet, halte ich es für unumgänglich, daß die Schulleitung die Lehrer auf die Regelung hinweist und sie auffordert, nur die ausdrücklich genannten Daten aufzunehmen.

8.2
Klassenbücher im Müll

Ein Mitarbeiter der Stadt Darmstadt machte mich auf den Fund von fünf Klassenbüchern einer Darmstädter Schule auf dem Gelände eines papierverarbeitenden Darmstädter Betriebs aufmerksam. Die Klassenbücher befanden sich in einem einwandfreien äußerlichen Zustand und enthielten nicht nur die Namen und Anschriften von Schülern sowie Daten über deren Eltern; in einigen Büchern waren darüber hinaus ärztliche Bescheinigungen mit Diagnosen, Schriftwechsel mit anderen Schulen im Zusammenhang mit einer Versetzung und anderes abgelegt.

Meine Nachforschungen bei der betroffenen Schule haben einmal mehr deutliche Mängel im Zusammenhang mit der Archivierung und Vernichtung personenbezogener Unterlagen aus dem Schulbereich aufgezeigt.

Angefangen hatte alles mit einer wohlgemeinten Aussonderungsaktion. Bei der Durchforstung des "Schularchivs" sortierte die stellvertretende Schulleiterin 15 Klassenbücher aus den Jahren 1979 bis 1983 aus. Da die Schule keine eigene Möglichkeit hatte, derartige Unterlagen selbst und damit vor Ort zu vernichten, übergab sie die Bücher dem Hausmeister, der sie in einen Papiercontainer auf dem Schulhof warf. Tags darauf wurde der Container vom Fuhr- und Reinigungsamt der Stadt Darmstadt zu dem erwähnten papierverarbeitenden Betrieb gebracht. Dort lagerten die Bücher mehr als ein Vierteljahr auf einer Papierhalde auf dem frei zugänglichen Betriebsgelände der Firma.

Meine weiteren Ermittlungen ergaben, daß die Stadt Darmstadt die Entsorgung ihrer gesamten Akten von diesem Betrieb vornehmen läßt. Die Mitarbeiter der Stadt sind durch eine Rundverfügung angewiesen, die Akten selbst auf das Förderband zu legen und den Transportvorgang bis zum Einfallen des Papiers in einen Bottich zu überwachen. In dieser Verfügung ist auch ausdrücklich darauf hingewiesen, daß das Schriftgut nicht auf dem Firmengelände gelagert werden darf. Die Mängel dieses Entsorgungskonzepts sind offensichtlich und durch den Fund der Klassenbücher eindrucksvoll dokumentiert.

Aber auch die betroffene Darmstädter Schule selbst hat in mehreren Punkten gegen bestehende Vorschriften verstoßen: In den "Aufbewahrungsbestimmungen für Schriftgut in den Schulen und bei den Wissenschaftlichen Prüfungsämtern für die Lehrämter" (Erlaß vom 24. Mai 1985, ABl. S. 409) ist geregelt worden, daß Klassenbücher nur für einen Zeitraum von zwei Jahren nach dem Ausscheiden der Schüler aus der Schule aufbewahrt werden dürfen (Ziff. I Nr. 8 des Erlasses). Die im Altpapier gefundenen Bücher wurden also mehr als zehn Jahre unzulässig im "Archiv" der Schule gelagert.

Nach Ablauf der Frist hätte die Schulleitung die Unterlagen zunächst aussondern und dem zuständigen Hauptstaatsarchiv zur Prüfung der Archivwürdigkeit anbieten müssen (siehe Ziff. V, Nr. 1 des Erlasses). Die Anbietungspflicht aussonderungsreifer Unterlagen gilt im übrigen ganz allgemein für alle öffentlichen Stellen in Hessen. Rechtsgrundlage hierfür ist § 10 HArchivG in Verbindung mit den "Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen" (StAnz. 1986, S. 2107). Erst wenn das Hauptstaatsarchiv die Archivierung aufgrund mangelnder Archivwürdigkeit der Unterlagen ablehnt, sind sie von der verwahrenden Behörde zu vernichten.

Ich habe daher der Schulleitung empfohlen, mit der Stadt Darmstadt zu verhandeln und gemeinsam mit anderen Schulen ein Entsorgungskonzept zu entwickeln. Soll mit der Aktenvernichtung ein Unternehmer beauftragt werden, muß dieser sich vertraglich verpflichten:

- die Aktenvernichtung im Inland vorzunehmen,
- niemanden Einsicht in die Unterlagen zu gestatten,
- innerhalb einer bestimmten Frist die Vernichtung nachzuweisen.

Außerdem muß sich die Schulleitung durch Stichproben von seiner Zuverlässigkeit überzeugen. Eine andere Möglichkeit wäre z. B., beim Schulamt einen leistungsfähigen Aktenvernichter zu plazieren und dort konzertiert eine Vernichtung vorzunehmen.

9. Forschung: Akteneinsicht in Strafakten zu Forschungszwecken

Die wissenschaftliche Forschung, auf welchem Gebiet auch immer, greift häufig auf Vorgänge der öffentlichen Verwaltung als Informationsquelle zurück. Insbesondere die kriminologische und rechtswissenschaftliche Forschung findet in Strafakten oft unverzichtbare Daten und Grundlagen, wie die Übersendung der entsprechenden Genehmigungsbescheide des Hessischen Ministeriums der Justiz nach § 33 Abs. 1 HDSG zeigt. Daß diese Vorschrift aber nicht nur Verfahrensfragen regelt, sondern auch abschließende inhaltliche Vorgaben für die Freigabe behördlicher Daten zu Forschungszwecken enthält, mußte ich in folgendem Fall gegenüber dem Justizministerium deutlich machen:

Ein anläßlich einer Diplomarbeit begonnenes Forschungsvorhaben hatte die handels- und gesellschaftsrechtlichen Vorgänge eines Unternehmens zum Gegenstand, wie sie der Öffentlichkeit oberflächlich durch Presseberichte über ein Strafverfahren bekannt gemacht worden waren. Wichtige Hinweise für die Arbeit wurden in bestimmten Teilen der Strafprozeßakten vermutet. Das zuständige Gericht hatte dem Antrag auf Akteneinsicht des Diplomanden zunächst entsprochen und sich dabei auf Nr. 183b, 185a der "Richtlinien für das Strafverfahren und das Bußgeldverfahren" vom 1. Mai 1991 gestützt. Der Fall wurde anschließend dem Hessischen Justizministerium bekannt, das auf folgende Rechtslage hinweisen mußte: Sollen personenbezogene Daten aus hessischen Strafverfahrensakten für konkrete wissenschaftliche Forschungsvorhaben zugänglich gemacht werden, findet sich die notwendige gesetzliche Grundlage ausschließlich in § 33 Abs. 1 HDSG. Diese Vorschrift zwingt zur gründlichen Abwägung der öffentlichen Interessen an dem Forschungsvorhaben gegenüber den schutzwürdigen Belangen der Betroffenen, deren Daten offenbart werden sollen, ehe die formale Freigabeentscheidung erfolgt. Geht es dabei um Datenbestände der hessischen Landesverwaltung, ist sogar die – regelmäßig mit zahlreichen Auflagen – versehene vorherige Genehmigung des zuständigen Ministeriums notwendig (§ 33 Abs. 1 Satz 3 HDSG).

Die Anwendung der Nr. 185a der o. g. Richtlinien, die überwiegend auf rein strafverfahrensrechtliche Aspekte abstellt, ist also hinfällig geworden. Im Hinblick auf meinen Verdacht, daß diese Rechtslage teilweise unbekannt ist, hat das Hessische Justizministerium die nachgeordneten Justizbehörden entsprechend informiert.

10. Archive

10.1
Aufbewahrung und Archivierung von Personalakten des Justizministeriums

Im Rahmen eines Hochschulforschungsprojekts sollte die persönliche und berufliche Entwicklung verschiedener Juristen beleuchtet werden, die als Richter oder Ankläger in Prozessen zu geschichtlich bedeutsamen Ereignissen in der NS-Zeit mitgewirkt hatten. Dabei war unter anderem ein Jurist in das Blickfeld gerückt, der in der früheren Wehrmachtsgerichtsbarkeit als Oberfeldrichter tätig gewesen war und 1949 in den hessischen Justizdienst, ebenfalls als Richter, übernommen wurde. Er verstarb 1971.

Das Ergebnis der Forschungsarbeit, die unter anderem auf zahlreichen Unterlagen aus privaten und öffentlichen Archiven beruhte, sollte in Buchform veröffentlicht werden und auch ein Foto des Richters enthalten. Verfügbar war dafür jedoch nur das Foto, das sich in der Personalakte des Richters befand, die das hessische Justizministerium weiterhin verwahrte.

Die rechtliche Prüfung der Zulässigkeit der Freigabe des Fotos zu diesem Zweck führte zur Frage, welche Vorschriften überhaupt für "abgelegte" Personalakten gelten. Die einzige Regelung, die hier als Rechtsgrundlage der Freigabeentscheidung in Betracht kam und den oft komplizierten Abwägungsprozeß zwischen dem persönlichen Interesse des Betroffen oder dem postmortalen Schutz der Menschenwürde einerseits und dem Forschungsinteresse andererseits zwingend vorsieht, findet sich in § 15 Abs. 4 HArchivG. Die Anwendung des Archivgesetzes mit seinen differenziert geregelten Schutzfristen für personenbezogenes Archivgut ist allerdings nur möglich, wenn die betroffene behördliche Unterlage überhaupt vorher "archiviert" wurde. Dies setzt – neben der Übergabe der Akte – die positive Entscheidung des zuständigen Hauptstaatsarchivs voraus, daß die ihm angebotene Akte archivwürdig ist i. S. v. § 1 Abs. 4 HArchivG. Anderenfalls hat die aktenverwahrende Behörde die Akte zu vernichten. Das Verfahren der Berechnung der einzelnen Aufbewahrungsfristen für die verwahrende Behörde, der Übergabe an das Hauptstaatsarchiv sowie der ordnungsgemäßen Vernichtung ergibt sich aus dem Erlaß zu den "Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen" vom 20. Oktober 1986 (StAnz. 1986, S. 2107). Speziell für Personalakten gilt seit 1. Dezember 1993 nach § 107f HBG eine einheitliche Frist von fünf Jahren nach ihrem Abschluß.

Die korrekte Beachtung der genannten Verfahren hätte also im vorliegenden Falle dazu führen müssen, daß das Justizministerium die betroffene Personalakte nach der abgelaufenen Aufbewahrungsfrist dem Wiesbadener Hauptstaatsrchiv zur Archivierung übergeben und damit eine rechtlich korrekte Entscheidung über die Verkürzung der Schutzfristen nach § 15 Abs. 4 ArchivG ermöglicht hätte. Diese Entscheidung liegt ausschließlich beim Hessischen Ministerium für Wissenschaft und Kunst.

Ich habe daher das Justizministerium aufgefordert, die Aufbewahrungsfristen aller Personalakten in seinem Bereich zu überprüfen, um sicherzustellen, daß die Vorgänge entweder dem Hauptstaatsarchiv zur Förderung der wissenschaftlichen Forschung überlassen oder ordnungsgemäß vernichtet werden. Im übrigen habe ich dem Justizministerium zu dem geschilderten Fall mitgeteilt, daß ich unter Berücksichtigung der rechtlichen Vorgaben des § 15 HArchivG die Freigabe des Fotos zu dem angegebenen Forschungszweck für zulässig hielte. Denn das öffentliche Interesse an der Durchführung des Forschungsvorhabens überwiegt das postmortale Schutzbedürfnis des betroffenen Richters. Dabei war zu berücksichtigen, daß § 22 Kunst- und Urhebergesetz (KunstUrhG) generell die Verwendung von fotografischen Ablichtungen zehn Jahre nach dem Tod des Betroffenen freigibt.

10.2
Neue Benutzungsordnung für Hessische Staatsarchive

Im Oktober 1989 ist das neue Hessische Archivgesetz in Kraft getreten. Es verpflichtet, angelehnt an entsprechende Bestimmungen des kurz zuvor erlassenen Bundesarchivgesetzes für die Bundesverwaltung, grundsätzlich die gesamte hessische Landesverwaltung, die entstandenen behördlichen Unterlagen – nach Ablauf der Aufbewahrungsfristen – auszusondern und dem örtlich zuständigen Hauptstaatsarchiv zur Übernahme anzubieten (§ 10 Abs. 1 ArchivG). Davon sind sogar Unterlagen umfaßt, die besonderen Rechtsvorschriften über Geheimhaltung oder den Datenschutz unterworfen sind.

Die Nutzung des öffentlichen Archivguts steht nach Ablauf bestimmter Schutzfristen jeder Person zu, die ein berechtigtes Interese an der Nutzung glaubhaft macht (§ 14 ArchivG). Näheres ist in der "Benutzungsordnung für die Staatsarchive des Landes Hessen" geregelt, die jedoch schon aus dem Jahr 1973 stammt. Es ist äußerst dringlich, die Benutzungsordnung, die nicht nur das Verfahren der Nutzung des Archivs durch private und öffentliche Stellen regelt, sondern auch weitere archivrechtliche Definitionen enthält, der neuen Rechtslage anzupassen.

Das zuständige Hessische Ministerium für Wissenschaft und Kunst legte mir Ende 1993 den ersten Entwurf einer neuen Benutzungsordnung zur Stellungnahme vor. In einer gemeinsamen Besprechung wurde der Text so überarbeitet, daß er – unter Übernahme von sinnvollen Bestimmungen anderer Bundesländer die Rechte und Pflichten des Archivbenutzers konkret regelt und – auch unter datenschutzrechtlichen Gesichtspunkten transparent macht. Beispielsweise soll beim Antrag auf Archivnutzung darauf verzichtet werden, den Beruf des Antragstellers aufzunehmen. Andererseits ist der Benutzungszweck vom Antragsteller umfassend zu schildern. Dies ist vor allem dann von entscheidender Bedeutung, wenn von der geplanten Veröffentlichung von Forschungsarbeiten auch personenbezogene Daten betroffen sind, die dem Archivgut entnommen wurden. Meine Forderungen wurden überwiegend berücksichtigt, so daß in diesem Jahr mit dem Erlaß einer Benutzungsordnung zu rechnen ist, die zugleich gesetzeskonform und benutzerfreundlich ist.

11. Kommunen

11.1
Prüfungen

1994 habe ich die Kommunen Mühltal und Kriftel geprüft. Gegenstand meiner Prüfungen waren neben der allgemeinen Gebäudesicherheit vor allem die Führung der Melde- und Wahlunterlagen sowie der Personalakten, der Umgang mit nicht mehr aktuellen Akten im Archiv sowie die Datensicherheit im PC-Netz.

11.1.1
Zugang und Sicherheit der Dienstgebäude und Diensträume

Häufig nutzen Kommunen das Rathaus sowohl als Diensträume für die Kommunalverwaltung als auch als Bürgerhaus für Veranstaltungen, Ausstellungen etc. Daraus ergeben sich besondere Anforderungen an die Abschottung der Diensträume.

In Mühltal ist durch die baulichen Verhältnisse eine strikte Trennung zwischen Verwaltungs- und Veranstaltungsräumen gegeben. In Kriftel hingegen mußten die Sicherheitsprobleme, die sich durch die Doppelfunktion des Gebäudes stellen, durch besonders sorgfältige Sicherungen der Diensträume ausgeglichen werden. Bei den Mitarbeitern ist ein entsprechendes Problembewußtsein vorhanden: Zum Beispiel werden hier auch bei kurzer Abwesenheit die Büros sehr viel konsequenter verschlossen, als ich das in anderen Verwaltungen gesehen habe.

Ganz allgemein ist zu diesem Thema festzustellen, daß die Mitarbeiter regelmäßig darauf aufmerksam gemacht werden müssen, daß sie die Türen zu ihren Büros auch bei kurzer Abwesenheit verschließen müssen. Die Aufnahme eines entsprechenden Hinweises in eine Dienstanweisung allein genügt sicher nicht, vielmehr sind auch entsprechende Kontrollen durchzuführen.

Bei einer der beiden Kommunen ist das Rathaus aufgrund verschiedener Umstände, die ich hier nicht näher erläutern möchte, nicht ausreichend vor Einbrüchen geschützt. Das Problem ist der Kommune schon länger bekannt; die Umsetzung der in einem kriminalpolizeilichen Gutachten zur Gebäudesicherheit geforderten Maßnahmen scheiterte bislang an den finanziellen Möglichkeiten. Aber auch kleinere, unter Kostengesichtspunkten nicht aufwendige Maßnahmen können zu einem größeren Maß an Sicherheit führen:

- Beispielsweise wurden bei beiden Kommunen Unterlagen mit personenbezogenen Daten, die vernichtet werden sollten, allgemein zugänglich vor dem Schredder gelagert. Durch entsprechende organisatorische Änderungen läßt sich dies ohne großen Aufwand vermeiden.
- In Mühltal gelang es mir, unbemerkt ein eingegangenes Fax zu kopieren und die Kopie mitzunehmen. Dasselbe wäre jedem beliebigen anderen Besucher auch möglich gewesen. Dieses Problem konnte inzwischen durch den Einbau eines Türschließers und einer Alarmglocke, die eingehende Faxe der zuständigen Mitarbeiterin meldet, mit unerheblichen finanziellen Mitteln beseitigt werden.
- Ebenfalls in Mühltal fand ich auf einem Flur ein großes unverschlossenes Regal mit sämtlichen Bauakten der Kommune. Die Akten sollten wegen einer Umstellung des Aktensystems alsbald umsortiert werden. Auch wenn es sich nur um ein "Provisorium" handelt, ist die Aufbewahrung solcher Unterlagen in unverschlossenen Regalen auf einem Flur, der noch dazu im frei zugänglichen Besucherbereich liegt, ein Verstoß gegen den Datenschutz.

11.1.2
Führung der Melde- und Wahlunterlagen sowie der Personalakten

Die Meldedaten wurden mit dem Verfahren "Grundstufe Einwohnerwesen", einem landesweit von den Kommunalen Gebietsrechenzentren eingesetzten Verfahren zur Verwaltung der Meldedaten, über das jeweils zuständige Kommunale Gebietsrechenzentrum verarbeitet. Hierbei gibt es aus datenschutzrechtlicher Sicht folgende Probleme:

Bei der "Grundstufe Einwohnerwesen" können die Kommunen des Nebenwohnsitzes bei Personen, die in demselben KGRZ-Bereich ihren Hauptwohnsitz haben, auf alle Daten dieser Personen zugreifen. Dies ist unzulässig, da das Meldeamt des Nebenwohnsitzes nach § 3 Abs. 3 HMG ausdrücklich nur auf einen Teil der Meldedaten zugreifen darf. Das Meldeamt in Kriftel nutzte nicht nur die erweiterten Abfragemöglichkeiten, sondern speicherte auch alle Angaben, die der Bürger auf seinem Meldevordruck gemacht hatte, unabhängig davon, ob ein Haupt- oder Nebenwohnsitz angemeldet wurde. Hier müssen das Melderegister überprüft und die unrechtmäßig gespeicherten Daten gelöscht werden.

Die Wahlunterlagen wurden von beiden Kommunen vorbildlich geführt; insbesondere befanden sich keine Unterstützungsunterschriften für Wahlvorschläge oder alte Wählerverzeichnisse, die nach § 94 KWO grundsätzlich sechs Monate nach der Wahl zu vernichten sind, in den Akten.

Eine stichprobenartige Durchsicht der Personalakten ergab, daß die Akten ordnungsgemäß, nämlich gesondert von den anderen Akten, in einem verschlossenen Stahlschrank aufbewahrt wurden.

Im einzelnen sind mir jedoch folgende Mängel aufgefallen:

- Urlaubs- und Fehlzeitenkarten bzw. Krankmeldungen wurden unbegrenzt aufbewahrt. Nach § 107f Abs. 2 HBG sind Unterlagen über Beihilfen, Heilfürsorge, Heilverfahren, Unterstützungen, Erholungsurlaub, Erkrankungen, Umzugs- und Reisekosten nur fünf Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufzubewahren, danach sind sie zu vernichten.

- Gleitzeitunterlagen wurden in Mühltal ca. zwei Jahre aufbewahrt. Eine derartig lange Aufbewahrung von Zeitkartenkonten ist datenschutzrechtlich nicht zulässig. Ich sehe bei automatisierten Zeiterfassungssystemen eine Aufbewahrungszeit/Speicherdauer von drei Monaten, entsprechend Nr. 10 der Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen (StAnz. 1986 S. 2107) als ausreichend an. Danach ist die Kenntnis dieser Daten in aller Regel für die Aufgabenerfüllung des Dienstherrn nicht mehr erforderlich.
- Ebenfalls in Mühltal fand ich in einigen Personalakten Schreiben an die Versorgungskasse, die mehrere Bedienstete betrafen. Bei einer Einsichtnahme in seine Personalakte würde der einzelne Bedienstete zwangläufig auch Informationen über seine Kollegen erlangen. Hier ist eine Bereinigung der Personalakten erforderlich, indem auf den Kopien der Schreiben jeweils die Namen der anderen Bediensteten unkenntlich gemacht werden.
- Unterlagen von Stellenbewerbern, mit denen kein Arbeitsverhältnis mit der Kommune zustande kam, dürfen nicht aufbewahrt, sondern müssen dem Bewerber zurückgegeben werden. Auch die Aufbewahrung von Kopien dieser Unterlagen ist selbstverständlich unzulässig; eine Ausnahme gilt nur für das eigentliche Bewerbungsschreiben.

11.1.3
Archive

Bei beiden Kommunen befinden sich die Archive in ordnungsgemäß verschlossenen Räumen im Dach- bzw. Kellergeschoß.

In Kriftel haben jedoch unter datenschutzrechtlichen Gesichtspunkten zuviele – nämlich 14 – Personen Zugang zu den Archivräumen. Besonders im Hinblick auf die im Archiv aufbewahrten Personalunterlagen ist dies bedenklich. Entweder müssen die Personalunterlagen im Archivraum gesondert verschlossen aufbewahrt werden, oder die Verteilung der Zugangsrechte muß neu überdacht werden. Letzteres wurde mir zwischenzeitlich zugesichert.

In beiden Archiven befanden sich Unterlagen, die unter datenschutzrechtlichen Gesichtspunkten nicht mehr aufbewahrt werden dürfen, da sie für die Erfüllung der Aufgaben der Kommunen nicht mehr erforderlich sind. Beide Archive sollten daher unter Zugrundlegung der Fristen in den o.g. Aufbewahrungsbestimmungen bereinigt werden.

Ein besonderes Augenmerk ist hierbei auf alte Meldekarteien zu richten, die nach dem geänderten Hessischen Meldegesetz 50 Jahre gesondert aufzubewahren sind. Werden die alten Meldekarteien auf Mikrofilm übernommen, ist eine gesonderte Aufbewahrung ohne weiteres möglich.

In Mühltal fand ich im Archiv Durchschriften von Sozialhilfebescheiden seit dem Jahr 1979.

Träger der Sozialhilfe sind in Hessen die kreisfreien Städte und die Landkreise, also nicht die kreisangehörigen Gemeinden. In der Vergangenheit war es üblich, daß die Kreise den Wohnsitzgemeinden Durchschriften der Sozialhilfebescheide übersandten. Begründet wurde dies in der Regel damit, daß die Wohnsitzgemeinden eher in der Lage seien, die Angaben der Antragsteller auf ihre Richtigkeit hin zu überprüfen und damit Mißbrauch zu verhindern. Ich habe bereits in meinem 16. Tätigkeitsbericht, Ziff. 7.1 darauf hingewiesen, daß diese Praxis rechtswidrig ist. Damit ist selbstverständlich auch die weitere Aufbewahrung der seinerzeit übersandten Bescheide nicht zulässig. Die Gemeinde hat mir inzwischen mitgeteilt, daß sie diese Unterlagen vernichtet hat.

11.1.4
Probleme beim Einsatz von Novell-Netzen

Zu den Problemen beim Einsatz von PC-Netzen habe ich mich bereits in den vergangenen Jahren geäußert (vgl. 22. Tätigkeitsbericht, Ziff. 21.2). Auch bei den diesjährigen Prüfungen habe ich wieder eine Reihe von Mängeln festgestellt.

Auffallend war bei beiden Prüfungen, daß die Strukturierung des Datenbestands auf dem Server unzureichend bzw. nicht fein genug war. Daher war es nicht möglich, die Rechtezuweisung so zu gestalten, daß nur die jeweils zuständigen Mitarbeiter auf "ihren" Datenbestand zugreifen konnten.

Mit der eigentlichen Einstellung der dafür notwendigen Paramenter am Server ist es jedoch noch nicht getan. Gerade bei der Zuweisung von Rechten, aber auch in allen anderen Fragen waren Mängel bei der Dokumentation von Systemeinstellungen festzustellen. Schriftliche Regelungen zum Einsatz der Geräte, zur Verwendung von Notfall-Kennungen oder zur Datensicherung fehlten ganz oder waren unzureichend.

Als ein weiterer Schwachpunkt ist die mangelhafte Unterbringung der Server zu nennen. Die Server waren nicht nur in Räumen offen zugänglich aufgestellt, in denen auch Mitarbeiter, die nicht für die Datenverarbeitung zuständig waren, ihre Arbeitsplätze hatten; darüber hinaus waren sie auch für Besucher der Verwaltung zugänglich.

Grundsätzlich sollte ein Server in einem dafür eigens vorgesehenen Raum aufgestellt werden. Der Zugriff Unbefugter ist durch eine restriktive Schlüsselvergabe auszuschließen. Sind die Möglichkeiten dazu nicht gegeben, so ist auch eine Aufstellung in einem geeigneten Schrank möglich, wenn dieser sowohl vor unbefugter Bedienung als auch vor Diebstahl ausreichend Schutz bietet.

Die Sicherungsbänder sowie besonders wichtige Teile der Systemunterlagen sind selbstverständlich so aufzubewahren, daß sie beispielsweise durch einen Brand nicht zusammen mit dem Server zerstört werden und auch nicht in unbefugte Hände gelangen können.

Leider mußte ich über den Bereich der Netze hinaus feststellen, daß sowohl auf vernetzten als auch auf unvernetzten PC, die über keine Schutzsoftware verfügten, sensible Daten gespeichert wurden. In allen Fällen, in denen unbefugte Zugriffe nicht allein durch räumliche und organisatorische Maßnahmen ausgeschlossen werden, habe ich die Verwaltungen darauf hingewiesen, daß die Datenhaltung nur auf dem Server oder – bei weniger sensiblen Daten – auf Disketten erfolgen darf. Die Disketten sind unter Verschluß zu halten und durch eine Registrierung in ihrem Bestand zu erfassen.

11.2
Aufzeichnung von Vermittlungsgesprächen in Telefonzentralen

Wiederholt gab es in der Vergangenheit bei verschiedenen öffentlichen Einrichtungen Planungen, sämtliche eingehenden Telefongespräche digital aufzuzeichnen, um bei Drohanrufen die Ernsthaftigkeit der Drohungen jederzeit überprüfen zu können. So hatte auch eine hessische Kommune in ihrer zentralen Telefonvermittlungsstelle das folgende Verfahren eingerichtet:

Zum Zwecke der Aufzeichnung von Drohanrufen wurde der Inhalt sämtlicher ankommenden Telefongespräche an den Vermittlungsplätzen der Telefonzentrale automatisch aufgezeichnet. Dabei waren alle Vermittlungplätze mit einer digitalen Aufzeichnungsbox verbunden. Diese Boxen sowie ein Kassettengerät, das die digitalen Signale in Sprache umwandeln und aufzeichnen konnte, befanden sich in einem durch Codekartenleser gesicherten Technikraum in einem verschlossenen Stahlschrank. Die Aufzeichnungsdauer betrug maximal acht Minuten, danach überspielte sich der Digitalspeicher wieder. Das heißt, eingehende Gespräche waren maximal acht Minuten lang gespeichert, es sei denn, ein Mitarbeiter der Telefonzentrale hätte durch Knopfdruck – im Falle eines Drohanrufs – automatisch den Mitschnitt in Sprache umwandeln und auf Kassette überspielen lassen.

Obwohl die Kommune umfangreiche organisatorische Maßnahmen zur Sicherung der Aufzeichnungen und zum Schutz vor unbefugter Auswertung getroffen hatte, war ich der Auffassung, daß die lückenlose Aufzeichnung sämtlicher eingehender Telefonanrufe – unabhängig ob Drohanruf oder nicht – sowohl gegen § 201 StGB als auch gegen Datenschutzrecht verstößt. Die Gemeinde war zwar auch der Auffassung, daß die Aufzeichnung eine Verletzung der Vertraulichkeit des Wortes i. S. v. § 201 StGB darstellt, allerdings war man der Meinung, daß dieses Handeln durch § 34 StGB gerechtfertigt sei, um mögliche Gefährdungen von gemeindlichen Bediensteten abwehren zu können. Dieser Argumentation habe ich folgendes entgegengehalten: Zwar können sich möglicherweise auch staatliche Stellen auf rechtfertigenden Notstand bei ihrem Handeln berufen, aber der staatliche Rückgriff auf § 34 StGB ist jedenfalls nur in außerordentlicher, unvorhersehbarer Lage bei tatsächlicher Gefahr für höchste Rechtsgüter zulässig. § 34 StGB gibt staatlichen Institutionen kein Recht, in geschützte Rechtsgüter einzelner Privatpersonen einzugreifen, indem z. B. jedes nicht öffentlich gesprochene Wort eines Anrufers bei der Gemeinde aufgezeichnet wird. Eine Rechtfertigung nach § 34 StGB und damit eine gerechtfertigte Aufzeichnung von Telefongesprächen kommt nur dann in Betracht, wenn ein gegenwärtiger – aktueller – Anlaß einer Gefahr für ein Rechtsgut der Verwaltung bzw. ihrer Mitarbeiter vorliegt. Unzweifelhaft ist die ganz überwiegende Mehrheit der ankommenden Telefongespräche nicht krimineller Natur. Ob und wann tatsächlich ein Drohanruf bei der Zentrale der Verwaltung eingeht, ist nicht absehbar, so daß auch nicht argumentiert werden kann, daß eine Aufzeichnung der Abwehr einer bestehenden gegenwärtigen Gefahr dient. Dies wäre vielmehr dann zu bejahen, wenn im Falle eines kriminellen Anrufes mitgeschnitten würde.

Zwar hat die Verwaltung ein berechtigtes Interesse daran, ihre Mitarbeiter vor möglichen Drohanrufen und Terrorangriffen zu schützen, und die Telefonverbindung ist unter Umständen die einzige Spur, die zum Täter führt. Diesem Interesse der Verwaltung steht jedoch das grundsätzlich geschützte Persönlichkeitsrecht aller nicht kriminellen Anrufer entgegen. Die vage und latente Gefährdung der Rechtsgüter der Mitarbeiter durch potentielle Drohanrufe steht der sich täglich vielfach wiederholenden Beeinträchtigung der Rechtsgüter zahlreicher Anrufer gegenüber. Daraus ergibt sich, daß die Voraussetzungen einer Anwendbarkeit des § 34 StGB auf staatliches Handeln in diesem Fall nicht erfüllt sind. Zulässig (und möglich) ist vielmehr der aktuelle Mitschnitt eines Telefongespräches, wenn sich herausstellt, daß es sich um einen Drohanruf handelt.

Aufgrund der von mir vorgetragenen rechtlichen Bedenken hat die Verwaltung die Aufzeichnung der Gespräche eingestellt.

11.3
Information über Grundstückskauf

Vielerorts in Hessen verlangen die Gemeinden beim Abschluß von Grundstückskaufverträgen, daß ihnen die kompletten Verträge vorgelegt werden, und zwar unabhängig davon, ob den Gemeinden ein Vorkaufsrecht zusteht oder nicht.

Die Gemeinden sehen eine derartige Forderung durch § 28 Abs. 1 BauGB gedeckt, wonach der Verkäufer der Gemeinde den Inhalt eines Kaufvertrags unverzüglich mitzuteilen hat; dies löse eine generelle Verpflichtung zur vollständigen Vorlage eines jeden Kaufvertrags aus.

Datenschutzrechtlich halte ich diese Forderungen nicht für zulässig. Vielmehr kann die Vorlage der Kaufverträge nur dann verlangt werden, wenn dies zur Aufgabenerfüllung der über das Vorkaufsrecht entscheidenden Stelle auch erforderlich ist. Dieses Erfordernis kann aber nur dann gegeben sein, wenn überhaupt ein Vorkaufsrecht besteht, wenn also die Voraussetzungen der §§ 24, 25 BauGB vorliegen – geregelt ist hier, in welchen Fällen der Gemeinde überhaupt ein Vorkaufsrecht zustehen kann –; denn nur dann hat die Gemeinde anhand des Kaufvertrags zu entscheiden, ob sie ihr Vorkaufsrecht ausüben will oder nicht. Besteht hingegen kein Vorkaufsrecht, muß die

Kommune also gar keine Entscheidung über eine eventuelle Ausübung treffen, ist auch der Inhalt des Kaufvertrags ohne Belang, mithin die Übersendung von Kaufverträgen zur Aufgabenerfüllung der Gemeinde nicht erforderlich.

Datenschutzrechtlich angemessen ist ein zweistufiges Verfahren, wie es u.a. in Bayern praktiziert wird. Zunächst wird die Gemeinde in einem ersten Schritt über die Umstände unterrichtet, die es ihr erlauben zu prüfen, ob für das verkaufte Grundstück überhaupt ein Vorkaufsrecht besteht. Kommt die Ausübung des Vorkaufsrechts in Betracht, dann kann die Gemeinde in einem zweiten Schritt die Übermittlung des vollständigen Inhalts des Kaufvertrags verlangen.

Dieses Verfahren entspricht dem Grundsatz, daß nur die jeweils notwendigen Daten an Dritte übermittelt werden.

11.4
Was macht die Ehefrau, wenn ihr Mann an der Sitzung der Stadtverordnetenversammlung teilnimmt?

Ein Stadtverordneter machte für die Teilnahme an einer Sitzung der Stadtverordnetenversammlung statt der üblichen Aufwandsentschädigung Kosten für Kinderbetreuung geltend. Die Stadt war zwar grundsätzlich bereit, diese Kosten zu tragen, verlangte aber vom Stadtverordneten darzulegen, was seine Ehefrau zum Zeitpunkt der Sitzung gemacht habe. Über dieses Ansinnen gerieten der Stadtverordnete und mit ihm seine Frau zu Recht in Rage.

Nach § 27 Abs. 1 HGO haben ehrenamtlich Tätige einen Anspruch auf Entschädigung. Diese Entschädigung kann einmal in der Höhe des Durchschnittssatzes, der in einer Satzung festgelegt ist, geleistet werden oder aber in Höhe des tatsächlich entstandenen Verdienstausfalls. Daneben regelt § 27 Abs. 1 Satz 5 HGO im zweiten Halbsatz ausdrücklich, daß anstelle des in der Satzung festgelegten Durchschnittssatzes die tatsächlich entstandenen und nachgewiesenen Aufwendungen, die wegen Inanspruchnahme einer Ersatzkraft zur Betreuung von Kindern, Alten, Kranken und Behinderten entstehen, verlangt werden können. Voraussetzung für die Geltendmachung von Kinderbetreuungskosten ist nach dieser Vorschrift also lediglich, daß dem ehrenamtlich Tätigen diese Kosten auch tatsächlich entstanden sind. Diesen Nachweis konnte die Stadt berechtigterweise fordern. Sie konnte dagegen nicht verlangen, daß der Stadtverordnete Nachweis über die Betätigung seiner Ehefrau zum Zeitpunkt der Sitzung führte; denn die Regelung des § 27 Abs. 1 Satz 5 HGO enthält keinen Passus darüber, daß die Möglichkeit der Geltendmachung von Kinderbetreuungskosten erst dann besteht, wenn andere Betreuungsmöglichkeiten, z. B. durch einen anderen Elternteil, nachgewiesenermaßen nicht möglich sind.

11.5
Behörde bringt Nachbarn gegeneinander auf

Bei der Durchführung eines Bauvorhabens äußerte der Nachbar des Bauherren Bedenken gegen die erteilte Baugenehmigung und bat die Baubehörde um Prüfung und ggf. Änderung der Auflagen. Die Einwände wurden von der Baubehörde als ungerechtfertigt eingestuft und hatten daher auf den Fortgang des Bauvorhabens keinen Einfluß. Der Beschwerdeführer wurde entsprechend informiert. Aber auch der Bauherr erhielt vom Bauamt Kopien der dort eingegangenen Beschwerdebriefe.

Eine solche Information des Bauherren über nicht berücksichtigte Beschwerden halte ich unter datenschutzrechtlichen Gesichtspunkten für unzulässig, da die Übersendung der Kopien weder zur Fortführung des Bauvorhabens noch zur Erfüllung der Aufgaben der Baubehörde erforderlich war. Nur durch eine Akteneinsicht in die eigene Bauakte hätte sich der Bauherr über eingegangene Beschwerden informieren können.

11.6
Weitergabe einer Namensliste über gewährte Zuschüsse zum Musikunterricht an einen städtischen Ausschuß

Aufgrund einer Bürgerbeschwerde wurde ich darauf aufmerksam, daß in einer Kommune der Ausschuß für Jugend, Sport und Soziales über gewährte Zuschüsse zum Musikunterricht durch Listen mit personenbezogenen Daten informiert wird. Im einzelnen enthielten die Listen über die betroffenen Bürger Angaben zu Name, Adresse, Bankverbindung, gezahlten Unterrichtsgebühren, dem erhaltenen Zuschußbetrag und der Anzahl der Kinder mit Musikunterricht.

Meine Nachfrage nach dem Sinn der detaillierten Aufschlüsselung der gewährten Zuschüsse bewirkte, daß auch die Kommune und der Ausschuß feststellten, daß eine Kontrolle der Haushaltsmittel für Zuschüsse in den meisten Fällen auch ohne Personenbezug möglich ist.

Künftig sollen die Ausschüsse nur noch in anonymisierter Form informiert werden, wenn zur Entscheidungsfindung keine näheren Informationen über den Kreis von Zuschußempfängern notwendig sind.

11.7
Anwesenheitslisten über Bürgerversammlungen

Ein Landrat bat mich um datenschutzrechtliche Bewertung des folgenden Sachverhalts:

In einer Gemeinde seines Landkreises wurde eine Bürgerversammlung nach § 8a HGO abgehalten. Die Vertreter der Gemeindeverwaltung führten auf dieser Versammlung keine Anwesenheitsliste. Eine ebenfalls anwesende Bürgerinitiative brachte jedoch eine derartige Liste in Umlauf mit der Zielsetzung, das Interesse der anwesenden Bürgerinnen und Bürger an einer Mitarbeit in der Bürgerinitiative zu erfragen. Überschrieben war die Anwesenheitsliste mit

"Bürgerversammlung – Anwesenheitsliste; Datum, Ort". Der Urheber der Liste war nicht erkennbar. Nach Ende der Sitzung nahm die Bürgerinitiative die Liste an sich.

Im Verlauf der Sitzung trug sich auch ein Fraktionsvorsitzender einer im Gemeindeparlament vertretenen Partei in die Liste ein, verneinte aber das Interesse an einer Mitarbeit in der Bürgerinitiative. Diese Information über das Desinteresse des Fraktionsvorsitzenden an einer Mitarbeit in der Bürgerinitiative gelangte im anschließenden Kommunalwahlkampf an die Öffentlichkeit. Als Informanten kamen sowohl die Bürgerinitiative in Betracht als auch diejenigen Bürger, die sich nach dem Fraktionsvorsitzenden in die Liste eingetragen hatten.

Der Fraktionsvorsitzende beschwerte sich daraufhin bei der Gemeinde, die wiederum u.a. die folgenden Fragen geklärt wissen wollte:

1. Hätte sie das Führen einer Anwesenheitsliste durch die Bürgerinitiative verhindern müssen?
2. Ist ihr ein Versäumnis vorwerfbar, weil sie die Vertreter der Bürgerinitiative nicht auf die sensible Verwendung geschützter Daten hingewiesen hat?

Der Landrat vertrat in seiner Eingabe an meine Dienststelle die Auffassung, daß es jedenfalls seitens der Gemeinde keine Verpflichtung gegeben habe, eine Anwesenheitsliste zu führen.

Rechtsgrundlage für das Abhalten einer Bürgerversammlung ist § 8a HGO. Aus dieser Vorschrift ergibt sich nicht, in welcher Form eine Bürgerversammlung abzuhalten ist. Insbesondere besteht für die Versammlungsleitung – nach § 8a Abs. 3 HGO ist dies der Vorsitzende der Gemeindevertretung –, keine rechtliche Verpflichtung zum Führen einer Anwesenheitsliste. Seitens der Versammlungsleitung wäre das Führen einer derartigen Liste nur zulässig, wenn deutlich gemacht wäre, wer die Daten zu welchem Zweck erhebt und daß die Angabe der Daten freiwillig erfolgt.

So wenig jedoch § 8a HGO über den positiven Ablauf einer Bürgerversammlung aussagt, so wenig legt er fest, was dort unter gar keinen Umständen geschehen darf. Eine rechtliche Verpflichtung der Gemeinde, einer Bürgerinitiative zu untersagen, eine Anwesenheitsliste herumgehen zu lassen, enthält die Hessische Gemeindeordnung jedenfalls nicht. Auch trägt die Gemeinde keine Verantwortung dafür, wie die Bürgerinitiatvie die Daten verwendet. Allerdings wird man ein Einschreiten durch den Versammlungsleiter dann erwarten müssen, wenn die Bürgerinitiative sich erkennbar als "Verwaltung" geriert.

Im übrigen wird man von einem mündigen Bürger erwarten können, daß er sich bei Eintrag in eine derartige Liste, in der noch dazu das Interesse an der Mitarbeit in einer Bürgerinitiative erfragt wird, Gedanken über die Verwendung macht bzw. bei Zweifeln an der Herkunft der Liste dies in einer solchen Versammlung hinterfragt. Aus dem vorgetragenen Sachverhalt ergaben sich keine Anhaltspunkte dafür, daß sich die anwesenden Bürger rechtlich verpflichtet sahen, sich in die Liste einzutragen.

11.8
Fehlbelegungsabgabe

Starre Programmvorgaben, vorgegebene Formulare, Stempel etc. verleiten Behörden des öfteren ohne böse Absicht zur Beeinträchtigung des Rechts auf informationelle Selbstbestimmung der Bürger. Zum Beispiel im Zusammenhang mit der im Jahr 1993 eingeführten Fehlbelegungsabgabe für öffentlich geförderte Wohnungen sind mir solche Vorkommnisse bekannt geworden. Sie konnten ohne große Mühe oder finanziellen Aufwand abgestellt werden.

Ein Wohnungsamt kennzeichnete Briefumschläge mit Unterlagen zur Berechnung der Fehlbelegungsabgabe mit einem Stempelaufdruck "Fehlbelegungsabgabe". Es verstößt grundsätzlich gegen den Datenschutz, wenn man anhand eines verschlossenen Briefumschlages Rückschlüsse auf den Inhalt des Briefes ziehen kann. Die Beschwerde eines Bürgers führte dazu, daß das Wohnungsamt diese Stempel inzwischen nicht mehr verwendet.

In einer anderen Stadt wurde die Mieterin einer Sozialwohnung aufgefordert, Angaben zur Höhe ihres Einkommens nachzureichen, obwohl die tatsächlich zu zahlende Miete über der sogenannten Kappungsgrenze liegt und somit unabhängig vom Einkommen keine Fehlbelegungsabgabe zu zahlen ist.

Meine Nachfrage bei der Kommune ergab, daß mit Hilfe des eingesetzten EDV-Programms generell ohne Angaben zu den Einkommensverhältnissen keine Bescheide erstellt werden können. Daher wurden unabhängig vom Einzelfall alle im Fragebogen aufgeführten Daten beim Bürger erhoben. Inzwischen wurde das EDV-Programm zur Ermittlung der Fehlbelegungsabgabe so modifiziert, daß auch für Bürger, für die sich aufgrund der Miethöhe eine Einkommenserklärung erübrigt, entsprechende Bescheide erstellt werden können.

12. Melderecht

12.1
Online-Verbindung zwischen Polizei und Meldebehörde – Programmfehler

Ein Jugendlicher aus dem Main-Taunus-Kreis geriet in den Verdacht, eine Straftat begangen zu haben. Während seiner Vernehmung durch die Polizei wurde er gefragt, ob er adoptiert sei. Dies war tatsächlich der Fall. Verwundert fragte mich der Vater des Jungen, ob es rechtens sei, daß die Polizei, mit der sein Sohn noch nie etwas zu tun hatte, über diese Information verfügt.

Nach einer Stellungnahme der Polizeibehörde hatte der Beamte zum Zweck der Personalienüberprüfung die Daten der Meldebehörde des Wohnorts des Jugendlichen abgerufen. Nach § 13 der Meldedatenübermittlungsverordnung

vom 24. September 1990 (GVBl. I S. 590) dürfen die Meldebehörden personenbezogene Daten im automatisierten Verfahren zum Abruf für Polizeidienststellen bereithalten. Absatz 1 der Vorschrift zählt genau und abschließend den zum Abruf bereitzuhaltenden Datensatz auf. Zu diesen Daten gehört nicht die Information, daß ein Einwohner adoptiert ist. Trotzdem konnte anhand der nach § 10 Abs. 3 HDSG vom Kommunalen Gebietsrechenzentrum erstellten Protokolle festgestellt werden, daß der Polizei im Wege des Direktabrufs die Information zur Verfügung gestellt wurde, daß wegen einer Adoption eine gegenüber nichtöffentlichen Stellen geltende Auskunftssperre verfügt war. Dies war nicht mit § 13 Abs. 1 der Meldedatenübermittlungsverordnung vereinbar.

Das Hessische Innenministerium, das ich auf diesen Sachverhalt aufmerksam machte, hat sofort eine Korrektur des landeseinheitlichen ADV-Verfahrens "Grundstufe Einwohnerwesen" veranlaßt. Der Polizeibeamte, der den Jungen vernahm, wurde von seiner Dienststellenleitung belehrt. Er konnte zwar nicht wissen, daß das Datenverarbeitungsverfahren fehlerhaft war, hätte den Jugendlichen aber nicht auf die Adoption ansprechen dürfen. Schließlich wäre es möglich gewesen, daß der Jugendliche von seiner Adoption keine Kenntnis hatte.

Den Vater des Jugendlichen habe ich noch auf folgendes hingewiesen: Die nach § 34 Abs. 7 des Hessischen Meldegesetzes über die Daten seines Sohnes verfügte Auskunftssperre soll eigentlich genau das vermeiden, was sie im vorliegenden Falle bewirkt hat. Sie dient dem Ausforschungsverbot des § 1758 BGB und soll u.a. verhindern, daß die Tatsache der Adoption unberechtigten Dritten bekannt wird. Ist aber eine Adoption vollzogen und hat die Meldebehörde den früheren Familiennamen des Kindes gelöscht, weist gerade die Auskunftssperre auf die Adoption hin. Es kann daher zweckmäßig sein, auf die Auskunftssperre zu verzichten. Nach deren Wegfall kann niemand mehr unbeabsichtigt über die Adoption informiert werden. Selbst die Meldebehörde kann nicht mehr auf Anhieb erkennen, daß überhaupt eine Adoption stattgefunden hat.

12.2
Mangelhafte Aufklärung der Bürger bei der Beantragung von Führungszeugnissen

Die Vorlage eines Führungszeugnisses ist im öffentlichen Dienst regelmäßig und in der Privatwirtschaft gelegentlich Voraussetzung für die Einstellung von Stellenbewerbern. Auch um behördliche Genehmigungen zu erlangen, z.B. eine Fahrerlaubnis, einen Waffenschein oder eine Gewerbekonzession, werden Führungszeugnisse benötigt. Sie geben Auskünfte, ob über die Betroffenen in dem beim Generalbundesanwalt geführten Bundeszentralregister Straftaten registriert sind und wenn ja, welche. Aber nicht alle Eintragungen im Strafregister werden in das Führungszeugnis aufgenommen.

Je nachdem, ob das Führungszeugnis für private, allgemeine behördliche oder bestimmte behördliche Zwecke benötigt wird, gelten unterschiedliche Bagatellgrenzen (§ 32 BZRG). Beispielsweise wird eine Verurteilung zu einer Geldstrafe von 50 Tagessätzen nicht in das Führungszeugnis für private oder allgemeine behördliche Zwecke aufgenommen. Stand die Verurteilung aber im Zusammenhang mit der Ausübung eines Gewerbes und wird das Führungszeugnis für die Zulassung zu einem Gewerbe benötigt, erfolgt die Eintragung doch (§ 32 Abs. 4 BZRG). Nach einer bestimmten Frist wird eine im Register eingetragene Verurteilung nicht mehr in ein Führungszeugnis aufgenommen (§ 33 BZRG).

Bestimmte Behörden erhalten – teilweise nur für bestimmte Zwecke – unbeschränkte Registerauskünfte, z.B. die für waffenrechtliche Erlaubnisse zuständige Stelle (§ 41 BZRG). Für sie gelten keine Bagatellgrenzen und nicht die Frist, nach der eine Verurteilung nicht mehr in ein Führungszeugnis aufzunehmen ist. Erst nach Ablauf einer längeren Frist (Tilgungsfrist) wird eine Eintragung gelöscht, und der Betroffene hat wieder eine "weiße Weste" (§ 46 BZRG), wobei wiederum bestimmte Verurteilungen, z.B. zu lebenslanger Freiheitsstrafe, nicht der Tilgung unterliegen (§ 45 Abs. BZRG).

Das Führungszeugnis wird bei der Meldebehörde beantragt (§ 30 Abs. 2 BZRG). Damit die Behörde des Generalbundesanwalts erkennen kann, ob eine Verurteilung in den Registerauszug einzutragen ist, muß der Antragsteller der Meldebehörde mitteilen, ob das Führungszeugnis für private Zwecke oder für behördliche und, falls für behördliche, für welche Zwecke benötigt wird (Ziff. 2.16 – Zweite allgemeine Verwaltungsvorschrift zur Durchführung des BZRG – Beilage zum BAnz Nr. 153 vom 22. August 1985).

Dient die Urkunde behördlichen Zwecken, muß das Bundeszentralregister das Führungszeugnis unmittelbar der öffentlichen Stelle, die es benötigt, zustellen (§ 30 Abs. 5 BZRG). Der Betroffene kann nicht verlangen, daß ihm das Dokument nach Hause geschickt wird. Damit soll verhindert werden, daß evtl. Eintragungen, die in einem für private Zwecke bestimmten Auszug nicht aufzuführen wären, dem privaten Umfeld des Betroffenen bekannt werden. Außerdem könnte der Betroffene aufgrund privater "Zwangssituationen" in die Verlegenheit geraten, den Auszug interessierten Personen eben doch zu zeigen. Diese Möglichkeit soll ausgeschlossen werden, indem die Antragsteller erst gar keine Verfügungsgewalt über das für Behörden bestimmte Führungszeugnis erhalten.

Die "private Zwangssituation", die den Betroffenen veranlassen könnte, den Registerauszug gegen seinen Willen anderen Personen vorzulegen, erscheint nur auf den ersten Blick etwas weit hergeholt. Beispielsweise wurde vor kurzem unter den Datenschutzbeauftragten erörtert, wie der Entwicklung entgegen gewirkt werden kann, daß private Sicherheitsunternehmen dazu übergehen, von Stellenbewerbern die Vorlage einer Selbstauskunft der Polizei nach § 28 HSOG zu verlangen. Der Wille des Gesetzgebers ist eindeutig: § 30 Abs. 5 BZRG dient dem Schutz der Betroffenen. Trotzdem wird die Vorschrift sowohl von Antragstellern als auch von Meldebehörden oft mißverstanden. Regelmäßig wenden sich Personen an mich, die anführen, die Meldebehörde habe ihnen erklärt, daß sie das Führungszeugnis nicht einsehen dürften. Sie fürchten geheime Datenspeicherungen, die anderen Behörden übermittelt werden, ohne daß sie sie selbst zur Kenntnis nehmen dürfen.

Das ist natürlich nicht gewollt und auch nicht zutreffend. Die Behörde hat dem Antragsteller auf Verlangen Einsicht in das Führungszeugnis zu gewähren. Auch kann der Antragsteller verlangen, daß das Führungszeugnis, wenn es Eintragungen enthält, zunächst an ein von ihm benanntes Amtsgericht übersandt wird. Dort kann es der Betroffene einsehen und entscheiden, ob es vernichtet oder an die Behörde weitergeleitet werden soll. Die Meldebehörde ist gesetzlich verpflichtet (§ 30 Abs. 5 BZRG), die Antragsteller auf diese Möglichkeit hinzuweisen. Leider unterbleibt dieser Hinweis oft.

Ich habe das Hessische Innenministerium über diesen Sachverhalt informiert und gebeten, die Meldebehörden auf die Rechtslage hinzuweisen. Das Ministerium hat dem leider nicht entsprochen. Es sieht dazu noch keine Veranlassung; weil dort bisher keine Beschwerden eingegangen sind, geht es von einem Einzelfall aus. Da mir gegensätzliche Erkenntnisse vorliegen, habe ich erneut mit dem Ministerium Kontakt aufgenommen. Ich halte nach wie vor einen entsprechenden Hinweis an die Gemeinden für erforderlich.

12.3
Adreßlisten an Ausländerbeiräte

Im Vorfeld der Europawahl häuften sich die Anfragen von Einwohnermeldeämtern, ob an Ausländerbeiräte Listen von nichtdeutschen Wahlberechtigten herausgegeben werden dürfen. Die Ausländerbeiräte gaben in der Regel an, die Daten zu benötigen, um die Wähler über ihre Arbeit und die Europawahl zu informieren.

Eine Auskunft nach § 35 Abs. 1 HMG (Melderegisterauskünfte im Zusammenhang mit Wahlen) halte ich für unzulässig. Diese Vorschrift eröffnet die Möglichkeit, Auskünfte über Wahlberechtigte an Parteien oder Wählergruppen zu erteilen, die sich an einer Wahl beteiligen. Diese Voraussetzungen waren bei den Ausländerbeiräten anläßlich der Europawahl nicht erfüllt.

Etwas anderes gilt nach § 31 Abs. 1 HMG (Datenübermittlung an andere Behörden oder sonstige öffentliche Stellen).

Seit Einrichtung. Aufgaben und Befugnisse der Ausländerbeiräte in der Hessischen Gemeindeordnung geregelt sind, sind sie als öffentliche Stelle zu betrachten. Dies rechtfertigt sich aus ihrer gesetzlichen Stellung als Interessenvertreter der ausländischen Einwohner, welche die Organe der Gemeinde beraten und in allen wichtigen Angelegenheiten zu hören sind. Sie sind an öffentlichen Aufgaben im weiteren Sinne beteiligt. Für ihre Aufgaben sind ihnen Haushaltsmittel zur Verfügung zu stellen. Ihre Mitglieder sind ehrenamtlich und unabhängig; sie unterliegen der Verschwiegenheitspflicht und der Treuepflicht gegenüber der Gemeinde.

Folglich können den Ausländerbeiräten nach § 31 Abs. 1 HMG jeweils Grunddaten auf Anfrage zur Verfügung gestellt werden, wenn diese zur rechtmäßigen Erfüllung ihrer Aufgaben erforderlich sind. Um diese Erforderlichkeit festzustellen, hat die Meldebehörde eine Plausibilitätsprüfung der vorgetragenen Gründe vorzunehmen.

In den vorliegenden Fällen, wo Ausländerbeiräte Adreßlisten zu Informationszwecken verlangten, konnte ich bislang die Erforderlichkeit der Datenübermittlung nicht annehmen. Sicherlich wäre eine Datenübermittlung zweckmäßig gewesen. Dies reicht aber für die Annahme der Erforderlichkeit nicht aus, denn es war nicht anzunehmen, daß die betroffenen Ausländerbeiräte ihre Aufgaben nicht oder nicht vollständig erfüllen konnten. Es gibt zahlreiche andere Möglichkeiten, die ausländischen Wahlberechtigten zu informieren, beispielsweise durch Veröffentlichungen in Zeitungen, Postwurfsendungen, Informationsveranstaltungen und ähnliches. Gerade bei den verlangten listenmäßigen Datenübermittlungen besteht nämlich sehr leicht die Gefahr, daß – beabsichtigt oder unbeabsichtigt – Löschungen nicht ordnungsgemäß durchgeführt werden und so unzulässige Datensammlungen entstehen. Zudem ist mir bekannt, daß es auch ausländische Einwohner gibt, die die Übermittlung ihrer Daten an die Ausländerbeiräte nicht wünschen.

Wenn der betroffene Ausländerbeirat ein persönliches Anschreiben für sinnvoll hält, die Erforderlichkeit aber nicht vorliegt, kann er auf die sog. "Konsulatslösung" verwiesen werden. Das bedeutet, daß der Ausländerbeirat seine Anschreiben der Gemeinde bzw. dem zuständigen Kommunalen Gebietsrechenzentrum der Gemeinde zur Verfügung stellt. Die Schreiben werden dann dort adressiert, ohne daß es zu einer Datenübermittlung kommen muß.

Mit dieser Verfahrensweise wird sowohl dem Informationsbedürfnis des Ausländerbeirats als auch dem Schutz der persönlichen Daten der Betroffenen ausreichend Rechnung getragen.

12.4
Bekanntgabe der Anschrift des Frauenhauses durch ein Meldeamt

"Inwieweit ist das Einwohnermeldeamt berechtigt bzw. verpflichtet, Auskunft über die Adresse des Frauenhauses zu erteilen?"

Das war die Frage der Mitarbeiterin eines autonomen Frauenhauses, in dem es zu Belästigungen durch einen Mann gekommen war, der seine Frau suchte. Der offensichtlich zu Gewalttätigkeiten neigende Mann vermutete sie im Frauenhaus und hatte die Anschrift vom Einwohnermeldeamt erhalten. Die Frau war bereits zuvor aus Sicherheitsgründen anderweitig untergebracht worden.

Der zuständige Sachbearbeiter des Amts stellte sich auf den Standpunkt, das autonome Frauenhaus sei mit einer öffentlichen Einrichtung vergleichbar. Es gehöre zu den Aufgaben einer kommunalen Verwaltung, die sich als Dienstleistungsunternehmen verstehe, auskunfts- und hilfesuchenden Bürgern, die ein berechtigtes Interesse darlegen, entsprechende Auskünfte über Anschriften von Vereinen, Ärzten und öffentlichen Einrichtungen zu erteilen. Gegenüber der Mitarbeiterin des Frauenhauses lehnte er es ab, etwaige Auskünfte auf die Bekanntgabe der Telefonnummer

des Frauenhauses zu beschränken. Er sah in der Bekanntgabe der Anschrift des Frauenhauses auch kein datenschutzrechtliches Problem, da kein personenbezogenes Datum mitgeteilt worden sei.

Die Ansichten des Sachbearbeiters waren aus mehreren Gründen unzutreffend:

Zunächst wird die Adresse des Frauenhauses durch die Mitteilung an einen Dritten, der nach dem Aufenthalt einer bestimmten Frau forscht, zu einem personenbezogenen Datum, weil damit gleichzeitig die Adresse der Betroffenen offenbart wird.

Außerdem gehört es weder zu den im Hessischen Meldegesetz geregelten Aufgaben eines Meldeamts, Daten privater Einrichtungen zu verarbeiten, noch ist deren Verarbeitung zur Aufgabenerfüllung erforderlich. Hinzu kommt, daß die Frauen, die unter der Anschrift des Frauenhauses gemeldet sind, in der Regel aus Sicherheitsgründen eine Auskunftssperre beantragt haben.

Mit der freizügigen Bekanntgabe der Anschrift des Frauenhauses umgeht das Meldeamt den durch das Hessische Meldegesetz gewährten Schutz der Einzelperson.

Im übrigen hat die kommunale Verwaltung, auch wenn sie aus Bürgernähe freiwillige Leistungen erbringen will, den Grundsatz der Verhältnismäßigkeit zu beachten. Bei der Adresse des Frauenhauses handelt es sich natürlich nicht um eine allgemein zugängliche Adresse. Sie ist noch nicht einmal im Telefonbuch verzeichnet. Die Bekanntgabe der Adresse kann die schutzwürdigen Interessen der gesuchten Frau verletzen. Eine sachgerechte Interessenabwägung kann von dem auskunftsbereiten Verwaltungsmitarbeiter nicht verantwortet werden.

Letztendlich hat die betroffene Stadtverwaltung auf meine Intervention hin dann doch ihre Mitarbeiter angewiesen, bei zukünftigen Anfragen nach dem Frauenhaus nur die Telefonnummer bzw. die Anschrift des "Frauentreffs" der Stadt, der im Dienstgebäude Räumlichkeiten nutzt, mitzuteilen.

12.5
Auskünfte an Pächter eines Bürgerhauses

Eine Bürgerin hatte im Bürgerhaus ihrer Gemeinde einen Saal für ihre Geburtstagsfeier angemietet.

Das Bürgerhaus wird zwar durch einen Pächter bewirtschaftet, sie wollte sich jedoch um die Speisen und Getränke selbst kümmern. Um so erstaunter war sie, als sie bereits nach wenigen Tagen ein Anschreiben des Pächters erhielt, in dem er sich und sein versiertes Team als Ausrichter der Feier anbot.

Die Bürgerin wandte sich an mich mit der Bitte um Aufklärung.

Der Datenschutzbeauftragte der Gemeinde hat auf mein entsprechendes Schreiben hin umgehend reagiert. Aus Gründen der Arbeitserleichterung sei dem Pächter eine Durchschrift der Anmietungsbestätigung für die Antragsteller weitergeleitet worden, damit er von der Raumbelegung Kenntnis erhalten und seinerseits disponieren könne. Der Pächter jedoch nutzte die über die Beleginformation hinaus enthaltenen Daten für eigene Werbezwecke.

Diese Vorgehensweise wurde unverzüglich abgestellt. Dem Pächter wird in Zukunft lediglich noch die Vergabe des Raumes ohne Mitteilung des Namens und Anlasses des Nutzers bekanntgegeben.

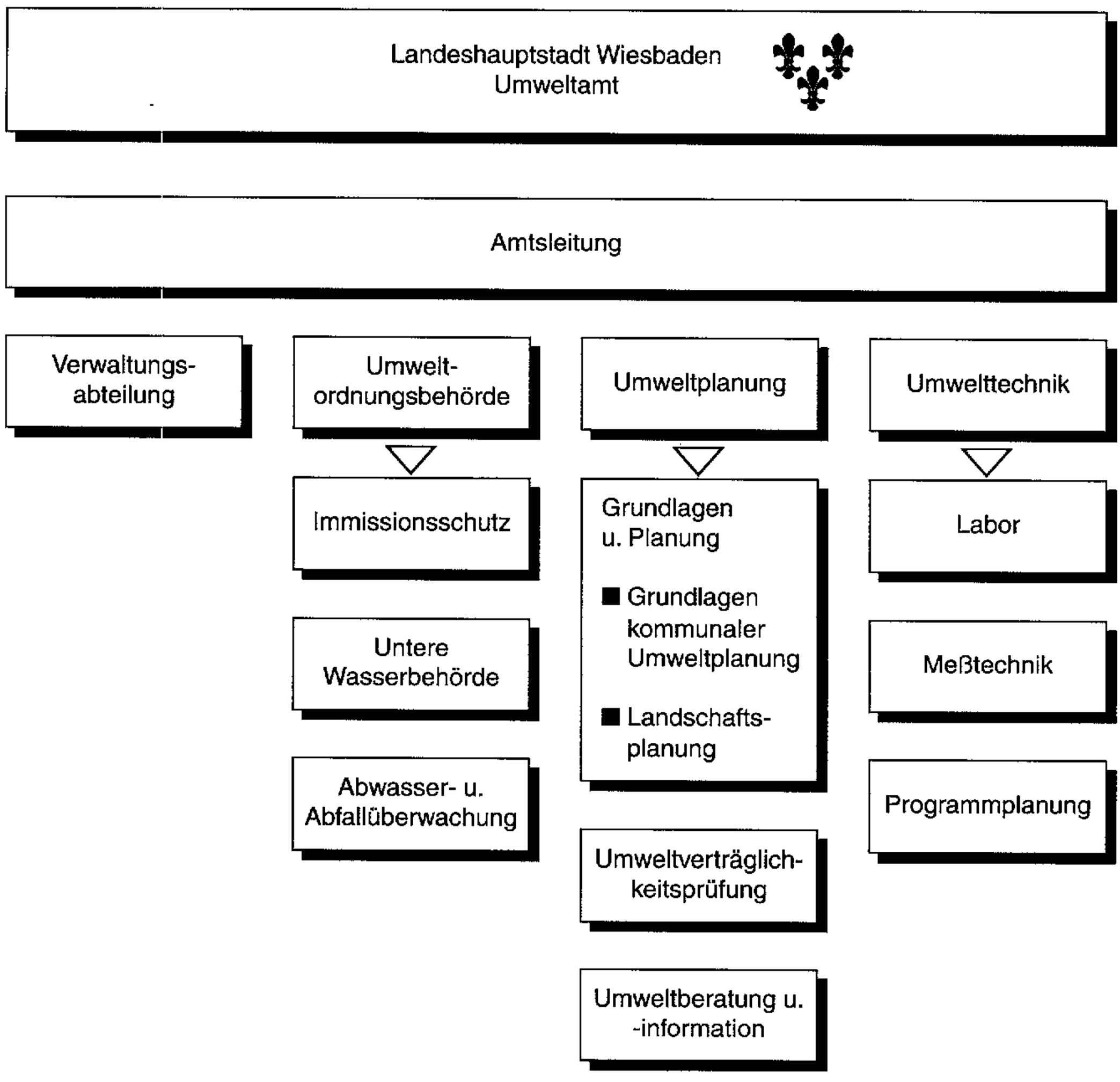
13. Umwelt

13.1
Prüfungen bei Umweltämtern

Datenschutz dient im Umweltbereich nicht selten als Vorwand, unbequeme Auskünfte nicht zu erteilen. Dies führt dazu, daß in der Öffentlichkeit manchmal der falsche Eindruck entsteht, der Datenschutz stehe einem wirksamen Umweltschutz im Wege. Um mir ein Bild von der Datenschutzsituation im Umweltbereich zu verschaffen, insbesondere um die bereits eingesetzten EDV-Verfahren, die Maßnahmen der Datensicherung und evtl. Datenschutzprobleme in der Umweltverwaltung kennenzulernen, habe ich bei einer Anzahl von Umweltämtern der Städte und Landkreise Prüfbesuche gemacht.

Um optimal wirksam sein zu können, müßte ein Umweltamt alle die Ämter zusammenfassen, die sich mit Umweltschutz beschäftigen; dies betrifft hauptsächlich die Gebiete des Immissionsschutzes (insbesondere Lärmbekämpfung), der Gewässerreinhaltung (insbesondere Abwasserbeseitigung) und der Abfallwirtschaft (also der Müllentsorgung und der Altlastenbeseitigung); daneben Teilgebiete aus anderen Ämtern, beispielsweise Bauaufsicht, Untere Naturschutzbehörde, Gesundheitsamt. Vorbildlich ist insoweit die Organisation der Umweltämter in mehreren hessischen Großstädten, beispielsweise in der Landeshauptstadt Wiesbaden und in Frankfurt am Main: In beiden Städten sind die Hauptgebiete des Umweltschutzes nämlich unter dem Dach des Umweltamts zusammengefaßt. In Wiesbaden geschieht dies in Form einer "Umweltordnungsbehörde" (siehe Grafik S. 51).

Daneben kommen in der Abteilung "Umweltplanung" auch die übrigen umweltrelevanten Aufgabengebiete zum Zuge.



In Frankfurt am Main bestehen die drei Bereiche "Verwaltung", "Umweltvorsorge" und "Umweltüberwachung" (siehe Grafik S. 52).

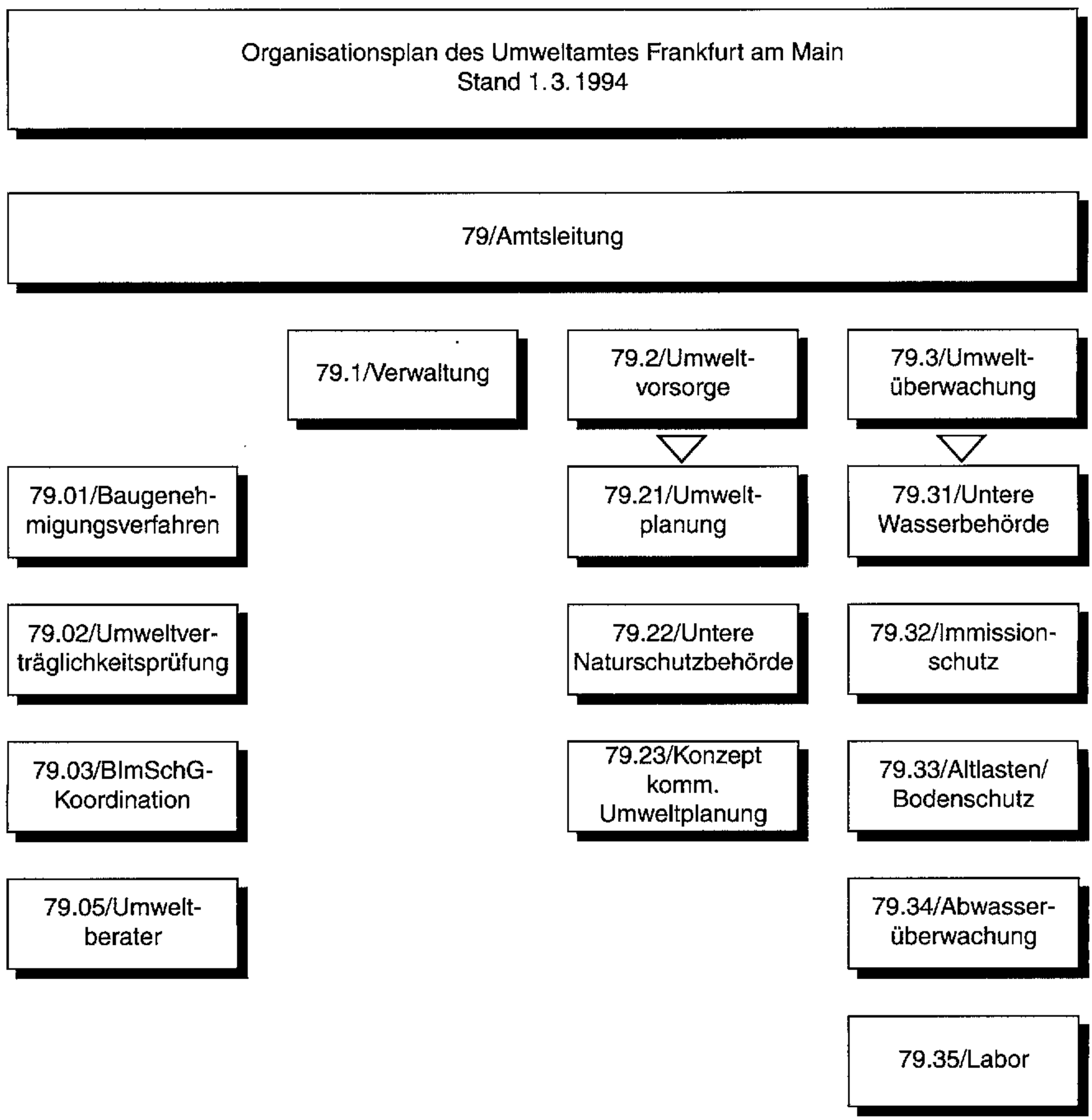
In beiden Organigrammen fällt auf, daß die (staatliche) Untere Wasserbehörde und die (kommunale) Abwasserüberwachung in einer Abteilung unter einem gemeinsamen Abteilungsleiter vereinigt sind. Das ist deshalb möglich, weil nach § 93 Abs. 4 HWG die Aufgaben der Unteren Wasserbehörde dem Magistrat als Weisungsaufgabe übertragen sind, d.h. der Magistrat ist Untere Wasserbehörde.

Anders ist dies jedoch bei den Landkreisen: Hier gehört die Untere Wasserbehörde zur unteren Staatlichen Verwaltungsbehörde "Der Landrat", während die kommunale Abwasserüberwachung Teil der selbständigen Behörde "Der Kreisausschuß" ist. Nur in der Person des Landrats haben beide eine gemeinsame Spitze.

Es liegt auf der Hand, daß die Verschiedenheit der Organisationsformen nicht dazu beiträgt, daß Aufgaben des Umweltschutzes effektiv bewältigt werden: Eine Datenübermittlung beispielsweise ist nur dann unproblematisch, wenn – in bestimmten Bereichen – von einer Zweckgleichheit der Aufgaben ausgegangen werden kann – so, wie sie ähnlich in § 105 HWG (s.u.) bestimmt ist.

Die Grundlage eines effektiven Umweltschutzes bilden rasche, präzise und ausführliche Informationen von einer Umweltdienststelle zur anderen. Um diese zu ermöglichen, haben einige Landesgesetze die strengeren Zweckbindungsvorschriften, die das Hessische Datenschutzgesetz zum Schutz des einzelnen enthält, zum Nutzen der Allgemeinheit im Sinne des Umweltschutzes erweitert, wie z.B. § 105 des Hessischen Wassergesetzes vom 22. Januar 1990 – HWG – (GVBl. I S. 114) und § 26 des Hessischen Abfallwirtschafts- und Altlastengesetzes vom 26. Februar 1991 – HAbfAG – (GVBl. I S. 106).

So bestimmt z.B. § 105 HWG, daß die zu einem in Satz 3 genannten Zwecke (Durchführung der Wasseraufsicht, von Genehmigungs-, Anzeige- oder Zulassungsverfahren, Durchführung der Gewässerüberwachung ...) verarbeiteten



personenbezogenen Daten zu jedem anderen in Satz 3 genannten Zwecke weiterverarbeitet werden dürfen; ähnlich ist die Regelung in § 26 HAbfAG. Durch diese Gleichsetzung mehrerer Umweltzwecke wird gewährleistet, daß die in einem Amt vorhandenen Umweltdaten nicht von einem anderen Amt für Umweltzwecke neu erhoben werden müssen. Dadurch wird nicht nur erheblicher zusätzlicher Aufwand an Personal- und Sachkosten vermieden, sondern vor allem eine zeitliche Verzögerung notwendiger Umweltmaßnahmen.

Ein Fall, zu dem ich mehrere Eingaben von Stadt- und Kreisverwaltungen erhalten hatte, zeigt besonders anschaulich die Schwierigkeiten, die einer raschen und effizienten Umweltverwaltung im Wege stehen können. Es ging dabei um die Frage der datenschutzrechtlichen Zulässigkeit einer Datenübermittlung zwischen der Unteren Wasserbehörde und der Kommunalen Abwasserüberwachung:

Nach § 105 Abs. 1 Ziff. 1 HWG i. V. m. § 94 Abs. 1 HWG ist die Untere Wasserbehörde berechtigt, zum Zwecke der Durchführung der Wasseraufsicht "die notwendigen personenbezogenen Daten zu erheben und in sonstiger Weise zu verarbeiten", z. B. also auch weiter zu übermitteln. Die "Verordnung über das Einleiten oder Einbringen von Abwasser mit gefährlichen Stoffen in öffentlichen Abwasseranlagen (Indirekteinleiterverordnung – VGS) vom 9. Dezember 1992 (GVBl. I S. 675) bestimmt in § 1, daß im Gegensatz zu der allgemeinen Erlaubnispflicht für das Einleiten gefährlicher Stoffe in öffentliche Abwasseranlagen bestimmte Arten von Einleitungen ausgenommen sind; dazu gehört nach § 1 Abs. 1 Ziff. 3c "mineralölhaltiges Abwasser" unter bestimmten Voraussetzungen. Eine solche Einleitung ist nach § 2 Abs. 1 Indirekteinleiterverordnung der Unteren Wasserbehörde schriftlich anzuzeigen. In der Praxis gilt diese Anzeigepflicht vor allem für Tankstellen und Kfz-Werkstätten.

Parallel dazu hat die Kommunale Abwasserüberwachung die Aufgabe, die von der betreffenden Stadt bzw. dem Landkreis betriebene Abwasser-Aufbereitungsanlage (Kläranlage) nach § 4 Abs. 1 der "Verordnung über die Eigenkontrolle von Abwasseranlagen (Abwassereigenkontrollverordnung – EKVO)" vom 22. Februar 1993 (GVBl. I S. 69) dahingehend zu überwachen, ob mineralölhaltige Abwässer in diese eingeleitet werden. Es lag deshalb nahe zu überlegen, ob nicht die bei der Unteren Wasserbehörde vorliegenden Anzeige-Daten bezüglich der Einleitung mineralölhaltiger Abwässer an die Kommunale Abwasserüberwachung übermittelt werden könnten.

Da die Kommunale Abwasserüberwachung jedoch nicht zu den in § 105 Abs. 1 HWG aufgeführten Behörden gehört, ist hier eine Anwendung dieser bereichsspezifischen Vorschrift nicht möglich. Nach den Vorschriften des Hessischen Datenschutzgesetzes muß einer Prüfung der Zulässigkeit der Datenübermittlung nach § 14 die Prüfung vorausgehen, ob der Grundsatz der Zweckbindung (§ 13 Abs. 1 HDSG) eingehalten oder aber eine seiner Ausnahmen (§ 13 Abs. 2 i.V.m. § 12 Abs. 2 HDSG) gegeben ist.

Bei näherer Betrachtung kann kein Zweifel daran bestehen, daß es sich sowohl bei der Unteren Wasserbehörde als auch bei der Kommunalen Abwasserüberwachung um die Aufgabe der "Überwachung von Abwasser mit mineralölhaltigen Inhaltsstoffen, das in öffentliche Abwasser eingeleitet wird", handelt. Das bedeutet: Auch bei einer Verschiedenheit der Aufgaben der Unteren Wasserbehörde und der Kommunalen Abwasserüberwachung im übrigen besteht eine Deckungsgleichheit bei dem hier betrachteten Zweck der Kontrolle der Einleitung mineralölhaltiger Abwässer. Der Grundsatz der Zweckbindung würde also durch eine Datenübermittlung von Unterer Wasserbehörde an Kommunale Abwasserüberwachung nicht verletzt. Ebensowenig ist zweifelhaft, daß die Datenübermittlung insoweit "zur Erfüllung von Aufgaben des Empfängers erforderlich ist" (§ 14 Abs. 1 HDSG), da § 4 der Eigenkontrollverordnung der Kommunalen Abwasserüberwachung diese Aufgabe zugewiesen hat.

In Zusammenarbeit zwischen den beteiligten Kommunal- bzw. Kreisverwaltungen, dem hessischen Umweltministerium und meiner Dienststelle konnte daher eine sowohl bürgerfreundliche als auch kostengünstige Lösung in der Weise erreicht werden, daß eine Datenübermittlung zwischen Unterer Wasserbehörde und Kommunaler Abwasserüberwachung – auch ohne die zunächst für erforderlich gehaltene Zustimmung der Betroffenen – aus der Sicht des Datenschutzes zulässig ist.

Ich habe die Erfahrungen aus diesem Fall – der mir sowohl von der Stadt Frankfurt als auch vom Landrat des Landkreises Fulda vorgelegt worden war – zum Anlaß genommen, dem hessischen Umweltministerium eine Ergänzung von § 105 HWG vorzuschlagen: In den Kreis der dort aufgeführten Behörden sollte auch die Kommunale Abwasserüberwachung einbezogen werden. Dann ist für die Datenübermittlung zwischen der Unteren Wasserbehörde und der Kommunalen Abwasserüberwachung eine klare Zulässigkeitsnorm vorhanden. Da der Kommunalbehörde dadurch nur ein Recht eingeräumt wird, dürfte eine solche Ergänzung des § 105 HWG auch aus der Sicht des Grundsatzes der kommunalen Selbstverwaltung ohne Bedenken sein. Diese Novellierung wäre durch den Abbau unnötiger bürokratischer Hemmnisse sowohl ein Beitrag zur besseren Effektivität der Umweltverwaltung als auch eine bürgerfreundliche Maßnahme.

Aber nicht nur die Verschiedenheit bei der Organisation der Umweltverwaltung – auf der einen Seite die "vollständigen" Umweltämter in Frankfurt und Wiesbaden, auf der anderen Seite das "Umweltamt" eines hessischen Landkreises, das ausschließlich aus der Unteren Naturschutzbehörde besteht – kann ein Hindernis für einen wirksamen Umweltschutz sein, sondern zuerst und vor allem die Gesetzgebung: Sie zeigt die Aufteilung des Umweltrechts in drei verschiedene Ebenen, nämlich Bundesgesetze (Emissionsschutz, zum Teil Wasserrecht), Landesgesetze und kommunale Satzungen. Diese verschiedenen Rechtsvorschriften sind weit davon entfernt, aufeinander abgestimmt zu sein. Während jedoch entsprechende Initiativen im Landes- und Kommunalbereich schon erfreuliche Verbesserungen bewirkt haben, ist dies auf der Ebene des Bundesrechts bisher erfolglos gewesen. Gerade im Bereich der Immissionsschutzgesetzgebung wirkt sich dies für die Tätigkeit der Umweltbehörden ungünstig aus. Es zeigt sich bei der genauen Betrachtung von Einzelfällen immer wieder – und meine Prüfbesuche haben diese Erfahrung bestätigt –, daß nicht der Datenschutz ein Hindernis für erfolgreiche Umweltschutzmaßnahmen ist, sondern die Mängel in der Gesetzgebung, die mit den geschilderten organisatorischen Unvollkommenheiten eng zusammenhängen. Auf lange Sicht wird sich dieses Problem befriedigend nur lösen lassen durch die gemeinsame Erarbeitung eines Umweltgesetzbuches zwischen Bund und Ländern unter Beteiligung der kommunalen Spitzenverbände. Gerade die praktische Erfahrung der Großstädte und Landkreise auf dem Gebiete der Umweltverwaltung sollte bei der Formulierung entsprechender Gesetze Berücksichtigung finden.

Bei meinen Bemühungen, mögliche Probleme zwischen Datenschutz und Umweltschutz zu lösen bzw. gar nicht entstehen zu lassen, habe ich erfreulicherweise vom hessischen Umweltministerium, der Landesanstalt für Umwelt sowie den kommunalen Umweltverwaltungen und den kommunalen Datenschutzbeauftragten tatkräftige Unterstützung erfahren. Ich werde auch, wie bisher, das Ministerium und die übrigen Stellen der Umweltverwaltung gerne weiterhin mit fachlichem Rat aus der Sicht des Datenschutzes unterstützen.

13.2
Umweltinformationsgesetz des Bundes

Am 8. Juli 1994 wurde das "Gesetz zur Umsetzung der Richtlinie 90/313/EWG des Rats vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (BGBl. I 1994 S. 1490) – Umweltinformationsgesetz (UIG) – vom Bundestag erlassen. Es gilt nach § 2 UIG auch für Landes- und Kommunalbehörden in Hessen. Mit seinem § 4 "Anspruch auf Informationen über die Umwelt" wird ein großer Schritt vorwärts getan auf dem Weg der Erweiterung demokratischer Bürgerrechte. Er lautet:

"Jeder hat Anspruch auf freien Zugang zu Informationen über die Umwelt, die bei einer Behörde... vorhanden sind."

Ich hatte bereits mehrfach darauf hingewiesen, daß dieses Recht auf Informationsfreiheit – auch als Akteneinsichtsrecht, freedom of information oder Informationszugangsrecht bezeichnet – eine wichtige Ergänzung des Grundrechts auf informationelle Selbstbestimmung ist und in Hessen – wie bereits in den meisten europäischen Ländern – eingeführt werden sollte (vgl. 14. Tätigkeitsbericht, Ziff. 11; 15. Tätigkeitsbericht, Ziff. 10; 18. Tätigkeitsbericht, Ziff. 3.3; 19. Tätigkeitsbericht, Ziff. 12.2; 20. Tätigkeitsbericht, Ziff. 17.2; 21. Tätigkeitsbericht, Ziff. 18.6 und 22. Tätigkeitsbericht, Ziff. 18.1, 23.1).

Da bisher die Richtlinie des Rates der Europäischen Union vom 7. Juni 1990 unmittelbar galt, bestehen schon eine Reihe praktischer Erfahrungen mit entsprechenden Bürgeranträgen auf Zugang zu Umweltinformationen bei den Umweltbehörden (Umweltbehörde ist in § 3 Abs. 1 UIG definiert als "jede Stelle i. S. d. § 1 Abs. 4 des Verwaltungsverfahrensgesetzes, die Aufgaben des Umweltschutzes wahrzunehmen hat"). Nach den Erkenntnissen aus meinen Prüfbesuchen bei den Umweltämtern (vgl. oben Ziff. 13.1) besteht das hauptsächliche Hindernis bei der Gewährung von Umweltinformationen durch die Behörden an die Bürger nicht etwa in der mangelnden Bereitschaft der betreffenden Mitarbeiter, den Aktenzugang zu gewähren. Diese Behördenangehörigen sind im Gegenteil vielfach hochmotiviert, den Informationsanspruch zu erfüllen, weil sie sich dadurch ein verstärktes Interesse am Umweltschutz und eine Unterstützung ihrer Arbeit versprechen; es ist vielmehr die oft rechtlich schwierige Frage, ob durch die Herausgabe der geforderten Umweltinformation eine Geheimhaltungsvorschrift, vor allem des Datenschutzes oder des Schutzes von Geschäftsgeheimnissen, im Einzelfall verletzt werden könnte, welche die Unsicherheit bei den Behörden verursacht. Der – leider nicht zur Verwirklichung gekommene – Entwurf eines Hessischen Umweltinformationsgesetzes sah aus diesem Grund eine Regelung vor, die den betroffenen Behörden wie auch den Bürgern dabei Hilfestellung gewähren sollte, nämlich die Beratung durch den Hessischen Datenschutzbeauftragten (vgl. 22. Tätigkeitsbericht, Ziff. 18.1).

Glücklicherweise versperrt das Bundesumweltinformationsgesetz eine solche Möglichkeit nicht. Es läßt den Bundesländern genug Spielraum für eine eigene Regelung, denn § 9 Abs. 2 Satz 1 UIG bestimmt:

"Die Länder können für ihren Bereich abweichende Regelungen über die Zuständigkeit treffen."

Das Land Hessen wäre also nicht daran gehindert, neben der generellen Zuständigkeit des betreffenden Ministeriums vorzuschreiben, daß der Hessische Datenschutzbeauftragte – zusätzlich als Beauftragter für Informationsfreiheit – die vom Umweltinformationsgesetz betroffenen Behörden und natürlichen Personen beraten und entsprechende Empfehlungen aussprechen kann. Zweckmäßigerweise würde eine solche Regelung bei der nächsten Novellierung des Hessischen Datenschutzgesetzes getroffen. Für eine Übergangszeit erscheint es jedoch durchaus denkbar, die Regelung durch Kabinettsbeschluß oder Ministererlaß vorläufig einzuführen, da es dabei nur um eine beratende Funktion ohne Exekutivbefugnisse geht.

Eine solche Regelung, wie sie bei den Vorberatungen des Hessischen Entwurfs eines Umweltinformationsgesetzes offenbar allseits akzeptiert war, könnte dazu beitragen, die bei den Umweltbehörden infolge der vielfach zu beobachtenden Unsicherheit bei der Anwendung des Gesetzes entstehende größere Belastung zu verringern. Sie könnte vor allem eine größere Zahl von Verfahren vor den Verwaltungsgerichten verhindern, welche man erwarten müßte, wenn es eine solche Beratung nicht gäbe.

14. Landwirtschaft

14.1
Datenübermittlung aus der Weinbaukartei an eine private Firma im Rahmen einer EG-Prüfung

Ein Mitglied des Hessischen Landtags machte mich während der Sitzung des Unterausschusses Informationsverarbeitung und Datenschutz des Hessischen Landtags im Dezember 1993 darauf aufmerksam, daß offenbar vom Weinbauamt Eltville Daten aus der Weinbaukartei an eine private Firma übermittelt worden seien. Es handelte sich, wie meine Recherchen ergaben, um eine Datenübermittlung im Rahmen der Überprüfung der Weinbaukartei seitens der EG-Kommission. Ich habe mich daraufhin an das Hessische Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz gewandt und darauf aufmerksam gemacht, daß die unterlassene Unterrichtung des Hessischen Datenschutzbeauftragten über das – bereits langfristig geplante – Projekt der EG-Kommission ein Verstoß gegen § 29 Abs. 1 und 3 HDSG darstelle, und gebeten, mich unverzüglich und ausführlich über die Angelegenheit zu unterrichten. Dies geschah in einer Stellungnahme Ende Januar 1994. Daraus ging hervor, daß die Überprüfung der Weinbaukartei seitens der EG-Kommission nach Art. 6 der Verordnung (EWG) Nr. 2392/86 vom 24. Juli 1986 (ABl. der Europäischen Gemeinschaften Nr. L 208/1 vom 31. Juli 1986) grundsätzlich rechtmäßig war. Geprüft werden sollten folgende Angaben in der Weinbaukartei:

- Die Genauigkeit der zugrundegelegten geographischen Referenzen,
- die Koordination zwischen markierten Rebflächen und den Betrieben sowie
- die Präzision und Genauigkeit einiger Daten, die die Produktion bzw. die Betriebe betreffen.

Zu diesem Zweck wurde von der EG-Kommission die Firma EFTAS in Münster beauftragt. Deren Prüfungen wurden in der Gemarkung Mittelheim/Rheingau im Mai und Juni 1993 durchgeführt.

Wenn auch Art. 3 der genannten Verordnung bestimmt: "Die Mitgliedstaaten tragen dafür Sorge, daß ... Maßnahmen zum Datenschutz getroffen werden, vor allem gegen Zugriff und Datenänderung", blieben nach der Auskunft des Ministeriums doch eine Reihe von Datenschutzfragen ungeklärt, insbesondere was die Rechtsstellung und Befugnisse

der Firma EFTAS anbetraf. Ich bat daher den Bundesminister für Ernährung, Landwirtschaft und Forsten um entsprechende Auskunft. Außerdem führte ich einen – unangemeldeten – Prüfbesuch bei der zuständigen Abteilung des (hessischen) Landwirtschaftsministeriums durch.

Aus den – mir bereitwillig überlassenen – Akten über die Weinbaukartei konnte ich mich überzeugen, daß das Landwirtschaftsministerium bei dem EG-Projekt von Anfang an bemüht war, den Datenschutz zu beachten. Die wechselseitige Information zwischen Fachabteilung und behördlichem Datenschutzbeauftragten des Ministeriums einerseits und dem Hessischen Landesamt für Regionalentwicklung und Landwirtschaft in Kassel als Mittelbehörde sowie Weinbauamt mit Weinbauschule in Eltville als untere Verwaltungsbehörde andererseits schien mir allerdings nicht nur etwas schwerfällig, sondern auch unvollkommen zu sein. Insbesondere die Zuziehung des jeweiligen behördlichen Datenschutzbeauftragten durch die Fachabteilung sollte in allen Angelegenheiten, die den Datenschutz berühren können, durch Organisationserlaß klar geregelt werden. Bisher scheint es dem Zufall bzw. dem guten Willen des jeweiligen Abteilungsleiters überlassen zu sein, ob der behördliche Datenschutzbeauftragte in solchen Angelegenheiten informiert wird. Ein – von mir mit Mißtrauen betrachteter – Vermerk auf einem Briefentwurf: "Nicht für den Datenschutzbeauftragten bestimmt" erwies sich allerdings als harmloser Hinweis darauf, daß inzwischen ein überarbeiteter Entwurf vorlag.

Meine Prüfung ergab zwar, daß mit der Firma EFTAS auch bestimmte Datenschutzmaßnahmen vertraglich vereinbart worden waren; offen blieb allerdings, ob die Firma als Auftragnehmer i.S.v. § 4 Abs. 2 HDSG tätig geworden war oder aber als selbständige datenverarbeitende Stelle.

Erst im Juni 1994 teilte mir das Bundeslandwirtschaftsministerium auf meine Anfrage mit, daß die Firma kein "beliehenes" Unternehmen, also keine "öffentliche Stelle" i.S.v. § 16 BDSG (diese Vorschrift entspricht § 16 HDSG) sei. Damit stand fest, daß das Weinbauamt bei der Datenübermittlung an die Firma EFTAS die Voraussetzungen von § 16 Abs. 1, 2 HDSG zu beachten hatte. Das heißt, der Empfänger – die Firma EFTAS – muß ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft machen, und es dürfen keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange der betroffenen Winzer beeinträchtigt werden können. Darüber hinaus darf die Firma die Daten nur zu dem Zweck verwenden, zu dessen Erfüllung sie übermittelt wurden.

Durch einen weiteren Prüfbesuch beim Weinbauamt in Eltville im Juli 1994 konnte ich mich davon überzeugen, daß sowohl bei der Information der betroffenen Winzer als auch bei den Abmachungen mit der Firma EFTAS die Voraussetzungen des § 16 Abs. 1, 2 HDSG eingehalten wurden. Die Firma hatte folgende Erklärung zum Datenschutz abgegeben:

- "Ich bestätige, die personenbezogenen Daten, die mir im Rahmen der im Auftrag der EG zur Überprüfung der Weinbaukartei in Hessen zu erstellenden Verläßlichkeitsstudie bekannt werden, vertraulich zu behandeln und nur zum Zwecke der Erfüllung des EG-Auftrages zu verwenden.
- Ich versichere, personen- bzw. betriebsbezogene Daten nicht weiterzuleiten. Nach Vorlage des Abschlußberichtes an die EG-Kommission werden sämtliche Unterlagen an das Weinbauamt mit Weinbauschule Eltville zurückgegeben."

Der zweite Satz der Erklärung der Firma EFTAS über die Rückgabe sämtlicher Unterlagen an das Weinbauamt Eltville war zum Zeitpunkt meiner Prüfung – also mehr als ein Jahr nach der Tätigkeit der Firma in Mittelheim – immer noch nicht erfüllt. Aus der Sicht des Datenschutzes ist dies zu kritisieren, allerdings ohne daß hier das Weinbauamt oder das Ministerium eine Schuld trifft. Erst auf mehrfache Mahnung der Firma EFTAS hat diese – wie mir das Ministerium im September 1994 mitteilte – dem Weinbauamt Eltville die vollständigen Unterlagen Ende August 1994 übersandt. Die Verzögerung wurde damit begründet, daß es der Firma erst nach der Annahme des Abschlußberichts durch die EG-Kommission gestattet gewesen sei, die Unterlagen zurückzusenden.

Aus meiner Sicht ist diese Praxis unbefriedigend, da sie den Mißbrauch personenbezogener Daten begünstigt. Bei rechtzeitiger Information meiner Dienststelle durch das zuständige Ministerium wäre es möglich gewesen, für die EG-Prüfung eine Lösung zu finden, die auch aus der Sicht des Datenschutzes akzeptabel gewesen wäre.

14.2

Datenübermittlung aus der Weinbaukartei an das Amt für Regionalentwicklung, Landschaftspflege und Landwirtschaft

Das Weinbauamt mit Weinbauschule Eltville richtete an mich die Anfrage, ob die Übermittlung der Adressen von Bewirtschaftern der Flächen bestimmter Flurstücke im Rheingau zum Ankauf von Flächen für Naturschutzzwecke an das Amt für Regionalentwicklung, Landschaftspflege und Landwirtschaft zulässig sei.

Grundsätzlich dürfen personenbezogene Daten nur für den Zweck weiterverarbeitet werden, für den sie erhoben oder gespeichert worden sind (§ 13 Abs. 1 HDSG). Daten aus der Weinbaukartei können also nur ausnahmsweise für einen anderen Zweck – wie Ankauf von Flächen für Naturschutzzwecke – verwandt werden. Dann nämlich, wenn einer der (Ausnahme-)Tatbestände des § 12 Abs. 2 HDSG erfüllt ist.

Dies war der Fall: Das hessische Landwirtschaftsministerium hatte mir bestätigt, daß die Erhebung bei den Betroffenen einen unverhältnismäßigen Aufwand erfordern würde: In den wenigsten Fällen seien die Bewirtschafter von Grundstücken über das Katasteramt oder über Grundbucheintragungen zu ermitteln. § 14 des Flurbereinigungsgesetzes sieht deshalb für die Ermittlung von Beteiligten die öffentliche Bekanntmachung vor, die sehr zeitaufwendig ist. Darüber hinaus bestanden keine Anhaltspunkte dafür, daß schutzwürdige Belange der Betroffenen beeinträchtigt werden können. Daher war eine Übermittlung der – ursprünglich für andere Zwecke gespeicherten – Daten nach

§ 13 Abs. 2 i.V.m. § 12 Abs. 2 Ziff. 5 und § 14 Abs. 1 HDSG zur rechtmäßigen Erfüllung von Aufgaben des Amtes für Regionalentwicklung, Landschaftspflege und Landwirtschaft Limburg zulässig.

14.3
Ernährungssicherstellung und Datenschutz

Im vergangenen Jahr bat mich das Hessische Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz um Stellungnahme zu dem Entwurf einer Ernährungswirtschaftsmeldeverordnung (EWMV-E) des Bundes. Ermächtigungsgrundlagen für eine solche Verordnung finden sich im Ernährungssicherstellungsgesetz in der Fassung der Bekanntmachung vom 27. August 1990 (BGBl. I S. 1802), geändert durch Artikel 43 der Verordnung vom 26. Februar 1993 (BGBl. I S. 278), und dem Ernährungsvorsorgegesetz vom 20. August 1990 (BGBl. I S. 1766), geändert durch Artikel 44 der Verordnung vom 26. Februar 1993 (BGBl. I S. 278).

Während das Ernährungssicherstellungsgesetz die Versorgung der Bevölkerung mit Nahrungsmitteln im Verteidigungsfall gewährleisten soll, gilt das Ernährungsvorsorgegesetz bei Versorgungskrisen in Friedenszeiten, hervorgerufen durch Natur- und Umweltkatastrophen, massive Störungen der Weltmärkte bei landwirtschaftlichen Produkten oder durch Unfälle in großtechnischen oder kerntechnischen Anlagen.

In der Ernährungswirtschaftsmeldeverordnung sind diejenigen Betriebe aufgelistet, die zur Abgabe von Meldungen verpflichtet sind. Dabei handelt es sich um ernährungswirtschaftliche Betriebe, die für die Versorgung der Bevölkerung mit Nahrungsmitteln von besonderer Bedeutung sind. Abgefragt werden – mit einer Reihe von Formularen – u.a. auch die Privatanschriften des Betriebsinhabers bzw. des Leiters der Betriebsstätte. Weder aus den Ermächtigungsgrundlagen noch aus der Ernährungswirtschaftsmeldeverordnung selbst ist jedoch ersichtlich, ob und aus welchem Grund es erforderlich sein soll, die Privatanschriften der genannten Personen zu erheben und zu speichern, zumal in beiden genannten Gesetzen vorgesehen ist, daß die zuständigen Behörden im Krisenfall berechtigt sind, von anderen Behörden (beispielsweise Meldebehörden) eben diese Angaben zu fordern.

Im übrigen habe ich das Ministerium darauf hingewiesen, daß es den Betriebsfragebogen an den in § 12 Abs. 4 HDSG geforderten Angaben mangelt. Diese Vorschrift verlangt, daß der Betroffene, bei dem Daten erhoben werden, in geeigneter Weise über den Zweck der Datenerhebung aufzuklären ist. Werden Daten bei dem Betroffenen aufgrund einer durch Rechtsvorschrift festgelegten Auskunftspflicht erhoben, dann ist er auf die Rechtsgrundlage hinzuweisen. Ich habe daher empfohlen, bei Verwendung der Formulare in Hessen ein Vorblatt beizufügen, das diesen Anforderungen entspricht.

15. Behördliche Datenschutzbeauftragte

Im Februar 1994 hatte ich bei der Hessischen Landesregierung angeregt, die Funktion des behördlichen Datenschutzbeauftragten in den jeweiligen Organisationsplänen der Ministerien und nachgeordneten Behörden zu kennzeichnen und mir mitzuteilen. Dadurch sollten künftig Verzögerungen in der Wahrnehmung meiner Kontrollaufgaben vermieden werden, wie sie in der Vergangenheit öfter entstanden waren, weil der behördliche Datenschutzbeauftragte mir nicht bekannt bzw. seine Stelle zeitweise nicht besetzt war.

Meine Anregung hatte ein erfreuliches Echo und wurde von der Hessischen Staatskanzlei und dem Hessischen Innenministerium unterstützt. Da die Übersendung der Organisationspläne z.T. praktische Probleme verursachte, erklärte ich mich gegenüber dem – federführenden – Innenministerium einverstanden mit einer einfachen Mitteilung durch die jeweilige Behörde.

Trotzdem mußte ich zum Jahresende feststellen, daß meine Information leider sehr lückenhaft geblieben ist. Nur von der Staatskanzlei und vier weiteren Ministerien, nämlich dem Ministerium des Innern, dem Ministerium für Frauen, Arbeit und Sozialordnung, dem Ministerium für Umwelt, Energie und Bundesangelegenheiten und dem Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz, sind mir bisher deren behördliche Datenschutzbeauftragte mitgeteilt worden. Mehrere Ministerien haben lediglich ihre nachgeordneten Behörden zu einer solchen Mitteilung veranlaßt: Dies betrifft z.B. Bibliotheken, Gerichte, Ämter für Arbeitsschutz und Sicherheitstechnik, Hochschulen, Museen, Landesämter, Forschungseinrichtungen. Von zwei Ressorts habe ich überhaupt nichts gehört.

Da künftig der Zusammenarbeit des Hessischen Datenschutzbeauftragten mit den behördlichen Datenschutzbeauftragten nach meiner Einschätzung eine wesentlich höhere Bedeutung zukommen wird, möchte ich meine Anregung wiederholen, mir die behördlichen Datenschutzbeauftragten namentlich mitzuteilen und mich über die jeweiligen Änderungen auf dem laufenden zu halten.

16. Ausländerrecht

16.1
Einbürgerung von Ausländern

In den vergangenen Monaten habe ich mich bei der Stadt Wiesbaden und dem Regierungspräsidium in Darmstadt über das Einbürgerungsverfahren informiert und eine Reihe von Einbürgerungsakten eingesehen.

16.1.1
Zum Ablauf des Verfahrens

Die Einbürgerung von Ausländern bzw. deutschen Volkszugehörigen erfolgt nach unterschiedlichen Rechtsvorschriften. Vorgesehen ist sie u.a. im Ausländergesetz (§§ 85, 86), im Reichs- und Staatsangehörigkeitsgesetz (§§ 8, 9, 13) und im Gesetz zur Regelung von Fragen der Staatsangehörigkeit (§ 9). Hinzu kommen eine Fülle von Richtlinien, Verwaltungsvorschriften und Erlassen auf Bundes- und Landesebene, welche die Gesetze ausfüllen oder konkretisieren. Zurecht haben meine Gesprächspartner in den Behörden auf die Rechtszersplitterung und die Notwendigkeit eines einheitlichen Einbürgerungsrechts hingewiesen. Stellt sich die Lage für den Rechtsanwender mitunter schon schwierig dar, so gilt dies um so mehr für den Bürger, der sich in der Flut der teilweise immer wieder geänderten Vorschriften schwer zurechtfinden dürfte.

Der Antrag auf Einbürgerung wird bei der unteren Verwaltungsbehörde gestellt, während die Entscheidungen von den Regierungspräsidien – in einigen Fällen mit Zustimmung des hessischen Innenministeriums – getroffen werden. Beide Behörden – untere Verwaltungsbehörde und Regierungspräsidium – holen im Laufe des Verfahrens eine Menge von Informationen über den Einbürgerungsbewerber ein. Teilweise werden die Auskünfte vom Einbürgerungsbewerber selbst verlangt, teilweise werden Auskunftsverlangen an verschiedene Behörden gerichtet.

Je nach den unterschiedlich verorteten Einbürgerungsverfahren kommen beispielsweise in Betracht

- Stellungnahme der Ausländerbehörde
- Stellungnahme des Landeskriminalamts über anhängige Ermittlungsverfahren oder sonstige strafrechtliche Erkenntnisse
- Bestätigung der Meldebehörde
- Stellungnahme des Sozialamts über den Bezug von Sozialhilfe
- Stellungnahme des Arbeitsamts, ob die Arbeitslosigkeit selbst zu vertreten ist
- Stellungnahme des Amtsgerichts über einen Eintrag ins Schuldnerverzeichnis
- Stellungnahme des Finanzamts
- Auskunft aus dem Bundeszentralregister
- Anfrage beim Hessischen Landesamt für Verfassungsschutz, wenn Hinweise auf eine politisch-extremistische Betätigung des Einbürgerungsbewerbers vorliegen.

Diese Informationen, einschließlich der beim Bewerber selbst erhobenen, werden in der Akte beim Regierungspräsidium gesammelt und bewertet – ein interessantes Tätigkeitsfeld für den Datenschützer.

16.1.2
Mängel des Verfahrens

Nach meinen Stichproben ist es um den Datenschutz im Einbürgerungsverfahren – jedenfalls im Zuständigkeitsbereich des Regierungspräsidiums Darmstadt und der Stadt Wiesbaden – nicht allzu schlecht bestellt. Ein streng formalisiertes Verfahren trägt dazu bei, daß in der Praxis nur die Auskünfte eingeholt werden, die in den einschlägigen Vorschriften für den jeweiligen Fall vorgesehen sind. Die von einigen Bürgern geäußerte Vermutung, daß – entgegen anderslautenden rechtlichen Bestimmungen – eine Regelanfrage oder gehäufte Anfragen an das Landesamt für Verfassungsschutz gerichtet werden, kann ich nicht bestätigen. In keiner der von mir eingesehenen Akten konnte ich einen derartigen Hinweis erkennen.

Folgende Mängel habe ich festgestellt:

- Die beim Einbürgerungsbewerber einzuholende Einwilligung in die Datenübermittlung verschiedener Behörden an die Einbürgerungsbehörde entspricht nicht datenschutzrechtlichen Anforderungen. In einer "Erklärung zum Einbürgerungsantrag" wird eine pauschale Einwilligung in die Auskunftserteilung aller am Einbürgerungsverfahren beteiligten Stellen verlangt. Das bedeutet, daß sich der Betroffene damit einverstanden erklären soll, daß Datenübermittlungen praktisch "auf Vorrat" stattfinden dürfen, die in seinem konkreten Einbürgerungsverfahren möglicherweise gar nicht erforderlich sind. Eine wirksame Einwilligungserklärung setzt hingegen voraus, daß für den Betroffenen klar feststeht, bei welchen öffentlichen Stellen welche Arten von Daten über ihn eingeholt werden. Der Betroffene ist weiterhin unter Darlegung der Rechtsfolgen darauf hinzuweisen, daß er die Einwilligung verweigern kann. Ich habe das Regierungspräsidium Darmstadt aufgefordert, das entsprechende Formular in der dargestellten Weise abzuändern. Das hessische Innenministerium habe ich gebeten, eine Präzisierung der einschlägigen Erlaßvorschrift vorzunehmen.

- Die Einbürgerung von jugendlichen Ausländern, die im Bundesgebiet aufgewachsen sind, knüpft das Gesetz an einen sechsjährigen Schulbesuch (§ 85 Nr. 2 AuslG). Ich habe festgestellt, daß sich zum Nachweis des Schulbesuchs in vielen Fällen die Ablichtungen der Schulzeugnisse in den Akten befinden. Da Kriterien wie der Erfolg des Schulbesuchs nach den Rechtsvorschriften keine Rolle spielen, ist die Vorlage von Zeugnissen nicht erforderlich; ausreichend ist die Vorlage der Bescheinigung der Schule über die Tatsache des Schulbesuchs.

- Bei bestimmten Einbürgerungsverfahren nach dem Reichs- und Staatsangehörigkeitsgesetz wird eine Auskunft darüber verlangt, ob der Einbürgerungsbewerber in das Schuldnerverzeichnis beim Amtsgericht eingetragen ist. Dies gilt aber nur dann, wenn für die Einbürgerungsbehörde bereits Anhaltspunkte vorliegen, daß der Betroffene seinen finanziellen Verpflichtungen nicht nachkommt. In einigen der von mir eingesehenen Akten wurden Auskünfte aus dem Schuldnerverzeichnis eingeholt, ohne daß Anhaltspunkte für finanzielle Schwierigkeiten ersichtlich waren.

– Soweit das Sozialamt im Einbürgerungsverfahren gefragt wird, ob der Einbürgerungsbewerber Sozialhilfe bezieht, soll sich das Amt auch dazu äußern, ob der Sozialhilfebezug "selbst zu vertreten ist". Hier hatte ich Anlaß klarzustellen, daß das Sozialamt nur verpflichtet ist, die bereits bekannten Informationen mitzuteilen, aber keinesfalls die Anfrage zum Anlaß nehmen darf, selbst Ermittlungen über die Gründe des Sozialhilfebezugs anzustellen.

Gravierende Mängel mußte ich in dem für Einbürgerungen zuständigen Dezernat des Regierungspräsidiums Darmstadt bei den technischen und organisatorischen Maßnahmen zur Datensicherung feststellen. Die Diensträume waren beispielsweise für jedermann zugänglich, und die Aufbewahrung der Akten entsprach nicht datenschutzrechtlichen Anforderungen. Ich werde mich in nächster Zeit mit diesen Problemen beim Regierungspräsidium beschäftigen.

16.2
Ausländerzentralregistergesetz

Am 1. Oktober 1994 ist das Gesetz über das Ausländerzentralregister (AZRG; BGBl. I S. 2265) in Kraft getreten. Zu den nicht verabschiedeten Vorläufern des Gesetzes habe ich mich bereits in meinem 15. Tätigkeitsbericht (Ziff. 7) und im 20. Tätigkeitsbericht (Ziff. 5.3) geäußert. Die Konzeption dieser Vorläufer wurde im wesentlichen beibehalten, wenn auch viele Regelungen geändert wurden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu dem Entwurf des nunmehr vorliegenden Gesetzes einen Beschluß gefaßt (Ziff. 31.4), dessen Forderungen der Gesetzgeber jedoch nicht berücksichtigt hat.

16.2.1
Das Ausländerzentralregister beim Bundesverwaltungsamt

Worum es geht, ist nicht neu: Seit mehr als 40 Jahren existiert das Ausländerzentralregister beim Bundesverwaltungsamt in Köln. Von der anfangs betriebenen Karteikartensammlung entwickelte es sich mit Hilfe der elektronischen Datenverarbeitung zu einer umfassenden Informationssammlung über Ausländer, die den verschiedensten Benutzern offen steht. Derzeit enthält das Register Daten zu mehr als acht Millionen Ausländern. Mit dem stetigen Ausbau des Registers wurden Fakten geschaffen, die der Gesetzgeber nicht verändert hat. Das Ausländerzentralregistergesetz stellt deshalb vor allem eine gesetzliche Absicherung der bestehenden Praxis dar, teilweise werden aber auch neue Kommunikationswege eröffnet.

16.2.2
Aufgaben und Inhalt des Registers

Wichtigste Aufgabe des Registers ist es, die Arbeit der Ausländer- und Asylbehörden zu unterstützen. Zu diesem Zweck enthält das Register Informationen nicht nur über Ausländer, die sich in der Bundesrepublik Deutschland aufhalten, sondern unabhängig vom Wohnsitz auch über solche, die irgendeinen Kontakt zu deutschen Behörden haben bzw. hatten, sei es, daß ihr Aufenthalt abgelehnt wurde, eine Ausweisung oder Abschiebung erfolgte oder Einreisebedenken bestehen.

Der zulässige Umfang der Informationen wird im einzelnen festgelegt: aktenführende Ausländerbehörde, Personalien, rechtliche Stellung, Angaben zum Aufenthalts- und zum Asylrecht, zu Einreisebedenken, der Untersagung der politischen Betätigung etc. (§ 3 AZRG). Wie bereits in den Vorentwürfen vorgesehen, wird bei bestimmten ausländerrechtlichen Maßnahmen nicht nur der Hinweis auf die Entscheidung gespeichert, sondern auch der Begründungstext an die Registerbehörde übersandt (§ 6 Abs. 5 AZRG). Die ersuchende Behörde erlangt dann die gewünschten Informationen direkt von der Registerbehörde, ohne daß sie die entsprechende Akte bei einer anderen Stelle anfordern muß. Die Gefahren eines derartigen Verfahrens für den Datenschutz liegen auf der Hand: Die Informationen werden nicht mehr im Kontext des Aktenvorgangs beurteilt, und im Einzelfall können verkürzte aus dem Zusammenhang gerissene Daten für Entscheidungen herangezogen werden.

Das Register soll darüber hinaus ganz anderen Zwecken dienen, nämlich für die Aufgaben der Sicherheitsbehörden bereitstehen. Es geht nicht nur darum, daß die Polizeibehörden des Bundes und der Länder, die Staatsanwaltschaften, Gerichte sowie die Nachrichtendienste Zugriff auf die in erster Linie ausländerrechtliche Fragen betreffenden Informationen erhalten und diese dann für ihre Zwecke nützen können. Die Sicherheitsbehörden können vielmehr – und dies geht über die bisherige Praxis hinaus – bestimmte ihnen vorliegende Erkenntnisse über Ausländer direkt in das Register eingeben. Gespeichert werden beispielsweise die INPOL-Fahndungsmeldungen des Bundeskriminalamts, soweit es um Ausschreibungen zur Festnahme oder Aufenthaltsermittlung geht (§ 2 Abs. 2 Nr. 6 AZRG). Gleiches gilt für Informationen über Ausländer, bei denen "tatsächliche Anhaltspunkte für den Verdacht bestehen", daß sie bestimmte Straftaten planen, begehen oder begangen haben (§ 2 Abs. 2 Nr. 7 AZRG). Diese Informationen dienen nicht mehr einem Informationsbedarf zur Erfüllung ausländerrechtlicher Aufgaben, sondern der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden eigentlich aber eigene Informationssysteme zur Verfügung wie beispielsweise INPOL beim Bundeskriminalamt, die Polizeisysteme der Länder oder das nachrichtendienstliche Informationssystem (NADIS) des Verfassungsschutzes. Die Integration der Informationen der Sicherheitsbehörden in das Ausländerzentralregister führt zu einer aus datenschutzrechtlicher Sicht problematischen Verknüpfung von zu unterschiedlichen Zwecken gesammelten Daten. Für den einzelnen Betroffenen bedeutet dies, daß die Informationen über ihn aus ganz unterschiedlichen Lebensbereichen zusammengeführt werden und damit die Gefahr der Erstellung von Persönlichkeitsprofilen besteht.

16.2.3
Kommunikation mit dem Register

Der Kreis der öffentlichen und privaten Stellen, die Daten an das Register liefern und aus dem Register empfangen, ist sehr weit gehalten.

Auf Ersuchen wird an alle öffentlichen Stellen ein begrenzter Datensatz übermittelt (§ 14 AZRG). Ein umfangreicherer, je nach Behörde im Umfang differenzierter, Datensatz steht zur Übermittlung bereit u.a. für Ausländer- und Asylbehörden, öffentliche Stellen, die grenzpolizeiliche Aufgaben erfüllen, Polizeibehörden des Bundes und der Länder, Staatsanwaltschaften, das Zollkriminalinstitut, die Bundesanstalt für Arbeit, die Verfassungsschutzbehörden, den Militärischen Abschirmdienst und den Bundesnachrichtendienst. Allen genannten öffentlichen Stellen ist der Abruf im automatisierten Verfahren gestattet (§ 22 AZRG).

Der Online-Abruf wird zwar von einem besonderen Zulassungsverfahren abhängig gemacht, in dem eine "Vielzahl von Übermittlungsersuchen" oder eine "besondere Eilbedürftigkeit" darzulegen sind. Diese Voraussetzungen bauen aber keine wirksame Hürde auf, zumal die automatisierte Eingabe voraussetzungslos gestattet wird und dann die technische Infrastruktur für den Online-Abruf schon bereit steht. Der direkte Zugriff im Online-Verfahren ist unter Gesichtspunkten der Verwaltungseffizienz sicher von Vorteil, birgt aber datenschutzrechtliche Gefahren. De facto arbeitet die zugreifende Behörde mit dem fremden Datenbestand, als ob es sich um eigene Daten handelt. Eine präventiv wirkende Kontrolle der Rechtmäßigkeit des Abrufs ist nicht möglich. Besonders problematisch ist der Direktzugriff der drei Nachrichtendienste auf einen – wenn auch reduzierten – Datensatz (§ 22 Abs. 1 Nr. 8 AZRG). In allen bereichsspezifischen Gesetzen ist für die Nachrichtendienste der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen.

Eine Datenübermittlung auf konventionellem Weg sieht das Gesetz auch an Behörden anderer Staaten und an zwischenstaatliche Stellen vor (§ 26 AZRG). Voraussetzung für die Weitergabe ist u.a. die Einwilligung des Betroffenen; allerdings sind zahlreiche Ausnahmen vorgesehen. An sonstige nichtöffentliche Stellen kommt eine Übermittlung für bestimmte im Gesetz genannte Zwecke in Betracht, beispielsweise bei Vorlage eines Vollstreckungstitels (§ 27 AZRG).

Vorgesehen sind nicht nur Auskünfte zu einer bestimmten einzelnen Person, sondern auch zu einer Mehrzahl von Personen, die durch gemeinsame Merkmale als Gruppe gekennzeichnet sind (Gruppenauskunft, § 12 AZRG). Als gemeinsames Merkmal kann jedes im Register zu einer Person zu speichernde Datum herangezogen werden (also beispielsweise Alter, Staatsangehörigkeit, Vorliegen von Einreisebedenken, Verdacht der Begehung bestimmter Straftaten etc.). Datenschutzrechtlich bedenklich ist die Gruppenauskunft zu Zwecken der Gefahrenabwehr und der Strafverfolgung sowie zur Aufklärung bestimmter Vorgänge im Ausland, die für die Bundesrepublik von sicherheitspolitischer Bedeutung sind. Die Gruppenauskunft wird damit zu einer Art Rasterfahndung speziell für Ausländer.

Jede öffentliche Stelle kann zur Feststellung des Aufenthalts eines Ausländers einen Suchvermerk in das Register einstellen (§ 5 AZRG). Sobald der Registerbehörde von anderer Stelle eine Mitteilung oder Anfrage zu der gesuchten Person zugeht, ist sie imstande, an die ersuchende Stelle entsprechende Informationen weiterzugeben.

Damit enthält das Ausländerzentralregister die Funktion einer Fahndungsdatei. Die Nachrichtendienste können nicht nur zum Zweck der Aufenthaltsermittlung, sondern auch "zur Feststellung anderer Sachverhalte" einen Suchvermerk einstellen. Eine Konkretisierung dieser Sachverhalte erfolgt nicht, so daß davon auszugehen ist, daß die Nachrichtendienste zu allen im Zusammenhang mit ihren Aufgaben stehenden Fragestellungen Suchvermerke übermitteln können.

16.2.4
Rechte des Betroffenen

Verbesserungen aus datenschutzrechtlicher Sicht gibt es gegenüber den Vorläufern des Gesetzes im Hinblick auf die Rechte der betroffenen Ausländer. Vorgesehen sind jetzt ein Auskunftsrecht gegenüber der Registerbehörde (§ 34 AZRG), die Pflicht zur Aufnahme von Übermittlungssperren (§ 14 AZRG), zur Berichtigung (§ 35 AZRG), Löschung (§ 36 AZRG) und Sperrung (§ 37 AZRG).

16.3
Aufenthaltsgestattung mit Polizeivermerk

Ein Asylbewerber aus Liberia wurde von einem Arbeitgeber auf einen Eintrag in seiner Aufenthaltsgestattung hingewiesen. Die Bedeutung des Eintrags war dem Ausländer bis dahin nicht bekannt. Der Eintrag lautete: "Nach Schwarzfahrt festgenommen und ausländerrechtlich überprüft"; es folgten Datum, Namenszeichen, die Abkürzung einer Polizeidienstbezeichnung und ein Stempelabdruck einer Polizeistation. Ein anderer Polizeibeamter hatte – ebenfalls mit Namenskürzel und Dienstbezeichnung – hinzugefügt: "Verdacht des Ladendiebstahls".

Über eine Anwältin wandte sich der Ausländer an mich. Er sah sich durch den Eintrag in seine Aufenthaltspapiere diskriminiert. Da der Vermerk offensichtlich unzulässig war – eine Rechtsvorschrift, die solche Einträge zuläßt, ist nicht vorhanden –, wandte ich mich telefonisch an die zuständige Polizeidienststelle. Der Leiter der Schutzpolizei der zuständigen Polizeidirektion konnte kaum glauben, daß "seine" Polizeibeamten solche Eintragungen vornehmen. Nachdem ich ihm aber eine Kopie des Passes zufaxte, reagierte er prompt. Die Bediensteten, welche die Vermerke angebracht hatten, hätten einen Erlaß des Hessischen Ministeriums des Innern vom 5. Juli 1986 falsch verstanden.

Nach diesem Erlaß kann in Pässe oder Paßersatzpapiere nicht EG-angehöriger Ausländer ein Stempelabdruck angebracht werden, aus dem hervorgeht, daß eine polizeiliche Kontrolle stattgefunden hat. Voraussetzung dafür ist, daß aus dem Paß- oder Paßersatzpapier kein Einreisedatum hervorgeht und der begründete – aber zu ausländerrechtlichen Maßnahmen nicht ausreichende – Verdacht besteht, daß der ausländische Staatsangehörige sich bereits länger als drei Monate – also unerlaubt – im Bundesgebiet aufhält. Diese Einträge dienen der Bekämpfung der illegalen Einreise in die Bundesrepublik und sollen dem unerlaubten Aufenthalt von Ausländern begegnen. Diese Voraussetzungen lagen im konkreten Fall nicht vor.

Die Polizeidienststelle bestätigte, daß der Eintrag widerrechtlich erfolgt war, entschuldigte sich bei dem Asylbewerber und veranlaßte bei der Ausländerbehörde die Ausstellung eines neuen Paßersatzpapiers. In einer Dienstbesprechung der Polizeidirektion wurden alle Mitarbeiter über den Sachverhalt und die Unzulässigkeit derartiger Eintragungen informiert. Eine Beschwerde, mit der sich die Anwältin direkt an die Polizei wandte, wurde als Dienstaufsichtsbeschwerde bearbeitet.

Kurz vor Redaktionsschluß dieses Berichts erhielt ich Kenntnis von einer in Darmtadt geübten Praxis: Auch dort notieren Polizeibeamte bestimmte Vermerke in Ausweisdokumente von Asylbewerbern. Die Vermerke in den mir vorgelegten Kopien von Aufenthaltsgestattungen lauten z.B. "angetroffen, Herrengarten am 3. August 1994 ... (Unterschrift), AG LUI, Platzverweis!" oder "angetroffen in Darmstadt, Holzstraße 20, 20. Oktober 1994, 23.00 Uhr, AG lui, ... (Namenskürzel)". Eine der Kopien enthielt gleich fünf solcher Einträge. Aus einem der Dokumente ging durch einen Eintrag der Ausstellungsbehörde ausdrücklich hervor, daß sich der Asylbewerber in Darmstadt aufhalten durfte. Das Polizeipräsidium Darmstadt habe ich um Stellungnahme gebeten. In meinen nächsten Tätigkeitsbericht werde ich über den Fortgang der Angelegenheit berichten.

17. Verfassungsschutz

17.1
Verbrechensbekämpfungsgesetz

Am 1. Dezember 1994 ist das Verbrechensbekämpfungsgesetz (BGBl. I S. 386) in Kraft getreten. Das Artikelgesetz sieht Änderungen für eine Reihe von Gesetzen vor, u.a. das Strafgesetzbuch, die Strafprozeßordnung, das Ausländergesetz, das Asylverfahrensgesetz.

Aus datenschutzrechtlicher Sicht wichtig sind die Änderungen von Vorschriften im Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (BGBl. I 1968 S. 949 mit zahlreichen Änderungen). Diese sehen eine Erweiterung der Befugnisse des Bundesnachrichtendienstes bei der Fernmeldeaufklärung vor.

Die Datenschutzbeauftragten haben in einem Beschluß vom 26./27. September 1994 (hier unter Ziff. 31.9) eine Reihe von Vorgaben für die Befugniserweiterung aufgestellt, die der Gesetzgeber aber nicht berücksichtigt hat.

Für die schon bisher praktizierte Überwachung des Fernmeldeverkehrs durch den Bundesnachrichtendienst ist es unter datenschutzrechtlichen Gesichtspunkten wichtig, daß – anders als bei zielgerichteten Maßnahmen der technischen Überwachung zur Strafverfolgung – keine Begrenzung auf bestimmte Personengruppen erfolgt. Vielmehr werden in der Art einer Rasterfahndung ohne Vorliegen eines Anfangsverdachts in großer Zahl Unbeteiligte in Abhörmaßnahmen mit einbezogen.

Die im Verbrechensbekämpfungsgesetz vorgesehene Erweiterung betrifft zum einen die Sachverhalte, bei denen Abhörmaßnahmen vorgenommen werden dürfen. Nach dem Gesetz über den Bundesnachrichtendienst (BGBl. I 1990 S. 2979) hat der BND die Aufgabe, Erkenntnisse über das Ausland zu sammeln, die von "außen- oder sicherheitspolitischer Bedeutung" für die Bundesrepublik Deutschland sind. Von "sicherheitspolitischer Bedeutung" sollen nun nicht nur die in § 3 G 10 Gesetz bislang ausdrücklich erwähnte militärische Bedrohung, sondern auch andere Aktivitäten sein, wenn sie für die Sicherheit und den Bestand der Bundesrepublik Deutschland als Ganzes eine ernste Gefahr darstellen können. So darf der Bundesnachrichtendienst nach dem Verbrechensbekämpfungsgesetz Telefongespräche auch dann abhören, wenn es um die internationale Verbreitung von Kriegswaffen, die unbefugte Verbringung von Betäubungsmitteln, internationale Geldfälschung und die damit zusammenhängende Geldwäsche geht (Art. 13 § 3).

Eine wesentliche Änderung besteht auch darin, daß der Bundesnachrichtendienst – nunmehr gesetzlich abgesichert – die aus der Fülle der Telefongespräche mittels Suchbegriffen gewonnenen Erkenntnisse unter bestimmten Voraussetzungen an andere Behörden, insbesondere an die Polizei und die Strafverfolgungsorgane, weitergeben darf. Damit wirkt der Bundesnachrichtendienst – ohne ausdrückliche Änderung seiner Aufgaben – an der Verbrechensbekämpfung mit. Zwar muß man abwarten, wie sich einzelne der vorgesehenen Regelungen in der Praxis bewähren; insbesondere wird sich zeigen, ob und wie die Informationserhebung durch den Bundesnachrichtendienst von polizeilichen Interessen gesteuert wird, ob der Bundesnachrichtendienst also gezielt im Rahmen der Fernmeldeaufklärung Informationen für polizeiliche und für Zwecke der Strafverfolgung erhebt.

Alles deutet jedoch darauf hin, daß hier ein wesentlicher Schritt hin zu einer Aufweichung des sogenannten Trennungsgebots zwischen Geheimdiensten und Polizei erfolgt.

Über Reichweite und Verfassungsrang des Trennungsgebots ist viel geschrieben und diskutiert worden. Reduziert auf das Wesentliche besagt es, daß es eine im Einzelfall unkontrollierte Polizei nach den Erfahrungen mit der Geheimen Staatspolizei und mit der Staatssicherheit nicht mehr geben darf. Es macht Sinn, Geheimdienste außerhalb allgemeiner Kontrolle zu stellen, weil sie sonst ihre Arbeit nicht tun könnten. Die zwingende Konsequenz dieser

Option ist dann aber die strikte Aufgabenbeschränkung der Dienste und ihre exekutive Abstinenz. Staatliche Intervention in Freiheitsräume von Menschen ohne Möglichkeit der Betroffenen, diese Intervention zu bemerken, zu durchschauen, zu kritisieren und zu kontrollieren, war bei uns bislang ein totalitäres Schreckgespenst.

17.2
Einbeziehung des Ehegatten in die Sicherheitsüberprüfung

Die Ehefrau eines Mitarbeiters des Landesamts für Verfassungsschutz hatte sich an mich gewandt, weil sie mit der Einbeziehung in die Sicherheitsüberprüfung ihres Mannes nicht einverstanden war. Da sie nie in polizeilicher oder extrem politischer Hinsicht auffällig geworden war, sah sie nicht ein, daß sie vom Landesamt für Verfassungsschutz überprüft werden und ihre Daten im Nachrichtendienstlichen Informationssystem der Verfassungsschutzbehörden (NADIS) gespeichert werden sollten. Sie hatte deshalb die in § 3 Abs. 3 VerfSchutzG vorgesehene Zustimmung verweigert.

Die Dienststellenleitung der Beschäftigungsbehörde des Ehemannes bestand jedoch auf der Einbeziehung der Ehefrau. Die Behörde erinnerte sie mehrfach, führte mit ihr Gespräche und richtete Appelle an sie, ihr Einverständnis zu erteilen. Nachdem alle Bemühungen erfolglos blieben, wurde dem Ehemann die Versetzung zu einer anderen Dienststelle angedroht. Als die Versetzung konkrete Formen annahm, bat mich die Ehefrau um Rat.

Ich nahm Akteneinsicht und führte ein Gespräch mit den zuständigen Mitarbeitern des Landesamts für Verfassungsschutz. Danach konnte ich nachvollziehen, weshalb die Dienststellenleitung auf der Einbeziehung der Ehefrau des Bediensteten in die Sicherheitsüberprüfung beharrte. Als Mitarbeiter des Landesamts für Verfassungsschutz ist der Betroffene ständig mit der Bearbeitung von Angelegenheiten betraut, die einer besonderen Geheimhaltung bedürfen. Die Ermächtigung betraf die höchste Geheimhaltungsstufe – also "streng geheim". Außerdem konnte den Unterlagen der Dienststellenleitung entnommen werden, daß sowohl der Betroffene selbst als auch Angehörige bereits Zielobjekt von Aktivitäten ausländischer Geheimdienste waren. Ich empfahl der Ehefrau, ihre Zustimmung zu erteilen.

Freilich kann in solchen Fällen von einer freien Willensentscheidung, wie es § 3 Abs. 3 VerfSchutzG suggeriert, nicht wirklich gesprochen werden. Denn die einzige Alternative zur Erteilung der Zustimmung war, die Versetzung des Ehemanns zu einer anderen Dienststelle hinzunehmen.

18. Polizei

18.1
Datenerhebung durch den Einsatz von V-Personen, Verdeckten Ermittlern sowie technischer Mittel

In der Vergangenheit habe ich wiederholt über die besonderen Befugnisse der Ermittlungsbehörden, personenbezogene Daten mit verdeckten Mitteln zu erheben, berichtet (19. Tätigkeitsbericht, Ziff. 7.1; 21. Tätigkeitsbericht, Ziff. 5.1; 22. Tätigkeitsbericht, Ziff. 4.2).

Während die einschlägigen Vorschriften des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (§§ 15, 16 HSOG) dann anwendbar sind, wenn eine Straftat noch nicht begangen wurde, sondern ihre bevorstehende Begehung verhindert werden soll oder andere Gefahren abgewehrt werden sollen, setzen die Vorschriften der Strafprozeßordnung (§§ 100c, 110a StPO) voraus, daß eine Straftat bereits begangen wurde.

Die genannten Vorschriften sind seit geraumer Zeit in Kraft, so daß erste Erfahrungen mit ihrer Anwendung vorliegen mußten. Ich habe mir daher beim Hessischen Landeskriminalamt folgende Fallgruppen angesehen:

- Fälle, in denen Verdeckte Ermittler eingesetzt wurden,
- Fälle, in denen mit V-Personen zusammengearbeitet wurde,
- Fälle, in denen das nicht öffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet wurde.

18.1.1
V-Personen und Verdeckte Ermittler

V-Personen sind Personen, welche die Ermittlungsbehörden vertraulich unterstützen, ohne daß sie ihnen angehören und ohne daß Dritten die Zusammenarbeit bekannt ist.

Verdeckte Ermittler sind Polizeivollzugsbeamte, die unter einer Legende, d.h. unter einer veränderten Identität, Kontakt zur kriminellen Szene aufnehmen.

V-Personen und Verdeckte Ermittler können nach den Vorschriften des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung eingesetzt werden, wenn dies zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person erforderlich ist. Zulässig ist ihr Einsatz auch dann, wenn Tatsachen die Annahme rechtfertigen, daß in § 15 Abs. 2 Satz 1 HSOG genannte Straftaten begangen werden sollen und dies zur Verhütung dieser Straftaten erforderlich ist. Ihr Einsatz ist nur zulässig, wenn andere Maßnahmen erheblich weniger Erfolg versprechen würden oder die polizeiliche Aufgabenerfüllung mit Hilfe anderer Maßnahmen wesentlich erschwert wäre. Der Einsatz verdeckter Ermittler bedarf außerdem der richterlichen Anordnung.

Im Ermittlungsverfahren dürfen Verdeckte Ermittler nach § 110a StPO eingesetzt werden, wenn zureichende tatsächliche Anhaltspunkte dafür vorliegen, daß eine Straftat von erheblicher Bedeutung auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung, auf dem Gebiet des Staatsschutzes oder gewerbs- oder gewohnheitsmäßig oder von einem Bandenmitglied oder in anderer Weise organisiert begangen worden ist. Zur Aufklärung von Verbrechen dürfen Verdeckte Ermittler auch eingesetzt werden, soweit aufgrund bestimmter Tatsachen die Gefahr der Wiederholung besteht. Der Einsatz ist nur zulässig, soweit die Aufklärung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Zur Aufklärung von Verbrechen dürfen Verdeckte Ermittler außerdem eingesetzt werden, wenn die besondere Bedeutung der Tat den Einsatz gebietet und andere Maßnahmen aussichtslos wären. Eine Regelung für die Zusammenarbeit der Ermittlungsbehörden mit V-Personen enthält die Strafprozeßordnung nicht.

18.1.2
Technische Mittel

Unter technischen Mitteln sind Mittel für Foto-, Film-, Video- und Tonaufnahmen zu verstehen. Ihren Einsatz läßt das Hessische Gesetz über die öffentliche Sicherheit und Ordnung unter denselben Voraussetzungen zu wie den Einsatz von V-Personen und Verdeckten Ermittlern. Im Ermittlungsverfahren darf nach § 100c StPO das nicht öffentlich gesprochene Wort mit technischen Mitteln abgehört und aufgezeichnet werden, wenn bestimmte Tatsachen den Verdacht begründen, daß jemand eine in § 100a StPO bezeichnete Straftat begangen hat und die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise aussichtslos oder wesentlich erschwert wäre.

18.1.3
Umgang der Ermittlungbehörden mit den neuen Befugnissen

Die Zusammenarbeit zwischen Polizei und Staatsanwaltschaft beim Einsatz von V-Personen und Verdeckten Ermittlern im Rahmen der Strafverfolgung ist in einer gemeinsamen Richtlinie der Justizminister / Senatoren und der Innenminister / Senatoren der Länder dezidiert geregelt. Das Hessische Landeskriminalamt hat darüber hinaus Richtlinien sowohl für den Einsatz von V-Personen und Verdeckten Ermittlern als auch für das Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes im präventiven und repressiven Bereich erlassen.

Die Fälle, in denen die Polizei von ihren besonderen Befugnissen präventiv, also zur Verhütung einer Straftat oder zur Gefahrenabwehr Gebrauch gemacht hatte, waren die Ausnahme; in der Regel wurden sie in laufenden Ermittlungsverfahren eingesetzt. Aber auch in den Ermittlungsverfahren ginge die Initiative für ihren Einsatz grundsätzlich von der Polizei aus, die in einem Vermerk an die Staatsanwaltschaft darlegte, weshalb die bisherigen Ermittlungen nicht zum Erfolg geführt hatten, und daher anregte, einen richterlichen Beschluß für eine Maßnahme nach §§ 100c bzw. 110a StPO zu beantragen. Hier fiel auf, daß die Polizei in ihrem Vermerk an die Staatsanwaltschaft noch um eine ausführliche Begründung der Notwendigkeit der zu beantragenden Maßnahme bemüht war. Die Beschlüsse selbst wurden von den Ermittlungsrichtern formularmäßig gefaßt und enthielten als Begründung oft nicht mehr als eine Wiederholung des Gesetzestextes. Ob dies dem Sinn und Zweck des Richtervorbehalts entspricht, möchte ich hier offen lassen.

In sämtlichen von mir geprüften Fällen lagen die gesetzlichen Voraussetzungen für den Gebrauch der besonderen Befugnisse zur verdeckten Datenerhebung vor. In vielen Fällen wurde von den Ermittlungsbehörden auch der erhoffte Erfolg erreicht.

Dennoch habe ich aufgrund meiner Prüfung erhebliche Zweifel an der Effektivität der neuen Methoden. Die Erwartungshaltung der Öffentlichkeit an eine Polizei, der immer weiterreichende Einsatzinstrumente zur Verfügung gestellt werden, ist zwangsläufig hoch. Die Polizei jedoch ist aufgrund ihrer Ausstattung kaum in der Lage, die ihr gesetzlich eingeräumten Befugnisse und Möglichkeiten in größerem Umfang zu nutzen. Letztlich würde es der Kriminalitätsbekämpfung eher dienen, die Polizei mit den erforderlichen personellen und sachlichen Mitteln zu versehen, statt sie zu Lasten der Grundrechte des einzelnen mit immer weiterreichenden gesetzlichen Eingriffsmitteln auszustatten. (Zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen vgl. auch den Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994, hier Ziff. 31.9.)

18.2
Unterrichtung über polizeiliche Datenspeicherungen

Nachdem mit dem Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 18. Dezember 1989 die polizeiliche Datenverarbeitung erstmals auf eine gesetzliche Grundlage gestellt wurde und mit Wirkung vom 25. März 1994 die Vorschriften über die Datenerhebung durch den Einsatz von V-Personen, Verdeckten Ermittlern und technischen Mitteln neu gefaßt wurden (siehe auch Ziff. 4.1), fand im vergangenen Jahr eine weitere datenschutzrechtliche Bestimmung des neuen hessischen Polizeirechts Anwendung: die Unterrichtung der Betroffenen über die automatisierte polizeiliche Datenverarbeitung.

Nach dieser Bestimmung (§ 20 Abs. 9 HSOG) sind die betroffenen Personen, sobald die Aufgabenerfüllung dadurch nicht mehr gefährdet wird und ihre Anschrift ohne erheblichen Verwaltungsaufwand ermittelt werden kann, darüber zu unterrichten, wenn ihre personenbezogenen Daten länger als drei Jahre in automatisierten Dateien der Polizei

gespeichert werden. Die Vorschrift war bereits Bestandteil des Gesetzes zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung vom 18. Dezember 1989, wurde aber im Zuge einer weiteren Novellierung mit einer dreijährigen Übergangsfrist versehen (§ 111 Abs. 2 HSOG).

Eine Auswertung des Datenbestands des Hessischen Polizeiinformationssystems ergab, daß ca. 119.000 Personen von dieser Regelung betroffen waren. Die Polizei nutzte den ihr zur Verfügung stehenden Übergangszeitraum und nahm umfangreiche Datenbereinigungsarbeiten vor. Sie entwickelte ein Raster mit einer Reihe von Kriterien (z. B. mehrmaliges in Erscheinung treten bei der Polizei, Gewaltanwendung, schwerwiegendes Delikt u. ä.), nach denen ein Verzicht auf sämtliche Informationen die Aufgabenerfüllung gefährden würde. Alle Vorgänge, in denen keines der Kriterien erfüllt war, wurden gelöscht. Auf diese Art und Weise bereinigte die Polizei ihren Datenbestand und reduzierte die Anzahl der Betroffenen um ca. 27.000.

In den verbleibenden 92.000 Fällen fragte die Polizei die Anschrift der Betroffenen bei den Meldebehörden ab. Dies war nach § 14 der Meldedatenübermittlungsverordnung zulässig. Viele waren "nach unbekannt" verzogen, ohne festen Wohnsitz, oder es lag den hessischen Meldebehörden keine aktuelle Anschrift vor. In diesen Fällen unterblieb die Mitteilung. Dies ist mit § 20 Abs. 9 HSOG vereinbar. Denn die Mitteilung soll nur erfolgen, wenn die Anschrift ohne erheblichen Verwaltungsaufwand ermittelt werden kann. Schließlich soll nicht zur Erfüllung einer der Transparenz der Datenverarbeitung dienenden Bestimmung eine zusätzliche Datenerhebung stattfinden.

Die verbleibenden ca. 36.000 Personen, deren Meldeanschriften festgestellt werden konnten, wurden unter Angabe ihrer Personalien darüber informiert, daß ihre personenbezogenen Daten länger als drei Jahre in automatisierten Dateien der Polizei gespeichert sind. Ca. 3.200 Personen wandten sich daraufhin mit Auskunfts- und/oder Löschungsanträgen an das Landeskriminalamt. Ca. 50 Personen baten mich um Prüfung der Rechtmäßigkeit der Datenspeicherung. Die von der Polizei vorgenommene Einzelfallbearbeitung führte zu weiteren ca. 500 Datensatzlöschungen.

Wenn sich der einzelne gegen eine Verarbeitung seiner Daten nicht wehren kann, weil sie aus übergeordneten, dem Allgemeinwohl dienenden Interessen – hier der vorbeugenden Bekämpfung von Straftaten – aufgrund eines Gesetzes auch gegen seinen Willen zulässig ist, so soll er doch Kenntnis von der Verarbeitung seiner Daten erlangen. Er soll nicht nur erfahren können, welche Daten zur Person gespeichert werden, sondern auch die Chance haben, falsche Datenspeicherungen korrigieren zu lassen. Und er soll die Möglichkeit haben, unabhängige Kontrollinstanzen einzuschalten.

Mit dem beschriebenen, mit mir abgestimmten Verfahren wurde dem Gebot der Transparenz der Datenverarbeitung, wie es das Bundesverfassungsgericht in seinem Volkszählungsurteil formuliert hat, Rechnung getragen.

18.3
Verwechslungsfälle

Daß eine Person mit einer anderen verwechselt wird, ist nicht unbedingt ein Problem der automatisierten Datenverarbeitung. Je umfassender jedoch eine Datensammlung ist, desto höher ist die Wahrscheinlichkeit, daß mehrere Personen mit den gleichen Familien- und Vornamen und weiteren Identifizierungsmerkmalen in einer Datei erfaßt sind. Ein nicht weiter dramatischer Sachverhalt. Unangenehm kann die Sache aber werden, wenn gegen die Person, mit der man verwechselt wird, schwere Vorwürfe erhoben werden und man plötzlich nachweisen soll, nicht ein anderer, z. B. ein Mörder oder Zuhälter zu sein.

18.3.1
Der Zuhälter

Eine Person, über die wegen einer leichten Körperverletzung und Nötigung im Straßenverkehr ein Eintrag im Hessischen Polizeiinformationssystem existiert, erhielt davon Kenntnis, daß dort auch noch die Angabe: Spitzname "Jolly" gespeichert war. Da er weder so gerufen wurde noch eine sonstige Erklärung dafür hatte, wandte er sich an mich und bat um Prüfung der Rechtmäßigkeit der polizeilichen Datenspeicherung. An wen ich mich auch wandte, ob an die Beamten des Landeskriminalamtes oder an die des zuständigen Polizeipräsidiums, spontan antworteten mir die Bediensteten nach Nennung von Vor- und Familienname des Betroffenen: "Aah! Sie suchen Jolly?"

Ich sah beim zuständigen Polizeipräsidium die Akten ein. Es gab zu zwei Personen, deren Vor- und Familienname identisch waren, Kriminalakten und Datenspeicherungen im Hessischen Polizeiinformationssystem. Auf den jeder Personalakte vorgehefteten Personalblättern stand in beiden Fällen der Namenszusatz: Spitzname "Jolly". Bei der einen Person handelte es sich um einen stadtbekannten Zuhälter, der fast jedem Kriminalbeamten der Region bekannt ist. Seine Kriminalakte umfaßt zehn Bände. In über hundert Fällen wurde wegen der verschiedensten Delikte gegen ihn ermittelt. Dem Vorgang war zu entnehmen, daß er im Milieu Jolly genannt wurde. Die Akte zu der anderen Person enthielt nur wenige Blatt. Es handelte sich um den Vorgang wegen leichter Körperverletzung und Nötigung im Straßenverkehr. Dem Vorgang konnte nicht entnommen werden, wie der das Personalblatt ausfüllende Beamte dazu kam, den Spitznamen aufzuführen. Es bleibt nur die Vermutung, daß auch er "Jolly" kannte und den Namen der namensgleichen Person mit dem Spitznamen assoziierte. Bei der Erfassung des Falls im Hessischen Polizeiinformationssystem wurde der Spitzname übernommen und stand landesweit allen Polizeidienststellen zum automatisierten Abruf zur Verfügung.

18.3.2
Der Mörder

Eine Person, die unter dem Verdacht steht, eine andere Person getötet zu haben, verwendete verschiedene Alias-Personalien, von denen eine auf eine andere existente Person zutrifft. Diese andere Person wurde des öfteren mit dem Beschuldigten verwechselt. Zuletzt wurde sie bei der Einreise aus dem Ausland bei der Grenzkontrolle im Flughafen Frankfurt am Main vorläufig festgenommen. Erst nach längeren Recherchen klärte sich der Irrtum auf, und die Person kam wieder auf freien Fuß.

18.3.3
Maßnahmen

In dem Datensatz der Person, die mit dem Zuhälter verwechselt wurde, wurde der Spitzname gelöscht. Außerdem wurde ein Vermerk angebracht, der sinngemäß lautete: "nicht identisch mit ... (Jolly)".

Der vermeintliche Mörder wandte sich an die Datenschutzbeauftragte der Flughafen AG. Diese bat mich um Hilfe. Ich schaltete das Hessische Landeskriminalamt ein und bat darum, Maßnahmen zu treffen, die es dem Betroffenen bei künftigen Verwechslungen ermöglichen, möglichst schnell den Irrtum aufzuklären. Da in diesem Falle aber auch Geburtsdatum und Geburtsort mit den von der anderen Person verwendeten Personalien übereinstimmten, mußte die Polizei ganz sicher gehen, daß die Person nicht doch der Gesuchte war. Sie nahm mit seinem Einverständnis seine Fingerabdrücke ab, verglich sie mit denen des Beschuldigten und stellte fest, daß er tatsächlich ein anderer ist. Er erhielt eine Bescheinigung des Polizeipräsidiums, in der ihm bestätigt wurde, daß er nicht mit der im polizeilichen Fahndungssystem unter den gleichen Personalien zur Festnahme ausgeschriebenen Person identisch ist. In den Datensatz des Beschuldigten wurde ein Vermerk angebracht, der sinngemäß lautete "Achtung! Nicht verwechseln mit ... (es folgten die Personalien, die zu dem Beschuldigten als Aliasangaben gespeichert sind). Verwechslungsgefährdete Person weist sich aus mit Reisepaß-Nr. ... ausgestellt am ...".

18.4
Fahndung nach Ausbrechern aus psychiatrischen Krankenhäusern

Hat jemand eine rechtswidrige Tat im Zustand der Schuldunfähigkeit oder der verminderten Schuldfähigkeit begangen, so ordnet das Gericht als Maßregel der Besserung und Sicherung die Unterbringung in einem psychiatrischen Krankenhaus an, wenn die Gesamtwürdigung des Täters und seiner Tat ergibt, daß von ihm infolge seines Zustands erhebliche rechtswidrige Taten zu erwarten sind und er deshalb für die Allgemeinheit gefährlich ist (§ 63 StGB). Die Maßregeln der Besserung und Sicherung vollzieht in Hessen der Landeswohlfahrtsverband, eine Körperschaft des öffentlichen Rechts, in seinen psychiatrischen Krankenhäusern. Als Vollzugsbehörde darf er erkennungsdienstliche Maßnahmen (Abnahme von Finger- und Handflächenabdrücken, Aufnahme von Lichtbildern, Feststellung äußerlicher körperlicher Merkmale, Messungen) am Täter vornehmen, insbesondere bei erhöhter Fluchtgefahr. Die erkennungsdienstlichen Unterlagen werden bei den Personalakten des Täters aufbewahrt, können aber auch zu kriminalpolizeilichen Sammlungen gegeben werden (§ 34 Abs. 1, 2 MaßregelvollzG). Ergreift der Täter die Flucht, kann die Vollzugsbehörde seine Festnahme veranlassen und zu diesem Zweck die erkennungsdienstlichen Unterlagen der Polizei übergeben, falls sie ihr nicht ohnehin schon zur Verfügung stehen (§ 35 MaßregelvollzG).

Im letzten Jahr hatte mich der Landeswohlfahrtsverband nach der Flucht eines Täters, der nicht erkennungsdienstlich behandelt worden war, um Stellungnahme gebeten, welche Daten er zu Fahndungszwecken an die Polizei übermitteln darf. Die Frage war auch, ob die Polizei Informationen über das soziale Umfeld des Täters, z. B. die Anschriften von Angehörigen, erhalten kann. Die gewünschten Informationen waren zwar in den ärztlichen Unterlagen vorhanden, der Landeswohlfahrtsverband hatte jedoch Bedenken, ob ihrer Weitergabe ein Zeugnisverweigerungsrecht des Arztes und die ärztliche Schweigepflicht entgegenstünden.

Die Strafprozeßordnung bestimmt, daß für die Vollstreckung von Maßregeln der Besserung und Sicherung die Vorschriften über die Strafvollstreckung (§§ 449 bis 462 StPO) sinngemäß gelten (§ 463 Abs. 1 StPO). Entsprechend anwendbar ist insbesondere § 457 StPO, der den Haftbefehl und den Steckbrief regelt. Nach § 457 Abs. 1 StPO stehen die der Staatsanwaltschaft im Ermittlungsverfahren eingeräumten Befugnisse nach § 161 StPO auch der Vollstreckungsbehörde zu. Maßnahmen, die die Staatsanwaltschaft im Ermittlungsverfahren zur Ergreifung des Beschuldigten treffen darf, dürfen also auch gegen den Verurteilten im Vollstreckungsverfahren benutzt werden, vor allem gegen einen Verurteilten, der aus dem Strafvollzug bzw. Maßregelvollzug entwichen ist.

Nach dem genannten § 161 StPO kann die Staatsanwaltschaft von allen Stellen, die Aufgaben öffentlicher Verwaltung wahrnehmen, Auskunft verlangen und Ermittlungen jeder Art entweder selbst vornehmen oder durch die Behörden und Beamten des Polizeidienstes vornehmen lassen. Wenn nicht eine ausdrückliche gesetzliche Vorschrift die Auskunftspflicht einschränkt, dürfen die Behörden die Auskunft nicht verweigern. Die Auskunftspflicht kann in Fällen wie dem vorliegenden nach § 53 Abs. 1 StPO eingeschränkt sein. Nach dieser Vorschrift steht Ärzten über das, was ihnen in dieser Eigenschaft anvertraut worden oder bekanntgeworden ist, ein Zeugnisverweigerungsrecht zu. Dementsprechend unterliegen ärztliche Untersuchungsbefunde, auf die sich das Zeugnisverweigerungsrecht erstreckt, nach § 97 StPO einem Beschlagnahmeverbot. Allerdings kann der Arzt auf sein Zeugnisverweigerungsrecht verzichten und auch die einem Beschlagnahmeverbot unterliegenden Sachen freiwillig herausgeben.

Davon war im vorliegenden Fall auszugehen. § 53 StPO enthält jedoch keinen Rechtfertigungsgrund für den Bruch der ärztlichen Schweigepflicht nach § 203 StGB. Danach darf der Arzt ein fremdes Geheimnis, das ihm anvertraut

worden oder sonst bekanntgeworden ist, nicht unbefugt offenbaren. Der Begriff des Geheimnisses ist weit auszulegen; geheim sind Tatsachen, die höchstens einem beschränkten Personenkreis bekannt sind. Danach könnten die Informationen "Anschriften von Angehörigen" und "Beschreibung der Person" unter den Begriff des Geheimnisses fallen. Die Informationen und Kenntnisse zu diesen Fragen dürfen nicht unbefugt an die Polizei weitergegeben werden. Aufgrund einer Rechtsgüterabwägung muß sich also ergeben, daß das Interesse des Betroffenen an der Geheimhaltung der Tatsachen geringer ist als das Interesse der Allgemeinheit an ihrer Offenbarung.

Dies war hier der Fall. Von der Polizei wurden nur die Daten abgefragt, die für ein Ergreifen des entwichenen Täters unerläßlich waren. Das Interesse des Betroffenen an der Geheimhaltung dieser Daten war geringer zu bewerten als das Interesse der Allgemeinheit daran, die Gefahr weiterer erheblicher Straftaten abzuwenden.

18.5
Rahmendienstanweisung zum Datenschutz bei Arbeitsplatzrechnern und anderen IT-Geräten für die Hessische Vollzugspolizei

Im September 1994 wurde die Rahmendienstanweisung, die mir bei Redaktionsschluß zum 22. Tätigkeitsbericht im Entwurf vorgelegen hatte, mit einigen Änderungen in Kraft gesetzt. Die Dienstanweisung legt insbesondere fest,

- was bei der Einrichtung und Änderung von PC-Arbeitsplätzen zu beachten ist,
- welche allgemeinen Datenschutzmaßnahmen gelten und
- welche technischen und organisatorischen Datenschutzmaßnahmen zu treffen sind.

Ein Schwerpunkt der Regelungen liegt bei dem Einsatz privater PC, der sich, wie im 22. Tätigkeitsbericht ausgeführt, als regelungsbedürftig herausgestellt hatte.

Die Rahmendienstanweisung sieht strenge Restriktionen vor, unter denen ein Einsatz privater PC, privater Standard-Software und privat erstellter Anwendungen zu dienstlichen Zwecken erlaubt ist. Auf einige wesentliche Punkte möchte ich hinweisen:

- Der Einsatz bedarf in jedem Fall der vorherigen Genehmigung durch den Dienststellenleiter. Die Genehmigung darf nur erteilt werden, wenn u.a. ein dringendes Bedürfnis zur Automatisierung besteht, das auf absehbare Zeit nicht durch dienstliche Geräte befriedigt werden kann, und keine personenbezogene Daten gespeichert werden; der Einsatz zum Zweck der Textverarbeitung schließt eine Genehmigung nicht aus.
- Es muß grundsätzlich sichergestellt sein, daß die Geräte ständig dienstlich verfügbar sind.
- Programme und Arbeitsergebnisse müssen gegen unbefugte Nutzung geschützt werden.
- Der Einsatz privater PC oder privater Software muß beantragt werden. Dazu ist in der Rahmendienstanweisung detailliert geregelt, welche Angaben zu machen sind. Der Antrag läuft über den behördlichen Datenschutzbeauftragten, der eine Stellungnahme beifügt.
- Die in einer Genehmigung zu regelnden Punkte sind ebenfalls genau aufgeführt. Die Genehmigung ist jederzeit frei widerruflich.
- Die Dienststellen haben eine Kopie jeder Genehmigung (ohne Anlage) dem Hessischen Landeskriminalamt zu übersenden. Von dort werden die Meldungen jeweils zum 1. Juli eines jeden Jahres in listenmäßig aufbereiteter Form dem Hessischen Ministerium des Innern vorgelegt.
- Wenn private PC und Datenträger in den privaten Bereich zurückgeführt werden sollen, muß der Systemverwalter die vorhandenen dienstlichen Daten physisch löschen.
- Dienstlich genutzte private PC und Datenträger unterliegen uneingeschränkt der dienstlichen Kontrolle und der Kontrolle durch den Hessischen Datenschutzbeauftragten.
- Privat beschaffte Standard-Software darf nicht auf dienstlichen PC eingesetzt werden.
- Eine Schulung bzw. Unterweisung für die Bedienung privater PC und privater Standard-Software wird dienstlich nicht angeboten und finanziert.
- Der Umgang mit privaten und dienstlichen Disketten ist geregelt.

Die Übergangsvorschriften sehen u.a. vor, daß Anwendungen auf privaten PC, an denen ein dienstliches Interesse besteht, im Rahmen verfügbarer Haushaltsmittel auf dienstlichen Geräten zu realisieren sind.

Die Verarbeitung personenbezogener Daten ist, mit der Ausnahme einer Textverarbeitung, auf privaten PC nicht zulässig. Bei Schriftstücken wird davon ausgegangen, daß diese nach dem Ausdruck gelöscht werden. Eine Archivierung ist nur in anonymisierter Form gestattet.

Wenn die Vorschriften der Rahmendienstanweisung konsequent umgesetzt sind, ist der Einsatz privater PC und privater Software aus Datenschutzsicht unproblematisch. Ich beabsichtige, die Einhaltung der Regelungen zu prüfen.

19. Ordnungswidrigkeiten

19.1
Lichtbildvergleich in Ordnungswidrigkeitenverfahren

Immer wieder wird mir die Frage gestellt, ob bei Verkehrsordnungswidrigkeiten das in einem Paß- oder Personalausweisregister hinterlegte Lichtbild eines Ausweisinhabers zur Identifizierung eines Verkehrsteilnehmers herangezogen

werden darf. Die den Fragen zugrundeliegenden Sachverhalte sind meist sehr ähnlich: Bei Verkehrskontrollen (Geschwindigkeits- oder Ampelüberwachungsanlagen) werden Bilder von Verkehrsteilnehmern gefertigt, die sich ordnungswidrig verhalten haben.

Da es zur rechtmäßigen Aufgabenerfüllung der Verwaltungsbehörde gehört, Ordnungswidrigkeiten zu verfolgen und zu ahnden, ist die Ordnungswidrigkeitenbehörde auch gehalten, den Sachverhalt aufzuklären. Sie fragt dazu zunächst anhand des auf dem Lichtbild zu erkennenden Kfz.-Kennzeichens bei der Kraftfahrzeugzulassungsstelle die Daten des Kraftfahrzeughalters ab. Die damit verbundene Datenübermittlung ist nach § 35 Abs. 1 StVG zulässig. Nach § 55 OWiG wird der Kraftfahrzeughalter mit dem Tatvorwurf konfrontiert und erhält Gelegenheit, sich zu der Beschuldigung zu äußern. Gibt der Betroffene den Verkehrsverstoß zu und bezahlt er ein ihm angebotenes Verwarnungsgeld, ist der Fall erledigt. Gibt er an, welche andere Person den Verkehrsverstoß beging, wird gegen diese ein Ordnungswidrigkeitenverfahren eingeleitet. Häufig kommt es vor, daß die Kfz.-Halter sich nicht äußern oder nur erklären, das Fahrzeug zur Tatzeit nicht geführt zu haben. Äußert sich der Kfz.-Halter nicht, ist die Beweislage (also z.B. das Radarfoto und die Kfz.-Halterauskunft) aus Sicht der Verwaltungsbehörde zu vage, um nun einen Bußgeldbescheid zu erlassen. Auch wenn der Kfz.-Halter erklärt, das Fahrzeug zur Tatzeit nicht gefahren zu haben, muß die Verwaltungsbehörde annehmen, daß er der falsche Adressat eines Bußgeldbescheides wäre. Da es sich nicht um einen Halt- oder Parkverstoß handelte, kann das Verfahren auch nicht auf dem Wege der Halterhaftung (§ 25a StVG) erledigt werden.

Die Verwaltungsbehörde ist zu diesem Zeitpunkt nicht verpflichtet, das Verfahren einzustellen. Es ist weder ermessensfehlerhaft noch unverhältnismäßig, Ermittlungen dahingehend anzustellen, wer die auf dem Beweisfoto abgebildete Person ist. Nach der Erfahrung der Verwaltungsbehörden kommt es oft vor, daß der Kfz.-Halter am Ende doch für den Verkehrsverstoß verantwortlich war oder (insbesondere dann, wenn er von seinem Aussageverweigerungsrecht Gebrauch machte) ein anderes erwachsenes, zu seinem Haushalt gehörendes Familienmitglied das Fahrzeug führte.

Die Ordnungswidrigkeitenbehörde bittet nun die zuständige örtliche Polizeibehörde um die Feststellung des Fahrers. Die Polizeibehörde lädt den Betroffenen vor oder versucht, ihn zu Hause anzutreffen. Kommt der Betroffene der Vorladung nicht nach – er ist dazu nicht verpflichtet – oder kann er nicht angetroffen werden, kann die mit den Ermittlungen beauftragte Stelle gegenüber der Paß- oder Personalausweisbehörde ein Ersuchen nach § 22 Abs. 2 PaßG oder 2b Abs. 2 PersonalausweisG stellen. Die ersuchende Behörde muß aufgrund von Gesetzen oder Rechtsverordnungen berechtigt sein, solche Daten zu erhalten. Dies ist der Fall: Nach § 53 OWiG gehört es zu den originären Aufgaben der Polizei, Ordnungswidrigkeiten zu erforschen. Außerdem darf die ersuchende Behörde ohne Kenntnis der Daten nicht in der Lage sein, die ihr obliegende Aufgabe zu erfüllen. Auch diese Voraussetzung ist erfüllt. Ohne die Kenntnis, wer das Fahrzeug zur Tatzeit führte, kann das Ordnungswidrigkeitenverfahren nicht fortgeführt werden. Schließlich müssen die Daten bei dem Betroffenen nicht oder nur mit unverhältnismäßig hohem Aufwand erhoben werden können. Da der Betroffene vorgeladen worden war oder versucht wurde, ihn zu Hause anzutreffen, wurde mit verhältnismäßig hohem Aufwand versucht, die Daten beim Betroffenen zu erheben. In diesen Fällen ist also der Vergleich zwischen einem bei einer Radarüberwachung angefertigten und dem bei einer Ausweisbehörde hinterlegten Lichtbild zulässig.

Im Gegensatz zum allgemeinen Datenschutzrecht trägt die Verantwortung für die Zulässigkeit dieser Datenübermittlungen nicht die übermittelnde Stelle, sondern der Datenempfänger. Die Auskunftsersuchen dürfen nur von Bediensteten gestellt werden, die vom Behördenleiter dazu besonders ermächtigt wurden. Außerdem müssen die Ersuchen aktenkundig gemacht werden (§ 2b Abs. 3 PersonalausweisG, § 22 Abs. 3 PaßG).

19.2
Weitere Ermittlungsmaßnahmen in Ordnungswidrigkeitenverfahren

Neben den unter Ziff. 19.1 beschriebenen Maßnahmnen führt die Polizei in Ordnungswidrigkeitenverfahren auch Befragungen von Familienangehörigen, Nachbarn und weiteren Dritten (z.B. Arbeitgebern) unter Vorlage der Beweisfotos durch. Zwar sehe ich die Befragung Dritter als eine zulässige Ermittlungsmaßnahme an, sie darf aber aufgrund ihres verhältnismäßig intensiven Eingriffs in das Recht auf informationelle Selbstbestimmung des Betroffenen (es werden personenbezogene Daten gegenüber Dritten bekannt gegeben) nicht regelmäßig eingesetzt werden. Die Befragung Dritter kann nur im Einzelfall angezeigt sein, wenn weniger einschneidende Maßnahmen erfolglos oder unmöglich sind, bzw. aus besonderen Gründen nicht zur Verfügung stehen. Zunächst ist der Halter des Fahrzeugs zu ermitteln und anzuhören. Verweigert er die Einlassung oder bestreitet er, gefahren zu sein, ist der unter Ziffer 19.1 beschriebene Lichtbildvergleich möglich. Nur für den Fall, daß der Lichtbildvergleich nicht zum Erfolg führt, ist die Befragung Dritter angemessen.

In diesem Zusammenhang entsteht bei der Vorlage des Beweisfotos ein datenschutzrechtliches Problem, wenn auf dem Foto weitere unbeteiligte Personen (Beifahrer) zu erkennen sind.

Die Vorlage des Beweisfotos offenbart dann nicht nur Daten über den Fahrer, sondern gleichzeitig auch über den unbeteiligten Beifahrer. Gegebenenfalls lassen sich auch Erkenntnisse über deren Beziehungen zueinander schließen, die mit dem Ordnungswidrigkeitsverfahren selbstverständlich nichts zu tun haben und für die Durchführung des Verfahrens auch nicht erforderlich sind. Allerdings kann die Vorlage des Fotos Nachteile persönlicher Art für den Betroffenen haben.

Dieser Umstand verführt in der Praxis mitunter dazu, daß im Rahmen der Ermittlungen der Betroffene darauf hingewiesen wird, daß das Beweisfoto mit der abgebildeten Beifahrerin beispielsweise der Ehefrau vorgelegt werden

kann. Befürchtet der Betroffene hierdurch private Nachteile, wird er den Verkehrsverstoß zugeben, um die Einvernahme Dritter zu vermeiden.

Daß dies kein theoretisches Fallbeispiel ist, belegen entsprechende Beschwerden zu diesem Thema.

Ich halte die regelmäßige Verwendung von Beweisfotos, auf denen auch unbeteiligte Personen zu erkennen sind, zu Ermittlungszwecken in Ordnungswidrigkeitsverfahren für nicht erforderlich und unverhältnismäßig. Allerdings akzeptiere ich den Einwand, daß der Beifahrer im Einzelfall als Zeuge in Frage kommen kann und es zum Ermittlungsauftrag der Polizei gehört, diesen Zeugen zu identifizieren. Man muß daher eine praktische Vorgehensweise finden, die den datenschutzrechtlichen Gesichtspunkten Rechnung trägt und gleichzeitig den Ermittlungsauftrag der Polizei nicht behindert.

Eine solche Lösung – mit der alle Beteiligten zufrieden sind – hat Nordrhein-Westfalen gefunden: Dort erfolgt die erste Auswertung eines Beweisfotos mittels einer technischen Maske, die nur den Fahrer auf dem Foto erkennen läßt. Sollte es im Laufe des Verfahrens auf die Identifizierung des Beifahrers ankommen, wird im Einzelfall ein vollständiger Abzug des Fotos gefertigt. Eine entsprechende Lösung strebe ich für Hessen an.

Aber auch jetzt schon sind die Grundsätze der Verhältnismäßigkeit und Erforderlichkeit bei den Ermittlungen zu beachten. Das bedeutet, daß das Beweisfoto, sobald es zur Fahrerermittlung Dritten vorgelegt wird, so behandelt wird (geschwärzt und abgedeckt), daß der Dritte den Beifahrer nicht erkennen kann. Erst, wenn es im Rahmen der Ermittlungen auf die Identifizierung des Beifahrers ankommt, kann das erweiterte Foto vorgelegt werden.

20. Straßenverkehr: Inhalt einer Führerscheinakte für Zwecke der medizinisch-psychologischen Untersuchung

Bei der Neuerteilung einer Fahrerlaubnis nach vorangegangener Entziehung wegen wiederholter verkehrsrechtlicher Verstöße ordnet die Verwaltungsbehörde in der Regel die Beibringung eines Gutachtens einer medizinisch-psychologischen Untersuchungsstelle an (§ 15c Abs. 3 StVZO).

Da eine Untersuchung von Amts wegen oder eine Übermittlung der untersuchungserheblichen Daten von Amts wegen unzulässig wäre, fordert die Verwaltungsbehörde den Betroffenen auf, sein Einverständnis zur Vorlage der Führerscheinakte an den Gutachter zu erteilen und zu erklären, ob das spätere Gutachten direkt an die Verwaltungsbehörde oder an den Betroffenen geschickt werden soll.

In der Praxis wird nach Vorlage der Einverständniserklärung in der Regel die komplette Führerscheinakte an den Gutachter übersandt. In der Akte befinden sich sämtliche Vorgänge und Daten, die über den Betroffenen im Zusammenhang mit dem Straßenverkehr angefallen sind.

Ich halte diese Vorgehensweise für rechtswidrig:

Der Untersuchungsumfang hat sich auf die Fragen zu beschränken, die im einzelnen Fall zur Aufklärung der mitgeteilten Zweifel der Verwaltungsbehörde an der Eignung des Betroffenen beantwortet werden müssen. Entsprechend der verbreiteten Praxis erhält der Gutachter aber auch Unterlagen, die für die Beantwortung der Fragestellung nicht benötigt werden. Hier kommt es also zu einer nicht erforderlichen Datenübermittlung, die nach § 11 HDSG unzulässig ist.

Sie ist auch nicht durch das Einverständnis des Betroffenen gedeckt. Der Betroffene befindet sich bei der Abgabe der Einverständniserklärung in einer Zwangslage, da er eine neue Fahrerlaubnis nur erhält, wenn er ein Eignungsgutachten beibringt, die Gutachterstelle wiederum nur tätig wird, wenn die Akten vorgelegt und die Daten preisgegeben werden.

Die hier im überwiegenden Interesse der Allgemeinheit (Gefährdung durch ungeeignete Kraftfahrer) vorgenommene Einschränkung des Rechts auf informationelle Selbstbestimmung findet dort ihre Grenze, wo Daten preisgegeben werden sollen, die zu dieser Interessenwahrung nicht mehr erforderlich sind.

Der Bundesminister für Verkehr hat in seinen Richtlinien für die Prüfung der körperlichen und geistigen Eignung von Fahrerlaubnisbewerbern und -inhabern (Eignungsrichtlinien) vom 1. Dezember 1982 (VkBl. S. 469) unter Ziff. 5 daher auch festgelegt, daß dem Gutachter nur die Dinge zu übersenden sind, die im Hinblick auf die Fragestellung Aufschluß geben und nicht einem Verwertungsverbot unterliegen.

Ich bin daher der Meinung, daß

- die Verwaltungsbehörde das Einverständnis des Betroffenen nur insoweit einholen darf, als es sich auf die Übersendung der erforderlichen Akten bezieht,
- die Verwaltungsbehörde im Einzelfall die Akte vor Übersendung auf Erforderlichkeit des Inhalts hin zu überprüfen hat; nicht erforderliche Teile sind von der Akte zu trennen; falls dies nicht oder nur mit unverhältnismäßigem Aufwand möglich ist, sind sie als nicht verwertbar zu kennzeichnen,
- der Untersuchungsstelle dieses und ggf. weitere Verwertungsverbote mitzuteilen sind.

21. Sparkassen kopierten rechtswidrig Pässe und Personalausweise ihrer Kunden

Zu etlichen berechtigten Beschwerden hat im Berichtsjahr das Geldwäschegesetz vom 25. Oktober 1993 (BGBl. I S. 1770) geführt. Sparkassenkunden, die ein Konto eröffnen oder Geld überweisen wollten, sahen sich vor die Alternative gestellt, entweder ihren Ausweis kopieren zu lassen oder auf die Kontoeröffnung bzw. die Transaktion zu verzichten. Zur Rechtfertigung ihres Vorgehens beriefen sich die Sparkassen fälschlich auf das Geldwäschegesetz.

Das Gesetz, mit dem das Aufspüren von Gewinnen aus schweren Straftaten ermöglicht werden soll, um zu verhindern, daß illegal erworbene Vermögenswerte in den legalen Finanzkreislauf zurückgeführt ("gewaschen") werden, erlegt den Kreditunternehmen Identifizierungs-, Dokumentations- und Meldepflichten auf. Es verlangt von den Instituten, vor der Annahme von Bargeld, Wertpapieren oder Edelmetallen im Wert von 20.000 DM oder mehr die Identität des Kunden festzustellen und zu dokumentieren. Die Identifizierungspflicht besteht außerdem, wenn mehrere Transaktionen durchgeführt werden, die zusammen einen Betrag von 20.000 DM und mehr ergeben, und tatsächliche Anhaltspunkte dafür bestehen, daß zwischen ihnen eine Verbindung besteht. Gekoppelt damit ist eine Meldepflicht der Banken und Sparkassen: Sie müssen bei Verdacht, daß eine Finanztransaktion der Geldwäsche dient, die Strafverfolgungsbehörden informieren.

Die Identifizierung geschieht durch Feststellung des Namens aufgrund eines Personalausweises oder Reisepasses sowie des Geburtsdatums und der Anschrift, soweit sie darin enthalten sind. Außerdem müssen Art, Nummer und ausstellende Behörde des amtlichen Ausweises festgestellt werden. Diese Angaben hat das Institut zu notieren. Nach § 9 Abs. 1 Satz 2 GwG sollen, soweit möglich, die zur Feststellung der Identität vorgelegten Dokumente kopiert werden. Demzufolge kann die Sparkasse bei Finanztransaktionen ab 20.000 DM den Ausweis kopieren, muß aber nicht so verfahren. Sie könnte selbst bei diesen Geschäften die erforderlichen Daten schriftlich in die eigenen Unterlagen übertragen. Möglich wäre auch, den Ausweis nur teilweise zu kopieren, denn zu den gesetzlich vorgeschriebenen Identifikationsmerkmalen gehören nicht das Bild und die Angaben über Körpergröße und Augenfarbe.

Auf die Identifizierung und das damit verbundene Kopieren des Ausweises kann verzichtet werden, wenn der Kunde dem Finanzinstitut persönlich bekannt ist und bei früheren Gelegenheiten die Identität geprüft und aufgezeichnet worden ist. Damit soll einem unnötigen bürokratischen Aufwand bei längeren Geschäftsverbindungen begegnet werden. Das Geldwäschegesetz sieht jedenfalls keine Verpflichtung der Kreditinstitute vor, bei Kontoeröffnungen und Transaktionen unter DM 20.000 die Identität der Kunden festzustellen und die Feststellung durch eine Ausweiskopie zu dokumentieren.

Allerdings hat sich nach § 154 Abs. 2 AO derjenige, der ein Konto führt, Wertsachen verwahrt oder als Pfand annimmt oder ein Schließfach überläßt, zuvor Gewißheit über die Person und Anschrift des Verfügungsberechtigten zu verschaffen und die Angaben festzuhalten. Damit soll sichergestellt werden, daß niemand auf einen falschen oder erdichteten Namen für sich oder einen Dritten ein Konto errichtet oder Buchungen vornehmen läßt. Auch die Abgabenordnung schreibt jedoch nicht das Kopieren von Ausweisen vor.

Weder das Geldwäschegesetz noch die Abgabenordnung bieten somit eine Rechtsgrundlage für das Kopieren von Ausweisen bei Kontoeröffnungen und Finanztransaktionen von unter 20.000 DM. Auch aus sonstigen Rechtsvorschriften, etwa dem Bundesdatenschutzgesetz, ergibt sich keine derartige Verarbeitungsbefugnis. Es genügt auch nicht, daß das Kopieren vorsorglich erfolgt, weil es später einmal notwendig werden könnte. Zum einen wäre die Maßnahme unverhältnismäßig, da über eine Vielzahl von Konten wohl kaum jemals Transaktionen, die die Wertgrenze des Geldwäschegesetzes überschreiten, abgewickelt werden. Zum andern wäre es eine Datenverarbeitung auf Vorrat, und die ist unzulässig, da sie dem Erforderlichkeitsgrundsatz widerspricht.

Trotz der eindeutigen Rechtslage konnte ich zunächst den Sparkassen- und Giroverband Hessen-Thüringen nicht dazu bewegen, seine Mitglieder zur Einstellung der Kopierpraxis aufzufordern. Der Verband berief sich in erster Linie auf eine (fehlerhafte) Interpretation der Kopiervorschrift des Geldwäschegesetzes durch Ziff. 10 der Verlautbarung des Bundesaufsichtsamts für das Kreditwesen über "Maßnahmen der Kreditinstitute zur Bekämpfung und Verhinderung der Geldwäsche" vom 4. November 1993. Darin regt die Aufsichtsbehörde an, "... Kopien bei allen Geschäften, bei denen nach dem Betriebsablauf eine Identifizierung am Schalter erfolgen kann, zu erstellen. Längerfristig soll, soweit möglich, die Aufzeichnung durch Erstellen einer Kopie auch bei Geschäften erfolgen, bei denen eine Identifizierung im Kassenbereich erfolgt."

Für die Sparkassen ist hier in der Tat eine mißliche Situation dadurch entstanden, daß zwei für sie zuständige Kontrollbehörden unterschiedliche Anforderungen an die Datenverarbeitung stellen. Mittlerweile haben sich jedoch der Sparkassen- und Giroverband Hessen-Thüringen und die Sparkassen meiner Auffassung angeschlossen und das Kopieren der Ausweise bei Kontoeröffnungen und Transaktionen unter 20.000 DM eingestellt. In einem Rundschreiben des Verbandes öffentlicher Banken heißt es nun: "Es besteht Einigkeit darüber, daß § 9 Abs. 1 Satz 2 GwG ... in seinem Regelungsgehalt auf die Geschäftsvorfälle nach dem Geldwäschegesetz beschränkt ist. Daraus ergibt sich, daß derzeit keine gesetzliche Fotokopierpflicht hinsichtlich der Ausweisdokumente existiert, die zur Legitimation bei Konto- oder Depoteröffnung nach § 154 AO vorgelegt werden."

Bei Stichprobenkontrollen in mehreren Sparkassen konnten meine Mitarbeiter feststellen, daß entsprechend dem Rundschreiben verfahren wird. Verhindert wurde somit, daß die Sparkassen eine Art privates Paßnebenregister führen.

22. Telekommunikation

22.1
Postreform II

Für den Datenschutz im Bereich Telekommunikation haben sich durch die sog. Postreform II die Rahmenbedingungen im Berichtsjahr entscheidend verändert (zur ersten Reform von 1989 vgl. 18. Tätigkeitsbericht, Ziff. 16.2.3). Mit

dem Gesetz zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz – PTNeuOG) vom 14. September 1994 (BGBl. I S. 2325), das am 1. Januar 1995 in Kraft tritt, hat der Gesetzgeber den Weg frei gemacht für eine Umwandlung der Postunternehmen in Aktiengesellschaften. Kurz zuvor waren durch das Gesetz zur Änderung des Grundgesetzes vom 30. August 1994 (BGBl. I S. 2245) die verfassungsrechtlichen Voraussetzungen für die Privatisierung der bislang in unmittelbarer Bundesverwaltung geführten Unternehmen geschaffen worden.

Der Gesetzgeber hat leider nur wenige Forderungen der Datenschutzbeauftragten aufgegriffen. Das Postneuordnungsgesetz ist ein Artikelgesetz, das mehrere neue Gesetze und eine Vielzahl von Gesetzesänderungen umfaßt. Hier interessieren in erster Linie die Art. 5 (Änderung des Gesetzes über Fernmeldeanlagen), Art. 7 (Gesetz über die Regulierung der Telekommunikation und des Postwesens (PTRegG), und Art. 12 Abs. 16 mit seinen Bestimmungen zur Anwendbarkeit des Bundesdatenschutzgesetzes und zur Kontrollkompetenz des Bundesdatenschutzbeauftragten.

22.1.1
Folgen der Privatisierung für den Grundrechtsschutz und die Datenschutzkontrolle

Durch die Umwandlung der Deutschen Bundespost TELEKOM in eine Aktiengesellschaft und die Liberalisierung der Telekommunikationsdienste wird das grundgesetzlich garantierte Fernmeldegeheimnis (Art. 10 GG) nicht mehr unmittelbar gelten, denn die Grundrechte binden unmittelbar nur öffentliche Stellen. Die Geheimhaltung der Telekommunikation wird im Privatbereich primär durch Strafvorschriften geschützt. Um zu verhindern, daß die Privatisierung zu einer Verschlechterung der verfassungsrechtlichen Position der Bürger führt, muß daher im Grundgesetz sichergestellt werden, daß jeder, der Telekommunikationsdienstleistungen erbringt, das Fernmeldegeheimnis zu wahren hat. Bei der Grundgesetzänderung zur Privatisierung der Post hat der Bundestag diese Forderung jedoch unberücksichtigt gelassen.

Der Bundesbeauftragte für den Datenschutz wird nur noch für eine Übergangszeit, nämlich solange die TELEKOM noch über ein Monopol verfügt, die Kontrollkompetenz haben (Art. 12 Abs. 16 PTNeuOG). Das wird nicht mehr sehr lange sein, denn ein Beschluß des Rates der Europäischen Union vom 22. Juli 1993 (93/C 213/01) sieht für spätestens Ende 1997 die Aufhebung der Telefondienstmonopole vor. Danach würden die für die Datenverarbeitung im nicht-öffentlichen Bereich zuständigen Aufsichtsbehörden die Kontrollkompetenz erhalten. Damit verbunden wäre eine Schwächung der Kontrolle, da die Aufsichtsbehörden, anders als der Bundesdatenschutzbeauftragte, nur tätig werden dürfen, wenn sie Anhaltspunkte für eine Rechtsverletzung haben. Eine präventive Kontrolle wäre nicht mehr mögich. Darüber hinaus wäre eine Zersplitterung der Datenschutzaufsicht die Folge. Der Datenschutz bei Telekommunikationsnetzen und -diensten muß aber auf Dauer von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien von Amts wegen kontrolliert werden können.

In der Beschlußempfehlung und dem Bericht des Bundestagsausschusses für Post und Telekommunikation vom 27. Juni 1994 (BT-Drucks. 12/8060, S. 200) findet sich immerhin die Feststellung, es bestehe "Einigkeit darüber", daß, wenn die TELEKOM über kein Monopol mehr verfüge, in Absprache mit den Bundesländern eine zentrale Kontrollstelle für den Datenschutz bestimmt werden solle.

22.1.2
Auskunft an Strafverfolgungsbehörden über den Fernmeldeverkehr

Obgleich das Fernmeldeanlagengesetz (FAG) durch das Postneuordnungsgesetz umfangreich geändert und ergänzt worden ist, wurde die dringend notwendige Überarbeitung des § 12 FAG unterlassen. Die Vorschrift regelt die Weitergabe von Telekommunikationsdaten für Strafverfolgungszwecke. Nicht nur die Datenschutzbeauftragten kritisieren diese Bestimmung schon seit langem, sondern auch der Bundesrat hat bereits im August 1991 (BR-Drucks. 416/91) eine Neuregelung verlangt. Der Paragraph stammt aus dem Jahr 1927 und hat durch die technische Entwicklung eine völlig neue Bedeutung erlangt.

Im analogen Netz werden einzelne Verbindungsdaten nur erfaßt, wenn Fangschaltungen oder Zählvergleichseinrichtungen installiert sind. In der digitalen Telekommunikation ist das grundlegend anders. Dort werden zwangsläufig Datum, Uhrzeit, Dauer, Rufnummer des Anschlusses, von dem aus angerufen wird, und die Zielnummer gespeichert. Auf diese Daten können nach § 12 FAG Gerichte und Staatsanwaltschaften in strafrechtlichen Ermittlungsverfahren jeder Art, also selbst bei Bagatelldelikten, ohne besondere Voraussetzungen zugreifen. Gemessen an der "Fangschaltungsentscheidung" des Bundesverfassungsgerichts vom 25. März 1992 (BVerfGE 85,386) dürfte diese Befugnisnorm verfassungswidrig sein.

22.1.3
Anrufe bei Beratungseinrichtungen und Einzelgebührennachweis

Es gibt eine Reihe von Beratungseinrichtungen (z.B. Telefonseelsorge, Drogenberatung, AIDS-Beratung), deren Tätigkeit, Wirkung und Erfolg auf anonymen Kontakten zu den Anrufern beruht. Die Anonymiät darf nicht dadurch aufgehoben werden, daß Anrufe bei diesen Stellen im Einzelgebührennachweis, den der Anschlußinhaber beantragen kann, ausgewiesen werden. Die TELEKOM-Datenschutzverordnung (TDSV) vom 1. Juli 1991 (BGBl. I S. 1390) und die Teledienstunternehmen-Datenschutzverordnung (UDSV) vom 18. Dezember 1991 (BGBl. I S. 2337) schreiben deshalb vor, daß Anrufe bei Personen und Einrichtungen, die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln, aus dem Nachweis nicht ersichtlich sein dürfen.

Mit ihrer noch weitergehenden Forderung, jedem Anschlußinhaber freizustellen, ob und wie seine Rufnummer auf Einzelgebührennachweisen erscheinen soll, konnten sich die Datenschutzbeauftragten nicht durchsetzen. Diese Lösung würde auch die Anonymität von Anrufen bei Beratungseinrichtungen einfach und effektiv gewährleisten. Die Vorschrift in § 10 Abs. 2 Satz 1 Nr. 4 PTRegG ist sogar noch restriktiver als es die ohnehin schon zu engen Regelungen der TDSV und UDSV sind.

Ich erwarte nunmehr von der Landesregierung, daß sie sich dafür einsetzt, daß zumindest ein Teil der Regelungsdefizite kompensiert wird durch die von der Bundesregierung nach § 10 PTRegG mit Zustimmung des Bundesrates zu erlassene Rechtsverordnung zum Datenschutz.

22.2
EU-Richtlinie zum Datenschutz in Telekommunikationsnetzen (ISDN-Richtlinie)

Die Kommission der Europäischen Union hat dem Rat der Europäischen Union am 13. Juni 1994 einen geänderten Vorschlag für eine EG-Richtlinie zum Datenschutz in Telekommunikationsnetzen vorgelegt ("Geänderter Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und digitalen Mobilfunknetzen"; KOM (94) 128 endg. – COD 288). Das Kürzel ISDN steht für "Integrated Services Digital Network", das Einheitsnetz für Sprach-, Text-, Daten- und Bildkommunikation. Zu dem vorausgegangenen Vorschlag der Kommission, der vom 27. Juli 1990 datiert (KOM (90) 414 endg. – SYN 288), hatte das Europäische Parlament eine Reihe von Änderungen beschlossen.

Die Richtlinie soll die in Vorbereitung befindliche allgemeine EU-Datenschutzrichtlinie ergänzen (zu letzterer siehe Ziff. 30.1 dieses Berichts). Sie ist eine Reaktion auf die rapide zunehmende Digitalisierung der öffentlichen Telekommunikationsnetze in der Europäischen Union. Digitalisierung bedeutet, daß der Verbindungsaufbau und die Übertragung der Informationen im Wege der elektronischen Datenverarbeitung erfolgen. Auf die binär codierten Informationen, die sog. Bit-Folgen, d.h. mittels Elektronik verwirklichte Ja- und Nein-Aussagen, kann mit Computern sowohl innerhalb des Netzes als auch im Teilnehmerendgerät direkt zugegriffen werden. Das ermöglicht einerseits eine Vielzahl neuer Telekommunikationsfunktionen, wie z.B. die Anzeige der Rufnummer des Anrufers oder die Anrufweiterschaltung, führt aber andererseits auch zu neuen Risiken für die Vertraulichkeit der Kommunikation.

Diese Gefahren machen naturgemäß nicht vor den nationalen Grenzen halt. Deshalb haben die Datenschutzbeauftragten des Bundes und der Länder ihre Forderung nach einer EU-Richtlinie für den Datenschutz im ISDN mehrmals bekräftigt (vgl. 22. Tätigkeitsbericht, Ziff. 23.5 sowie Ziff. 31.10 dieses Berichts), und auch das Europäische Parlament hat in einer Entschließung vom 16. September 1993 die Kommission aufgefordert, unverzüglich einen geänderten Richtlinienvorschlag vorzulegen (ABl. Nr. C 268 vom 4. Oktober 1993, S. 166).

Ziel der von der Kommission vorgeschlagenen Richtlinie ist die Schaffung unionsweit einheitlicher Bedingungen für den Datenschutz in Telekommunikationsnetzen, um abweichende nationale Regelungen zu verhindern, da diese den Binnenmarkt für Telekommunikationsdienste und Endgeräte gefährden könnten. Mit Hinweis auf das Subsidiaritätsprinzip, wonach die Union nur das regeln darf, was die Mitgliedstaaten nicht ausreichend selbst regeln können (Art. 3b EG-Vertrag), hat die Kommission etliche der ursprünglich vorgeschlagenen Bestimmungen gestrichen. Bedauerlicherweise verzichtet der Vorschlag nun so weit wie möglich auf technische Vorgaben. Es wird beispielsweise nicht mehr verlangt, daß die Möglichkeit zur fallweisen Unterdrückung der Rufnummernanzeige angeboten werden muß. Auch die ursprüngliche Anforderung, daß der anrufende Teilnehmer bei Aufbau der Verbindung automatisch über die Anrufweiterschaltung informiert werden muß, wurde gestrichen.

Der geänderte Vorschlag sieht eine unangemessene Privilegierung von Diensteanbietern vor. Für öffentliche, digitale Telekommunikationsdienstleistungen von anderen Diensteanbietern als Telekommunikationsorganisationen (Netzbetreibern) und für andere Telekommunikationsdienste, die über das öffentliche Netz angeboten werden, gelten z.B. nicht die Vorschriften über die Anzeige der Rufnummer und die Anrufweiterschaltung. Die Datenschutzbeauftragten des Bundes und der Länder haben dies in ihrem Beschluß vom 26./27. September 1994 kritisiert und die Bundesregierung aufgefordert, darüber hinaus auf weitere Verbesserungen hinzuwirken. Das betrifft u.a. die ungenügende Zweckbindung, die Speicherung von Inhaltsdaten nach Beendigung der Übertragung, die Erstellung elektronischer Profile der Teilnehmer und den Einzelgebührennachweis (vgl. Ziff. 31.10 dieses Berichts).

Angesichts der anstehenden Liberalisierung der Telekommunikationsmärkte bleibt zu hoffen, daß der Rat der Europäischen Union und das Europäische Parlament möglichst bald die ISDN-Richlinie erlassen.

23. Statistik: Novellierung des Landesstatistikgesetzes

Am 27. September 1994 hat die Landesregierung dem Landtag einen zuvor mit dem Hessischen Datenschutzbeauftragten weitgehend abgestimmten Gesetzentwurf zur Novellierung des Hessischen Landesstatistikgesetzes (HessLStatG) vorgelegt (Drucks. 13/6570). Neben der Streichung einer Übergangsvorschrift für die Verrechtlichung von Landes- und Kommunalstatistiken sieht der Entwurf einige Klarstellungen und zusätzliche Informationspflichten vor.

Das Landesstatistikgesetz vom 19. Mai 1987 (GVBl. I S. 67) setzt die rechtlichen Anforderungen, die das Bundesverfassungsgericht in seinem Volkszählungsurteil von 1983 an die amtliche Statistik gestellt hat, für den Landes- und Kommunalbereich um. Es regelt die allgemeinen materiell-rechtlichen Bedingungen (z.B. das Statistikgeheimnis)

sowie Organisation und Verfahren der Landes- und Kommunalstatistik. Außerdem enthält es ergänzend zum Bundesstatistikgesetz Bestimmungen für die Durchführung von Bundesstatistiken und Statistiken der Europäischen Union, die in der Regel dem Land obliegt.

Nach dem Landesstatistikgesetz müssen Landes- und Kommunalstatistiken in einem Gesetz bzw. einer Satzung angeordnet werden (§§ 7 Abs. 1 und 12 Abs. 1 HessLStatG). Die Vorschrift ist eine Konsequenz aus dem genannten Volkszählungsurteil, in dem das Bundesverfassungsgericht festgehalten hat, daß Statistiken mit Auskunftspflicht einer gesetzlichen Grundlage bedürfen. Für Landes- und Kommunalstatistiken, die zum Zeitpunkt des Inkrafttretens des Gesetzes bereits durchgeführt wurden, schob § 23 HessLStatG den Verrechtlichungszwang bis zum 1. Mai 1989 auf. Damit sollte zum einen verhindert werden, daß bereits existierende Statistiken wegen mangelnder Rechtsgrundlage nicht mehr weitergeführt werden konnten. Gleichzeitig setzte der Gesetzgeber sich und den Kommunen eine nicht allzu lange Frist für die Schaffung verfassungskonformer Bedingungen für diese Statistiken. Mehr als fünfeinhalb Jahre danach gibt es jedoch immer noch kein Sammelgesetz über landesrechtliche Einzelstatistiken.

Die Landesregierung ist inzwischen zu der Auffassung gelangt, daß für Landesstatistiken mit Auskunftspflicht kein Bedarf vorhanden ist. Der Informationsbedarf läßt sich nach ihrer Einschätzung mit Hilfe von Statistiken ohne Auskunftspflicht und statistischen Umfragen decken: "Es bestehen keine belegbaren Erkenntnislücken, die den Aufwand rechtfertigen, der mit einer zwangsweisen statistischen Erhebung verbunden ist." (Drucks. 13/6570, S. 5). Dieser Meinung ist der Hessische Datenschutzbeauftragte schon seit langem (vgl. etwa 15. Tätigkeitsbericht, Ziff. 8.1.3). Gegen die Streichung des § 23 HessLStatG bestehen daher auch keine Bedenken.

Nach dem Wortlaut des § 7 HessLStatG erfordern auch Statistiken, die auf der Grundlage freiwilliger Beteiligung der zu Befragenden durchgeführt werden, eine bereichsspezifische gesetzliche Regelung. Das ist jedoch verfassungsrechtlich nicht geboten. Nimmt der Bürger freiwillig an einer statistischen Erhebung teil, liegt kein Eingriff in sein Recht auf informationelle Selbstbestimmung vor. Im Gesetzentwurf wird dies jetzt klargestellt. Freilich muß garantiert sein, daß der Bürger auch keinem faktischen Zwang ausgesetzt ist, an der Befragung teilzunehmen. Das wäre beispielsweise der Fall, wenn eine bedeutsame Leistungsgewährung an die Beantwortung geknüpft würde.

Der Gesetzentwurf enthält außerdem zusätzliche grundrechtssichernde Maßnahmen. Er präzisiert und erweitert die in § 14 HessLStatG festgelegten Informationspflichten, die das Statistische Landesamt bei der Durchführung von Statistiken hat: Die Betroffenen müssen ausdrücklich auf die Freiwilligkeit der Teilnahme hingewiesen werden, und sie müssen über die verschiedenen Arten der Auskunftserteilung unterrichtet werden. In Betracht kommt z.B., daß die Auskunft mündlich, schriftlich, gegenüber Erhebungsbeauftragten oder direkt gegenüber dem Statistischen Landesamt erteilt werden kann.

Der Unterausschuß Informationsverarbeitung und Datenschutz des Hessischen Landtags hat am 7. November 1994 den Gesetzentwurf beraten (Beschlußprotokoll UID/13/7 vom 8. November 1994) und dem federführenden Hauptausschuß vorgeschlagen, dem Plenum zu empfehlen, den Entwurf mit einer kleinen, von mir angeregten, Präzisierung anzunehmen.

24. Presseerklärungen der Regierung

Darf die Regierung in Presseerklärungen finanzielle Verhältnisse von Bürgern offenbaren?

Tierparks, in denen Tiere wildlebender Arten gehalten werden, bedürfen der Genehmigung der oberen Naturschutzbehörde. Diese Genehmigung wurde dem Eigentümer eines Vogelparks entzogen. Die Behörde begründete die Schließungsverfügung damit, der Betreiber habe gegen das Hessische Naturschutzgesetz verstoßen. Teile der Anlage seien ungenehmigt errichtet worden. In diesem Fall verlange das Gesetz ein unverzügliches Verbot der Nutzung. Bei einer Kontrolle durch die Artenschutzbehörde seien außerdem Verstöße gegen internationale Artenschutzbestimmungen festgestellt worden.

Fünf Monate später teilte die oberste Aufsichtsbehörde, das Hessiche Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz, in einer Pressererklärung mit, einer baldigen Wiedereröffnung des Vogelparks stehe nichts mehr im Wege. Die Genehmigung zur Wiedereröffnung werde jedoch nur auf Widerruf erteilt und sei an die Erfüllung verschiedener Auflagen gebunden. Der Betreiber müsse innerhalb von zwei Monaten nach Erlaß des Bescheids eine Sicherheitsleistung erbringen, da wegen seiner schlechten Vermögensverhältnisse nicht sichergestellt sei, daß er die notwendigen Umbauten zur artgerechten Haltung der Tiere überhaupt finanzieren könne. Ein Bürger, der die Erklärung in der Zeitung gelesen hatte, sah darin einen Verstoß gegen den Datenschutz und bat mich um Überprüfung der Angelegenheit.

Es geht hier um ein Problem, zu dem es kaum gesetzliche Regelungen gibt, nämlich um das Verhältnis von Informationsinteresse der Öffentlichkeit und Persönlichkeitsschutz. Dem durch Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 GG garantierten Recht auf informationelle Selbstbestimmung steht die ebenfalls verfassungsrechtlich gesicherte Pressefreiheit (Art. 5 Abs. 2 GG) gegenüber. Pressefreiheit bedeutet nicht nur Äußerungsfreiheit, sondern umfaßt auch den Schutz der Informationsbeschaffung durch die Medien. Behörden können der Presse nicht nach Belieben Auskünfte verweigern. Deshalb verpflichtet das Hessische Gesetz über Freiheit und Recht der Presse in der Fassung vom 20. November 1958 (GVBl. II 74-2) die Behörden, der Presse die gewünschten Auskünfte zu erteilen.

Der presserechtliche Auskunftsanspruch gilt freilich nicht schrankenlos. Da auch der Persönlichkeitsschutz verfassungsrechtlich garantiert ist, sieht das Pressegesetz vor, daß Auskünfte über persönliche Angelegenheiten verweigert werden können, wenn kein berechtigtes Interesse an der öffentlichen Bekanntgabe besteht (§ 3 Abs. 1 Satz 2 Nr. 2 PresseG).

Restriktionen enthält allerdings nicht nur das Pressegesetz. Die Unterrichtung der Presse über die finanziellen Verhältnisse des Vogelparkbetreibers war zweifelsohne eine Datenübermittlung im Sinne des Hessischen Datenschutzgesetzes, so daß sich die Frage stellte, ob dessen Übermittlungsvorschriften hier vorrangig zu beachten waren. Nach §§ 11 und 16 HDSG dürfen öffentliche Stellen personenbezogene Daten an private Dritte weitergeben, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist oder der Empfänger ein berechtigtes Informationsinteresse glaubhaft gemacht hat und keine Beeinträchtigung schutzwürdiger Belange des Betroffenen erkennbar ist.

Der Gesetzgeber hat bei der Novellierung des Hessischen Datenschutzgesetzes 1986 bewußt auf Spezialvorschriften für den Pressebereich verzichtet und eventuelle Regelungen dem Pressegesetz vorbehalten. Daraus läßt sich schließen, daß § 3 Abs. 1 PresseG, obgleich er weniger konkrete Vorgaben enthält als die Übermittlungsvorschriften des Hessischen Datenschutzgesetzes, die für die Beurteilung der Datenübermittlung an die Presse vorrangige Norm ist.

Im Ergebnis macht es ohnehin keinen Unterschied, ob man die Presseerklärung nach dem Pressegesetz oder dem Hessischen Datenschutzgesetz beurteilt. Die Behörden müssen bei der Erteilung von Auskünften in jedem Fall den verfassungsrechtlich garantierten Persönlichkeitsschutz der Betroffenen berücksichtigen. Notwendig ist daher eine Abwägung zwischen den schutzwürdigen Interessen der Betroffenen und dem öffentlichen Informationsinteresse. Daten, die wegen ihres streng persönlichen Charakters nach der Rechtsprechung des Bundesverfassungsgerichts nicht einmal einem parlamentarischen Untersuchungsausschuß zur Verfügung gestellt werden dürfen, können folglich auch nicht der Presse mitgeteilt werden. Gesetzliche Übermittlungsverbote sind eine weitere Informationssperre. Eine Sonderregelung enthält § 69 Abs. 1 Nr. 3 SGB X für die öffentliche Bekanntgabe von Sozialdaten. Sie ist nur zulässig, wenn die öffentliche Richtigstellung unwahrer Tatsachenbehauptungen des Betroffenen im Zusammenhang mit einem Verfahren über die Erbringung von Sozialleistungen erforderlich ist.

Über die Schließung des Vogelparks war in Presse, Funk und Fernsehen detailliert berichtet worden. Dabei seien, so das Ministerium in einer von mir angeforderten Stellungnahme, vom Betreiber selbst Einkommen und Einnahmeverluste vorgerechnet und die Kosten für die Erfüllung der Auflagen kritisiert worden. Die Presseerklärung habe der Klar- und Richtigstellung von behördlichen Maßnahmen gedient, die von dritter Seite verzerrt wiedergegeben worden seien.

Da die Tierhaltung des Vogelparks in die öffentliche Diskussion geraten war, bestand ein berechtigtes Interesse der Öffentlichkeit, die Entscheidungskriterien für die Wiedereröffnung zu erfahren. Zu diesen Kriterien gehörte eben auch die Sicherheitsleistung, so daß der Hinweis auf die Vermögensverhältnisse unvermeidbar war. Ein überwiegendes schutzwürdiges Interesse des Betreibers, das einer Veröffentlichung entgegengestanden hätte, war nicht zu erkennen und die Presseerklärung daher zulässig.

25. Datensicherheitskonzepte

25.1
Allgemeine Anmerkungen

25.1.1
Überblick

In meinem letzten Tätigkeitsbericht Ziff. 21 habe ich auf Risiken hingewiesen, die sich aus der Abhängigkeit von einer korrekt funktionierenden Informations- und Kommunikationstechnik ergeben.

Wenn man sich im Einzelfall auf die IT-Sicherheit beschränkt, wie sie im IT-Sicherheitshandbuch des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erläutert wird, werden gesellschaftliche oder rechtliche Fragestellungen nur eingeschränkt berücksichtigt. Dort heißt es, "bei der IT-Sicherheit geht es um den Schutz der Anwendungen der Informationstechnik vor möglichen Bedrohungen, die die Verfügbarkeit der IT-Systeme und die Integrität und die Vertraulichkeit der verarbeiteten Informationen gefährden". Aber auch wenn man auf eine umfassende Aufarbeitung im Rahmen einer Technikfolgenabschätzung verzichtet, führt diese Betrachtung eines Teils des Gesamtproblems zu Forderungen, die umgesetzt werden müssen.

Bei Prüfungen mußte ich oft Mängel an technischen und organisatorischen Datenschutzmaßnahmen feststellen, die durch ein Datenschutz-/Datensicherheitskonzept hätten verhindert werden können. Ich halte es daher in aller Regel für erforderlich, ein derartiges Konzept zu erarbeiten und umzusetzen. Diese Forderung wird nicht nur von Datenschutzbeauftragten erhoben. In den "Mindestanforderungen der Rechnungshöfe des Bundes und der Länder zum Einsatz der Informationstechnik" vom Mai 1991 heißt es unter Punkt 7.2.1: "Die zur Aufrechterhaltung der Sicherheit geeigneten Maßnahmen sind aus einer Risikoanalyse abzuleiten und in einem Sicherheitskonzept darzustellen."

Auch die Hessische Landesregierung hat in ihrer Stellungnahme zum 20. Tätigkeitsbericht (LTDrucks. 13/2651) sowie in Ihrem "Bericht zum Berichtsantrag der Abgeordneten Wilke, Hahn, Pfeil (FDP) und Fraktion betreffend Risikoanalysen und Sicherheitskonzepte für den Einsatz der Informationstechnik in der hessischen Landesverwaltung" (LTDrucks. 13/2990) die Erforderlichkeit von angemessenen Sicherheitskonzepten bzw. Sicherheitsanalysen festgestellt.

Es besteht ein weitgehender Konsens, wonach Sicherheitskonzepte erstellt werden müssen. Allerdings gibt es unterschiedliche Vorgehensweisen, wie ein Konzept entwickelt werden kann.

In der Zeitschrift KES 4.94 wurden – nicht repräsentativ – 32 Unternehmen, die Sicherheitsberatungen vornehmen, zu Leistungen und Preisen befragt. Als Vorgehensweisen wurden die (checklistengestützte) Schwachstellenanalyse,

CRAMM, DDIS, MARION, Risk-Watch, Security-by-Analysis, selbstentwickelte Verfahren sowie Verfahren nach dem IT-Sicherheitshandbuch des BSI zur Auswahl gestellt. Es waren Mehrfachnennungen möglich. Spitzenreiter waren die Schwachstellenanalyse (97 v.H.), Verfahren nach dem IT-Sicherheitshandbuch des BSI (63 v.H.) und selbstentwickelte Verfahren (30 v.H.).

Auf das IT-Sicherheitshandbuch des BSI möchte ich kurz eingehen, da es insbesondere für die öffentliche Verwaltung relevant ist. Für die Bundesverwaltung ist das Erstellen von Sicherheitskonzepten nach dem Vorgehensmodell des IT-Sicherheitshandbuchs vorgeschrieben. Das IT-Sicherheitshandbuch geht von einem Schutzstufenkonzept aus. Über die Ermittlung der Schutzbedürftigkeit, einer Bedrohungsanalyse und einer Risikoanalyse führt das Vorgehensmodell zum Sicherheitskonzept. Dabei werden aufbauend auf die Bedrohungs- und Risikoanalyse die erforderlichen Maßnahmen ermittelt.

Diese Vorgehensweise ist aufwendig und hat dazu geführt, daß eine Vereinfachung vorgesehen wurde. Im KBSt-Brief 2/93 wurden die Grundzüge dargestellt. Als Arbeitsgrundlage dient das IT-Grundschutzhandbuch, welches für Anwendungen mit mittlerem Schutzbedürfnis eine pauschale Bedrohungs- und Risikoanalyse voraussetzt und die in diesem Fall nötigen Maßnahmen festlegt. Das Handbuch liegt derzeit in einer ersten Version vor und soll dieses Jahr veröffentlicht werden.

25.1.2
Sicherheit am PC-Arbeitsplatz

Vor mehr als einem Jahr hat das Hessische Ministerium des Innern einen Leitfaden "Sicherheit am PC-Arbeitsplatz" bei der HZD in Auftrag gegeben. Damit sollte den Dienststellen insbesondere in übersichtlicher Form dargelegt werden, welche Sicherheitsmaßnahmen an einem PC-Arbeitsplatz mit mittlerem Schutzbedarf erforderlich sind. Diese Initiative habe ich sehr begrüßt. Während der Leitfaden erarbeitet wurde, stellte das BSI interessierten Stellen den Prototypen des IT-Grundschutzhandbuchs zur Verfügung, in dem, über das Thema des Leitfadens hinaus, z. B. auch auf UNIX-Systeme, UNIX-Netze oder TK-Anlagen eingegangen wurde. Bei dem Vergleich der beiden Vorlagen konnte man feststellen, daß das Ausgangsthema inhaltlich ähnlich angegangen wurde. Da nicht klar war, ob, wann und in welcher Form das IT-Grundschutzhandbuch veröffentlicht würde und die Darstellungen abwichen, wurde der Leitfaden fertiggestellt.

Das IT-Grundschutzhandbuch wurde im Juli 1994 in der Version 1 für die Bundesverwaltung veröffentlicht. Auf dieser Basis wurde Ende des Jahres im UA-Büroautomation des Landesautomationsausschuß (LAA) diskutiert, ob das IT-Grundschutzhandbuch des BSI oder der Leitfaden Grundlage für Datensicherheitsmaßnahmen bei PC mit mittlerem Schutzbedarf sein sollte. Als Ergebnis sollte dem LAA vorgeschlagen werden, das IT-Grundschutzhandbuch als Grundlage für Sicherheitsüberlegungen – nicht nur zu PC-Arbeitsplätzen – des IT-Managements bzw. von IT-Sicherheitsverantwortlichen zu empfehlen und den Leitfaden zu einer Hilfe für den Endanwender umzugestalten.

25.2
Einzelne Projekte

In der hessischen Landesverwaltung sind im letzten Jahr in einigen Fällen Sicherheitskonzepte erstellt oder begonnen worden. Dabei sind das Umweltministerium, die Polizei und die Staatskanzlei zu nennen. In die beiden erstgenannten Projekte bin ich beratend eingebunden.

Obwohl in allen Fällen auf dem IT-Sicherheitshandbuch des BSI aufgebaut wird, gibt es im Detail Unterschiede. Der wesentliche Unterschied ist in den beteiligten Stellen zu sehen. Das Umweltministerium baut weitgehend auf den Leistungen einer Unternehmensberatung auf. Die Staatskanzlei arbeitet vordringlich mit der HZD zusammen. Die Polizei geht das Problem mit eigenem Personal an, wobei eine externe Stelle beratend tätig ist. Alle Ansätze sind nach meiner Einschätzung unter den jeweils gültigen Rahmenbedingungen sorgfältig ausgewählt und umgesetzt worden. Ich werde den Fortschritt der Projekte begleiten, um dadurch Erfahrungen für zukünftige, ähnliche Fälle gewinnen zu können. Bei einer Festlegung des Vorgehensmodells zur Erstellung von Sicherheitskonzepten für die hessische Landesveraltung sollten die Ergebnisse in jedem Fall berücksichtigt werden.

25.2.1
Das Hessische Ministerium für Umwelt und Bundesangelegenheiten

Das Hessische Ministerium für Umwelt und Bundesangelegenheiten hat von einer Unternehmensberatung Vorschläge erarbeiten lassen, wie die Informationsverarbeitung zukünftig gestaltet werden soll. Dabei wurden mehrere Konzepte für erforderlich angesehen, zu denen ein Sicherheitskonzept gehört. 1994 wurde nach einer öffentlichen Ausschreibung ein externes Beratungsunternehmen ausgewählt, welches auf Grundlage des IT-Sicherheitshandbuchs und des IT-Grundschutzhandbuchs das Konzept erstellt.

25.2.2
Polizei

Im Rahmen des Projekts Hessisches Polizeiarbeitsplatzsystem (HEPOLAS) wird ebenfalls ein Sicherheitskonzept erstellt. Die Polizei erarbeitet mit eigenen Mitarbeitern, nach dem IT-Sicherheitshandbuch vorgehend, die Dokumente. Das BSI ist beratend eingebunden. Das Sicherheitskonzept ist, im Gesamtzusammenhang gesehen, wichtig. Nur dadurch besteht eine Möglichkeit festzustellen, ob die erforderlichen Sicherheitsmaßnahmen ergriffen wurden.

Leider hat es in dem Projekt Verzögerungen gegeben, die speziell das Sicherheitskonzept betrafen. Es wurden zwar von vornherein bei der Entwicklung von HEPOLAS Sicherungsmaßnahmen vorgesehen, aber ob diese ausreichend sind, kann nur der Abgleich mit dem Konzept zeigen. Wenn sich Defizite abzeichnen, hätte dies nachteilige Folgen für das Projekt, da die Erfahrung gezeigt hat, daß Sicherheitsmaßnahmen nachträglich nur schwer in Anwendungen integriert werden können.

Im Ergebnis sollte es gelingen, einen nach Meinung aller Beteiligten ausreichenden Sicherheitsstand zu erreichen.

25.2.3
Staatskanzlei

Die Staatskanzlei hat in den letzten zwei Jahren in enger Zusammenarbeit mit der HZD ein Sicherheitskonzept für ihre Informationsverarbeitung erstellt. Ende 1994, d.h. bei Redaktionsschluß, befand es sich in der Abstimmung. In der nächsten Zeit dürfte es verabschiedet werden.

Die gewonnenen Erfahrungen können über die HZD den Dienststellen des Landes zugute kommen.

26. Einsatz von Verschlüsselungsverfahren

Unter Ziff. 21.1 habe ich in meinem 22. Tätigkeitsbericht allgemeine Anmerkungen zu Problemen der Datensicherheit und des Datenschutzes in offenen Kommunikationsnetzen gemacht. Die dort genannten Beispiele für schon existierende Lösungen betrafen teilweise nur spezielle Probleme oder unterlagen nicht meiner Kontrollkompetenz.

Mittlerweile gibt es erste Projekte in Hessen, in denen die geschilderten Bedrohungen berücksichtigt und entsprechende Sicherheitsmaßnahmen geplant sind. An zwei Projekten aus dem Gesundheitsbereich, die sich zur Zeit in der Realisierung befinden, hat man mich zu einem frühen Zeitpunkt beteiligt.

26.1
Datenübertragung zwischen der AOK Hessen und Arbeitgebern

Zwischen Krankenkassen und Arbeitgebern gibt es eine Reihe von Datenübermittlungen, die derzeit noch in Form von Listen oder mit anderen Datenträgern erfolgen. Die AOK Hessen führt einen Pilotversuch mit der Lufthansa durch, in dem Mitteilungen, die z.B. im Rahmen der Lohnfortzahlung im Krankheitsfall zu machen sind und bisher per Briefpost erfolgen, mittels Datenfernübertragung (DFÜ) vorgenommen werden.

Die technische Realisierung sieht vor, Dateien mit FTAM (File Transfer, Access and Management) zwischen den Rechnern der Kommunikationspartner auszutauschen. Dabei sind insbesondere die folgenden Sicherheitsziele für die Übertragung als wesentlich erachtet worden:

- Die übertragenen personenbezogenen Daten sind sensibel und dürfen Unbefugten nicht zur Kenntnis gelangen. Die Vertraulichkeit muß gewährleistet sein.
- Aufgrund der Daten werden Geldzahlungen vorgenommen, so daß die Authentizität des Urhebers der Daten, AOK oder Arbeitgeber, feststellbar sein muß.
- Die Integrität der Daten muß gewährleistet sein.

Um dies zu erreichen, ist vorgesehen, PC zwischen dem öffentlichen Netz und dem Rechner des jeweiligen Kommunikationspartners einzubinden. Auf diesen PC soll eine Software installiert werden, welche die zu übertragenden Dateien

- verschlüsselt (damit wäre die Vertraulichkeit zu erreichen) und
- elektronisch signiert (damit können die Authentizität der Urheber nachgewiesen, sowie die Integrität der Daten verifiziert werden).

Als Verschlüsselungsalgorithmen sind DES und RSA (vgl. Ziff. 27) vorgesehen. Zum Schlüsselmanagement ist der Ausbau einer Clearingstelle geplant, welche die öffentlichen Schlüssel der Kommunikationspartner verwaltet. Die Erzeugung der privaten und öffentlichen Schlüssel soll dezentral bei den beteiligten Stellen erfolgen.

Die AOK Hessen führt den Pilotversuch stellvertretend für alle AOK durch. Wenn der Versuch erfolgreich ist, soll das Verfahren bundesweit übernommen werden. Wegen der grundsätzlichen Fragestellungen und der Bedeutung für künftige Anwendungen wird der Versuch von mehreren Datenschutzbeauftragten begleitet. Neben mir sind es der Bundesbeauftragte für den Datenschutz sowie die Landesbeauftragten für den Datenschutz Hamburg, Bremen und Rheinland-Pfalz. Erste Ergebnisse dürften schon Mitte dieses Jahres vorliegen.

26.2
Umsetzung der Pflegeversicherung; Einbeziehung externer Gutachter

Der Medizinische Dienst der Krankenkassen in Hessen plant, im Rahmen der Umsetzung der Pflegeversicherung externe Gutachter einzusetzen. Diese werden entsprechend den Anweisungen des Medizinischen Dienstes der Krankenkassen tätig und untersuchen Patienten. Anhand der Gutachten wird u.a. entschieden, welche Pflegestufe für eine Person gilt.

Dazu wurde ein Konzept entwickelt, wie welche Abläufe automatisiert werden sollen. Soweit die externen Gutachter betroffen sind, läßt sich das Konzept wie folgt skizzieren: Es ist vorgesehen, die Gutachter mit Laptops auszustatten. Die Informationen des Medizinischen Dienstes der Krankenkassen über die zu untersuchenden Personen sollen per DFÜ an den Gutachter gesandt werden. Nachdem die Gutachten fertiggestellt sind, werden sie, wieder per DFÜ, an den Medizinischen Dienst der Krankenkassen geschickt, um dort weiterbearbeitet zu werden. Nach der Versendung werden das Gutachten und die zugehörigen Patientendaten auf dem Laptop gelöscht.

Das Konzept stellt hohe Anforderungen an den technischen Datenschutz und die Datensicherheit.

- Der Rechner des Medizinischen Dienstes der Krankenkassen muß u.a. wegen der in Software realisierten Verschlüsselungsfunktionen besonders gesichert werden. Unberechtigte Zugriffe über die DFÜ-Schnittstellen stellen dabei ein erhebliches Risiko dar.
- Die Laptops unterliegen größeren Sicherheitsrisiken als Rechner, die in einem Gebäude untergebracht sind; so ist das Risiko eines Diebstahls besonders hoch. Es soll deshalb ein gesondertes Sicherheitskonzept für die Laptops erstellt werden, das neben anderen Maßnahmen eine Verschlüsselung aller gespeicherten Daten vorsieht.
- Neben diesen auf die Rechner bezogenen Sicherungsmaßnahmen soll die Datenübertragung ebenfalls dem neuesten technischen Stand entsprechen. Dazu ist vorgesehen, die Daten verschlüsselt und mit elektronischer Signatur versehen auszutauschen (vgl. 22. Tätigkeitsbericht, Ziff. 31.1.3.1.3). Das Schlüsselmanagement soll durch den Medizinischen Dienst der Krankenkassen erfolgen.

Wenn mir detailliertere Angaben vorliegen, kann geprüft werden, inwieweit Anforderungen des Datenschutzes erfüllt sind. Die Umsetzung der Vorgaben wird dann entscheiden, ob Vorbehalte anzumelden sind.

27. Workshop Kryptografie

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird durch eine Reihe von Arbeitskreisen unterstützt. Die Arbeitskreise stellen den Informationsaustausch zwischen den Datenschutzbeauftragten sicher und bereiten Entschließungen der Konferenz vor. Der AK-Technik, unter dem Vorsitz des Landesbeauftragten für den Datenschutz Mecklenburg-Vorpommern, bearbeitet den Bereich der technischen und organisatorischen Fragen des Datenschutzes. Zu speziellen Themen werden Workshops abgehalten.

Im letzten Jahr wurde in Wiesbaden ein Workshop zu Teilaspekten der Kryptografie durchgeführt, an dem Vertreter des Bundesamtes für Sicherheit in der Informationstechnik (BSI), des Bundesministeriums des Innern sowie aus Wissenschaft und Wirtschaft teilnahmen.

Eine allgemeine Darstellung zu Aspekten der Datensicherheit in offenen Kommunikationsnetzen hatte ich im 22. Tätigkeitsbericht gegeben (Ziff. 21.1). Bei dieser Gelegenheit muß ich auf einen Druckfehler hinweisen. Unter dem Punkt 21.1.2.4 befindet sich eine Tabelle, der die Zuordnung zwischen Sicherheitsdiensten und Sicherheitsmechanismen zu entnehmen ist. In der ersten Zeile muß zu dem Sicherheitsmechanismus "Verschlüsselung" bei "Vertraulichkeit" ein "X" eingefügt werden. Auf dem Workshop wurden einige der im 22. Tätigkeitsbericht angeführten Punkte vertieft behandelt; insofern ist dieses Kapitel ein Bilanzbeitrag, auf dessen Informationen ich mich wegen der gegebenen Aktualität an dieser Stelle beziehe.

Die in dem Workshop behandelten Themen lassen sich mehreren Blöcken zuordnen:

- Verschlüsselungsverfahren
- Publikation von Verschlüsselungsverfahren
- Neue Entwicklungen in der elektronischen Kommunikation.

Bei den folgenden Informationen handelt es sich, soweit nicht besonders vermerkt, um Aussagen der Experten, die noch nicht bewertet sind.

27.1
Verschlüsselungsverfahren (vgl. 22. Tätigkeitsbericht, Ziff. 21.1.3.1)

27.1.1
Sicherheit von Verschlüsselungsverfahren

Die Diskussion über die Sicherheit von Verschlüsselungsverfahren beschränkt sich allzuoft auf die mathematischen Algorithmen. Die konkrete Einbettung der Verschlüsselungsverfahren in das technische System oder ein angemessenes Schlüssel-Management sind aber zumindest ebenso wichtig. Das fängt an bei den Zufallszahlengeneratoren und hört auf bei der Frage nach der benötigten Verschlüsselungsgeschwindigkeit. Neben der Güte eines Algorithmus sind dies entscheidende Punkte, die über die Wirksamkeit einer Verschlüsselung entscheiden.

Wenn im Datenschutz hohe Sicherheit gewollt wird, kann man diese nach Meinung von Experten erreichen durch

- Einsatz des DES bzw. Triple-DES,
- Zertifizierung des Produkts durch das BSI bezüglich der anderen Sicherheitsaspekte und
- ein eigenes Schlüsselmanagement.

27.1.2
DES (vgl. 22. Tätigkeitsbericht, Ziff. 21.1.3.1.1)

Ende der 70er Jahre wurde der DES (Data Encryption Standard) für den nicht-VS-Bereich publiziert. Dabei handelt es sich um einen symmetrischen Verschlüsselungsalgorithmus. Er litt unter dem Makel, daß die NSA (National Security Agency) in die Entwicklung involviert war. So wurde aus dem ursprünglichen 64 Bit Schlüssel ein 56 Bit Schlüssel. Es wurde die Vermutung geäußert, damit sei es staatlichen Stellen möglich, das Verfahren zu brechen. Die öffentliche Debatte hat in den folgenden Jahren aber die Güte des Verfahrens bestätigt. Abgesehen von der Tatsache, daß die Schlüssellänge mit 56 Bit außerordentlich klein ist, handelt es sich um ein sehr gutes Chiffrierverfahren.

Die Schlüssellänge von 56 Bit ist ein wichtiges Kriterium. Sie ist in vielen Bereichen nicht ausreichend, weil Hardware vorstellbar ist, die in absehbarer Zeit alle Schlüssel durchprobieren kann. Das Problem stellt sich insbesondere, wenn Informationen verschlüsselt werden, die über Jahre gegen unberechtigte Zugriffe geschützt sein müssen. In diesen Fällen ist das original DES-Verfahren nach Meinung von Experten obsolet. Es kann Anwendungen geben, bei denen es nicht vorstellbar ist, daß ein Angreifer den Aufwand treibt und deshalb der DES eingesetzt werden kann.

Aufgrund des Einwandes der geringen Schlüssellänge wird der DES in den letzten Jahren oft nicht in der Originalform, sondern als Triple-DES mit einer Schlüssellänge von 112 Bit angeboten. Nach den heutigen Erkenntnissen entzieht sich der Triple-DES dem Angriff durch Ausprobieren aller denkbaren Schlüssel. Der Einsatz des Triple-DES wird als nicht sicherheitskritisch angesehen, soweit die anderen Rahmenbedingungen wie adäquate Schlüsselverwaltung u.ä. gewährleistet sind.

27.1.3
RSA (vgl. 22. Tätigkeitsbericht, Ziff. 21.1.3.1.2)

Seit Ende der 70er Jahre wurden mehrere Public-Key-Verfahren vorgeschlagen. Es hat sich der RSA-Algorithmus (benannt nach den Forschern Rivest, Shamir und Adleman) durchgesetzt, der vor allem für Schlüsselaustauschverfahren eingesetzt wird. Ende der 70er Jahre wurde ein 512-Bit RSA als sicher angesehen. Auch heute ist im allgemeinen niemand in der Lage, ein 512-Bit RSA zu brechen. Die Entwicklung läßt dies aber in einigen Jahren möglich erscheinen. Deshalb ist in der Tendenz eine größere Modullänge zu fordern. Der Vorteil des RSA-Verfahrens ist dabei, daß die Modullänge beliebig aufgebläht werden kann. So ist ein 1024 Bit RSA bei sorgfältiger Wahl der Parameter, mit heutigen Methoden, nicht zu knacken.

27.1.4
Neue Entwicklungen

- IDEA
  IDEA ist ein Blockchiffrieralgorithmus, der vor fünf Jahren als Ersatz für den DES entwickelt wurde. Die Schlüssellänge beträgt 128 Bit. Es sind bisher keine erfolgreichen Attacken bekannt.

- Skipjack
  Skipjack ist ein Blockchiffrieralgorithmus, der im Clipperchip (s.u.) implementiert ist. Die Schlüssellänge beträgt 80 Bit. Die Autorenschaft liegt beim NSA. Er ist nicht publiziert.

- DSS (Digital Signatur Standard; neuer amerikanischer Standard) Er eignet sich für digitale Signaturen, aber nicht zum Verschlüsseln.

- SHA (Secure Hashing Algorithem; neuer amerikanischer Standard) Hashfunktionen sind ein kryptografischer Baustein, der in praktisch allen Kryptosystemen gebraucht wird.

- PGP
  PGP (Pretty Good Privacy) ist ein mit allen Quelltexten veröffentlichtes Verschlüsselungsverfahren. Es nutzt das RSA-Verfahren, wobei beliebige Schlüssellängen gewählt werden können, und das IDEA-Blockchiffrierverfahren. Die Sitzungsschlüssel werden mit RSA verschlüsselt, die Daten mit IDEA. PGP ist für elektronische Unterschriften und für e-mail geeignet. Es sollte nicht auf UNIX-Rechnern im Multi-User-Betrieb benutzt werden, da der Superuser die verschlüsselt gespeicherten Paßwörter ausspähen könnte.

  Das Schlüsselmanagment von PGP ist dezentral. Ein Teilnehmer erzeugt zuerst ein Schlüsselpaar. Dann wird per e-mail oder Diskette der öffentliche Schlüssel versandt. Zur Authentisierung werden kryptografische Checksummen erzeugt, die parallel zur Schlüsselverteilung per Telefon ausgetauscht werden können.

- MIC
  Der Algorithmus MIC wurde vom BSI entworfen. Die Schlüssellänge ist 120 Bit. Es ist eine Verschlüsselungsroutine, die unter MS-DOS zur lokalen Verschlüsselung von Dateien nach Maßgabe eines über Tastatur eingegebenen Schlüssels vorgesehen ist. E-mail Dateien können verschlüsselt werden.

  Das Problem der Schlüsselverteilung besteht weiterhin, da kein asymmetrisches Schlüsselverteilverfahren vorgesehen ist.

27.2
Offenlegung von Verschlüsselungsverfahren

Es gibt zwei konträre Auffassungen zu der Frage, ob Verschlüsselungsalgorithmen in einer (Fach-)Öffentlichkeit diskutiert werden sollen.

Nach der einen Auffassung sollte ein Verschlüsselungsverfahren nicht in einer (Fach-)Öffentlichkeit diskutiert werden, da ein geheimes Verfahren für potentielle Angreifer eine sehr hohe Hürde darstellt.

- Ein gutes geheimes Verfahren kann kaum analysiert werden.
- Zur Kenntnis gelangte geheime Schlüssel führen nicht automatisch zur Entschlüsselung.
- Designkriterien der Entwickler werden nicht bekannt.

Diese Auffassung wird insbesondere für Bereiche wie den staatlichen Geheimschutz vertreten. Unabhängig vom Einsatzbereich wird ausgesagt, daß ein hardwaregetragenes, geheimgehaltenes Verfahren eine höhere Sicherheit bietet als ein publiziertes Verfahren.

Demgegenüber steht die Meinung, daß für Bereiche, die nicht besonderen Rahmenbedingungen unterliegen – hier wären als Beispiele der staatliche Geheimschutz oder eine Verschlüsselung in Kommunikationsnetzen mit hohen Geschwindigkeiten zu nennen – nur offengelegte Verfahren einzusetzen sind.

- Die Geheimhaltung bringt keine zusätzliche Sicherheit im Vergleich zu einem publizierten Verfahren, das von einer (Fach-)Öffentlichkeit für sicher erachtet wird.
- Die Geheimhaltung führt zu einem Mißtrauen gegenüber dem Verfahren, da Hintertüren befürchtet werden.
- Wenn die weite Verbreitung eines Verfahrens gewünscht und – gezwungenermaßen – eine softwaretechnische Implementation vorgenommen wird, ist eine Geheimhaltung kaum aufrecht zu halten.

In der Konsequenz halte ich es unter Beachtung der jeweiligen Rahmenbedingungen für sinnvoll, den normalen Benutzern ein Verfahren zu geben, das öffentlich dokumentiert wird und seine Sicherheit nicht aus der Geheimhaltung bezieht, sondern aus der Tatsache, daß eine (Fach-)Öffentlichkeit keine Einwände hat.

27.3
Neue Entwicklungen in der elektronischen Kommunikation (vgl. 22. Tätigkeitsbericht, Ziff. 21.1.3.1.3)

27.3.1
Überwachung elektronischer Kommunikation

In Deutschland und den meisten Staaten mit vergleichbarem Rechtssystem gibt es die Möglichkeit, das Fernmeldegeheimnis unter bestimmten gesetzlichen Voraussetzungen zu durchbrechen. Diese Möglichkeit wird allgemein nicht in Frage gestellt.

Beim Vorliegen einer elektronischen Kommunikation stellen sich neue Fragen:

- Was geschieht, wenn bei Vorliegen sämtlicher rechtlicher Voraussetzungen die Stelle, welche die Überwachung vornehmen soll, mit einem Chiffrat konfrontiert wird? Soll dies hingenommen oder nach Möglichkeiten gesucht werden, damit umzugehen?
- Was ist, wenn ein gesellschaftliches Interesse an der Strafverfolgung besteht? Gibt es Möglichkeiten den Einsatz derartiger Verfahren zu reglementieren oder so zu gestalten, daß unter wohldefinierten Voraussetzungen eine Entschlüsselung möglich wird?

Die Debatte ist einige Jahre alt. Mit der Ankündigung des Clipper-Standards vor ca. zwei Jahren in den USA hat sie an Intensität zugenommen.

27.3.1.1
Situation in den USA

In den USA gibt es die "Clipper-Initiative" als Teil des "Key-ESCROW"- Programms (Escrowing: treuhänderische Hinterlegung von Chiffrierschlüsseln). Clipper ist das Angebot eines Chiffriersystems an jedermann, das eine sichere Kommunikation erlaubt, aber unter gewissen Voraussetzungen einen Zugriff auf die Daten durch staatliche Stellen möglich macht. Niemand ist verpflichtet, Clipper einzusetzen, es soll aber im staatlichen Bereich (der USA) genutzt werden. Man hofft dort, daß es in andere Bereiche diffundiert und zum Quasistandard wird.

Es werden bei zwei Institutionen treuhänderisch Schlüssel hinterlegt. Die Kenntnis der beiden Schlüssel erlaubt es, ein Chiffrat zu entschlüsseln. Es gibt zu jedem Clipper-Chip einen Schlüssel, der im sog. "Law-Enforcement-Access-Field" im Datenstrom verschlüsselt mitübertragen wird. Der legale Abhörer entschlüsselt mit den Angaben der ESCROW-Agencies das Feld und erhält den Session-Key.

Dabei stellen sich die folgenden Fragen:

- Wer hat unter welchen Voraussetzungen Zugang zu den Schlüsseln?
- Was geschieht, wenn einmal ein Schlüssel offenbart wurde?

Der Stand der Diskussion in den USA ist, soweit bekannt:

- Es gibt enorme Akzeptanzprobleme.
- Da es sich um ein nicht publiziertes, vom NSA erstelltes Verfahren handelt, werden weitere Eingriffsmöglichkeiten befürchtet.
- Die Idee, daß der Staat die Mittel zur Sicherung privater Kommunikation bereitstellt, wird kritisiert.

Um den Einfluß des Staates zu verringern, wurden Änderungen vorgeschlagen. Hier sind die sog. "fairen Systeme" zu nennen. Im Grundsatz wird zugestimmt, daß Überwachungen nötig sein können und daß es Institutionen ähnlich den ESCROW-Agencies geben muß. Den Institutionen wird jedoch nicht die gesamte Kontrolle überlassen. Insbesondere sollen sie oder ein anderer Dritter nicht mit der Erzeugung der Schlüssel betraut werden.

Der Vorschlag sieht vor, daß die Benutzer des Systems ihre Schlüssel nach bestimmten, festgelegten Standards selbst erzeugen. Dies wird Kontrollinstanzen mittels spezieller Protokolle, sog. Zero-Knowledge-Protokolle, mitgeteilt.

Es setzt ein "Secret-Sharing-System" ein. Die Schlüssel werden in mehrere Teile aufgeteilt. Jeder Teil wird einer ESCROW-Agency mitgeteilt. Jetzt könnte vereinbart werden, bei einer Maßnahme den Schlüssel herauszugeben, wenn mehrere Stellen die Anforderung erhalten.

Ohne Kontrolle könnten die ausgegebenen Teilschlüssel zu einem nicht existierenden Schlüssel gehören. Das vorgeschlagene Protokoll sieht vor, daß die Empfänger beweisen können, daß sie Teile des legitimen Schlüssels erhalten haben. Damit ist dem Interesse aller gedient, denn zunächst hat niemand außer dem Erzeuger den Schlüssel gekannt. Mit den "fairen Systemen" existiert ein Kompromiß zu den ESCROW-Agencies.

Es sind auch alternative Protokolle entwickelt worden, die den Einwand entkräften, durch einmal durchgeführte Abhörmaßnahmen seien die Schlüssel für die Zukunft bekannt. Nach diesen Protokollen ist ein Schlüssel nur drei Monate gültig, danach wäre eine neue Abhörgenehmigung erforderlich. Das gilt nicht für Clipper in der jetzigen Form, da der Schlüssel nicht geändert wird.

27.3.1.2
Situation in Deutschland

Es ist in Deutschland derzeit nicht geplant, ein System wie Clipper einzuführen. Die Debatte bezüglich der Aufrechterhaltung von Überwachungsmöglichkeiten im Zeitalter fortschreitender Verschlüsselungsmöglichkeiten ist in der Schwebe. Es gibt keine konkreten Gesetzesvorhaben, sondern nur Überlegungen im Bereich des Bundesminsteriums des Innern.

27.3.1.3
Situation in Frankreich

Einige Länder, wie Frankreich, haben einen anderen Zugang gewählt. Der Einsatz der Kryptografie ist per Gesetz unter einen Genehmigungsvorbehalt gestellt. Dabei wird unter Ansehen der Person und des Systems entschieden.

27.3.1.4
Weitere Ansätze (vgl. 22. Tätigkeitsbericht, Ziff. 21.1.3.1.4)

Ein weiterer Ansatz, der von einigen Institutionen in Deutschland favorisiert wird, ist eine Schlüsselversorgung durch vertrauenswürdige Dritte (Trusted Third Parties) in Trust Centern. Dies ist der Sache nach, ähnlich der Clipper-Initiative, eine treuhänderische Verwaltung der Schlüssel durch Dritte. Man hat begleitende Regularien, unter welchen rechtlichen Voraussetzungen auf die Geheimnisse zugegriffen werden kann. Es gibt in Deutschland zur Zeit keine Rechtsgrundlage, diesen Ansatz zu realisieren. Es wäre aufgrund der TDSV/UDSV sogar verboten, die Schlüssel zu speichern, da sie zur Erbringung einer Leistung nicht erforderlich sind.

Es bedarf gesetzlicher Regelungen zur Umsetzung der erforderlichen G10-Maßnahmen, was noch nicht geschehen ist. Wenn die Regelungen vorhanden sind, kann eine Umsetzung versucht werden. Danach würde den Überwachungsbehörden, wenn die rechtlichen Voraussetzungen gegeben sind, eine Chipkarte zur Verfügung gestellt. Auf dieser Chipkarte befände sich der geheime Schlüssel der überwachten Person. Der Prozeß wäre durch die Herausgabe einer Chipkarte gut nachvollziehbar und kontrollierbar. Es wäre gewährleistet, daß

- der Schlüssel nicht beliebig kopiert werden kann und
- nicht beliebig vielen Dienststellen unkontrolliert zur Verfügung steht.
- Es ist nachweisbar, wenn der Schlüssel übergeben wurde, und
- es könnte konfiguriert werden, wie oft er benutzt werden darf.

27.3.2
Neue Mechanismen (Ergänzung zum 22. Tätigkeitsbericht, Ziff. 21.1.3 bzw. 21.1.3.2)

- Failstop
  Failstop-Signaturen liegt die Annahme zugrunde, daß es gelingt, die Signatur einer Person zu knacken. Im Failstop-Verfahren ist es möglich zu beweisen, daß eine Fälschung vorliegt. Die Funktionsweise läßt sich grob so darstellen, daß zu einem Public-Key sehr viele geheime Schlüssel passen, aber nur einer ist der geheime Schlüssel der Person. Dabei ist es möglich, die Wahrscheinlichkeit dafür einzustellen, daß ein Fälscher genau diesen trifft.
- elektronische Signaturen (vgl. 22. Tätigkeitsbericht, Ziff. 21.1.3.2)
  Es gibt Planungen innerhalb der Bundesregierung, ob man eine gesetzliche Regelung vorsehen könnte oder sollte, die letztlich die elektronische Signatur in Teilbereichen der eigenhändigen Unterschrift gleichstellt.

Der Diskussionsstand stellt sich wie folgt dar:

Die Idee, die diskutiert wird, geht dahin, die zivilrechtlichen Formvorschriften zu ändern. Teilweise wird die Auffassung vertreten, daß in den Fällen, in denen das Gesetz als Voraussetzung der Rechtsgültigkeit einer Willenserklärung die eigenhändige Unterschrift vorsieht, nunmehr auch digitale Signaturen anerkannt werden. Ein offenes Problem ist, welchen Beweiswert ein digital signiertes Dokument vor Gericht haben wird. Solange Beweisvorschriften nicht geändert werden, ist es ein Augenscheinsobjekt, das jedes Gericht frei würdigen kann. Das Gericht ist allerdings nicht gezwungen, bestimmte Folgerungen, wie bei einer eigenhändigen Unterschrift, zu ziehen. Danach würde zur Zeit kein zwingender Grund bestehen, Beweisvorschriften zu ändern. Die Befürworter von Änderungen argumentieren, digitale Signaturverfahren machten nur Sinn, wenn sie so sicher seien, daß es in Streitfällen zu schnellen gerichtlichen Verfahren käme. Deswegen müßten die Formvorschriften im Bürgerlichen Gesetzbuch sowie die Beweisvorschriften in der Zivilprozeßordnung geändert werden.

Es ist unklar, welche konkreten Anforderungen das jeweilige Verfahren erfüllen muß (mathematisches Signaturverfahren, Implementierung, allgemeine Organisation der Trust Center, rechtliche Organisation der Trust Center usw.), damit ein Richter davon ausgehen kann, daß ein digital signiertes Dokument authentisch ist.

27.3.3
Ausblick auf soziale und politische Implikationen von Sicherungsinfrastrukturen

Betrachtet man die Entwicklung der elektronischen Kommunikation, so drängt es sich auf, soziale und politische Implikationen von Sicherungsinfrastrukturen zu untersuchen. Im Rahmen eines Projekts beschäftigt sich die "Projektgruppe für verfassungsverträgliche Technikgestaltung" (provet) mit dieser Fragestellung. Die Ergebnisse des Projekts werden in Kürze veröffentlicht.

An dieser Stelle sollen die Inhalte nur sehr knapp angedeutet werden.

Unter dem Begriff "Sicherungsinfrastruktur" sind technische Systeme öffentlicher Schlüsselverfahren, Betreiber und Regeln für die jeweilige Zusammenarbeit zu verstehen. Ausgehend von der Annahme, daß die Bedeutung der Telekooperation zunehmen wird, ergibt sich als eine Voraussetzung ein vertrauenswürdiges Schlüsselverfahren. Dabei sind verschiedene Aspekte zu beachten und noch zu klären:

- Mathematische Verfahren
  Es müssen die anzuwendenden Algorithmen – beispielsweise kämen DES und RSA in Frage – festgelegt werden.
- Implementierung
  Die Anwendungen müssen so eingebunden werden, daß Manipulationen ausgeschlossen sind.
- Fragen der Organisation
  Es ist offen, welche Voraussetzungen ein Trust Center erfüllen muß, um vertrauenswürdig zu sein. Dazu gehören die erforderlichen Sicherungsfunktionen oder die Organisation. Unklar ist, welche Funktionen privat oder öffentlich sein müssen bzw. sollen und wie eine Aufsicht aussehen kann.
- Rechtliche Aspekte
  Unter den rechtlichen Fragestellungen ist besonders wichtig, wie es rechtsstaatlich gewährleistet werden kann, daß ein Handeln sicher zurechenbar ist. Weitere Probleme betreffen Haftungsregelungen und Anforderungen an die Gestaltung der Rechtsordnung, damit die Trust Center wirklich vertrauenswürdig sind.

27.3.4
Problem der Offenlegung geheimer Schlüssel

Wenn eine verschlüsselte Kommunikation überwacht wird, müssen geheime Schlüssel bekanntgegeben werden, die unter Umständen auch zu elektronischen Signaturen dienen könnten.

Um dies auszuschließen, wird es für erforderlich erachtet, in weiteren Gesetzgebungsverfahren ausdrücklich festzulegen, daß die geheimen Schlüssel für digitale Signaturverfahren nicht gespeichert werden dürfen. Es darf nur ein Unikat geben.

In dem hier unter 27.3.1.4 dargestellten Ansatz werden in einem Trust Center Schlüssel erzeugt und auf einer Chipkarte gespeichert. Die Schlüssel für die digitale Signatur und für die elektronische Kommunikationsverschlüsselung sind unterschiedlich. Der geheime Anteil des Signaturschlüssels wird sofort vernichtet und ist nicht rekonstruierbar. Er liegt nur in der persönlichen Chipkarte vor und ist Dritten nicht zugänglich.

Aus Kenntnis der Problematik wurde bei den amerikanischen Standards für die digitale Signatur der DSS gewählt, der sich nur für die elektronische Signatur eignet.

27.4
Probleme aus der Nutzung von Verschlüsselungsverfahren

In den bisherigen Schilderungen wurde davon ausgegangen, daß die Kommunikation über ein öffentliches Netz erfolgt, so daß das G10-Gesetz Anwendung findet. Es ist aber möglich, mit Disketten Daten auszutauschen, die z. B. mit dem DES bzw Triple-DES verschlüsselt sind. Das G10-Gesetz ist darauf nicht anwendbar.

Beispielsweise könnten Strafverfolgungsbehörden Kommunikationsteilnehmern, die per Diskette verschlüsselt Daten ausgetauscht haben, eine Straftat vorwerfen. Sie würden befragt, ob sie Daten ausgetauscht hätten. Diese würden bestätigen, mit DES verschlüsselt Daten ausgetauscht zu haben. Daraufhin würde die Herausgabe des Schlüssels verlangt, was mit dem Hinweis auf die Rolle als Verdächtige abgelehnt würde.

Es bliebe den Strafverfolgungsbehörden nur der Versuch, Dritte zu finden, die den Schlüssel kennen. In dieser Situation stellt sich für die Strafverfolgungsbehörden ein großes Problem. Nicht nur was die Kommunikation betrifft, sondern auch die Benutzung von PC und Laptops usw. Wo bisher noch Beweise in schriftlicher Form vorgelegen haben, gibt es künftig elektronische Dokumente, die eventuell verschlüsselt sind und im Strafverfahren nicht verwandt werden können. Es ist auch richtig, daß diese Entwicklung höchstwahrscheinlich nicht mehr aufzuhalten ist. Diese Frage wird zur Zeit im Bereich der Bundesregierung geprüft.

28. Viren in der Datenverarbeitung

Bereits in meinem 19. Tätigkeitsbericht, Ziff. 15.4 hatte ich mich mit dem Problem der Viren beschäftigt.

In der Zwischenzeit wurde ich immer wieder darauf hingewiesen, daß dieses Problem die öffentlichen Stellen in Hessen zunehmend beschäftigt. Ich habe diese Hinweise zum Anlaß genommen, in einem Rechenzentrum zu klären, ob die dort in der Vergangenheit angelieferten Disketten mit Viren verseucht waren. Das Ergebnis war eindeutig und alarmierend: Bei neun von dreizehn öffentlichen Stellen, die regelmäßig Daten zur weiteren Verarbeitung anlieferten, wurden Programmviren festgestellt.

Während in dem im 19. Tätigkeitsbericht geschilderten Fall vor vier Jahren die Verseuchung offensichtlich durch den Einsatz privater Software verursacht worden war, hat sich die Situation ("Viruslandschaft") zwischenzeitlich verändert. Zum einen ist die Erstellung bzw. Erzeugung neuer Viren durch Virenbaukästen vereinfacht worden und somit auch für Personen mit wenig Programmiererfahrung möglich, zum anderen ist die Hauptquelle der Computerviren nicht mehr die Raubkopie. Nach einer Analyse des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind primär folgende Quellen für die Verbreitung verantwortlich:

- Originalsoftware bevorzugt aus dem ostasiatischen Raum, Treibersoftware für Peripheriegeräte, Maus und Bildschirmgeräte
- Demo-Disketten
- vorinstallierte Geräte
- Wartungs- und Service-Personal.

Generell kann man sagen, daß ein Befall durch Computerviren jeden treffen kann und nur in ganz wenigen Fällen absolut unmöglich ist. Das BSI hat sich mit dem Problem beschäftigt und in seiner Schriftenreihe zur IT-Sicherheit einen Band "Computerviren" herausgegeben. Die nachstehenden Maßnahmen, die einem Virenbefall vorbeugen sollen, sind diesem Band entnommen:

- regelmäßig Datensicherung durchführen
- Sicherungskopien von Datenträgern sicher aufbewahren
- Schreibschutz bei allen Disketten setzen, auf die nicht geschrieben werden muß
- aktuelle Virenschutzsoftware verwenden
- alle neu erworbenen Programme und Datenträger vor Benutzung auf Viren überprüfen
- Notfall-Diskette erstellen
- Bootreihenfolge im CMOS-RAM auf "C:,A:" einstellen
- mehrere Partitionen im Rechner einrichten
- Computer und Datenträger vor unbefugter Benutzung schützen
- alle ausgehenden Disketten mit einem Virensuchprogramm überprüfen und mit Schreibschutz versehen
- Mitarbeiter über Computerviren schulen
- Verfahrensweise bei Verdacht des Virenbefalls klären.

Sinnvolle Maßnahmen, wie vorgegangen werden kann, wenn ein Virenbefall festgestellt wurde, können wiederum (laut BSI) sein:

- bei Verdacht auf Virusbefall die Arbeit wie gewohnt beenden
- Computer ausschalten
- unerfahrene Benutzer sollten einen Fachmann zu Rate ziehen
- von virenfreier, schreibgeschützter Systemdiskette booten (siehe Notfall-Diskette)
- mit aktuellem Virensuchprogramm die Festplatte untersuchen, dabei ein Protokoll erstellen
- bei Virusbefall: Virusmeldung an das BSI ausfüllen
- Virus von der Festplatte entfernen
- Computer ausschalten
- Rechner wie gewohnt über die Festplatte starten und erneut mit dem Virensuchprogramm die Festplatte überprüfen
- alle anderen Datenträger auf Virenbefall untersuchen und Viren entfernen
- versuchen, die Quelle der Vireninfektion festzustellen; wenn dies erfolgreich war, anschließend bei Programmdisketten das BSI und den Hersteller, bei Datendisketten den Hersteller der Diskette informieren
- andere Anwender warnen.

Wegen der großen Relevanz von Vertraulichkeit, Integrität und Verfügbarkeit auch und gerade für den Schutz personenbezogener Daten werde ich im Jahr 1995 Prüfungen durchführen, um festzustellen, wie in der behördlichen Praxis mit diesem Problem umgegangen wird.

29. Autobahnmaut

In letzter Zeit wird in Bund und Ländern im Zusammenhang mit politischen Zielen und Kriterien wie

- Verkehrslenkung
- gerechte Anlastung der Wegekosten
- private Finanzierungsmöglichkeiten
- Verbesserung der Infrastruktur Autobahn, Schienenverkehr
- Umweltschutz (Schadstoffemission, Rohstoffverbrauch)

über verschiedene Varianten von Benutzungsgebühren und Steuerveränderungen im Verkehrsbereich diskutiert.

Dabei geht es um die Alternativen

- zeitbezogene Autobahngebühr (Vignette)
- Mineralölsteuererhöhung
  und
- streckenbezogene Straßenbenutzungsgebühr

jeweils mit oder ohne Reduktion oder Streichung der Kraftfahrzeugsteuer.

Nach der politischen Auseinandersetzung über die Autobahnvignette hat sich der Schwerpunkt der öffentlichen Diskussion auf die strecken- und zeitbezogene Straßenbenutzungsgebühr (road-pricing) verlagert.

Dabei geht es darum, in Abhängigkeit von der zurückgelegten Wegstrecke eine bestimmte Gebühr zu erheben, deren Höhe zusätzlich von zeitlichen Parametern wie Wochentag, Tageszeit und Fahrtdauer (Fahren im Stau wird teurer) abhängen kann. Auch Wochen- und Monatskarten für bestimmte Strecken oder andere Pauschalsysteme sind denkbar. Die konkrete Ausgestaltung wird u.a. durch die politische Zielsetzung festgelegt.

Die technischen Möglichkeiten der automatischen Gebührenerhebung werden in verschiedenen Feldversuchen getestet. Während der Feldversuch des baden-württembergischen Verkehrsministeriums auf der B27 in Stuttgart u.a. klären soll, ob man im Innenstadtbereich Autofahrer durch eine Straßengebühr beeinflussen kann, verstärkt auf den öffentlichen Nahverkehr umzusteigen, geht es bei dem Feldversuch auf der A555 zwischen Bonn und Köln um die Erhebung einer streckenbezogenen Autobahngebühr, ohne daß die Fahrzeuge an der Mautstelle die Geschwindigkeit stark reduzieren müssen oder gar angehalten werden.

29.1
Feldversuch auf der A555

29.1.1
Gebührenerhebung

Die Systeme, die am Feldversuch auf der A555 teilnehmen, verwenden unterschiedliche Übertragungseinrichtungen für die Kommunikation und unterschiedliche Verfahren zur Erhebung der Gebühren.

Die Kommunikation zwischen Fahrzeug und Systeminfrastruktur kann entweder über eigens hierfür zu installierende Funkeinrichtungen an Schilderbrücken über oder Baken neben der Autobahn erfolgen, oder sie kann das vorhandene D-Funknetz (Mobilfunk, GSM) oder ein ebenfalls vorhandenes Satelliten-Navigationssystem (GPS) benutzen. Auch für die Technik, die als Bordsystem im Fahrzeug zur Gebührenerhebung installiert wird, gibt es verschiedene Möglichkeiten: Sie kann einen Code als Fahrzeugkennung senden, mit dem der Betreiber – eventuell monatlich zusammengefaßt – die berechnete Gebühr später im sogenannten Postpaid-Verfahren von einem Gebührenkonto des Halters abbucht, oder im Fahrzeuggerät steckt eine vorbezahlte Chipkarte, ähnlich wie die Telefonkarte, die wieder aufgeladen werden kann (Prepaid-Verfahren). Von dieser bucht der Betreiber über einen entsprechenden Impuls beim Vorbeifahren an der Mautstelle die Gebühr ab, dem Fahrer werden der abgebuchte Betrag und das Restguthaben angezeigt. Oder im Fahrzeug steckt sogar ein Rechner mit Chipkarte, der selbst aufgrund eines Signals von der Mautstelle oder über Satelliten-Ortung die anfallende Gebühr ausrechnet, anzeigt und in der Regel von der vorbezahlten Chipkarte, evtl. aber auch von einem Konto, abbucht.

Es ist offensichtlich, daß schon in der Phase der Gebührenerhebung die politischen Ziele des Staates in ein Spannungsverhältnis zu den Freiheitsrechten der Bürger treten, falls registriert wird, wer wann welche Strecke befahren hat. Bei den sog. geschlossenen Systemen werden eine Fahrzeugkennung sowie Ort und Zeitpunkt der Auffahrt auf die Autobahn mindestens bis zum Zeitpunkt der Abfahrt gespeichert, dann wird die Gebühr berechnet und abgebucht. Damit sind jeweils alle Fahrzeuge, die gerade auf der Autobahn fahren, registriert. Bei den sog. offenen Systemen wird das Vorbeifahren an bestimmten Maut-Stellen mit einer Gebühr belegt; dies geschieht ohne Registrierung von Zu- und Abfahrt und kann bei direkter Abbuchung von einer Prepaid-Chipkarte im Fahrzeug vollständig anonym erfolgen.

Umgekehrt ergibt sich aber spätestens, wenn die erhobenen Gebühren (z. B. im Fahrzeuggerät) protokolliert werden, die Frage, ob die Gebühren fahrzeughalter- oder fahrerbezogen erhoben werden und wie die Vertraulichkeit im Innenverhältnis Fahrzeughalter-Fahrzeugbenutzer gewährleistet werden kann.

29.1.2
Kontrolle

Um Umgehung oder Manipulation der Gebührenerfassung festzustellen und gegebenenfalls auch im Nachhinein beweisen zu können, sind Kontrollverfahren erforderlich: Der Betreiber möchte die Nicht- oder Falschzahler zur Kasse bitten. Hierfür müssen Daten wie Fahrzeugkennzeichen, Fahrzeugklasse, Ort und Zeit erfaßt werden. Dies soll technisch beispielsweise mittels fotografischer oder opto-elektronischer Verfahren geschehen. Umgekehrt möchte der Autobahnbenutzer die Gewähr bekommen, daß ihm nicht zu hohe Gebühren abgebucht werden und gegebenenfalls reklamieren können.

Es dürfte schwierig sein, ein Kontrollverfahren zu entwickeln, das einerseits hinreichend beweissicher ist und andererseits den Anforderungen des Datenschutzes genügt.

Zunächst stellt sich das Problem, nur die Nicht- oder Falschzahler, nicht aber auch die Richtigzahler zu erfassen. Hierzu wäre evtl. eine Kommunikation zwischen Fahrzeug und Betreiber/Erhebungsstelle in beiden Richtungen erforderlich. Weiter ist zu klären, ob die Kontrollstellen ortsfest installiert werden, ob zeitlich eine Voll- oder eine Stichprobenerfassung vorgenommen wird usw.

Zu befürchten ist, daß im Rahmen derartiger Verfahren erhobene personenbezogene Daten zur Erstellung von Bewegungsprofilen einzelner oder beliebig vieler Bürger oder zur Fahrtroutenverfolgung genutzt werden könnten.

Deshalb werden Systeme, die eine generelle Videoüberwachung des fließenden Verkehrs voraussetzen, abgelehnt, weil sie sich bei nur geringen Modifikationen auf eine Vollkontrolle umstellen lassen.

29.2
Datenschutzrechtliche Anforderungen

Im Arbeitskreis "Technische und organisatorische Datenschutzfragen" der Konferenz der Datenschutzbeauftragten des Bundes und der Länder sind die Informatiker und Techniker dieser Dienststellen vertreten. Er hat die Aufgabe, die Konferenz zu Fragen aus diesem Bereich fachlich zu beraten und Entscheidungen vorzubereiten.

Dieser Arbeitskreis hat die folgenden datenschutzrechtlichen Anforderungen an automatisierte Verfahren zur Erhebung von Straßenbenutzungsgebühren (road-pricing-Systeme) formuliert:

"1. Anonymität

Der Grundsatz der "datenfreien Fahrt" muß auch künftig gewährleistet sein. Je weniger personenbezogene oder personenbeziehbare Daten erhoben, verarbeitet oder genutzt werden, desto geringer ist auch die Gefahr einer mißbräuchlichen Datennutzung. Aus diesem Grund ist das Anonymitätskriterium die wichtigste Datenschutzanforde-

rung. Jedenfalls sollten bei regelgerechter Straßenbenutzung keine personenbezogenen Daten entstehen. Das bedeutet, daß auch keine Angaben erhoben oder verarbeitet werden, die im nachhinein die Herstellung des Personenbezugs ermöglichen.

Grundsätzlich bieten Verfahren, bei denen Gebühren im voraus entrichtet werden (Prepaid-Verfahren) bessere Voraussetzungen für die Wahrung der Anonymität als solche Systeme, bei denen zunächst Verkehrsdaten erhoben und dann den Benutzern in Rechnung gestellt bzw. von deren Konten abgebucht werden (Postpaid-Verfahren).

Soweit die Speicherung von Benutzerdaten gleichwohl erforderlich ist (z.B. für den Nachweis der Richtigkeit der Gebührenerhebung), sollten diese Daten dezentral beim Benutzer gespeichert werden. Die Erhebung von Benutzerdaten im Regelbetrieb durch "Erhebungsstellen" und deren Übermittlung an Konzentratoren oder zentrale Abrechnungseinheiten sollte unterbleiben.

Die Überwachung der Gebührenerhebung sollte so gestaltet werden, daß die Identität des Benutzers nur dann aufgedeckt wird, wenn ein begründeter Mißbrauchsverdacht besteht. Die Überwachung, ob ein Mißbrauch vorliegt, sollte grundsätzlich nur stichprobenweise und nicht vollständig erfolgen, da Systeme mit flächendeckender Mißbrauchskontrolle eine Infrastruktur voraussetzen, die für eine vollständige Erfassung auch der regelgerechten Straßenbenutzung "zweckentfremdet" werden könnte. Dabei sollte die Kontrolldichte so gering wie möglich sein und könnte sich an der bisherigen Kontrollpraxis bezüglich der Einhaltung von Geschwindigkeitsbegrenzungen orientieren.

2. Vertraulichkeit

Sofern personenbezogene Daten erhoben werden, müssen sie vertraulich behandelt werden. Die unbefugte Kenntnisnahme durch Dritte ist durch technische und organisatorische Maßnahmen auszuschließen. Insbesondere ist folgendes zu gewährleisten:

- Alle Komponenten, die sicherheitsrelevante Informationen austauschen, müssen sich partnerweise gegenseitig authentifizieren.
- Die Identität eines Straßenbenutzers sollte nur bei Mißbrauchsverdacht und nur vom Systembetreiber aufgedeckt werden können.
- Daten, die Aufschluß über die Identität oder den Aufenthaltsort des Benutzers geben, sind durch kryptographische Verfahren gegen eine unbefugte Kenntnisnahme zu sichern.
- Bei dezentraler Datenspeicherung (z. B. auf einer Chipkarte) darf der Zugang nur nach Eingabe eines benutzerspezifischen Codes möglich sein.
- Soweit personenbezogene Daten bei vermutetem Mißbrauch zentral gespeichert werden, ist zu gewährleisten, daß die Daten von anderen vom Systembetreiber verarbeiteten Daten strikt abgeschottet werden und nach Rechnungsbegleichung, bzw. wenn ein Mißbrauch nicht nachgewiesen werden kann, unverzüglich gelöscht werden.
- Die Vertraulichkeit im Verhältnis Fahrzeughalter – Fahrzeugbenutzer muß gewahrt werden (benutzer- statt fahrzeuggebundene Erhebung).

3. Integrität

Es ist zu gewährleisten, daß die richtigen Daten jeweils den richtigen Benutzern zugeordnet werden und keine Über-, Unter- oder Doppelerfassung erfolgt. Der Abbuchungsimpuls darf nicht derart streuen, daß er etwa – z.B. beim Spurwechsel – andere Fahrzeuge erfaßt. Auch bei der Fahrzeug- bzw. Benutzeridentifizierung (z.B. durch Kennzeichenerfassung) im Falle vermuteten Mißbrauchs ist die Zuordnung zu den richtigen Fahrzeugen sicherzustellen.

Alle sicherheitsrelevanten Informationen sind mit geeigneten Verfahren gegen Manipulationen zu schützen.

4. Transparenz

Das gesamte Verfahren muß für die Teilnehmer durchschaubar sein, d.h. die Benutzer müssen die realistische Chance haben, sowohl über den generellen Ablauf als auch über die Datenerhebung und -speicherung im Einzelfall Bescheid zu wissen:

- Bei dezentraler Speicherung sollte der Benutzer nachvollziehen können, welche Entgelte wann wo abgebucht wurden.
- Das System sollte den Benutzer rechtzeitig darauf hinweisen, wenn das Guthaben erschöpft oder für die Abbuchung der Maut zu gering ist.
- Sofern im Rahmen von Überwachungsmaßnahmen eine Aufdeckung der ansonsten geheimen Fahrzeugidentität erfolgt, muß dies für den Fahrzeugbenutzer erkennbar sein.
- Abbuchungen, Funktionsstörungen und Manipulationsversuche müssen dem Benutzer angezeigt werden und sind dezentral (z.B. auf der Chipkarte) revisionssicher zu protokollieren. Über Zusatzeinrichtungen, etwa bei Tankstellen, sollte der Benutzer die Möglichkeit haben, den Speicherinhalt der Protokolldatei auszudrucken und die Buchungsdatensätze anschließend zu löschen.

5. Stabilität gegen die Rücknahme von Datenschutzmaßnahmen

Die Systemkomponenten sind so zu gestalten, daß die Datenschutz- und Datensicherungsfunktionen stabil sind und nicht einseitig durch den Systembetreiber oder durch Dritte zurückgenommen oder unterlaufen werden können. Alle zum Einsatz kommenden Geräte müssen der Qualitätssicherungsnorm ISO 9001 genügen.

Systeme, die eine generelle Videoüberwachung des fließenden Verkehrs voraussetzen, werden abgelehnt, weil sie sich bei nur geringen Modifikationen auf eine Vollkontrolle umstellen lassen."

29.3
Präsentation des Feldversuchs

Für den Feldversuch auf der A555 wurde mit dem Bundesbeauftragten für den Datenschutz als Kontrollinstanz für das Bundesverkehrsministerium festgelegt, daß der Arbeitskreis Technik die dort getesteten technischen Lösungen dahingehend überprüfen und nach einheitlichen Maßstäben bewerten soll, inwieweit sie in all ihren technischen Details geeignet sind, die datenschutzrechtlichen Anforderungen zu erfüllen.

Im Mai 1994 wurden im Versuchszentrum "Eichkamp" vom Bundesverkehrsministerium und den mit der Durchführung des Feldversuchs beauftragten Unternehmen TÜV Rheinland und Heusch/Boesefeldt ein Grundsatzgespräch mit dem Arbeitskreis Technik geführt und die Ziele des Feldversuchs dargestellt. Anschließend wurden die im Fahrzeug eingesetzten Geräte vorgestellt, hiermit die Teststrecke abgefahren und zeitgleich dazu über die Notwendigkeit diskutiert, bereits im Rahmen der Erprobung der technischen Systeme datenschutzrechtliche Fragen zu erörtern. Dabei wurde deutlich, daß ein Dissens zwischen den Datenschutzbeauftragten und den Vertretern des Bundesverkehrsministeriums darüber bestand, ob und zu welchem Zeitpunkt die einzelnen Systeme hinsichtlich der Einhaltung datenschutzrechtlicher Grundsätze untersucht werden sollten.

Die Datenschutzbeauftragten sahen entgegen den Vorstellungen des Bundesverkehrsministeriums die Notwendigkeit, bereits während des Feldversuchs diese Prüfung vorzunehmen, damit die Firmen noch die Möglichkeit hätten, ihre Systeme datenschutzgerecht auszugestalten. Während des Gesprächs wurde deutlich, daß die Vertreter des Bundesverkehrsministeriums befürchteten, einzelne Firmen könnten durch die Beurteilung der Datenschutzbeauftragten entweder sich gehalten sehen, aus dem Feldversuch auszuscheiden, oder diese zum Anlaß nehmen, entgegen der vertraglichen Vereinbarung mit der – angeblichen – Datenschutzunbedenklichkeit für ihr System zu werben. Die Vertreter der Datenschutzbeauftragten machten deutlich, daß nicht beabsichtigt sei, ein "Datenschutzzertifikat" auszustellen; man wolle sich lediglich informieren und den Firmen evtl. Hinweise geben, welche Voraussetzungen aus datenschutzrechtlicher Sicht erforderlich seien.

Im Anschluß wurde vom TÜV Rheinland im Versuchszentrum Art und Umfang der Datenspeicherungen im Rahmen des Versuchs erläutert. Wegen der fortgeschrittenen Zeit war es nicht mehr möglich, die einzelnen am Versuch teilnehmenden Firmen aufzusuchen, so daß Informationen über die technischen Verfahren der einzelnen Systeme nicht eingeholt werden konnten. Dies wurde von den Vertretern der Datenschutzbeauftragten bedauert.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, daß bei dem Feldversuch auf der A 555 auch datenschutzrechtliche Erfordernisse berücksichtigt werden sollen. Sie sind bereit, Vorschläge für eine datenschutzgerechte Gestaltung der Technik, der Organisation und der rechtlichen Rahmenbedingungen einzubringen. Hierfür wollen sie zunächst den am Großversuch teilnehmenden Firmen in einem zweitägigen Workshop die Gelegenheit geben, ihre Systeme zu präsentieren. Auf Anregung des Bundesverkehrsministeriums wurde dieser Workshop auf einen späteren Termin im Januar 1995 verschoben.

29.4
Weiteres Vorgehen

Ich hoffe, daß bald fundierte Darstellungen des Feldversuchs mit Informationen über die technischen und organisatorischen Prozesse in den verschiedenen Phasen (Gebührenerhebung, Abbuchung, Kontrolle etc.) vorliegen. Auf dieser Basis und unter Verwendung der Ergebnisse des noch durchzuführenden Workshops könnten dann datenschutzrechtliche Analysen erfolgen mit dem Ziel, Vorschläge für eine datenschutzgerechte Systemgestaltung einzubringen.

Dabei erscheint es mir besonders wichtig, daß die Anforderungen des Datenschutzes bei der Modellbildung und bei der Festlegung der Systemarchitektur von Anfang an integriert werden. Nur so läßt sich rechtzeitig – ggf. unter Einbeziehung der am Feldversuch teilnehmenden Firmen – klären, ob und wie eine datenschutzfreundliche Technikgestaltung zur streckenbezogenen Straßenbenutzungsgebühr realisiert werden kann.

Für den Echteinsatz dürfen nur Verfahren mit geringstmöglichem Eingriff in das allgemeine Persönlichkeitsrecht, d.h. Systeme, bei denen möglichst wenig personenbezogene Daten erhoben werden, in Erwägung gezogen werden.

Solche Systeme müssen dann in einem notwendigen Abwägungsprozeß (Technikfolgenabschätzung) anderen Varianten von Benutzungsgebühren und Steuerveränderungen im Verkehrsbereich gegenübergestellt werden.

30. Bilanz

30.1
EU-Richtlinie zum Datenschutz (19. Tätigkeitsbericht, Ziff. 2; 20. Tätigkeitsbericht, Ziff. 16.3; 21. Tätigkeitsbericht, Ziff. 18.2)

Die Chancen, daß das Europäische Parlament und der Rat der Europäischen Union in absehbarer Zeit eine Richtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr erlassen, sind 1994 gestiegen.

Vor vier Jahren hatte die EG-Kommission, angestoßen von den Datenschutzinstitutionen der Mitgliedsländer, einen ersten Entwurf vorgelegt (KOM (90) 314 endg. – SYN 287; abgedruckt auch in BRDrucks. 690/90). Nachdem das Europäische Parlament 1992 über 100 Änderungsanträge zu diesem Entwurf beschlossen hatte (PE 160.503, Sitzungsprotokoll EP), präsentierte die Kommission im Oktober 1992 einen geänderten Vorschlag für eine Richtlinie des Rates (KOM (92) 422 endg. – SYN 287; gleichfalls abgedruckt in BTDrucks. 12/8329). Dort war noch von einer Richtlinie des Rates die Rede. Durch den am 1. November 1993 in Kraft getretenen Vertrag über die Europäische Union (Maastricht-Vertrag) kann jedoch der Rat die Richtlinie nur noch gemeinsam mit dem Parlament erlassen.

Zur Zeit ist der Rat der Europäischen Union dabei, seinen gemeinsamen Standpunkt zu dem geänderten Richtlinienvorschlag festzulegen. Unter deutschem Vorsitz bemüht sich gegenwärtig die Ratsarbeitsgruppe "Wirtschaftsfragen" (Datenschutz) darum, zu den noch offenen Streitpunkten einen Konsens der Mitgliedstaaten herbeizuführen.

Umstritten war und ist insbesondere die Frage des anwendbaren einzelstaatlichen Rechts bei grenzüberschreitender Datenverarbeitung. Die Arbeitsgruppe konnte sich noch nicht darüber einigen, ob für den Fall, daß ein Verantwortlicher der Verarbeitung (das deutsche Recht spricht nur von datenverarbeitender Stelle) eine Niederlassung in einem oder mehreren Mitgliedstaaten hat, das Recht des Staates, in dem der Verantwortliche seinen Sitz hat, oder das Recht des Staates, in dem sich die Niederlassung befindet, gelten soll. Offen ist weiterhin, wie sichergestellt werden kann, daß ein national höheres Schutzniveau von der Richtlinie unberührt bleibt und nicht an geringere Standards angepaßt werden muß. Die Möglichkeit zur Beibehaltung eines höheren Schutzniveaus ist besonders aus deutscher Sicht eine essentielle Forderung. Bei der Festlegung des Umfangs der Meldepflicht für Dateien scheint sich dagegen eine akzeptable Lösung abzuzeichnen. Hier muß eine Regelung verhindert werden, die in Deutschland zu zusätzlichen Melde- und Kontrollpflichten und damit zu einem zusätzlichen bürokratischen Aufwand führen würde, für den Datenschutz aber keine Verbesserung brächte. Eine zufriendenstellende Regelung scheint für die Absicherung des deutschen Kontrollsystems gefunden worden zu sein.

Hat der Rat seinen gemeinsamen Standpunkt festgelegt, sieht das weitere Verfahren folgendermaßen aus: Rat und Kommission müssen das Parlament über ihren jeweiligen Standpunkt unterrichten. Billigt das Europäische Parlament den gemeinsamen Standpunkt, setzt der Rat die Richtlinie in der Fassung des gemeinsamen Standpunktes in Kraft. Das Europäische Parlament könnte aber auch noch Änderungen verlangen. Es könnte sogar die Richtlinie ganz verhindern, was freilich nicht zu erwarten ist.

30.2
Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Landes Hessen (22. Tätigkeitsbericht, Ziff. 2)

In meinem letzten Tätigkeitsbericht (Ziff. 2) hatte ich den Entwurf des Hessischen Ministeriums des Innern für ein Sicherheitsüberprüfungsgesetz begrüßt. Ich hatte festgestellt, daß der Entwurf gegenüber dem Entwurf der Bundesregierung für ein Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes unter datenschutzrechtlichen Gesichtspunkten eine Reihe von Verbesserungen enthält. Das Bundesgesetz ist mittlerweile vom Bundestag verabschiedet worden und in Kraft getreten (BGBl. 1994 I, 867).

Leider wurde der hessische Entwurf im Berichtszeitraum nicht in das Gesetzgebungsverfahren eingebracht, so daß er in der laufenden Legislaturperiode nicht mehr verabschiedet werden kann. Ich halte eine gesetzliche Grundlage der Sicherheitsüberprüfung für dringend erforderlich und hoffe, daß sich der Gesetzgeber dieser Aufgabe in der nächsten Legislaturperiode annimmt.

30.3
Datenschutz bei den Staatsanwaltschaften (22. Tätigkeitsbericht, Ziff. 7.1)

Im letzten Tätigkeitsbericht hatte ich über meine Prüfungen bei verschiedenen Staatsanwaltschaften berichtet. Meine Empfehlungen wurden von den Staatsanwaltschaften größtenteils aufgegriffen und sollen möglichst bald umgesetzt werden.

Probleme gibt es allerdings weiterhin mit der Sicherung des Dienstgebäudes und der Diensträume einer der größeren Staatsanwaltschaften (vgl. 22. Tätigkeitsbericht, Ziff. 7.1.1). Eine Eingangskontrolle durch den Pförtner kann auf Grund von Stelleneinsparungen im Justizwachtmeisterdienst nicht vorgenommen werden. Auch der Einbau einer neuen Schließanlage scheitert an den Kosten. Hinzu kommt, daß sich der Leitende Oberstaatsanwalt dieser Behörde nicht in der Lage sieht, die Einhaltung einer praktikablen Hausverfügung, nach der die Dienstzimmer bei Abwesenheit zu verschließen sind, durchzusetzen.

30.4
Reform der Strafprozeßordnung (22. Tätigkeitsbericht, Ziff. 7.2)

Im letzten Tätigkeitsbericht hatte ich über den Arbeitsentwurf eines Strafverfahrensänderungsgesetzes (StVäG) 1993 berichtet, der von einer Unterarbeitsgruppe des Strafrechtsausschusses der Justizministerkonferenz erarbeitet worden war. Inzwischen hat der Bundesrat beschlossen, den nur unwesentlich veränderten Entwurf als Entwurf eines Strafverfahrensänderungsgesetzes 1994 in den Bundestag einzubringen. Die im Gesetzentwurf vorgesehenen Datenschutzregelungen bleiben weit hinter dem Standard zurück, den der hessische Gesetzgeber beispielsweise mit der Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung erreicht hat. Dies ist um so weniger verständlich,

als das Hessische Ministerium der Justiz den Vorsitz der Unterarbeitsgruppe hatte und somit wohl maßgeblichen Einfluß auf die inhaltliche Gestaltung des Entwurfs ausüben konnte.

30.5
Einsicht in Vereinsregisterakten (22. Tätigkeitsbericht, Ziff. 7.3)

Im vergangenen Jahr hatte ich von einem Fall berichtet, in dem beim Amtsgericht im Zusammenhang mit der Eintragung eines Vereins in das Vereinsregister ein umfangreicher Vorgang entstanden war. Er enthielt neben den vom Verein eingereichten Schriftstücken Stellungnahmen der Verwaltungsbehörde und der Industrie- und Handelskammer, einen unbeschränkten Auszug aus dem Bundeszentralregister über eines der Vorstandsmitglieder sowie ein unaufgefordert eingegangenes, denunzierendes Schriftstück des früheren Ehemannes eines Vorstandsmitglieds. Da sich das Einsichtsrecht in das Vereinsregister nach § 79 BGB nur auf die vom Verein eingereichten Unterlagen bezieht und bei den Gerichten, soweit ich dies feststellen konnte, keine organisatorischen Vorkehrungen getroffen sind, dies sicherzustellen, hatte ich das Hessische Ministerium der Justiz um eine Stellungnahme gebeten.

Es antwortete, daß eine organisatorische Vorkehrung zur Sicherung gegen unberechtigte Einsicht in Vereinsregisterakten bisher nicht bestehe. Ein vom Ministerium eingeleiteter Meinungsaustausch zwischen den Landesjustizverwaltungen im Jahre 1992 mit dem Ziel, bundeseinheitlich zu erreichen, daß zum Vereinsregister – wie bereits im Handels- und Genossenschaftsregister praktiziert – pro Registerblatt ein Sonderband geführt werden soll, sei am Widerstand der Mehrheit der Landesjustizverwaltungen gescheitert. Wegen der Bundeseinheitlichkeit der Aktenordnung sei bisher von einer isolierten Regelung des Sachverhalts für Hessen abgesehen worden.

Jetzt hat das Ministerium den geschilderten Fall zum Anlaß genommen, eine organisatorische Regelung zu schaffen, die den datenschutzrechtlichen Belangen der Betroffenen Rechnung trägt. Durch unveröffentlichten Runderlaß vom 18. März 1994 hat das Ministerium der Justiz angeordnet, daß ab sofort bei allen neuen Vereinsregisterangelegenheiten Sonderbände für bestimmte, dem Datenschutz unterliegende Schriftstücke angelegt werden. In bestehenden Vereinsregisterangelegenheiten bleibt die Anlegung von Sonderbänden im Hinblick auf den damit verbundenen Verwaltungsaufwand der jeweiligen Entscheidung der Behördenleitung überlassen. Auf die Einhaltung des Datenschutzes durch andere geeignete Maßnahmen (z. B. durch Herausnahme der fraglichen Schriftstücke vor Gewährung der Einsichtnahme) wurde in dem Erlaß besonders hingewiesen.

30.6
Arbeitsgruppe Korruptionsbekämpfung (22. Tätigkeitsbericht, Ziff. 20)

Die von der Landesregierung 1993 eingesetzte Arbeitsgruppe, die ein ressortübergreifendes Konzept für die Bekämpfung der Korruption in der Landesverwaltung entwickeln soll, hat im Herbst 1994 ein erstes Arbeitsergebnis vorgelegt. Der Entwurf eines gemeinsamen Runderlasses über den "Ausschluß von Bewerbern und Bietern wegen schwerer Verfehlungen, die ihre Zuverlässigkeit in Frage stellen", dem die Landesregierung am 4. Oktober 1994 zugestimmt hat, liegt z. Z. mehreren Verbänden (kommunalen Spitzenverbänden, Bauverbänden, Architektenkammer usw.) zur Stellungnahme vor.

Bewerber, Bieter und Unternehmen, die nachweislich eine schwere Verfehlung begangen haben, die ihre Zuverlässigkeit als Auftragnehmer in Frage stellt, würden danach bei Aufträgen, die von Dienststellen des Landes erteilt werden oder im wesentlichen aus Zuwendungen des Landes bezahlt werden, grundsätzlich von der Teilnahme am Wettbewerb um den Auftrag ausgeschlossen.

In der Arbeitsgruppe war lange Zeit umstritten, wie die landesweite Wirkung der Vergabesperre am einfachsten zu gewährleisten sei. Der Ausschluß vom Wettbewerb soll in der Regel von der Mittelbehörde oder der Dienststelle verfügt werden, in deren Zuständigkeitsbereich die Verfehlung festgestellt wurde. Für den Informationsaustausch kamen zwei Verfahren in Betracht: informelle Unterrichtung der Ressorts oder zentrales Melde- und Informationssystem. Beide wären datenschutzrechtlich zulässig. Der Entwurf sieht eine zentrale Melde- und Informationsstelle für Vergabesperren vor. Die Stelle soll bei der Oberfinanzdirektion Frankfurt eingerichtet werden. Ihr werden Ausschlüsse vom Wettbewerb mit folgenden Angaben gemeldet:

1. Behörde,
2. Datum,
3. Aktenzeichen,
4. Name eines Ansprechpartners,
5. Telefonnummer des Ansprechpartners,
6. Umfang der Sperre,
7. betroffenes Unternehmen,
8. Gewerbezweig/Branche,
9. Anschrift,
10. Handelsregisternummer (falls bekannt).

Vor der Vergabe eines Auftrags mit einem Wert über 30.000 DM bei Dienstleistungsaufträgen, 50.000 DM bei Lieferaufträgen und 100.000 DM bei Bauaufträgen muß die Vergabestelle bei der Melde- und Informationsstelle nachfragen, ob der vorgesehene Auftragnehmer vom Wettbewerb ausgeschlossen ist. Ist dies der Fall, teilt die Melde- und Informationsstelle der Vergabestelle die oben beschriebenen Daten mit. Bei geplanten Vergaben unterhalb der genannten Wertgrenzen steht die Anfrage im Ermessen der Vergabestelle. Die Wiederzulassung eines Bewerbers muß

der Melde- und Informationsstelle ebenfalls mitgeteilt werden. Diese hat daraufhin die betreffenden Angaben über die Sperre zu vernichten.

Besonders wegen seiner größeren Effektivität und Praktikabilität habe ich von Anfang an das zentrale Meldeverfahren empfohlen.

30.7
Neuer landeseinheitlicher Personalbogen (22. Tätigkeitsbericht, Ziffer 10.1.2)

Im Zusammenhang mit der Neuordnung des Personalaktenrechts hatte ich darauf hingewiesen, daß der einheitliche Personalbogen für die Einstellung in den öffentlichen Dienst überarbeitet werden muß. Das bisher gültige Formular enthielt einige unzulässige Fragen. Nunmehr legt § 107 Abs. 4 HBG den Rahmen der zulässigen Fragen fest: Es dürfen diejenigen Daten erhoben werden, die zur Begründung des Dienstverhältnisses erforderlich sind. Dabei ist darauf zu achten, daß bestimmte Angaben von jedem Bewerber benötigt werden, andere erst dann, wenn die konkrete Einstellungsentscheidung schon getroffen ist. Schließlich gibt es auch Daten, die zwar zur Abwicklung des Dienstverhältnisses erforderlich sind – etwa zur Berechnung des Ortszuschlags –, die aber mit getrennten Vordrucken von der jeweils festsetzenden Stelle erfragt werden. Eine besondere Schwierigkeit bei der Gestaltung des Bogens ergibt sich zudem daraus, daß dieser als erstes Blatt Bestandteil der Personalakte wird und als solcher dann von der Beschäftigungsbehörde auch jeweils aktualisiert werden soll.

Aus dem alten Personalbogen sind nunmehr Fragen zu den wirtschaftlichen Verhältnissen, zu Geburtsdatum und Geburtsort der Ehepartner und zum Kindschaftsverhältnis nicht übernommen worden. Gleichzeitig wird darauf hingewiesen, daß nur die Angaben, welche üblicherweise zu einer Bewerbung gehören, auch schon zu diesem Zeitpunkt belegt werden müssen. Alle anderen Angaben sind erst bei der konkreten Einstellung mitzuteilen bzw. zu belegen. Bei der Frage nach besonderen Kenntnissen wie Kurzschrift oder Datenverarbeitungskenntnisse wird nunmehr ausdrücklich auf die Freiwilligkeit der Angaben hingewiesen.

Ich hoffe, daß der Erlaß zur Einführung dieses Personalbogens in Kürze in Kraft gesetzt wird. Damit wird ein weiterer Schritt zur Verbesserung der Arbeitsabläufe in den Personalverwaltungen im Interesse der Beschäftigten getan.

Wiesbaden, den 21. Februar 1995

gez. Professor Dr. Hassemer

31. Materialien

31.1
Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 in Potsdam zur

Informationsverarbeitung im Strafverfahren

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiterverarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz – BTDrucks. 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittlungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren – auch mit Zwangsmitteln – erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten.

   Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend und normenklar festzulegen.

1.1 Insgesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird.

Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegriffen werden muß. Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrunde liegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Ein Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Datender jeweils anderen Behörden wäre datenschutzrechtlich nach derzeitiger Rechtslage als Übermittlung des gesamten Datenbestandes einer Stelle an die anderen Stellen zu bewerten. Damit ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei abstrakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden – also auch von anderen Staatsanwaltschaften – Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit – ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens – von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu "Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 "Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 3. November 1988).

31.2
Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 in Potsdam zu

Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Ländern verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte "Gesundheitskarten", etwa "Service-Karten" von Krankenversicherungen und privaten Anbietern, "Notfall-Karten", "Apo(theken)-Cards" und "Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienten-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen "Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller – etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse – mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichtert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse ggf. ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die "Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten – wie den Medizinern – und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest – vorbehaltlich weiterer Punkte – die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht – etwa durch Integration auf einem Chip – die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall und ohne Benachteiligung – z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung – entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Umfang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.
- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

31.3
Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 in Potsdam zum

Abbau des Sozialdatenschutzes (gegen die Stimme Bayerns)

Der Gesetzgeber hat in den vergangenen Monaten die Möglichkeit der Überprüfung von Sozialleistungsempfängern ohne deren vorherige Befragung oder Kenntnis in drastischem Umfang vermehrt. Insbesondere durch das seit dem 1. Juli 1993 geltende Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms ist das Kontrollinstrumenta-

rium von Sozial- und Arbeitsämtern noch einmal erheblich erweitert worden. Ohne Rücksicht auf konkrete Anhaltspunkte für einen unberechtigten Leistungsbezug im Einzelfall sind künftig automatisierte Datenabgleiche zwischen Sozialhilfeträgern sowie zwischen diesen und der Arbeitsverwaltung bzw. der Kranken-, Unfall- und Rentenversicherung gestattet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist sehr besorgt über diese Entwicklung, die zu einem immer dichteren Datenverbundsystem im Sozialleistungsbereich und zu immer nachhaltigeren Eingriffen in das Recht auf informationelle Selbstbestimmung aller Betroffenen, d.h. auch und gerade der großen Mehrheit rechtstreuer Antragsteller und Leistungsbezieher, führt.

Mit Nachdruck wenden sich die Datenschutzbeauftragten gegen Versuche von Sozialverwaltungen, bei der Umsetzung der neuen Kontrollregelungen durch extensive Interpretation über den gesetzlich vorgegebenen Rahmen hinauszugehen. So erlaubt beispielsweise der neu gefaßte § 117 Abs. 3 des Bundessozialhilfegesetzes entgegen der Handhabung einzelner Kommunen keinen automatisierten Datenabgleich zwischen Sozialhilfedatei und Kraftfahrzeug-Register, sondern nur den Vergleich von Angaben in Verdachtsfällen.

Die dargestellte Entwicklung macht es erneut notwendig, auf die verfassungsrechtliche Qualität des Grundsatzes der Datenerhebung beim Betroffenen hinzuweisen. An dem Prinzip, daß bei der Überprüfung der Leistungsberechtigung und der Nachweise Auskünfte zunächst beim Antragsteller anzufordern sind und nur aufgrund konkreter Verdachtsmomente Nachfragen bei dritten Stellen oder Datenabgleiche erfolgen dürfen, muß für den Regelfall festgehalten werden, soll der Einzelne mündiger Bürger bleiben und nicht zum bloßen Objekt staatlicher Verhaltenskontrolle werden.

Sorge äußert die Konferenz auch über die hartnäckigen Bestrebungen, Datenbestände der Sozialverwaltung für immer neue Zwecke und Adressaten zu öffnen. Beispiele dafür sind die im Gesetzgebungsverfahren zum 2. SGB-Änderungsgesetz im letzten Augenblick gescheiterten Anträge, Polizei und Staatsschutz in unvertretbarem Umfang Zugriff auf Daten Arbeitsloser und sonstiger Sozialleistungsempfänger zu geben. Das Sozialgeheimnis muß ein wirksamer Sonderschutz für die besonders sensiblen Daten in der Sozialverwaltung bleiben. Nur dies entspricht der Abhängigkeit des Einzelnen von staatlichen Leistungen und der sich daraus ergebenden speziellen Verletzlichkeit seines Rechts auf informationelle Selbstbestimmung.

31.4
Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 in Potsdam zum
Ausländerzentralregistergesetz (gegen die Stimme Bayerns)

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens acht Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 2. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern – worauf die Entwurfsbegründung hinweist – der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen, unter denen u.a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen – wenn auch reduzierten – Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

31.5
Beschluß der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 in Potsdam zum

Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz – PTNNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-DRS. 114/94 = BT-Drs. 12/6717)

I.
Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.
Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten insbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer – auch nach dem Wegfall der Monopole – einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kriterien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltnachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufern bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.
Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

31.6
Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 in Potsdam zu

Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

– Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleibt die Zuständigkeit des BKA als nationale Stelle für EUROPOL unberührt.

– Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, z. B. durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

31.7
Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 in Potsdam zu

Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als zehn Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Jusitzverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z. B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz),
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

31.8
Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 in Potsdam

Art. 12 Verbrechensbekämpfungsgesetz zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.

Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

31.9
Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 in Potsdam

Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.
   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.
2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d.h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.
3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

31.10
Beschluß der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 in Potsdam

Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 (KOM(94) 128 endg. – COD 288)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.
2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei "berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.
3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.
4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte – wie im ursprünglichen Richtlinienentwurf vorgesehen – untersagt werden.
5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte – wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah – auf Unionsebene garantiert werden.
6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z.B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.

7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z.B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedstaaten, diese Anregungen zu unterstützen.

31.11
Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25. August 1994 (Potsdam) zum

Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung, KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 – Beschluß –).

Gegen den vorgelegten Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen – insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung – bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.
   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotene Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht, wie in Art. 3 vorgesehen, von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff "statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 – allerdings mit einem anderen Begriffsinhalt – definiert wird. Der Begriff "statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte – ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) – auch die Festlegung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3b EG-Vertrag. Dieser gebietet hier, daß – jedenfalls grundsätzlich – die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.
   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.