Unterrichtung

Landesbeauftragter für den Datenschutz
Niedersachsen

Hannover, den 7. 1. 1993

An den
Herrn Präsidenten des Niedersächsischen Landtages
Hannover

Betr.: **Elfter Bericht über die Tätigkeit des Niedersächsischen Datenschutzbeauftragten**

Sehr geehrter Herr Präsident!

Hiermit erstatte ich gemäß § 18 Abs. 3 des Niedersächsischen Datenschutzgesetzes den XI. Tätigkeitsbericht für die Zeit vom 1. Januar 1991 bis zum 31. Dezember 1992.

Mit vorzüglicher Hochachtung
Dr. Dronsch

Inhaltsverzeichnis

Anlagen

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

1 Beschluß der Sonderkonferenz am 29. Januar 1991 zum Vorschlag der EG-Kommission für eine **Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten**

2 Beschluß der 41. Konferenz am 8. März 1991 zu **Telekommunikation und Datenschutz**

3 Entschließung der Konferenz vom 25. Juni 1991 — gegen die Stimme Bayerns — zum Bundesratsentwurf eines **Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität**

4 Entschließung der 42. Konferenz am 26./27. September 1991 zum **Datenschutz im Recht des öffentlichen Dienstes**

5 Entschließung der 43. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 23./24. März 1992 in Stuttgart zum **Arbeitnehmerdatenschutz**

6 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum **Grundrecht auf Datenschutz** vom 28. April 1992

7 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur **Neuregelung des Asylverfahrens** (BT-Drs. 12/2062) vom 28. April 1992

8 Entschließung der Konferenz der Datenschutzbeauftragten vom 1./2. Oktober 1992 (zum heimlichen **Abhören in und aus Wohnungen**)

9 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung — **Gesundheitsstrukturgesetz 1993** — (BR-Drs. 560/92)

10 Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992 zum **Datenschutz bei internen Telekommunikationsanlagen**

11 Schreiben des Landesbeauftragten für den Datenschutz Niedersachsen an den Präsidenten des Niedersächsischen Landtages vom 6. November 1991 zur **Umgestaltung der Vorläufigen Niedersächsischen Verfassung in eine endgültige Niedersächsische Verfassung**

12 **Normen, Standards und Empfehlungen für den IuK-Technikeinsatz** in der Landesverwaltung (Auszug)

Abkürzungen

AB (M)	Arbeitsbeschaffungs- (Maßnahme)
Abb.	Abbildung
Abs.	Absatz
ADV	Automatisierte Datenverarbeitung
a. F.	alte Fassung
AFG	Arbeitsförderungsgesetz
AFIS	Automatisches Fingerabdruckidentifikationssystem
AOK	Allgemeine Ortskrankenkasse
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
APIS	Arbeitsdatei PIOS Innere Sicherheit (PIOS steht für Personen, Institutionen, Objekte, Sachen)
Art.	Artikel
AsylVerfG	Asylverfahrensgesetz
AuslG	Ausländergesetz
Az.	Aktenzeichen
AZR	Ausländerzentralregister
BAFl	Bundesamt für die Anerkennung von Flüchtlingen
BAG	Bundesarbeitsgericht
BauGB	Baugesetzbuch
BBG	Bundesbeamtengesetz
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BKA (G)	(Gesetz über das) Bundeskriminalamt
BÜROMIN	Bürokommunikation der Ministerien
BRRG	Beamtenrechtsrahmengesetz
BSHG	Bundessozialhilfegesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BT-Drs	Bundestagsdrucksache
BTM	Betäubungsmittel
BVerfG (E)	Bundesverfassungsgericht (Entscheidungssammlung)
BZR (G)	Bundeszentralregister (-Gesetz)
bzw.	beziehungsweise
ca.	circa
(MS-) DOS	(ADV-Betriebssystem für Personal Computer)
DAMASKUS	Datei zur Massenauswertung von Kfz-Kennzeichen und sonstigen Daten — Auswertungssystem des LKA Niedersachsen
DANA	Datenschutznachrichten
DÖV	Die Öffentliche Verwaltung
DV	Datenverarbeitung
DVBl.	Deutsches Verwaltungsblatt
ED	Erkennungsdienst
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
f (f).	und folgende Seite (n)

gem.	gemäß
GEZ	Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten
GMBl.	Gemeinsames Ministerialblatt (herausgegeben vom Bundesministerium des Innern)
GG	Grundgesetz
ggf.	gegebenenfalls
GO LT	Geschäftsordnung des Landtags
GVBl.	Gesetz- und Verordnungsblatt
i.d.F.	in der Fassung
IMA-IuK	Interministerieller Arbeitskreis Informations- und Kommunikationstechnik
INPOL	(bundesweites) Informationssystem der Polizei
ISO	International Standardisation Organisation
ISDN	Integrated Services Digital Network
ITSEC	EG-einheitliche Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik
ITSEM	Information Security Evaluation Manual
IuK-	Informations- und Kommunikations-
IuK-Reg	Einsatz der IuK-Technik bei Bezirksregierungen
i.V.m.	in Verbindung mit
JVA	Justizvollzugsanstalt
Kfz	Kraftfahrzeug
KpS	Kriminalpolizeiliche personenbezogene Sammlungen
KJHG	Kinder- und Jugenhilfegesetz (SGB VIII)
LAN	Local Area Network (Lokales Netzwerk)
LfD	Landesbeauftragter für den Datenschutz
LIS	Landesinformationsstelle
LKA	Landeskriminalamt
LT-Drs	Landtagsdrucksache
LWL-	Lichtwellenleiter-
MDK	Medizinischer Dienst der Krankenversicherung
MHH	Medizinische Hochschule Hannover
MIKADO	Modulares Informations- und Kommunikationssystem Automatisierter Dezentraler Online-Anwendungen
MiStra	Anordnung über Mitteilungen in Strafsachen
MiZi	Anordnung über Mitteilungen in Zivilsachen
NADIS	Nachrichtendienstliches Informationssystem
NATO	North Atlantic Treaty Organisation
NBG	Niedersächsisches Beamtengesetz
NDO	Niedersächsische Disziplinarordnung
NDR	Norddeutscher Rundfunk
Nds.	Niedersächsische (r/s)
NDSG	Niedersächsisches Datenschutzgesetz
NDSG-E	Entwurf eines NDSG vom 4.6.1992 (LT-Drs 12/3290)
Nds. MBl.	Niedersächsisches Ministerialblatt
Nds. Rpfl.	Niedersächsische Rechtspflege
Nds. SOG	Niedersächsisches Gesetz über die öffentliche Sicherheit und Ordnung
NGefAG	Niedersächsisches Gefahrenabwehrgesetz
NGO	Niedersächsische Gemeindeordnung
NHG	Niedersächsisches Hochschulgesetz

Nieders.	Niedersächsische (r/s)
NJW	Neue Juristische Wochenschrift
NMG	Niedersächsisches Meldegesetz
Nr.	Nummer
NStZ	Neue Zeitschrift für Strafrecht
NVerfSchG	Niedersächsisches Verfassungsschutzgesetz
NVwZ	Neue Zeitschrift für Verwaltungsrecht
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (Artikelgesetz zur Änderung des StGB, der StPO usw.)
OVG	Oberverwaltungsgericht
PersVG	Personalvertretungsgesetz
PC	Petsonal Computer
PKS	Polizeiliche Kriminalstatistik
POLAS	Polizeiliches Auskunftssystem (in Niedersachsen)
PStG	Personenstandsgesetz
PsychKG	Gesetz über Hilfen für psychisch Kranke und Schutzmaßnahmen
RdErl.	Runderlaß
RdNr.	Randnummer
RDV	Recht der Datenverarbeitung
RiStBV	Richtlinien für das Straf- und Bußgeldverfahren
S.	Seite
SchwbG	Schwerbehindertengesetz
SED	Sozialistische Einheitspartei Deutschlands (in der ehemaligen DDR)
SGB	Sozialgesetzbuch
sog.	sogenannt (e/r)
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
SVBl.	Schulverwaltungsblatt
TB	Tätigkeitsbericht
TÜV	Technischer Überwachungsverein
u.	und
u. a.	unter anderem, und andere
u. ä.	und ähnliches
UNIX	(ADV-Betriebssystem für Mehrplatzsysteme)
usw.	und so weiter
u. U.	unter Umständen
v.	von, vom
VGH	Verwaltungsgerichtshof
VGO	Vollzugsgeschäftsordnung
vgl.	vergleiche
VNV	Vorläufige Niedersächsische Verfassung
VV	Verwaltungsvorschrift
VwGO	Verwaltungsgerichtsordnung
ZAB	Zentrale Ausländerbehörde (für Asylsuchende)
ZASt	Zentrale Anlaufstelle für Asylsuchende
z. B.	zum Beispiel
ZEVIS	Zentrales Verkehrsinformationssystem
ZPO	Zivilprozeßordnung
z. Zt.	zur Zeit

1. Vorbemerkung

Mit dem vorliegenden XI. Tätigkeitsbericht ist zum dritten Male ein Zwei-Jahres-Bericht erstellt worden. Ging der zweijährige Zeitraum beim IX. und X. Tätigkeitsbericht auf einen Wunsch des Niedersächsischen Landtages zurück, so ist nunmehr in § 18 Abs. 3 Satz 1 NDSG in der Fassung des Gesetzes zur Neuregelung der Stellung des Landesbeauftragten für den Datenschutz vom 28. Mai 1991 (Nieders. GVBl. S. 195) eine klare Rechtsgrundlage vorhanden.

Der XI. Tätigkeitsbericht behält die bewährte und vertraute Gliederung bei. Wegen des Hinzukommens zweier neuer Abschnitte, „Europa" (6) und „Niedersächsische Landesbibliothek" (26), erfolgte der Austausch von Kapitelnummern. Da meine Dienststelle seit einem Jahr auch für den Datenschutz im nicht-öffentlichen Bereich" zuständig ist, wurden entsprechende Kapitel am Ende angefügt (34 bis 36).

2. Zur Situation

2.1 Niedersachsen

Der letzte Tätigkeitsbericht endet mit der Aussage: „In Niedersachsen besteht für den Datenschutz zur Zeit Anlaß zu Optimismus." Diese optimistische Einschätzung hat auch für die Jahre 1991 und 1992 Berechtigung. Sie beruht darauf, daß die neue Niedersächsische Landesregierung zahlreiche datenschutzrechtlich relevante Vorhaben in Angriff genommen hat. Aber auch das sei gesagt: Um datenschutzrechtlich optimale Lösungen muß gerungen werden; Datenschutz muß oft Zentimeter für Zentimeter erkämpft werden. Wenn Rudolf v. Jhering, der große deutsche Rechtsgelehrte — in Aurich geboren — vom „Kampf ums Recht" (1873) sprach, so haben diese Worte auch für das Datenschutzrecht Aktualität.

Das erste bedeutsame Vorhaben war das Gesetz zur Neuregelung der Stellung des Landesbeauftragten für den Datenschutz vom 28. Mai 1991 (Nieders. GVBl. S. 195). Es geht auf eine Initiative aller vier Landtagsfraktionen zurück. In die Vorläufige Niedersächsische Verfassung wurde ein neuer Art. 46 a eingefügt, der die Aufgaben, die Wahl und die Rechtsstellung des Landesbeauftragten regelt. Des weiteren wurden die § 17 bis 20 NDSG neu gefaßt; die Befugnisse des Landesbeauftragten (vgl. 3.2) und das Anrufungsrecht der Bürgerinnen und Bürger wurden verbessert. Wegen der Würdigung des Gesetzes vom 28. Mai 1991, das einstimmig vom Niedersächsischen Landtag verabschiedet wurde, darf ich auf meine Aufsätze in den Zeitschriften Niedersächsischer Städtetag (1991, S. 145) und Datenschutz und Datensicherung (1991, S. 440) hinweisen.

Das zweite hervorzuhebende Gesetz ist das Gesetz über den Verfassungsschutz im Lande Niedersachsen (Niedersächsisches Verfassungsschutzgesetz — NVerfSchG) vom 3. November 1992 (Nieders. GVBl. S. 283). Ich verweise auf Abschnitt 14.1 dieses Tätigkeitsberichts.

Als drittes Vorhaben ist der zweite Schritt zur Neuregelung des allgemeinen Datenschutzrechts in Niedersachsen — im Anschluß an das obengenannte Gesetz vom 28. Mai 1991 — zu nennen. Dieser Schritt wurde im April 1991 durch Vorlage eines Referentenentwurfs eines Gesetzes zur Sicherung der

informationellen Selbstbestimmung (Niedersächsisches Datenschutzgesetz — NDSG —) eingeleitet. Am 16. Januar 1992 fand ein „Expertenhearing" statt, an dem auch ich teilnahm. Die Beschlußfassung des Niedersächsischen Landesministeriums über die Einbringung beim Landtag erfolgte am 2. Juni 1992. Die erste Lesung des Entwurfs eines Niedersächsischen Datenschutzgesetzes (LT-Drs 12/3290) im Landtag fand am 17. Juni 1992 statt. Aus dieser Lesung möchte ich einen Satz des Innenministers herausgreifen: „Wir wollen ja eher eine gläserne Verwaltung als den gläsernen Bürger in unserem Lande schaffen."

Der Gesetzentwurf stellt einen beachtlichen Beitrag zur Sicherung des Grundrechts auf informationelle Selbstbestimmung dar. Die wesentlichen Verbesserungen gegenüber der jetzigen Rechtslage bestehen darin, daß die Akten in den Anwendungsbereich des Gesetzes einbezogen werden, das Zweckbindungsprinzip gesetzlich verankert wird, die Rechte der Betroffenen erheblich erweitert werden und besondere Datenschutzregelungen für einige Bereiche (Datenverarbeitung bei Dienst- und Arbeitsverhältnissen, Verarbeitung personenbezogener Daten für Forschungsvorhaben, Fernmessen und Fernwirken, öffentliche Auszeichnungen) erfolgen. Nicht aufgegriffen hat der Gesetzentwurf den im Expertenhearing angesprochenen Problembereich, wie die Risiken neuer Verarbeitungstechniken rechtlich in den Griff zu bekommen sind („vorgezogener Datenschutz"). In einer Pressemitteilung vom 3. Juni 1992 habe ich meinem Wunsch Ausdruck gegeben, daß die parlamentarischen Beratungen zügig verlaufen, ferner, daß der Gesetzentwurf in Detailfragen noch verbessert wird.

Als viertes datenschutzrechtlich bedeutsames Gesetzesvorhaben ist der Entwurf eines Niedersächsischen Gefahrenabwehrgesetzes (NGefAG) zu nennen. Ich verweise auf Abschnitt 12.4 dieses Tätigkeitsberichtes.

Schließlich sei hervorgehoben, daß einige schon beschlossene Gesetze oder vorgelegte Gesetzentwürfe datenschutzrechtliche Detailregelungen enthalten: z.B. das Gesetz zur Änderung des Niedersächsischen Abfallgesetzes vom 7. November 1991 (Nieders. GVBl. S. 295), das Niedersächsische Abfallabgabengesetz vom 17. Dezember 1991 (Nieders. GVBl. S. 373), der Entwurf eines Zehnten Gesetzes zur Änderung der Niedersächsischen Gemeindeordnung und der Niedersächsischen Landkreisordnung betr. Frauenbeauftragte (LT-Drs 12/3260) sowie der Entwurf eines Vierten Gesetzes zur Änderung des Niedersächsischen Schulgesetzes (LT-Drs 12/3300). Bei einigen Vorhaben — z. B. bei der Errichtung eines niedersächsischen Krebsregisters (Nr. 2.4. der Koalitionsvereinbarung vom 19. Juni 1990) — ergibt sich ein Zeitdruck im Hinblick auf den Ablauf der Legislaturperiode. Im übrigen verweise ich auf die speziellen Ausführungen in diesem Tätigkeitsbericht.

2.2 Bundesrepublik Deutschland

Das neue Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990 (BGBl. I S. 2954) — in Kraft getreten am 1. Juni 1991 — ist bereits im letzten Tätigkeitsbericht an dieser Stelle kritisch gewürdigt worden.

Ergänzend ist folgendes hervorzuheben: Die nordwestdeutschen Landesdatenschutzbeauftragten haben am 3. Juni 1991 in einer gemeinsamen Erklärung kritisiert, daß § 24 Abs. 6 BDSG, der eine Widerspruchsmöglichkeit der Betroffenen gegen eine Datenschutzkontrolle vorsieht, einen Eingriff in ihre Rechte darstellt. Auf der Datenschutzkonferenz am 26./27. September 1991 ist zwischen den Landesbeauftragten Einvernehmen in der Auffassung erzielt worden, daß dem Bund die Kompetenz fehlt, die Kontrollrechte der Landesbeauftragten durch § 24 Abs. 6 BDSG einzuschränken (vgl. auch Simitis, in:

Simitis/Dammann/Geiger/Mallmann/Walz, Kommentar zum BDSG, 4. Auflage 1992, § 1 RdNr. 58). Im übrigen haben sich die Bundes- und Landesdatenschutzbeauftragten auf dieser Konferenz darüber verständigt, nach welchen Grundsätzen sie bei der Anwendung und Auslegung von § 24 Abs. 2 BDSG verfahren werden.

Schließlich ist zum BDSG folgendes anzumerken: Die Kritik an dem neuen Gesetz stimmt darin überein, daß der Datenschutz im nicht-öffentlichen Bereich jetzt noch stärker hinter dem Datenschutz im öffentlichen Bereich zurückbleibt (vgl. z.B. Dammann, Das neue Bundesdatenschutzgesetz, NVwZ 1991, S. 640 ff., 641 und 643). Da ich seit dem 1. Januar 1992 Aufsichtsbehörde für den nicht-öffentlichen Bereich bin, liegt jetzt hinreichende Praxiserfahrung vor, daß ich mit Nachdruck auf diesen Mißstand aufmerksam machen muß.

Was noch ausstehende Umsetzungen des Volkszählungsurteils des Bundesverfassungsgerichts vom 15. Dezember 1983 auf Bundesebene anbetrifft, ist insbesondere die Novellierung der Strafprozeßordnung anzumahnen.

2.3 Verfassung und Datenschutz

Seit dem Volkszählungsurteil vom 15. Dezember 1983 hat das Bundesverfassungsgericht — gestützt auf Art. 2 Abs. 1 (freie Entfaltung der Persönlichkeit) in Verbindung mit Art. 1 Abs. 1 GG (Menschenwürde) — in ständiger Rechtsprechung ein Recht des einzelnen anerkannt, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Aus der letzten Zeit sei etwa auf den Beschluß des BVerfG vom 19. Dezember 1991 (NJW 1992, S. 815) hingewiesen, der sich mit dem Fall befaßt, daß ein Arbeitgeber (Herausgeber einer Zeitschrift) ein Telefongespräch eines Arbeitsnehmers (Chefredakteur) abhörte. Nicht zuletzt unter politisch-psychologischen Aspekten drängt sich die Überlegung auf, das Recht auf informationelle Selbstbestimmung ausdrücklich verfassungsgesetzlich zu regeln.

Im Zusammenhang mit der deutschen Einigung werden Fragen zur Änderung oder Ergänzung des Grundgesetzes aufgeworfen. Diese erstrecken sich auch auf den Grundrechtsbereich; ich verweise etwa auf den Bericht „Stärkung des Föderalismus in Deutschland und Europa sowie weitere Vorschläge zur Änderung des Grundgesetzes" der Kommission Verfassungsreform des Bundesrates vom 14. Mai 1992 (Bundesrats-Drs. 360/92). Die Datenschutzbeauftragten des Bundes und der Länder haben auf ihrer Konferenz am 28. April 1992 in Stuttgart — bei Gegenstimme Bayerns und in Abwesenheit Sachsens — eine Entschließung gefaßt, mit der sie der Gemeinsamen Verfassungskommission von Bundestag und Bundesrat einen konkreten Formulierungsvorschlag für das Grundrecht auf Datenschutz unterbreiten (vgl. Anlage 6 dieses Tätigkeitsberichts). In der Entschließung hat die Konferenz auch empfohlen, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Rechts auf informationelle Selbstbestimmung im Alltag von entscheidender Bedeutung ist, im Grundgesetz zu verankern.

Insbesondere wenn diese Bemühungen auf Bundesebene scheitern, ergibt sich das Anliegen, das Recht auf informationelle Selbstbestimmung in die Landesverfassungen aufzunehmen. In einigen Bundesländern ist dies bereits geschehen, erstmals 1978 in Nordrhein-Westfalen. Die Vorläufige Niedersächsische Verfassung (VNV) von 1951 ist ein sogenanntes Organisationsstatut, das keine Grundrechte kennt. Im Zuge der deutschen Wiedervereinigung hat sich die Notwendigkeit ergeben, eine endgültige Niedersächsische Verfassung zu schaffen. Mit Beschluß vom 10. Oktober 1990 hat der Niedersächsische Land-

tag einen Sonderausschuß „Niedersächsische Verfassung" eingesetzt, der Vorschläge zur Änderung der VNV erarbeiten soll. Was die im Landtag vertretenen Parteien anbetrifft, enthält nur der gemeinsame Verfassungsentwurf der Fraktionen der SPD und der Grünen (LT-Drs 12/3008 und 12/3160) eine Regelung des informationellen Selbstbestimmungsrechts. Ich begrüße diesen Vorschlag nachdrücklich, wenngleich er in den Details diskussionsbedürftig ist. Erfreulicherweise stimmen die Verfassungsentwürfe der Fraktionen der SPD und der Grünen, der CDU (LT-Drs 12/3210) sowie der FDP (LT-Drs 12/3250) darin überein, die unabhängige Datenschutzkontrolle — in Anknüpfung an Art. 46 a VNV — auch in der künftigen Landesverfassung zu verankern. Ich selbst habe mit Schreiben vom 6. November 1991 dem Herrn Landtagspräsidenten einen Formulierungsvorschlag für ein Grundrecht auf informationelle Selbstbestimmung unterbreitet (Anlage 11).

2.4 Europäisches Datenschutzrecht

Ein Bericht über die Situation des Datenschutzes wäre unvollständig, wenn der europäische Bereich ausgespart bliebe. Das europäische Datenschutzrecht gewinnt eine immer größere Bedeutung, so daß ihm ein eigener Abschnitt dieses Tätigkeitsberichts gewidmet werden soll (6).

3. Der Landesbeauftragte

3.1 Status

Das bereits unter 2.1 genannte Gesetz zur Neuregelung der Stellung des Landesbeauftragten für den Datenschutz vom 28. Mai 1991 hatte u. a. eine grundlegende Statusänderung des Datenschutzbeauftragten zum Ziel. Dieser ist nicht mehr Beamter auf Lebenszeit, allein berufen durch das Niedersächsische Landesministerium. Der neue Art. 46 a Abs. 2 VNV regelt vielmehr, daß der Landtag — auf Vorschlag des Landesministeriums — den Landesbeauftragten für den Datenschutz mit einer Mehrheit von zwei Dritteln der anwesenden Abgeordneten, mindestens jedoch der Mehrheit der Abgeordneten wählt. Diese Neuregelung hat den Zweck, den Landesbeauftragten in seiner Unabhängigkeit zu stärken und seine Bedeutung als Kontroll- und Beratungsorgan zu erhöhen. Gemäß dem neuen § 17 Abs. 1 Satz 2 NDSG wird der Landesbeauftragte nach der Wahl durch den Landtag auf die Dauer von acht Jahren in ein Beamtenverhältnis auf Zeit berufen; nach Satz 3 sind die Wahl und die Berufung für eine weitere Amtszeit zulässig. In Art. 46 a Abs. 3 VNV ist nunmehr verfassungsrechtlich geregelt, daß der Landesbeauftragte unabhängig und nur dem Gesetz unterworfen ist. Hatten die Koalitionsvereinbarung der SPD und der Grünen vom 19. Juni 1990 und die Regierungserklärung des Ministerpräsidenten vom 22. Juni 1990 noch angekündigt, daß der Landesbeauftragte der Dienstaufsicht des Landtagspräsidenten unterstehen soll, so beläßt es der neue § 17 Abs. 3 Satz 1 NDSG bei der Anbindung an das Innenministerium.

Der Landtag wählte mich in seiner Sitzung vom 21. Juni 1991 zum Landesbeauftragten. Es wurden 145 gültige Stimmen abgegeben; davon waren 142 Ja-Stimmen und 3 Nein-Stimmen. Dieses Ergebnis ist persönlich erfreulich und dürfte meiner Tätigkeit eine breite Akzeptanz sichern. Die Ernennung zum Landesbeauftragten erfolgte am 28. Juni 1991.

3.2 Kompetenzen

Zum ersten Male seit 1978 kann in einem Tätigkeitsbericht erfreulicherweise hervorgehoben werden, daß die Kompetenzen des Landesbeauftragten erweitert wurden.

Die wesentlichste Kompetenzerweiterung regelte das Niedersächsische Landesministerium mit Beschluß vom 17. Dezember 1991 (vgl. Nds. MBl. 1992 S. 230): „Als zuständige Aufsichtsbehörde nach § 38 des Bundesdatenschutzgesetzes (BDSG) vom 20.12.1990 (BGBl. I S. 2954) wird die oder der Landesbeauftragte für den Datenschutz bestimmt ... Dieser Beschluß tritt am 1.1.1992 in Kraft ..."

Die Konzentration der Datenschutzkontrolle für den nicht-öffentlichen Bereich, d. h. die Abkehr von der Zersplitterung auf die vier niedersächsischen Bezirksregierungen, war dringend erforderlich. Ob die Konzentration beim Landesbeauftragten die beste Lösung ist, sollte nach einiger Zeit praktischer Erfahrung noch einmal geprüft werden. Die zentrale Frage ist, ob sich die Weisungsgebundenheit des Landesbeauftragten im nicht-öffentlichen Bereich mit seiner verfassungskräftigen Unabhängigkeit verträgt. Alle Bediensteten der Geschäftsstelle haben sich mit großem Engagement der neuen Aufgabe angenommen. Im einzelnen wird auf die Abschnitte 34 bis 36 dieses Tätigkeitsberichts verwiesen.

Auch das Gesetz zur Neuregelung der Stellung des Landesbeauftragten für den Datenschutz vom 28. Mai 1991 (vgl. 2.1) brachte Kompetenzerweiterungen: In § 18 Abs. 1 Satz 2 NDSG wird — neben Gerichten und Landesrechnungshof — auch der Landtag der Kontrolle durch den Landesbeauftragten unterworfen, soweit er in Verwaltungsangelegenheiten tätig ist. In § 18 Abs. 2 Satz 1 und 2 NDSG ist eine Pflicht des Landesbeauftragten verankert worden, die Auswirkung der automatisierten Datenverarbeitung auf die Arbeitsweise der datenverarbeitenden Stellen im staatlichen und kommunalen Bereich zu beobachten. Nach § 18 Abs. 2 Satz 3 ist der Landesbeauftragte rechtzeitig über Planungen des Landes zum Aufbau automatisierter Informationssysteme zu unterrichten, und zwar auch dann, wenn keine personenbezogenen Daten verarbeitet werden. Durch die Regelung in § 18 Abs. 4 Satz 2 und 3 NDSG werden die Verfassungsschutzbehörde, die Behörden der Staatsanwaltschaft und der Polizei sowie die Landesfinanzbehörden hinsichtlich der Kontrolle durch den Landesbeauftragten grundsätzlich mit den übrigen Behörden des Landes gleichgestellt.

§ 26 des Niedersächsischen Verfassungsschutzgesetzes vom 3. November 1992 regelt, daß dem Ausschuß für Angelegenheiten des Verfassungsschutzes „Hilfe von seiten der oder des Landesbeauftragten für den Datenschutz" zu geben ist.

Was den Umfang meiner Kompetenzen anbetrifft, hat es in den beiden Berichtsjahren gravierende und nicht ausräumbare Streitpunkte mit den Ressorts nicht gegeben.

3.3 Beratung der Landesregierung

Leider sind auch 1991 und 1992 Fälle zu verzeichnen, in denen mich die Ressorts bei der Vorbereitung allgemeiner Regelungen des Landes und des Bundes nicht oder nicht rechtzeitig beteiligten. Mit Schreiben vom 1. Juli 1992 habe ich die Staatssekretärinnen und Staatssekretäre der niedersächsischen Ministerien auf diesen Mißstand hingewiesen und um Abhilfe gebeten.

3.4 Eingaben

Die Eingaben erstrecken sich, merkwürdigerweise bis auf den Komplex der Ausländerangelegenheiten, auf alle gesellschaftlichen Bereiche. Eine beachtliche Zunahme der Eingaben ist im Bereich des Umweltrechts zu verzeichnen. Im allgemeinen haben sich die betroffenen Stellen durchaus kooperativ verhalten. Gelegentlich hat es allerdings Schwierigkeiten bei der Aufklärung der Sachverhalte gegeben.

Einige Kommunen haben versucht, die Aufklärung hinauszuzögern oder zu verhindern. Besonders hartnäckig hat sich eine kreisfreie Stadt im Nordwesten Niedersachsens gezeigt. Sie schaltete auf meine Bitte um Stellungnahme hin in einem Fall aus dem Krankenhausbereich sofort einen Rechtsanwalt ein. Als die Stadt sich schließlich nach längerem Zögern zur Sache äußerte, ging sie auf wesentliche Fragen nicht ein. Ich habe diese unzureichende Auskunftserteilung beanstandet. Angesichts dieses Verhaltens war es auch nicht verwunderlich, daß ich auch in der Sache einen Rechtsverstoß feststellen mußte.

Das bereits unter 2.1 genannte Gesetz zur Neuregelung der Stellung des Landesbeauftragten für den Datenschutz vom 28. Mai 1991 hat eine Regelung getroffen, wonach sich die Bediensteten von Behörden und sonstigen öffentlichen Stellen in allen Angelegenheiten des Datenschutzes jederzeit an den Landesbeauftragten wenden können, auch wenn sie nicht selbst betroffen sind. Einer Einhaltung des Dienstweges bedarf es nicht, wenn die Bediensteten auf einen Verstoß gegen datenschutzrechtliche Vorschriften oder einen sonstigen Mangel bei der Verarbeitung personenbezogener Daten hingewiesen haben und diesem Hinweis binnen angemessener Frist nicht abgeholfen worden ist. Das Recht der öffentlichen Bediensteten wie aller Bürgerinnen und Bürger, sich in eigenen Angelegenheiten an den Landesbeauftragten für den Datenschutz wenden zu können, bleibt selbstverständlich weiterhin bestehen.

3.5 Akteneinsicht

Auch in den beiden Berichtsjahren gab es Streitfälle wegen Einsicht in die Akten der Geschäftsstelle. In meiner grundsätzlichen Auffassung, daß kein allgemeines Akteneinsichtsrecht der beschwerdeführenden Personen besteht (vgl. X 3.5), sehe ich mich durch jüngere wissenschaftliche Äußerungen bestätigt (z. B. Ordemann/Schomerus/Gola, BDSG, 5. Auflage 1992, § 23 Anm. 5.4). In diesem Zusammenhang kann ich Personen, die sich an mich mit Eingaben gewandt haben oder die sich in Zukunft an mich wenden wollen, weitgehende Vertraulichkeit zusagen. Nach § 12 Abs. 3 BDSG steht mir ebenso wie dem Bundesbeauftragten für den Datenschutz das Recht auf Zeugnisverweigerung zu (§ 23 Abs. 4 BDSG). Dieses Recht ist ergänzt durch ein strafprozessuales Beschlagnahmeverbot (§ 96 StPO).

3.6 Geschäftsstelle

Die beengte Unterbringung in dem Geschäfts- und Bürohaus „Schwarzer Bär 2" hatte die Arbeit der Bediensteten meiner Dienststelle zunehmend erschwert. Am 19. November 1991 konnten in der „Brühlstraße 9" endlich neue, angemessene Diensträume bezogen werden. Die Ausstattung meiner Dienststelle mit Informations- und Kommunikationstechnik wurde dadurch verbessert, daß sieben weitere BÜROMIN-Arbeitsplätze eingerichtet wurden. Die bisherige Textverarbeitungsanlage wurde dadurch abgelöst. Zugleich habe ich mir damit eine Testumgebung für das Datenschutz- und Datensicherungskonzept des Projektes BÜROMIN sowie für einen datenschutzgerechten

Einsatz von Mehrplatzanlagen unter dem Betriebssystem UNIX geschaffen. Den Referaten 14 (Innerer Dienst) und 69 (Zentrale Stelle für Organisationsangelegenheiten) des Niedersächsischen Innenministeriums möchte ich an dieser Stelle für ihre vielfältige Unterstützung danken.

Erfreulich ist auch die Entwicklung der Stellenausstattung meiner Geschäftsstelle. Im Haushaltsjahr 1991 wurden eine zusätzliche Stelle der Besoldungsgruppe (BesGr) A 14 und — im Hinblick auf die Übernahme der Aufsichtsbefugnisse im nicht-öffentlichen Bereich — zwei zusätzliche Stellen der BesGr A 12 bewilligt. Der Haushaltsplan 1992 brachte eine zusätzliche Stelle der BesGr A 15. Die nun erreichte Stellenausstattung ist aber — auch im Vergleich zu den Geschäftsstellen anderer Landesbeauftragter — immer noch nicht zufriedenstellend. Ich bin sehr dankbar, daß bei der ersten Beratung des Entwurfs eines neuen NDSG am 17. Juni 1992 im Landtag ein prominenter Abgeordneter sagte, der richtigen Tendenz, immer meht Aufgaben auf die Behörde des Datenschutzbeauftragten zu übertragen, müsse „aber auch noch etwas gegenüberstehen, nämlich die entsprechende personelle und materielle Ausstattung."

3.7 Außenprüfungen und Beratungen

1992 mußte ich meine Prüfungs- und Beratungshäufigkeit im öffentlichen Bereich zugunsten der neuen Zuständigkeit als Aufsichtsbehörde für den nichtöffentlichen Bereich etwas reduzieren. Durch die gemeinsame Prüfung mit Mitarbeitern des Niedersächsischen Landesverwaltungsamtes (vgl. 34.1) konnte ich sicherstellen, daß die Prüfungen in beiden Bereichen nach gleichen Kriterien entsprechend der Sensibilität der verarbeiteten Daten und der Verarbeitungsform durchgeführt werden.

Im öffentlichen Bereich wurden Beratungsgespräche und Kontrollen bei mehreren Gemeinden, Städten und Landkreisen, bei der Polizei, bei der Kassenärztlichen Vereinigung Niedersachsen und bei der Kassenzahnärztlichen Vereinigung Niedersachsen, der Architektenkammer Niedersachsen sowie im Innenministerium durchgeführt. Erstmals habe ich auch den Einsatz privater Lehrer-PC überprüft (vgl. 27.8). Auf die Kontrollen im nichtöffentlichen Bereich wird unter 35.2 eingegangen.

Ich begrüße die zunehmende Bereitschaft, mich bereits im Planungsstadium von DV-Verfahren oder auch von Bauvorhaben zum Zweck der Datensicherung zu beteiligen. Dadurch können bereits frühzeitig Datenschutzaspekte berücksichtigt werden, die ansonsten später mit höherem Aufwand nachgebessert werden müßten.

3.8 Dateienregister im öffentlichen Bereich

Neuanmeldungen und Änderungen von Dateien werden nur noch vereinzelt zum Dateienregister gemeldet. Dieses führe ich nicht auf einen Stillstand der Datenverarbeitung, sondern eher darauf zurück, daß die Verpflichtung nach dem NDSG und der Niedersächsischen Datenschutzregisterordnung (NDSRegO) in Vergessenheit geraten ist. Deshalb sei an dieser Stelle nochmals auf § 18 Abs. 5 NDSG und die Vorschriften der NDSRegO hingewiesen.

Insbesondere die von den Notaren abgegebenen Registermeldungen (vgl. auch 31.20) lösen häufig Rückfragen und erklärenden Schriftwechsel aus.

Vielen Notaren ist nicht bekannt, daß die Registermeldungen nach der Anlage 1 zur Niedersächsischen Datenschutzregisterordnung vom 22. Dezember 1978 (Nieders. GVBl. S. 823) abzugeben sind.

Aus den eingehenden Kopien der genehmigten Anträge auf Verarbeitung personenbezogener Daten von Schülerinnen und Schülern auf privaten Rechnern von Lehrkräften ist ersichtlich, daß offensichtlich zunehmend mehr Lehrerinnen und Lehrer vom Notizbuch auf die Elektronik umsteigen. Wie unter 3.7 ausgeführt, habe ich angefangen, die Datenschutz- und Datensicherungsmaßnahmen in diesem Bereich zu überprüfen.

Das Ministerium für Wissenschaft und Kultur hat auf meine Anregung im vorherigen Tätigkeitsbericht hin die Hochschulen nochmals auf die Registerpflicht für Forschungsdateien mit personenbezogenen Daten hingewiesen. Eine Resonanz hierauf ist leider nicht festzustellen. Ich werde nunmehr gezielt im Hochschulbereich die Einhaltung der Registerpflicht für Forschungsdateien mit personenbezogenen Daten überprüfen.

3.9 Öffentlichkeitsarbeit

Wie in den vorangegangenen Jahren konnte meine Dienststelle auch während des Berichtszeitraumes nicht allen Wünschen gerecht werden, die im Zusammenhang mit Bildungsveranstaltungen an mich herangetragen wurden. Hierfür ist meine Dienststelle nicht ausgestattet. Die Anfragen kommen aus allen gesellschaftlichen Bereichen. Dennoch haben die Angehörigen der Dienststelle und ich versucht, neben der sonstigen Arbeit Zeit für Seminare, Fortbildungsveranstaltungen, Vorträge und Konferenzen freizuhalten. Es wurde zielgruppenorientiert versucht, insbesondere dort den Datenschutzgedanken weiterzutragen, wo dies sich in der Praxis niederschlagen kann. Zielgruppen waren beispielsweise:

- Kommunale Bedienstete im Rahmen des Fortbildungsangebotes der Kommunalen Studieninstitute,
- Lehrkräfte von Schulen anläßlich der Lehrerfortbildung,
- Polizeibeamte bei der Fachhochschule der Polizei sowie der Polizei-Führungsakademie in Münster-Hiltrup,
- Personalräte,
- Studierende bei einer AStA-Veranstaltung der Universität Göttingen,
- Landräte im Rahmen einer Informationsveranstaltung des Niedersächsischen Landkreistages,
- Bedienstete von Gesundheitsämtern und Landeskrankenhäusern,
- Justizvollzugsbedienstete oder
- Richter und Staatsanwälte.

Aus meiner Sicht ist es ein Nachteil, daß Datenschutz im Rahmen des öffentlichen Bildungsangebots eher ein Mauerblümchendasein pflegt. Ich halte es für sinnvoll und notwendig, entsprechend dem Querschnittscharakter des Datenschutzes, diesen in das Pflichtprogramm bei der Ausbildung privater wie öffentlicher Bediensteter, die mit personenbezogenen Daten zu tun haben, aufzunehmen. Die Verbreitung automatisierter Datenverarbeitung steht immer mehr in einem eklatanten Mißverhältnis zur datenschutzrechtlichen Sensibilität und zu den Datenschutzkenntnissen bei Anwenderinnen und Anwendern sowie bei den Betroffenen.

Vom X. Tätigkeitsbericht, auf den in diesem Bericht immer wieder Bezug genommen wird, steht noch eine beschränkte Anzahl an Exemplaren zur unentgeltlichen Verteilung zur Verfügung. Sonderdrucke mit Auszügen aus den Be-

richten zum Thema „Datenschutz in Schulen" (bis IX. TB) sowie „Adoption und Apdoptionsgeheimnis" (bis X. TB) stoßen weiterhin auf allgemeines Interesse. Eine Neuauflage älterer Berichte erscheint mir im Hinblick auf die rasanten technischen und rechtlichen Veränderungen nicht angebracht. Sobald das neue NDSG in Kraft getreten sein wird, werde ich die Öffentlichkeit in angemessener Weise auf die neue Rechtslage hinweisen. Daß hierfür ein hoher Bedarf besteht, zeigen die Anfragen nach dem BfD-Info 1 des Bundesbeauftragten für den Datenschutz, in dem das 1991 in Kraft getretene BDSG dargestellt wird. Wegen der großen Nachfrage kann ich davon leider nur noch Einzelexemplare verteilen. Dieses Info wird in Kürze durch ein BfD-Info 2 ergänzt werden, welches die wesentlichsten Gebiete personenbezogener Datenverarbeitung auf Bundesebene darstellt. Weiterhin sind bei mir erhältlich:

— Orientierungshilfe Datenschutz und Datensicherung mit einem umfangreichen Fragenkatalog zu technischen und organisatorischen Maßnahmen,
— eine Literaturliste zum allgemeinen Datenschutzrecht,
— eine Liste der wichtigsten Datenschutzzeitschriften sowie
— eine Liste mit Einrichtungen, welche Datenschutz in ihrem Bildungsangebot führen.

3.10 Zusammenarbeit mit anderen Kontrollorganen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder tagte in den beiden Berichtsjahren insgesamt sechsmal. Die Entschließungen sind als Anlagen zu diesem Bericht abgedruckt. Die Entschließungen zum „Datenschutz im Recht des öffentlichen Dienstes" (Anlage 4) und zum „Arbeitnehmerdatenschutz" (Anlage 5) wurden im Arbeitskreis Personalwesen vorbereitet, in dem Niedersachsen den Vorsitz hat.

Im Zuge der Vereinigung Deutschlands hat sich die Datenschutzkonferenz erweitert, zunächst um die Ansprechpartner für Datenschutz in den neuen Bundesländern (als Gäste), dann — ausgenommen noch Thüringen — um die von den Landtagen gewählten Landesbeauftragten. Aus Respekt vor der Wertschätzung, die der Datenschutz in den neuen Bundesländern erfährt, fand die 42. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26. und 27. September 1991 im kultur- und geschichtsträchtigen Weimar statt.

Den Aufbau des Datenschutzes in Sachsen-Anhalt, dem Partnerland Niedersachsens, haben die Angehörigen der Geschäftsstelle und ich unterstützt. Dies konnte sich aber in Grenzen halten, da ein erfahrener niedersächsischer Beamter, der auch einige Jahre meiner Geschäftsstelle angehörte, Referatsleiter für Datenschutz und später Landesbeauftragter in Magdeburg geworden ist.

4. Entwicklungen und Probleme der Informations- und Kommunikationstechnik in Verwaltung und Wirtschaft

4.1 Stand der automatisierten Datenverarbeitung

Die sprunghafte Entwicklung der Informations- und Kommunikationstechnik (IuK-Technik), die ich schon in meinem X.Tätigkeitsbericht dargestellt habe, geht ungebrochen weiter. IuK-Technik hat praktisch in jedem Büro, in jedem Betrieb und jedem Haushalt Einzug gehalten. Miniaturisierung und Verbilli-

gung der Mikroelektronik führen zu einem verstärkten Technik-Einsatz in Wirtschaft und Verwaltung; die Vollausstattung aller Büroarbeitsplätze erscheint zunehmend möglich. Wachsender Technik-Einsatz macht jedoch Wirtschaft und Verwaltung verletzlich. Ein Stromausfall oder Anschläge auf zentrale Rechenzentren, Verseuchung von Rechnern oder gar Rechnernetzen mit Computerviren oder sonstige Katastrophen gefährden die Funktions- und Handlungsfähigkeit von IuK-Betreibern und -Nutzern. So kann z.B. nach Expertenmeinung ein 24-Stunden-Ausfall von Rechnersystemen im Banken- oder Versicherungsbereich dort den wirtschaftlichen Ruin verursachen.

IuK-Technik ist begleitet von einer wachsenden Informationsflut. Dies beschleunigt den Trend zur Informationsgesellschaft. Die technologische Entwicklung bewirkt jedoch nur dann Informationsgleichheit, wenn alle Beteiligten über gleiche Zugangsmöglichkeiten zu den Informationsquellen verfügen. Das ist mit verstärktem Technik-Einsatz weniger als bei konventionellen Quellen gewährleistet.

IuK-Technik bewirkt neue Gefahren für die Sicherung des informationellen Selbstbestimmungsrechts und stellt damit eine Herausforderung für den Datenschutz dar. Dies läßt sich wie folgt beschreiben:

— Neben oder anstelle der papiermäßigen Aufzeichnung tritt die elektronische Speicherung von Daten. Dadurch entstehen redundante, also mehrfach nebeneinander vorhandene, oder neue Datensammlungen. Der Speicherumfang nimmt zu.

— Lokale Netzwerke (Local Area Networks — LAN) und Telekommunikationsdienste ermöglichen den Zugriff auf gespeicherte Daten unabhängig vom Ort der Speicherung. Mit zunehmender Vernetzung wird die strenge Kanalisation von Informationsflüssen aufgehoben. Ihre Kontrollierbarkeit nimmt ab.

— Die klassische Datenerfassung mittels Tastatur wird durch optische und akustische Verfahren der Datenerhebung ergänzt und vereinfacht. Dadurch wird die Speicherungs- und Nutzungsbereitschaft selbst in „Technik-Nischen" geweckt. Vollständige Speicherung ermöglicht bisher faktisch unmögliche Nutzungen und regt neue Auswertewünsche an.

— Datenbestände und ihre Methoden der Auswertung werden in integrierten Systemen zusammengefaßt und ohne Aufwand miteinander verknüpfbar gemacht. Dies weckt neue Begehrlichkeiten.

— Auch unstrukturierte Informationen (freie Texte) lassen sich inhaltlich auswerten. „Künstliche Intelligenz" ermöglicht sogar die Überwachung und Erschließung des gesprochenen Wortes sowie stehender und bewegter Bilder.

— „Expertensysteme" mit Lernfähigkeiten können Sachverhalte selbständig bewerten und Entscheidungen treffen, ohne daß eine „menschliche Sachbearbeitung" beteiligt sein muß.

Automatisierte „Bürokommunikation" und „Vorgangsbearbeitung" sind die Trendsetter der gegenwärtigen IuK-Planungen und -Neueinsätze. Damit werden bisherige Nischen der Automatisierten Datenverarbeitung (ADV) erschlossen und bisher konventionelle Büroarbeitsplätze technisiert. Dabei werden die klassischen Großrechnersysteme verlassen und eine größere Anzahl kleinerer, untereinander vernetzter Computer verbunden. Im Fachjargon spricht man von „Downsizing" und verspricht größere Effektivität, Flexibilität und Kostenersparnis. Erklärtes Ziel der Projektbetreiber ist es, der Bearbeite-

rin und dem Bearbeiter alle Entscheidungskriterien sowie alle Werkzeuge für die Verwaltungsaufgabe direkt am Arbeitsplatz verfügbar und damit die Verwaltung insgesamt leistungsfähiger zu machen.

Gespräche mit IuK-Einsteigerinnen und -Einsteigern zeigen, daß bei den Stichworten „Datenschutz und Datensicherung" Unkenntnis und Verwunderung vorherrschen. Eine Datenschutz-Relevanz wird vielfach nicht gesehen, „da ja nur Texte verarbeitet würden, zugegeben jetzt mit IuK-Unterstützung". Unklar ist oft, daß auch die Textverarbeitung in einem Bürokommunikationssystem als eine dateimäßige Verarbeitung personenbezogener Daten im Sinne des modernen Datenschutzrechts anzusehen ist. Unklar ist oft auch, daß Systemdateien von Betriebssystemen bzw. von Bürokommunikationssystemen klassische Dateien im Sinne des Datenschutzrechts sind, die auch sensitive Betroffenendaten enthalten können, mit denen z.B. Leistungs- und Verhaltenskontrollen durchgeführt werden können (z.B. Namen der betroffenen Bürgerinnen und Bürger, der Autorinnen und Autoren von Texten, der Erfasserinnen und Erfasser, Datum, Uhrzeit, Veränderungen, Auswertungen).

Bürokommunikationssysteme bieten einen „elektronischen Schreibtisch" mit den Funktionen Textverarbeitung, Graphik, Aktenablage, Dokumentenverwaltung, Datenbanken, Tabellenkalkulation, elektronische Post für interne und externe Kommunikation sowie Informationsbeschaffung aus zentralen Informationssystemen. Dabei wird jedem Benutzer die Auswahl und Verwendung der Funktionen des Systems selbst überlassen. Gespeichert und übermittelt werden eine Vielzahl formatierter und unformatierter personenbezogener Daten, z.B. Gesprächsprotokolle, Telefonverzeichnisse, Telefonnotizen, Antragsunterlagen, Verwaltungsentscheidungen, Adressen für wiederkehrende Verteiler, personenbezogene Dateien. Dies sind häufig sensible personenbeziehbare Informationen, mitunter auch mit politischer Brisanz. Deren Speicherung, Nutzung und Übermittlung können einen tiefen Eingriff in das informationelle Selbstbestimmungsrecht Betroffener bewirken.

Vorgangsbearbeitungssysteme unterstützen die Bearbeiterin und den Bearbeiter bei der ordnungsgemäßen Abwicklung von komplexen Fachaufgaben. Hierbei werden Hilfen für die in einem Arbeitsschritt auszuführenden Aufgaben angeboten. Die einzelnen Arbeitsschritte werden durch steuernde Elemente miteinander verbunden. Vorgangsbearbeitungssysteme bieten den Benutzerinnen und Benutzern Vorschläge für die Art der Bearbeitung an, z. B. durch eine Auswahl von definierten Bürofunktionen. Die Bearbeitungswerkzeuge entsprechen denen der Bürokommunikation; auch ein Datenbanksystem ist in aller Regel integriert. Gespeichert und längerfristig archiviert wird nicht nur die Tatsache der Kontakte zwischen Verwaltung sowie Bürgerinnen und Bürgern; gespeichert werden auch die Antragsdaten sowie die gesamten Kommunikationsinhalte. Es gibt auch schon Versuche einer papierlosen Aktenführung. Überwiegend rechtliche Probleme bei der Frage der Dokumenten-Echtheit und der elektronischen Unterzeichnung von Dokumenten hindern derzeit noch die schnelle Einführung des „papierlosen Büros".

Die aufgezeigten Technik-Anwendungen und -Möglichkeiten verändern nicht nur unseren Arbeitsplatz; sie wirken auch in unsere Privatsphäre hinein. Wirtschaft und Verwaltung entwickeln neue Kommunikations- und Entscheidungswege. Der Umgang mit Bürgerinnen und Bürgern vollzieht sich nach neuen Regeln und in neuen Formen. IuK-Technik bietet dabei nicht nur Verbesserungschancen für alle Betroffenen, sondern führt fast zwangsläufig zu neuen Gefahren und Folgen für den Datenschutz, wie die folgenden Beispiele zeigen:

— Wachsende Digitalisierung führt zu Benutzerprofilen, so z. B. die Benutzungsdaten der Telekommunikation, die elektronisch vollzogenen Zahlungen, die Protokollierung von Benutzer-Aktivitäten am Computer. Damit wird das Verhalten von Nutzerinnen und Nutzern sowie Betroffenen potentiell durchsichtig, kontrollierbar und manipulierbar.

— „Bürokommunikationssysteme" speichern die Kommunikationsinhalte zwischen Verwaltung, Unternehmen sowie Bürgerinnen und Bürgern. Auch die ankommende Papier-Post kann und wird heute elektronisch gespeichert und auswertbar gemacht.

— Die zunehmende Vernetzung von Unternehmens- und Verwaltungsbereichen ermöglicht es leichter als jemals zuvor, die gespeicherten Daten auch für „artfremde" Zwecke zu nutzen, ohne daß dies wirksam kontrolliert werden kann.

— Wachsende Informationsflut führt nicht zwangsläufig zu einer informierten Gesellschaft, da relevante Informationen häufig nur wenigen „Berechtigten" zugänglich sind. Dies kann auch die verfassungsrechtliche Gewaltenteilung von Exekutive und Legislative beeinflussen.

Das Niedersächsische Datenschutzgesetz von 1978 konnte diese Technik-Revolution nicht vorhersehen und hat deshalb auch keine befriedigenden Antworten auf die Technik-Herausforderungen gegeben. Wie bei allen Datenschutzgesetzen der ersten Generation war das NDSG-Konzept auf das Verhindern von Mißbrauch ausgerichtet; materiellrechtliche Regelungen bestehen aus Geboten und sanktionsbewehrten Verboten. Demgegenüber versuchen die Datenschutzgesetze der zweiten Generation feste Regeln für den Umgang mit personenbezogenen Daten zu geben und Generalklauseln zu vermeiden, so z. B. Regeln für das Erheben und Nutzen personenbezogener Daten, die Zweckbindung erhobener Daten, besondere Absicherungen bei Abrufberechtigungen von Dritten.

Der jetzt dem Landtag vorliegende Entwurf eines völlig überarbeiteten NDSG folgt dem Konzept neuerer Landesdatenschutzgesetze, ohne jedoch dabei neue und konkretere Antworten auf die Technik-Herausforderungen zu geben. Zwar enthält der Entwurf Verbesserungen zur Technikkontrolle in der Entwurfs-Fassung (so z. B. die sanfte Anpassung der Datensicherheitsmaßnahmen in § 7 NDSG, die Notwendigkeit der laufenden Überprüfung und Anpassung der Sicherungskonzepte „nach dem Stand der Technik" in § 7 NDSG, weitergehende Dokumentationspflichten in § 8 NDSG und die Abruf-Regelung in § 12 NDSG), doch reicht das bisherige Konzept mittelfristig nicht aus, um den neuen Risiken der IuK-Technik zu begegnen.

Die zunehmende Verbreitung von Personal Computern (PC) und deren Vernetzung zu umfassenden Rechnernetzen, der Einsatz von tragbaren Geräten im Außendienst (Laptop), die Verwendung von privaten PC für dienstliche Zwecke durch Lehrer, Richter, Polizei- und Finanzbeamte, die „Bürokommunikation der Ministerien (BÜROMIN)", der „Einsatz der IuK-Technik bei den Bezirksregierungen (IuK-Reg)", das „Landesinformationssystem (LIS)", das „Telekommunikationssystem der Niedersächsischen Landesregierung (KOMNET)" und das „Telekommunikationssystem der Niedersächsichen Landesverwaltung (TELENET)" bedürfen verfahrensmäßiger Regelungen, die eine notwendige Risikoabschätzung in diesen Bereichen nahezu unbegrenzter Möglichkeiten der Informationsverarbeitung vorschreiben, die die verschiedenen Phasen der Entwicklung, Prüfung und Freigabe von Informationssystemen unter Beteiligung einer interessierten Öffentlichkeit festlegen und die Kontrollierbarkeit des Verfahrenseinsatzes ermöglichen.

Das Bundesverfassungsgericht hat im Volkszählungsurteil die Forderung an den Gesetzgeber erhoben, „mehr als früher auch organisatorische und verfahrensrechtliche Regelungen zu treffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenwirken". Ich bin mir bewußt, daß ein solches Technikrecht sehr flexibel angelegt sein muß, um einer sich dynamisch verändernden Technik gerecht zu werden. Ich räume weiter ein, daß es derzeit für ein vergleichbares Technikrecht allenfalls Ansätze gibt, so z.B. im Entwurf eines „Gesetzes über den Einsatz der Informationstechnik in der Berliner Verwaltung — IT-Gesetz" oder in der Verordnungs-Verpflichtung der Landesregierung in § 7 Abs. 4 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen.

Gleichwohl halte ich mit Blick auf die Zukunft insbesondere die Einführung einer Technikfolgenabschätzung, eine Lizenzierungspflicht für Hard- und Software bei sensitiven Anwendungen (vgl. 4.2) sowie Voraussetzungen und Aufgaben einer Systemverwaltung und Wartung von IuK-Systemen (vgl. 4.3) für regelungsbedürftig. Um Möglichkeiten zum Überprüfen und Nachbessern solcher Regelungen zu erhalten, sollte nach einer Erprobungszeit über Anwendungserfahrungen berichtet und die Regelungen überprüft werden.

Für den NDSG-Entwurf empfehle ich, in Verwaltungs-Vorschriften die technischen und organisatorischen Maßnahmen nach § 7 Abs. 2 NDSG-E zu konkretisieren sowie Prüfungs-, Freigabe- und Dokumentationspflichten festzuschreiben.

4.2 Technikfolgenabschätzung und Lizenzierung

4.2.1 Der Kontext

Da Datenverarbeitungs-Regelungen — wie beschrieben — äußerst schwierig bestimmbar sind und als alleinige Verarbeitungsschranke immer weniger taugen, muß insbesondere bei der Gestaltung der Technik angesetzt werden. Der Hessische Datenschutzbeauftragte hat dies sehr bildhaft dargestellt: „Fernkopierer ohne eine den Datenschutz garantierende Ausrüstung dürfen genauso wenig auf den Markt kommen wie Autos ohne Bremsen" (18. TB S. 17). Doch wo gibt es den „TÜV", der das überprüft, und wie sollte das geregelt werden?

In der öffentlichen Verwaltung Niedersachsens sollten die „speichernden Stellen" bzw. die Betreiber von IuK-Projekten verpflichtet werden, vor der Entscheidung über die erstmalige Einrichtung oder die wesentliche Änderung eines automatisierten Verfahrens eine Technikfolgenabschätzung vorzunehmen. Hierzu könnte der Untersuchungsbericht, deren Erstellung die IuK-Technik-Grundsätze vor Einführung eines IuK-Verfahrens vorschreiben, um die Komponente „Risikoanalyse" erweitert werden. Es sollte Pflicht werden, die Risiken des geplanten IuK-Systems abzuschätzen und zu bewerten sowie mögliche Alternativen zu entwerfen. Die Unterstützung durch externe Sachverständige wäre denkbar und wünschenswert. Auch ich biete meine Mithilfe an.

Im nicht-öffentlichen Bereich ist ausreichender Datenschutz zunehmend ein Wettbewerbs-Argument. Das Ergebnis einer eigenen Technikfolgen-Abschätzung und -Bewertung könnte durchaus in die Produkt- und Service-Werbung eingebracht werden. Darüber hinaus sollte die Sicherung von Firmengeheimnissen besondere Motivation für eine Technikfolgenabschätzung sein.

Ein besonderes Gewicht bei der Festlegung von Sicherheitskriterien für IuK-Systeme sowie der Prüfung und Bewertung der Implementierungsqualität von ausgewählten Lösungsvarianten dürften neutrale Validierungsstellen gewinnen. Eine solche Stelle könnte in einem Lizensierungs- und Genehmigungsverfahren überprüfen und sicherstellen, ob für die IuK-Systeme jeweils festzulegende Mindeststandards gewährleistet sind. Hierfür käme das Bundesamt für Sicherheit in der Informationstechnik (BSI) in Betracht, das 1991 gegründet worden ist. Das BSI hat u.a. die Aufgabe, Produkte und Systeme der Informationstechnik zu überprüfen und zu zertifizieren. Die Vorgängerbehörde des BSI hatte dazu schon die „IT-Sicherheitskriterien" erarbeitet und veröffentlicht sowie ein IT-Evaluationshandbuch herausgebracht. Die BSI-Konzepte sind inzwischen in die „EG-einheitlichen Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik — ITSEC", die am 15. Juli 1992 durch den Bundesminister des Innern bekanntgemacht worden sind (GMBl. 1992 S. 545 ff.) eingeflossen. Zu ITSEC gehört das „Information Technology Security Evaluation Manual — ITSEM", das zunächst in einem Entwurf vorliegt. ITSEC und ITSEM sind die gegenwärtigen Prüfgrundlagen für das BSI. Um sie über die EG hinaus zum internationalen Prüfstandard zu machen, sind sie in den Normungsprozeß bei der International Standardisation Organisation (ISO) eingebracht worden. Damit würde das bisher in den USA verwendete „Orange Book", das in Kanada abgewandelte „Orange Book" und das „Blue Book" der NATO vereinheitlicht.

Die kurze Darstellung des derzeit bestehenden Instrumentariums läßt ein Problem deutlich werden: Für die Nichtfachleute sind die technischen Begriffe, Institutionen, Abkürzungen, Regelungskonzepte und Verfahren kaum mehr zu überblicken und zu durchschauen. Es besteht die Gefahr, daß Sicherheit in der Informationstechnik zum Steckenpferd einiger weniger Experten wird. Dies kann aber nicht im Sinne des Datenschutzes in einer demokratischen Gesellschaft sein. Interessierte Bürgerinnen und Bürger sowie Politik und Verwaltung, sind aufgerufen, sich mit Fragen der Risiken der Informationstechnik und dem zur Verfügung stehenden Instrumentarium stärker vertraut zu machen.

4.2.2 Folgerungen für Niedersachsen

Für die öffentliche Verwaltung Niedersachsens sollte mittelfristig zumindest bei sensitiven Anwendungen (mit besonderer Eingriffstiefe) eine Lizenzierungspflicht erwogen werden. Eine solche Prüfung und Zertifizierung von allgemeinen Produkten, wie z. B. bestimmten Standardprogrammen, Betriebssystemen, Datenbanken, speziellen Hardware-Einrichtungen erfolgt derzeit durch das BSI. Auch Zertifikate vergleichbarer internationaler Einrichtungen sollten anerkannt werden.

Anders ist dagegen die Prüfung und Bewertung der gesamten Einsatzumgebung zu sehen. Hierbei sind sowohl die bauliche Situation, die technischen Sicherheitsanforderungen als auch die personellen Besonderheiten einer konkreten IuK-Anwendung zu betrachten. Das BSI wäre bei einer so umfangreichen Inanspruchnahme überfordert. Für diese umfassende Prüfung und Bewertung von IuK-Verfahren der öffentlichen Verwaltung Niedersachsens wäre an eine Landeslösung zu denken, z. B. eine besondere Prüfgruppe aus Vertreterinnen und Vertretern der Verwaltung, Mitgliedern der Personalvertretung sowie wissenschaftlichen Sachverständigen. Die Prüfgruppe könnte beim Niedersächsische Landesverwaltungsamt angesiedelt werden. Vertreterinnen und Vertreter von gesellschaftlichen Interessenverbänden könnten in einer öffentlichen Diskussion und bei der politischen Bewertung von neuen IuK-Verfahren einbezogen werden. Auch ich biete meine aktive Beteiligung an.

Die in einem solchen Prüfverfahren festgestellten Mängel wären abzustellen. Meine späteren Kontrollen würden deren Einhaltung sicherstellen, meine sonstigen Kontrollpflichten würden dadurch erleichtert. Die Lizenzierung könnte auch Berichtspflichten nach Erprobungsphasen umfassen, um so Rückbezüge und Korrekturen zu ermöglichen. Präventiver Datenschutz, größere Transparenz und Akzeptanz wären die großen Vorteile dieser neuen Technikfolgenabschätzung und der Technikprüfung.

4.3 Systemverwaltung und Wartung

Bei allen IuK-Systemen — gleich ob PC-Netz, UNIX-Anlage (vgl. 4.5 und X 4.4), ISDN-fähige Nebenstellenanlage oder Großrechner — sind an Systemverwaltung und Wartung hohe Anforderungen hinsichtlich Fachkunde und Zuverlässigkeit zu stellen. Mit diesen Aufgaben Betraute haben umfassende Zugangsrechte zu allen Geräten. Die Systemverwalter haben Zugriffsrechte auf sämtliche Ressourcen; sie können zumeist Dateien lesen und verändern; sie können die Zugriffsrechte auf sie und die Eigentumsrechte an ihnen verändern; sie können die Systeminformationen über Dateien manipulieren, die Paßwort-Datei bearbeiten, Benutzerinnen bzw. Benutzer hinzufügen oder sperren sowie deren Berechtigungen verändern. Die Möglichkeiten der Systemverwalter sind praktisch unbegrenzt; sie sind kaum kontrollierbar, denn selbst die Systemprotokolle können von ihnen verändert oder gelöscht werden. Da die meisten datenverarbeitenden Stellen zur Eigen-Wartung ihrer IuK-Technik nicht in der Lage sind, da ausreichend geschultes Personal fehlt, bedienen sie sich externer Wartungstechniker oder gar externer Spezialisten in Fernwartungs-Zentralen, die in der ganzen Welt verteilt sein können. Diese Fachleute verfügen fast immer über umfassendere Systemkenntnisse und Anwendungserfahrungen als eigene Bedienstete; eine durchgreifende Kontrolle der Fremdarbeiten dürfte selten sein. Dabei ist umstritten und nicht abschließend geklärt, wie der Umgang mit personenbezogenen Daten bei externen Systembetreuern und Wartungstechnikern datenschutzrechtlich zu bewerten ist. Unstreitig ist aber, daß

- Systemverwaltung und Wartung zwingend erforderlich sind, um die Funktionalität eines Informations- und Kommunikations-Systems (IuK-System) zu erhalten,
- die reine Hardware-Wartung datenschutzrechtlich unbedenklich ist,
- die Offenbarung von personenbezogenen Daten an Wartungsstellen mitunter die einzig praktikable Möglichkeit ist, Fehler zu diagnostizieren und zu beheben und
- der Umgang mit personenbezogenen Daten anläßlich einer Wartung eine datenschutzlich relevante Verwendung von Daten ist.

Ich stufe in Übereinstimmung mit dem Niedersächsischen Innenministerium die (Fern-)Wartung als besondere Verarbeitung bzw. Nutzung im Sinne des Datenschutzrechts ein. Auch wenn Software-Wartung grundsätzlich nicht zu einem Zugriff auf personenbezogene Daten berechtigt, kann dies dennoch im Einzelfall erforderlich sein, um den ordnungsgemäßen Betrieb eines IuK-Systems zu gewährleisten bzw. wiederherzustellen. Software-Wartung kann dabei zu einer Beeinflussung des Kontextes personenbezogener Daten führen und somit verändernd wirken. Einen lesenden Zugriff auf personenbezogene Daten zu Wartungszwecken sehe ich als eine „Nutzung" im Sinne von § 3 Abs. 2 Nr. 7 NDSG-E an. Ich ordne daher — wie auch schon in der Vergangenheit — Wartungsarbeiten durch Fremdkräfte (gleich ob Wartung vor Ort oder Fernwartung) datenschutzrechtlich der Auftragsdatenverarbeitung zu.

Wegen der besonderen Risiken der Systemverwaltung und Wartung würde ich eine Rechtsvorschrift begrüßen, die das Erfordernis besonderer persönlicher Zuverlässigkeit des Systemverwalters bzw. der Wartungskräfte, eine Verpflichtung zur vollständigen Kontrolle der Systemarbeiten und besondere Dokumentationspflichten umfaßt.

4.4 Personal Computer, Laptop und Notebook

Wiederholt habe ich auf Datenschutz- und Datensicherungsprobleme beim Einsatz von Personal Computern (PC) hingewiesen. Unter X 4.5 habe ich aktuelle Probleme beschrieben und besondere Sicherungsmaßnahmen vorgestellt. PC-Sicherheit hat auf Fachmessen und Symposien auch weiterhin Konjunktur. Die Aussage der Datenschutzbeauftragten des Bundes und der Länder hinsichtlich stationärer Anlagen in ihrer Entschließung vom 10. Oktober 1988, „...auf den Einsatz von PC und kleinerer Datenverarbeitungsanlagen muß verzichtet werden, wenn die Datensicherheit mit den verfügbaren Maßnahmen nicht im erforderlichen Umfang gewährleistet werden kann...", muß in der öffentlichen Verwaltung immer weniger in Erinnerung gerufen werden.

In Verwaltung und Wirtschaft läßt sich nun aber ein deutlicher Trend hin zu mobilen IuK-Geräten (z.B. Notebooks, Laptops) erkennen. Besonders die „Schoßhündchen" — wie man laptop aus dem englischen Ursprung lap dog wörtlich übersetzen müßte — erfreuen sich großer Verbreitung. Auch bei Laptops sind grundsätzlich die gleichen Gefahren wie beim Einsatz von Personal Computern abzusichern. Das besondere Risiko beim mobilen Einsatz sehe ich im Diebstahl und im unbeabsichtigten Verlust. Während beim Einsatz in herkömmlicher Büroumgebung der Zugang zu den Geräten gesichert werden kann, verlassen beim mobilen Einsatz von Laptops sowohl die Daten als auch das Gerät den Kontrollbereich der Behörde oder des Unternehmens. So kann ein Laptop im Auto vergessen oder in einem Sitzungssaal unbeaufsichtigt liegengelassen werden. Bereits ein kurzfristiger Zugriff bietet vielfältige Gelegenheiten zur unbefugten Kenntnisnahme schutzwürdiger Daten. Mißbrauchsgefahren bestehen nicht nur in unbefugtem Lesen (Verlust der Vertraulichkeit), sondern auch durch unbefugte Modifikation von Daten (Verlust der Integrität) und in der Beeinträchtigung der Funktionalität (Verlust der Verfügbarkeit, z. B. durch das Einschleusen von Viren, trojanischen Pferden o. ä.). Deshalb sollten zum Mindest-Standard dieser Geräte Hardware-Sicherungen gegen Manipulationsversuche (z .B. durch Verplombung des Rechners) sowie Software-Sicherungen gegen das unberechtigte Lesen, Entwenden oder Manipulieren von zu schützenden Daten (z. B. Paßwortkontrolle, Verschlüsseln der Daten, Protokollierung der Benutzer-Aktivitäten) verpflichtend eingeführt werden.

Ein weiteres Problem ist der Einsatz von privateigenen Personal Computern. Eine derartige „Privatisierung" öffentlicher Aufgabenerledigung kann nur schwer unter Kontrolle gehalten werden, das Risiko des Datenmißbrauchs durch Dritte wird in besonderem Maße erhöht. Auch wenn bzw. gerade weil ein ausnahmsloses Verbot von privateigenen IuK-Geräten bisher nicht realistisch erscheint, trete ich grundsätzlich für ein Verbot mit Erlaubnisvorbehalt ein. Der Einsatz könnte im Ausnahmefall bereichsspezifisch ausdrücklich geregelt werden. Hierbei müßte festgeschrieben werden, daß der Einsatz privateigener PC nur bei unabweisbarem dienstlichem Bedürfnis zugelassen ist, daß der Einsatz der Genehmigung durch die Leitung der speichernden Stelle bedarf, daß Meldepflichten einzuhalten sind und daß der Einsatz der Kontrolle auch im privaten Bereich unterliegt. Weiter sollte klargestellt werden, daß das NDSG (einschließlich der Regelungen über das Datengeheimnis und der Vorschriften über die technischen und organisatorischen Sicherheitsmaßnahmen) anzuwenden ist (vgl. 4.6.8, 4.6.9 und 27.9).

Das Innenministerium plant, die Nutzung von privaten PC im Bereich der Landespolizei neu zu regeln. Die geplante Erlaßregelung enthält ein grundsätzliches Verbot der Nutzung privater PC mit restriktiven Ausnahmetatbeständen, eine ausdrückliche Genehmigung der Dienststelle mit Beteiligung der dort für den ADV-Einsatz und den Datenschutz zuständigen Stellen, ein Vernetzungsverbot, die Pflicht zur Datensicherung, die dem Stand der Technik entsprechen muß, und Dokumentationspflichten. Auf meine Frage nach der dienstlichen Erforderlichkeit der Nutzung privater PC hat das Innenministerium geantwortet, daß die Haushaltslage des Landes nur ein Drittel der erforderlichen Anschaffungen an Bildschirmarbeitsplätzen zulasse und deshalb die private Initiative notwendig sei. Sie sei geeignet, durch rationelle und effektive Arbeitsweise am einzelnen Arbeitsplatz die Kriminalitätsbekämpfung und Gefahrenabwehr zu fördern. Bis zum Frühjahr 1992 waren bereits mehr als 200 private PC gemeldet und genehmigt. Ich halte meine grundsätzlichen datenschutzrechtlichen Bedenken aufrecht.

4.5 UNIX

Die unter Ziffer 4.1 aufgezeigten Trends in der IuK-Technik zeigen bei Mehrplatzsystemen eine deutliche Hinwendung zu UNIX als Betriebssystem. UNIX ist ein offenes System, das auf Rechnern unterschiedlichster Herstellerfirmen betreibbar ist. Die Zahl der UNIX-Neuinstallationen ist wohl aus diesem Grund sprunghaft angestiegen. Ein weiterer Zuwachs wird aus Expertensicht erwartet.

Meine unter X 4.4 gegebenen Hinweise auf Sicherungs-Schwachstellen gelten uneingeschränkt fort. Zwar bietet UNIX eine Vielzahl an datenschutzrelevanten Sicherungsmöglichkeiten, doch können die Sicherheits-Optionen bei nachlässiger Anwendung auch gravierende Sicherheitsrisiken auslösen. Ich wiederhole noch einmal meinen Hinweis, daß die Systemverwaltung von entscheidender Bedeutung für die Funktionsfähigkeit und für die Sicherheit eines UNIX-Betriebs ist. Die Systemverwaltung ist neben den Sicherheitsrisiken bei einer UNIX-Vernetzung die größte Schwachstelle aus der Sicht des Datenschutzes. Daher ist auf Qualifikation, Zuverlässigkeit und Schulung der Systemverwalterin bzw. des Systemverwalters besonderes Augenmerk zu legen. Die Systemverwaltung bei Einsatz eines UNIX-Systems muß personell so ausgestattet werden, daß genügend Zeit zur Verfügung steht, um Datenschutz- und Datensicherungsmaßnahmen in ausreichendem Maße und mit ausreichender Sorgfalt planen und durchführen zu können. Die Einhaltung der Datenschutz- und Datensicherungsgebote muß unbedingt kontrolliert werden.

Trotz dieser Probleme ist bei UNIX-Systemen ein recht hoher Sicherheitsstandard möglich, wenn die Systeme entsprechend konfiguriert werden. Hierfür bedarf es gerade bei diesem Betriebssystem einer sorgfältigen Abarbeitung aller relevanten Punkte. Um Systemverwalter und Datenschutzbeauftragte hierbei zu unterstützen, habe ich eine Orientierungshilfe für den Betrieb von UNIX-Systemen in Form eines Prüfkonzeptes erstellt.

Das UNIX-Prüfkonzept besteht aus einer Zusammenstellung einzelner Fragen und Forderungen, die während einer behörden- bzw. unternehmensinternen Prüfung abgearbeitet werden könnten. Die Ergebnisse der Prüfung werden durch Ankreuzen in der Prüfliste festgehalten, so daß am Ende eine Liste der notwendigen Nachbesserungen vorliegt. In der Prüfliste werden Maßnahmen zur Benutzerverwaltung angesprochen, wobei im wesentlichen zwischen der Systemverwaltung, den Benutzern mit und den Benutzern ohne Zugriff auf die Betriebssystem-Ebene unterschieden wird. Besondere Beachtung finden

die Systemverwaltung, der Zugriffsschutz durch Paßwort, die Dateiverwaltung, das Zugriffsrecht auf Dateien, die Verschlüsselung und Protokolldateien. Ein weiteres, sehr wichtiges Kapitel behandelt die Netzverwaltung, wobei Maßnahmen zu lokalen Netzen und zu Fernübertragungen unterschieden werden. Schließlich werden Maßnahmen zur Gerätesicherung und zur Datenträgerkontrolle behandelt.

Auch das UNIX-Prüfkonzept geht — wie von mir seit langem bei anderen IuK-Techniken praktiziert — von einem Schutzstufenkonzept aus. Danach werden die personenbezogenen Daten nach dem Grad möglicher Beeinträchtigung schutzwürdiger Belange in fünf Kategorien eingeteilt:

Schutzstufe A — frei zugängliche Daten,
Schutzstufe B — Daten mit geringem Mißbrauchsrisiko,
Schutzstufe C — Daten, deren Mißbrauch die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse beeinträchtigen kann,
Schutzstufe D — Daten, deren Mißbrauch das Ansehen oder die wirtschaftlichen Verhältnisse erheblich beeinträchtigen kann,
Schutzstufe E — Daten, deren Mißbrauch Gesundheit, Leben oder Freiheit der Betroffenen beeinträchtigen kann.

Je höher die Schutzstufe liegt, desto höhere Ansprüche sind auch an die technische Sicherheit zu stellen.

Das UNIX-Prüfkonzept wurde im Rahmen des Projektes BÜROMIN der niedersächsischen Ministerien (vgl. 4.6.2) erstellt und bereits praktisch erprobt. Die Endbearbeitung ist nach einer weiteren Erprobungszeit 1993 geplant. Interessierte können das Prüfkonzept bei mir anfordern.

4.6 Automation in der Landesverwaltung

4.6.1 Automatisierte Stellenbewirtschaftung (ASTEB)

Das verwaltungsgerichtliche Streitverfahren um die Frage notwendiger Mitbestimmung nach § 80 a Nds. PersVG bei Einführung der automatisierten Stellenbewirtschaftung in den Schulabteilungen der Bezirksregierungen hat durch zwei Beschlüsse des OVG Lüneburg (beide vom 26. August 1991, Az.: 18 L 4/90 sowie 18 L 2/90) sein vorläufiges Ende gefunden (vgl. auch VIII 4.4, 4.6, IX 15.2 u. X 4.6).

Das Gericht verneinte, daß die vom Kultusministerium geplante automatisierte Stellenbewirtschaftung ein automatisiertes Verfahren zur Vorbereitung oder zum Vollzug personalrechtlicher Maßnahmen darstelle, dessen Einführung der Mitbestimmung des Personalrates nach § 80 a Nds. PersVG unterliege. Nach dem Willen des Gesetzgebers sei ein Mitbestimmungsrecht noch nicht gegeben, wenn ein elektronisches Datenerfassungssystem — wie hier — die Dienststelle nur in die Lage versetze, aus den gewonnenen Daten Folgerungen für Personalmaßnahmen zu ziehen, ohne daß solche Maßnahmen durch das Verfahren unmittelbar vorbereitet oder vollzogen würden. Auch mache § 80 a dieses Gesetzes die jeweiligen Personalvertretungen nicht zu Datenschutzbeauftragten, die in umfassender Weise die Interessen der von ihnen vertretenen Bediensteten wahrzunehmen hätten.

Das Gericht stellte weiter fest, daß die Entscheidung zum Einsatz des automatisierten Verfahrens in bezug auf die zu speichernden Daten und deren geplante Nutzung nach dem Nds. PersVG mitbestimmungspflichtig ist, nicht jedoch die (programmgemäße) Speicherung von Einzeldaten.

4.6.2 Bürokommunikation in den Ministerien (BÜROMIN)

Das Pilotprojekt BÜROMIN umfaßt das Innenministerium, das Ministerium für Wirtschaft, Technologie und Verkehr sowie das Frauenministerium. Im Innenministerium befinden sich 66 untereinander vernetzte Arbeitsplatzrechner (UNIX-Workstation), im Wirtschaftsministerium sind es 56. Zusätzlich ist das Frauenministerium mit 6 isolierten UNIX-PC ausgestattet. Als Anwendungsprogramm wird an allen Rechnern der angeschlossenen Ministerien das Bürokommunikationssystem ALIS eingesetzt. Zusätzlich wurde im Wirtschaftsministerium örtlich begrenzt das Datenbanksystem ORACLE installiert. Auch meine Geschäftsstelle hat sich seit Anfang 1992 zunächst mit einem Testgerät, ab Mitte des Jahres mit sechs weiteren Arbeitsplatzrechnern aktiv am BÜROMIN-Versuch beteiligt. Damit wurde bei mir die vorhandene Textverarbeitungsanlage abgelöst und zugleich die für meine Prüfaufgabe im Projekt BÜROMIN erforderliche Testumgebung geschaffen.

Im Oktober 1992 habe ich eine Prüfung der Datenschutz- und Datensicherungsmaßnahmen im Innenministerium durchgeführt. Meine folgenden Beschreibungen und Bewertungen beziehen sich auf diese Prüfung; sie sind aber auch auf die anderen Versuchsfelder übertragbar.

Mit BÜROMIN werden personenbezogene Daten dateimäßig verarbeitet; deshalb sind Vorkehrungen und Regelungen für die Bereiche Datenschutz und Datensicherung zu treffen. Hierbei sind rechtliche, organisatorische, technische und bauliche Aspekte zu beachten. Auch in einem Bürokommunikationssystem muß das Organisations-Prinzip lauten: „Verboten ist, was nicht ausdrücklich erlaubt ist". Dabei ist grundsätzlich zu gewährleisten, daß

1. die Informationsverarbeitung nach für den Betroffenen erkennbaren Regeln erfolgt,
2. Verstöße gegen die informationelle Selbstbestimmung verhindert werden,
3. die Informationsverarbeitung nicht zu einer unangemessenen Kontrolle des Verhaltens und der Leistung der mit ihr beauftragten Bediensteten führt.

Eine Abschätzung der Sensitivität der im Innenministerium bearbeiteten personenbezogenen Daten führt derzeit zu einer Einordnung bis maximal zur Schutzstufe C (Gefährdung des Ansehens) des von mir verwendeten Schutzstufenkonzepts (vgl. 4.5). Die Prüfung dereinzelnen Kontrollbereiche wurde entsprechend ausgelegt.

Die in BÜROMIN vorhandenen Maßnahmen zum Datenschutz und zur Datensicherung lassen sich in die drei Teilbereiche Betriebssystem, Programm sowie bauliche und organisatorische Datensicherungsmaßnahmen gliedern.

Mit dem Projekt BÜROMIN ist ein Bürokommunikationssystem unter dem Betriebssystem UNIX installiert und eingeführt worden, das sich durch folgende Eigenschaften auszeichnet:

— Das Betriebssystem ermöglicht einen benutzerbezogenen Zugriffsschutz auf das System als Ganzes und auf jede einzelne Datei.
— Das Bürokommunikationssystem grenzt die Arbeitsbereiche der Benutzerinnen und Benutzer wirkungsvoll gegeneinander ab und ermöglicht einen individuellen Zugriffsschutz.
— Der Systembetriebsraum ist abgegrenzt und gesichert, das Lichtwellenleiter-Netz ist ausschließlich in kontrollierten Bereichen verlegt, an den Workstation der Benutzerinnen und Benutzer sind keine Disketten-Laufwerke.

Das Datenschutz- und Datensicherungskonzept war zum Zeitpunkt der Prüfung nicht in vollem Maße umgesetzt worden. So war zu kritisieren, daß die optionalen Schutzmöglichkeiten des Systems nicht hinreichend ausgenutzt und verbleibende Schwachstellen nicht durch zusätzliche Schutzvorkehrungen abgesichert worden sind. So verbleiben vermeidbare Datenschutz-Gefährdungen. Ich habe daher gefordert, daß die folgenden Datenschutz- und Datensicherungs-Forderungen umgehend erfüllt werden:

- Für die Systemverwaltung sind in einer Dienstanweisung Berechtigungen, Befugnisse und Verantwortlichkeiten schriftlich festzulegen. Die Vertretung, der Umgang mit dem Super-User-Paßwort, das Verhalten in Notfallsituationen sind zu regeln.
- Regelungen zur Zugriffskontrolle mittels Paßwort (für alle Benutzerinnen und Benutzer: begrenzte Anzahl an Fehlversuchen, Paßwort-Alterung; für das Super-User-Paßwort: Änderung nach Vertretung, versiegelte Hinterlegung) sind zu treffen und deren Einhaltung systemseitig abzusichern.
- Die datenschutzgerechte Protokollierung und die systematische Auswertung sowie eine Datenschutz-Kontrolle sind umgehend sicherzustellen.
- Sicherungsdatenträger sind gesichert unterzubringen (Schutz gegen Rauch, Feuer, Wasser, Diebstahl).
- Die Betriebssystemebene ist für „normale" Anwender zu sperren.
- Zu allen personenbezogenen Dateien, für die nach § 8 Abs. 1 NDSG-E eine Dateibeschreibung zu erstellen ist, müssen entsprechende Registermeldungen an den Landesbeauftragten für den Datenschutz abgegeben werden (dies gilt nicht für Dateien, die ausschließlich aus verarbeitungstechnischen Gründen vorübergehend vorgehalten werden).
- Die Benutzerdienstanweisung muß überarbeitet werden.
- Für das Innenministerium ist schnellstmöglich eine Datenschutzbeauftragte oder ein Datenschutzbeauftragter zu bestellen. Diese Person muß Kontrollaufgaben und Maßnahmen zur teilweise noch fehlenden Bewußtseinsbildung im Bereich BÜROMIN mit übernehmen; sie sollte entsprechend geschult werden.

Darüber hinaus habe ich eine ganze Reihe weiterer technischer und organisatorischer Maßnahmen zur Ergänzung und Verbesserung des Datenschutzes und der Datensicherheit empfohlen:

- Das Vier-Augen-Prinzip beim Zugriff mit Super-User-Rechten sollte verpflichtend eingeführt werden; bei Daten der Schutzstufe E wäre dies unabdingbar.
- Jeder Benutzerin und jedem Benutzer sollte nach Systemaufruf (Login) das Datum des letzten Login und des letzten erfolglosen Login-Versuches angezeigt werden.
- Die Einführung von Zugriffskontrollverfahren mittels Chipkarte sollte erprobt werden. Insbesondere bei Verarbeitung von Daten ab der Stufe D sollte dies verpflichtend sein.
- Die ausschließlich unverschlüsselte Übertragung von Daten über das Netz stellt einen Schwachpunkt dar; auch Paßwörter werden unverschlüsselt übertragen. Spätestens bei Daten der Schutzstufen D und E sollten Paßwörter und Daten verschlüsselt übertragen werden. Es wird empfohlen, allen benutzenden Personen eine Verschlüsselungsfunktion anzubieten.
- Sämtliche Arbeitsplatzrechner sollten über eine Pausenfunktion verfügen, die vor einem erneuten Zugriff die Eingabe des Paßwortes erzwingt. Diese Pausenfunktion sollte sowohl durch einfache Bedienung (Funktionstastendruck) als auch automatisch (z.B. nach 10 Minuten unbenutzter Tastatur/Maus) aktiviert werden.
- APC-Benutzerinnen und -Benutzer sollten grundsätzlich zum Thema Datenschutz- und Datensicherung geschult werden.

Die Forderung, daß nach Ende des BÜROMIN-Versuchs die Software-Anbieter einen Zertifizierungsnachweis vorlegen müssen, der mindestens der Funktionsklasse F2 und der Qualitätsstufe Q3 des IT-Sicherheitshandbuches entsprechen solle, wurde nicht erfüllt. Die Software-Anbieter behaupten allerdings, daß die Betriebssysteme ULTRIX und AIX die Forderungen der C2-Stufe des „Orange Book" erfüllen (vgl. 4.2.1). Die technischen Möglichkeiten einer umfassenden Protokollierung und auch eine datenschutzgerechte Paßwortgestaltung mit diesen Systemen seien vorhanden. Die Firmen sollten zum Nachweis ihrer Behauptungen aufgefordert werden.

Die Datenschutz-Kontrolle des Projekts BÜROMIN hat deutlich gemacht, daß die Umsetzung der meisten Kritikpunkte nicht aufgrund technisch oder organisatorisch unüberwindlicher Hindernisse ausgeblieben ist, sondern in erster Linie aufgrund von Zeitmangel. Meine wichtigste Forderung am Ende des Pilotprojektes lautet daher, UNIX-Systeme dürfen nur mit einer personell ausreichend ausgestatteten Systemverwaltung gestartet und betrieben werden.

Das vorgefundene Konzept BÜROMIN läßt grundsätzlich eine datenschutzgerechte Datenverarbeitung zu. Ohne größeren Zukauf von Soft- oder Hardware können Daten bis zur Schutzstufe C („Gefährdung des Ansehens") unter angemessener Verwendung der angebotenen Sicherungsfunktionen des Betriebssystems verarbeitet werden.

Die aufgezeigten Schwachpunkte sind nicht UNIX-spezifisch; alternative PC-Konzepte haben ähnliche oder auch andere Schwachpunkte. Proprietäre Systeme auf Großrechnerbasis könnten u. U. einen besseren Datenschutz ermöglichen; sie wären aber nur schwerlich geeignet, das zugrundeliegende Anforderungsprofil zeitgerecht zu erfüllen.

Für einen datenschutzgerechten Betrieb von Bürokommunikationssystemen im Innenministerium und im Ministerium für Wirtschaft, Technologie und Verkehr sind personelle Erweiterungen der System- und Benutzerverwaltung notwendig. Es sollten bei vergleichbaren Einsätzen Gruppen mit fachkundiger Führung und ausreichender Personalausstattung in den Bereichen Installation, Systemverwaltung und Benutzerbetreuung als ständige Einrichtung geschaffen werden.

Sollten zukünftig in BÜROMIN auch Daten der Schutzstufe D („Gefährdung der Existenz") verarbeitet werden, sind Zusatzeinrichtungen, z.B. die Verschlüsselungsfunktion und eine stärkere Abgrenzung der entsprechenden Benutzergruppen, notwendig. Daten der Stufe E („Gefahr für Leib und Leben") dürfen in der jetzigen Systemumgebung und unter dem vorhandenen Konzept aus der Sicht des Datenschutzes und der Datensicherheit nicht verarbeitet werden.

Meine Datenschutz-Kontrolle hat unmittelbare Reaktionen ausgelöst. Dadurch sind viele meiner Forderungen bereits umgesetzt worden. Mit der Erfüllung weiterer Forderungen ist begonnen worden. Ein Zertifizierungsnachweis der eingesetzten Betriebssysteme ULTRIX und AIX wurde nicht erbracht.

4.6.3 Einsatz der IuK-Technik bei den Bezirksregierungen (IuK-Reg)

Das Projekt „Konzept und Pilotprojekt für den Einsatz der IuK-Technik bei den Bezirksregierungen (IuK-Reg)" hat ernüchternde Erkenntnisse über die am Markt angebotenen „Vorgangssteuerungssysteme" erbracht. Das Projekt wird im Rahmen des IuK-Gesamtkonzepts für die Landesverwaltung durchgeführt; als Versuchsfeld wurden einige Dezernate der Bezirksregierung Braun-

schweig ausgewählt. Das Gesamtprojekt war nach Ist-Erhebungen und Analysen in zwei getrennten Losen — für Hardware und Software — ausgeschrieben und vergeben worden. Während die Hardware-Ausstattung (UNIX-Server in Verbindung mit DOS-Clients) sich im Laufe der zweijährigen Versuchsarbeiten bewährte, wurde die Zusammenarbeit mit der Software-Firma kurzfristig beendet.

Nach einer kritischen Bewertung und einer notwendigen Neuorientierung liegt das erklärte Ziel des Projekts nun in der Vorgangsbearbeitung, nicht mehr in der Vorgangssteuerung. Darunter versteht die Projektgruppe „eine dokumentbezogene Bearbeitung". Anders ausgedrückt heißt das: die Projekte BÜROMIN und IuK-Reg haben nun das gleiche Projektziel, sie verwenden nur andere Mittel. Während BÜROMIN ein einheitliches Bürokommunikations-Werkzeug unter UNIX einsetzt, verwendet IuK-Reg für die Textverarbeitung und Tabellenkalkulation DOS-Werkzeuge und für Datenbank sowie E-Mail UNIX-Werkzeuge. In beiden Projekten werden der Sachbearbeiterin bzw. dem Sachbearbeiter die Auswahl und die individuelle Steuerung der Vorgangsbearbeitung überlassen.

Wie im Projekt BÜROMIN wird auch bei IuK-Reg die Zertifizierungsforderung, die Bedingung für den Softwareanbieter war, nicht erfüllt. Auch das übrige Datenschutz- und Datensicherungskonzept ist bisher nur unvollständig umgesetzt worden. Da das Projektende auf das erste Quartal 1993 verschoben worden ist, werde ich erst dann meine Prüfung und Detailbewertung vornehmen.

4.6.4 Eichdateninformationssystem (EIDIS)

EIDIS soll die Eichämter in Niedersachsen und das Dezernat Eichwesen im Landesverwaltungsamt durch den Einsatz von IuK-Technik unterstützen. Im Mittelpunkt soll ein Eichvorschriften-Informations-System stehen, daß allen Eichbediensteten über das öffentliche Fernsprechnetz in ISDN-Technik vor Ort zur Verfügung stehen soll. Das Technik-Konzept von EIDIS sieht ein PC-Netz mit LAN-Netzsoftware im Landesverwaltungsamt, ISDN-Anschlüsse für PC unter dem Betriebssystem MS-DOS in den Eichämtern, Telefax-Anschlüsse sowie den Einsatz von 75 mobilen Erfassungsgeräten (Notebook, Laptop) vor.

Da ein Datenschutz- und Datensicherungskonzept bisher fehlt, ist der Untersuchungsbericht des Interministeriellen Arbeitskreises Informations- und Kommunikationstechnik (IMA-IuK, vgl. Nr. 5 der IuK-Technik-Grundsätze, Nds. MBl. Nr. 29/1990, 988 ff.) datenschutzrechtlich nicht bewertbar. Ich habe deshalb eine Datei-Errichtungsanordnung entsprechend den IuK-Technik-Grundsätzen nachgefordert. Sie steht nach nunmehr einem Jahr noch immer aus.

4.6.5 Automatisierung des Bibliothekswesens

Das Ministerium für Wissenschaft und Kultur hat durch Erlaß vom 25. August 1992 ein landeseinheitliches Bibliotheksautomationssystems PICA bei den staatlichen wissenschaftlichen Bibliotheken in seinem Geschäftsbereich eingeführt. Der Niedersächsische Bibliotheksverbund von gegenwärtig 23 Bibliotheken wird jetzt weiterentwickelt zum Bibliotheksverbund Niedersachsen/Sachsen-Anhalt. Dies soll am 1. Juli 1994 mit dem Niederländischen Bibliotheksverbund zu einer grenzüberschreitenden Leihverkehrsregion verknüpft werden.

Mit der eingeführten Bibliotheksautomation werden in großem Umfang personenbezogene Daten verarbeitet. Auf die Erforderlichkeit einer bereichsspezifischen gesetzlichen Regelung habe ich das Ministerium bei meiner frühzeitigen Beteiligung an den Erlaß-Entwürfen hingewiesen. Mit dem Ministerium besteht Einigkeit, daß in Kürze im Rahmen der Novellierung des Niedersächsischen Hochschulgesetzes (NHG) eine gesetzliche Ermächtigung für eine Rechtsverordnung aufgenommen wird, in der Art und Umfang der Datenverarbeitung im Rahmen eines Bibliotheksautomationssystems, insbesondere geplante automatisierte Abrufverfahren näher festgelegt werden (LT-Drs 10/3810, § 121 Abs. 2 NHG-E). Die im Erlaß genannte Rechtsgrundlage genügt nicht mehr verfassungsrechtlichen Erfordernissen und wird derzeit überarbeitet. Nicht nur aus hochschulrechtlicher, sondern auch aus datenschutzrechtlicher Sicht wäre die erwogene Einbeziehung von privaten Firmenbibliotheken insbesondere dann bedenklich, wenn eine gemeinsame Nutzerdatei eingeführt werden sollte. Ähnliche Probleme entstünden bei einem Verbund mit Nutzungsdaten bei Bibliotheken außerhalb Niedersachsens. Die Einrichtung von automatisierten Abrufmöglichkeiten bedürfen einer gesonderten Rechtsvorschrift. Ein Abruf personenbezogener Ausleihdaten durch Dritte ist derzeit nicht erlaubt. Ein derartiger Verbund der Nutzerdateien ist zumindest für die lokalen Systeme in Hannover avisiert. Ich habe die Erlaßregelung für eine Übergangszeit hingenommen, weil die gesetzliche Regelung bereits absehbar ist. Die Prüfung der technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes und der Datensicherung plane ich für das kommende Jahr.

4.6.6 MIKADO bei der Polizei

MIKADO ist nicht etwa ein neues Spielzeug der Polizei, sondern ein „Modulares Informations- und Kommunikationssystem Automatisierter Dezentraler Online-Anwendungen". Es dient der Vorgangsverwaltung polizeilicher Tätigkeit auf dezentralen Mehrplatzsystemen unter dem Betriebssystem UNIX. MIKADO wird seit Oktober 1991 in einem Mehrstufenkonzept landesweit eingeführt; es soll die älteren Pilotversuche Elvis, DISKUS und AVV ersetzen. Zu datenschutzrechtlichen Problemen und Fragen verweise ich auf 12.7.

4.6.7 „Automatisierte Bodenordnung" bei den Katasterämtern

Die Bodenordnung nach dem Baugesetzbuch ist eine Aufgabe der Gemeinden im eigenen Wirkungskreis. Die vermessungs- und katastertechnischen Arbeiten der Bodenordnungsverfahren werden von den Aufgabenträgern nach § 1 Nds. Vermessungs- und Katastergesetz wahrgenommen. 1991 waren bei 34 von 52 Katasterämtern Geschäftsstellen der Umlegungsausschüsse von insgesamt 128 Gemeinden tätig.

Für die verwaltungsmäßige Abwicklung der gemeindlichen Bodenordnung wird seit neuestem ein UNIX-Programm „Automatisierte Bodenordnung (ABO)" landesweit eingesetzt. Hierfür werden die vorhandenen UNIX-Rechner der Katasterämter verwendet. Das Datenschutz- und Datensicherungs-Konzept dieser Rechner war mehrfach Gegenstand von Kontrollen. Es wird auch für diesen Anwendungsfall als ausreichend angesehen. Verbesserungswürdig sind die Paßwort-Prüfungen sowie die Protokollierung der Benutzeraktivitäten und deren automationsunterstützte Auswertung. Hier ist die Herstellerfirma mit Nachbesserungen des Betriebssystems gefordert.

4.6.8 „Schoßhündchen" für Landgerichte

Das Justizministerium plant die Beschaffung und den Einsatz von tragbaren Computern (lap dog oder laptop, vgl. 4.5) für die Prüftätigkeit der Bezirksrevisoren bei den Landgerichten. Die Revisoren erhalten damit Automationsunterstützung beim Erstellen von Protokollen während örtlicher Prüfungen von Gerichtszahlstellen, Gerichtsvollziehern und Notaren. Die Prüftätigkeit kann dann weitgehend an Ort und Stelle bis hin zum Schreiben der Beanstandungen abgeschlossen werden. Ein Datenaustausch mit dem Schreibdienst erscheint entbehrlich.

Das Justizministerium plant zunächst einen Piloteinsatz bei einem Landgericht; anschließend sollen alle niedersächsischen Landgerichte entsprechend ausgestattet werden. Zum Einsatz kommen Laptops der Rechnerklasse 386 SX mit dem Betriebssystem MS-DOS und die Textsoftware WORD.

Ich habe für den geplanten Laptop-Einsatz ein Datenschutz- und Datensicherungskonzept eingefordert. Dabei habe ich Maßnahmen gegen Hardware-Manipulationen (z. B. durch Verplomben der Rechner), eine durchgreifende Authentizitäts- und Identitätsprüfung (z. B. durch Verwendung von Sicherheitssoftware), die Protokollierung der Benutzeraktivitäten und eine Verschlüsselungsmöglichkeit für die einem besonderen Berufs- und Amtsgeheimnis unterliegenden Daten gefordert. In einer Dienstanweisung sollten darüber hinaus der befugte Einsatz der Geräte, die ausschließliche Verwendung zugelassener Software, die Kennzeichnung und Behandlung beweglicher Datenträger, die Aufbewahrung der Laptops, ihre Verwendung für private Zwecke sowie die Kontrolle ordnungsgemäßer Verwendung geregelt werden.

4.6.9 „Schoßhündchen" auch für die Flurbereinigung

Durch Flurbereinigung wird das Grundeigentum im ländlichen Raum neu geordnet. Die Beteiligten werden für ihre alten Rechte abgefunden; neue Rechte werden begründet. Hierzu werden Daten aus dem Grundbuch und aus dem Liegenschaftsbuch übernommen und in den Teilnehmernachweis und später in den Flurbereinigungsplan übertragen. Nach Rechtskraft des Plans werden diese Daten an die öffentlichen Register rückübermittelt.

Während die Kommunikation mit der Katasterverwaltung schon seit längerem automationsunterstützt mittels Datenträgeraustausches erfolgt, wird der Austausch mit der Grundbuchverwaltung noch manuell erledigt, verbunden mit viel Doppelarbeit. Die Agrarstrukturverwaltung beabsichtigt nun, das Erheben und Erfassen der Grundbuchdaten zu automatisieren und dafür Laptops in den Grundbuchämtern mit eigenem Personal einzusetzen. Hierfür sollen vorhandene UNIX-Rechner verwendet und die vorhandene Software ihrer UNIX-Mehrplatzsysteme übernommen werden.

Der Zugang zu der Anwendung „Automatisierte Behandlung von Rechten in Verfahren nach dem Flurbereinigungsgesetz — ARBFlurb —", so der Organisationsuntersuchungsbericht ABRFlurb, sei durch Kennungen, Paßwörter sowie über differenzierte Zugangsberechtigungen zu sichern. UNIX böte auch ohne zusätzliche Software den angemessenen Schutz für die Informationen über Grundstücksbestände, Eigentümer und Berechtigte sowie über deren Rechte. Mit einer derartigen Aussage konnte ich mich für diesen Laptop-Einsatz nicht zufrieden geben. Auch für ARBFlurb habe ich ein Datenschutz- und Datensicherungskonzept sowie eine spezielle Dienstanweisung gefordert.

4.6.10 „Maintenance Management System"

Hinter diesem anspruchsvoll klingenden Titel — abgekürzt VISONIK MMS — verbirgt sich ein Programm zur Unterstützung betriebstechnischer Dienste, das die Universität Osnabrück zur Verwaltung und Unterhaltung ihrer umfangreichen Liegenschaften einsetzen möchte. Lagerverwaltung, Gebäudeverwaltung, Gebäude-Management, Instandhaltung, Kapazitätsplanung, Budget- und Kostenkontrolle sowie Statistik sind die Schlagworte des Firmenprospekts. Nur sehr versteckt ist aus dem Voruntersuchungsbericht des Ministeriums für Wissenschaft und Kultur erkennbar, daß auch personenbezogene Daten über Personal, Mieter, Kunden und Lieferanten gespeichert werden können. Ob dies so ist und wie diese Daten geschützt werden, müssen die Projektbetreiber noch untersuchen und dem IMA-IuK beantworten.

4.6.11 AIDA in der Arbeitsgerichtsbarkeit

„AIDA Nds." steht für „Automation von Arbeitsabläufen in der niedersächsischen Arbeitsgerichtsbarkeit". „MERVE" ist das Pilotprojekt zur Erprobung mehrplatzfähiger Kleinrechner und vernetzter PC als Informations- und Kommunikationssystem in der Verwaltung (vgl. IX 4.6 c)). AIDA ist im Rahmen des Pilotprojekts MERVE beim Sozialministerium entwickelt worden. Es wird seit 1988 bei den Arbeitsgerichten Braunschweig, Emden und Oldenburg testweise eingesetzt. Nunmehr soll es landesweit verwendet werden. AIDA Nds. ist auf der Basis der Programmiersprache MUMPS für MS-DOS- und UNIX-Rechner entwickelt worden und beeinhaltet die Funktionen Textverarbeitung und Datenbankverwaltung. Mit dem Verfahren werden die Daten der Rechtsstreitigkeiten (Namen, Anschriften, Termine) erfaßt und Schreibarbeiten der Geschäftsstellen (Ladungen, Beschlüsse) erleichtert. Auch die nach der Aktenordnung vorgeschriebenen Register und Kalender sowie die monatlichen Statistiken werden automationsunterstützt geführt.

Das Datenschutz- und Datensicherungs-Konzept, das mir auf Anforderung vorgelegt wurde, weist Schwächen auf. Unbefriedigend ist, daß die Arbeiten des Systemverwalters nicht kontrolliert werden können, daß das Paßwort nicht von der benutzenden Person selbst, sondern nur vom Systemverwalter eingegeben und verändert werden kann, daß er das Paßwort jeder Benutzerin und jedes Benutzers jederzeit lesen und benutzen (mißbrauchen) kann und daß keine systemseitige Protokollierung der Benutzer-Aktivitäten möglich ist.

4.6.12 DISPO in der Steuerverwaltung

DISPO ist ein Dialogverfahren zur Stellenbewirtschaftung, der Personaleinsatzverwaltung, zur Personalplanung und zum Aufstellen des Personalhaushalts. Als speichernde Stellen im Sinne des Datenschutzrechts sind die Personal- und Organisationsreferate der Oberfinanzdirektionen und die mit Personal-und Organisationsaufgaben befaßten Stellen der Niedersächsischen Fachhochschule für Verwaltung und Rechtspflege (Fachbereich Steuerverwaltung) bezeichnet worden.

Das Finanzministerium hat mir eine vorbildliche Datei-Errichtungsanordnung vorgelegt. Die Datenschutz- und Datensicherungsmaßnahmen, die mit mir frühzeitig abgestimmt worden sind, sehen eine differenzierte Zugriffsregelung mit durchgreifender Paßwortkontrolle vor. Alle Bediensteten erhalten nach Erstspeicherung und bei jeder Änderung einen Speicherauszug mit allen über sie gespeicherten personenbezogenen Daten („Kontoauszug"). Nutzung, Auswertung, Übermittlung, Berichtigung und Löschung sind geregelt.

Ich habe keine datenschutzrechtlichen Bedenken gegen den Einsatz dieses Verfahrens geltend gemacht. Auch die Zustimmung der Personalvertretung erfolgte im Gegensatz zu vergleichbaren Anwendungen sehr „geräuscharm".

4.6.13 DIBS/VBDV — Wunsch des finanziellen öffentlichen Dienstrechts

DIBS/VBDV ist das schreckliche Kürzel für „Dialogisierte Bezügesachbearbeitung und verteilte Bezügedatenverarbeitung". DIBS ist vor vielen Jahren konzipiert worden; mehrere Untersuchungsberichte haben die Erforderlichkeit zu belegen versucht und mit jedem Jahr kommen neue Wünsche und Erwartungen hinzu. Beschlossen und eingeführt ist DIBS jedoch noch immer nicht. Am Datenschutz- und Datensicherungskonzept liegt das nicht. Das Konzept ist auf mein Betreiben 1991 erstellt und von mir als angemessen akzeptiert worden.

Da inzwischen das geplante Rechnerkonzept längst überholt ist und überdacht werden muß, muß auch das Sicherheitskonzept den veränderten Vorstellungen angepaßt und überprüft werden.

4.6.14 APC in den Schulaufsichtsämtern

Die Schulaufsichtsämter haben Arbeitsplatzcomputer (APC) erhalten, um die erforderlichen Daten für die Unterrichts- und Personalversorgung ihrer Schulen speichern und verarbeiten zu können. Eingesetzt werden PC unter dem Betriebssystem MS-DOS und als Software dBase und WORD. Das Datenschutz- und Datensicherungs-Konzept ist mit mir abgestimmt worden. Es sieht mit dem Einsatz der Datensicherungssoftware Safeguard Plus eine differenzierte Zugriffskontrolle und eine Protokollierung der Benutzeraktivitäten vor. Alle betroffenen Personen erhalten nach Ersterfassung ein Datenblatt mit allen über sie gespeicherten Daten. Die Datei-Errichtungsanordnung, an der ich mitgearbeitet habe, legt den Datenkatalog, die Zweckbestimmung und die zulässige Nutzung der Daten fest.

4.6.15 „Einleiterüberwachung" und „Abwasserabgabe" für den Umweltschutz

Ganz „nüchtern" und ohne das sonst übliche prägnante Kürzel hat das Umweltministerium die zwei IuK-Verfahren „Einleiterüberwachung" und „Abwasserabgabe" vorgestellt. Die Verfahren sind als PC-Lösungen geplant; sie sollen 1993 programmiert und 1994 landesweit eingeführt werden. Damit soll das zugegeben komplizierte Geflecht der Übersicht, Genehmigung, Überwachung, Untersuchung und Berechnung von Abwässern entwirrt und koordiniert werden. Geplante Einsatzorte der PC-Programme für MS-DOS-Rechner sollen die Staatlichen Ämter für Wasser und Abfall (StÄWA), das Landesamt für Ökologie und die Dezernate 502 der Bezirksregierungen sein. Auch der Datenaustausch zwischen den Überwachungsbehörden und den Labors könnte durch Verwendung einheitlicher Software verbessert und erleichtert werden. Das IuK-Verfahren „Automation des Wasserbuchs" soll in einer späteren Phase in das Verfahren eingebunden werden.

Das Datenschutz- und Datensicherungs-Konzept sieht den Einsatz der Sicherheits-Software Safeguard Plus mit Hardware-Boot-Schutz vor. So soll sichergestellt werden, daß Benutzer nur die zur jeweiligen Aufgabenerfüllung erforderlichen Daten einsehen können. Die Benutzer-Aktivitäten sollen protokolliert werden. Ich teile die Ansicht der Konzeptentwickler, daß der Einsatz einer entsprechenden Sicherheits-Software in allen Einsatz-PC erforderlich ist.

4.6.16 „Begleitscheinverfahren" bei Entsorgung von Abfällen

Die Entsorgung von Sonderabfällen muß sorgfältig überwacht werden, sie ist wegen knapper Entsorgungsmöglichkeiten mit einer Abgabe belegt. Das Umweltministerium hat sein Konzept einer landeseinheitlichen Abgabenberechnung und Überwachung vorgestellt. Die Abgabenerhebung wurde den Bezirksregierungen zugewiesen. Sie erhalten Automationsunterstützung mit den Funktionen Überprüfung und Plausibilisierung der Angaben der Abfallerzeuger, Überwachung und Erinnerungsverfahren über Zahlungseingänge, Erstellen von Abgabenbescheiden, Datenaustausch über Leitung zwischen den Dezernaten 502 und den Kassen, Erstellen abfallstatistischer Daten und Bereitstellen der Grunddaten für das Umweltinformationssystem des Landes Niedersachsen.

Geplant ist der Einsatz auf UNIX-Rechnern mit der Datenbank ORACLE und der Benutzeroberfläche OSF Motif V 1.1. Die Testphase und die spätere flächendeckende Einführung waren für 1992 vorgesehen. Ein Datenschutz- und Datensicherungs-Konzept liegt mir noch nicht vor, so daß ich eine vom Umweltministerium gewünschte Stellungnahme bisher nicht abgeben konnte.

4.6.17 WABIS — ein Wasser- und Abfall-Informationssystem

„Informationen im Abfallbereich sind bisher nicht ausreichend abgedeckt". So begründet kurzgefaßt das Umweltministerium in seiner IMA-IuK-Vorlage eines Software-Vorhabens den Umstand, daß dessen Einsatzorte nicht konkret genannt sind. Als Ziele von WABIS werden der Aufbau eines Deponiekatasters für Sonderabfall, Siedlungsabfall, Abfälle aus betriebseigenen Deponien, der Aufbau von Altlastenkatastern, von Rüstungsaltlasten-Katastern und der Aufbau eines allgemeinen Informationssystems genannt. WABIS orientiert sich an den Projekten Niedersächsisches Umweltinformationssystem (NUMIS) und Führungsinformationssystem (FIS). Es soll ein entsprechendes Datenbank-Design erhalten.

WABIS soll auf UNIX-Rechnern lauffähig sein. Das Datenbanksystem ORACLE und die Benutzeroberfläche OSF Motif V 1.1 sollen auch hier zum Einsatz kommen. Die Software-Entwicklung ist für 1993/94 geplant. Auch für dieses Vorhaben liegt ein Datenschutz- und Datensicherungs-Konzept noch nicht vor. Meine erbetene datenschutzrechtliche Bewertung mußte daher zurückgestellt werden.

4.7 Automation in der Kommunalverwaltung

Die Informationsverarbeitung im kommunalen Bereich verändert sich „evolutionär". Zu diesem Ergebnis kommt die 1992 zum zweiten Mal durchgeführte Befragung der Leitstelle für Informations- und Kommunikationstechniken der Arbeitsgemeinschaft der kommunalen Spitzenverbände. Die 466 befragten Kommunen bleiben auch weiterhin ihren Kommunalen Datenzentralen treu. Während einige Kreisverwaltungen zusätzlich autarke Systeme einsetzen, tendieren Städte und Gemeinden dahin, ihre Mischform der Datenverarbeitung aufzulösen und sich entweder für die Kommunale Datenzentrale oder für die autarke Datenverarbeitung zu entscheiden. Große Wanderbewegungen und revolutionäre Technik-Entscheidungen sind nicht erkennbar. Wie auch in der Landesverwaltung gewinnt der „VerwaltungsComputer" — wie der Mehrplatzrechner in der Kommunalverwaltung genannt wird — zunehmend an Bedeutung. Die Anzahl hat sich von 40 auf 77 gegenüber 1989 fast verdop-

pelt. Auch die Kommunalverwaltung entscheidet sich dabei überwiegend für offene Systeme unter dem Betriebssystem UNIX. Aus der fast unübersehbaren Software-Palette werden neben den traditionellen Verfahren Bürokommunikationssysteme ausgewählt. Die IuK-Leitstelle stellt bedauernd fest: „Die Vielfalt am Softwaremarkt mag zwar aus der Sicht des Wettbewerbs zu begrüßen sein, Infrastrukturkonzepten (wie Integration, Kommunikation) und Kriterien des Investitionsschutzes ist diese Entwicklung nicht förderlich."

Seit 1989 hat sich in den Städten und Gemeinden die Zahl der IuK-Arbeitsplätze verdoppelt. Dabei verzeichnen die PC überdurchschnittliche Zuwachsraten; sie übertreffen die „unintelligenten" Bildschirme um das 3- bis 6fache. In der niedersächsischen Kommunalverwaltung ist heute jede vierte Angestellten- bzw. Beamtenstelle mit IuK-Technik ausgestattet. Einige Verwaltungen besitzen bereits jetzt eine Vollausstattung; weitere streben dies an. Allgemeine Prognosen für 1995 zeigen in die Nähe von 50 % im Landesdurchschnitt. Als Automationswünsche werden genannt: Verbesserung und Erweiterung der großen „Wesen" (Finanz-, Personal-, Einwohner- und Sozialwesen), Neuentwicklung von Ratsinformationssystemen, Abwasserinformationssystemen sowie weiteren Umweltverfahren und Einführung der „Digitalen Karte".

Den Kommunalen Datenzentralen wächst zunehmend die Aufgabe zu, als Beratungs- und Softwarestelle die kommunale Datenverarbeitung zu entwickeln und zu koordinieren. Dies wird schon jetzt erfolgreich in organisierter Verbundarbeit (UNIX-Verbund Nds.) oder durch einzelne Initiativen praktiziert.

Die Erhebung der IuK-Leitstelle und ihre Auswertung hat mir deutlich gemacht, daß meine bisherigen Informationsquellen über die kommunale Datenverarbeitung nicht ausreichen, meiner gesetzlichen Aufgabe nach § 18 Abs. 2 NDSG (Fassung 1991) hinreichend nachzukommen. Danach habe ich u. a. darauf zu achten, ob die automatisierte Datenverarbeitung die Wirkungsmöglichkeiten der staatlichen und kommunalen Verwaltung und der Organe der kommunalen Gebietskörperschaften auch in deren Verhältnis zueinander und untereinander verändert. Ich werbe um eine frühzeitige Unterrichtung über kommunale IuK-Projekte, so wie dies über den Interministeriellen Arbeitskreis für Informations- und Kommunikationstechnik (IMA-IuK) für Projekte der Landesverwaltung geschieht.

4.8 Normen, Standards und Empfehlungen

Das Innenministerium hat erneut die „Normen, Standards und Empfehlungen der IuK-Technik in der Landesverwaltung" überarbeitet, um sie dem Stand der technischen Entwicklung anzupassen. Die dritte, geänderte Fassung liegt dem Interministeriellen Arbeitskreis Informations- und Kommunikationstechnik (IMA-IuK) zur Befassung vor. Damit wird erneut ein Zwei-Jahresrhythmus der Fortschreibung eingehalten, mit dem versucht wird, dem raschen Tempo der Technikentwicklung zu folgen.

„Dem Datenschutz und der Datensicherung wird — ihrem Stellenwert entsprechend — in der Neufassung der Normen und Standards eine höhere Priorität eingeräumt" heißt es in dem Vorwort. Das habe ich wörtlich genommen und ein eigenständiges Kapitel „Datenschutz und Datensicherung" entworfen und empfohlen. Meinem Vorschlag ist gefolgt worden. Aufgabe und Grundsätze des Datenschutzes und der Datensicherung sowie organisatorische, technische und bauliche Maßnahmen bei DOS-, bei UNIX- und bei Kommunikationssystemen werden ausführlicher als bisher und an einer Stelle

zusammengefaßt beschrieben. Es werden konkrete Empfehlungen zur Beschaffung und zum Einsatz angemessener Sicherheitseinrichtungen gegeben. Dieser Datenschutz-Beitrag der „Normen und Standards" ist in der Anlage 12 dieses Berichts abgedruckt.

4.9 Vertrauen ist gut, Kontrolle ist besser: Protokollierung

Bei meinen Außenprüfungen stelle ich immer wieder fest, daß die Eigenkontrolle ordnungsgemäßer Datenverarbeitung nur unzureichend oder gar nicht erfolgt. Dabei gilt auch für die „Automation" die alte Lebensweisheit „Vertrauen ist gut, Kontrolle ist besser". Durch automatisierte Aufzeichnung von Protokolldaten wird die Datenverarbeitung nachprüfbar und transparent gemacht; zugleich wird damit einer mißbräuchlichen Verwendung vorgebeugt, weil keiner darauf vertrauen kann, daß Verstöße unentdeckt bleiben. Öffentliche und nicht-öffentliche Stellen sind nach § 9 des Bundesdatenschutzgesetzes (BDSG) bzw. § 7 des Entwurfs eines neuen Niedersächsischen Datenschutzgesetzes (NDSG-E) verpflichtet, technische und organisatorische Maßnahmen einzurichten, damit nachträglich überprüft und festgestellt werden kann, wer welche personenbezogenen Daten zu welcher Zeit in ein Automationssystem eingegeben bzw. übermittelt hat. Versuche mißbräuchlicher Verarbeitung personenbezogener Daten müssen immer aufgezeichnet und nachträglich untersucht werden.

Protokollierung ist jedoch kein Selbstzweck, sondern ist nur sinnvoll und datenschutzrechtlich vertretbar, wenn die Protokoll-Daten auch tatsächlich ausgewertet werden. Eine vollständigeRegistrierung aller Nutzungs-Aktivitäten kann auch aus Sicht des Datenschutzes bedenklich sein, da auf diese Weise eine neue Sammlung personenbezogener Daten über betroffene Bürgerinnen und Bürger sowie Beschäftigte entsteht, die zu zweckfremder Nutzung reizt. Informationen über die DV-Benutzung, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung des ordnungsgemäßen Betriebs einer DV-Anlage gespeichert werden, dürfen nicht für andere Zwecke verarbeitet werden (§ 14 Abs. 4 BDSG, § 10 Abs. 4 NDSG-E). Solche Daten über Beschäftigte dürfen nicht zu Zwecken der Verhaltens- und Leistungskontrolle genutzt werden (§ 24 Abs. 5 NDSG-E). Die Zweckbindung ist u. a. durch von der eigentlichen Datensammlung getrennte und sorgfältige Aufbewahrung der Protokolldateien zu sichern.

Protokollumfang, Kontrolldichte und Löschungsfristen sind von der Sensitivität der jeweiligen Anwendung abhängig. Bei deren Festlegung sind alle systemseitigen Möglichkeiten — z. B. durch Einstellen von Parametern oder Setzen von „Schaltern" — zu nutzen. Gestaltungs- und Prüfgrundsätze habe ich in einer Informationsschrift „Hinweise zu Protokolldateien" dargestellt. Die Information kann kostenlos bei mir bezogen werden.

4.10 Paßwortschutz

Fast jede Außenprüfung — gleich ob in der öffentlichen Verwaltung oder im nicht-öffentlichen Bereich — endet mit Kritik an der Zugriffskontrolle der IuK-Systeme. Dabei sollte doch jede Betreiberin und jeder Betreiber eines IuK-Systems ein besonderes Interesse haben, die „eigenen Daten" vor den neugierigen Augen der Konkurrenz oder unberechtigter Dritter zu schützen. Ich sehe mich bei meinen Kontrollbesuchen immer wieder veranlaßt, Defizite anzusprechen und grundlegende Informations- und Überzeugungsarbeit zu leisten.

Das Paßwort-Verfahren ist das am meisten verwendete Zugriffskontroll-Verfahren. Ein „Kochrezept" als Hilfe für Benutzerinnen und Benutzer könnte wie folgt aussehen:

— Paßwort nirgends notieren und niemandem mitteilen!
— Mindestens 6 Zeichen aus Buchstaben, Ziffern und Zeichen gemischt!
— Mindestens 1 Sonderzeichen verwenden!
— Paßwort regelmäßig ändern, aber nicht zu oft!
— Keine Trivialpaßwörter verwenden!

Um sich auch ein kompliziertes Paßwort leicht merken zu können, sollte man aus einem einprägsamen Satz, Lied oder Vers jeden x-ten Buchstaben auswählen und Sonderzeichen einstreuen, so z. B.: „Eile mit Weile" = EimiWe?

Unter X 4.5 und in der Anlage 12 sind weitere Empfehlungen für Auswahl und Umgang mit Paßwöttern enthalten. Systemverwalter und behördeninterne Datenschutzbeauftragte sind aufgerufen, diese Grundsätze bekanntzumachen und deren Einhaltung zu überprüfen. Sie sollten alle systemseitigen Möglichkeiten zum datenschutzgerechten Umgang mit Paßworten ausnutzen, so z. B. Paßwort-Mindestlänge, Änderungszwang, Ausschluß von Trivialworten, verschlüsselte Speicherung, Anzeige des letzten Login und des letzten erfolglosen Login, Reaktionsverzögerung bei Fehlversuchen, Fehlversuchs-Höchstzahl. Auch ich werde bei meinen kommenden Prüfungen die gewählten Paßwort-Verfahren durchgreifend prüfen.

4.11 Behördeninterne Datenschutzbeauftragte

Mittlerweile haben alle obersten Landesbehörden für ihren eigenen Bereich Datenschutzbeauftragte bestellt. Nach dem Entwurf des neuen Landesdatenschutzgesetzes sind alle öffentlichen Stellen verpflichtet, eine Beauftragte oder einen Beauftragten für den Datenschutz zu bestellen, wenn sie personenbezogene Daten verarbeiten und hierbei in der Regel mindestens fünf Bedienstete ständig beschäftigen. Von dieser Regelung erhoffe ich mir eine Stärkung des Datenschutzes und eine Unterstützung meiner Tätigkeit.

4.12 Schwachstelle Postversand — Adressen per Computer

„Renner" bei Eingaben wegen sonstiger technischer und organisatorischer Probleme waren Verstöße gegen datenschutzgerechte Versandformen und Beschriftungen.

So wurde von einem Amtsgericht im Adreßfeld das Wort „Klage" ausgedruckt, ein anderes Amtsgericht meinte in der Anschrift den Vermerk „als Erbin des am ... verstorbenen ..." anbringen zu müssen. In beiden Fällen lagen Verstöße gegen die Allgemeine Verfügung des Justizministeriums zur Bezeichnung des zuzustellenden Schriftstücks auf der Zustellungsurkunde vom 7. Januar 1971 (Nds. Rpfl. S. 30) vor.

Im kommunalen Bereich wurden von einer Stadt Verwarnungen nach dem Ordnungswidrigkeitengesetz als Drucksache versandt. Ich halte in Übereinstimmung mit dem Innenministerium eine Versendung mit verschlossenem Briefumschlag für erforderlich.

In einem anderen Fall erschienen Geburtsname, -tag und -ort im Anschriftenfeld eines Fensterbriefumschlages; durch eine programmseitige Änderung im Bescheidaufbau wurde dieser Mangel für die Zukunft behoben.

Auf dem Umschlag zu einem Wohngeldbescheid wurde von einer Stadt der Stempel „Amt für Wohnungswesen, Abteilung für Wohngeld" aufgebracht, der direkte Rückschlüsse auf den Inhalt der Sendung zuließ. Die Stadt sah ein, daß diese Absenderangabe zumindest rechtlich bedenklich ist und wird zukünftig die neutrale Kurzbezeichnung der Organisationseinheit angeben.

Ein Hinweis „BSeuchG" als Identifizierungsmerkmal auf einem Briefumschlag war „aus Versehen" notiert worden; die betreffende Stadt hat versichert, daß eine derartige Kennzeichnung in Zukunft unterbleibt.

Auf dem Briefumschlag zur Postzustellungsurkunde eines Finanzgerichts wurde bisher der Aufdruck „Lohnsteuerhaftung" angebracht. Das Finanzgericht wird zukünftig nur noch das Aktenzeichen und die Art des Schriftstückes angeben.

Diese beispielhafte Aufzählung zeigt, daß vielfach bestehende Regelungen nicht eingehalten werden oder Nachlässig- und Gedankenlosigkeit eine Beeinträchtigung von Persönlichkeitsrechten der Bürgerinnen und Bürger nach sich ziehen. Hier sind alle Verwaltungsangehörige zu etwas mehr Nachdenklichkeit aufgerufen.

5. Datenschutz beim Landtag

5.1 Behandlung von Landtagspetitionen

Mehrere Eingaben — zum Teil an den Landtag, zum Teil an mich gerichtet — haben die Frage aufgeworfen, ob die derzeitige Behandlung von Landtagspetitionen mit dem Recht der Petenten auf informationelle Selbstbestimmung vereinbar ist.

Jede an den Landtag gerichtete Petition wird mit einer Eingabe-Nummer, dem Namen der einsendenden Person und deren Wohnort sowie einem kurzen Betreff versehen. Nach Beratung in nichtöffentlicher Sitzung gibt der zuständige Ausschuß jeweils eine Beschlußempfehlung für den Landtag ab. Die Beschlußempfehlungen werden nach § 52 Abs. 3 der Geschäftsordnung des Landtages (GO LT) in Eingabenübersichten zusammengefaßt, die auch die genannten Angaben zur Person enthalten. Die Eingabenübersichten werden als Landtagsdrucksachen verteilt und sind damit der Öffentlichkeit zugänglich. Sie bilden die Grundlage für die öffentliche Beratung und Beschlußfassung des Landtages.

Zu Eingaben, die der Landtag der Landesregierung zur Erwägung oder Berücksichtigung überwiesen hat, teilt diese nach § 54 Abs. 3 GO LT schriftlich mit, was sie in der Sache veranlaßt hat. Auch diese Mitteilungen werden als Landtagsdrucksachen verteilt. Sie enthalten häufig nähere Darstellungen der persönlichen Verhältnisse der Petenten, z. B. zu Steuerschulden, Freiheitsentziehungen, psychiatrischer Behandlung. Die Veröffentlichung soll den Abgeordneten die Möglichkeit geben, eine erneute Beratung der Eingabe zu fordern, wenn ihnen die Mitteilung der Landesregierung nicht befriedigend erscheint.

Der Landtag, der die Problematik im Auschuß für Rechts- und Verfassungsfragen sowie im Geschäftsordnungsausschuß eingehend erörtert hat, hat mich um eine datenschutzrechtliche Bewertung dieses Verfahrens gebeten.

Ich habe Bedenken gegen die Wiedergabe der personenbezogenen Daten der Petenten in den veröffentlichten Eingabenübersichten geäußert. Zunächst kann nicht unterstellt werden, daß eine Person, die sich an den Landtag wendet, der Veröffentlichung ihrer Daten konkludent zustimmt. Eine solche Annahme würde voraussetzen, daß allen einsendenden Personen der Verfahrensablauf bei der parlamentarischen Behandlung von Eingaben, insbesondere die Veröffentlichung in den Landtagsdrucksachen, bekannt wäre. Hiervon kann nach den bisherigen praktischen Erfahrungen nicht ausgegangen werden.

Nach dem das Datenschutzrecht beherrschenden Erforderlichkeitsprinzip darf in das informationelle Selbstbestimmungsrecht nur eingegriffen werden, wenn die Aufgabenerfüllung dies unabdingbar notwendig macht. Nach meiner Einschätzung ist es nicht erforderlich, in die Eingabenübersichten Angaben zur Person der jeweiligen Einsenderin bzw. des Einsenders aufzunehmen. Deshalb habe ich vorgeschlagen, künftig auf die Wiedergabe von Namen und Wohnort im Zusammenhang mit den Beschlußempfehlungen an den Landtag zu verzichten.

Der Gesetzgebungs- und Beratungsdienst des Landtags hat hiergegen eingewandt, das Verfassungsprinzip der Öffentlichkeit parlamentarischer Verhandlung (Art. 9 Abs. 1 VNV) verlange diese Angaben. Das Öffentlichkeitsgebot solle u. a. eine Kontrolle der Abgeordneten durch die Wählerinnen und Wähler ermöglichen. Gerade im Petitionswesen sei es von wesentlicher Bedeutung, daß jede Bürgerin und jeder Bürger nachprüfen könne, auf wessen Eingabe hin der Landtag welchen Beschluß gefaßt habe. Etwaigen Mutmaßungen über Inkorrektheiten könne so von vornherein der Boden entzogen werden.

Dieser Gesichtspunkt überzeugt mich nicht. Zwar kommt dem Öffentlichkeitsgebot als demokratischem Grundprinzip zweifellos ein hoher Rang zu. Dennoch unterliegt auch dieses Prinzip Einschränkungen, etwa wenn es um staatliche Geheimhaltungsinteressen, aber auch um den Schutz von Persönlichkeitsrechten (vgl. das Flick-Urteil des Bundverfassungsgerichts — BVerfGE 67, 100 —) geht. Schließlich darf die praktische Bedeutung der öffentlichen Kontrolle gerade bei der Behandlung von Petitionen nicht überschätzt werden. Werden — wie dies im Regelfall geschieht — bei der Beratung im Landtag lediglich der Name der einsendenden Person, deren Wohnort, der Betreff der Eingabe und der Beschlußvorschlag des zuständigen Ausschusses genannt, dürfte aufgrund dieser spärlichen Angaben eine effektive Kontrolle der Tätigkeit der Abgeordneten ohnehin kaum möglich sein.

Im Bund und in den übrigen Ländern wird — bei weitgehend gleicher Verfassungslage — denn auch datenschutzfreundlicher verfahren. Sowohl der Deutsche Bundestag als auch die Länderparlamente der alten Bundesländer stellen — wie eine Umfrage ergeben hat — sicher, daß die Petentin bzw. der Petent für die Öffentlichkeit anonym bleibt. Im Bund und in einigen Ländern werden die Beschlußempfehlungen des zuständigen Ausschusses in Eingabenübersichten ohne Namensangabe der Petenten veröffentlicht; in den anderen Ländern werden die Eingaben in den Ausschüssen in nichtöffentlicher Sitzung abschließend beraten. In Baden-Württemberg erhalten die Abgeordneten eine (nicht veröffentlichte) Liste, die ihnen Aufschluß über Person und Wohnort der Petenten gibt. In den als Landtagsdrucksachen öffentlich zugänglichen Beschlußvorlagen sind anonymisierte detailliertere Angaben über die einzelnen Eingaben, über die Stellungnahme der Regierung sowie über die zu treffende Landtagsentscheidung enthalten.

Im Hinblick auf die — nach meiner Ansicht in diesem Zusammenhang überzogene — Auslegung des Öffentlichkeitsprinzips durch den Gesetzgebungs- und Beratungsdienst haben die beteiligten Ausschüsse alle Verfahrensweisen

dieser Art abgelehnt. Künftig soll jedoch den Petenten in der Eingangsbestätigung die Behandlung der Eingaben näher erläutert und die Möglichkeit eröffnet werden, sich im Falle von Einwendungen gegen die öffentliche Behandlung ihrer Angelegenheit mündlich oder schriftlich mit der Landtagsverwaltung in Verbindung zu setzen.

Bezüglich der Eingaben, die der Landesregierung zur Erwägung oder Berücksichtigung überwiesen worden sind, bestand Einvernehmen, daß auf eine Veröffentlichung der Antworten der Landesregierung verzichtet werden kann. Abdrucke der Antworten sollen künftig an die Mitglieder der zuständigen Ausschüsse verteilt werden. § 54 Abs. 3 GO LT ist entsprechend geändert worden. Die jeweils örtlich zuständigen Abgeordneten oder weitere Abgeordnete können auf Wunsch ebenfalls entsprechende Abdrucke erhalten. Mit dieser Regelung kann ein datenschutzgerechtes Verfahren jedenfalls in diesem Punkt sichergestellt werden.

5.2 Parlamentarische Datenverarbeitung

Der Landtag unterliegt nicht meiner Kontrolle, soweit er in Wahrnehmung parlamentarischer Aufgaben personenbezogene Daten verarbeitet. Die besondere Stellung des Landtags als unmittelbar vom Volk gewähltes Organ läßt keine staatliche Fremdkontrolle zu. Dessenungeachtet ist die parlamentarische Datenverarbeitung für die Betroffenen ein Eingriff. Deshalb wird der Bundestag prüfen, ob eine Regelung in das Bundesdatenschutzgesetz aufgenommen und die Bundestagsgeschäftsordnung um eine „Datenschutzordnung des Bundestages" erweitert werden soll. Im Rahmen der Diskussion über den Entwurf eines neuen NDSG besteht für den Niedersächsischen Landtag die Möglichkeit, sich Klarheit darüber zu schaffen, wie im eigenen Hause der Datenschutz sichergestellt werden kann.

6. Europa

Bis hinein in die 80er Jahre waren in Sachen Datenschutz auf übernationaler Ebene fast nur Aktivitäten des Europarates zu vermelden, der Empfehlungen für allgemeine und bereichsspezifische Datenschutzregelungen an die Mitgliedstaaten herausgab. Immer wieder war von seiten der Datenschutzinstanzen wie von der Wissenschaft beklagt worden, daß trotz Intensivierung der informationellen Beziehungen im immer stärker zusammenrückenden Europa keine Anstrengungen unternommen werden, das informationelle Selbstbestimmungsrecht bei gemeinsamen Datenbanken und bei grenzüberschreitendem Datenaustausch sicherzustellen.

6.1 EG-Datenschutzpaket

Mit einem „Datenschutzpaket" signalisierte die EG-Kommission am 27. Juni 1990, daß sie sich nunmehr auch in Fragen des Datenschutzes für zuständig ansieht. Ziel dieses Pakets ist es, einen einheitlichen Schutzstandard in der EG festzulegen und so Hemmnisse des Datentransfers im Binnenmarkt aus Datenschutzgründen zu verhindern. Das Paket enthielt Vorschläge für

— eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten,
— eine Entschließung zur Ausweitung des Anwendungsbereichs der Richtlinie auf Materien außerhalb des EG-Rechts,
— eine Erklärung der Kommission, die Richtlinie auf EG-Institutionen anzuwenden,
— eine Richtlinie zum Datenschutz im Bereich der Telekommunikation,
— eine Empfehlung der Kommission zum Beitritt der EG zur Datenschutzkonvention des Europarates sowie schließlich
— einen Beschluß des Rates auf dem Gebiet der Informationssicherheit.

Im Berichtszeitraum fanden die Kommissionsvorschläge große Beachtung und im Grundsatz positive Resonanz, von seiten der Privatwirtschaft aber auch heftige Kritik. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder verteidigte den Entwurf für eine Datenschutzrichtlinie in seiner grundsätzlichen Tendenz und machte Verbesserungsvorschläge (vgl. Anlage 1). Am 15. Juli 1992 wurden dann EG-einheitliche Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik bekanntgemacht (GMBl. 1992, S. 545). Während bei Fragen der Informationssicherheit Einigung hergestellt werden konnte, war die Diskussion über das materielle EG-Datenschutzrecht Ende 1992 noch nicht abgeschlossen. Sowohl die allgemeine wie auch die Telekommunikations-Richtlinie für den Datenschutz befinden sich noch im Normgebungsverfahren. Bei der Telekommunikation-Richtlinie liegen die Standpunkte der Kommission der EG einerseits und des Europäischen Parlaments andererseits schon nahe beieinander (abgedruckt in DANA 2/3-1992, S. 9 ff, vgl. 3.1.1). Äußerst umstritten ist dagegen der Entwurf einer allgemeinen Datenschutz-Richtlinie. Zu bedauern ist auch, daß sich die Kommission nicht in der Lage sah, zumindest vorläufig den Richtlinienentwurf für EG-Institutionen für verbindlich zu erklären.

6.2 EG-Datenschutzrichtlinie

Nachdem das Europäische Parlament seine Änderungsvorschläge zum Entwurf der Datenschutzrichtlinie formuliert hatte, wurde von der Kommission am 15. Oktober 1992 ein überarbeiteter Richtlinienentwurf vorgelegt (abgedruckt in RDV 1/1993). Ziel dieses Richtlinienentwurfes ist es, den „freien Verkehr personenbezogener Daten zwischen Mitgliedsstaaten" der EG zu gewährleisten (Art. 1 Abs. 2 des Entwurfes). Um dieses Ziel zu erreichen, soll ein Mindeststandard an Datenschutz festgeschrieben werden, der dazu führt, daß der Datenaustausch über die Grenze wegen mangelnden Datenschutzes nicht mehr untersagt werden kann. Ich halte es für eine förderalistische Selbstverständlichkeit und für eine verfassungsrechtliche Notwendigkeit, daß der nationale Gesetzgeber über die Richtlinie hinausgehende Datenschutzvorschriften erlassen kann. Das Ziel, Wettbewerbsverfälschungen in der EG zu verhindern, so der 7. Erwägungspunkt des Richtlinienentwurfes, darf nicht dazu benutzt werden, daß der Grundrechtsschutz auf der Strecke bleibt und nationales Recht auf dem Niveau der Richtlinie gleichgeschaltet wird. Mit der Richtlinie können auch keine Kompetenzveränderungen vorgenommen werden. Insofern ist es mehr als mißverständlich, wenn Art. 33 des Entwurfes der Kommission eine „Rechtsetzungsbefugnis" zuschreibt, um die einheitliche Anwendung der Richtlinie zu gewährleisten.

Ein Einfallstor für den unbeschränkten Datenaustausch gegenüber Drittländern enthält Art. 26 des Entwurfs, wonach die EG-Kommission feststellt, ob ein Drittland als Übermittlungsvoraussetzung ein „angemessenes Schutzniveau gewährleistet", ohne daß die Anhörung der Datenschutzkontrollinstanzen zwingend vorgeschrieben wäre.

Zu begrüßen ist es, daß der Richtlinienentwurf Schutzbestimmungen enthält, die dem deutschen Datenschutzrecht bisher unbekannt sind, so etwa ein verstärkter Schutz besonders sensibler Daten, wie Angaben über rassische und ethnische Herkunft, über politische und religiöse Anschauungen, über Gesundheit und Sexualleben (Art. 8 des Entwurfs). Während nach bundesdeutschem Recht der Widerspruch gegen die Datennutzung zu Werbezwecken nur zur Sperrung führt, normiert der Entwurf eine Löschungspflicht. Prinzipiell zu begrüßen ist auch das Verbot einer beschwerenden Verwaltungsmaßnahme oder einer Entscheidung im privaten Bereich, „die ausschließlich aufgrund einer automatisierten Verarbeitung ergangen ist, die ein Persönlichkeitsprofil erstellt". Unklar ist aber, weshalb die Richtlinie die nationalen Gesetzgeber verpflichtet, von diesem positiven Ansatz weitgehende Ausnahmen zuzulassen (Art. 16 des Entwurfs).

Kritikwürdig ist weiterhin die äußerst schwammige Formulierung zur Zweckbindung. Dadurch, daß — anders als vom Europäischen Parlament gefordert — Akten nicht von der Richtlinie erfaßt werden sollen, besteht das Risiko, daß der unbefriedigende Rechtszustand nach dem BDSG im privaten Bereich festgeschrieben oder gar verschlechtert wird. Weiterhin erscheinen mir die Strafvorschriften, welche nach dem Entwurf erlassen werden müssen, als ein ungeeignetes Instrument zum Schutz der Privatsphäre. Bedenken müssen schließlich vorgebracht werden, daß die Richtlinie den nationalen Gesetzgebern bis Mitte 1994 Zeit lassen möchte, ihre Vorschriften anzupassen, und daß die Anwendung der materiellen Regelungen bis Mitte 1997 hinausgezögert werden kann. Ich gehe davon aus, daß der freie Binnenmarkt für personenbezogene Daten erst dann etabliert werden kann, wenn die Richtlinie vollständig in nationales Recht umgesetzt wurde.

6.3 Schengen

Die polizeiliche, ausländerrechtliche und justitielle Zusammenarbeit der EG-Mitgliedstaaten hat im Schengener Zusatzabkommen, das am 19. Juni 1990 unterzeichnet wurde, konkrete rechtliche Gestalt bekommen (BT-Drs 12/2453). Fast zeitgleich erfolgte die Unterzeichnung des Dubliner EG-Asylabkommens vom 15. Juni 1990. Für den Bereich des Asylrechts sind Dubliner und Schengener Abkommen inhaltlich weitgehend identisch. Beide Vertragstexte bedürfen für ihr Inkrafttreten der Ratifikation durch die nationalen Parlamente. Während das Asylübereinkommen für die gesamte EG gelten soll, wollen sich mit dem Schengen-Vertrag zunächst nur 9 der 12 EG-Mitglieder binden, neben den Schengen-Kernländern Frankreich, Bundesrepublik Deutschland, Belgien, Niederlande und Luxemburg auch Italien, Spanien und Portugal sowie durch Unterzeichnung am 6. November 1992 Griechenland.

Im Rahmen der Prüfung, ob das Land Niedersachsen dem Schengener Zusatzabkommen zustimmen könne, wies der Niedersächsische Ministerpräsident auf datenschutzrechtliche Defizite hin. Ich habe eine detaillierte datenschutzrechtliche Überprüfung des Vertragswerks durchgeführt und das Ergebnis den zuständigen niedersächsischen Ministerien mitgeteilt.

Gegenüber den ersten Entwürfen weist der jetzt vorliegende Vertragstext einige datenschutzrechtliche Verbesserungen auf, die auf Forderungen der Datenschutzbeauftragten zurückgehen. Dessenungeachtet bestehen weiterhin Defizite, die durch Nachbesserungen des sich immer noch im Ratifizierungsverfahren befindlichen Vertrags behoben werden können:

— Durch mangelnde Einbindung des Vertrags in den organisatorischen Rahmen der Europäischen Gemeinschaft fehlt auf europäischer Ebene sowohl die parlamentarische als auch die justitielle Kontrolle.
— Die Umsetzung bedarf teilweise noch nationaler bereichsspezifischer Datenschutzregelungen, etwa auch im niedersächsischen Polizeirecht.
— Die ausnahmslose Meldepflicht aller Drittausländer und Drittausländerinnen könnte manche an die polizeiliche Meldepflicht auch der Westdeutschen in der ehemaligen DDR erinnern.
— Die Abstimmung ausländer- und asylrechtlicher Maßnahmen zwischen den Vertragsstaaten setzt den Austausch höchst sensibler Personendaten voraus. Es ist nicht festgelegt, in welchem Umfang die Unterrichtung erfolgt. Die Datenübermittlungen können existentielle Eingriffe in das Leben der Drittausländer und Drittausländerinnen zur Folge haben.
— Die Vertragsstaaten verpflichten sich, nach Übermittlung der hierfür nötigen Informationen, bestimmte nach fremdem Recht verhängte ausländerrechtliche und polizeiliche Maßnahmen auszuführen, auch wenn deutsches Recht solche Maßnahmen nicht zuließe. Dies dürfte einen Verstoß gegen den Gesetzesvorbehalt bei Grundrechtseingriffen darstellen.
— Datenübermittlungen werden nicht von einem der Bundesrepublik entsprechenden Datenschutzstandard abhängig gemacht, sondern von der Geltung der insofern unzureichenden Europäischen Datenschutzkonvention.
— Es bleibt unklar, welchen datenschutzrechtlichen Verpflichtungen polizeiliche Verbindungsbeamte unterworfen sind.
— Einzelne Maßnahmen zielen nicht auf die Bekämpfung von konkreten Gefahren und Staftaten, sondern auf das sogenannte „Vorfeld". Dadurch werden auf europäischer Ebene Maßnahmen erlaubt, deren Zulässigkeit nach nationalem Verfassungsrecht äußerst umstritten ist.
— Die Installierung des Schengener Informationssystems (SIS) wirft eine Vielzahl von Fragen auf, die im Vertrag nicht beantwortet werden. Das SIS wird eine neue Qualität für die internationale polizeiliche Zusammenarbeit und den Informationsaustausch mit sich bringen. Mit dem sekundenschnellen Zugriff durch die Polizeien aller Partnerländer werden polizeiliche Maßnahmen in einem anderen Staat erfolgen, deren materiellrechtliche Zulässigkeit nach nationalem Recht nicht mehr geprüft werden kann. Die im SIS eingegebenen Daten unterliegen nicht mehr der alleinigen Verfügbarkeit der eingebenden Stelle und entwickeln ein Eigenleben, welches ausschließlich vom abfragenden Staat bestimmt wird.
— Die Ausschreibung zur Einreiseverweigerung im SIS-System unterliegt auch nicht ansatzweise gemeinsamen Standards. Bei der Zurückweisung von Drittausländerinnen und Drittausländern machen sich die Staaten gegenseitig zu ausländerrechtlichen Erfüllungsgehilfen.

Schließlich muß darauf hingewiesen werden, daß die im Vertragsentwurf geplanten zusätzlichen Befugnisse der Regierungen schon heute nicht mehr als ausreichend angesehen werden. So ist die Rede von supranationalen polizeilichen Lagezentren, von einer europaweiten daktyloskopischen Sammlung mit 10-Finger-Formeln der Asylsuchenden aller EG-Staaten (vgl. 13.5) oder von europäischen Haft- oder Straftaten/Straftäter-Dateien. Solche Vorhaben sind nicht akzeptabel, solange es in Europa kein gemeinsames Datenschutzrecht im institutionellen Rahmen der EG gibt, das den Anforderungen des bundesdeutschen Verfassungsrechts entspricht.

6.4 Maastricht

Nachdem die EG-Kommission mit ihren Richtlinienvorschlägen zu erkennen gegeben hatte, daß sie dem Datenschutz wie dem Grundrechtsschutz allge-

mein einen hohen Stellenwert bei der Integration Europas beimißt, war zu hoffen, daß sich auch die EG-Staatschefs bei der Ausarbeitung eines Vertrages über die Schaffung der Europäischen Union, unterzeichnet am 7. Februar 1992, von entsprechenden Überlegungen leiten lassen würden. Diese Hoffnungen haben getrogen. Der sog. Maastricht-Vertrag enthält außer einem generellen Bekenntnis zu den Grundrechten und Grundfreiheiten in Art. F keine Aussage zum Datenschutz. Zwar wird den Bürgerinnen und Bürgern ein europäisches Petitionsrecht zugestanden. Ein Bürgerbeauftragter sowie ein Rechnungshof sollen installiert werden. Die Einrichtung einer europäischen Datenschutzkontrollinstanz wurde aber versäumt. Eine solche Instanz ist im Hinblick auf die teilweise sehr unterschiedliche Datenschutzgesetzgebung in den Ländern und in Anbetracht der in der EG massiv zunehmenden Datenströme unverzichtbar. Anders als auf nationaler Ebene, wo bei der Rechtsetzung die Datenschutzkontrollinstanzen beteiligt werden, gibt es auf EG-Ebene kein solches Korrektiv. Immer wieder muß ich feststellen, daß das nationale Datenschutzrecht durch EG-Rechtsakte auf kaltem Wege ausgehebelt wird. Zu administrativen Überwachungs- und Kontrollzwecken z. B. bei der Subventionsvergabe werden in der EG Datenerhebungen und Übermittlungen in gewaltigem Umfang vorausgesetzt. Es gibt aber keinerlei Anzeichen dafür, daß in diese EG-Regelungen ein Mindeststandard bereichsspezifischer datenschutzrechtlicher Regelungen materiellrechtlicher oder technisch-organisatorischer Art in Zukunft aufgenommen werden sollte. Dieses Defizit im Grundrechtsschutz hätte durch Aufnahme eines Datenschutzrechts und durch Institutionalisierung einer EG-Datenschutzkontrolle im Maastricht-Vertrag behoben werden können — eine verpaßte Chance!

Ausdrücklich zu begrüßen ist eine Zusatzerklärung zum Maastricht-Vertrag, die das Ziel verfolgt, den „Zugang der Öffentlichkeit zu den Informationen, über die die Institutionen verfügen", zu erweitern. Es ist zu hoffen, daß hier der Zeitraum bis 1993 für die Erstellung eines ersten Berichts nicht voll in Anspruch genommen werden wird und bald rechtsetzende Aktivitäten folgen. Das Beispiel der EG-Richtlinie zur Realisierung der Informationsfreiheit im Umweltbereich hat mit ihrer Fristsetzung auf Ende 1992 eine positive Auswirkung auf die nationalen Gesetzgeber gehabt (vgl. 17.1).

Obwohl dem Datenschutz im Maastricht-Vertrag keine Beachtung zuteil wurde, ist es dessen offensichtliches Ziel, die informationellen Beziehungen zwischen den EG-Staaten zu intensivieren. Dies kommt darin zum Ausdruck, daß sich die Parteien verpflichten, transeuropäische Netze im Bereich der Telekommunikation aufzubauen und die technische Normung und Forschung auch im informationstechnischen Bereich zu intensivieren. Mehrfach besondere Erwähnung findet auch die Zusammenarbeit in Angelegenheiten der Asyl-, der Justiz- und der Innenpolitik, insbesondere bei der Bekämpfung der illegalen Einwanderung und bei der Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität. Der „Aufbau eines unionsweiten Systems zum Austausch von Informationen im Rahmen einer Europäischen kriminalpolizeilichen Zentralstelle (Europol)" wird vereinbart. Ohne die Ratifizierung und das Inkrafttreten des Maastricht-Vertrages abzuwarten, beschlossen die EG-Innen- und Justizminister am 18. September 1992 die Einrichtung einer Arbeitsgruppe zur Bekämpfung der organisierten Kriminalität. Die erste Abteilung von Europol nahm am 1. Januar 1993 ohne jede rechtliche Grundlage ihre Arbeit auf. Dies hat auch für das Land Niedersachsen datenschutzrechtliche Relevanz, da der Europol-Stelle Zugriff zu den INPOL-Verbunddateien eingeräumt werden soll, in denen sich auch von der niedersächsischen Polizei angelieferte Daten befinden und deren Verarbeitung sich nach meiner Auffassung nur nach niedersächsischem Recht richten kann (vgl. 12.3).

Die im Maastricht-Vertrag genannten Zielsetzungen und deren vorgezogene Realisierung sind zwangsläufig mit einer massiven Intensivierung des Austauschs auch von Personendaten verbunden. Im Hinblick auf das bisherige Datenschutzbewußtsein innerhalb der EG-Administration ist zu befürchten, daß Belange des Persönlichkeitsschutzes auf der Strecke bleiben.

6.5 Datensammelei auf dem Bauernhof

Ein typisches Beispiel hierfür ist die Datenverarbeitung aufgrund von EG-Normen zum Zweck der Subventionsvergabe im Landwirtschaftsbereich: Mit der Verordnung (EWG) Nr. 3766/91 des Rates vom 12. Dezember 1991 sollen die Erzeuger von Sojabohnen, Raps- und Rübsensamen und Sonnenblumenkernen von der EG unterstützt werden (Ölsaatenbeihilfe). Um die Unterstützung der EG zu erlangen, muß der Landwirtschaftsbetrieb Angaben über die genutzten Flächen machen und einen detaillierten Anbauplan vorlegen. In einer weiteren Verordnung der EG (Verordnung der Kommission vom 10. März 1992 Nr. 615/92) heißt es dann: „Zur Abwehr der Gefahr der unrechtmäßigen Erlangung von Gemeinschaftsmitteln soll eine strenge Kontrollregelung mit Verwaltungskontrollen und physischen Kontrollen eingeführt werden". Die Kontrollen sollen erfolgen „durch systematischen Vergleich mit verfügbaren, einschlägigen früheren Angaben, in den Fällen, in denen Zweifel verbleiben, durch statistische Erhebung und mittels Fernerkundung." Art. 17 der Verordnung könnte als eine Art Datenverarbeitungsermächtigungsklausel gelten: „Die Mitgliedstaaten treffen alle erforderlichen zusätzlichen Maßnahmen zur Durchführung dieser Verordnung. Sie nehmen insbesondere Kontrollen der Unterlagen vor sowie zusätzliche Überprüfungen in den Fällen, in denen Erzeuger im Jahr mehr als einen Antrag einreichen oder in denen je Feldstück mehr als ein Antrag gestellt wird. Zu diesem Zweck machen die Mitgliedstaaten bei der Bearbeitung der Anträge auf Direktzahlungen, falls möglich und kostengünstig, von EDV Gebrauch. Die Mitgliedstaaten unterstützen einander im erforderlichen Umfang bei den in dieser Verordnung vorgesehenen Kontrollen."

Der in Niedersachsen für die Beantragung der Ölsaatenbeihilfe verwendete Vordruck folgt der Linie der EG-Vorgaben, ohne daß in ausreichendem Maße auf die datenschutzrechtlichen Anforderungen geachtet worden wäre (vgl. auch 28.2). Die gesamte Rückseite des Antragformulars ist gefüllt mit „Erklärungen/Verpflichtungen". So erklärt sich in Nr. 21 der Antragsteller einverstanden, daß bei der Bearbeitung des Antrags alle bisher gemachten Angaben im Zusammenhang mit der Beantragung flächenbezogener Förderungsmaßnahmen zum Vergleich herangezogen werden können (z.B. Gasölverbilligung, Flächenstillegung).

Sicherlich ist es ein gewaltiger Mißstand in der EG, daß unberechtigterweise Fördermittel in Anspruch genommen werden. Der dadurch entstehende Schaden soll in Milliardenhöhe gehen. Dieser Umstand rechtfertigt es aber nicht, auf rechtsstaatliche Erfordernisse wie Normenklarheit und Bestimmtheit und auf die Einhaltung des Gesetzesvorbehalts zu verzichten. Das Niedersächsische Landwirtschaftsministerium teilt im konkreten Fall meine Einschätzung, daß die EG-Verordnung den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts nicht genügt. Auch die Einwilligungserklärung hält einer rechtlichen Prüfung nicht stand, da weder Handlungsalternativen angeboten werden, noch über die Notwendigkeit der Erklärung und Folgen der Nichteinwilligung informiert wird. Der offensichtlich eingeplante Abgleich mit früheren Anträgen erweist sich in den meisten der genannten Fällen als ungeeignetes Kontrollmittel. Meine Feststellungen sind um so schmerzlicher, als die verwendeten Antragsfomulare nicht nur in Niedersachsen verwendet werden, sondern bundesweit abgestimmt sind.

Aufgrund meiner Intervention thematisierte das Niedersächsische Landwirtschaftsministerium die datenschutzrechtlichen Probleme bei einer Länder-Referentenbesprechung. Da die Ölsaatenbeihilfe 1992 ausläuft, konnte man keine direkten Schlußfolgerungen mehr aus meiner Kritik ziehen. Künftig sollen landwirtschaftliche Kontrollen sowie Sanktionen in einer Verordnung für alle Produkte geregelt werden. Dieser Vorschlag ist aber nicht minder umstritten: Geplant ist eine Datenbank, in welcher Betriebe, Parzellen und Tiere in ein detailliertes Verzeichnis aufgenommen werden.

Die Kontrollpläne der EG-Beamten haben damit noch lange kein Ende gefunden. So sollen EG-weit alle durchnumerierten landwirtschaftlichen Parzellen per Satellit daraufhin überwacht werden, ob sie tatsächlich, wie von den Landwirtschaftsbetrieben angegeben, stillgelegt oder auf besondere Art genutzt werden (vgl. 28.1). Tiere von subventionierten Betrieben sollen alphanumerisch registriert und fälschungssicher mit nur einmal verwendbarer Ohrmarke gekennzeichnet werden. Die Hannoversche Allgemeine Zeitung titulierte diese Form des Datenerhebens als den „totalen Agrar-Überwachungsstaat". Abgesehen von Datenschutzgesichtspunkten, die einer derart umfassenden und rechtlich nicht gesicherten Überwachung entgegenstehen, stellt sich die Frage, ob der Nutzen solcher Maßnahmen den verwaltungstechnischen Aufwand rechtfertigt.

7. Statistik

7.1 Volkszählung 1987

Auswirkungen der Volkszählung 1987 bekam jetzt ein Bürger von seinem Finanzamt zu spüren. Das Finanzamt hatte Angaben der Gebäude- und Wohnungszählung im Statistischen Vierteljahresbericht Hannover ausgewertet, in der auch Tabelleneinsen enthalten waren. Es benutzte die Statistikzahl als Mietspiegel im wahrsten Sinne des Wortes und konnte so den vom Steuerpflichtigen in seiner Steuererklärung angegebenen Wert um fast 1,— DM/qm erhöhen.

Ich habe die Veröffentlichung von Tabelleneinsen als Verletzung der Vorschriften des Niedersächsischen Statistikgesetzes sowie des Volkszählungsgesetzes gegenüber der betreffenden Kommune beanstandet. Sie hat nunmehr ein Anonymisierungsverfahren eingeführt, das eine Rückerkennbarkeit zukünftig verhindern soll. Das Verfahren wurde mit mir abgestimmt.

7.2 Volkszählung 2000?

Das Bundesverfassungsgericht hat in seiner Entscheidung zur Volkszählung 1983 festgestellt, daß der Gesetzgeber vor der Anordnung jeder zwangsweise durchzuführenden Totalerhebung gehalten ist zu prüfen, ob diese nach dem jeweils aktuellen Stand der sozialwissenschaftlichen und statistischen Methoden noch verhältnismäßig ist. Seine „Methodenwahl" ist jeweils wissenschaftlich neu zu legitimieren, verbunden mit der Pflicht, bei geänderten Umständen ggf. von einer Befragung aller Bürgerinnen und Bürger abzusehen. Anläßlich der Volkszählung 1987 wurde nun von Gegnerinnen und Gegnern bestritten, daß diese Erhebung noch den Erfordernissen des Verfassungsgerichts entspräche. Diese Bewertung hat das Verfassungsgericht nicht geteilt. Für mich bleibt auch nach Auswertung der Volkszählung 1987 die Frage offen, ob diese sehr weit in das informationelle Selbstbestimmungsrecht der Menschen eingreifende Vollerhebung sinnvoll war.

Schon jetzt werden Konzepte für die Volkszählung im Jahr 2000 entwickelt. Im November 1991 veranstaltete das Statistische Bundesamt einen Fachkongreß unter dem Titel „Volkszählung 2000 — oder was sonst?" Es schien vorrangig zu interessieren, wie die Zählung effektiver durchgeführt werden kann, beispielsweise durch den Einsatz von Laptops. Im Sinne des Datenschutzes wenig glücklich ist auch der Vorschlag, zentrale Landesmeldebehörden einzurichten, wo Meldedaten mit Zusatzangaben angereichert werden sollen. Eine solche Registerzählung würde es erfordern, daß von vornherein gegenüber den bisherigen Beständen ein erheblich umfangreicherer Datenbestand vorgehalten werden müßte. Das Nachdenken, ob auf die gut zweitausend Jahre alte Methode „Volkszählung" verzichtet werden kann, scheint nicht weit vorangekommen zu sein.

7.3 Landesamt für Statistik

Durch Beschluß des Landesministeriums wurde mit Wirkung vom 1. Juli 1991 ein Niedersächsisches Landesamt für Statistik eingerichtet (Nds. MBl. S. 803). Damit wurde auch dem von mir eingebrachten Vorschlag, im Interesse einer datenschutzgerechten Abschottung der Statistik von anderen Verwaltungsaufgaben die Statistik aus dem Landesverwaltungsamt herauszulösen, Rechnung getragen. Die Aufgaben der Landesstatistikbehörde sind in einer Statistischen Ordnung vom 11. Oktober 1988 (Nds. MBl. S. 927) festgelegt.

7.4 Gebäude- und Wohnungsstichprobe

Das nicht zuletzt durch Kritik der Datenschutzbeauftragten von der Bundesregierung fallengelassene Vorhaben aus dem Jahre 1989, eine Gebäude- und Wohnungsstichprobe durchzuführen, ist nunmehr wieder aufgegriffen worden. In den neuen Entwurf eines Wohnungsstatistikgesetzes sind die wesentlichen Punkte aus dem gescheiterten Entwurf von 1989 übernommen und um eine Vollerhebung in den neuen Bundesländern ergänzt worden. Ich werde meine datenschutzrechtliche Kritik am Erhebungsprogramm und -verfahren erneuern und gegenüber den beteiligten Ressorts artikulieren.

7.5 Bevölkerungsstatistik

Auch der neue Entwurf zum Gesetz über die Bevölkerungsstatistik stößt auf eine Vielzahl von datenschutzrechtlichen Kritikpunkten. Dies sieht auch der Bundesminister der Justiz so. Die Kritikpunkte wurden dem Bundesminister des Innern vorgelegt. Eine Reaktion ist noch nicht erkennbar.

7.6 Krankenhausstatistik

Die von einer Kommunalen Datenverarbeitungszentrale erwogene Erstellung der Krankenhausstatistik in Kombination mit den für die Mitgliedskrankenhäuser durchgeführten Patientenabrechnungsverfahren habe ich als unzulässig angesehen. Schon die Weitergabe von Patientendaten zu Abrechnungszwecken an eine außenstehende Datenverarbeitungszentrale im Rahmen von Auftragsdatenverarbeitung ist nicht unproblematisch. Noch problematischer erscheint mir aber eine Auftragsdatenverarbeitung von sensitiven medizinischen Daten, wie sie zur Erstellung der Krankenhausstatistik benötigt werden. Überdies enthält die Krankenhausstatistik-Verordnung in Verbindung mit § 28 Abs. 1 des Krankenhausfinanzierungsgesetzes keine Befugnis zur perso-

nenbezogenen Erfassung und Speicherung von Statistikdatensätzen. Die Kommunale Datenverarbeitungszentrale hat das geplante Verfahren nicht realisiert.

7.7 Strafverfolgungsstatistik

Das Strafverfolgungsstatistikgesetz ist noch nicht verabschiedet. Ich bezweifele, daß die Strafrechtspflegestatistiken zukünftig überhaupt noch erhoben werden können, weil neun Jahre nach dem Volkszählungsurteil der „Übergangsbonus" sehr fraglich geworden ist und die Statistiken ohne gesetzliche Grundlage sind.

Mit der Forderung nach Vorlage eines Referentenentwurfes für ein Strafverfolgungsstatistikgesetz, auf dessen Grundlage eine weitere Diskussion stattfinden kann, stehen die Datenschutzbeauftragten nicht allein. Auch Vertreter der Statistischen Ämter, der Wissenschaft und der Justizminister der Länder fordern ein baldiges Gesetz. Ich habe mich mit dem Niedersächsischen Justizministerium in Verbindung gesetzt, das zur Zeit den Vorsitz in der Bund-Länder-Konferenz der Justizminister innehat.

7.8 Kinder- und Jugendhilfestatistik

Gegen die Absicht einer Stadt, die in den §§ 98 bis 103 KJHG (SGB VIII) geregelte Kinder- und Jugendhilfestatistik u.a. mit den Merkmalen Straße und Hausnummer der Wohnanschrift zu ergänzen und dann für Zwecke der Jugendhilfeplanung nach § 80 KJHG nutzbar zu machen, habe ich Zweifel geltend gemacht. Ich bin der Ansicht, daß eine Bundesstatistik mit den genannten Zusatzangaben nicht als eigene Geschäftsstatistik geführt werden darf. Auch wäre mit dieser Kommunalstatistik ein Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen verbunden, weil mit geringem Zusatzwissen eine Identifizierung möglich wäre. Zudem besteht für die geplante Übermittlung personenbeziehbarer Daten durch die Träger der freien Wohlfahrtspflege keine Rechtsgrundlage.

7.9 Agrarberichterstattung

Die vom Niedersächsischen Innenministerium entworfene Verordnung, in der u.a. Regelungen zur Bestimmung der Erhebungsstelle und zur Sicherung des Statistikgeheimnisses getroffen werden, ist immer noch nicht in Kraft getreten, obwohl die Erhebungen seit mehreren Jahren durchgeführt werden. Das Innenministerium ist aufgerufen, sich für eine baldige Verabschiedung der Verordnung einzusetzen.

7.10 EG-Statistiken

Die unter X 7.9 erwähnte Verordnung des EG-Rates vom 11. Juni 1990 beinhaltet die Leitlinien für die Übermittlung von statistischen Daten an das Statistische Amt der Europäischen Gemeinschaften. Damit soll sichergestellt werden, daß die Kommission alle erforderlichen Maßnahmen trifft, um die Vertraulichkeit der übermittelten Daten zu gewährleisten. Nach dem jetzt vorliegenden Entwurf eines Gesetzes zur Gewährleistung der Geheimhaltung der dem Statistischen Amt der Europäischen Gemeinschaften (SAEG) übermittelten vertraulichen Daten werden die Beamten und sonstigen Bediensteten des

SAEG für die Anwendung von Strafvorschriften deutschen Amtsträgern gleichgestellt; dadurch ist bei einer Geheimhaltungsverletzung eine Strafverfolgung möglich. Diese Regelung ist grundsätzlich zu begrüßen. Allerdings bleibt insgesamt zu bemängeln, daß es wegen Fehlens einer europäischen Datenschutz-Instanz keine direkten Einflußmöglichkeiten auf die Vorhaben des SAEG gibt.

7.11 EXPO 2000

Die Durchführung der Bürgerbefragung in Hannover zur EXPO 2000 wurde von mir auf Datenschutzverstöße hin kontrolliert. Viele Bürgerinnen und Bürger hatten in Eingaben und telefonischen Anfragen die Befürchtung geäußert, daß die auf den Antwortkarten befindliche Codenummer Rückschlüsse auf ihre Person zulasse. Der Kontrollbesuch bei der Landeshauptstadt ergab keinen Grund zu datenschutzrechtlichen Beanstandungen. Die Codenummer ließ lediglich Rückschlüsse auf den Wohnbezirk der befragten Personen zu. Eine Rückerkennung auf die antwortende Person war nicht möglich; die für die Zustellung der Befragungsvordrucke notwendige Datei wurde vernichtet.

Allerdings habe ich die unzureichende Information der Bürgerinnen und Bürger über den Verfahrensablauf der Befragung zur EXPO 2000 kritisiert; Aufregung und Ärger hätten vermieden werden können.

Auch in der Stadt Laatzen fand eine Bürgerbefragung zur geplanten EXPO 2000 statt. Erfreulicherweise suchte die Stadt von sich aus das Beratungsgespräch mit mir.

8. Archivwesen: Demnächst ein neues Gesetz für Niedersachsen

Meine im X. Tätigkeitsbericht geäußerte Hoffnung, im nächsten, also dem vorliegenden Bericht ein verabschiedetes Archivgesetz darstellen zu können, hat sich nicht erfüllt. Ende 1991 beschloß das Kabinett den Entwurf eines Archivgesetzes (NArchG), zu dem ich nochmals detailliert Stellung nahm. Ich konnte erreichen, daß in Hinblick auf den Datenschutz noch einige Klarstellungen und Verbesserungen vorgenommen wurden.

Die federführende Staatskanzlei sah es nicht als erforderlich an, durch besondere Regelungen die Erschließbarkeit elektronischer Datenträger sicherzustellen (vgl. X 8.2). Automatisiert gespeicherte Informationen sollen vielmehr durch dauernde Datenpflege mit modernem Gerät auswertbar sein. Bei systemtechnischen Änderungen ist vorgesehen, die vorhandenen Daten auf das neue System zu übertragen. Um zu vermeiden, daß löschungspflichtige elektronisch gespeicherte Daten für Archivzwecke nicht verloren gehen, sieht der Entwurf vor, daß schon während der Verarbeitung, nicht erst zum Zeitpunkt der geplanten Löschung, über die Archivwürdigkeit entschieden wird.

Inzwischen stellt der Entwurf klar, daß unzulässig gespeicherte Daten nicht der Anbietungspflicht unterliegen und auch nicht vom Archiv übernommen werden dürfen.

Unklar war zunächst, ob im Einzelfall schutzwürdige Belange von Betroffenen nach Ablauf der relativ langen Schutzfristen die archivalische Nutzung ausschließen sollten. Archivgut soll nach dem künftigen § 5 Abs. 2 NArchG 30 Jahre nach der letzten inhaltlichen Bearbeitung, bei Unterlagen zu einer bestimmten Person 10 Jahre nach deren Tod für die archivalische Nutzung freigegeben werden. Die Schutzfristen haben zweifellos auch die Aufgabe, Verletzungen des Persönlichkeitsrechts zu verhindern, und dürften für diesen Zweck zumeist ausreichen. Es ist daher aus datenschutzrechtlicher Sicht akzeptabel, daß der Entwurf zum Niedersächsischen Archivgesetz darauf verzichtet, den Datenschutz als ein Beispiel für ein Nutzungsverbot nach Fristablauf aufzuführen. Dessenungeachtet sind meines Erachtens Fälle denkbar, in welchen das Schutzfristensystem sowohl zum Schutz Betroffener wie auch Dritter, also etwa Verwandter, nicht ausreicht. Auch in solchen Ausnahmefällen kann nach der aktuellen Formulierung des Entwurfes die Archivnutzung ausgeschlossen werden.

Ausdrücklich zu begrüßen ist schließlich, daß sich die Staatskanzlei bereiterklärte, den Betroffenen neben dem Anspruch auf Auskunft einen Anspruch auf Akteneinsicht einzuräumen.

Am 1. Dezember 1992 hat das Kabinett beschlossen, den Entwurf ins Gesetzgebungsverfahren einzubringen. Es ist zu hoffen, daß dieser schlanke, datenschutzrechtlich ausgereifte Entwurf in Bälde die parlamentarischen Hürden nimmt und die gesetzlose Zeit in den staatlichen Archiven Niedersachsens beendet. Nach Verabschiedung des Gesetzes bedarf es dann Ausführungsvorschriften, welche den Umgang mit dem Archivmaterial konkretisieren. Es wurde mir zugesagt, daß ich auch bei dem Erlaß dieser Vorschriften rechtzeitig beteiligt werde.

Auch wenn demnächst ein Niedersächsisches Archivgesetz in Kraft treten wird, so bestehen im Lande immer noch keine alle öffentlichen Archive umfassenden Rechtsvorschriften, da der Regelungsbereich des NArchG aus Rücksicht auf die kommunale Selbstverwaltung kommunale Archive nicht mit erfaßt. Die meisten Kommunen haben zwar eigene Archive, eine Satzung hierfür ist aber in vielen Fällen nicht vorhanden. Nachdem für staatliche Archive die Regelungslücke ausgefüllt wird, muß nun auch dieses Defizit behoben werden.

9. Neue Medien

9.1 Telekommunikation

9.1.1 Rechtsgrundlagen in Bewegung

„Telekommunikation und Datenschutz" scheint zu einem Dauerthema von Datenschutzbeauftragten, von Wissenschaftlerinnen und Wissenschaftlern sowie von Bürgerrechtsgruppen zu werden. In zahlreichen Beschlüssen haben nationale und internationale Datenschutzgremien auf die besonderen Gefährdungen durch eine dynamische Technikentwicklung auf dem Gebiet der Telekommunikation hingewiesen (vgl. Anlage 2). Sie haben bessere rechtliche Absicherungen des Brief-, Post- und Fernmeldegeheimnisses und des nicht öffentlich gesprochenen Wortes eingefordert. Die nationalen Reizthemen Speicherung der kompletten Verbindungsdaten einschließlich der Zielnummern

in einem zentralen Postcomputer, Ausdruck dieser Daten in einem Einzelentgeltnachweis und zwangsweise Anzeige der Rufnummer des anrufenden Anschlusses am Apparat der oder des Angerufenen schienen durch zwei Datenschutzverordnungen aus dem Jahr 1991 zum größten Teil bereinigt zu sein: Am 1. Juli 1991 trat die „Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TELEKOM-Datenschutzverordnung — TDSV)" vom 24. Juni 1991 (BGBl. I S. 1390) in Kraft. Die „Verordnung über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (Teledienstunternehmen-Datenschutzverordnung — UDSV)" wurde am 12. Dezember 1991 mit Zustimmung des Bundesrates von der Bundesregierung beschlossen und am Tag nach Verkündung in Kraft gesetzt (BGBl. I S. 2337).

Noch bevor die Regelungen vollständig umgesetzt waren, wurde auch schon deren Überarbeitung erforderlich. Das Bundesverfassungsgericht stellte in seinem „Fangschaltungsbeschluß" vom 25. März 1992 (NJW 1992, 1875) u. a. fest, daß die Erfassung von Ferngesprächsdaten mittels Fangschaltung und Zählervergleichseinrichtungen einer gesetzlichen Grundlage bedarf und daß § 30 des Postverfassungsgesetzes keine ausreichende gesetzliche Ermächtigung zum Erlaß solcher Regelungen bildet. Das Urteil und andere neuere Entscheidungen des BVerfG zwingen die Bundesregierung dazu, alle Regelungen der TDSV und der UDSV völlig neu zu überdenken.

Nach Vorstellung der Datenschutzbeauftragten des Bundes und der Länder sollten die Einschränkungen des Fernmeldegeheimnisses, die sich insbesondere aus der Speicherung von Verbindungsdaten ergeben, unverzüglich durch Gesetz geregelt werden. Interne Begrenzungen des Fernmeldegeheimnisses, die der Bundesminister für Post und Telekommunikation (BMPT) bisher mit „immanenten Schranken" oder „postbetrieblichen Erfordernissen" begründet hat, sind nach der Rechtsprechung des BVerfG nicht mehr anzuerkennen. Dabei kann sich der Gesetzgeber nicht damit begnügen, lediglich eine Verordnungsermächtigung in das Postverfassungsgesetz und das Fernmeldeanlagengesetz aufzunehmen. Die zu schaffenden gesetzlichen Regelungen müssen grundlegende inhaltliche Festlegungen enthalten, in welchem Umfang die Netzbetreiber und Diensteanbieter personenbezogene Daten ihrer Kundinnen und Kunden verarbeiten dürfen. Es sollte der Grundsatz festgeschrieben werden, daß Verbindungsdaten nach Beendigung der Verbindung zu löschen sind. Dies ist dann realisierbar, wenn die Gebühren in der jeweiligen Ortsvermittlungsstelle errechnet werden. Von dieser Verfahrensweise darf nur dann abgewichen werden, wenn die Kundin oder der Kunde einen Einzelentgeltnachweis beantragt, auf dem allerdings nur um mindestens vier Stellen verkürzte Zielnummern ausgewiesen sein sollten. Damit würde das Regel-Ausnahme-Verhältnis der bisherigen TDSV-Regelung umgekehrt.

Die erforderliche gesetzliche Regelung der Datenverarbeitung in der Telekommunikation sollte auch einheitliche Verarbeitungsregeln für die sonstigen Dienste (z.B. Telefax, Telebox, Mailbox, Mobilfunk) enthalten. Lediglich Detailregelungen der Datenverarbeitung dürfen durch Rechtsverordnung getroffen werden. Dabei müßten allerdings die geltenden TDSV und UDSV grundlegend überarbeitet werden.

Ein weiterer Änderungszwang wird sich recht bald aus der „Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im dienstintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen" ergeben. Die EG-Richtlinie wird nach eingehender Beratung im Parlament derzeitig von der Kommission überarbeitet. Die Verabschiedung dieser Richtlinie ist in Kürze zu erwarten. Sie sieht aus Sicht des Datenschutzes einige Verbesserungen gegenüber TDSV und UDSV vor; z. B. ver-

pflichtet sie zur Zielnummernverkürzung und zur Wahlmöglichkeit der fallweisen Unterdrückung der Rufnummernanzeige. TDSV und UDSV sind spätestens nach Verabschiedung der EG-Richtlinie inhaltlich anzupassen (vgl. 6.1).

9.1.2 Verbindungsdaten

§ 5 TDSV und § 5 UDSV regeln wortgleich den Umfang der Daten, die zur Bereitstellung von Telekommunikationsdienstleistungen erhoben und verarbeitet werden dürfen. Dazu zählen neben der Kennung des anrufenden Anschlusses, die in Anspruch genommene Dienstleistung, personenbezogene Berechtigungskennungen und Kartennummern, der Zeitpunkt der Verbindung und die Rufnummer des angerufenen Anschlusses. Bei mobilen Anschlüssen wird auch die Standortkennung als Verbindungsdatum gespeichert. Die Verbindungsdaten dürfen über das Verbindungsende hinaus vollständig gespeichert werden, so z. B.

— zum Ermitteln und Abrechnen der Entgelte,
— zum Erkennen, Eingrenzen und Beseitigen von Störungen und
— zum Abrechnen mit anderen Netzbetreibern.

Die Forderung der Datenschutzbeauftragten des Bundes und der Länder nach frühestmöglicher Löschung nicht mehr erforderlicher Daten (z.B. der Zielrufnummer) wurde nicht hinreichend erfüllt (vgl. Anlage 2).

Auf eine positive Teillösung möchte ich trotz meiner Kritik hinweisen: Die Telefonkunden haben die Wahlmöglichkeit erhalten, ob mit Versenden der Entgeltrechnung die Verbindungsdaten vollständig gelöscht oder ob sie unter Verkürzung der Zielrufnummer um die letzten drei Ziffern 80 Tage nach Rechnungsversand gespeichert bleiben sollen. Bei Beziehern von Einzelentgeltnachweisen bleiben die Verbindungsdaten für diese Zeit vollständig gespeichert. Den angerufenen Teilnehmern (Zielnummer) wurden bei dieser Regelung keine schützenswerten Belange zuerkannt.

9.1.3 Rufnummernanzeige

Mit moderner Telekommunikationstechnik ist es möglich, die Rufnummer der Anruferin bzw. des Anrufers auf dem Anzeigedisplay des angerufenen Telefons anzuzeigen. Diese neue Funktion mag von vielen begrüßt werden, weil es so möglich wird, lästige oder ersehnte Anrufe vor Aufnahme des Hörers zu erkennen und entsprechend zu reagieren. Diese Funktion ist aber bei Personen und Einrichtungen, die auf Vertrauensschutz und Anonymität des Partners angewiesen sind, höchst unerwünscht oder gar bedenklich. Im Sinne der informationellen Selbstbestimmung sollten Telefonkunden selbst entscheiden können, ob sie im Einzelfall ihre Rufnummer beim angerufenen Apparat anzeigen lassen wollen oder nicht. Dies schreibt auch die EG-Richtlinie zum Datenschutz bei ISDN vor. TDSV und UDSV dagegen kennen nur ein „Entweder — Oder". Telefonkunden können zwischen Anzeige bei jedem Anruf oder dem dauernden Ausschluß wählen. Erst ab 1. Januar 1994 soll den Telefonkunden die Wahlmöglichkeit bei jedem Anruf offenstehen, vorausgesetzt die eingesetzten Geräte verfügen über entsprechende Funktionen.

Das Konzept der Deutschen Bundespost TELEKOM zur Technikentwicklung läßt Zweifel zu, ob das erkennbare Datenschutz-Anliegen dieser Wahlmöglichkeit wirklich verfolgt wird. Offenbar plant die TELEKOM bis Ende der neunziger Jahre ISDN-Anschlüsse auch ohne fallweise Möglichkeit der Unter-

drückung der Rufnummernanzeige anzubieten, „sofern der Markt dies erfordert." Diese erkennbare Planungsabsicht und ihr Hinweis „auf den Markt" stehen in deutlichem Widerspruch zu § 9 Abs. 1 Satz 2 TDSV. Dies kann aus der Sicht des Datenschutzes nicht hingenommen werden.

9.1.4 Vertrauensschutz für Beratungsstellen

Durch Rufnummernanzeige und Einzelentgeltnachweis mit dem vollständigen Ausdruck aller geführten Gespräche einschließlich vollständiger Zielnummer kann die Arbeit derjenigen Personen und Institutionen beeinträchtigt werden, die in ihrer Beratungsfunktion in besonderem Maße auf Anonymität der Kontakte angewiesen sind. Auf diese Gefahren und auf besondere Schutzmaßnahmen habe ich in einer Presseerklärung und durch ein Aufklärungsschreiben an betroffene Ressorts der Landesregierung sowie an die kommunalen Spitzenverbände hingewiesen. Ich habe empfohlen, die in Betracht kommenden Stellen auf die bestehenden Risiken aufmerksam zu machen und ihnen folgende Handlungsempfehlung zu geben:

— Beratungseinrichtungen sollten bei der TELEKOM und sonstigen von ihnen in Anspruch genommenen Telekommunikations-Diensteanbietern beantragen, daß ihre Telefonnummern nicht auf Einzelentgeltnachweisen der Teilnehmerinnen und Teilnehmer erscheinen. Der Anruf bei Personen, Behörden und Organisationen, die besonderen Verschwiegenheitsverpflichtungen unterliegen und die Beratungsaufgaben in sozialen oder kirchlichen Bereichen ganz oder überwiegend über Telefon abwickeln, darf aus dem Einzelentgeltnachweis nicht ersichtlich sein. Auf Antrag einer solchen Person, Behörde oder Organisation ist der Dienstebetreiber verpflichtet, durch technische Vorrichtungen die Beachtung der Vorschrift des § 6 Abs. 9 Satz 5 TDSV (ebenso UDSV) sicherzustellen. Antragsberechtigt sind gesundheitliche, psychologische und psychiatrische Beratungsstellen, Suchtberatungsstellen, Ehe- und Schwangerschaftsberatungsstellen, Frauenhäuser und Beratungsstellen für vergewaltigte oder mißhandelte Frauen, Erziehungs- und Jugendberatungsstellen, Schuldnerberatung, Telefonseelsorge, Personal- und Betriebsräte, allgemeine Beratungsstellen, in denen auch in sozialen Angelegenheiten beraten wird, sowie Einrichtungen der Wohlfahrtsverbände.

— Beratungseinrichtungen können beantragen, daß auf ihren Telefonapparaten die Nummer der Anruferin bzw. des Anrufers generell nicht angezeigt wird. Für Sprachkommunikationsdienste ist auf Antrag die Übermittlung der Rufnummer des anrufenden Anschlusses an den angerufenen Anschluß einer der genannten Personen, Organisationen und Behörden in der Vermittlungsstelle dieses Anschlusses auszuschließen (jeweils § 9 Abs. 1 Satz 3 TDSV und UDSV). Auch ich habe für meine Geschäftsstelle dies beantragt, um mein mir auferlegtes Beratungsgeheimnis zu wahren und Benachteiligungen von Menschen, die mich telefonisch um Rat bitten, auszuschließen. Eine Antwort steht noch aus. Forderungen nach entsprechender Sicherung des Berufsgeheimnisses von Psychologen, Ärzten, Anwälten und Journalisten sind abgelehnt worden. Die Antragstellung ist auch dann sinnvoll, wenn (noch) keine digitalisierten Telefonanlagen installiert sind. Dadurch werden rechtzeitige Vorkehrungen gegen die dargestellten Gefahren ermöglicht. Sie führen außerdem zu Vermerken im Telefonbuch, daß bestimmte Stellen keine Rufnummernanzeige zulassen.

9.2 Interne Telekommunikationsanlagen

Wenn heute eine neue Telefonanlage ausgewählt und installiert wird, kommt nur noch neueste Digitaltechnik zum Einsatz. ISDN-Fähigkeit ist „Stand der Technik". ISDN-Nebenstellenanlagen — wie solche internen Telekommunikationsanlagen auch genannt werden — sind Rechnersysteme, die Kommunikationswege schalten sowie Sprache, Texte, Daten und Bilder übertragen und speichern. Die dabei angewandte Digitaltechnik bewirkt nicht nur bessere und störungsfreie Verständigung beim Telefonieren, sondern führt auch zu neuen Nutzungsformen, so z.B. zu der gleichzeitigen Benutzung von Telefax- und Teletex-Diensten oder der Steuerung eines lokalen Rechnernetzes. Durch die neue Technik werden in bisher nicht gekannter Weise Verbindungs-, Abrechnungs- und Benutzungsdaten gespeichert. ISDN-Nebenstellenanlagen verarbeiten personenbezogene Daten in automatisierter Form. Für einen ordnungsgemäßen Betrieb einer solchen Anlage sind die erforderlichen technischen und organisatorischen Maßnahmen gemäß § 6 NDSG zu treffen. Maßstab dafür, welche Maßnahmen im einzelnen zu realisieren sind, ist nicht allein die Frage, welche Daten konkret verarbeitet werden sollen, sondern auch, welche Möglichkeiten — auch ungenutzte — diese Systeme bieten. Sowohl die Auswahl der einzelnen Leistungsmerkmale, mit denen eine solche Anlage ausgestattet werden soll, als auch die Beachtung der Einhaltung des Schutzes des gesprochenen Wortes müssen unter Datenschutzgesichtspunkten erfolgen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer „Entschließung zum Datenschutz bei internen Telekommunikationsanlagen" vom 1./2. Oktober 1992 auf den Schutz des Fernmeldegeheimnisses und des nicht öffentlich gesprochenen Wortes gerade auch bei Arbeitnehmerinnen und Arbeitnehmern hingewiesen. Sie fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen Telekommunikationsanlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden (vgl. Anlage 10).

Ich habe eine „Orientierungshilfe für die Beschaffung und den Einsatz von ISDN-Nebenstellenanlagen" erarbeitet und an behördliche Datenschutzbeauftragte verteilt. Die Orientierungshilfe kann bei mir von allen Interessierten bezogen werden.

9.3 Fernwirken und Fernmessen

Mein langjähriger „Ruf" nach einer landesgesetzlichen Regelung zur Durchsetzung und Sicherung datenschutzrechtlicher Mindestanforderungen beim TEMEX-Dienst (vgl. IX 9.3 und X 9.3) ist vom Niedersächsischen Innenministerium nunmehr gehört und umgesetzt worden. § 26 NDSG-E enthält eine Regelung, die sich in erster Linie an öffentlich-rechtliche Unternehmen richtet. Das neue NDSG wird eine Unterrichtungspflicht einführen, die zu mehr Transparenz für die Betroffenen führt. Betroffene können so die Vor- und Nachteile einer von einem Versorgungsunternehmen vorgesehenen technischen Lösung für sich selbst abwägen. Sie dürfen auch nicht durch einen rechtlichen oder faktischen Anschluß- und Benutzungszwang in ihrer Entscheidungsfreiheit beeinflußt werden.

9.4 Telefax

Unter X 9.4 habe ich auf besondere Gefahren sowie auf datenschutzrechtliche Probleme und Sicherheitsrisiken beim Telefax-Dienst der Deutschen Bundes-

post aufmerksam gemacht. Zahlreiche Anfragen und Beratungswünsche belegen ein lebhaftes Echo. Noch nicht abgeschlossen ist die Klärung des Anliegen der Landeshauptstadt Hannover, ärztliche Gutachten als Grundlage einstweiliger Unterbringung nach § 3 PsychKG per Telefax zu übermitteln. Eine offene Telefax-Übertragung ist mit dem (strafbewehrten) Schutz des Arztgeheimnisses nicht vereinbar. Die Aufforderung der Stadt, an alle mit ihr zusammenarbeitenden psychiatrischen Kliniken und Krankenhäuser, Gutachten nur noch per Telefax zu übertragen, halte ich solange für datenschutzrechtlich bedenklich, wie nicht der gesamte Übertragungsvorgang einschließlich des Weges gesichert ist. Bei der datenschutzrechtlichen Beurteilung der Telefax-Übermittlung ist „das schwächste Glied in der Kette" entscheidend.

Die Sicherheitsrisiken bei Telefax, die ich vor zwei Jahren beschrieben habe, bestehen heute unverändert, auch wenn einige technische Lösungsansätze für eine gesichertere Übertragung erkennbar sind. Im folgenden fasse ich meine bisher gegebenen Hinweise und Empfehlungen zum datenschutzgerechten Einsatz von Telefax-Geräten zusammen:

1. Telefax ist abhörbar! Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden. Die absendende Person trägt die Verantwortung für die gesicherte Übertragung und für den befugten Empfang.

2. Daten, die einem besonderen Berufs- oder Amtsgeheimnis unterliegen oder aus anderen Gründen als „sensibel" einzustufen sind (Sozial-, Steuer-, Personal- und medizinische Daten), dürfen grundsätzlich nicht gefaxt werden!

3. Stellen Sie Telefax-Geräte so auf, daß Unbefugte keine Kenntnis vom Inhalt eingehender oder übertragener Telefax-Schreiben erhalten können.

4. Nutzen Sie alle geräteseitigen Sicherungs-Maßnahmen (z.B. Anzeige der störungsfreien Übertragung, gesicherte Zwischenspeicherung, Abruf nur nach Paßworteingabe)!

5. Überprüfen Sie sofort die vom empfangenden Gerät abgegebene Kennung, damit die Verbindung bei Wählfehlern sofort abgebrochen werden kann.

6. Verständigen Sie sich vor der Absendung sensibler Daten mit dem Adressaten über den genauen Zeitpunkt der Übertragung und sichern Sie, daß keine unbefugten Personen Einblick nehmen können.

7. Denken Sie an Ihre Dokumentationspflichten, z. B.
   — Vorblatt der Behörde bzw. des Unternehmens,
   — Anzahl der Kopien angeben,
   — Originale mit Verifikationsstempel versehen,
   — Protokolle sorgfältig aufbewahren.

8. Die richtige Bedienung und die zulässige Nutzung von Telefax-Geräten sollten in einer schriftlichen Dienstanweisung geregelt sein.

Telefax-Geräte sind kleine Rechner mit begrenzter Speicherfähigkeit. Fast alle Geräte speichern die Verbindungsdaten in einem besonderen Protokollbereich, einige speichern darüber hinaus auch die ankommenden und die abzusendenden Faxinhalte. Ein Bürger hat mich darauf aufmerksam gemacht, daß er nach Erwerb eines Gebrauchtgerätes alle Aktivitäten des Vorbesitzers rekonstruieren konnte; an die Löschung hatte keiner gedacht. Das Löschen wird der Benutzerin bzw. dem Benutzer allerdings auch nicht leicht gemacht. Zwar ist eine Löschfunktion geräteseitig vorhanden; sie ist jedoch meist nur Wartungs-

technikern zugänglich. Vor Verkauf oder Weitergabe von Altgeräten sollte diese Schwachstelle beachtet werden; notfalls ist die Herstellerfirma zu befragen.

9.5 Landesrundfunkgesetz

Die Niedersächsische Staatskanzlei hat mich frühzeitig über Novellierungsabsichten zum Niedersächsischen Landesrundfunkgesetz informiert und mir Gelegenheit zur Mitarbeit an den datenschutzrechtlichen Bestimmungen gegeben. Ich begrüße ausdrücklich, daß mir die Datenschutzkontrolle auch gegenüber privaten Veranstaltern gesetzlich zugewiesen werden soll. Damit folgt der Entwurf neueren Entwicklungen, so z. B. in den Ländern Bayern, Hamburg und Berlin. Die materiellrechtlichen Regelungen sollen sich an denen des Staatsvertrags über den Rundfunk im vereinten Deutschland vom 31. August 1991 (GVBl. 1992, S. 41) orientieren. Da die Abstimmung noch im Gange ist, kann über weitere Details nicht berichtet werden.

10. Personenstandswesen

10.1 Datenschutz im Adoptionsverfahren

Die Wahrung des Adoptionsgeheimnisses ist ein Thema, mit dem sich meine Dienststelle seit ihrer Einrichtung immer wieder auseinandersetzen muß. Im einem Merkblatt, welches interessierte Aufnahme fand, habe ich die Auszüge aus dem I. bis zum X. Tätigkeitsbericht zusammengefaßt. Das Merkblatt kann weiterhin bei mir angefordert werden. Wie Eingaben aus dem Berichtszeitraum zeigen, hat sich das Thema in Niedersachsen aber noch lange nicht erledigt.

In einer Eingabe wurde die Verletzung des Datenschutzes im Zusammenhang mit dem Verfahren zur Beurkundung der Geburt eines zur Adoption freigegebenen Kindes gerügt. Die Petentin hatte ihr Kind nicht an ihrem Wohnort, sondern in einem Krankenhaus einer anderen niedersächsischen Stadt entbunden. Sie hatte dort einen privaten Träger mit der Adoptionsvermittlung einschließlich aller Behördengänge beauftragt. Folgerichtig wurde beim Standesamt des Geburtsortes beantragt, daß der Meldebehörde der Petentin keine Mitteilung über die Geburt des Kindes gemacht werden sollte.

Dennoch hatte die Kindesmutter durch das örtliche katholische Pfarrbüro in ihrer Heimatgemeinde erfahren, daß dort die Daten ihres Kindes unter ihrer Wohnadresse dateimäßig verarbeitet wurden. Wie sich herausstellte, hatte das Standesamt der Wohngemeinde eine Meldung des Geburtsstandesamtes erhalten. Auch die Geschäftsstelle eines freien Trägers im Heimatbereich der Kindesmutter hatte von der Geburt des zur Adoption freigegebenen Kindes Kenntnis erhalten.

Das Geburtsstandesamt hatte korrekterweise eine Kopie aus dem dortigen Geburtenbuch an das Wohnort-Standesamt der Petentin übersandt. Rechtsgrundlage hierfür ist § 15 Abs. 1 Nr. 1 PStG, wonach für den Fall, daß ein eheliches Kind nach der Geburt in Adoptionspflege gegeben wird, es gleichwohl zunächst in das Familienbuch der leiblichen Eltern einzutragen ist. Erst mit dem Ausspruch der Adoption scheidet das Kind aus der Familie der leiblichen Eltern aus, was frühestens acht Wochen nach der Geburt möglich ist.

Nach § 276 Abs. 1 Satz 1 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden vom 28. März 1985 (Bundesanzeiger Nr. 68a) hat der Geburtsstandesbeamte dem Familienbuchführer die Geburt des Kindes mitzuteilen, damit es in Spalte 9 des Familienbuches der Eltern eingetragen werden kann.

Während der Standesbeamte des Geburtsortes von einer Mitteilung an die Meldebehörde abgesehen hat, hat das Standesamt am Wohnort der Kindesmutter ohne Verpflichtung die dortige Meldebehörde informiert. Dadurch ist es zu den von der Petentin beanstandeten Datenübermittlungen gekommen. Ich habe die Verletzung des Adoptionsgeheimnisses durch das Wohnort-Standesamt gegenüber dem dortigen Gemeindedirektor gemäß § 19 NDSG beanstandet.

In ihrer Stellungnahme zur Beanstandung hat die Gemeinde den Fehler eingestanden und ausdrücklich darauf hingewiesen, daß es sich dabei um einen Einzelfall handelte, der bedauert wird. Der Standesbeamte ist belehrt worden, sich an die Vorschriften der Dienstanweisung zu halten. Im übrigen seien bei der Meldebehörde die Daten des Kindes umgehend gelöscht worden.

Wegen der Bedeutung des Vorgangs hat das Niedersächsische Innenministerium diesen in anonymisierter Fassung dem Fachverband der Standesbeamten in Niedersachsen zur Kenntnis gegeben, mit der Zielsetzung, in Schulungsveranstaltungen besonders auf die Wahrung des Adoptionsgeheimnisses einzugehen. Auf der Sitzung des Fachausschusses der Standesbeamten Niedersachsens Mitte September 1992 wurde die Sache eingehend erörtert. Es besteht also Hoffnung, daß ich in Zukunft nicht mehr über Verstöße gegen das Adoptionsgeheimnis berichten muß.

10.2 Erteilung von Personenstandsurkunden an „Erbenermittler"

Bei Standesämtern gehen häufiger Anfragen von „Erbenermittlern" mit dem Antrag auf Ausstellung von Personenstandsurkunden ein. Erbenermittler sind Privatpersonen, die im Auftrag des Nachlaßgerichts oder einer Erblasserin oder eines Erblassers versuchen, berechtigte Erben ausfindig zu machen. Hierfür können sie, soweit ein rechtliches Interesse besteht, Personenstandsurkunden beim zuständigen Standesamt beantragen. Da diese Unternehmen teilweise sowohl als Erbenermittler als auch als Genealogen (Ahnenforscher) firmieren, hatte ein Standesamt die Vermutung, daß neben der Erbenermittlung die Daten gespeichert werden, um für Zwecke der Ahnenforschung oder z. B. auch für Anfragen von Inkassofirmen eine Datenbank vorzuhalten.

Besonders deutlich wird dabei der Wunsch nach einer Vielzahl von Daten, wenn die Urkundenanforderung mit der Bitte gekoppelt ist, nach Möglichkeit eine Ablichtung aus dem Personenstandseintrag mit allen zum Eintrag vermerkten Hinweisen zu erstellen. Häufig werden auch Auskünfte aus den Sammelakten erbeten, obwohl die einschränkenden Vorschriften des § 61 PStG und des § 48 der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden allgemein bekannt sind. Das Standesamt hat bei mir angefragt, wie die Vorschrift des § 61 PStG unter datenschutzrechtlichen Gesichtspunkten zu beurteilen ist.

Von besonderer Bedeutung ist dabei die Auslegung des Begriffes „rechtliches Interesse". Es ist zu beachten, daß das rechtliche Interesse nur dann besteht, wenn der Auftrag zur Erbenermittlung von ordentlich bestellten Nachlaßpflegern ergangen ist. Die Standesbeamten geraten bei Ablehnungen von Urkundenanforderungen immer wieder unter Begründungsdruck, da das rechtliche

Interesse zum Erhalt von Urkunden lediglich „glaubhaft zu machen" ist. Der Standesbeamte braucht, so ein einschlägiger Gesetzeskommentar, „in eine Nachprüfung nicht einzutreten". Wohl aber muß bei einer mangelnden Glaubhaftmachung eine Nachprüfung erfolgen.

11. Ausweis- und Meldewesen

11.1 Ausweis und Reisepaß im Postamt

Unter X 16.12 hatte ich die Auffassung des Innenministeriums zitiert, nach der die Übertragung von gemeindlichen Aufgaben, wie der Ausstellung eines Reisepasses oder Personalausweises, auf andere Behörden unzulässig ist. Ich habe erfahren, daß dessenungeachtet Gemeinden vermehrt mit der Deutschen Bundespost Verwaltungsvereinbarungen abgeschlossen haben, die der Bundespost das Recht einräumen, Anträge auf Reisepässe und Personalausweise entgegenzunehmen und ausgestellte Ausweispapiere auszuhändigen. Diese Verfahrensweise ist rechtswidrig, solange die Deutsche Bundespost als unzuständige Stelle Daten der antragstellenden Person verarbeitet. Zur rechtlichen Absicherung der im Interesse der Bürgerinnen und Bürger eingeführten Praxis beabsichtigt das Innenministerium, die Ausweisbehörden im Niedersächsischen Ausführungsgesetz zum Gesetz über Personalausweise zu ermächtigen, andere öffentliche Stellen mit der Entgegennahme von Anträgen und der Aushändigung von Personalausweisen zu beauftragen. Entsprechend muß die Allgemeine Verwaltungsvorschrift zur Durchführung des Paßgesetzes ergänzt werden.

11.2 Einsichtnahme der Polizei in das Personalausweis- bzw. Paßregister

Paß- und Ausweisbehörden sind keine Auskunfteien. Das Personalausweis- und das Paßgesetz enthalten restriktive Vorschriften, die den Zugriff auf die Register bewußt erschweren sollen. Die um Auskunft bittende Behörde darf ohne Kenntnis der Registerdaten nicht in der Lage sein, die ihr übertragene Aufgabe zu erfüllen. Weitere Voraussetzung ist, daß die Daten bei den Betroffenen nicht bzw. nur mit unverhältnismäßigem Aufwand erhoben werden können oder aber die Behörde wegen der Art der Aufgabe von der Datenerhebung bei den Betroffenen absehen muß. Übermittlungsersuchen an die Paß- und Ausweisbehörden dürfen nur Bedienstete stellen, die hierzu besonders ermächtigt sind (vgl. dazu näher den datenschutzgerechten RdErl. des Innenministeriums vom 21. August 1991, Nds. MBl. S. 114). Der Anlaß des Ersuchens sowie die Herkunft der Daten und Unterlagen sind bei der ersuchenden Stelle zu dokumentieren. Aus diesen Rregelungen ergibt sich, daß Personalausweis- und Paßregister nur in äußerst begrenztem Umfang für Datenübermittlungen zur Verfügung stehen.

Aus Eingaben ist mir bekannt, daß Polizeidienststellen die in den Registern vorhandenen Fotografien auswerten, auch um in Verkehrsordnungswidrigkeitenverfahren die Identität von Betroffenen (bei Radarfotos) zu ermitteln. Mit der Einsichtnahme der Polizei in das Register wird in das Recht auf informationelle Selbstbestimmung der Betroffenen eingegriffen. Es erhebt sich die Frage, welche Eingriffsschwelle sich aus dem gesetzgeberischen Willen, diese Datei nicht als Auskunftsregister auszugestalten, und dem Grundsatz der Verhältnismäßigkeit ergibt. In Rheinland-Pfalz wurde beispielsweise durch Dienstvorschrift bestimmt, daß bei Verkehrsordnungswidrigkeiten eine Nut-

zung der Register in der Regel nicht in Betracht kommt. Ich halte dies für einen Schritt in die richtige Richtung. Nicht jede Ordnungswidrigkeit kann die Auswertung des Personalausweis- bzw. Paßregisters rechtfertigen (vgl. 30.1).

Eine Paßbehörde ist an mich mit der Frage herangetreten, ob die Polizei die Herausgabe von Paßbildern unbescholtener Bürgerinnen und Bürger verlangen kann. Bezweckt wurde damit, sog. Wahllichtbildvorlagen, die Zeugen gemeinsam mit den Fotografien von Tatverdächtigen vorgelegt werden, zu ergänzen. Diese Nutzung des Paßregisters halte ich als unverhältnismäßigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen für unzulässig. Auch nach Auffassung des Innenministeriums kommt diese Vorgehensweise schon vom Gesetz her nicht in Betracht.

11.3 Melderechtsrahmengesetz

Nach dem Gesetzentwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes (BT-Drs. 12/2376 vom 6. April 1992) sollen u. a. die Wahlberechtigten das Recht erhalten, der Weitergabe ihrer Daten von der Meldebehörde an Träger von Wahlvorschlägen vor Wahlen zu widersprechen. Niedersächsische Wahlberechtigte haben dieses Widerspruchsrecht schon aufgrund des Niedersächsischen Meldegesetzes (NMG). Auf das Widerspruchsrecht wird bei der Anmeldung sowie mindestens einmal jährlich durch öffentliche Bekanntmachung hingewiesen (vgl. § 34 Abs. 4 NMG).

Die umstrittene Krankenhaus- und Hotelmeldepflicht soll nach dem Gesetzentwurf beibehalten werden. Die (Identitäts-)Angaben können in Niedersachsen für Zwecke der Meldebehörde, der Polizei, der Staatsanwaltschaft und der Verfassungsschutzbehörde verwendet werden (vgl. §§ 18 bis 20 NMG). Die Datenschutzbeauftragten des Bundes und der Länder (mit Ausnahme Bayerns) hatten sich gegen die Meldepflichten ausgesprochen, weil damit alle Hotelgäste und Krankenhauspatienten als Gefahrenquellen bzw. potentielle Straftäter angesehen werden (vgl. X Anlage 16). Ich habe einen erneuten Vorstoß beim Niedersächsischen Innenministerium unternommen, im Rahmen der Beratungen zum o.a. Gesetzentwurf für eine Abschaffung der Krankenhaus- und Hotelmeldepflicht einzutreten. Das Innenministerium ist meiner Anregung nicht gefolgt.

11.4 „Kranzdamen" aus dem Melderegister

Eine niedersächsische Gemeinde hatte der örtlichen Schützengesellschaft Adressenaufkleber mit Namen und Anschriften aller 14- bis 17jährigen Einwohnerinnen zur Verfügung gestellt. Die Daten stammten aus dem Melderegister. Mit Hilfe der Adressenaufkleber hatte die Schützengesellschaft den genannten Personen das Angebot unterbreitet, beim historischen Schützenfest als sogenannte „Kranzdamen" besondere Funktionen zu übernehmen.

Die Datenübermittlung aus dem Melderegister an die Schützengesellschaft war unzulässig. Da half auch nicht der Hinweis der Gemeinde, daß das alljährliche Schützenfest auf eine langjährige Tradition zurückblicken kann und ein Stück lebendiger Stadtgeschichte verkörpert. Eine Gruppenauskunft, und darum handelte es sich melderechtlich bei der Weitergabe der Adressenaufkleber, darf nur erteilt werden, soweit sie im öffentlichen Interesse liegt. Diese Voraussetzung erfordert eine Abwägung der beteiligten Interessen. Dabei überwiegen die schutzwürdigen Belange der 14- bis 17jährigen jungen Damen. Bei ihnen handelt es sich um Minderjährige, die dem Sorgerecht der Erziehungsberechtigten unterliegen. Sie sind wegen ihres Alters besonders

schutzwürdig. Die Fortführung dieser örtlichen Tradition ist auf Melderegisterdaten nicht angewiesen. Die Schützengesellschaft könnte nämlich ihre Interessen durch öffentliche Aufrufe oder Zeitungsanzeigen verfolgen.

11.5 Sammellisten für die Aktion „Rußlandhilfe"

Bei Gruppenauskünften aus dem Melderegister (vgl. 11.4) ist ein besonderer Aspekt zu berücksichtigen: Eine großzügige Handhabung führt dazu, daß nur schwer kontrollierbare Datensammlungen größeren Umfangs in private Hände gelangen. Deshalb müssen auch bei an sich unterstützungswerten Aktionen datenschutzrechtliche Belange Berücksichtigung finden.

Eine Gemeinde hatte die Koordination bei einer Sammlung für die notleidende Bevölkerung in der damaligen Sowjetunion übernommen. Die Sammlung selbst wurde von den örtlichen Vereinen durchgeführt. Den Helferinnen und Helfern wurde zur Abgrenzung der Sammelbezirke aus dem Melderegister eine Einwohnerliste zusammengestellt, auf der Namen, Wohnort, Straße und Hausnummer verzeichnet waren. Auch in diesem Fall hätte die vorzunehmende Abwägung der beteiligten Interessen zugunsten des Rechts auf informationelle Selbstbestimmung der betroffenen Einwohner ausfallen müssen. Die Festlegung der Sammlungsbezirke hätte auch ohne die Übermittlung von personenbezogenen Daten aus dem Melderegister erfolgen können. Karitative Verbände verwenden bei ihren Haussammlungen keine Einwohnerlisten. Es bestand kein überwiegendes öffentliches Interesse, das die Weitergabe personenbezogener Daten hätte rechtfertigen können.

11.6 Adreßbücher: Datenschutz im Kleingedruckten

Während des Berichtszeitraumes sind mehrere Bürgerinnen und Bürger an mich herangetreten, die sich darüber wunderten, daß ihre Daten in einem Adreßbuch nachzulesen waren. Einige befürchteten, daß es potentielle Einbrecher durch die Veröffentlichung leichter haben. Ich mußte in meiner Antwort darauf hinweisen, daß die Meldebehörden nach § 34 Abs. 3 NMG Adreßbuchverlagen Auskunft über Vor- und Familiennamen, Doktorgrad und Anschriften von den Einwohnern, die das 18. Lebensjahr vollendet haben, erteilen dürfen. Die Betroffenen haben jedoch das Recht, der Weitergabe ihrer Daten zu widersprechen. Sie sind auf dieses Recht bei der Anmeldung und mindestens einmal jährlich durch öffentliche Bekanntmachung hinzuweisen (vgl. 11.3).

Den an mich gerichteten Eingaben und Erfahrungen der Landesbeauftragten für den Datenschutz in anderen Bundesländern entnehme ich, daß der Hinweis auf das Widerspruchsrecht in der Praxis leerläuft. Die Veröffentlichung erfolgt überwiegend in den regionalen Tageszeitungen unter der Rubrik Bekanntmachungen. Die Betroffenen können dort, im allgemeinen kleingedruckt zwischen Werbeanzeigen placiert, erfahren, daß ihre Gemeinde die Weitergabe ihrer Daten zur Erstellung eines Adreßbuches plant oder (allgemein) der Datenübermittlung an Adreßbuchverlage widersprochen werden kann. In aller Regel wird ein solcher Hinweis bei der täglichen Zeitungslektüre überlesen. Die Information der Meldebehörde erreicht die Bürgerinnen und Bürger nicht. Die bestehenden Vorschriften reichen nach meinen Erfahrungen nicht aus, die Betroffenen davor zu schützen, daß ihre Daten gegen ihren Willen an Adreßbuchverlage weitergegeben werden. Ich fordere daher, im Niedersächsischen Meldegesetz festzulegen, daß Datenübermittlungen an Adreßbuchverlage nur mit — vorheriger — Einwilligung der Betroffenen erfolgen dürfen.

11.7 Übermittlung von Melderegisterdaten an den NDR bzw. die GEZ

Wenn eine Rundfunkteilnehmerin bzw. ein Rundfunkteilnehmer nach einem Umzug die neue Anschrift nicht mitgeteilt hat und mit der Zahlung der Rundfunkgebühr in Verzug geraten ist, beantragt die Gebühreneinzugszentrale der öffentlich-rechtlichen Rundfunkanstalten (GEZ) in Köln bei der Meldebehörde Auskunft über die neue Anschrift der betreffenden Person. Bisher werden die Auskunftsersuchen formulargestützt gestellt. Die Sachbearbeitung in der Meldebehörde erfolgt bei jeder einzelnen Anfrage individuell. Dabei können — der gesetzlichen Verpflichtung nach § 4 NMG entsprechend — ggf. besondere Umstände des Einzelfalles berücksichtigt werden. Nunmehr ist beabsichtigt, das Verfahren zu automatisieren: Die aktuelle Anschrift eines Gebührenschuldners, der mit den bereits im GEZ-Datenbestand gespeicherten Adreßdaten nicht mehr erreichbar ist, soll durch Abfrage und Übermittlung im Datenträgeraustauschverfahren ermittelt werden. In diesem Fall erfolgt die Übermittlung aus dem Melderegister an der Sachbearbeiterin bzw. dem Sachbearbeiter vorbei ausschließlich systemintern. Die Vorteile liegen auf der Hand. Sowohl bei der Meldebehörde als auch bei der GEZ reduzieren sich Verwaltungsaufwand, Bearbeitungsdauer und Kosten.

Die beantragte Auskunft ist der GEZ in aller Regel zu erteilen. Nur wenn der Meldebehörde besondere Umstände bekannt sind, aus denen sich Anhaltspunkte für eine mögliche Beeinträchtigung schutzwürdiger Belange der Betroffenen ergeben, muß sie eine besondere Prüfung und Abwägung vornehmen, bei denen es im Einzelfall zur Versagung der Auskunft kommen kann. Liegen schutzwürdige Interessen von Betroffenen vor, wird im Melderegister eine Auskunftssperre eingetragen. In diesen Fällen soll verhindert werden, daß ein Bekanntwerden von Melderegisterdaten zu erheblichen Nachteilen für die betroffenen Personen führt, beispielsweise zu einer Gefährdung von Leben, Gesundheit oder persönlicher Freiheit. Auskunftssperren beziehen sich allerdings ausschließlich auf die Datenweitergabe an Private. Für Datenübermittlungen im öffentlichen Bereich — und dazu zählt die Datenübermittlung an den NDR bzw. die GEZ — stellen Auskunftssperren unmittelbar kein Hindernis dar; sie werden bei einem automatisierten Abgleich übergangen. Im manuellen Verfahren hingegen wird die Sachbearbeiterin bzw. der Sachbearbeiter bei der Meldebehörde durch den Sperrvermerk auf vorliegende schutzwürdige Interessen aufmerksam gemacht. Da im Zusammenhang mit der Auskunftssperre keine weiteren Informationen im Melderegister gespeichert werden dürfen, finden schutzwürdige Belange bei einem automatisierten Melderegisterabgleich auf Veranlassung einer öffentlichen Stelle keine Beachtung. Aus dem Kreis der Meldebehörden sind mir Fälle genannt worden, in denen es auch im Fall der Datenübermittlung an Behörden oder sonstige öffentliche Stellen zum Schutz der betroffenen Person unabdingbar ist, vor der Erteilung der Melderegisterauskunft eine Einzelfallabwägung vorzunehmen.

Die Automatisierung von Verwaltungsverfahren soll hier nicht grundsätzlich kritisiert oder gar abgelehnt werden. Die mit dem Technikeinsatz verbundenen Vorteile dürfen allerdings nicht durch eine Vernachlässigung von Persönlichkeitsrechten erkauft werden. Es muß sichergestellt sein, daß das Recht auf informationelle Selbstbestimmung in automatisierten Verfahren in gleicher Weise Berücksichtigung finden kann wie bei manueller Arbeitsweise. Ich habe deshalb gefordert, daß bei dem automatisierten Melderegisterabgleich und der Übermittlung im Datenträgeraustauschverfahren an GEZ/NDR eine Einzelfallprüfung möglich bleiben muß. Ich begrüße, daß das Innenministerium diesen Ansatz aufgegriffen und im Erlaß vom 16. Oktober 1992 die Fälle, in denen Auskunftssperren im Melderegister vermerkt sind, von dem automatisierten Abgleich ausgenommen hat.

11.8 Nichterteilung von Melderegisterauskünften

Eine Stadt hatte einen Antrag auf Auskunftserteilung der zur Person gespeicherten Daten zunächst versehentlich nicht bearbeitet und dann die Angaben — aus nicht im Zusammenhang mit dem Auskunftsantrag stehenden Gründen — gelöscht. In § 27 NMG ist das melderechtliche „Grundrecht" verankert, Zugang zu den eigenen Daten zu erhalten. Ich habe diesen krassen Fall der Versagung eines elementaren Rechts beanstandet. Meine Rüge ändert leider nichts daran, daß der Anspruch der Betroffenen auf Auskunft über ihre Daten im Löschungsfall nicht mehr erfüllt werden kann. Damit kann auch nicht mehr aufgeklärt werden, ob die gespeicherten und eventuell im Einzelfall an Dritte übermittelten Daten richtig waren. Die Stadt wird dafür Sorge tragen, daß zukünftig eine Auskunftserteilung vor der Löschung erfolgt.

Schwierig ist es, dem Recht auf informationelle Selbstbestimmung der Betroffenen dann gerecht zu werden, wenn es gegenüber auskunftssuchenden Dritten um die Darstellung der Begründung geht, warum sie keine Auskunft über Betroffene erhalten. Dritte können ein legitimes Interesse haben, bestimmte Grunddaten der Betroffenen wie die Anschrift von der Meldebehörde zu erfragen. Auf der anderen Seite kann es auch gute Gründe bei Betroffenen geben, eine Melderegisterauskunft an Dritte zu verhindern. Die Betroffenen können in solchen Fällen eine Auskunftssperre eintragen lassen. Damit sich dadurch aber nicht etwa eine Schuldnerin bzw. ein Schuldner der gerechten Verfolgung entziehen kann, muß die Meldebehörde im Einzelfall abwägen, ob sie nun eine Auskunft an die Dritten erteilt oder nicht. Die Begründung der Ablehnung gegenüber den auskunftssuchenden Dritten muß dann angesichts des Rechts der Betroffenen, möglichst nichts über sie auszusagen, neutral gehalten werden. Eine Stadt hatte in einem solchen Fall formuliert: „... (gebe ich) wegen eines hier anhängigen Verfahrens derzeit keine Auskunft." Ich halte diese Formulierung für zu weitgehend. Die Stadt teilt meine Auffassung. Sie wird bei entsprechenden Anfragen zukünftig gemäß der Vorgabe in Nr. 35.7 der Verwaltungsvorschriften zum NMG die Auskunft erteilen: „... (ist) aufgrund melderechtlicher Vorschriften nicht zulässig."

Ob ein rechtliches Interesse glaubhaft gemacht ist, ist im wesentlichen „Tatfrage". Dabei kommt es entscheidend darauf an, daß die Möglichkeit einer Erbfolge plausibel gemacht wird und sich die Person, auf die sich das Auskunftsersuchen bezieht, in den zu ermittelnden Stammbaum einfügt. Es ist nicht auszuschließen, daß professionelle Erbenermittler gegenüber den Standesbeamten massiv auftreten, um in den Besitz der gewünschten Urkunden zu gelangen. Um zu verhindern, daß Personenstandsdaten „auf Vorrat" gesammelt werden, sollten an die Glaubhaftmachung des rechtlichen Interesses strenge Anforderungen gestellt werden.

12. Polizei

12.1 Datenverarbeitung bei der Polizei

Schaut man in die Tätigkeitsberichte der Datenschutzbeauftragten des Bundes und der Länder, so nehmen die Ausführungen zum Polizeibereich einigen Raum ein. Hieraus den Schluß zu ziehen, es bestünden entsprechend umfangreiche Zweifel an der datenschutzgerechten Handlungsweise der Polizei, ist — jedenfalls bezogen auf Niedersachsen — falsch. Nach meinen Erfahrungen besteht ein polizeiliches Eigeninteresse und Bewußtsein, personenbezogene

Daten nur befugt zu verarbeiten. Das besondere Interesse eines Datenschutzbeauftragten an der Polizei ist also nicht auf einem pauschalen Mißtrauen begründet. Es gibt aber objektive Umstände, die in hohem Maße geeignet sind, das Recht auf informationelle Selbstbestimmung bei der polizeilichen Datenverarbeitung zu tangieren. Die Polizei ist im Rahmen der Aufgabenbereiche Gefahrenabwehr und Strafverfolgung mehr als andere Behörden auf die Verwendung großer Mengen sensibler, vielfach noch nicht gesicherter Daten angewiesen. Ihre Verarbeitung wird zudem durch immer perfektioniertere technische Verfahren unterstützt, die alle verfügbaren Informationen ggf. bundesweit verwertbar machen (vgl. zur INPOL-Neukonzeption Nr. 12.3). Ich sehe ein gemeinsames Anliegen von Polizei und Datenschutzbeauftragtem darin, für einen rechtsstaatlichen Umgang mit personenbezogenen Daten zu sorgen. Als Landesbeauftragter für den Datenschutz habe ich in besonderer Weise darauf zu achten, daß das grundgesetzlich verankerte Recht des einzelnen, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen, bei der Abwägung mit berechtigten Belangen polizeilicher Arbeit nicht zu kurz kommt. Dies heißt konkret etwa den Schutz Unbeteiligter vor staatlichen Maßnahmen, Vernichtung nicht mehr erforderlicher Informationen und Durchschaubarkeit der Datenströme.

Eine seriöse Abwägung kommt mit Schlagworten wie „Datenschutz kontra Tatenschutz" oder „Sicherheit vor Datenschutz" nicht aus. Für wenig hilfreich halte ich Emotionen schürende Verhaltensweisen. Der höchste deutsche Kriminalbeamte, der Präsident des Bundeskriminalamtes, beklagt, „daß die polizeiliche Erkenntnisgewinnung durch den Datenschutz und die Fortentwicklung des Rechts zurückgeschnitten worden ist" (Süddeutsche Zeitung vom 19. Juli 1991). Die mit solchen Aussagen erzielte Wertung, der Datenschutz behindere erforderliche polizeiliche Aufklärungsarbeit, liegt schlicht neben der Sache. Ein einfacher Blick etwa in die polizeiliche Kriminalstatistik Niedersachsens (vgl. auch 12.19) belegt, daß sich die Aufklärungsquote vor und nach Inkrafttreten des Niedersächsischen Datenschutzgesetzes (1978) wie auch vor und nach dem Volkszählungsurteil des Bundesverfassungsgerichts (1983) praktisch nicht verändert hat. Also weniger Sicherheit durch mehr Datenschutz? In den letzten 10 bis 15 Jahren hat ein ungebremster Ausbau polizeilicher Informationssysteme stattgefunden (vgl. z.B. VIII 12). Mir ist kein wichtiges Vorhaben polizeilicher Datenverarbeitung in Niedersachsen bekannt, das aus Datenschutzgründen nicht realisiert wurde. Bei dem mit hohem Kostenaufwand erfolgten Ausbau der Datenverarbeitung ist der Kreis der zu speichernden Personen beständig erweitert worden. Nach alledem müßte vielmehr die Frage nach der Effektivität der Informationssysteme gestellt werden. Mehr Sicherheit durch mehr polizeiliche Informationsverarbeitung?

12.2 Bundeskriminalamt

Das geltende Gesetz über das Bundeskriminalamt (BKAG) aus dem Jahr 1973 entspricht in keiner Weise den vom Bundesverfassungsgericht aufgestellten Anforderungen zur Normenklarheit und Verhältnismäßigkeit. Die aus datenschutzrechtlicher Sicht unzulänglichen Regelungen im Referentenentwurf für eine neues BKA-Gesetz (einschließlich der Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten) aus dem Jahr 1990 habe ich schon in X 12.2 dargestellt. Ein aktueller Gesetzentwurf liegt nach wie vor nicht vor.

12.3 INPOL-Neukonzeption

Eine datenschutzrechtliche Beurteilung der polizeilichen Datenverarbeitung in Niedersachsen kann nur dann mit der gebotenen Sorgfalt vorgenommen werden, wenn zugleich die bundesweite gesamtpolizeiliche Verarbeitung in die Betrachtung einbezogen wird. Die Länderpolizeien arbeiten auf der Grundlage des BKAG mit dem Bundeskriminalamt zusammen. Als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen verarbeitet das Bundeskriminalamt zur Verbrechensbekämpfung Daten, die es in der Regel nicht selbst erhoben hat. Die Daten sind dem Bundeskriminalamt von den Polizeibehörden der Länder übermittelt worden. Eine wesentliche Ausprägung der Zentralstellenfunktion des Bundeskriminalamtes ist das im Verbund betriebene INPOL-System. Es strukturiert als gemeinsames, arbeitsteiliges Informationssystem der Polizeien des Bundes und der Länder die polizeiliche Datenverarbeitung unter der Bezeichnung „INPOL-Bund". Praktisch liegt insoweit eine Einheit der Datenverarbeitung vor — eine Einheit, die über das Schengener Informationssystem (SIS, vgl. X 12.3), bezogen auf Fahndungen über die Bundesgrenzen hinaus, noch vergrößert wird. Daneben gibt es unter der Bezeichnung „INPOL-Land" z. B. für den Kriminalaktennachweis vergleichbare Systeme der Länderpolizeien.

INPOL-Bund umfaßt zur Zeit im wesentlichen die personenbezogenen Anwendungen:

— Personen- und Sachfahndung,
— Kriminalaktennachweis (KAN),
— Haftdatei,
— Erkennungsdienst und Daktyloskopie (Erfassung von Fingerabdrücken und Fingerspuren),
— Arbeitsdateien für besondere Kriminalitätsbereiche, PIOS-Dateien, wie z. B. Innere Sicherheit — APIS,
— Falldateien für bestimmte Kriminalitätsbereiche, wie z.B. Rauschgift (FDR),
— Spurendokumentationen in Ermittlungsverfahren (SPUDOK-Dateien).

Die Weitergabe niedersächsischer Daten in INPOL-Bund sowie die Speicherung und Nutzung der Daten in den INPOL-Anwendungen greifen in das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger ein. Eine Suche nach erlaubenden gesetzlichen Grundlagen führt zu der erstaunlichen Erkenntnis, daß die Materie weder im Gesetzentwurf über ein Niedersächsisches Gefahrenabwehrgesetz noch im BKA-Gesetz inhaltlich geregelt ist. Der Umgang mit den Daten wird durch verwaltungsinterne Bestimmungen (INPOL-Konzeption/Grundsätze) gesteuert. Die Entscheidungen trifft die nichtöffentlich tagende Konferenz der Innenminister des Bundes und der Länder, die gleichsam als „Ersatzgesetzgeber" agiert.

Nunmehr ist eine INPOL-Neukonzeption in Planung. Danach ist vorgesehen, das INPOL-Kommunikationsnetz schrittweise mit den anderen Sondernetzen der Polizeien zusammenzuführen. Im Ergebnis soll eine freizügige Kommunikation aller Teilnehmer ermöglicht werden. Ich habe gegenüber dem Niedersächsischen Innenministerium betont, daß es nicht hinnehmbar wäre, gegebenenfalls vorhandene niedersächsische Zweckbindungsregelungen unter dem Vorzeichen eines offenen Informationsaustauschs bundesweit unterlaufen zu können. In meiner Stellungnahme zum Gesetzentwurf über ein Niedersächsischen Gefahrenabwehrgesetz (vgl. 12.4) habe ich die Verantwortlichkeit des Landes Niedersachsen für die von ihm erlangten Daten hervorgehoben. Nur das Land trägt die Verantwortung für die Zulässigkeit, Richtigkeit, Dauer und weitere Verarbeitung der von ihm an das Bundeskriminalamt übermittelten Daten. Ich hielte es für außerordentlich bedauerlich, wenn das Innenministe-

rium weiterhin an der angedeuteten Ansicht festhielte, die — organisatorische — Zentralstellenkompetenz des Bundeskriminalamtes ermögliche auch eine eigenständige materielle Datenverarbeitung durch das Bundeskriminalamt.

12.4 Niedersächsisches Gefahrenabwehrgesetz

Kurz vor Redaktionsschluß hat die Landesregierung den Gesetzentwurf zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG) in den Landtag eingebracht (LT-Drs 12/4140).

Mit dem jetzt so bezeichneten „Niedersächsischen Gefahrenabwehrgesetz" (NGefAG) soll die niedersächsische Polizei Grundlagen erhalten, die nahezu jede Bürgerin und jeden Bürger zum Gegenstand polizeilichen Handelns machen können.

Ursache hierfür ist eine rechtspolitisch bedeutsame und folgenreiche Weichenstellung in der Frage, was alles zur Gefahrenabwehr gehört. Ein Überblick mag zunächst verdeutlichen, wie die zukünftigen Aufgabenfelder polizeilicher Arbeit aussehen. Die Polizei hat nach dem NGefAG

- Vorbereitungen zu treffen, um künftige Gefahren abzuwehren (wird gesetzlich neu eingeführt),
- konkrete Gefahren abzuwehren,
- Straftaten zu verhüten (wird gesetzlich neu eingeführt),
- für die Verfolgung von Straftaten vorzusorgen (wird gesetzlich neu eingeführt),

und nach der Strafprozeßordnung (StPO)

- Strafttaten zu verfolgen.

Das Gemeinsame an den bisherigen zwei Aufgaben, konkrete Gefahren abzuwehren (präventive Gefahrenabwehr nach Polizeirecht) und Straftaten zu verfolgen (repressive Gefahrenabwehr nach Strafprozeßrecht), waren handfeste Aufgabenbeschreibungen und Eingriffsvoraussetzungen. Diese traditionelle Struktur mit ihren auch datenschutzrechtlich praktikablen Grenzlinien (konkrete Gefahr/Anfangsverdacht nach § 152 Abs. 2 StPO) wird aufgegeben. Die oben gekennzeichneten zusätzlichen drei neuen Aufgaben führen zu einer doppelten Vorverlagerung. Gemeinsam ist den neuen Aufgaben nämlich, daß die polizeiliche Tätigkeit nun im „Vorfeld" von Gefahren und Straftaten erfolgen kann. Eine Datenverarbeitung im Vorfeld gerät aber in die die gefährliche Nähe der im Volkszählungsurteil des Bundesverfassungsgerichts als unzulässig erachteten Datenvorratshaltung. Fließende Aufgabenübergänge erschweren zudem Kontrollmöglichkeiten. Polizeiliches Handeln kann nicht mehr präzise bestimmten Aufgaben zugeordnet werden. Der Gesetzentwurf vermeidet — ebenfalls in Abkehr von der bisherigen Übung — eine gesetzliche Beschreibung der neuen Aufgaben. Es liegt der Schluß nahe, daß jedes Handeln letztlich auf eine Aufgabe zurückgeführt werden können soll. Datenschutzrechtlich haben die neuen Vorfeldaufgaben keine — tendenziell vom Bundesverfassungsgericht geforderte — Begrenzung der Verwendung von personenbezogenen Daten zur Folge, sondern eine umfassende Weiterung.

Diese neue Struktur des NGefAG ist verantwortlich für einen umfänglichen Ausbau der polizeilichen Eingriffsnormen (Befugnisse). Die Polizei erhält — und das ist schon fast zwingend für Tätigkeiten im Vorfeld — bisher ge-

setzlich nur den Verfassungsschutzbehörden vorbehaltene heimliche Ermittlungsmethoden. Es handelt sich um den geheimen Einsatz von z. B. Videokameras bei nicht dem Versammlungsgesetz unterliegenden Veranstaltungen bzw. Ansammlungen und z. B. in U-Bahnhöfen, Parkhäusern, Ministerien, Gerichtsgebäuden, Banken, Museen, usw. Hinzu kommen die besonderen (geheimen) Mittel und Methoden, wie die längerfristige Beobachtung, die Verwendung von optischen und akustischen technischen Mitteln (Video/Wanzen) z. B. in Wohnungen, der Einsatz von Vertrauenspersonen (freie Mitarbeiterinnen und Mitarbeiter, auch V-Leute genannt) und die Kontrollmitteilungen (beobachtende Fahndung).

Diese vom Gesetzentwurf als „verdeckt" bezeichneten Maßnahmen sind sehr problematisch. In einem demokratischen Rechtsstaat sollten staatliche Eingriffe grundsätzlich offen und für die Bürgerinnen und Bürger erkennbar vorgenommen werden. Nur wenn der Staat ihnen „mit offenem Visier" gegenübertritt, sind sie doch in der Lage, ihr Recht auf informationelle Selbstbestimmung auch wahrnehmen zu können und sich gegebenenfalls zu wehren. Es kommt noch eines hinzu: Ein Vorfeld hat naturgemäß (fast) keine Begrenzungen. Oben habe ich dargelegt, daß angesichts der fehlenden Aufgabenbeschreibungen im Gesetz die Zielrichtung einer Maßnahme weitgehend offenbleiben muß. Wie steht es nun mit der Schwelle, ab der gehandelt werden darf? Auch hier wirkt sich die fehlende Begrenzung eines Vorfeldes aus. Ausgangspunkt der möglichen Eingriffe sind nach dem Entwurf „Tatsachen, die die Annahme rechtfertigen". Das kann eine einfache Beobachtung sein. In manchen Fällen der Datenerhebung und Speicherung von Angaben versucht nun der Gesetzentwurf, den Anwendungsbereich der Eingriffe wieder einzugrenzen, indem er sie von einer „Straftat von erheblicher Bedeutung" abhängig macht. Die Straftaten werden zwar in einem Katalog dargestellt. Nur ist die Aufzählung derart umfassend, daß von einer wahrhaft eingrenzenden Wirkung schwerlich die Rede sein kann. Nicht vorgesehen sind die Rasterfahndung und der Einsatz von verdeckten Ermittlern (unter falscher Identität handelnde Polizeibedienstete). Diese Instrumente gibt es aber im Bereich der Strafverfolgung (vgl. 31.1).

Im Ergebnis führen die neuen Vorfeldaufgaben weg von der bisherigen Eingriffsschwelle „konkrete Gefahr". Bewirkt wird nichts anderes als eine Vorverlagerung der bei der Strafverfolgung geltenden Voraussetzung des Anfangsverdachts, soweit es um die Vorsorge für die Verfolgung von Straftaten und Verhütung von Straftaten geht.

Für die niedersächsischen Bürgerinnen und Bürger haben die neuen Aufgaben mit den vorgesehenen Befugnissen einschneidende Folgen. Wurden bisher grundsätzlich nur die für die konkrete Gefahr Verantwortlichen (Störer) oder Tatverdächtige polizeilich erfaßt, so können nunmehr zulässigerweise auch Daten verarbeitet werden über Zeugen, Hinweisgeber, Auskunftspersonen, Kontakt- und Begleitpersonen, potentielle Straftäter und Opfer von Straftaten, Menschen in der Nähe von schützenswerten Personen (wie z. B. das Personal eines Hotels, in dem ein Staatsgast wohnt, oder Nachbarn eines als gefährdet einzustufenden Politikers), Ärztinnen und Ärzte, Dolmetscherinnen und Dolmetscher, Sachverständige, Abschleppunternehmer, Betreiber/Inhaber/Sicherheitsingenieure von bestimmten Anlagen, Veranstaltungsleiter bzw. Veranlasser von Veranstaltungen. Die Aufzählung ließe sich fortsetzen. Und dies alles ggf. ohne Einwilligung oder Wissen der Betroffenen. Hierin liegt eine ungeheuere Ausweitung der betroffenen Personenkreise, die mich zu der diesen Punkt einleitenden Bemerkung veranlaßt hat. Jede und jeder, die bzw. der mit der Polizei in Kontakt kommt, ob als Zeuge oder Auskunftsperson, kann per Computer mit den polizeilichen Systemen überprüft werden. Im Hinblick auf den unter 12.1 angesprochenen Ausbau der Informationssysteme drängt sich der Eindruck auf, hier werde nur rechtlich nachvollzogen, was

weitsichtige Polizeifachleute schon längst ins Werk gesetzt haben. Fazit: Die Datenverarbeitung geht so weit, daß die Polizei — so Prof. Denninger — gewissermaßen vor dem Täter am Tatort sein kann.

Ich hatte seit Jahren mit Nachdruck eine Novellierung des Nds. SOG auf der Grundlage des Volkszählungsurteils des Bundesverfassungsgerichts gefordert. Gegen den früheren Referentenentwurf habe ich schwerwiegende datenschutzrechtliche Bedenken geltend gemacht. Sie gründeten auf den hier dargelegten Positionen sowie einer Reihe von nicht nachvollziehbaren Abweichungen von der derzeitigen polizeilichen Praxis und den datenschutzrechtlichen Standards des in der Beratung befindlichen Entwurfs eines Gesetzes zur Sicherung der informationellen Selbstbestimmung (NDSG). Es steht außer Frage, daß auch die am 15. Juni 1992 durchgeführte Anhörung von Experten aus Wissenschaft und Praxis zu einigen datenschutzrechtlichen Verbesserungen im nun vorliegenden Gesetzentwurf geführt hat. Dennoch fällt generell die Vorgehensweise des Gesetzentwurfs auf, bei der Speicherung und Übermittlung von personenbezogenen Daten das für das Recht auf informationelle Selbstbestimmung wichtige Spannungsverhältnis zwischen Grundregel und Ausnahme zugunsten unübersichtlicher Ausnahmen und damit zu Lasten des Selbstbestimmungsrechts zu lösen. Statt dessen wäre es ohne weiteres möglich, auch mit „einfachen" Regelungen das Selbstbestimmungsrecht des einzelnen ohne Vernachlässigung der berechtigten Belange der Polizei zu berücksichtigen. Dies belegt das seit einiger Zeit geltende Polizeirecht des Landes Schleswig-Holstein. Ich werde in den parlamentarischen Beratungen insbesondere auf dieses Mißverhältnis hinweisen, um so auch den Schutz unbeteiligter Personen gleichgewichtig auszugestalten.

12.5 Videoüberwachung — Bilder sprechen Bände

Das Recht am eigenen Bild gehört ohne Zweifel zum klassischen Bereich des allgemeinen Persönlichkeitsrechts, und die Aufnahme des Bildnisses eines Menschen ist datenschutzrechtlich eine Datenerhebung. Beim privaten Fotografieren denkt niemand an den Datenschutz — warum auch. So Fotografierte wollen ein Bild. Sie werden ins rechte Licht gerückt, und sie erhalten nach der Aufnahme das Positiv wie das Negativ. Wenn das Bild gut ist, behält man es jahrelang.

Bei den von der Polizei angefertigten Bildern ist (fast) alles anders. Die Betroffenen wissen in der Regel nicht, daß sie fotografiert werden, was mit den Aufnahmen weiter passiert und wo sie wie lange aufbewahrt werden. Der Einsatz technischer Mittel zur Bild- und Tonaufzeichnung gewinnt im Rahmen der polizeilichen Arbeit zunehmend an Bedeutung. Es gibt Kameras, die Verkehrsknotenpunkte beobachten und dann „durchlaufende" Bilder (Übersichtsaufnahmen) an Verkehrsleitstellen übertragen. Aus datenschutzrechtlicher Sicht besonders bedeutsam sind Videokameras/Camcorder. Sie werden zu bestimmten Anlässen zur Beobachtung oder — in Verbindung mit Geschwindigkeitsmeßgeräten — gegen Verkehrssünder eingesetzt. Im Bereich der Gefahrenabwehr erfolgt die Verwendung von Videokameras für folgende Zwecke: Vorgangsdokumentation, Objektschutz, Dokumentation von Ereignissen zur Lageinformation, Beobachtung von (Groß-)Veranstaltungen und Erstellung von Beweismitteln. Videokameras haben gegenüber dem Auge einer Polizeibeamtin oder eines Polizeibeamten immense Vorteile. Die von der niedersächsischen Polizei eingesetzten Video-Systeme besitzen eine simultane Aufzeichnungsmöglichkeit, Zusatzinformationen können eingeblendet und Ausschnitte vergrößert werden. Entscheidend ist aber die Zuverlässigkeit der Aufzeichnungen. Sie „vergessen" keine Informationen und sind daher als qualitativ hochwertige Bild- (und Ton-)Beweise wichtig für Gerichtsverfahren.

Die wesentlichen Wirkungen des Einsatzes von Videokameras lassen sich wie folgt zusammenfassen: Aus Sicht der Polizei soll schon mit dem Zeigen der Kameras präventiv das Verhalten der Menschen so beeinflußt werden, daß eben keine Gefahrensituationen eintreten. Aus Sicht der Betroffenen haben klar sichtbare Videokameras eine „abschreckende" Wirkung (vgl. auch die Antwort der Landesregierung auf eine Kleine Anfrage, LT-Drs 10/4117). Hieraus kann nur der Schluß gezogen werden, daß der offene Einsatz von Kameras geeignet ist, Gefahren abzuwehren. Dies gilt insbesondere dann, wenn auf den Einsatz hingewiesen wurde. Das Hinweisschild „Radarkontrolle" hat ja ebenso seine Wirkungen. Eine heimliche Videobeobachtung kann demnach das Verhalten von Menschen nicht beeinflussen. Sie ist nicht geeignet, Gefahren abzuwehren (zur Vermeidung von Mißverständnissen: Es geht nicht um die Geeignetheit als Beweismittel im Bereich der Strafverfolgung). Die datenschutzrechtliche Konsequenz kann dann nur lauten, auf den erkennbaren Hinweis auf den Einsatz von Videokameras und der offenen Handhabung zu bestehen. Aber auch bei der offenen Videobeobachtung müssen die Einsatzbereiche aus Gründen des Persönlichkeitsrechts möglichst eng gehalten werden, da das unbefangene Verhalten der Menschen merklich beeinflußt wird (zur Videobeobachtung anläßlich Demonstrationen vgl. X 12.4). Heimliche Videoaufnahmen und -aufzeichnungen werden von der SPD-Fraktion im Deutschen Bundestag als unzulässig angesehen (vgl. deren Gesetzentwurf eines Bundesinformationsgesetzes — BISG, BT-Drs. 11/3730).

Aus Sicht des Datenschutzes ist bei einem fachlich gebotenen Einsatz von Videokameras wichtig, die Voraussetzungen für die Aufnahme (Datenerhebung), Aufzeichnungen (Speicherung), Vernichtung der Aufzeichnungen (Löschung) und weitere andere Verwendungsmöglichkeiten der Aufzeichnungen (Zweckdurchbrechungen) mit dem Recht auf informationelle Selbstbestimmung in Einklang zu bringen.

Aus polizeilicher Sicht liegen bei durchlaufenden Bildern und sonstigen Übersichtsaufnahmen keine Datenerhebungen vor. Der einzelne figuriere ja bei Übersichtsaufnahmen im Bildkontext der Gesamtaufnahme nur als anonymes Bildelement, und durchlaufende Bilder seien nicht auf Identifizierung gerichtet. Bei der datenschutzrechtlichen Betrachtungsweise kommt es aber auf die Bestimmbarkeit des Menschen an. Ausschlaggebend für das Vorliegen einer Datenerhebung ist dann, ob das eingesetzte Video-System technisch eine Identifizierung ermöglicht (vgl. OVG Bremen, Urteil v. 24. April 1990, NVwZ 90, 1189 und X 12.4). Nur dieser Ansatz berücksichtigt auch die Situation Betroffener, die nicht wissen, welche Technik in der Videokamera steckt. Leider läßt das geplante Niedersächsische Gefahrenabwehrgesetz diesen für die Zulässigkeit einer Maßnahme entscheidenden Aspekt offen.

Ein Beispiel: Eine Demonstration hatte drei Stunden gedauert. Gefertigt wurden Videoaufzeichnungen mit einer Gesamtlänge von 3 1/2 Stunden und 163 Fotos (vgl. Antwort der Landesregierung auf eine Kleine Anfrage, LT-Drs 11/4118). Der Zweck des polizeilichen Handelns gebietet, Videoaufzeichnungen ohne Auswertung unverzüglich zu vernichten, wenn die erwartete Gefahr nicht eingetreten ist — so noch ein einschlägiger Erlaß des Innenministeriums aus dem Jahr 1985. In den mir bekannten Fällen hält sich die Polizei an diese Vorgabe. Ist eine Gefahr eingetreten oder besteht sogar der Verdacht auf eine Straftat, so liegt es nahe, Angaben über ggf. miterfaßte Unverdächtigte zu löschen und das Beweismittel der zuständigen Verwaltungsbehörde bzw. Staatsanwaltschaft zu übergeben. Im Gegensatz hierzu schafft das geplante Niedersächsische Gefahrenabwehrgesetz durch die neuen Aufgaben „Vorsorge für die Veränderung von Straftaten und Verhütung von Straftaten" weitere polizeiinterne Aufbewahrungs- und Verwendungsmöglichkeiten, die zeitlich nicht begrenzt sind. Ich habe große Zweifel, ob etwa Vorgänge des Zeitgeschehens auf Vorrat aufgezeichnet und aufbewahrt werden dürfen (vgl. BVerfG, Beschluß v. 1. Oktober 1987, NJW 1988, 329, 330 f.)

Ich habe die hier dargelegten Positionen im Rahmen meiner Stellungnahme zum Entwurf eines Niedersächsischen Gefahrenabwehrgesetzes gegenüber dem Innenministerium geltend gemacht. Sollte das geplante Gesetz insoweit unverändert in Kraft treten, so haben sich niedersächsische Bürgerinnen und Bürger darauf einzustellen, daß die Polizei unsichtbar mit von der Partie sein kann. Sie soll die Möglichkeit erhalten, mit versteckter Kamera Videoaufnahmen und -aufzeichnungen z. B. bei Sportwettkämpfen, kulturellen Veranstaltungen, Volksfesten und bei den in Nr. 12.4 genannten Verkehrseinrichtungen zu machen.

12.6 DAMASKUS oder: Die Reise nach Jerusalem

Hinter DAMASKUS verbirgt sich ein automatisiertes Verfahren, das eine Massenauswertung von personenbezogenen Daten zu Zwecken der Strafverfolgung ermöglicht. Ziel ist dabei, durch Abgleich verschiedener Dateien mit umfangreichen Datenmengen möglichst wenige Datensätze als Anhaltspunkte für polizeiliche Ermittlungen zu gewinnen. Vergleichbar dem Gesellschaftsspiel „Reise nach Jerusalem" kreist das Suchprogramm durch alle vorhandenen Datensätze und siebt die für Ermittlungsansätze interessanten heraus. Typisches Beispiel: Durch Zeugenaussagen erhält die Polizei fragmentarische Hinweise auf das mögliche Täterfahrzeug. Durch Abgleich dieser Hinweise mit dem Bestand der Fahrzeugdaten des Kraftfahrtbundesamtes werden alle Halter von Kraftfahrzeugen festgestellt, die nach der Zeugenaussage als Tatfahrzeug in Betracht kommen. Ein Abgleich dieser Halterdaten mit dem Datenbestand im polizeilichen Informationssystem zeigt zusätzlich, welche Halter bereits „polizeilich in Erscheinung getreten" sind. Der Anwendungsbereich von DAMASKUS beschränkt sich nicht nur auf Kraftfahrzeugdaten. Fälle aus der Praxis zeigen, daß z. B. sämtliche Personaldaten einer Firma oder die Daten aller an einem Bundeswehrstandort stationierten Soldaten mit polizeilichen Dateien verglichen wurden.

Man kann natürlich sagen, daß die Polizei alle Möglichkeiten nutzen muß, um einem Täter auf die Spur zu kommen. Nur: Zu bedenken ist, daß bei diesen Verfahren unvermeidlich in das Recht auf informationelle Selbstbestimmung zahlreicher unverdächtiger Bürgerinnen und Bürger eingegriffen wird, und zwar ohne Kenntnis der Betroffenen. Unser Rechtstaat gebietet es dagegen, Nichtverdächtige möglichst weitgehend von polizeilichen Ermittlungen auszunehmen. Ich habe in der Vergangenheit (vgl. IX 12.7 und X 12.7) für das DAMASKUS-Verfahren eine bereichsspezifische gesetzliche Grundlage bzw. für die Übergangszeit verbindliche Richtlinien gefordert. Das Innenministerium hat bislang für Regelungen keinen Bedarf gesehen, weil die Polizei DAMASKUS nur in wenigen Fällen anwende. Inzwischen hat sich jedoch herausgestellt, daß dem Fachressort und auch mir nicht alle DAMASKUS-Anwendungen, sondern nur die von den Standardfällen abweichenden gemeldet wurden. Der Bundesgesetzgeber hat in der Zwischenzeit mit dem Erlaß des Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG, vgl. 31.1) die Strafprozeßordung um § 98 c ergänzt und damit eine Rechtsgrundlage für den maschinellen Datenabgleich geschaffen. Nach dieser Vorschrift dürfen personenbezogene Daten aus einem Strafverfahren zur Aufklärung einer Straftat mit anderen Strafverfolgungs-, Strafvollstreckungs- und Gefahrenabwehrdaten abgeglichen werden. In der Praxis wird hier wohl nur noch der Grundsatz der Verhältnismäßigkeit Einhalt gebieten können.

Ich werde prüfen, ob die mir gemeldeten Fallgestaltungen zukünftig zumindest teilweise in den Anwendungsbereich des ebenfalls neuen § 98 a StPO, der Regelung über die Rasterfahndung, fallen. Wenn der Datenabgleich auch

mit anderen als Strafverfolgungs-, Strafvollstreckungs- oder Gefahrenabwehrdateien erfolgt, kann die Maßnahme auf § 98 c StPO nicht mehr gestützt werden. Rasterfahndungen dürfen nur zur Verfolgung bestimmter, abschließend aufgezählter Straftaten von erheblicher Bedeutung durchgeführt werden. Der Abgleich muß durch den Richter, bei Gefahrenverzug durch die Staatsanwaltschaft angeordnet werden.

Bei den DAMASKUS-Anwendungen bleibt insbesondere ungeklärt, welche Speicherungsmöglichkeiten auch hinsichtlich der Daten von Unverdächtigen, welche Zweckbindungen bzw. Löschungspflichten bestehen. Ich halte deshalb verbindliche Richtlinien nach wie vor für erforderlich.

12.7 Nichts ist unmöglich ... MIKADO

Gibt es noch Bürgerinnen und Bürger, die bisher keinen Kontakt zur Polizei hatten? Etwa als Anzeigeerstatter, Zeuge, Finder, Hinweisgeber, Verantwortlicher, Beteiligter, Fahrzeughalter oder auch Verdächtiger? Diese Frage zu verneinen bedeutet gleichzeitig festzustellen, daß Daten über alle Bürgerinnen und Bürger bei der Polizei gespeichert sind oder zumindest waren. Denn jeder Vorgang, den die Polizei bearbeitet, führt zur Speicherung von personenbezogenen Daten. Während die Daten früher in Sachbearbeiterakten und polizeilichen Tagebüchern schlummerten, kann man auf sie im Zeitalter automatisierter Vorgangsverwaltungssysteme in Sekundenschnelle zugreifen. Jeder Kontakt mit der Polizei hinterläßt in diesen Informationssystemen eine elektronische Spur. Angesichts der möglichen Vernetzung mit anderen Systemen können die Betroffenen „nicht mehr wissen, wer was wann und bei welcher Gelegenheit über sie weiß", um das Bundesverfassungsgericht zu zitieren.

Das Landeskriminalamt beschäftigt sich mit der Entwicklung eines landeseinheitlichen dezentralen Informations- und Kommunikationssystems (MIKADO), das die Erstellung, Bearbeitung und Verwaltung aller Vorgänge bei der Polizei sowie deren Auswertung und statistische Aufbereitung auf jeder Polizeidienststelle zum Ziel hat. MIKADO wird in der aktuellen Entwicklungsstufe bereits heute bei einigen Polizeidienststellen eingesetzt. Es eröffnet die Möglichkeit, Personen in insgesamt 26 verschiedenen Rollen zu speichern. Allein die Datenfelder zu den Personenangaben lassen die Erfassung von insgesamt 149 Einzelangaben zu. Hierzu gehören beispielsweise Informationen wie arbeitslos, internationaler Straftäter, Konsument harter Drogen, Opfereignung für das Täter-Opfer-Ausgleichsverfahren, ausgeübter Beruf, Mundart, Stimme, Sprachmerkmale, äußere Erscheinung, Motive von Tätowierungen, Art und Lage von körpertlichen Merkmalen usw.. Außerdem können zu Personen freitextliche Hinweise erfaßt werden. Die beispielhafte Aufzählung verdeutlicht, daß es bei MIKADO nicht um ein reines Vorgangsverwaltungssystem im Sinne eines Aktenfindungs-, Textverarbeitungs- und Dokumentationssystems geht. MIKADO stellt Daten über Personen für die polizeiliche Arbeit bereit. Für die Beurteilung der damit verbundenen datenschutzrechtlichen Risiken wird es insbesondere darauf ankommen, wie die zu beachtende Zweckbindung technisch sichergestellt werden kann, ob Schnittstellen zu anderen Systemen geschaffen werden und welche Löschungsfristen man vorsieht.

Meine bisherigen Anregungen zur Verbesserung der technischen und organisatorischen Datenschutz- und Datensicherungs-Maßnahmen (vgl. X 4.6 Nr. f) wurden inzwischen weitgehend aufgegriffen. Die Systemverwaltung wurde örtlichen Systembetreuern übertragen; deren Aufgaben und Befugnisse wurden festgelegt. Alle für die normale Systemverwaltung notwendigen Kommandos bzw. Funktionen wurden in einem sogen. „Administrator-Menue" vorstrukturiert, so daß umfassende Super-User-Funktionen nur in Ausnahme-

fällen und nur auf ausdrückliche Weisung vorgenommen werden dürfen. Grundsätzlich sind keine Shell-Berechtigungen erteilt worden. Die Paßwort-Datei wird vom örtlichen Systembetreuer aufgebaut und verwaltet. Die Benutzerin oder der Benutzer wählt jedoch ihr bzw. sein Paßwort selbst. Ein Paßwortwechsel wird nicht vom System erzwungen, sondern muß vom Systembetreuer überwacht werden. Das Datum des letzten Login oder des letzten erfolglosen Login wird der Benutzerin bzw. dem Benutzer leider nicht angezeigt.

Das Speichern und Verändern von Daten wird im einzelnen Datensatz mit UNIX-ID und Datum der Speicherung (unveränderbar) bzw. Datum der Änderung festgehalten. Speicher- bzw. Änderungsinhalt werden zur Gewährleistung der Datenbank-Konsistenz in einer besonderen „audit-Datei" gespeichert und zusätzlich gesichert. Abfragen von „Nicht-Sachbearbeitern" werden in einer Protokolldatei festgehalten, die periodisch ausgedruckt und kontrolliert wird.

Die MIKADO-Datenbank wird kontinuierlich reorganisiert. Dabei werden Daten, deren Speicherung länger als 15 Monate zurückliegt und deren Vorgangsbearbeitung abgeschlossen wurde, automatisch gelöscht. Danach verbleibt ein reduzierter Auskunftsbestand in einer besonderen Auskunftsdatenbank. Bei manueller Löschung werden Kerndaten des ursprünglichen Datensatzes sowie das Löschdatum und die Uhrzeit in einer besonderen Textdatei protokolliert.

Ich werde meine datenschutzrechtlichen Vorstellungen insbesondere zur Zweckbindung von Vorgangsverwaltungsdaten in das weitere Verfahren einbringen.

12.8 Dauer von Speicherungen in elvis

Bei den Kriminalpolizeiinspektionen Hildesheim und Osnabrück wurde 1985 das „Elektronische Vorgangsverwaltungs- und Informationssystem (elvis)" als Pilotprojekt — zunächst auf drei Jahre angelegt — eingeführt. Mit dem Verfahren wurden beispielsweise die Tagebuchführung, die polizeiliche Kriminalstatistik, der kriminalpolizeiliche Meldedienst und die Auswertung automatisiert. Die Errichtungsanordnung für elvis sieht vor der Beendigung des Probelaufs keine Löschung von Daten vor. Nachdem das System nunmehr seit acht Jahren eingesetzt wird, stellt sich die Frage, ob die (fehlende) Löschungsregelung in der Errichtungsanordnung noch mit den KpS-Richtlinien zu vereinbaren ist. Dort sind Löschungen nach kürzerer Frist, bei Kindern z. B. nach zwei Jahren, vorgesehen. Ich habe das Innenministerium um Überprüfung gebeten. Die Errichtungsanordnung für elvis muß schon bereits deshalb überarbeitet werden, weil die dort enthaltene Aufzählung hinsichtlich der Speicherungsmöglichkeiten über personengebundene Hinweise (vgl. 12.10) nicht mehr den aktuellen Kriterien entspricht.

12.9 Dialogprotokolldatei und ihre Fremdnutzung

Unter X 12.6 habe ich die Neuregelung der Protokollierungen bei Abfragen aus den polizeilichen Informationssystemen POLAS und INPOL sowie die Verwertung der Dialogprotokolldatei zu kriminalistischen Zwecken angesprochen.

Durch die automatisierte Aufzeichnung von Protokolldaten wird die Datenverarbeitung nachprüfbar. Zugleich wird einer mißbräuchlichen Verwendung vorgebeugt, weil kein Anwender darauf vertrauen kann, daß Verstöße unent-

deckt bleiben. Die Kontrolle eines Datenabrufes ist aber nur möglich, wenn Abfrageveranlasser und Abfragegrund bekannt sind. Ich habe deshalb zusätzlich zu den bisher gespeicherten Angaben die Protokollierung dieser Daten gefordert. Über den Umfang der Zusatzprotokollierungen konnte ich mit dem Innenministerium noch kein Einvernehmen erzielen. Während das Innenministerium die Speicherung von Abfrageveranlasser und -grund nur bei 1 ‰ der Abfragen für realisierbar und ausreichend hält, fordere ich zumindest eine Zusatzprotokollierung entsprechend dem ZEVIS-Verfahren (vgl. IX 30.2). Sie liegt zur Zeit bei 2 % der Abfragen. Die seit längerem angemahnte Neufassung der Errichtungsanordnung für die Protokolldatei liegt mir noch nicht vor.

Die Informationen aus der Dialogprotokolldatei werden nicht nur zu Datenschutzkontrollzwecken, sondern auch als zusätzliche Ermittlungshilfe genutzt. Es kann anhand der Protokolldaten beispielsweise festgestellt werden, über welche Personen in einem bestimmten Zeitraum von einem bestimmten Datensichtgerät Abfragen an INPOL/POLAS getätigt worden sind. Bei diesem Zugriff der Polizei auf die Dialogprotokolldatei geht es dann um die Verarbeitung von personenbezogenen Daten, die für die Polizei eigentlich gar nicht da sind. Entweder handelt es sich um Angaben, die die Polizei in ihren speziell für ihre Aufgabenerfüllung eingerichteten Dateien nicht (mehr) vorhalten darf, weil die Speicherungsfristen abgelaufen sind. Oder es handelt sich um Daten von sog. Negativabfragen, bei denen aus polizeilicher Sicht keinerlei Anlaß zur Registrierung der abgefragten Personen bestand. Ich habe in der Vergangenheit die Nutzung der Protokolldatei für polizeiliche Zwecke für eine Übergangszeit unter der Bedingung mitgetragen, daß der Zugriff auf wenige sonst nicht aufklärbare, schwere Vorfälle beschränkt bleibt. Die Praxis der Fremdnutzungen macht deutlich, daß meine datenschutzrechtlichen Vorbehalte berechtigt waren: 1991 wurden 41 Fremdnutzungen der Dialogprotokolldatei durchgeführt. In den ersten drei Quartalen des Jahres 1992 wurden bereits 20 Selektionen zu kriminalistischen Zwecken vorgenommen. Die Zahl der Fremdnutzungen durch die niedersächsische Polizei zeigt, daß trotz der restriktiven Verfahrensregelungen im Erlaß vom 3. Juli 1991 (Genehmigungsvorbehalt durch den Leiter des Landeskriminalamtes, Dokumentationspflichten) in erheblichem Umfang in das Recht der Betroffenen auf Datenlöschung eingegriffen wird, wenn sie für die Aufgabenerfüllung nicht (mehr) benötigt werden.

Das Innenministerium beabsichtigt, die Fremdnutzungsmöglichkeiten der Dialogprotokolldatei im zukünftigen Gefahrenabwehrgesetz (vgl. 12.4) im Vergleich zu der Erlaßregelung vom 3. Juli 1991 noch zu erleichtern. Der Gesetzentwurf sieht die Verwendung der Protokolldaten u.a. zur Aufklärung einer Straftat aus dem Katalog des § 100 a Strafprozeßordnung vor, ohne die im Erlaß enthaltenen weiteren Zugriffsvoraussetzungen zu nennen. Mit dem Gesetzentwurf wird von der Leitlinie des in der Beratung stehenden Niedersächsischen Datenschutzgesetzes abgewichen. Danach dürfen Protokolldateien nur zu Datenschutzkontroll- und Datensicherungszwecken genutzt werden.

12.10 Speicherung von personengebundenen Hinweisen

Die Speicherung personengebundener Hinweise (bewaffnet, gewalttätig, Ausbrecher, Ansteckungsgefahr, geisteskrank, BTM-Konsument, Freitodgefahr, Prostitution) ist datenschutzrechtlich in mehrfacher Hinsicht bedenklich. Es besteht keine Rechtsgrundlage, aus der eine Bürgerin oder ein Bürger entnehmen kann, wer, wann, mit welchen Inhalten und zu welchem Zweck Hinweise zu ihrer Person im polizeilichen Informationssystem speichern darf. Wegen

der besonderen Sensitivität der Hinweise bedarf es eingehender Überprüfungen, ob und unter welchen Voraussetzungen polizeiliche Zwecke die Speicherung personengebundener Hinweise (vgl. VII 12.3) rechtfertigen. Zudem besteht die Gefahr, daß die in den Hinweisen enthaltenen bruchstückhaften Informationen zur Grundlage von Entscheidungen gemacht werden.

12.10.1 Von „Prostitution" bis „geisteskrank"

Für die Vergabe personengebundener Hinweise hat der Arbeitskreis II der Arbeitsgemeinschaft der Innenministerien der Bundesländer am 6./7. September 1988 Kriterien festgelegt. Dabei wurden u. a. die personengebundenen Hinweise „Prostitution" und „geisteskrank" zugelassen. Ich habe Zweifel, ob der personengebundene Hinweis „Prostitution" unter Berücksichtigung des Grundsatzes der Verhältnismäßigkeit für die polizeiliche Aufgabenerfüllung erforderlich ist. Prostitution ist nicht strafbar. Die Ausübung der Prostitution ist weder ausreichend für die Annahme einer konkreten Gefahr noch ein Anhaltspunkt für die künftige Begehung einer Straftat durch die Betroffenen. Der personengebundene Hinweis „geisteskrank" darf nach den Kriterien vergeben werden, wenn ärztlich festgestellt ist, daß die betroffene Person an einer Geisteskrankheit leidet. Auch hier stellt sich für mich die Frage, warum die Polizei diese Angabe benötigt. Ich habe meine datenschutzrechtlichen Bedenken gegenüber dem Niedersächsischen Innenministerium vorgetragen. Eine Antwort steht noch aus.

12.10.2 Der unvergeßliche Rausch

Mit den Kriterien für die Vergabe personengebundener Hinweise wurden auch ihre jeweiligen Laufzeiten im polizeilichen Informationssystem festgelegt. Danach darf der personengebundene Hinweis „BTM-Konsument" für die Dauer der Aufbewahrung der Kriminalakte über die Betroffenen im System vorgehalten werden. Ein Petent, der vor 10 1/2 Jahren wegen eines Verstoßes gegen das Betäubungsmittelgesetz verurteilt worden ist, mußte bei der Einsichtnahme in die Polizeiakte über einen Verkehrsunfall, an dem er beteiligt war, mit Erstaunen feststellen, daß er dort als „BTM-Konsument" bezeichnet wurde. Die Verkehrspolizei war bei dem Abgleich der personenbezogenen Daten des Petenten mit dem polizeilichen Informationssystem anläßlich des Unfalls auf den entsprechenden Hinweis gestoßen und hatte ihn in ihre Verkehrsunfallakte übernommen. Das polizeiliche Vorgehen wurde u. a. auf diese Information abgestellt. In der Kriminalakte des Betroffenen waren seit seiner Verurteilung keine weiteren Erkenntnisse angefallen. Dieser Fall zeigt, daß eine derartig lange Speicherungsdauer von personengebundenen Hinweisen nicht nur einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung bewirkt, sondern auch der Polizei einen nicht immer aktuellen Sachverhalt vermittelt. Ich halte es nicht für gerechtfertigt, Betroffene nach einem derartig langen Zeitraum weiterhin als „BTM-Konsumenten" zu bezeichnen, ohne daß weitere Erkenntnisse bekanntgeworden sind.

Unabhängig von dieser Grundsatzfrage konnte ich dem Einsender die Löschung des Hinweises (einschließlich der Vernichtung der Kriminalakte) mitteilen. Die Polizei hatte nämlich die Aufbewahrungsfrist für das Vorhalten der Kriminalakte nicht den Vorschriften entsprechend berechnet.

12.11 Speicherungen über Suizidversuche bei der Polizei?

Anders als in Hamburg, Hessen und Schleswig-Holstein speichert die niedersächsische Polizei Daten über Personen, die versucht haben, sich das Leben zu nehmen. Erfährt die Polizei von einem Suizidversuch, wird über die Person eine Kriminalakte angelegt. Im polizeilichen Informationssystem POLAS/INPOL wird sie für mindestens zwei Jahre mit dem personengebundenen Hinweis „Freitodgefahr" ausgewiesen. Das Innenministerium sieht die Speicherung als erforderlich an, damit die Polizei bei Kontakten mit Suizidgefährdeten die richtigen Maßnahmen ergreifen und in Todesermittlungsverfahren die Frage eines Fremdverschuldens richtig beurteilen kann. Die Einwilligung der betroffenen Person wird nicht eingeholt. Eine verfassungsgemäße Befugnisnorm kann die Polizei für die Suizidspeicherungen nicht vorweisen. Allenfalls könnte es im Interesse der Funktionsfähigkeit der Sicherheitsbehörden hingenommen werden, wenn für eine Übergangszeit bis zum Erlaß gesetzlicher Bestimmungen auf der Grundlage einer bestehenden Verwaltungsvorschrift verfahren wird. Eine solche Verwaltungsvorschrift liegt mit den Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen vor. Ziffer 2.2.10 der Richtlinien läßt die Speicherung von Daten über gefährdete Personen zu. Eingriffe in das Recht auf informationelle Selbstbestimmung sind unter Berufung auf den Übergangsbonus allerdings nur zulässig, wenn sie zur Aufgabenerfüllung unerläßlich sind.

Der Selbstmordversuch in einer Polizeidatei neben Einbruchdiebstahl, Erpressung und Betrug gespeichert? Das wirft z.B. die Frage nach der polizeilichen Zuständigkeit auf. Ob ein Recht zur Selbsttötung besteht, ist umstritten. Bei schwerwiegenden Selbstgefährdungssituationen, wie z.B. Selbsttötungsversuchen, sollen ausnahmsweise polizeiliche Maßnahmen zum Schutz von Individualgütern des Handelnden gerechtfertigt sein. Es wird jedoch vorausgesetzt, daß die betreffende Person im Begriff steht, eine Selbsttötung vorzunehmen. Polizeirechtlich ist demnach der Zweck des Tätigwerdens begrenzt auf die Unterbindung der Selbsttötung (Gefahrenbeseitigung). Ausnahmen sind eng auszulegen. Nach Beseitigung der Gefahr liegt ein bedrohtes Schutzgut nicht mehr vor. Auch die Gründe für das ursprünglich gerechtfertigte Tätigwerden bestehen bei der späteren Suizidspeicherung nicht mehr. Aus datenschutzrechtlicher Sicht ist eine fachgesetzlich nicht mehr vorgesehene weitere Verwendung personenbezogener Daten nicht erforderlich.

Die Polizei hat die Aufgabe, Gefahren abzuwehren. Ein Suizidversuch begründet für sich allein keine konkrete Gefahrensituation. Erst wenn im Zeitpunkt der Speicherung mit hinreichender Wahrscheinlichkeit im Einzelfall mit einem erneuten Suizidversuch gerechnet werden muß, wäre eine konkrete Gefahrensituation denkbar. Der Literatur habe ich entnommen, daß nach einem Suizidversuch in der Regel keine Wiederholungsgefahr besteht, daß viele Suizidenten über ihre Rettung Dankbarkeit empfinden und deshalb gute Aussichten bestehen, sie endgültig für das Leben zurückzugewinnen. Die Suizidspeicherung kann deshalb überhaupt nur in Betracht kommen, wenn über den Versuch hinaus weitere tatsächliche Anhaltspunkte den Schluß zulassen, ein weiterer Suizidversuch werde folgen. Ich frage mich, wie die Polizei im Hinblick auf die spärlichen Informationen, die sie bei Suizidvorfällen erhält, eine derartige gesicherte Prognose vornehmen kann.

Die Polizei erhält nur Kenntnis über solche Suizidversuche, die ihr angezeigt werden. Über Suizidgefährdete, die ausschließlich von den Gesundheitsbehörden betreut werden, erhält die Polizei keine Informationen. Ihre Datensammlung über Suizidversuche ist daher unvollständig und zufällig. Die Polizei kann keineswegs sicher sein, daß bei Personen, die nicht mit dem personengebunden Hinweis „Freitodgefahr" gespeichert sind, tatsächlich auch kei-

ne Suizidgefahr besteht. Die Speicherung von Suizidvorfällen ist deshalb allgemein nicht geeignet, die Gefahr abzuwehren.

Was aber bedeutet es für den Gefährdeten, wenn er Kenntnis von seiner Speicherung erhält? In seiner besonderen psychischen Situation kann die Angst vor der Bloßstellung zu einer (weiteren) Herabsetzung des Selbstwertgefühls führen. Nicht ohne Grund hat es die Konferenz der Leiter psychiatrischer Krankenhäuser abgelehnt, daß Daten über Selbstmordgefährdete im Polizeicomputer gespeichert werden.

Um zu erfahren, welche Bedeutung der Suizidspeicherung in der polizeilichen Praxis zukommt, habe ich bei einer Kriminalpolizeiinspektion sämtliche Suizidakten und daran anknüpfende Speicherungen in POLAS/INPOL geprüft. Das Ergebnis war eindeutig. Eine Prognose zur Wiederholungsgefahr hatte die Polizei in aller Regel nicht vorgenommen. Auch wenn die Polizei selbst die Wiederholungsgefahr bezweifelt, wird gespeichert.

Ein Beispiel: Eine Frau informierte die Polizei über einen Suizidversuch ihrer Nachbarin (vermutlich Tabletteneinnahme). In einem Vermerk notiert das Polizeirevier daraufhin, die Wiederholungsgefahr könne nicht beurteilt werden. Trotzdem wurde eine Kriminalakte angelegt und der personengebundene Hinweis „Freitodgefahr" in POLAS gespeichert.

Schon Hinweise darauf, daß jemand möglicherweise einen Suizidversuch unternehmen wird, führen zu Speicherungen.

Zwei Beispiele: Ein Landeskrankenhaus meldete eine wegen Alkoholproblemen eingewiesene Patientin als vermißt. Die Frau soll mehrfach Suizidabsichten geäußert haben, akute Selbstmordgefahr bestehe aber nicht. Auch hier erfolgte die Suizidspeicherung. Als eine Frau ihren Sohn als vermißt meldete, gab sie an, sie habe Angst, ihr Sohn könne sich etwas antun. Der Sohn selbst erklärte nach seiner Rückkehr der Polizei, er habe zu keiner Zeit Selbstmordgedanken gehabt. Er wollte für sich allein sein, um mit sich ins reine zu kommen. Konkrete Hinweise auf eine Suizidgefahr enthält die Kriminalakte jedoch nicht.

Nach Aussagen von Fachleuten sind Ankündigungen von Selbsttötungen oft das Ergebnis menschlicher und sozialer Isolierung, z. B. bei alten Menschen, die vereinsamt in Depressionen verfallen und beschließen, „Schluß zu machen". Die Suizidankündigung soll die Mitmenschen auf die Not aufmerksam machen und zur Hilfeleistung bewegen. Auch wenn keine ernsthafte Suizidabsicht besteht, wird die Person bei der Polizei zum Suizidgefährdeten.

Ein Beispiel: Der Betroffene hinterließ in einer Spielhalle einen Zettel mit einer Suizidandrohung. Obwohl die Polizei in einem Vermerk selbst ausführte, ihr sei der Mann als Suizidandroher hinreichend bekannt, seine Handlungen seien jedoch als nicht ernsthaft einzuschätzen, wurden die Unterlagen zur Kriminalakte genommen und der personengebundene Hinweis „Freitodgefahr" vergeben.

Ich konnte bei meiner Prüfung nicht feststellen, daß die Polizei aufgrund eines einzigen Freitodhinweises einen Suizidversuch verhindern konnte bzw. der Hinweis bei der polizeilichen Arbeit relevant gewesen wäre. Polizeiliche Maßnahmen wurden stets durch Information der oder des Betroffenen selbst oder von Dritten ausgelöst.

Bei zwei Dritteln der Fälle hat die Polizei sich an ihre eigenen Vorgaben zur Laufzeit des Hinweises in POLAS/INPOL nicht gehalten. Der personengebundene Hinweis stand länger als die festgelegten zwei Jahre im System zur

Verfügung, in einem Fall sogar über 12 Jahre, ohne daß weitere Anhaltspunkte für eine Wiederholungsgefahr bekannt wurden. Die Aufnahme von Suizidvorfällen in die Kriminalakte führt darüber hinaus zu einer Verlängerung von bestehenden Deliktsspeicherungen, wenn die Aussonderungsprüffrist für die Delikte vor der für Suizidversuche abläuft. Das Innenministerium hält diese Praxis unter Berufung auf eine statistische Auswertung, die zum Ergebnis hatte, daß in ca. 50 % der Suizidfälle auch deliktisches Verhalten bekannt geworden ist, für gerechtfertigt. Diese Auffassung teile ich nicht. Die Herstellung einer Kausalität zwischen Suizidversuch und kriminellem Verhalten führt dazu, daß Suizidversuche kriminalisiert werden. Aus der Tatsache eines Suizidversuchs ergeben sich keine Anhaltspunkte dafür, daß die betreffende Person straffällig werden wird.

Das Ergebnis meiner Prüfung führte zu einer Beanstandung von zahlreichen Einzelfällen. Unter Hinweis auf die zuvor dargelegten Gründe habe ich zusätzlich empfohlen, die in Niedersachsen vorhandenen Suizidspeicherungen zu löschen und zukünftig von Speicherungen dieser Art abzusehen. Das Innenministerium hat lange überlegt, wie es auf mein Beanstandungsschreiben reagieren soll. Zunächst ergänzte es vorübergehend den Entwurf zum Niedersächsischen Gefahrenabwehrgesetz um eine Ermächtigungsgrundlage bezüglich Suizidspeicherungen, damit das praktizierte Verfahren zukünftig im Gesetz abgesichert ist. In der nun vorliegenden Fassung des Gesetzentwurfs ist eine entsprechende Vorschrift nicht mehr vorgesehen. Eine schriftliche Stellungnahme des Innenministeriums zu meiner Beanstandung lag bis Redaktionsschluß nicht vor.

12.12 Datenspeicherung bei unerlaubten Schwangerschaftsabbrüchen

Nach § 218 StGB macht sich strafbar, wer eine Schwangerschaft unerlaubt abbricht. In diesem Zusammenhang stellte sich die Frage, wie die Polizei mit den Daten von Frauen umgeht, die dieser Straftat verdächtig sind oder eine solche begangen haben. Meine Nachfrage im Niedersächsischen Innenministerium ergab, daß die niedersächsische Polizei zwei Frauen im Kriminalaktennachweis (KAN) wegen unerlaubter Abtreibung erfaßt hatte. Hierzu muß man wissen, daß der Kriminalaktennachweis bundesweit abrufbare Hinweise über Kriminalakten enthält, die über beschuldigte oder tatverdächtige Personen angelegt sind, denen Fälle schwerer oder überregional bedeutsamer Straftaten zur Last gelegt werden. Aufgrund meiner Anfrage wurden die Daten in einem Fall sofort gelöscht, da die genannten Voraussetzungen für die Aufnahme in den Kriminalaktennachweis nicht vorlagen. Im zweiten Fall erfolgte die Einstellung in dem Kriminalaktennachweis, weil andere Delikte diese Zuordnung rechtfertigten. Hier wurde der Hinweis „Abtreiberin" gelöscht. Weiterhin waren zwei Frauen wegen unerlaubter Abtreibung im Kriminalaktenindex (KAI) gespeichert, der alle in Niedersachsen angelegten Kriminalakten erfaßt. Auf KAI kann landesweit zugegriffen werden. Das Niedersächsische Innenministerium hat auch diese Daten gelöscht und die Polizeidienststellen durch Erlaß vom 15. April 1991 angewiesen, keine weiteren Speicherungen aus diesem Anlaß in Kriminalpolizeilichen Sammlungen vorzunehmen. Diese Regelung wird von mir ausdrücklich begrüßt. Die Speicherung von personenbezogenen Daten im Zusammenhang mit Straftaten nach § 218 StGB ist für die polizeiliche Aufgabenerfüllung nicht erforderlich. Frauen entschließen sich zum unerlaubten Schwangerschaftsabbruch aus einer einmaligen, ihnen unausweichlich erscheinenden Konfliktsituation. Von einer Wiederholungsgefahr kann somit nicht ausgegangen werden. Bei Einmaltäterinnen verbietet sich eine Datenspeicherung bei der Polizei von vornherein wegen Verstoßes gegen den Grundsatz der Verhältnismäßigkeit.

12.13 Informationsaustausch bei sportlichen Großveranstaltungen

Bund und Länder haben sich zur Verbesserung des Informationsaustausches bei sportlichen Großveranstaltungen auf ein neues Verfahren verständigt. Mit ihm sollen rechtzeitige Informationen über alle für den Polizeieinsatz bedeutsamen Erkenntnisse und eine umfassende Auswertung einsatzrelevanter Fakten erreicht werden. Zu diesem Zweck wurden für alle Bundesländer beim Landeskriminalamt Nordrhein-Westfalen eine Zentrale Informationsstelle (ZIS) und in jedem Bundesland eine Landesinformationsstelle (LIS) eingerichtet. Für jeden Verein der Fußballbundesliga wurde eine zuständige Polizeibehörde bestimmt. Diese sammelt vor einem Auswärtsspiel ihres Vereins alle einsatzrelevanten Erkenntnisse und übermittelt sie an die für die Heimmannschaft zuständige Polizeidienststelle, an die ZIS und an die zuständigen LIS. Nach einem Spiel berichtet die Polizeibehörde, in deren Bereich das Spiel ausgetragen wurde, über den Einsatzverlauf und weitere Erkenntnisse an die Behörde der Auswärtsmannschaft, die ZIS und die zuständigen LIS. Der LIS obliegt es, vor und nach einem Spiel die betroffenen Stellen über alle Umstände zu berichten, die sie von Behörden erhalten hat, die nicht in das Verfahren integriert sind. Darüber hinaus steht sie als Ansprechstelle zur Verfügung und steuert Informationen auf Landesebene. In Niedersachsen wurde die LIS im Lagezentrum des Innenministeriums eingerichtet. Zusammenarbeit und Aufgabenstellung hat das Niedersächsische Innenministerium im Runderlaß vom 22. Oktober 1991 (Nds. MBl. 1992 S. 503) festgelegt.

Ich habe mich im Niedersächsischen Innenministerium über die Arbeitsweise der LIS informiert. Bei der Einsichtnahme in den im Rahmen des Informationsaustausches anfallenden Schriftverkehr habe ich festgestellt, daß die Informationsstelle der Ankündigung entsprechend bislang keine personenbezogenen Daten verarbeitet. Eine Ausnahme bildet der Informationsaustausch während der Fußballeuropameisterschaft in Schweden im Juni 1992. Auf Anfrage schwedischer Behörden wurden auf den eingerichteten Kommunikationswegen personenbezogene Daten übermittelt. Die LIS in Niedersachsen hat die Unterlagen mit personenbezogenen Daten auf meine Veranlassung hin vernichtet.

Es ist beabsichtigt, den Aufgabenbereich der LIS um die Verarbeitung personenbezogener Daten zu erweitern. Sie soll als Verbundteilnehmer der Datei „Gewalttäter Sport" (vgl. 12.14) unmittelbaren Zugriff auf personenbezogene Daten erhalten und selbst Speicherungen vornehmen können.

12.14 Datei „Gewalttäter Sport"

Es ist nicht zu verkennen, daß gewalttätige Ausschreitungen im Zusammenhang mit Sportveranstaltungen die Polizei vor schwierige Probleme stellen. Die Innenministerkonferenz hat im Mai 1991 beschlossen, eine Datei „Gewalttäter Sport" einzurichten, die der Polizei Erkenntnisse für organisatorische und taktische Überlegungen sowie Anhaltspunkte für Gefahrenabwehrmaßnahmen gegen Störer liefern soll. Die Datenschutzbeauftragten des Bundes und der Länder sind, abweichend von der Vorgabe der Innenministerkonferenz, an der Prüfung der Frage, ob die Datei eingerichtet werden soll, bedauerlicherweise nicht beteiligt worden. Datenschutzrechtliche Vorstellungen konnten in das Verfahren deshalb nur im Nachhinein eingebracht werden. Bisher wurde die Datei „Gewalttäter Sport" nicht realisiert.

Inzwischen liegen jedoch die „Richtlinien für den Meldedienst Gewalttäter Sport" im Entwurf vor. Diese setzen die Installierung der Datei „Gewalttäter Sport" voraus. Datenschutzrechtlich sind folgende Punkte problematisch:

— Die Datenschutzbeauftragten des Bundes und der Länder haben von Anfang an gefordert, für die Datei „Gewalttäter Sport" eine Bedarfsanalyse durchzuführen. Neben der Darstellung von typischen Einsatzsituationen wäre zu erläutern, inwieweit Dateiauskünfte vor Ort unter den Bedingungen eines Polizeieinsatzes in polizeiliche Maßnahmen gegen gewalttätige Störer umgesetzt werden können und weshalb die bestehenden Dateien bzw. Informationssysteme hierfür nicht ausreichen. Nach dem derzeitigen Informationsstand bestehen hinsichtlich der Geeignetheit und Erforderlichkeit der Datei offene Fragen. Auch polizeiintern ist der Nutzeffekt der Datei umstritten. Der Niedersächsische Innenminister hat in der Presseerklärung Nr. 128 vom 3. Mai 1991 geäußert, die Datei sei für den polizeilichen Einsatz wenig hilfreich, da sie kaum sinnvoll präventiv einzusetzen sei.

— Die Datei soll als sogenannte Verbunddatei beim Bundeskriminalamt geführt werden. Verbundteilnehmer werden sein: die Polizeibehörden, in deren Zuständigkeitsbereich ein Verein der Fußballbundesliga ansässig ist, Grenzschutz- und Bahnpolizeiämter, Landes- und Zentrale Informationsstellen (vgl. 12.13), die Grenzschutzdirektion und das Bundeskriminalamt. Zu Abfragen sollen außerdem alle Polizeibehörden und die Dienststellen des Bundesgrenzschutzes berechtigt sein. Die umfassende Zugriffsregelung ist aus datenschutzrechtlicher Sicht zu weitgehend. Zugriff auf die Datei dürfen anlaßbezogen nur die Polizeidienststellen haben, die mit der Gefahrenabwehr im Zusammenhang mit einer Sportveranstaltung befaßt sind.

  Die Speicherung in einer Verbunddatei kommt nur in Betracht, wenn die Betroffenen nicht nur regional, sondern als „reisende Gewalttäter" auftreten. Diese Einschränkung ist in dem Richtlinienentwurf nicht vorgesehen. Alle in einem Straftatenkatalog aufgeführten Sachverhalte und bestimmte Gefahrenabwehrmaßnahmen sollen zu einer Meldepflicht der zuständigen Behörde gegenüber der Verbunddatei führen.

— Beschreibende Merkmale über Betroffene dürfen nur anhand eines festgelegten Datensatzes vorgenommen werden. Der Richtlinienentwurf sieht den Eintrag der personengebundenen Hinweise „bewaffnet" und „gewalttätig" vor. Insoweit müssen sich die sachbearbeitenden Dienststellen an die Kriterien für die Vergabe personengebundener Hinweise halten. Bedenklich bleibt die Möglichkeit, in einem Freitextfeld ohne Vorgaben Sachverhaltsbeschreibungen vornehmen zu können.

— Im Richtlinienentwurf wird der Forderung der Datenschutzbeauftragten entsprechend die Speicherfrist auf zwei Jahre beschränkt. Es ist allerdings nicht ersichtlich, warum diese Frist nach dem Richtlinienentwurf erst mit der Erfassung in der Datei und nicht mit dem auslösenden Ereignis beginnen soll.

— Der Richtlinienentwurf enthält keine Aussagen über die Zusammenarbeit zwischen den zuständigen Polizeibehörden und den Veranstaltern von Sportereignissen. Dabei ist insbesondere festzulegen, ob und wenn ja unter welchen Voraussetzungen Datenübermittlungen an Veranstalter in Betracht kommen.

Ich werde meine Bewertung des Richtlinienentwurfs in das Verfahren einbringen.

12.15 Palästinenserdaten in der Staatsschutzdatei APIS

Die Arbeitsdatei PIOS Innere Sicherheit (APIS) ist eine beim Bundeskriminalamt, Abteilung für Staatsschutz, geführte Verbunddatei zur Bekämpfung politisch motivierter Straftaten. Sie ermöglicht, Zusammenhänge zwischen Personen, Institutionen, Objekten, Sachen und Ereignissen herzustellen. Daraus sollen Erkenntnisse für polizei- und ermittlungstaktisches Vorgehen gewonnen werden.

Die Staatsschutzdatei APIS kam auch während des Golfkrieges zum Einsatz. Vor dem Hintergrund der sich immer deutlicher abzeichnenden Gefahr von Anschlägen terroristischer Gruppierungen aus dem Nahen Osten gegen Einrichtungen der Allianzkräfte haben Bund und Länder beschlossen, durch das Bundesamt für Verfassungsschutz und den Bundesnachrichtendienst in Abstimmung mit dem Bundeskriminalamt eine „Gefährderliste" aufzustellen. Diese Liste wurde den Polizeidienststellen der Länder zur Überprüfung der aufgeführten Personen übersandt. In Niedersachsen waren hiervon 80 Personen betroffen. Das Niedersächsische Landeskriminalamt hat das Ergebnis der Überprüfungen sowie Erkenntnisse aus eigenen Ermittlungen an das Bundeskriminalamt übermittelt. 20 Personen aus Niedersachsen wurden in diesem Zusammenhang in APIS gespeichert.

Nach den Feststellungen des Bundesbeauftragten für den Datenschutz handelte es sich bei den Palästinenserdaten um typische Vorfeldinformationen. Sie zeichneten sich dadurch aus, daß sie Personen betrafen, bei denen Anhaltspunkte dafür sprachen, daß sie „verfassungsfeindliche Absichten" verfolgen. Es fehlten jedoch tatsächliche Anhaltspunkte, wonach die betroffenen Personen aus sonstigen konkreten Gründen in Verbindung mit terroristischen Gewalttätern oder deren Unterstützern standen. Jedenfalls bestanden nach Beendigung der Golfkrise keine hinreichenden tatsächlichen und konkreten auf den gespeicherten Personenkreis bezogene Anhaltspunkte mehr, die eine weitere Speicherung in APIS hätten rechtfertigen können. Das Bundeskriminalamt hat die Datensätze im April 1992 in der Datei APIS gelöscht und die erstellten Akten vernichtet. Nach der Darstellung des Landeskriminalamtes wurden bei der niedersächsischen Polizei in diesem Zusammenhang keine Dateien oder Kriminalakten angelegt.

12.16 Lichtbildvorzeigekartei „Sexualstraftäter"

Der folgende Fall zeigt, welchen erheblichen Eingriffen in das Recht auf informationelle Selbstbestimmung eine Bürgerin oder ein Bürger ausgesetzt sein kann, wenn erste Verdachtsmomente zu polizeilichen Aktivitäten führen:

Ein Taxifahrer hatte einen stark angetrunkenen weiblichen Fahrgast zur angegebenen Adresse gebracht. Dort angekommen, weckte er die im Taxi eingeschlafene Frau. Nach einer Auseinandersetzung über die Höhe des Fahrpreises weigerte sie sich, aus dem Taxi auszusteigen. Der Taxifahrer bat über Funk die Taxizentrale, polizeiliche Hilfe anzufordern. Der Polizei erklärte die Frau, sie sei von dem Taxifahrer sexuell belästigt worden. Der Mann habe sie unsittlich berührt. Einige Tage später erstattete sie Strafanzeige. Der Taxifahrer erhielt daraufhin unter Androhung der zwangsweisen Vorführung eine Vorladung zur erkennungsdienstlichen Behandlung gem. § 81 b StPO. Seinem Rechtsanwalt wurde auf Nachfrage von der Polizei erläutert, die Maßnahme würde nicht der Identitätsfeststellung dienen. Die Fotografien des Taxifahrers sollten zur Lichtbildervorzeigekartei „Sexualstraftäter" genommen werden. Auf den nachfolgenden Widerspruch hat die Polizei die Anordnung der er-

kennungsdienstlichen Behandlung aufgehoben. Noch vor Abgabe des Verfahrens an die Staatsanwaltschaft hat die Polizei die zuständige Straßenverkehrsbehörde über den Verdacht unterrichtet und um Überprüfung gebeten, ob der Taxifahrer charakterlich geeignet ist, Fahrgäste zu befördern.

Die Kriminalpolizei führt zur Aufklärung von Straftaten eine Lichtbildvorzeigekartei „Sexualstraftäter". Nach der Feststellungsanordnung werden in diese Datei Sexualstraftäter, die der Polizei bekannt geworden und erkennungsdienstlich behandelt worden sind, aufgenommen. Lichtbilder, Personalien und nähere Angaben zur Straftat werden gespeichert. Zeugen und Geschädigten wird Einsicht in die Vorzeigekartei gewährt. Ich habe meine Zweifel geäußert, ob für die Führung der Kartei überhaupt ausreichende Rechtsgrundlagen vorliegen. Im Einzelfall habe ich gerügt, daß der betroffene Taxifahrer in die Lichtbildvorzeigekartei „Sexualstraftäter" aufgenommen werden sollte, obwohl nach der Feststellungsanordnung für diese Kartei nur die Speicherung von rechtskräftig Verurteilten erlaubt war. Die Aufnahme einer Person in eine Lichtbildervorzeigekartei stellt einen schweren Eingriff in das Recht auf informationelle Selbstbestimmung dar, weil die Fotografien zur Einsichtnahme von Zeugen und Geschädigten und damit zur Datenübermittlung an Private vorgehalten werden. Eine Einordnung in die Vorzeigekartei kann daher nur in schwerwiegenden Fällen und bei Wiederholungsgefahr zulässig sein. Beide Voraussetzungen lagen im vorliegenden Fall nicht vor.

Die Datenübermittlung an die Straßenverkehrsbehörde ist ebenfalls unter Verletzung datenschutzrechtlicher Bestimmungen erfolgt. Eine rechtfertigende Rechtsgrundlage lag nicht vor. Bis zum Inkrafttreten einer normenklaren Rechtsgrundlage kann zwar eine bestehende Praxis hingenommen werden, soweit sie für die geordnete Weiterführung einer funktionsfähigen Verwaltung unerläßlich ist. Die noch vor Abgabe an die Staatsanwaltschaft erfolgte Datenübermittlung war hier bei Würdigung der Gesamtumstände allerdings verzichtbar. Dieser Bewertung hat sich die Polizei im nachhinein ebenfalls angeschlossen. Zukünftig werden entsprechende Datenübermittlungen nur vorgenommen, wenn die Staatsanwaltschaft eine entsprechende Entscheidung getroffen hat bzw. der Ausgang des Strafverfahrens sie angezeigt sein läßt.

12.17 Kriminalakten

Unter VIII 12.9 habe ich ausgeführt, daß die Anlegung einer Kriminalakte weitreichende Folgen für die betroffenen Bürgerinnen und Bürger haben kann, die — einmal registriert — als „polizeibekannte" Personen schnell in den Kreis der Verdächtigen einbezogen werden. Die in einer Kriminalakte gespeicherten Informationen können an andere Behörden übermittelt werden, beispielsweise wenn die gewerberechtliche Zuverlässigkeit einer Person überprüft werden soll. Angesichts der möglichen Auswirkungen für die Betroffenen sind an die Sorgfaltspflicht der aktenführenden Polizeidienststelle hohe Anforderungen zu stellen.

In den Richtlinien des Landeskriminalamtes über die Führung von Kriminalakten vom 15. Januar 1982 ist festgelegt, daß über lebende Personen jeweils nur eine Kriminalakte zu führen ist. Weitere in Niedersachsen vorhandene Kriminalakten sind bei der zuständigen Stelle zusammenzuführen. Die Zentralisierung von Kriminalakten aus verschiedenen Bundesländern ist dagegen nicht geregelt. Das führt dazu, daß zumindest in schwerwiegenden Fällen im Bundesgebiet mehrere Kriminalakten über eine Person geführt werden. Über den Kriminalaktennachweis (KAN) wird die Kommunikation zwischen den aktenführenden Polizeidienststellen gesteuert. Die jeweils vorhandenen Er-

kenntnisse werden im Rahmen des kriminalpolizeilichen Meldedienstes bzw. bei Erkenntnisabfragen bundesweit übermittelt. Nach meiner Auffassung dürften allerdings nicht nur Erkenntnisse aus dem Anfangsstadium eines strafrechtlichen (fremden) Ermittlungsverfahrens in die Kriminalakten aufgenommen werden. Auch Informationen über den Ausgang dieser Ermittlungsverfahren müßten gespeichert werden, damit die Unterlagen kein falsches Bild über die Betroffenen abgeben.

Eine Eingabe hat gezeigt, daß verkürzte Sachverhaltsspeicherungen bzw. -übermittlungen zu datenschutzrechtlich bedenklichen Situationen führen können. Das Landeskriminalamt führt eine Kriminalakte, in der hauptsächlich fremde Erkenntnisse aus anderen Bundesländern über den Betroffenen enthalten sind. Aus der Kriminalakte wurden die folgenden personenbezogenen Daten an zwei Polizeidienststellen in Baden-Württemberg per Fernschreiben übermittelt:

— Dem Übermittlungsschreiben war zu entnehmen, daß dem Betroffenen in einem Ermittlungsverfahren der Landespolizei Schleswig-Holstein mehrere Straftaten nachgewiesen worden seien. Die Empfänger der Daten wurden korrekterweise darauf hingewiesen, daß nähere Erkenntnisse bei der schleswig-holsteinischen Polizei eingeholt werden können.

  Nach Darstellung des Betroffenen stimmten diese Angaben nicht. Entsprechend meiner Auffassung, daß die aktenführende Dienststelle eine Aufklärungspflicht trifft, wenn die Richtigkeit der in einer Kriminalakte gespeicherten personenbezogenen Daten zumindest qualifiziert bestritten wird, hat das Niedersächsische Landeskriminalamt in Schleswig-Holstein nachgefragt. Ergebnis: Bei der schleswig-holsteinischen Polizei waren über diese Vorgänge gar keine Unterlagen mehr vorhanden. In Niedersachsen wurden mithin noch fremde (Teil-)Erkenntnisse zu einem Zeitpunkt verwendet und an Dritte weitergegeben, als sie schon längst von der (Ursprungs-)Polizeibehörde aufgrund deren kriminalistischen Bewertung für nicht mehr erforderlich befunden und vernichtet waren. Das Niedersächsische Landeskriminalamt hat die entsprechenden Unterlagen auch aus der hiesigen Kriminalakte entfernt.

— Der Betroffene war nach der Aktenlage zweier Diebstähle überführt worden. In der Kriminalakte befand sich hierzu ein Informationsschreiben des Bundeskriminalamtes über Straftaten mit ähnlicher Begehensweise. In dem Fernschreiben des Landeskriminalamtes wurden auch diese Diebstähle dem Betroffenen ohne weitere Erkenntnisse unterstellt.

  Dieser Umstand wurde gegenüber den Empfängern der Datenübermittlung richtiggestellt.

— Das LKA hat in dem Übermittlungsschreiben auch die Information über einen gegen den Betroffenen erlassenen Haftbefehl weitergegeben. Ob — wie der Petent behauptet —, der Haftbefehl wieder aufgehoben wurde, war nicht mehr zu klären. Das zuständige Gericht hatte die entsprechenden Unterlagen bereits vernichtet.

  Hier wurde die Darstellung des Petenten über die Aufhebung des Haftbefehls zur Kriminalakte genommen.

Für die Betroffenen ist von besonderer Bedeutung, für welchen Zeitraum die Polizei Kriminalakten aufbewahrt. Die Richtlinien für die Führung Kriminalpolizeilicher personenbezogener Sammlungen schreiben vor, daß das öffentliche Interesse, zu Zwecken der Strafverfolgung, Strafvollstreckung oder Gefah-

renabwehr auf polizeiliche Erkenntnisse zurückgreifen zu können, mit dem Recht auf informationelle Selbstbestimmung abzuwägen ist. Im Sinne einer verallgemeinernden Interessenabwägung sehen die Richtlinien eine regelmäßige Aussonderung nach 10 Jahren, in Fällen von geringerer Bedeutung grundsätzlich nach kürzerer Frist vor. Die jeweilige Frist beginnt an dem Tag, an dem das letzte Ereignis eingetreten ist, das die Aufnahme von Unterlagen in die Kriminalakte begründet hat. Diesen Grundsatz hat eine Polizeidienststelle nicht beachtet, als sie den Aufbewahrungszeitraum einer Kriminalakte nicht vom Zeitpunkt der Straftat, sondern vom Zeitpunkt der Beendigung der dem Betroffenen auferlegten Bewährungsfrist aus berechnet hat. Das Niedersächsische Innenministerium hat diesen Vorgang zum Anlaß genommen, die Leiter der Kriminalpolizeien auf die Vorschriften zur Berechnung der Aufbewahrungsfristen hinzuweisen.

12.18 Doppelt gespeichert hält länger

Wenn die Polizei in Ordnungswidrigkeitenverfahren Anzeigen bearbeitet und Ermittlungen angestellt hat, behält sie nach Abgabe des Originalvorganges an die zuständige Verwaltungsbehörde Durchschriften für sich zurück. Das Niedersächsische Innenministerium hält diese Praxis für geboten, damit einerseits eine umfassende Kontrolle der Polizeidienststellen im Rahmen der Fachaufsicht ermöglicht wird, andererseits Beschwerden und Eingaben beantwortet werden und Polizeibeamte sich auf ihre Zeugenaussage vor Gericht vorbereiten können. Die Durchschriften werden in Anlehnung an die Niedersächsische Aktenordnung bisher fünf Jahre aufbewahrt. Das Innenministerium beabsichtigt, diese Frist durch eine spezielle Regelung zu verkürzen. In Abhängigkeit von der Höhe der Geldbuße sollen die Durchschriftensammlungen zwischen einem Jahr und in schwerwiegenden Fällen z. B., wenn neben der Geldbuße ein Fahrverbot angeordnet wird, fünf Jahren vorgehalten werden. Ich kann nicht nachvollziehen, weshalb die Höhe der Geldbuße für die Dauer der Aufbewahrung von Durchschriften aus Ordnungswidrigkeitenverfahren eine Rolle spielen soll. Im Zusammenhang mit der Kontrolle der Polizeidienststellen bzw. der Vorbereitung auf eine Zeugenaussage ist diese Differenzierung jedenfalls nicht erforderlich. Die Durchschriftensammlung führt zu einer aus datenschutzrechtlicher Sicht problematischen Doppelspeicherung und unzulässigen Vorratsspeicherung. Im Ergebnis entstehen bei der Polizei gesonderte Datensammlungen über „Verkehrssünder" und sonstige ordnungswidrig handelnde Personen — ähnlich wie die Kriminalakten über Beschuldigte im Strafverfahren. Eine Anlehnung an die Richtlinien über das Führen und Aufbewahren von Kriminalakten verbietet sich schon deshalb, weil — anders als im Strafverfahren — für die Durchführung von Ordnungswidrigkeitenverfahren eine ausschließliche Zuständigkeit der Verwaltungsbehörden besteht.

Die Erforderlichkeit, Durchschriften aus Ordnungswidrigkeitenverfahren bei der Polizei vorzuhalten, kann ich — wenn überhaupt — nur aus Gründen der reinen Vorgangsverwaltung erkennen. Die Dauer der Aufbewahrungsfrist muß sich deshalb an diesem Zweck orientieren. Ich habe mich gegenüber dem Innenministerium für eine Aufbewahrungsfrist von einem Jahr zum Zweck der Vorgangsverwaltung ausgesprochen. Das Innenministerium hatte die Neuregelung zum 1. Januar 1992 angekündigt, hat sie aber noch immer nicht vorgenommen.

Mir erscheint es wichtig, in der Neuregelung die ausschließliche Zweckbindung der in den Durchschriftensammlungen gespeicherten Daten festzuschreiben. Daß insoweit Regelungsbedarf besteht, zeigt der folgende Sachverhalt, mit dem ich mich im Rahmen einer Eingabe zu befassen hatte:

Eine Polizeidienststelle hatte im Laufe eines Ermittlungsverfahrens wegen Nötigung im Straßenverkehr einer anderen Polizeidienststelle mitgeteilt, daß wegen verschiedener Vorgänge aus der Vergangenheit über den Beschuldigten bereits eine Akte angelegt worden sei. Die Akte wurde abgelichtet und in das aktuelle Verfahren eingebracht. Bei den übersandten Unterlagen handelte es sich um solche aus gegen den Petenten geführten Straf- und Ordnungswidrigkeitenverfahren in Verkehrssachen. Personenbezogen gesammelt wurde hier über einen Zeitraum von 10 Jahren. Die Polizeidienststelle erklärte hierzu, die Unterlagen seien aus der manuell geführten Vorgangsverwaltung, in der Ermittlungsersuchen nach Erledigung fortlaufend abgelegt würden, entnommen worden. Eine besondere Akte über den Petenten gebe es nicht. Die polizeiliche Aufsichtsinstanz ist mit mir allerdings der Meinung, daß die Formulierung der Polizeidienststelle in dem Übersendungsbericht auf eine speziell für den Petenten angelegte Akte hindeutet. In diesem Verfahren wurden mehrere Rechtsverstöße begangen: Durchschriften wurden länger aufbewahrt als es für die Aufgabenerfüllung erforderlich war, es wurde eine besondere „Verkehrssünderakte" angelegt, ohne daß hierfür eine Rechtsgrundlage bestand, und es wurden unter Mißachtung des Zweckbindungsgebotes aus den Durchschriftensammlungen Daten an Dritte übermittelt.

Die Durchschriftenakte wurde inzwischen vernichtet.

12.19 Die Polizeiliche Kriminalstatistik

Die Polizeiliche Kriminalstatistik (PKS) wird entgegen ihrer Bezeichnung nicht nur als Statistik, sondern auch als kriminalpolizeiliches Arbeitsmittel bei der Aufklärung von Straftaten, mithin als Straftäterdatei, eingesetzt. Auf die dagegen bestehenden datenschutzrechtlichen Bedenken habe ich bereits hingewiesen (vgl. X 12.13). Das Innenministerium beabsichtigt, im Landeskriminalamt ein zusätzliches, von der PKS unabhängiges Auswertungssystem zu installieren, das später durch das Auswertungsmodul des MIKADO-Systems (vgl. 12.7) ersetzt werden soll. Nach der Einrichtung des Auswertungssystems werden die Daten in der PKS-Datei anonymisiert. Das Innenministerium hat das Landeskriminalamt am 13. Juni 1991 angewiesen, in der Übergangszeit Selektionen zu Strafverfolgungszwecken aus der PKS-Datei nur noch durchzuführen, wenn die Maßnahme der Aufklärung besonders schwerer Straftaten (alle Verbrechen, alle in § 100 a StPO genannten Vergehen, alle uneingeschränkt meldepflichtigen Straftaten im Rahmen des kriminalpolizeilichen Meldedienstes) dient. Mit der nur noch für einen kurzen Zeitraum geplanten Nutzung der PKS-Datei für repressive kriminalpolizeiliche Zwecke habe ich mich einverstanden erklärt. Ich habe allerdings darauf hingewiesen, daß für die Einrichtung der neuen Auswertungsdatei kein Übergangsbonus gilt. Die Einrichtung bedarf einer normenklaren Rechtgrundlage. Außerdem erwarte ich, daß die in der PKS-Datei für statistische Zwecke nicht mehr erforderlichen Daten nach Einrichtung des Auswertungssystems gelöscht werden.

12.20 Datenübermittlung der Polizei an Presse, Hörfunk und Fernsehen

Die Veröffentlichung von personenbezogenen Daten führt zu einem schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung. Datenschutzrechtlich handelt es sich hierbei um die Übermittlung an einen unbestimmten Personenkreis. Die Veröffentlichung unterläuft die ursprüngliche Zweckbindung der erlangten Daten und löst sie auf. Die Weitergabe persönlicher Angaben an die Öffentlichkeit ist die intensivste Form der Übermittlung.

Es ist weder vorhersehbar noch bestimmbar, wer von den Daten Kenntnis erlangen wird und wie sie verwendet werden. Die Gefahr der sozialen Abstempelung liegt nahe (vgl. BVerfG, Beschluß v. 24. Juli 1990, NVwZ 1990, 1162 — Planfeststellung — und BVerfG, Beschluß v. 9. März 1988, NJW 1988, 2031 — Entmündigung). Beeinträchtigungen des Rechts auf informationelle Selbstbestimmung bedürfen einer gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für die Bürgerin bzw. den Bürger erkennbar ergeben und die damit dem rechtstaatlichen Gebot der Normenklarheit entspricht. Das Innenministerium hat meiner Forderung entsprechend für die Öffentlichkeitsfahndung im Gesetzentwurf für ein Niedersächsischen Gefahrenabwehrgesetz eine Rechtsgrundlage vorgesehen. Danach wird der Polizei erlaubt, zum Zweck der Ermittlung des Aufenthaltsortes einer Person Daten und Abbildungen öffentlich bekanntzugeben, wenn die Abwehr einer Gefahr für Leib oder Leben auf andere Weise nicht möglich ist oder Tatsachen die Annahme rechtfertigen, daß eine Person eine Straftat von erheblicher Bedeutung begehen wird, und wenn die Verhütung oder die Vorsorge für die Verfolgung dieser Straftat auf andere Weise nicht möglich ist. Ich habe in diesem Zusammenhang gefordert, daß die Aufhebung der Anonymität von (mutmaßlichen) Täterinnen und Tätern nur bei Straftaten von besonderer Bedeutung und auch nur dann zulässig sein sollte, wenn weniger einschneidende Schritte der Aufklärungsarbeit als aussichtslos zu bewerten sind. Bei Kindern und Jugendlichen überwiegt in der Regel das schutzwürdige Privatinteresse der Betroffenen. Ich habe mich dagegen ausgesprochen, daß personenbezogene Daten von Zeugen veröffentlicht werden. Bei diesem Personenkreis halte ich ein Eindringen in die Persönlichkeitssphäre nicht für gerechtfertigt.

Datenübermittlungen der Polizei an Presse, Hörfunk und Fernsehen im Rahmen der allgemeinen Öffentlichkeitsarbeit können sich auf das Niedersächsische Pressegesetz stützten. Nach § 4 Abs. 2 Nr. 3 dieses Gesetzes können Auskünfte gegenüber der Presse verweigert werden, wenn sie ein schutzwürdiges privates Interesse, z.B. das Recht auf informationelle Selbstbestimmung, verletzen würden. Zur Erleichterung der bei der Auskunftserteilung vorzunehmenden Güterabwägung will das Innenministerium eine Erlaßregelung vornehmen. Der Erlaßentwurf enthielt zunächst Aussagen, die ich aus datenschutzrechtlicher Sicht nicht mittragen konnte. Ich habe gefordert, daß im Rahmen der Öffentlichkeitsarbeit an Presse, Hörfunk und Fernsehen keine Daten weitergegeben werden dürfen, die Rückschlüsse auf eine bestimmte Person zulassen. Hierzu zählt auch die Verwendung von Namenskürzeln, weil dem Umfeld der Betroffenen durch Zusatzinformationen schnell klarwerden kann, um wen es sich handelt. Die Information der Öffentlichkeit gebietet die Veröffentlichung personenbezogener Daten in der Regel nicht. Ausnahmen sind nur dann denkbar, wenn der Sachverhalt gerade im Hinblick auf die betroffene Person für die Allgemeinheit von erheblicher Bedeutung ist. Eine identifizierende Berichterstattung kann ausnahmsweise gerechtfertigt sein, wenn es um Personen der Zeitgeschichte oder um solche geht, die ein öffentliches Amt bekleiden. Auch die Angaben zu Ursachen und Tatmotiven müssen so abgefaßt sein, daß kein Personenbezug hergestellt werden kann. Das Innenministerium hat meine datenschutzrechtlichen Anmerkungen bei der Überarbeitung des Erlaßentwurfes berücksichtigt.

12.21 Datenschutz bei Telefonüberwachungen? Bitte warten ... bitte warten ...

In Niedersachsen steht eine datenschutzgerechte Regelung über die Weitergabe von personenbezogenen Daten aus Telefonüberwachungen noch aus. Aus datenschutzrechtlicher Sicht ist in diesem Zusammenhang fraglich, ob Er-

kenntnisse aus Abhörmaßnahmen in Strafverfahren durch die Polizei zur Gefahrenabwehr benutzt werden dürfen.

In Hessen wurden solche Erkenntnisse in einer parlamentarischen Debatte personenbezogen weitergegeben, um Anschuldigungen gegen den Hessischen Ministerpräsidenten entgegentreten zu können. Als Konsequenz aus diesem Vorfall haben in Hessen Innen- und Justizministerium durch Erlaß festgelegt, daß die Polizei personenbezogene Daten, die aufgrund strafprozessualer Eingriffe in das Fernmeldegeheimnis erlangt worden sind, grundsätzlich nur mit Zustimmung der ermittelnden Staatsanwaltschaft weitergeben darf. Die Weitergabe ist zu dokumentieren. Sind die Daten zu löschen, ist der Empfänger zu unterrichten, damit die Daten dort ebenfalls unverzüglich getilgt werden. Nur wenn die Staatsanwaltschaft nicht erreichbar ist, darf die hessische Polizei solche Daten — und das auch nur zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit und Ordnung und bei Gefahr im Verzuge — übermitteln. Die Genehmigung der Staatsanwaltschaft ist in diesen Fällen unverzüglich nachträglich einzuholen.

Das Niedersächsische Innenministerium hat auf meine Initiative im Juli 1991 eine der hessischen Vorschrift vergleichbare Erlaßregelung angekündigt. Eine datenschutzgerechte Neufassung des zur Zeit noch gültigen Erlasses vom 19. November 1971 ist bisher jedoch nicht erfolgt.

12.22 Zusammenarbeit zwischen der Polizei und Privatfirmen

Presseberichten war zu entnehmen, daß der Polizei eines anderen Bundeslandes vorgeworfen wurde, personenbezogene Daten aus polizeilichen Dateien über Arbeitnehmerinnen und Arbeitnehmer an den Arbeitgeber weitergegeben zu haben. Ich habe diese Berichte zum Anlaß genommen, Datenübermittlungen durch die niedersächsische Polizei an private Firmen zu hinterfragen. Das Innenministerium hat mir mitgeteilt, im Rahmen sicherheitsempfindlicher Beschäftigungsverhältnisse (z. B. bei Atomanlagenbetreibern) finde ein Datenaustausch mit Einwilligung der Betroffenen statt. Außerdem würden die personenbezogenen Daten von Beschäftigten im unmittelbaren Umfeld gefährdeter Personen mit deren Einverständnis durch den Abgleich mit polizeilichen Dateien überprüft.

12.23 Übermittlung von Kfz-Fahndungsdaten an private Stellen

Daten über Kraftfahrzeuge, nach denen die Polizei fahndet, werden im Rahmen der INPOL-Anwendungen in der Sachfahndungsdatei beim BKA gespeichert. Aus dieser Datei werden seit Januar 1992 elektronisch Fahrzeugidentifizierungsnummer, Kennzeichen, sachbearbeitende Dienststelle mit Aktenzeichen und das Datum der Fahndungsausschreibung an drei Kraftfahrzeughersteller übermittelt. Dem HUK-Verband werden Fahrzeugidentifizierungsnummer, Kennzeichen, sachbearbeitende Dienststelle und Tatzeit mitgeteilt. Datenschutzrechtlich sind diese Übermittlungen relevant, weil sich aus der Fahrzeugidentifizierungsnummer und dem Kennzeichen ein Personenbezug herstellen läßt. Auch eine sog. „Sachfahndungsdatei" kann daher Personenbezüge enthalten. Die übermittelten Daten werden in den Datenverarbeitungssystemen der Empfänger aufgenommen und stehen den angeschlossenen internen Teilnehmern (z. B. Niederlassungen, Vertragswerkstätten, auch im Ausland) permanent zur Verfügung. Die Hersteller wurden verpflichtet, die Daten nur für Zwecke des Abgleichs mit Reparaturaufträgen, Ersatzteil- und

Schlüsselbestellungen zu verwenden. Auf diese Weise soll es ihnen ermöglicht werden, gesuchte Fahrzeuge zu entdecken und damit die polizeiliche Fahndung zu unterstützen. Die an den HUK-Verband übermittelten Daten dienen zur Überprüfung von sichergestellten bzw. kontrollierten Fahrzeugen, die nach Osteuropa verschoben wurden.

Im Ergebnis habe ich mich diesen Übermittlungen nicht entgegengestellt. Ein objektiver Ansatz bei Fahndungsmaßnahmen, der aus polizeilicher Sicht Erfolge verspricht, ist im Vergleich mit einer Vorgehensweise, die von Daten über Personen ausgeht, datenschutzrechtlich vorzuziehen. Überwiegende datenschutzrechtliche Interessen sprechen jedenfalls nicht grundsätzlich gegen eine Übermittlung von Kfz-Fahndungsdaten an private Stellen.

Meine Bedenken sind eher grundsätzlicher Natur. Die Einbeziehung privater Personen und Institutionen in die polizeiliche Fahndung könnte zu Weiterungen führen, bei denen auch sensiblere Daten als die hier benutzten übermittelt werden. Das Verfahren unterscheidet sich auch nicht mehr wesentlich von einer Rasterfahndung. Es macht insoweit aus Sicht der Betroffenen keinen Unterschied, ob Fahndungsdaten mit anderen polizeilichen Systemen oder mit privaten Datenbeständen abgeglichen werden.

Ich werde mögliche Entwicklungen dieser Art mit Aufmerksamkeit beobachten.

13. Ausländerangelegenheiten

Während die Diskussion über den Datenschutz in Ausländerangelegenheiten vor zwei Jahren noch von der Auseinandersetzung über die Novellierung des Ausländergesetzes bestimmt war, verlagerte sich das Schwergewicht in den letzten zwei Jahren immer mehr auf den Asylbereich.

Die Zahl der Asylanträge hat in der vergangenen Zeit massiv zugenommen. Nach Angaben des Bundesinnenministeriums gab es 438 191 Anträge im Jahr 1992. Das Niedersächsische Innenministerium erwartet für 1992 bundesweit 650 000 Asylanträge. Mit der Unterbringung der Flüchtlinge haben die zuständigen Stellen des Landes alle Hände voll zu tun. Die großen Antragszahlen und die massive Belastung der Behörden dürfen jedoch nicht dazu führen, das allgemeine Persönlichkeitsrecht und den Datenschutz für Flüchtlinge zu vernachlässigen.

An der Bearbeitung von Asylverfahren wirkt eine Vielzahl unterschiedlicher Stellen mit, vorrangig

- die für die Unterbringung zuständigen Zentralen Anlaufstellen (ZASt) und die Gemeinden, insoweit ist die Zuständigkeit des Ministeriums für Bundes- und Europaangelegenheiten gegeben,
- die für ausländerrechtliche Behandlung zuständigen, dem Innenministerium unterstellten Zentralen Ausländerbehörden (ZAB) bei den Zentralen Anlaufstellen,
- das für die Anerkennung als politisch Verfolgter zuständige Bundesamt für die Anerkennung von Flüchtlingen (BAFl) mit seinen Außenstellen in den Zentralen Anlaufstellen.

Die Situation wird dadurch noch komplizierter, daß nach dem neuen Asylverfahrensgesetz ab 1. April 1993 für die ausländerrechtliche Behandlung der Asylsuchenden das BAFl zuständig wird. Die Zuständigkeit für die Abschiebung bleibt jedoch bei den Ausländerbehörden des Landes. Überspitzt formuliert könnte man sagen, daß der beste „Datenschutz" für die Asylsuchenden darin besteht, daß die zuständigen Behörden aufgrund ihrer Überlastung und ihrer mangelnden Ausstattung gar nicht in der Lage sind, alle nach dem Gesetz vorgesehenen Datenverarbeitungsmaßnahmen durchzuführen.

Beteiligt am Verfahren sind weiterhin das Bundeskriminalamt, die Landespolizei, die Sozialämter, die Gesundheitsämter, die allgemeine Verwaltung der Kommunen sowie kirchliche Träger, bei der Abschiebung abgelehnter Asylsuchender der Bundesgrenzschutz. Durch diese vielen Verfahrensbeteiligten kommt es zwangsläufig zu einer Vielzahl von Datenübermittlungen, welche kaum überschaubar ist. Nach Angaben des Ministeriums für Bundes- und Europaangelegenheiten bedarf es derzeit schon bei den Anlaufstellen bis zu 30 Telefaxgeräte, um monatlich 24 000 Telefaxmitteilungen zu versenden.

So wichtig es ist, mit Hilfe des EDV-Einsatzes die Bearbeitungszeit der Asylbegehren zu verkürzen, so wichtig ist es, hierbei den Persönlichkeitsschutz der Asylsuchenden zu beachten. Leider scheint hier nicht überall die nötige Sensibilität zu bestehen. So erfuhr ich aus einem anderen Bundesland, daß dort die Landesregierung beschlossen hat, auf Bundesebene darauf hinzuwirken, einen „umfassenden Informations- und Datenverbund zwischen den berührten Stellen (Sozialhilfeträger, Unterbringungsverwaltung, Ausländerverwaltung, Arbeitsverwaltung, Träger der Sozialversicherung, Kfz-Zulassungsstellen, Polizei u. a.)" zu ermöglichen. Ich gehe davon aus, daß die Niedersächsische Landesregierung sich Bestrebungen der Verfahrensbeschleunigung widersetzt, die den „gläsernen Asylsuchenden" zur Folge hätten.

13.1 Asylverfahrensgesetz

Das Gesetz zur Neuregelung des Asylverfahrens vom 26. Juni 1992 (AsylVerfG) enthält erstmals auch detaillierte informationsrechtliche Regelungen (BGBl. I S. 1126). Leider wurden dabei die Vorschläge der Datenschutzbeauftragten nicht berücksichtigt. Dies betrifft insbesondere die Regelung des § 16 AsylVerfG, der eine ausnahmslose Verpflichtung zur Anfertigung von erkennungsdienstlichen Unterlagen aller Asylbewerberinnen und Asylbewerber vorsieht. Zwar hatten die Datenschutzbeauftragten auf ihrer Konferenz am 28. April 1992 darauf hingewiesen, daß die undifferenzierte Datenerhebung sowie die Nutzung dieser Daten für polizeiliche Zwecke mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar ist (vgl. Anlage 7). Der Gesetzgeber ließ sich hiervon jedoch nicht beeindrucken.

Im Rahmen der Diskussion um das Asylverfahrensgesetz wurde unter anderem vorgebracht, staatliche Leistungen, also hier der Schutz vor Verfolgung und Not und die Inanspruchnahme materieller Hilfe, insbesondere Sozialhilfe, setzten jeweils die eindeutige Feststellung der Identität des einzelnen voraus. Dies ist sicher im Grundsatz richtig. Doch ein hundertprozentiger Schutz vor Rechtsmißbrauch ist auch bei umfangreichsten Überwachungsmaßnahmen nicht möglich. Mit dem Hinweis auf Rechtsmißbrauch darf nicht die totale Datensammlung in einem großen gesellschaftlichen Bereich gerechtfertigt werden, die auch Menschen erfaßt, die sich völlig gesetzeskonform verhalten. Auch gegenüber ausländischen Menschen darf der Staat nur dann zu Zwangsmaßnahmen wie der Anfertigung von ED-Unterlagen greifen, wenn Anhaltspunkte für den Mißbrauch von staatlichen Leistungen bestehen.

13.2 ZASt-Verfahren

Es ist nicht verwunderlich, daß im Asylverfahren auf die Hilfe automatisierter Datenverarbeitung zurückgegriffen wird. Dies liegt auch im Interesse der Antragstellerinnen und Antragsteller, da hierdurch die Verfahrensdauer verkürzt werden kann. Voraussetzung ist aber, daß hierbei das Grundrecht auf informationelle Selbstbestimmung sowie die speziellen datenschutzrechtlichen Regelungen eingehalten werden. Es ist verwunderlich, daß auch in Niedersachsen erst zum Ende des Berichtszeitraumes mit der Automatisierung des Aufnahmeverfahrens begonnen wurde.

Anläßlich eines von meiner Seite gewünschten Gespräches wurde mir mitgeteilt, daß in Kürze in der ZASt Braunschweig eine automatisierte Datei mit dem Namen „ZASt-Verfahren" in Betrieb gehen solle. Wegen der Eile und weil das Verfahren noch nicht voll ausgereift sei, könne noch keine Errichtungsanordnung vorgelegt werden. Während des Gesprächs wurde eine Datensatzbeschreibung vorgelegt, gegen die ich keine prinzipiellen Einwände habe. Ich erinnerte das Ministerium daran, daß aufgrund der für die Landesverwaltung verbindlichen IuK-Technik-Grundsätze eine Verpflichtung besteht, in einer Errichtungsanordnung die wichtigsten Funktionen eines neu eingeführten Systems zu dokumentieren. Für das System „ZASt-Verfahren" lag eine solche Errichtungsanordnung erst zwei Monate nach der Inbetriebnahme vor.

Geplant ist in jeder der künftig sechs Anlaufstellen ein lokales Netz (LAN), in welchem neben Identifizierungsdaten Angaben zum Reiseverlauf, der Zugehörigkeit zu bestimmten Nationalitäten, Religionen und Familien sowie Unterbringungswünsche registriert werden. Mit Hilfe dieser Angaben sollen die Verwaltung der ZASt sowie die landesweite Verteilung der Asylsuchenden bewerkstelligt werden. In einem späteren Ausbaustadium sind informationelle Beziehungen zu anderen Stellen sowie die zentrale Systemverwaltung durch das Ministerium für Bundes- und Europaangelegenheiten vorgesehen. Für die Inbetriebnahme des Systems konnte ich, trotz der genannten formellen Mängel, grünes Licht geben. Klärungsbedarf besteht aber bei der Nutzung dieses Systems durch andere Stellen und bei der Vernetzung der lokalen Netzwerke. Das Ministerium sagte mir zu, mich über den weiteren Verfahrensgang auf dem laufenden zu halten.

13.3 Zentrale Ausländerbehörden

Bei der Zentralen Ausländerbehörde (ZAB) in Oldenburg wird mit Hilfe automatisierter Datenverarbeitung das Bearbeiten der Unterlagen und das Ausfüllen der Vordrucke für das Ausländerzentralregister (AZR) vorgenommen (vgl. 13.8). Bei der ZAB Braunschweig erfolgt derzeit noch konventionelle Datenverarbeitung. Automatisiert erfolgt ausschließlich die Abfrage, ob im AZR beim Bundesverwaltungsamt in Köln eine Notierung über die gemeldete Person vorhanden ist.

13.4 Automatisches Fingerabdruckidentifikationssystem (AFIS)

Nach Angaben des Innenministeriums kommen 75 bis 80 % der Flüchtlinge ohne Personalpapiere nach Niedersachsen. In diesen Fällen ist es prinzipiell nicht zu beanstanden, daß erkennungsdienstliche Unterlagen zum Zweck der Identifizierung angefertigt werden. Dies wird derzeit, je nach Kapazitätslage, von der Kriminalpolizei durchgeführt. Der Sinn dieser Maßnahme relativiert

sich aber aufgrund des Umstandes, daß das Bundeskriminalamt (BKA) bisher nicht in der Lage war, die angelieferten erkennungsdienstlichen Unterlagen auszuwerten.

Voraussetzung für die in § 16 AsylVerfG vorgesehene lückenlose Identifizierung aller Asylsuchenden mit Hilfe von Fingerabdrücken ist, daß der dadurch entstehende Verwaltungsaufwand tatsächlich auch bewältigt werden kann. Es geht nicht an, daß tausendfach ED-Unterlagen angefertigt werden, welche dann nicht genutzt werden und letztendlich wieder auch im Interesse des Datenschutzes vernichtet werden müssen, so wie dies in der Vergangenheit der Fall war. Bisher konnte das BKA, welches hier zur Amtshilfe herangezogen wird, mit Hilfe des halb-automatisierten Bund-Länder-Systems (BLS) im Jahr nur etwa 12 000 Fingerabdruckblätter von Asylsuchenden auswerten. Ziel ist nun, ein automatisiertes System der Fingerabdruckerkennung und Speicherung einzuführen. Nach einer EG-weiten Ausschreibung erhielt für die Realisierung eines „Automatischen Fingerabdruckidentifizierungssystems" (AFIS) im Februar 1992 ein französischer Anbieter den Zuschlag. Das am 3. Dezember 1992 in Betrieb gegangene AFIS soll jährlich 400 000 Datensätze erfassen können. Man erwartet von dem System, das eine schnelle Identifizierung der Asylsuchenden innerhalb von fünf Tagen ermöglicht, neben dem Effekt der Verfahrensbeschleunigung das Erkennen von mehrfach gestellten Asylanträgen sowie eine abschreckende Wirkung zur Reduzierung von Doppelantragstellungen. Es wird sich zeigen, ob, wie geplant, die derzeit noch nicht ausgewerteten ca. 150 000 Fingerabdruckblätter im Laufe des Jahres 1993 tatsächlich in das System eingegeben werden.

Erfaßt werden die sog. Langverformelungen der Abdrücke aller zehn Finger. Mit Hilfe dieser Langverformelung ist nicht nur eine eindeutige Identifizierung möglich, sondern auch die kriminalistische Zuordnung von Spuren. Wollte man nur die Identifizierung der Asylsuchenden sicherstellen, so wäre die Langverformelung eines Fingers oder, entsprechend einem älteren Verfahren, die Kurzverformelung aller zehn Fingerabdrücke ausreichend. Daß man sich hiermit nicht begnügen will, ist eine Verletzung des Erforderlichkeitsgebots. Zu kritisieren ist auch die Heranziehung der Polizei beim Anfertigen der ED-Unterlagen und insbesondere bei deren Speicherung. Es kann nicht begründet werden, weshalb die Angaben der Asylsuchenden gemeinsam mit den Angaben über potentielle und tatsächliche Straftäter beim Bundeskriminalamt gespeichert werden und dort auch zu anderen Zweck umfassend genutzt werden müssen.

13.5 AFIS international: EURODAC

Die Speicherung der AFIS-Unterlagen erhält dadurch eine zusätzliche Brisanz, daß der Aufbau der nationalen ED-Datei der Asylsuchenden nur ein Zwischenstadium ist für eine europäische Datei, welche von der Arbeitsgruppe der EG-Innen- und Justizminister vorbereitet wird. Diese EURODAC-Datei soll, nach dem erklärten Willen der Bundesregierung, ED-Unterlagen der Asylsuchenden aller EG-Staaten enthalten. Der Bundesdatenschutzbeauftragte unterrichtete mich über den Stand der Planungen. Auf ihrer Tagung am 2./3. Dezember 1991 gaben die für Einwanderungsfragen der EG-Mitgliedstaaten zuständigen Minister den Auftrag, eine Machbarkeitsstudie für EURODAC zu erstellen. Diese Studie wurde im Herbst 1992 vorgelegt. Darin werden vier Optionen für die Systemarchitektur vorgestellt und auf ihre Realisierbarkeit in finanzieller, zeitlicher und technischer Hinsicht untersucht. Es ist sowohl bei der Datenerfassung wie bei der Datenspeicherung eine zentrale wie eine dezentrale Lösung im Gespräch. Bei der Erfassung wird gar erwogen, die

Verformelung der Fingerabdrücke durch modernste Verfahren mit Hilfe eines „Life-Scan" maschinell vornehmen zu lassen. Danach muß die oder der Asylsuchende nur noch die Hand auf ein Lesegerät legen, welches die Hautlinien der Finger erfaßt, digitalisiert, in einen alphanumerischen Code umwandelt, speichert und mit den vorhandenen Datensätzen abgleicht.

Ich habe den zuständigen niedersächsischen Ministerien mitgeteilt, daß ich gegen das geplante Verfahren Bedenken habe. Diese richten sich zunächst gegen die eingeschlagene Vorgehensweise: Bevor eine Diskussion über die Notwendigkeit dieses Verfahrens erfolgte und noch bevor überhaupt mit der Schaffung der erforderlichen Rechtsgrundlagen begonnen wurde, wird die technische Machbarkeit eines derart sensiblen Systems detailliert untersucht. Ich habe die Befürchtung, daß mit der technischen Planung Fakten für die politischen und rechtlichen Entscheidungen geschaffen werden, die nicht mehr rückgängig gemacht werden können.

Sicher ist, daß eine derartige Totalerfassung der Flüchtlinge in der EG ein gewaltiges Mißbrauchspotential darstellt. Ein solches System lädt geradezu ein, für alle möglichen Zwecke, insbesondere zur Kriminalitätsbekämpfung, verwendet zu werden. Ohne auf die genaue rechtliche und technische Ausgestaltung des EURODAC-Planes einzugehen, meine ich, schon vor dem Grundansatz dieses Konzepts aus datenschutzrechtlicher Sicht warnen zu müssen. Dies gilt nicht nur in Hinblick auf das Persönlichkeitsrecht der Betroffenen selbst, sondern auch wegen des Pilotcharakters eines solchen Datenbanksystems für andere gesellschaftliche Bereiche. Würde eine Datei wie das geplante EURODAC über EG-Bürgerinnen und -Bürger geführt, so wäre deren Unzulässigkeit jedem Menschen einsichtig. Da hier jedoch Menschen aus Drittländern betroffen sind, scheint diese Sicht nicht mehr zwingend zu sein.

13.6 Gesundheitsuntersuchung von Asylsuchenden

Zufällig erfuhr ich, daß das Niedersächsische Sozialministerium zur Durchführung des § 62 AsylverfG im Erlaßwege die zwangsweise Gesundheitsuntersuchung aller Asylsuchenden regeln will. § 62 AsylVerfG sieht vor, daß die oberste Landesgesundheitsbehörde den Umfang und die Ärztin bzw. den Arzt der Untersuchung von Asylsuchenden bestimmt.

Ich begrüße es, daß das Sozialministerium auf die in der Öffentlichkeit immer wieder geforderte, aber äußerst fragwürdige zwangsweise AIDS-Untersuchung verzichtet hat. Ich habe klargestellt, daß nicht alle am Asylverfahren beteiligten Behörden über die medizinischen Untersuchungsergebnisse unterrichtet werden dürfen. § 62 Abs. 2 sieht nur die Mitteilung des Befundes vor, soweit dieser für die Unterbringungsstelle erforderlich ist. Alle anderen Übermittlungen bedürfen einer speziellen Rechtsgrundlage, etwa aus dem Ausländergesetz, dem Bundesseuchen- oder dem Geschlechtskrankheitengesetz. Schließlich habe ich angemahnt, Aufbewahrungsfristen für die entstehenden Unterlagen festzulegen.

13.7 Anwendung des Ausländergesetzes

Wegen der offenen Formulierung der Übermittlungsregelungen im AuslG und des Fehlens von Durchführungsvorschriften ist es von großer Bedeutung, daß sich die Anwendung dieser Vorschriften auf das datenschutzrechtlich zulässige Mindestmaß beschränkt. Insofern begrüße ich eine Entscheidung des

Niedersächsischen Oberverwaltungsgerichts (OVG), in welcher die Übermittlungspflichten an die Ausländerbehörde konkretisiert werden (Beschluß vom 6. März 1992, Az. 4 M 2122/91). Die Antragsteller in diesem Verfahren wandten sich dagegen, daß die Jugendbehörde einer kreisfreien Stadt die Ordnungsbehörde über die Erziehung außerhalb der eigenen Familie nach dem KJHG unterrichtete. Zwar sieht § 76 Abs. 2 AuslG vor, daß die Ausländerbehörde bzw. die Polizeibehörde unverzüglich über Ausweisungsgründe zu unterrichten ist. Auch ist richtig, daß nach § 46 Nr. 7 AuslG die Hilfe zur Erziehung außerhalb der eigenen Familie einen Ausweisungsgrund darstellen kann. Das OVG leitet aber aus dem Grundsatz der Verhältnismäßigkeit ab, daß eine Mitteilung nur dann zulässig ist, wenn sie auch zur Zweckerfüllung, also der Durchführung des AuslG, erforderlich ist. Da die Antragsteller teilweise Asylsuchende waren und teilweise eine Aufenthaltserlaubnis besaßen, welche durch § 46 Nr. 7 AuslG nicht verdrängt werden konnte, war die Inanspruchnahme der Hilfe zur Erziehung ausländerrechtlich irrelevant. Zwar läßt das Gericht offen, wie weit die Pflicht des Jugendamtes reicht zu prüfen, ob die Angaben für die ausländerrechtliche Entscheidung erforderlich sind. In jedem Fall sieht sich das Gericht selbst zu dieser Prüfung verpflichtet. Dies führt im Ergebnis dazu, daß die der Ausländerbehörde übermittelnde Stelle nicht nur überprüfen muß, ob die Mitteilung zu einer Ausweisung führen könnte, sondern, ob sie voraussichtlich diese Rechtsfolge auch haben wird. Die aus datenschutzrechtlicher Sicht erfreuliche Entscheidung hat zur Folge, daß bei der Ausländerbehörde von anderen Stellen keine Daten auf Vorrat gesammelt werden dürfen.

13.8 Ausländerzentralregister

Beim Bundesverwaltungsamt in Köln wird das Ausländerzentralregister (AZR) als automatisierte Datei geführt. In ihr sind z. Zt. 9,7 Mio. Ausländerinnen und Ausländer gespeichert. Man sollte meinen, daß der Gesetzgeber neun Jahre nach der Verkündung des Volkszählungsurteils des Bundesverfassungsgerichts eine bereichsspezifische Rechtsgrundlage für eine dermaßen umfangreiche Datensammlung geschaffen hat. Doch das von den Datenschutzbeauftragten seit langem geforderte Gesetz zum AZR ist bis heute noch nicht verabschiedet worden. Unter X 13.3 habe ich den Gesetzentwurf der Bundesregierung vom Juni 1989 kritisch dargestellt. Weder vom Verfahren her noch in der Ausgestaltung der materiellen Regelungen hat es seitdem durchgreifende Fortschritte gegeben. Es liegt zwar ein weiterer Entwurf der Bundesregierung zum Ausländerzentralregister mit Stand 15. Juli 1991 vor. Dabei wurde der Vorgängerentwurf jedoch trotz der massiven Bedenken, welche durch die Datenschutzbeauftragten geäußert worden sind, ohne wesentliche Änderungen übernommen.

13.9 Eingeschränkte Mitteilungspflicht der Ausländerbeauftragten

Nach § 76 Abs. 1 und 2 des Ausländergesetzes sind alle öffentlichen Stellen auf Ersuchen und bei bestimmten Sachverhalten von Amts wegen verpflichtet, bekanntgewordene ausländerrechtlich relevante Umstände und damit personenbezogene Daten der Ausländerbehörde mitzuteilen. Das Gesetz ermächtigt die Landesregierungen, die Stellen zu bestimmen, die Informationen nur weitergeben müssen, soweit dadurch die Erfüllung ihrer eigenen Aufgaben nicht gefährdet wird. Die Niedersächsische Landesregierung ist in der Verordnung vom 3. September 1992 (Nieders. GVBl. S. 241) der Anregung gefolgt,

den Kreis der öffentlichen Stellen, die lediglich der eingeschränkten Informationspflicht unterliegen, weit zu ziehen. In der Verordnung sind nicht nur die Ausländerbeauftragten des Landes, der Landkreise und der Gemeinden, sondern auch die Mitglieder kommunaler Ausländerbeiräte und von Ausländerausschüssen kommunaler Vertretungen genannt. Soweit diesen Einrichtungen in gleicher Weise wie den Ausländerbeauftragten die Wahrnehmung von Interessen der ausländischen Einwohnerinnen und Einwohner gegenüber kommunalen Organen obliegt, gilt für sie die eingeschränkte Mitteilungspflicht. Ich begrüße, daß Niedersachsen die bundesgesetzliche Ermächtigung datenschutzfreundlich umgesetzt hat.

14. Verfassungsschutz

14.1 Niedersächsisches Verfassungsschutzgesetz

Der Niedersächsische Landtag hat am 21. Oktober 1992 das Gesetz über den Verfassungsschutz im Lande Niedersachsen beschlossen. Seit Jahren hatte ich eine umfassende Neuregelung dieser Materie gefordert. Das Gesetz löst das aus dem Jahr 1976 stammende Verfassungsschutzgesetz ab, das den verfassungsrechtlichen Anforderungen zum Recht auf informationelle Selbstbestimmung, so wie sie im Volkszählungsurteil des Bundesverfassungsgerichts von 1983 näher dargelegt sind, nicht gerecht wurde. Verfassungsschutzbehörde ist nun das unter der Aufsicht des Niedersächsischen Innenministeriums stehende Landesamt für Verfassungsschutz; bisher hat die Abteilung 4 des Innenministeriums die Aufgaben wahrgenommen.

Das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 des Grundgesetzes entwickelte Recht auf informationelle Selbstbestimmung unterliegt im Bereich des Verfassungsschutzes einer besonderen Bewährungsprobe. Das Verfassungsschutzgesetz ist ein reines Informationsverarbeitungsgesetz; Verwaltungsvollzug gegenüber Personen findet nicht statt. Der Verfassungsschutz arbeitet geheim — eine Verfahrensweise, die zunächst einmal dem verfassungsrechtlichen Anspruch der Bürgerinnen und Bürger zuwiderläuft, selbst über die Preisgabe und Verwendung ihrer Daten zu bestimmen. Auf der anderen Seite sind Einschränkungen dieses Rechts im überwiegenden Allgemeininteresse hinzunehmen. Der hiernach gegenüber den Menschen mögliche Eingriff muß sich allerdings auf das zur Aufgabenerfüllung unbedingt notwendige Maß beschränken. Die Festlegung des im überwiegenden Allgemeininteresse liegenden erforderlichen Minimums an Datenverarbeitung ist in Angelegenheiten des Verfassungsschutzes außerordentlich schwer, zumal über die interne Arbeitsweise dieser Behörde relativ wenig bekannt ist. Zudem ist „Verfassungsschutz" ein eminent politischer Gegenstand. Dies wird besonders deutlich, wenn er aufgrund bekanntgewordener Aktivitäten Gegenstand öffentlicher Erörterungen wird. Ein Verfassungsschutzgesetz spiegelt immer auch ein Stück Selbstverständnis des Staates zu seinen Bürgerinnen und Bürgern wider. Mit der Entscheidung über die Aufgaben und Befugnisse legt das Gesetz fest, inwieweit der Staat selbstbewußt genug ist, auch völlig abwegige politische Meinungen sowie noch nicht strafrechtlich relevante Verhaltensweisen hinzunehmen; eben nicht zu registrieren, weil sie — noch — keine Gefährdungssituation darstellen. Angesichts spezifisch niedersächsischer Erfahrungen und Konstellationen und im Hinblick auf den Anspruch der jetzigen Landesregierung, verlorengegangenes Vertrauen zurückzugewinnen, durfte ein auch in datenschutzrechtlicher Hinsicht richtungweisender Wurf erwartet werden.

Das Niedersächsische Verfassungsschutzgesetz hat den Datenschutz in der Tat einige Schritte vorangebracht. Einen den Datenschutz befördernden „Wind of Change" kann ich jedoch nicht feststellen.

Als positive Beispiele bewerte ich:

— das bisher nicht vorhandene Recht der Betroffenen auf Auskunft über die zu ihrer Person gespeicherten Daten;
— die regelmäßige Überprüfung der in Dateien gespeicherten Daten nach fünf und die regelmäßige Löschung nach zehn Jahren;
— den Ausbau verfahrensrechtlicher Schutzvorkehrungen durch die Dokumentation von Datenübermittlungen des Landesamtes an andere als Verfassungsschutzbehörden, insbesondere in das Ausland und an Privatpersonen, sowie die Einrichtung eines parlamentarischen Kontrollausschusses;
— die besonderen Regelungen zum Schutz Minderjähriger;
— präzisere Aufgabenbestimmungen und die Hochzonung der Beobachtungsschwelle für Bestrebungen/Tätigkeiten auf solche, die auf Gewaltanwendung gerichtet sind oder ein aktiv kämpferisches, agressives Verhalten gegen die Prinzipien der freiheitlich demokratischen Grundordnung an den Tag legen;
— die — vorbildliche — gesetzliche Aufzählung der erlaubten nachrichtendienstlichen Mittel (z. B. ist der Einsatz von Wanzen in Wohnungen verboten), die grundsätzliche Zweckbindung der dabei gewonnenen Informationen sowie die Eingrenzung der zulässigen Verwirklichung von Straftatbeständen bei der Verwendung solcher Mittel;
— die verhaltenssteuernde Betonung des Grundsatzes der Verhältnismäßigkeit.

Wie erfreulich diese Beispiele aus datenschutzrechtlicher Sicht auch sind, ein Blick in das Gesetz belegt, daß hinter all den Beispielen zugleich ein „aber" zu setzen ist. So sind etwa die Möglichkeiten, ein Auskunftsverlangen abzulehnen, in einer sehr umfassenden Weise formuliert. Befürchtungen, das Gesetz mache das Landesamt zu einer Auskunftei, verkennen die Tragweite der mit unbestimmten Rechtsbegriffen gespickten Ablehnungsgründe.

In der zuvor genannten Aufzählung fehlen leider seit langem entwickelte strukturelle Forderungen. Qualitative datenschutzrechtliche Veränderungen hätten beispielhaft bedeutet:

— Mehr Mut zur Transparenz.
Zur Herstellung einer informierten Öffentlichkeit genügt es nicht, in den jährlichen Verfassungsschutzberichten die Summe der Haushaltsmittel für das Landesamt und die Gesamtzahl seiner Bediensteten anzugeben. Zu denken wäre an eine Liste der beobachteten Bestrebungen, die Nennung der Zahl der erfaßten Personen, der Anzahl der besonders in das Persönlichkeitsrecht eingreifenden nachrichtendienstlichen Mittel oder der Anzahl der Auskunftsverlangen/Ablehnungen.

— Mehr fachliche Phantasie.
Der lohnenswerte Versuch, im Rahmen des verfassungsrechtlich Möglichen, Aufgaben und datenschutzrelevante Eingriffsmöglichkeiten (Befugnisse) des Landesamtes zu überdenken — zumindest die Befugnisse einzelnen Aufgaben zuzuordnen —, wurde nicht unternommen. Dabei haben sich doch seit Wegfall der Mauer die politischen Rahmenbedingungen entscheidend verändert. Hierauf geht das Gesetz nicht ein. Aufgabenstrukturen und Befugnisse bleiben so, wie sie einmal vor 40 Jahren angelegt wurden. Darüber hinaus geht die Entwicklung in eine ganz andere Richtung: Die Verfassungsschutzbehörden sind auf der Suche nach neuen Aufgaben.

Die politischen Veränderungen haben im Frühjahr 1990 dazu geführt, auf Bundesebene Argumente für neue Aufgaben des Verfassungsschutzes vorzutragen. Dazu zählen etwa die Beobachtung der international organisierten Kriminalität (siehe Hannoversche Allgemeine Zeitung vom 30. Oktober 1992) und die Beobachtung der Lieferung sensitiver Stoffe/Anlagen in Krisengebiete. Jüngst hat der Präsident des Bundesamtes für Verfassungsschutz unter Hinweis auf die europäische Zusammenarbeit eine umfassendere Aufgabenstellung vorgeschlagen. Der Name dieses „echten Inlandsdienstes" solle „Bundesamt für innere Sicherheit" lauten (vgl. Süddeutsche Zeitung vom 1. November 1992).

— Mehr Gelassenheit beim Umgang mit personenbezogenen Daten.
Das Fehlen eines umfassend novellierten Niedersächsischen Datenschutzgesetzes mag hier eine Rolle gespielt haben. Nach wie vor ist es nach dem Verfassungsschutzgesetz möglich, Angaben über unbeteiligte Dritte, wie Anhänger und Mitläufer, zu sammeln. Alle erhobenen Daten können ohne weitere Prüfung aufbewahrt (gespeichert) werden. Eine Löschungsverpflichtung für personenbezogene Daten in Sachakten fehlt, so daß die Speicherung aller Informationen auf Dauer möglich ist. Der Umfang der zulässigerweise zu sammelnden Daten ist nicht näher bestimmt, obwohl es einen erheblichen Unterschied macht, lediglich Personengrunddaten, wie Name, Geburtsdatum und Anschrift, zu erfassen oder weitergehende Daten bis hinein in den privaten Bereich. Die vorhandenen Regelungen ermöglichen von Beginn an die Anfertigung zumindest partieller automatisierter Persönlichkeitsprofile. Unter Verkennung der tatsächlichen Abschottungssituation einer Verfassungsschutzbehörde wird eine allgemeine Zweckbindungsregelung der gewonnenen Daten für entbehrlich gehalten. Im Bereich der externen Zweckbindung (Datenübermittlungen) sind die Regelungen offen genug, unter den Sicherheitsbehörden kommunizieren zu können; jedenfalls erscheint es fast unmöglich, eine Datenübermittlung des Landesamtes an Dritte nicht für zulässig zu erachten.

— Mehr Landesverantwortlichkeit für die Daten seiner Bürgerinnen und Bürger.
Mangels näherer landesgesetzlicher Bestimmungen wird das Landesamt — schon zur Vermeidung einer Beeinträchtigung der Tätigkeit des Bundesamtes für Verfassungsschutz — vorhandene Informationen an die Bundesbehörde weitergeben. Die bundesgesetzlich vorgegebene Zusammenarbeitsverpflichtung aller Verfassungsschutzbehörden enthält jedoch Differenzierungsmöglichkeiten. So wird es dazu kommen, daß Unmengen auch von ungesicherten Daten und nicht gerichtsverwertbaren Informationen der bundesweiten Nutzung zugänglich werden.

Wenn auch das Niedersächsische Verfassungsschutzgesetz in einigen Punkten eigenständige Rechtsentwicklungen vorweist, so bleibt doch in der Sache (Aufgaben, Befugnisse, Zulässigkeit der Datenverarbeitung) festzustellen, daß es weitgehend dem Bundesverfassungsschutzgesetz angepaßt ist. Dies war erkennbar gewollt und beruht auf der verfassungsrechtlich verankerten Pflicht der Verfassungsschutzbehörden, untereinander zusammenzuarbeiten. Der Begriff der „Zusammenarbeit" hat entscheidende Bedeutung sowohl für den Bereich des Verfassungsschutzes wie für den Bereich der Polizei (dort geht es um die Aufgaben und Befugnisse des Bundeskriminalamtes). Im Bereich des Verfassungsschutzes findet die rechtliche Interpretation dieses zentralen Begriffs vorwiegend unter „Fachbrüdern" statt. Dies erinnert an Kommissionen, die damit beauftragt sind, DIN-Regeln zu entwickeln, die dann rechtlich zum „Stand der Technik" werden. Kommissionsmitglieder sind Fachleute der betroffenen Wirtschaftszweige. Ich halte eine Verbreiterung der rechtlichen Diskussion über den Begriff der „Zusammenarbeit" für tunlich — dies auch des-

halb, um nicht in naher Zukunft erkennen zu müssen, bei dem Landesamt für Verfassungsschutz handele es sich um eine Außenstelle des Bundesamtes.

Die Regelungen zur Zusammenarbeit führen datenschutzrechtlich zu Mehrfachspeicherungen. Z. B. könnten Datenübermittlungen, die dem Landesamt für Verfassungsschutz verwehrt wären, ggf. vom Bundesamt vorgenommen werden; über die Zusammenarbeit hätte ja das Bundesamt die Daten erhalten. Oder: Auf Anfrage beim (Wohnsitz) Landesamt für Verfassungsschutz erhält ein Betroffener die Auskunft, eine Speicherung personenbezogener Daten liege nicht vor. Die Auskunft ist korrekt. Ehemals vorhandene Informationen waren gelöscht. Der Betroffene erhält den Arbeitsplatz in einem anderen Bundesland trotzdem nicht, weil dort die Information des Bundesamtes vorgelegt worden ist, über den Betroffenen bestünden Hinweise auf „Bestrebungen".

Mit dem Niedersächsischen Verfassungsschutzgesetz vom 3. November 1992 (Nieders. GVBl. S. 283) sind nun die rechtlichen Rahmenbedingungen für die zukünftige Tätigkeit der Behörde gesetzt. Ich habe darauf aufmerksam gemacht, daß ein wesentlicher Faktor die Bediensteten des Landesamtes für Verfassungsschutz sind. Ihr verantwortlicher Umgang mit den eingeräumten Befugnissen wird ausschlaggebend dafür sein, ob der niedersächsische Verfassungsschutz ein „feiner" Verfassungsschutz ist.

14.2 Informationsverarbeitung über den Stellvertretenden Ministerpräsidenten in Sachsen-Anhalt

Der „Spiegel" hatte am 3. August 1992 berichtet, daß beim niedersächsischen Verfassungsschutz Informationen über den Stellvertretenden Ministerpräsidenten von Sachsen-Anhalt angefallen seien. Die Informationen habe der niedersächsische Dienst umgehend an das Kölner Bundesamt weitergeleitet. Der Präsident des Bundesamtes für Verfassungsschutz soll dann den Ministerpräsidenten des Landes Sachsen-Anhalt über die „Geheimdiensterkenntnisse" unterrichtet haben. Sofort nach Erscheinen des Artikels habe ich die den niedersächsischen Verfassungsschutz betreffenden Aspekte der Angelegenheit geprüft. Hinweise darauf, daß der niedersächsische Verfassungsschutz aktiv den Stellvertretenden Ministerpräsidenten Sachsen-Anhalts ausspioniert hat, habe ich nicht gefunden.

Meine datenschutzrechtliche Bewertung des Vorganges konnte ich noch nicht abschließen, weil zuvor bundesrechtliche Fragen zu klären sind. Ich habe deshalb Kontakt mit dem Bundesbeauftragten für den Datenschutz aufgenommen.

Nachdenklich muß eines stimmen: Der Vorgang beschreibt im Grunde die wundersame Wandlung eines Gerüchts in eine gleichsam „seriöse" Information — und das alles in einem sehr diffizilen Bereich. Das Rezept lautet wie folgt: Man nehme zunächst eine glaubwürdige Person. Das ist in diesem Fall ein Ex-Stasioffizier. Diese Person gibt — aus welchem Interesse auch immer — angebliches Wissen aus zweiter Hand (mit anderen Worten ein Gerücht) in die Kanäle der Geheimdienste, damit die Dinge zu einer „geheimdienstlichen Erkenntnis" reifen. Die Erkenntnis wiederum wandelt sich durch die Benutzung des Präsidenten des Bundesamtes für Verfassungsschutz zur offiziösen „Tatsache". Wie kann sich der Betroffene eigentlich dagegen wehren? Die Frage, wer wen instrumentalisiert, bleibt offen. Nach Darstellung des Bundesministers des Innern sind für das Ministerium für Staatssicherheit mindestens 209 000 Personen tätig gewesen (vgl. Verfassungsschutzbericht 1990, S. 170/171).

14.3 Extremisten im öffentlichen Dienst

Das Bundesamt für Verfassungsschutz (BfV) führt eine Datei über Extremisten im öffentlichen Dienst. Die Daten über Landes- und Kommunalbedienstete wurden durch die Landesämter für Verfassungsschutz übermittelt. Hierfür wurde ein Vordruck entwickelt, der neben den Personalien Angaben zum Dienstherrn, zum Dienstverhältnis, zur Dienstbezeichnung und zur Funktion der betroffenen Person enthält. Das BfV nutzt die Angaben in der Datei, um zahlenmäßige Übersichten über Extremisten im öffentlichen Dienst zu erstellen und zu veröffentlichen. Dabei wird nach Links- bzw. Rechtsextremisten, nach Beamten und Angestellten sowie nach Bediensteten in Bund, Land oder Kommunen unterschieden. Diese Statistik ist nach Darstellung des Niedersächsischen Innenministeriums kein Ausfluß des seinerzeitigen sog. Extremistenbeschlusses. Ich kann nicht erkennen, daß für die Zusammenstellung der Extremistenstatistik die Übermittlung von personenbezogenen Daten erforderlich ist. Eine Meldung in anonymisierter Form wäre ausreichend. Ein Anlaß zur Beanstandung besteht für mich nicht. Die niedersächsische Verfassungsschutzbehörde hat letztmalig für das Jahr 1990 ihre Meldung zur Arbeitsdatei über Extremisten im öffentlichen Dienst vorgenommen. Sämtliche in Niedersachsen hierzu angefallenen Unterlagen sind inzwischen vernichtet worden. Eine Fortsetzung des Meldeverfahrens ist nicht vorgesehen.

14.4 Sicherheitsüberprüfungen

Umfängliche Informationssammlungen entstehen bei Sicherheitsüberprüfungen. Solchen Überprüfungen unterliegen alle Personen, die eine sicherheitsempfindliche Tätigkeit ausüben. Dies ist der Fall, wenn man in lebens- oder verteidigungswichtigen Einrichtungen beschäftigt ist oder Kontakt zu im öffentlichen Interesse geheimhaltungsbedürftigen Unterlagen hat bzw. haben kann. Betroffen sind sowohl öffentliche Bedienstete als auch Beschäftigte in der Privatwirtschaft. Bei allen Sicherheitsüberprüfungsverfahren wirkt der Verfassungsschutz mit. Darüber hinaus ist er z. B. auch beteiligt im Einbürgerungsverfahren (vgl. VII 14.3). Ein neues Aktionsfeld hat sich durch die Wiedervereinigung im Hinblick auf eine frühere Mitarbeit bei der Stasi oder andere schuldhafte Verstrickungen mit dem SED-Unrechtsstaat ergeben.

Man gerät schnell in ein Sicherheitsüberprüfungsverfahren. Dies ist z. B. schon dann schon der Fall, wenn Betroffene aufgrund ihrer Tätigkeit sich Zugang zu offenen Informationen verschaffen können, die in ihrer Gesamtheit wiederum als vertraulich zu bewerten sind. Naturgemäß muß das Überprüfungsverfahren letztlich Feststellungen zur Zuverlässigkeit der überprüften Person treffen. Dies ist nur dann möglich, wenn zuvor die Person selbst, ggf. bis in den Bereich der Intimsphäre hinein, und ihr Umfeld überprüft werden. Zweifel an der Zuverlässigkeit können dann denknotwendigerweise nicht nur durch die überprüfte Person ausgelöst werden, sondern auch durch nahestehende Personen, wie Ehegatten oder Verlobte.

Es ist immer noch nicht bekannt, wieviel niedersächsische Bürgerinnen und Bürger von Sicherheitsüberprüfungen betroffen sind. Der Niedersächsische Verfassungsschutzbericht 1991 (Bericht) gibt die Anzahl der im NADIS (von den Verfassungsschutzbehörden des Bundes und der Länder gemeinsam genutztes elektronisches Hinweis- und Auskunftssystem) für Sicherheitsüberprüfungen gespeicherten niedersächsischen Aktenzeichen mit 24 300 an, bei 40 400 niedersächsischen Aktenzeichen insgesamt (Stand: 30. Juni 1992). Diese und weitere Angaben zu Sicherheitsüberprüfungen haben bisher in den jährlichen Verfassungsschutzberichten gefehlt. Ich begrüße die Neuerung als

einen ersten Schritt zu mehr Transparenz. Die Art der Darstellung mit „Aktenzeichen" darf jedoch nicht darüber hinwegtäuschen, daß aufgrund der Eingabe anderer Länder noch mehr niedersächsische Bürgerinnen und Bürger im NADIS gespeichert sein können. Auch sind nicht unmittelbar in das Sicherheitsüberprüfungsverfahren einbezogene Beteiligte, wie Auskunfts- und Referenzpersonen, in Akten des Verfassungsschutzes erfaßt. Bemerkenswert ist jedenfalls die Tatsache, daß im Rahmen einer Mitwirkungsaufgabe des Verfassungsschutzes mehr Personen vom niedersächsischen Verfassungsschutz gespeichert sind als im Zusammenhang mit der Extremismus/Terrorismusbeobachtung bzw. der Spionageabwehr. Nach dem Bericht enden Sicherheitsüberprüfungen ganz überwiegend mit dem Ergebnis „kein Sicherheitsrisiko".

Die bei Sicherheitsüberprüfungen gewonnenen, evtl. auch sehr sensiblen Informationen werden beim Verfassungsschutz in Sicherheitsüberprüfungsakten gesammelt. Die Nutzung der Informationen über die überprüften Personen zu allen Zwecken des Verfassungsschutzes ist prinzipiell möglich, ebenso die Verwendung zu Zwecken der straf- oder disziplinarrechtlichen Verfolgung. In den Sicherheitsakten der jeweiligen Einleitungsbehörde befinden sich die mehr technischen Unterlagen, wie Einleitung und Ergebnis des Sicherheitsüberprüfungsverfahrens. Die Sicherheitsakten werden getrennt von den Personalakten geführt. Im NADIS sind laut Bericht der Name und noch weitere zur Identifizierung erforderlichen Angaben gespeichert sowie das Aktenzeichen, aus dem sich die einspeichernde (aktenführende) Verfassungsschutzbehörde ergibt. Die Notwendigkeit der Einspeicherung im bundesweiten NADIS soll nach der Darstellung des Berichts überflüssige neue Überprüfungen bei Umzug, Stellenwechsel usw. ersparen.

Zur Bedeutung der Sicherheitsüberprüfungsakten noch der nachfolgende Hinweis: Es kann der Fall eintreten, daß eine Verfassungsschutzbehörde im Rahmen ihrer Mitwirkung in Überprüfungsverfahren Bedenken gegen die Ausübung einer sicherheitsempfindlichen Tätigkeit äußert. Dies kann im Bereich der Privatwirtschaft z. B. zur Ablehnung der Weiterbeschäftigung führen. Nun liegt es nahe, daß Betroffene wissen wollen, aufgrund welcher Informationen bzw. Bewertungen sie den Arbeitsplatz nicht erhalten bzw. verlieren. Die Chancen, offenbar belastendes Material einzusehen, stehen schlecht. Eine Verfassungsschutzbehörde kann sogar im gerichtlichen Verfahren einschlägige Aktenteile zurückbehalten. Die Behörde kann sich, gestützt auf § 99 VwGO, darauf berufen, es handele sich „um dem Wesen nach geheimhaltungsbedürftige Unterlagen" (vgl. VGH München, Beschluß v. 12. Februar 1990, DÖV 1990, 530 f.).

14.5 Sicherheitsüberprüfungsgesetz

Sicherheitsüberprüfungen können gravierende Eingriffe in das Recht auf informationelle Selbstbestimmung zur Folge haben. Um so erstaunlicher ist es, daß diese Verfahren bisher weithin gesetzlich nicht geregelt sind. Das am 21. November 1992 in Kraft getretene Niedersächsische Verfassungsschutzgesetz enthält zwar einige Aussagen zu Sicherheitsüberprüfungen, wie z. B. bei der Aufgabenbeschreibung (Mitwirkung an Überprüfung) oder durch Ausschluß der Anwendung nachrichtendienstlicher Mittel. Dies ändert aber nichts daran, daß präzise Regelungen zur gesamten Ausgestaltung des Verfahrens nach wie vor fehlen. Für Beamte soll jedoch die beamtenrechtliche Vorschrift über die Verantwortlichkeit der Beamten (§ 63 NBG) genügen, die zur Sicherheitsüberprüfung geeigneten und erforderlichen Angaben zu verlangen (vgl. BVerfG, Beschluß v. 10. Februar 1982, DVBl. 1988, 530 f.). Derzeit regeln im wesentlichen vielfältige interne Verwaltungsvorschriften die Ausgestaltung des Überprüfungsverfahrens. Bei der Datenverarbeitung ohne gesetzliche

Grundlage verweist die Exekutive auf den vom Bundesverfassungsgericht eingeräumten sog. „Übergangsbonus". Unter Berufung auf diesen Bonus gelten für die eingangs beschriebene Kontaktsituation bei öffentlich Bediensteten Niedersachens die vom Landesministerium beschlossenen „Niedersächsischen Sicherheitsrichtlinien" vom 1. Dezember 1989 (Nds. MBl. S. 1171 ff., vgl. IX 15.13 u. X 15.6). Für Beschäftigte in der Privatwirtschaft gilt das vom Bundesminister für Wirtschaft mit Wirkung vom 1. August 1986 erlassene „Geheimschutzhandbuch". Bestimmungen zum Bereich „Beschäftigung in lebens- oder verteidigungsnotwendigen Einrichtungen" finden sich in einem Beschluß der Innenministerkonferenz des Bundes und der Länder vom 13. Juni 1984, speziell für den atomrechtlichen Bereich in der „Richtlinie für die Sicherheitsüberprüfungen von Personal in kerntechnischen Anlagen, bei der Beförderung und Verwendung von Kernbrennstoffen" (GMBl. 1987, S. 337; vgl. IX 15.13). Für den Personenkreis „Flughafenpersonal" beabsichtigt der Bund, eine Rechtsverordnung zu erlassen (vgl. 14.7).

Ich habe seit Jahren, ebenso wie die anderen Datenschutzbeauftragten des Bundes und der Länder, ein bereichsspezifisches Sicherheitsüberprüfungsgesetz gefordert und datenschutzrechtliche Vorstellungen dazu entwickelt (vgl. VII Anlage 7 und Anlage 4 in diesem Tätigkeitsbericht). Der Gesetzgeber und nicht die Verwaltung ist aufgefordert, z. B. folgende Punkte zu regeln: den betroffenen Personenkreis, den Umfang der unerläßlichen Datenerhebungen, die Voraussetzungen für das Vorliegen eines Sicherheitsrisikos und die grundsätzliche Zweckbindung der gewonnenen Daten auf das Sicherheitsüberprüfungsverfahren.

Die Landesregierung hat sich nunmehr meiner Forderung nach einem bereichsspezifischen Sicherheitsüberprüfungsgesetz angeschlossen. Leitlinie soll der Regierungsentwurf des Bundes sein, da in Niedersachsen Angehörige des öffentlichen Dienstes vielfach Zugang zu geheimhaltungsbedürftigen Unterlagen des Bundes haben. Ein Regierungsentwurf des Bundes liegt nach wie vor nicht vor. Entwürfe werden beim Bund aufgrund eines Auftrages des Deutschen Bundestages vom 19. September 1990 diskutiert. Ich habe angesichts dieser Situation beim Niedersächsischen Innenministerium auf die zügige Erstellung eines eigenen Sicherheitsüberprüfungsgesetzes gedrungen. Dies auch deshalb, weil es in Niedersachsen bezüglich der Rechtmäßigkeit und Intensität von Sicherheitsüberprüfungen erhebliche Unruhe im staatlichen und im kommunalen Bereich gibt. Der Innenminister hat verlautbaren lassen, daß er ein eigenes Gesetzgebungsvorhaben vorantreiben werde, wenn die Verabschiedung eines Bundesgesetzes in absehbarer Zeit nicht möglich sei (vgl. Pressemitteilung Nr. 331/91 vom 10. Dezember 1991).

14.6 Niedersächsische Sicherheitsrichtlinien

Die unter 14.5 angesprochenen Niedersächsischen Sicherheitsrichtlinien hatten in § 12 Abs. 1 bisher vorgesehen, Überprüfungsverfahren mit Kenntnis der betroffenen Person und der einzubeziehenden Person (z.B. Ehegatte) durchzuführen. Auf die Frage, ob die Betroffenen mit dem Verfahren überhaupt einverstanden sind, kam es nicht an. Diese Vorgehensweise ist schon vor Inkrafttreten des neugefaßten Niedersächsischen Verfassungsschutzgesetzes aus rechtsstaatlichen Erwägungen geändert worden. Das Verfahren wurde von der Einwilligung z. B. der Ehepartnerin bzw. des Ehepartners und in bestimmten Fällen auch der bzw. des zu überprüfenden Bediensteten abhängig gemacht (vgl. RdErl. des Niedersächsischen Innenministeriums vom 29. Mai 1992, Nds. MBl. S. 890). Das nunmehr geltende Verfassungsschutzgesetz enthält entsprechende Bestimmungen. Ich habe die teilweise Umsetzung der

alten datenschutzrechtlichen Forderung nach der Einwilligung des Betroffenen bzw. der einbezogenen Person begrüßt. Die „Kenntnis" des Betroffenen von der Einleitung des Verfahrens in Fällen der Auswertung bereits vorhandenen Wissens halte ich nach wie vor nicht für ausreichend. Die Auswertung vorhandenen Wissens setzt die Weitergabe personenbezogener Daten durch Dritte an den Verfassungsschutz voraus. Datenschutzrechtlich liegt damit eine Übermittlung vor, mithin ein Eingriff in das durch Art. 2 Satz 1 GG i.V.m. Art. 1 Abs. 1 GG geschützte Recht auf informationelle Selbstbestimmung. Mangels Rechtsgrundlage — ein Sicherheitsüberprüfungsgesetz fehlt — ist die Weitergabe personenbezogener Daten nur mit Einwilligung des Betroffenen zulässig. Das Innenministerium schließt in seiner Stellungnahme nicht aus, auch diesen Fall im Sicherheitsüberprüfungsgesetz entsprechend meinen Vorstellungen zu verwirklichen.

14.7 Zuverlässigkeitsüberprüfung von Flughafenpersonal

Personen, die Zugang zu sicherheitsempfindlichen Bereichen auf Flughäfen haben, werden auf ihre Zuverlässigkeit überprüft. Der Bundesgesetzgeber hat für das Überprüfungsverfahren durch Änderung des Luftverkehrsgesetzes zum 1. April 1992 eine bereichsspezifische Rechtsgrundlage geschaffen. Nähere Bestimmungen will der Bundesminister für Verkehr in einer Verordnung regeln. Der Verordnungsentwurf sieht folgendes Verfahren vor:

Die Überprüfung der Zuverlässigkeit von Bewerberinnen und Bewerbern sowie Beschäftigten auf Arbeitsplätzen im sicherheitsempfindlichen Bereich der Flughäfen wird von der Luftfahrtbehörde, das ist in Niedersachsen das Ministerium für Wirtschaft, Technologie und Verkehr, gesteuert. Die Entscheidungsgrundlagen sollen von den Flugplatz- und Luftfahrtunternehmen, den Polizei- und den Verfassungsschutzbehörden übermittelt werden. Ggf. können auch bei anderen öffentlichen oder auch privaten Stellen Informationen eingeholt werden. Bei erstmaliger Überprüfung ist für die Durchführung des Verfahrens die Zustimmung der Betroffenen erforderlich. Bei der Überprüfung bereits zugangsberechtigter Personen bzw. bei Wiederholungsprüfungen reicht nach dem Luftverkehrsgesetz die Kenntnis der Betroffenen aus. Wenn Zweifel an der Zuverlässigkeit bestehen, wird den Flugplatz- und Luftfahrtunternehmen nach Anhörung der oder des Betroffenen dieses Ergebnis mitgeteilt. Die maßgeblichen Gründe dürfen den Unternehmen mitgeteilt werden, wenn es zur Durchführung von gerichtlichen Verfahren erforderlich ist. Die Betroffenen werden über das Ergebnis der Überprüfung durch das Flugplatz- oder Luftfahrtunternehmen unterrichtet.

Ich habe in meiner Stellungnahme zum Verordnungsentwurf umfangreiche datenschutzrechtliche Bedenken geltend gemacht.

Die Zuverlässigkeitsüberprüfung, die verfahrensrechtlich an die Sicherheitsüberprüfung für öffentliche Bedienstete angelehnt ist, greift in das Recht auf informationelle Selbstbestimmung bei einer Vielzahl von Personen ein. Für den Flughafen Hannover-Langenhagen bedeutet die Regelung, daß bei 4 500 Beschäftigten ca. 3 000 Erst-Überprüfungen pro Jahr durchgeführt werden (Fremdfirmen eingeschlossen). Diese Zahl führt zu der Forderung, nur die Personen zu überprüfen, bei denen dies aus Gründen der Sicherheit des Luftverkehrs unerläßlich ist.

Der Katalog der von den (zukünftigen) Arbeitgebern an die Luftfahrtbehörde zu übermittelnden Daten ist auf den erforderlichen Umfang zu beschränken. Die Aufforderung an die Flugplatz- und Luftfahrtunternehmen, auch bedeutsame Informationen über Sachverhalte mitzuteilen, die die Zuverlässigkeit in

Frage stellen können, ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Nach dem Verordnungsentwurf kommen hier alle Sachverhalte in Betracht, aus denen sich eine Erpreßbarkeit durch Dritte ergibt. Ich habe die Befürchtung, daß angesichts dieser nicht normenklaren Regelung alle negativen Informationen über die Betroffenen übermittelt werden.

Um zu verhindern, daß zweifelhafte, ungesicherte und nicht nachprüfbare Informationen verwertet werden, ist in der Verordnung festzuschreiben, daß durch die Polizei- und die Verfassungsschutzbehörden nur gerichtsverwertbare Daten übermittelt werden. In der Verordnung ist abschließend zu regeln, mit welchen Dateien die Polizei- und die Verfassungsschutzbehörden die personenbezogenen Daten der Betroffenen abgleichen dürfen. Dateien, in denen Daten schon aufgrund erster ungesicherter Anhaltspunkte gespeichert werden — wie z. B. die polizeilichen Staatsschutzdateien —, dürfen in dem Überprüfungsverfahren nicht herangezogen werden.

Die Beteiligung von Polizei- und Verfassungsschutzbehörden darf nicht dazu führen, daß über die Betroffenen neue Datensammlungen angelegt werden. Die Betroffenen sollten davor geschützt werden, daß ihre Daten für Zwecke außerhalb des Überprüfungsverfahrens genutzt werden.

Die Weitergabe von Verdachtsdaten nach Einstellung eines förmlichen Verfahrens, das den angestrebten Beweis gerade nicht erbracht hat, ist als unverhältnismäßiger Eingriff in das Recht auf informationelle Selbstbestimmung anzusehen. Informationen aus eingestellten Verfahren dürfen deshalb nicht an die Luftfahrtbehörden übermittelt werden.

Die Regelung über die Aufzählung von Erkenntnissen, die im Ergebnis Sicherheitsbedenken begründen sollen, ist normenklar auszugestalten. Die Entwurfsregelung eröffnet die Möglichkeit, alle denkbaren, für die Betroffenen nachteiligen Erkenntnisse zum Anlaß von Übermittlungen bzw. als Entscheidungsgrundlage zu nehmen.

Es leuchtet nicht ein, daß den Flugplatz- und Luftfahrtunternehmen die Gründe für Sicherheitsbedenken mitgeteilt werden dürfen, die Betroffenen aber nur eine Information über das Ergebnis der Prüfung erhalten.

Der Verordnungsentwurf regelt nicht, welche Möglichkeiten der Speicherung von personenbezogenen Daten in diesen Verfahren bestehen sollen. Ich halte differenzierende Bestimmungen über Speicherungen in Akten oder Dateien für notwendig. Offenbleibt in dem Entwurf auch, wie die Berichtigung, Sperrung und Löschung der im Rahmen der Zuverlässigkeitsüberprüfung angefallenen Daten sowie das Auskunftsrecht der Betroffenen gehandhabt werden sollen. Bei Personen, denen der Zugang zu den sicherheitsempfindlichen Bereichen verweigert wird, sehe ich eine Erforderlichkeit, Daten nach Abschluß des Verfahrens bei der Luftfahrtbehörde vorzuhalten, nicht. Im übrigen sind die Daten spätestens zu löschen, wenn eine Beschäftigung der betroffenen Person im sicherheitsempfindlichen Bereich nicht mehr vorgesehen ist.

14.8 Zusammenarbeit zwischen dem Verfassungsschutz und Privatfirmen

Der Verfassungsschutzbehörde eines anderen Bundeslandes wurde in Presseberichten vorgeworfen, personenbezogene Daten über Arbeitnehmerüberprüfungen unzulässigerweise an deren Arbeitgeber weitergegeben zu haben. Ich habe bei der niedersächsischen Verfassungsschutzbehörde Datenübermittlungen an Privatfirmen hinterfragt.

Nach der Antwort des Innenministeriums erfolgt eine direkte Datenübermittlung der niedersächsischen Verfassungsschutzbehörde an Privatfirmen nicht. Personen aus der Privatwirtschaft, die Zugang zu geheimhaltungsbedürftigen Verschlußsachen erhalten sollen, werden durch die Verfassungsschutzbehörde überprüft. Die Sicherheitsüberprüfung darf nur durchgeführt werden, wenn die betroffene Person vor Einleitung des Verfahrens schriftlich ihre Einwilligung gegeben hat. Die Verfassungsschutzbehörde teilt das Ergebnis der Überprüfung der für die Erteilung der Verschlußsachenermächtigung zuständigen Landesbehörde mit. Liegen Erkenntnisse vor, die ein Sicherheitsrisiko begründen und einer Verschlußsachenermächtigung entgegenstehen, erhält die überprüfte Person im Wege der Anhörung Gelegenheit, die Bedenken auszuräumen. Gegebenenfalls wird ein schriftlicher Ablehnungsbescheid an die betroffene Person gefertigt. Der Arbeitgeber wird in diesem Fall über das Ergebnis der Sicherheitsüberprüfung informiert. Gründe werden nicht mitgeteilt.

Ich begrüße, daß die frühere Praxis, auf der Grundlage des § 3 Abs. 2 Nr. 2 des Niedersächsischen Verfassungsschutzgesetzes a. F. einen Informationsaustausch zwischen der Verfassungsschutzbehörde und den Privatfirmen vorzunehmen, seit 1989 eingestellt worden ist. Die niedersächsische Verfassungsschutzbehörde hat die bei dieser Zusammenarbeit gewonnenen Daten inzwischen gelöscht.

15. Personalwesen

15.1 Bereichsspezifische Regelungen für Beamte

Aus datenschutzrechtlicher Sicht ist zu begrüßen, daß der Bundesgesetzgeber nunmehr für einen Teilbereich des öffentlichen Dienstrechts, das Personalaktenrecht, bereichsspezifische Regelungen im Beamtenrechtsrahmengesetz (BRRG) und im Bundesbeamtengesetz geschaffen hat. Das Neunte Gesetz zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 (BGBl. I S. 1030) ist am 1. Januar 1993 in Kraft getreten. In den Vorschriften haben eine Reihe von Forderungen der Datenschutzbeauftragten des Bundes und der Länder Berücksichtigung gefunden. Gleichwohl besteht noch ein langer Forderungskatalog, der sich in den Beschlüssen der Konferenz der Datenschutzbeauftragten zum Recht des öffentlichen Dienstes (vgl. Anlage 4) und zum Arbeitnehmerdatenschutz (vgl. Anlage 5) widerspiegelt. Ich hoffe, daß die Vorschriften des BRRG zügig in niedersächsisches Landesrecht umgesetzt werden.

Das Niedersächsische Innenministerium beabsichtigt, mit einem Gemeinsamen Runderlaß detaillierte Verwaltungsvorschriften zum Niedersächsischen Beamtengesetz (VV) zu erlassen, die — wie ich positiv feststellen kann — im großen und ganzen datenschutzfreundlich ausgestaltet sind. Ich habe zu dem mir vorgelegten Entwurf Stellung bezogen und möchte an dieser Stelle einige Anmerkungen wiedergeben.

Der VV-Entwurf sah zunächst vor, in jedem Bewerbungsfall ausnahmslos eine Erklärung über die wirtschaftlichen Verhältnisse von der Bewerberin oder dem Bewerber abzufordern. Dies halte ich für bedenklich. Zunächst ist der Begriff der „geordneten wirtschaftlichen Verhältnisse" relativ unbestimmt. Deshalb dürfte es kaum möglich sein, aus einer unzutreffenden Angabe für die Bewerberin oder den Bewerber nachteilige Folgen herzuleiten. Zudem sind die wirt-

schaftlichen Verhältnisse je nach dienstlichem Aufgabenbereich von unterschiedlicher Bedeutung. Ich habe deshalb folgende Formulierung vorgeschlagen:

„Falls die vorgesehene Verwendung es erfordert, kann von der Bewerberin oder dem Bewerber eine Erklärung verlangt werden, daß ihre oder seine wirtschaftlichen Verhältnisse geordnet sind."

Die Aussage im Entwurf, die Bewerberin oder der Bewerber sei „möglichst frühzeitig" aufzufordern, bei der Meldebehörde ein Führungszeugnis zu beantragen, könnte dahin verstanden werden, daß von jeder Bewerberin und jedem Bewerber ein Führungszeugnis verlangt wird. Dies wäre mit dem Grundsatz, daß eine Datenerhebung zur Aufgabenerfüllung erforderlich sein muß, nicht vereinbar. Nur wenn eine Einstellung in Betracht gezogen wird, d. h. nach der Vorauswahl, kann die Vorlage eines Führungszeugnisses gefordert werden.

Nach dem Entwurf sollte es der obersten Landesbehörde freigestellt sein, im Bewerbungsfall unbeschränkte Auskünfte über strafgerichtliche Verurteilungen aus dem Bundeszentralregister nach § 41 BZRG einzuholen. Diese Auskünfte enthalten auch Angaben über bereits getilgte Verurteilungen, über Maßregeln der Besserung und Sicherung und ähnliches. Ich vertrete die Auffassung, daß diese Angaben im Regelfall zur Prüfung der Einstellungsvoraussetzungen nicht erforderlich sind. Anderenfalls hätte der Gesetzgeber ein unbeschränktes Auskunftsrecht auch für die Gemeinden und die Landkreise sowie andere Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts geschaffen. Aus Sicht des Datenschutzes muß die Anforderung unbeschränkter Zentralregisterauskünfte regelmäßig unterbleiben. Nur in besonderen Fällen kann eine unbeschränkte Auskunft in Betracht kommen. Um eine gleichmäßige Verwaltungsübung zu gewährleisten, habe ich dem Innenministerium vorgeschlagen, in der Verwaltungsvorschrift zumindest beispielhaft einschlägige Fallgruppen zu nennen.

Von Bewerberinnen und Bewerbern soll eine Erklärung über anhängige Strafverfahren oder Ermittlungsverfahren gefordert werden. Dies darf nach meinem Dafürhalten nur von Personen erfolgen, die zur Einstellung vorgesehen sind. Anderenfalls würden Bewerberdaten im Übermaß erhoben werden.

Da Führungszeugnisse und unbeschränkte Auskünfte aus dem Bundeszentralregister ähnlich sensible Daten enthalten können wie ärztliche Gutachten über den Gesundheitszustand, habe ich gebeten, auch für sie die Aufbewahrung in einem verschlossenen Umschlag vorzusehen: „Dieser darf außer bei einer Einsichtnahme durch die Beamtin oder den Beamten oder von diesen Beauftragte nur geöffnet werden, wenn eine Personalangelegenheit die Einsichtnahme erfordert; Anlaß und Datum der Einsichtnahme sind auf dem Umschlag zu vermerken."

Zu kritisieren ist, daß der Erlaßentwurf auf den Vordruck eines Personalbogens verweist, der Daten enthält (Zeitpunkt der Eheschließung, der Scheidung, der Aufhebung der ehelichen Gemeinschaft), bei denen nicht ersichtlich ist, aus welchen Gründen sie festgehalten werden müssen.

Ich habe vorgeschlagen, die Versendung von Personalakten auch innerhalb der Behörde nur verschlossen zuzulassen. Hiervon können Ausnahmen nicht in Betracht kommen. Eine Weitergabe der nicht verschlossenen Akte von Hand zu Hand bleibt allerdings möglich.

Im Entwurf war vorgesehen, eine Einsichtnahme in ärztliche Zeugnisse und Gutachten aus Gründen der Fürsorge vorzuenthalten, wenn dies zwingend geboten erscheint. Ich habe empfohlen, am Grundsatz der Einsichtnahme festzuhalten und die Ausnahme zu streichen. Ich halte es für problematisch, der Beamtin oder dem Beamten aus Fürsorgegesichtspunkten die Einsichtnahme in ärztliche Zeugnisse und Gutachten zu verwehren. Das BRRG sieht eine solche Einschränkung des Akteneinsichtsrechts nicht vor. Sofern Bedienstete darauf beharren, den Inhalt einer — wenn auch für sie nachteiligen — ärztlichen Stellungnahme zu erfahren, sollte ihnen zumindest entsprechende Auskunft erteilt werden. Ich habe in diesem Zusammenhang auf die Regelung des § 25 SGB X hingewiesen.

Es ist eine alte Forderung des Datenschutzes (vgl. Anlage 4), Beihilfevorgänge und Abrechnungsunterlagen der Heilfürsorge und Heilverfahren in einer von der übrigen Personalverwaltung getrennten Organisationseinheit zu bearbeiten. § 56 a BRRG enthält allerdings insoweit nur eine Sollvorschrift. Nach der Gesetzesbegründung soll damit Problemen Rechnung getragen werden, auf die eine organisatorische Trennung in kleinen Dienststellen stößt. Wie eine Umfrage des Niedersächsischen Innenministeriums ergeben hat, sehen auch einige oberste Landesbehörden Schwierigkeiten im Falle einer strikten Abschottung der Beihilfebearbeitung. Soweit zur Begründung allerdings nur pauschal darauf verwiesen wird, eine Trennung zwischen Beihilfe- und Personalbearbeitung sei organisatorisch nicht zweckmäßig, muß ich betonen, daß dieser Gesichtspunkt nicht ausreicht, um eine Ausnahme vom grundsätzlichen Trennungsgebot zu rechtfertigen.

15.2 Entwurf eines Landesgleichberechtigungsgesetzes

Das Niedersächsische Frauenministerium hat mir einen Referentenentwurf eines Gesetzes zur Herstellung der beruflichen Gleichberechtigung von Frauen im öffentlichen Dienst in Niedersachsen (Landesgleichberechtigungsgesetz — LGG) vorgelegt.

Ich habe in meiner Stellungnahme darauf hingewiesen, daß die vorgesehene Regelung, wonach „Fähigkeiten aus der familiären oder sozialen Arbeit" für die Eignung bedeutsam sind, dazu führen kann, daß im Auswahlverfahren entsprechende Fragen gestellt werden. Der Umfang der Datenerhebung und weiteren Verarbeitung im Personalbereich dürfte damit zunehmen. Um zu vermeiden, daß dieser Auswahlgesichtspunkt dazu führt, familiäre Verhältnisse im Detail offenzulegen, sollte klargestellt werden, daß die genannten Kriterien eine derartige Ausforschung nicht rechtfertigen.

Der Entwurf sieht vor, die Frauenbeauftragte einer Behörde an allen personellen, sozialen und organisatorischen Maßnahmen, die Belange der weiblichen Beschäftigten berühren können, rechtzeitig zu beteiligen. Ich halte eine Klarstellung für erforderlich, ob das Beteiligungsrecht auch dann bestehen soll (z. B. bezüglich einer Teilnahme an Bewerbungsgesprächen), wenn im Einzelfall ausschließlich männliche Bewerber für die Auswahlentscheidung zur Verfügung stehen. Weiter habe ich angeregt, ausdrücklich zu regeln, daß die Frauenbeauftragte Einsicht in Bewerbungsunterlagen erhält. Eine Einsicht in Personalakten kann dagegen nur mit Zustimmung der betreffenden Bediensteten in Betracht kommen (vgl. 16.3). Außerdem muß betont werden, daß die Frauenbeauftragte nur die personenbezogenen Daten verarbeiten darf, die für ihre Aufgabenerfüllung erforderlich sind.

Ein weiterhin im Gesetzentwurf vorgesehener dienststellenübergreifender Informationsaustausch zwischen Frauenbeauftragten dürfte im allgemeinen keine Übermittlung personenbezogener Daten erfordern. Sofern diese im Einzelfall aber doch erforderlich sein sollte, sollte sie von der Zustimmung der Betroffenen abhängig gemacht werden. Anderenfalls bestünde die Gefahr, daß Frauenbeauftragte umfangreiche Datensammlungen über Bedienstete anderer Behörden anlegen.

Im Hinblick auf die Verschwiegenheitspflicht kann für die Frauenbeauftragte nichts anderes gelten als für die Mitglieder des Personalrats (vgl. § 69 Nds. PersVG). Ich habe deshalb gebeten, den Gesetzentwurf um eine entsprechende Regelung zu ergänzen.

Auch im Zusammenhang mit dem Entwurf eines Erlasses zur „Stellung und Zuständigkeit der Ressortbeauftragten für Frauenfragen" in den obersten Landesbehörden habe ich auf den Vorbehalt der Zustimmung der Betroffenen vor Einsichtnahme in deren Personalakte hingewiesen. Das Niedersächsische Innenministerium hat diesem Gesichtspunkt in seinem Erlaß über die Beauftragten für Frauenfragen in der Polizei Rechnung getragen.

15.3 Mißbrauch einer Uraltpersonalakte

Welche Versuchung zum Mißbrauch noch von einer uralten Personalakte ausgehen kann, zeigt folgender Fall:

Im Jahre 1946 war ein Bürger für wenige Wochen als Aushilfsangestellter bei einer südniedersächsischen Stadt tätig. Vor der Einstellung hatte er — wie damals gefordert — in einem Fragebogen der Alliierten Militärregierung Angaben zu seiner politischen Vergangenheit machen müssen.

Jahrzehnte später engagierte sich dieser Bürger, der inzwischen sein Berufsleben bei einem anderen Dienstherrn längst hinter sich gebracht hatte, in der Kommunalpolitik seiner Stadt. Er wurde in den Rat gewählt und trat sowohl gegenüber der Stadt als auch in der Öffentlichkeit vielfach in Erscheinung. Diese Aktivitäten brachten ihm nicht nur Freunde und Beifall ein.

1990 äußerten einige Bürger gegenüber der Stadt den Verdacht, der Betroffene habe sich im Dritten Reich für die NSDAP engagiert. Außerdem wurden Zweifel am Führen eines Ingenieurtitels geäußert.

Flugs entsann man sich bei der Stadt der alten, immer noch vorhandenen Personalakte. Man belebte den Vorgang, holte Erkundigungen über etwaige frühere Mitgliedschaften und Funktionen des ehemaligen Angestellten in der NSDAP und ihren Gliederungen ein und prüfte, ob dieser einen ordentlichen Fachhochschulabschluß vorweisen konnte. Hierbei anfallender Schriftwechsel wurde zur Personalakte genommen.

Zur Begründung dieses ungewöhnlichen Verhaltens erklärte die Stadt, sie bewahre Personalakten auf Dauer auf. Ihr ehemaliger Angestellter sei vor allem wegen seines — inzwischen längst beendeten — kommunalpolitischen Engagements als Person der Zeitgeschichte anzusehen. Deshalb sei die vorgenommene Sachaufklärung notwendig gewesen.

Die Stadt ist der Meinung, daß auch Jahrzehnte nach dem Ende eines Beschäftigungsverhältnisses Angaben in den Personalakten überprüft werden müßten, wenn Anhaltspunkte für Zweifel an deren Richtigkeit bestünden. Denn

es könne „ja wohl nicht angehen, daß Akten mit wahrheitswidrigem Inhalt auf Dauer aufbewahrt werden". Nach dieser Auffassung hört die Arbeit an einer Personalakte offenbar niemals auf.

Der Fall, der hier nicht in allen seinen Verästelungen geschildert werden kann, macht grundsätzliche Probleme des Personalaktenrechts deutlich.

Die Aufbewahrung von Personalakten der Arbeitnehmer im öffentlichen Dienst ist bisher durch Rechtsvorschriften nicht geregelt. Die vom Land erlassenen Richtlinien über die Führung von Personalakten (Gem.RdErl. des Innenministeriums und der übrigen Ministerien vom 27.09.1969, Nds. MBl. S. 998, zuletzt geändert durch Gem.RdErl. vom 31. Oktober 1990, Nds. MBl. S. 1325) sehen eine grundsätzliche Aufbewahrungsfrist von fünf Jahren vor. Sie beginnt mit Ablauf des Jahres, in dem der ausgeschiedene Bedienstete das 65. Lebensjahr vollendet hat. Für Kommunen enthalten diese Richtlinien keine Bindungswirkung; ihnen ist die Anwendung lediglich nahegelegt worden.

Dies heißt allerdings nicht, daß Personalakten kommunaler Angestellter ohne jede zeitliche Begrenzung aufbewahrt und genutzt werden dürfen. Die Aufbewahrung solcher Vorgänge berührt das informationelle Selbstbestimmungsrecht der Betroffenen. Dieses wird beeinträchtigt, wenn ein Arbeitgeber Daten eines Arbeitnehmers auf Dauer speichert (vgl. BAG, Urt. vom 6. Juni 1984, Der Betrieb 1984, 2626, 2628). Das Bundesarbeitsgericht geht davon aus, daß in derartigen Fällen eine Abwägung zwischen dem Interesse des Arbeitgebers an der Aufbewahrung und den Interessen der Arbeitnehmerin bzw. des Arbeitnehmers am Schutz der Privatsphäre vorzunehmen ist. Liegt ein berechtigtes Interesse des Arbeitgebers an einer weiteren Datenspeicherung nicht (mehr) vor, muß der Datenträger vernichtet werden.

Zweck der Personalakte ist es, zur Abwicklung des Beschäftigungsverhältnisses alle Vorgänge zusammenzufassen, die die dienstlichen und persönlichen Verhältnisse einer Arbeitnehmerin bzw. eines Arbeitnehmers betreffen und in einem inneren Zusammenhang mit dem Arbeitsverhältnis stehen. Auch nach Beendigung des Arbeitsverhältnisses ist eine Vernichtung der Personalakte rechtlich nicht ohne weiteres geboten. Unterlagen aus der Akte können noch für vielfältige, mit dem ehemaligen Arbeitsverhältnis zusammenhängende Zwecke, etwa im Hinblick auf Sozialversicherungsrechte oder Versorgungsansprüche, benötigt werden. Wenn jedoch — wie hier — Jahrzehnte nach dem Ende des Beschäftigungsverhältnisses derartige Zwecke keinerlei Rolle mehr spielen können, besteht kein anzuerkennendes Interesse des Arbeitgebers, die Personalakte weiter aufzubewahren. Eine solche Aufbewahrung kann auch nicht auf Zwecke gestützt werden, die mit dem früheren Beschäftigungsverhältnis in keinerlei Zusammenhang stehen (wie hier der vorgebrachte Gesichtspunkt, der Betreffende sei eine Person der Zeitgeschichte).

Ebenso verbietet es die Funktion der Personalakte, sie für beschäftigungsfremde Zwecke zu nutzen. Die Verwendung des Personalvorgangs zu Nachforschungen über die politische Vergangenheit des früheren Angestellten und über seine Berechtigung, einen Fachhochschulgrad zu führen, ist deshalb rechtswidrig, weil sie keinen Bezug zum früheren Beschäftigungsverhältnis mehr aufweist und arbeitsrechtliche Maßnahmen irgendwelcher Art von vornherein nicht in Betracht kommen können.

Ich habe das Niedersächsische Innenministerium aufgefordert, im Zuge der landesrechtlichen Umsetzung der Vorschriften des BRRG (vgl. 15.1) hinsichtlich der Aufbewahrungsdauer von Personalakten eine datenschutzgerechte Regelung zu treffen. Besonders in Fällen, in denen nur eine kurzfristige Beschäftigung in jungen Lebensjahren erfolgt, erscheint mir die derzeitige regelmäßige Aufbewahrung bis zum 70. Lebensjahr des ehemaligen Bediensteten nicht

vertretbar. Anstelle eines Erlasses ist aus meiner Sicht eine gesetzliche Regelung unabdingbar, um eine einheitliche Verfahrensweise im unmittelbaren und mittelbaren Landesbereich sicherzustellen.

15.4 Beihilfe

Unter X 15.18 hatte ich mich ausführlich mit datenschutzrechtlichen Problemen bei der Bearbeitung von Beihilfeanträgen befaßt. Die Forderungen der Datenschutzbeauftragten zur Schaffung gesetzlicher Grundlagen für ein datenschutzgerechtes Beihilfeverfahren (vgl. Entschließung der 42. Konferenz am 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes — Anlage 4) wurden vom Gesetzgeber bisher nur teilweise aufgegriffen. So wurde im Rahmen des 9. Gesetzes zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 (Art. 2, § 56 a BRRG) geregelt, daß Unterlagen über Beihilfen als Teilakte zu führen sind. Diese ist von der übrigen Personalakte getrennt aufzubewahren. Sie soll in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet werden. Damit ist der Forderung nach einer strikten Trennung der Beihilfe- und Personalsachbearbeitung noch nicht vollständig entsprochen worden. Zu begrüßen ist aber, daß in dieser Vorschrift eine Zweckbindungsregelung für die Beihilfeakte getroffen worden ist.

Auf Landesebene ist es als erfreulicher Erfolg anzusehen, daß das Niedersächsische Finanzministerium auf meine Anregung hin einen Entwurf für einen Gemeinsamen Runderlaß des Finanzministeriums und der übrigen obersten Landesbehörden zur Durchführung des § 17 Abs. 4 der Beihilfevorschriften erarbeitet hat. Danach ist vorgesehen, daß Beihilfeanträge in verschlossenem Umschlag den Beihilfestellen unmittelbar zuzuleiten sind. Nur diese sind künftig befugt, als Beihilfeangelegenheit gekennzeichnete Eingänge zu öffnen und mit einem Eingangsstempel zu versehen.

Der Erlaß soll den Gemeinden und Landkreisen sowie den der Aufsicht des Landes unterstehenden anderen Körperschaften, Anstalten und Stiftungen des öffentlichen Rechts zur Anwendung empfohlen werden — die Veröffentlichung im Niedersächsischen Ministerialblatt ist für Januar 1993 vorgesehen.

15.5 Übersendung von Personalakten an Verwaltungsgerichte

Mehrfach haben Petenten Kritik an der nach ihrer Ansicht unnötigen Vorlage von Personalakten bei Verwaltungsgerichten geübt (vgl. auch 20.12). Besondere Bedeutung erhält dieses Problem im Zusammenhang mit der Zunahme der sog. Konkurrentenklagen, mit denen unterlegene Bewerberinnen oder Bewerber die Besetzung eines Dienstpostens mit der ausgewählten Person zu verhindern suchen. Die Personalreferentinnen und -referenten der obersten Landesbehörden haben sich deshalb an mich gewandt. Nach ihrer Darstellung fordern die Verwaltungsgerichte in derartigen Fällen regelmäßig die Personalakten aller Beteiligten — d. h. sowohl der antragstellenden/klagenden Person wie der bzw. des ausgewählten Bediensteten — an. Nur selten beschränkten sich die Anforderungen auf die Vorlage von Zeugnissen, Beurteilungen, Synopsen mit Leistungsnachweisen u. ä. Diese Verfahrensweise habe in der Vergangenheit verschiedentlich dazu geführt, daß Verfahrensbeteiligte Einsicht in die kompletten Personalakten anderer bewerbender Personen genommen hätten.

Ich teile die Auffassung der Personalreferentinnen und -referenten, daß eine solche Praxis datenschutzrechtlich nicht hinnehmbar ist. Nach § 100 Abs. 1 der Verwaltungsgerichtsordnung (VwGO) haben die Verfahrensbeteiligten grundsätzlich das Recht, die Gerichtsakten sowie alle beigezogenen Verwaltungsvorgänge einzusehen. Die Behörde kann die Einsicht in ihre dem Gericht vorliegenden Akten nicht beschränken. Eine Einsichtnahme in bestimmte Personalunterlagen kann deshalb nur dadurch verhindert werden, daß diese Vorgänge dem Gericht von vornherein nicht vorgelegt werden.

Nach § 99 VwGO sind die Behörden allerdings zur Aktenvorlage gegenüber den Verwaltungsgerichten verpflichtet, soweit nicht einer der gesetzlich vorgesehenen Ausnahmetatbestände vorliegt. Personalakten gehören zwar zu den Vorgängen, die ihrem Wesen nach geheimzuhalten sind. Im Rahmen einer Konkurrentenklage muß jedoch das Interesse der bei der Bewerbung erfolgreichen Person an der Wahrung ihrer Persönlichkeitssphäre hinter dem allgemeinen Interesse an der Verwirklichung des Leistungsprinzips (Art. 33 Abs. 2 GG) zurücktreten. Die Behörde hat deshalb alle vom Gericht angeforderten Akten vorzulegen, die den Streitgegenstand betreffen.

Soweit die Personalunterlagen für die gerichtliche Entscheidung erforderlich sind, bestehen auch keine datenschutzrechtlichen Bedenken, wenn die nicht berücksichtigte Person Einsicht in die Verwaltungsvorgänge über ihre Konkurrentin bzw. ihren Konkurrenten nimmt. Dies ist zur Wahrnehmung ihrer rechtlichen Interessen notwendig. Da Art. 19 Abs. 4 GG einen lückenlosen und effektiven Rechtsschutz garantiert, muß die bei der Bewerbung erfolgreiche Person insoweit die Offenlegung ihrer persönlichen Daten hinnehmen. Problematisch wird es jedoch, wenn auf diese Weise auch solche — oft höchst sensible — Daten zugänglich werden, deren Kenntnis für die Rechtsverfolgung keineswegs notwendig ist.

Die mir bekanntgewordenen Einzelfälle deuten darauf hin, daß es gängige Praxis der Verwaltungsgerichte ist, regelmäßig (und undifferenziert) sämtliche Verwaltungsvorgänge anzufordern. In Verkennung der Reichweite dieser Aktenanforderungen leiten Verwaltungsbehörden den Gerichten von sich aus auch nicht benötigte Personalunterlagen zu, ohne daß offenbar von seiten der Gerichte eine derart umfassende Unterrichtung erwartet würde.

In dieser Einschätzung sehe ich mich durch einen Fall bestärkt, in dem sich ein Vorsitzender Richter, dessen Kammer nach eigenem Bekunden „routinemäßig" „die vollständigen Unterlagen" erbeten hatte, wie folgt geäußert hat: „Eine ausdrückliche Aufforderung zur Vorlage von Personalakten ist . . . nicht ergangen. Auch kann eine unspezifizierte Bitte, die vollständigen Unterlagen bzw. die Verwaltungsvorgänge vorzulegen, nicht dahin verstanden werden, daß z. B. etwa alle über den Kläger geführten Vorgänge vorzulegen sind. Vielmehr hat die um Aktenvorlage gebetene Behörde zunächst die Akten vorzulegen, die sich — freilich nach ihrer Einschätzung — auf den Streitgegenstand beziehen. Fordert das Gericht weitere Akten an und sieht sich die Behörde aus Rechtsgründen gehindert, diesem Verlangen zu entsprechen, so sehe ich es als ihre Aufgabe an, das dem Gericht mitzuteilen . . .".

Nach dem datenschutzrechtlichen Erforderlichkeitsprinzip sind den Gerichten nur die zur Entscheidungsfindung erforderlichen Akten, bei einer Konkurrentenklage somit nur die mit der Auswahlentscheidung im Zusammenhang stehenden Personalunterlagen, zuzuleiten. Dazu gehören im wesentlichen die Personal- und Befähigungsnachweise der ausgewählten Person und der antragstellenden/klagenden Person sowie ein Gesamtverzeichnis aller Bewerberinnen und Bewerber, das allerdings bezüglich der übrigen Bewerbungen anonymisiert werden muß.

Die vom Niedersächsischen Innenministerium vorbereiteten Verwaltungsvorschriften zum Niedersächsischen Beamtengesetz betonen, daß Personalakten den Gerichten „nur im erforderlichen Umfang" zur Verfügung zu stellen sind. Die Verwaltungsbehörden sind aufgerufen, ihre Verwaltungspraxis hieran zu orientieren. Verlangt allerdings ein Gericht trotz Gegenvorstellung der Verwaltungsbehörde die Vorlage sämtlicher Personalvorgänge, ist dieser Aufforderung selbstverständlich Folge zu leisten. Der Umfang der Aktenanforderung unterliegt der richterlichen Unabhängigkeit. Er ist damit auch einer Kontrolle durch den Datenschutzbeauftragten entzogen.

Letztlich wird sich eine befriedigende Lösung des Problems nur durch eine entsprechende Änderung der VwGO erreichen lassen. Der Bundesminister der Justiz hat bereits 1989 erklärt, er prüfe die Frage, ob und inwieweit die Regelungen zum Akteneinsichtsrecht in der VwGO einer Überarbeitung bedürfen. Ob und wann es zu einer datenschutzgerechten Regelung kommen wird, läßt sich nach Auskunft des Bundesressorts derzeit jedoch nicht absehen.

15.6 Personalübersichten

Eine berufsbildende Schule wollte eine Broschüre „BBS auf einen Blick" herausgeben. Darin sollten die Anschriften, die Pensionierungsdaten, die Geburtsdaten sowie diverse Statistiken über alle Mitarbeiterinnen und Mitarbeiter wiedergegeben werden. Die Daten sollten mit Hilfe eines PC verarbeitet werden.

In Übereinstimmung mit dem Niedersächsischen Kultusministerium bin ich der Auffassung, daß wohl eine Adressenliste der Mitarbeiterinnen und Mitarbeiter einer Schule im Sekretariat vorliegen muß, um Lehrkräfte und sonstige Beschäftigte aus dienstlichen Gründen erreichen zu können. Listen über Pensionierungs- und Geburtstagsdaten sind aus dienstlichen Gründen jedoch nicht erforderlich. Auch die angesprochenen Statistiken mußten auf datenschutzrechtliche Bedenken stoßen, da die Erstellung und Veröffentlichung von Statistiken in einschlägigen Rechtsvorschriften geregelt sind.

15.7 Telefondatenerfassung

Der behördliche Datenschutzbeauftragte einer niedersächsischen Fachhochschule hat bei mir angefragt, ob die Speicherung aller Dienstgesprächsdaten und die Kontrolle durch die Vorgesetzten zulässig ist. In der Eingabe war weiter darauf hingewiesen worden, daß der EDV-Ausdruck per Umlauf allen Mitarbeiterinnen und Mitarbeitern einer Organisationseinheit zur Kenntnis gegeben wurde.

Ich halte das geschilderte Verfahren für datenschutzrechtlich nicht akzeptabel. Hierdurch werden Bedienstetendaten anderen Mitarbeiterinnen oder Mitarbeitern bekannt, die sie nicht zur Aufgabenerledigung benötigen. Unstreitig ist, daß den jeweiligen Vorgesetzten im Rahmen der Dienstaufsicht die Möglichkeit zu eröffnen ist, die von ihren Mitarbeiterinnen und Mitarbeitern geführten Dienstgespräche zu überprüfen (vgl. auch X 15.11).

Gegenüber der Fachhochschule konnte erreicht werden, daß künftig eine Einzelversendung der Ausdrucke an die jeweiligen Benutzerinnen und Benutzer der Nebenstellen erfolgt. Damit wird dem Grundsatz der Erforderlichkeit entsprochen — der verwaltungsmäßige Mehraufwand erscheint im Sinne des Datenschutzes vertretbar.

15.8 Der lange Dienstweg bei Personalunterlagen

Die innerdienstliche Behandlung von Personalunterlagen läßt immer wieder zu wünschen übrig.

15.8.1 Prüfungsergebnisse der Landesfeuerwehrschulen

So erhielt ich davon Kenntnis, daß Beurteilungen von Prüfungsleistungen der niedersächsischen Feuerwehrschulen nach Öffnung des Eingangs in der Poststelle der Bezirksregierung die Runde machten. Kenntnis erlangte folgender Personenkreis:
— Mitarbeiterinnen und Mitarbeiter der Poststelle
— Botendienst im Hause
— Abteilungsleitung
— Dezernatsleitung
— Dezernentin bzw. Dezernent sowie
— die für die Postverteilung zuständige Person innerhalb des Dezernates.

Das Niedersächsische Innenministerium hat mir mitgeteilt, daß die über einen Zeitraum von mehreren Wochen angefallenen Beurteilungen von den Landesfeuerwehrschulen aus verwaltungsökonomischen Gründen als Sammelpost an die Bezirksregierungen zugestellt werden. Dort werden sie als Eingänge nach den Bestimmungen der Geschäftsordnung verteilt. Die Beurteilungen enthalten Angaben, die aus Gründen des Persönlichkeitsschutzes vertraulich zu behandeln sind und deshalb innerbehördlich nur dem unbedingt erforderlichen Personenkreis zugänglich sein dürfen. Um dies zu gewährleisten, sind die Landesfeuerwehrschulen angewiesen worden, künftig die Beurteilungen im verschlossenen Umschlag, mit Vertraulichkeitshinweis und einem gesonderten Anschreiben an die Bezirksregierungen zu versenden. Damit kann künftig eine datenschutzgerechte Handhabung erfolgen.

15.8.2 Ärztliche Schreiben in Kollegenhand

Von Lehrkräften an allgemeinbildenden und berufsbildenden Schulen ist in Eingaben beanstandet worden, daß die für sie zuständige Bezirksregierung ihnen Schreiben mit personalrechtlichem Inhalt über die Schulleitung bzw. über das Schulaufsichtsamt zugestellt hat. Die Schreiben enthielten sensible Daten zum Gesundheitszustand der Betroffenen wie z. B. zur Erforderlichkeit einer psychosomatischen Behandlung oder zur Frage der Dienstfähigkeit. Die Lehrkräfte haben die Befürchtung geäußert, daß durch die offene Zustellung der Schreiben der jeweiligen Bezirksregierung ein großer Personenkreis Kenntnis von ihrem Gesundheitszustand erhalten könnte.

Nach § 87 Abs. 1 NBG ist der Dienstherr gegenüber seinen Beamten zur Fürsorge verpflichtet. Ausfluß dieser Fürsorgepflicht ist es, Personalangelegenheiten vertraulich zu behandeln. Ein besonderes Schutzbedürfnis der Beamtin bzw. des Beamten besteht, wenn es um Fragen der Gesundheit und um Behandlungsmaßnahmen geht. Die Offenbarung solcher Angelegenheiten darf daher nur gegenüber einem begrenzten Personenkreis erfolgen, der die Kenntnis für beamten- oder verwaltungsrechtliche Entscheidungen benötigt. Der mit der Beamtin oder dem Beamten zu führende Schriftwechsel, der zum Bestandteil der Personalakte wird, ist daher ebenso vertraulich zu behandeln. Das Kultusministerium stimmt meiner Auffassung zu, daß es nicht erforderlich ist, die Information über den Gesundheitszustand einer Lehrkraft dem Schulaufsichtsamt oder der Schulleitung zur Kenntnis zu geben.

Die beteiligte Bezirksregierung versendet entsprechende Schreiben nunmehr nur noch verschlossen direkt an die betroffenen Bediensteten. Ich habe das Ministerium gebeten, eine verbindliche Regelung für alle niedersächsischen Bezirksregierungen zu treffen. Dies ist im Rahmen einer Dienstbesprechung mit den zuständigen Dezernenten der Bezirksregierungen geschehen.

15.8.3 Ein fürsorglicher Blick in Kurantragsdaten

Ein Polizeibeamter hatte auf Anraten seines Arztes bei dem zuständigen Dezernat der Bezirksregierung eine Kur beantragt, die abgelehnt wurde. Gegen den ablehnenden Bescheid legte er Widerspruch ein.

In dem Widerspruchsbescheid der Bezirksregierung wird eine Vielzahl von Krankheitsdaten des Petenten aufgeführt. Der Bescheid wurde ihm auf dem Dienstwege zugestellt, so daß der Kommandeur der Schutzpolizei bei der Bezirksregierung und der Leiter seiner Schutzpolizeiinspektion Kenntnis von den ärztlichen Angaben erhalten haben. Der Beamte befürchtete, daß durch die nach seiner Auffassung unzulässige Übermittlung seiner Daten berufliche Nachteile für ihn entstehen könnten.

In ihrer Stellungnahme hat die Bezirksregierung darzulegen versucht, daß das kritisierte Verfahren aus dienstlichen Gründen (u. a. einsatztaktische Gesichtspunkte, Fürsorgepflicht der vorgesetzten Dienststellen) erforderlich gewesen sei. Darüber hinaus wurden Organisationserlasse des Niedersächsischen Innenministeriums als „Rechtsgrundlagen" herangezogen.

Das Fachressort hat dagegen zu Recht betont, daß die im Rahmen von Maßnahmen der freien Heilfürsorge anfallenden personenbezogenen Daten nicht für andere als Heilfürsorgezwecke verwendet werden dürfen. Eine Zugangsberechtigung zu den im Rahmen der freien Heilfürsorge entstandenen Vorgängen haben nur die Beschäftigten der mit der Bearbeitung der Anträge und Abrechnungen betrauten Stelle. Ausnahmen von der Zweckbindung für die Verwendung der Unterlagen sind nur möglich, wenn die Berechtigten im Einzelfall einwilligen, die Einleitung oder Durchführung eines im Zusammenhang mit einem Antrag stehenden behördlichen oder gerichtlichen Verfahrens dies erfordert (z. B. Widerspruchsbescheid durch die Mittelinstanzen bei Antragsablehnung durch die Polizeidirektionen) oder soweit es zur Abwehr erheblicher Nachteile für das Gemeinwohl, einer sonst unmittelbar drohenden Gefahr für die öffentliche Sicherheit oder einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist.

Diese Voraussetzungen waren im vorliegenden Falle nicht erfüllt. Das Ministerium stimmt meiner Auffassung zu, daß es nicht erforderlich und damit auch nicht zulässig ist, die Personalstellen über Vorgänge der Heilfürsorge, die Gesundheitsdaten von Beamtinnen und Beamten enthalten, zu informieren. Hier ist lediglich eine Abstimmung, wie z. B. hinsichtlich des Termins eines Kurantritts, notwendig. Entsprechende Bescheide sind im verschlossenen Briefumschlag mit vorgehefteter Empfangsbestätigung zuzusenden. In Angelegenheiten der freien Heilfürsorge ist — wie das Innenministerium weiter ausgeführt hat — eine Verknüpfung mit Daten über die Polizeidienstfähigkeit nicht zulässig. Die Feststellung der Polizeidienstunfähigkeit ist beamtenrechtlich geregelt. Aussagen zur Polizeidienstfähigkeit dürfen von den Abrechnungsstellen der freien Heilfürsorge nicht erfolgen.

Damit sich ähnliche Fälle in Zukunft nicht wiederholen, hat das Innenministerium erklärt, es werde die betroffenen Behörden durch Erlaß auf den daten-

schutzgerechten Umgang mit Unterlagen in Heilfürsorgeverfahren hinweisen. Ich hoffe daher, daß zukünftig derartige unzulässige Datenübermittlungen im Polizeibereich nicht mehr erfolgen werden.

15.8.4 Der Amtsleiter als Postverteiler

Ein bei einem Schulaufsichtsamt beschäftiger Schulpsychologe beschwerte sich, daß von der Bezirksregierung an ihn gerichtete Schreiben durch das Sekretariat geöffnet und dem Leiter des Schulaufsichtsamtes zur Kenntnis gebracht wurden. Im Zusammenhang mit einer nicht genehmigten Nebentätigkeit war der Petent von der zuständigen Bezirksregierung zu einem dienstlichen Gespräch vorgeladen worden. Das Schreiben war über den Leiter des Schulaufsichtsamtes adressiert und sollte gegen Empfangsbestätigung ausgehändigt werden. Der betroffene Schulpsychologe war der Auffassung, daß die Bezirksregierung seine unmittelbar vorgesetzte Dienststelle sei, und hatte sich wegen der Übermittlung des ihn betreffenden personalrechtlichen Sachverhaltes bei dem Leiter seiner Dienststelle beschwert. Der Bescheid zu dieser Beschwerde wurde wiederum auf dem gleichen Postweg zugestellt. Darin wurde von der Bezirksregierung auf einen Runderlaß des Kultusministeriums vom 30. Juli 1980 (SVBl. 1980 S. 308) Bezug genommen. Der Petent vertrat die Auffassung, daß die Offenbarung des ihn betreffenden Sachverhaltes nicht für die Wahrnehmung der Leitungsaufgaben des Leiters des Schulaufsichtsamtes erforderlich war.

In Nr. 4 Abs. 3 des vorstehend genannten Organisationserlasses wird die Funktion der Leitung des Schulaufsichtsamtes umschrieben. Danach ist es nicht erforderlich, daß diese Kenntnis von Besprechungen und Schriftwechseln erhält, die einzelne Bedienstete der Dienststelle in dienstrechtlichen Angelegenheiten mit ihrem Dienstvorgesetzten — also der Bezirksregierung — führen, jedenfalls dann nicht, wenn es sich dabei um Angelegenheiten handelt, die den dienstlichen Einsatz der Bediensteten im Schulaufsichtsamt nicht unmittelbar betreffen. Deshalb ist es unzulässig, derartige Schriftstücke den Bediensteten auf dem Dienstwege über die Leiterin oder den Leiter des Schulaufsichtsamtes zuzuleiten.

Das Niedersächsische Kultusministerium hat mir mitgeteilt, daß die Bezirksregierungen hierüber unterrichtet worden sind. Ich gehe davon aus, daß derartige Übermittlungen in Personalangelegenheiten künftig nicht mehr erfolgen werden.

15.9 Rechnungsprüfung und Urlaub

Der Personalrat einer Handwerkskammer wandte sich an mich, weil der Rechnungsprüfungsausschuß bei dieser Dienststelle vom Verwaltungsleiter die Herausgabe der Urlaubskarteikarten aller Mitarbeiterinnen und Mitarbeiter verlangt hatte. Diese war vom Verwaltungsleiter aus datenschutzrechtlichen Gründen verweigert worden. Hintergrund des nicht begründeten Begehrens des Rechnungsprüfungsausschusses war möglicherweise der Wunsch, eine Übersicht über nicht angetretenen, sondern „ausgezahlten" Urlaub zu erhalten. Der Personalrat vertrat die Auffassung, daß kein berechtigtes Interesse des Rechnungsprüfungsausschusses an einer Einsicht in die Urlaubskartei besteht und selbst bei einer summarischen, nicht-reidentifizierbaren Zusammenstellung ein möglicher Einsichtsanspruch hinter den schützenswerten Interessen der Mitarbeiterinnen und Mitarbeiter zurückstehen müsse.

Die Handwerkskammer hat in ihrer Stellungnahme offengelassen, ob eine Urlaubsaufstellung ohne Namensnennung der einzelnen Mitarbeiterinnen und

Mitarbeiter den Erfordernissen der Rechnungsprüfung nach den bestehenden Vorschriften gerecht werden kann.

Nach den neuen Datenschutzgesetzen des Bund und der Ländern liegt eine unzulässige Zweckänderung gespeicherter Daten nicht vor, wenn sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen dient (vgl. § 14 Abs. 3 BDSG, § 10 Abs. 3 NDSG-E). Diese Verwendung ist jedoch nur zulässig, soweit sie zur Erfüllung dieser Aufgaben erforderlich ist.

Die Aufgaben und Befugnisse des Rechnungsprüfungsausschusses der Handwerkskammer leiten sich aus § 105 Abs. 2 Nrn. 8 und 9 der Handwerksordnung, § 26, 37 der Satzung der Handwerkskammer und der § 42 bis 47 der Haushalts-, Kassen- und Rechnungslegungsordnung der Handwerkskammer (HKRO) ab. Nach § 44 HKRO sind dem Rechnungsprüfungsausschuß alle Unterlagen vorzulegen und Auskünfte zu erteilen, die von ihm zur Erfüllung der Aufgaben für erforderlich gehalten werden. Gemäß § 43 Abs. 2 dieser Vorschrift erstreckt sich der Prüfungsauftrag auf die Einhaltung der für die Haushalts- und Wirtschaftsführung geltenden Vorschriften und Grundsätze, insbesondere auch darauf, daß die Einnahmen und Ausgaben sachlich und rechnerisch begründet und belegt sind und daß wirtschaftlich und sparsam verfahren sowie die Buchführung ordnungsgemäß und zweckentsprechend wahrgenommen wird. Mithin wird davon auch die Überprüfung der Personalausgaben umfaßt.

Der gesetzlich und tarifrechtlich zu gewährende Urlaubsanspruch ist ein Teil der Personalkosten. Zum Nachweis hierüber ist eine Urlaubskartei zu führen. Da sich die Prüfung des Rechnungsprüfungsausschusses gemäß § 43 Abs. 2 Nr. 2 HRKO darauf erstreckt, ob die Ausgaben sachlich begründet und belegt sind, muß nach Auffassung des Niedersächsischen Ministeriums für Wirtschaft, Technologie und Verkehr diesem Ausschuß im Rahmen der Überprüfung der Personalausgaben ermöglicht werden, die Urlaubskartei einzusehen. Nur so könne er sich davon überzeugen, ob die für die Haushalts- und Wirtschaftsführung geltenden Vorschriften eingehalten wurden. Auch eine Überprüfung der ordnungsgemäßen und zweckmäßigen Führung der Urlaubskartei gem. § 43 Abs. 2 Nr. 4 HRKO könne nur durch die vollständige Einsichtnahme in die Urlaubskartei erfolgen. Für die Erfüllung der Aufgaben des Rechnungsprüfungsausschusses sei es deshalb gemäß § 44 HRKO erforderlich, ihm die Einsichtnahme in die Urlaubskartei einzuräumen.

Dieser Argumentation kann ich mich nicht verschließen. Die Urlaubskartei enthält die Daten, die für die Berechnung und Abwicklung des Urlaubsanspruches erforderlich sind. Wenn der Prüfungsausschuß ohne Einsichtnahme in die Urlaubskartei nicht in der Lage ist, die ordnungsgemäße Anwendung der Vorschriften im Bereich der personalbezogenen Haushaltsführung zu überprüfen, muß ihm die Einsicht im Rahmen eines konkreten Prüfungsvorhabens möglich sein.

15.10 Dienstausweise

In meinem letzten Tätigkeitsbericht (X 15.8) hatte ich die Angabe der Personalausweisnummer in den Dienstausweisen der Landesbediensteten in Frage gestellt. Nach intensiven Bemühungen haben sich schließlich alle Ressorts der niedersächsischen Landesregierung mit dem Fortfall des Datums einverstanden erklärt und einer Änderung des Runderlasses vom 23. Juni 1958 zugestimmt. Der die Änderung beinhaltende Runderlaß des Niedersächsischen Innenministeriums vom 20. August 1991 wurde im Nds. MBl. S. 1170 veröffentlicht.

15.11 Mitteilungen gemäß § 13 des Schwerbehindertengesetzes

Bei der Anwendung des § 13 des Schwerbehindertengesetzes ergab sich die Frage, ob der Arbeitgeber im Schwerbehindertenverzeichnis seines Betriebes den genauen Grad der Behinderung angeben muß oder ob die Angabe „Grad der Behinderung mehr bzw. weniger als 50 %" genügt. Dieses Verzeichnis ist Vertreterinnen bzw. Vertretern des Arbeitsamtes und der zuständigen Hauptfürsorgestelle auf Verlangen vorzuzeigen.

Das Niedersächsische Sozialministerium teilte mir mit, daß die Verzeichnisse der Arbeitgeber ausschließlich für die Prüfung der Anzeigen benötigt werden und nach Auswertung in der Akte der Hauptfürsorgestelle verbleiben. Es sei ausreichend, wenn sich aus der Anzeige ergebe, ob es sich bei den angeführten Mitarbeiterinnen oder Mitarbeitern um Schwerbehinderte (Angabe SB und Aktenzeichen des Versorgungsamtes) oder um — den Schwerbehinderten gleichgestellte — Personen (Angabe GL und Aktenzeichen des Arbeitsamtes) handelt. Weitere Angaben zum Grad der Behinderung sind nach Auffassung des Fachressorts nicht erforderlich. Ich halte diese Bewertung des Fachressorts für datenschutzgerecht.

15.12 Disziplinarverfahren

Gegen einen Beamten war auf Veranlassung seiner Dienstbehörde ein Strafverfahren eingeleitet worden. Für Zwecke der Beweisführung hatte der Bedienstete die ihn behandelnden Ärzte von ihrer Schweigepflicht entbunden.

Nach Einstellung des Verfahrens gemäß § 153 Abs. 2 StPO erbat seine Dienstbehörde, die gegen ihn ein Disziplinarverfahren eingeleitet hatte, von der zuständigen Staatsanwaltschaft Einsicht in die Strafakten. In der der Dienstbehörde übersandten Akte befanden sich auch die im Strafverfahren gemachten Aussagen der Ärzte sowie von diesen vorgelegte ärztliche Unterlagen. Der Petent war zu Recht der Auffassung, daß die ärztlichen Angaben wegen der auf das Strafverfahren beschränkten Entbindung von der Schweigepflicht nicht seiner Dienstbehörde übermittelt werden durften.

Die Vorschrift über die disziplinarrechtliche Rechts- und Amtshilfe (§ 20 NDO) läßt die hier erfolgte Einschränkung des Arztgeheimnisses nicht zu. Die in einem Strafverfahren von einem Verfahrensbeteiligten abgegebene Entbindungserklärung von der ärztlichen Schweigepflicht kann nur für dieses Verfahren gelten. Für ein eventuell sich anschließendes Disziplinarverfahren — wie in dem der Eingabe zugrundeliegenden Fall — ist eine erneute Erklärung erforderlich. Erfolgt diese nicht, so muß die erbetene Akteneinsicht auf die Aktenteile beschränkt werden, die keine ärztlichen Unterlagen und Erklärungen enthalten, um den Entbindungsberechtigten insoweit zu schützen (vgl. Nr. 187 Abs. 1 der übergangsweise noch geltenden Richtlinien für das Straf- und Bußgeldverfahren — RiStBV).

15.13 Städtische AB-Maßnahmen

Eine kreisfreie Stadt hat einen Fragebogen für eine Beschäftigung im Rahmen von Arbeitsbeschaffungsmaßnahmen entwickelt, in dem u. a. nach der Höhe der derzeitigen Arbeitslosenhilfe und der Höhe der Miete gefragt wird. Die Stadt teilte mir mit, daß der Fragebogen den Bewerberinnen und Bewerbern nicht vorgelegt, sondern die Fragen im Rahmen eines Vorstellungsgespräches

erörtert werden. Die Angaben sollten kein Entscheidungskriterium für eine Einstellung darstellen, sondern der Einschätzung und Beratung in bezug auf mögliche Wohngeld- bzw. Sozialhilfeansprüche dienen. Darüber hinaus seien die derzeitigen Einkommensverhältnisse ein einstellungsrelevantes Kriterium, da soziale Gesichtspunkte zu berücksichtigen wären.

Ich habe der Stadt empfohlen, ihre Praxis hinsichtlich der Datenerhebung im Zusammenhang mit AB-Maßnahmen zu ändern. Zwar hat der Träger einer solchen Maßnahme eine Auswahlmöglichkeit, bei der auch soziale Gesichtspunkte von Belang sein können. Dennoch läßt sich aus Sicht des Datenschutzes nicht rechtfertigen, daß Bewerberinnen oder Bewerber nach der Höhe ihres bisherigen Einkommens und nach der Höhe ihrer Miete gefragt werden. Diese Daten sind für die Auswahlentscheidungen nicht erforderlich. Vielmehr muß eine abgestufte Datenerhebung (entsprechend den Grundsätzen der arbeitsgerichtlichen Rechtsprechung im Rahmen der Bewerberauswahl bei der Besetzung von Arbeitsplätzen im öffentlichen Dienst) erfolgen. Die Beratung (unter Einschaltung von Sozialarbeiterinnen bzw. Sozialarbeitern hinsichtlich Wohngeldansprüchen usw.) kann auch noch zu einem späteren Zeitpunkt, nämlich nach der eigentlichen Entscheidung über den ABM-Einstellungsvorgang, vorgenommen werden.

16. Kommunalverwaltung

16.1 Rat, Kreistag und Verwaltung

Der Landkreis Hannover führt seit kurzem automatisierte Dateien über die Kreistagsabgeordneten und über die Mandatsträger der kreisangehörigen Städte und Gemeinden. Die Daten der Kreistagsabgeordneten werden aus einem Personalbogen entnommen, den die Abgeordneten zu Beginn einer Wahlperiode ausgefüllt haben. Wie der Landkreis ausgeführt hat, sind die Daten nicht zur Weitergabe an Dritte, sondern lediglich für interne Verwaltungszwecke bestimmt. Gespeichert sind Name, Vorname sowie die Parteizugehörigkeit der Mandatsträger.

Der Landkreis hält eine Speicherung der Daten von Mandatsträgern der kreisangehörigen Städte und Gemeinden zur Erfüllung der Aufgaben der Kommunalaufsicht für erforderlich. Zum Beispiel hat der Landkreis zu überprüfen, ob bei Mandatsverlusten nach den kommunalwahlrechtlichen Vorschriften das Mandat auf die nächste Ersatzperson des Wahlvorschlages übergeht, auf dem die aus dem Gremium ausgeschiedene Person gewählt worden ist. Des weiteren wird bei mündlichen oder schriftlichen Anfragen zu kommunalverfassungsrechtlichen Problemen geprüft, ob es sich bei den Anfragenden tatsächlich um Ratsmitglieder handelt. Ebenso ist die Besetzung und namentliche Zusammensetzung der Räte im Rahmen der kommunalaufsichtsbehördlichen Überprüfung der Niederschriften über die Sitzungen der Räte, des Antragsrechtes der Ratsmitglieder, bei der Entsendung von Ratsmitgliedern in Drittorganisationen oder bei der Frage des Mitwirkungsverbotes von Bedeutung. Diese Argumente des Landkreises belegen die Notwendigkeit der Datenspeicherung.

16.2 Frauenbeauftragte

Nach dem Referentenentwurf eines Zehnten Gesetzes zur Änderung der Niedersächsischen Gemeindeordnung (NGO) und der Niedersächsischen Landkreisordnung (NLO) sollten kommunale Frauenbeauftragte das Recht erhalten, ohne Zustimmung der betroffenen Bediensteten Einsicht in deren Personalakten zu nehmen. Gegen diese Regelung habe ich Bedenken angemeldet, weil sie der besonderen Schutzbedürftigkeit der Personalakten nicht gerecht wird. Der Grundsatz der Vertraulichkeit stellt — neben seiner historischen Herausbildung als hergebrachter Grundsatz des Berufsbeamtentums im Beamtenbereich — ein letztlich im Persönlichkeitsrecht wurzelndes Recht der Bediensteten dar, das den Schutz ihrer Privat- und Intimsphäre durch den Dienstherrn/Arbeitgeber umfaßt.

Wegen des notwendigen besonderen Schutzes von Personalakten hat der Gesetzgeber ein Akteneinsichtsrecht für die Personalvertretung nicht vorgesehen. Mitglieder des Personalrats dürfen nur mit Zustimmung der Betroffenen Einsicht in deren Personalakte nehmen. Eine entsprechende Regelung habe ich dem Frauenministerium auch für die Frauenbeauftragte vorgeschlagen.

Auch wenn die Stellung der Frauenbeauftragten nach dem Gesetzentwurf nicht mit der des Personalrats vergleichbar ist, so hat auch dieser die Verpflichtung, darüber zu wachen, daß jede unterschiedliche Behandlung von Bediensteten wegen ihres Geschlechts unterbleibt (§ 66 Abs. 1 Satz 1 Nds. PersVG). Die Personalvertretungen haben auch ohne ein weitergehendes Akteneinsichtsrecht ihre Aufgaben bisher wirksam wahrnehmen können. Dies wird auch für die Frauenbeauftragten der Fall sein. Zudem kann davon ausgegangen werden, daß in Auswahlverfahren aussichtsreiche männliche Bewerber in der Regel schon im eigenen Interesse eine erbetene Zustimmung zur Akteneinsicht erteilen werden. Zur Aufgabenwahrnehmung ist demnach ein Akteneinsichtsrecht ohne Zustimmung der Bediensteten schon vom Ansatz her nicht erforderlich. Im übrigen würde ein solches Recht in der Praxis zwangsläufig dazu führen, daß die Frauenbeauftragte auch von höchst sensiblen personenbezogenen Daten Kenntnis erlangen könnte, die keinen Bezug zu ihrem gesetzlich vorgesehenen Auftrag mehr aufweisen. Ich habe darauf hingewiesen, daß die Gleichstellungsgesetze anderer Länder ebenfalls keine Akteneinsicht der Frauenbeauftragten ohne Zustimmung der Bediensteten zulassen.

Demgegenüber bestehen keine grundsätzlichen Bedenken dagegen, ein ausdrückliches Recht auf Einsicht in Bewerbungsunterlagen zu statuieren.

Der Gesetzentwurf der Landesregierung, der am 20. Mai 1992 im Landtag eingebracht wurde (LT-Drs 12/3260), enthält die von mir vorgeschlagene Regelung einer eingeschränkten Einsicht in Personalakten.

16.3 Kommunale Abgaben

Meine rechtzeitige Beteiligung an der Neufassung des Kommunalabgabengesetzes ermöglichte einige datenschutzrechtliche Verbesserungen und Klarstellungen. Es wurden Einzelheiten hinsichtlich der Erhebungsmerkmale in einer Fremdenverkehrsbeitragssatzung sowie die Beauftragung und die Mitteilungspflichten Dritter festgelegt. Durch die Neuregelung wird die in der Vergangenheit umstrittene und immer wieder zu Beschwerden führende Praxis der Gemeinden und Landkreise, für die Berechnung der Abgaben auf bei Dritten vorhandene Berechnungsgrundlagen (z. B. für die Berechnung von Abwassergebühren auf die Frischwasserbezugswerte der Wasserversorgungsunternehmen) zurückzugreifen, auf eine normenklare gesetzliche Grundlage gestellt.

Der Umfang der Datenerhebung zur Prüfung der Zweitwohnungssteuerpflicht war auch in diesem Berichtszeitraum wieder des öfteren Gegenstand von Eingaben und Beschwerden. Interessant war der Fragenkatalog einer Gemeinde, in dem u. a. nach Strom-, Gas- und Wasserverbräuchen, einem Zeitungsabonnement und Telefongebühren gefragt wurde, um den Lebensmittelpunkt zu ermitteln. Das Innenministerium vertrat die Auffassung, daß diese Fragen zur Feststellung eines für die Besteuerung erheblichen Sachverhaltes dienen würden. Es bliebe letztlich dem Betroffenen überlassen, die Auskünfte zu erteilen. Folge er dem Auskunftsersuchen nicht oder nicht vollständig, sei es nicht zu beanstanden, wenn die Gemeinde zu seinem Nachteil den Schluß ziehe, daß es sich bei der in ihrem Gebiet gelegenen Wohnung um eine zweitwohnungssteuerpflichtige Wohnung handele. Ich konnte diese Rechtsauffassung nicht widerlegen, wenngleich eine solche Verwaltungspraxis das Erforderlichkeitsprinzip arg strapaziert.

16.4 Datenübermittlung aus Bauakten

Ein Petent wandte sich an mich, weil eine Kommunalverwaltung (Untere Denkmalschutzbehörde) nach Erwerb eines unter Denkmalschutz stehenden Gebäudes Auskünfte aus Bauakten (betr. Umbaumaßnahmen) an eine Interessengemeinschaft gewährt hatte. Weiterhin habe die Untere Denkmalschutzbehörde einen Mitarbeiter seines Kreditinstitutes über die Höhe eines gegen ihn zu verhängenden Bußgeldes wegen eines Verstoßes gegen das Denkmalschutzgesetz unterrichtet; der Bank sei auch mitgeteilt worden, daß er noch keine Baugenehmigung habe. Dadurch sei ihm ein erheblicher Nachteil entstanden.

Ich mußte feststellen, daß alle erteilten Auskünfte aus datenschutzrechtlicher Sicht nicht zulässig waren. Es handelte sich jeweils um Datenübermittlungen an Stellen außerhalb der öffentlichen Verwaltung. Bei Berücksichtigung der schutzwürdigen Belange des Betroffenen hätten diese Übermittlungen nicht erfolgen dürfen. So war bei der Auskunft über das Vorliegen einer Baugenehmigung an die Interessengemeinschaft nicht auszuschließen, daß die Bekanntgabe eines unbeabsichtigten oder beabsichtigten Verstoßes gegen das Bauordnungsrecht beim Petenten zu Nachteilen wirtschaftlicher, sozialer oder persönlicher Art führen konnte. Auch hinsichtlich der Auskünfte an das Kreditinstitut haben die schutzwürdigen Belange das berechtigte Interesse des Kreditinstitutes überwogen. Das Kreditunternehmen wäre mit seinem Auskunftsbegehren an den Kunden selbst zu verweisen gewesen.

Die betroffene Kommunalbehörde hat eingeräumt, daß diese beiden Auskünfte unzulässigerweise erteilt worden sind. Ich habe die Datenschutzverstöße gegenüber dem vertretungsberechtigten Organ der betroffenen Gebietskörperschaft beanstandet. Ich habe empfohlen, Auskünfte aus Unterlagen des Bauordnungsbereiches in einer Dienstanweisung oder in ähnlicher schriftlicher Form zu regeln und die betroffenen Mitarbeiterinnen und Mitarbeiter der Behörde darüber zu unterrichten. Die Kommune hat mir mitgeteilt, daß innerbehördlich dafür Sorge getragen werde, daß künftig Verstöße gegen datenschutzrechtliche Bestimmungen nicht mehr stattfinden.

16.5 Datenschutz in der Poststelle

Der Arbeitsbereich Statistik und Wahlen einer Stadt hat die Behandlung der für ihn bestimmten Posteingänge durch die zentrale Poststelle problematisiert. Er fragte an, ob die Poststelle Schriftstücke mit sensiblem Inhalt, die bei

Posteingang automatisch geöffnet wurden, wieder einzutüten hat und nur in einem verschlossenen Umschlag über die Dienstpost dem Fachamt zuleiten darf.

Im einzelnen ging es um folgende Unterlagen:
1. Mitteilungen über einen Ausschluß vom Wahlrecht (vgl. auch 31.9), die nach den geltenden Bestimmungen (MiStra und MiZi) in einem verschlossenen Brief an die für die Führung des Wählerverzeichnisses zuständige Behörde zu richten sind.
2. Auskünfte aus dem Bundeszentralregister an Behörden, die nach § 44 BZRG nur den mit der Entgegennahme oder Bearbeitung betrauten Bediensteten zur Kenntnis gebracht werden dürfen.
3. Statistikunterlagen, für deren Verarbeitung nach den Statistikgesetzen personelle, organisatorische und technische Maßnahmen zur Abschottung der für die Statistik zuständigen Organisationseinheit von den anderen Organisationseinheiten sicherzustellen sind.

Aus datenschutzrechtlicher Sicht ist die Forderung des Fachamtes nach unmittelbarer, ungeöffneter Zuleitung der erkennbar für sie bestimmten Posteingänge und der Weiterleitung versehentlich geöffneter Eingänge im geschlossenen Umschlag zu begrüßen.

Während im BZRG und im Landesstatistikgesetz für die unter 2. und 3. angesprochenen Bereiche datenschutzrechtliche Regelungen bestehen, fehlen diese bisher für Mitteilungen über einen Ausschluß vom Wahlrecht. Für einen Übergangszeitraum — bis zum Inkrafttreten der notwendigen Rechtsvorschriften — sind jedoch die Bestimmungen der Verwaltungsvorschriften MiStra und MiZi zu beachten. Danach werden die Mitteilungen über einen Ausschluß vom Wahlrecht in einem verschlossenen Umschlag übersandt. Dieser muß ungeöffnet von der Poststelle an die für die Führung des Wählerverzeichnisses zuständige Stelle weitergeleitet werden. Im Regelfall wird dies das Einwohnermeldeamt sein, in der Phase der Wahlvorbereitungen das Amt bzw. die Abteilung Statistik und Wahlen.

Ich habe der betroffenen Stadt empfohlen, als Ergänzung ihrer Satzung über die statistische Dienststelle und ihrer Abschottung auch in ihrer Allgemeinen Dienstanweisung eine Anordnung über den Umgang mit Posteingängen für das Arbeitsgebiet Statistik und Wahlen aufzunehmen.

16.6 Grundeigentümeradressen für Werbezwecke

Die Weitergabe einer Anschriftenliste der Haus- und Grundstückseigentümer aus der Grundsteuerdatei einer Gemeinde an ein Gasversorgungsunternehmen für Werbezwecke habe ich wegen des Verstoßes gegen die Vorschriften der Abgabenordnung über das Steuergeheimnis beanstandet. Eine Offenbarungsbefugnis besteht nicht. Die Datenübermittlung hätte vermieden werden können, wenn das Schreiben des Gasversorgungsunternehmens durch die Gemeinde versandt worden wäre. Die Gemeinde hat versichert, daß sie künftig die Vorschriften einhalten wolle.

16.7 Unterrichtung von Ortsvorstehern

§ 55 h NGO regelt die Aufgabenstellung des Ortsvorstehers einer Ortschaft als Teil einer Gemeinde. Vor dem Hintergrund dieser Vorschrift hat eine Kommunalverwaltung bei mir angefragt, ob es datenschutzrechtlich unbedenklich ist, ihren Ortsvorstehern zur Erfüllung ihrer Aufgaben Kenntnis über jede Eigentumsveränderung der Grundstücke im Gemeindegebiet zu geben.

Ich mußte der Gemeinde mitteilen, daß eine Unterrichtung des Ortsvorstehers über Eigentumsveränderungen im gesamten Gemeindegebiet unzulässig ist. Selbst die Kenntnis von jeder Eigentumsveränderung in der Ortschaft ist für ihn nicht nötig. Eine Übermittlung personenbezogener Daten kommt nur in Betracht, soweit sie zur Aufgabenerfüllung erforderlich ist (vgl. § 10 Abs. 1 NDSG). Hinsichtlich seiner Aufgabe, die Belange seiner Ortschaft zu wahren, ist der Ortsvorsteher in gleichem Umfang wie die Mitglieder von Ortsräten nach Maßgabe von § 55 g NGO zu informieren. Der Umfang der Informationen, die der Ortsvorsteher zur Erledigung seiner Verwaltungsaufgaben benötigt, bestimmt sich nach den Hilfsfunktionen, die er entsprechend der Hauptsatzung der jeweiligen Gemeinde wahrzunehmen hat.

16.8 Bewerbungen in kommunalen Vertretungskörperschaften

Ein Mitglied eines Schulausschusses einer niedersächsischen Gemeinde kritisierte in einer Eingabe das Besetzungsverfahren einer Schulleiterstelle. Von der zuständigen Bezirksregierung sei eine Kollegin für die Besetzung der Schulleiterstelle in seiner Gemeinde vorgeschlagen worden, die bereits kommissarisch die Schule geleitet habe. Üblicherweise würden die Mitglieder des Schulausschusses in einer Ausschußsitzung um Stellungnahme gebeten. Da in dem der Eingabe zugrundeliegenden Verfahren eine Sitzung des Ausschusses in den Sommerferien erforderlich gewesen wäre, schickte die Gemeinde sämtlichen Ausschußmitgliedern sowie deren Vertreterinnen und Vertretern eine schriftliche Anfrage zur geplanten Stellenbesetzung. In dem Schreiben waren auch die Prüfungsergebnisse der ersten und zweiten Lehramtsprüfung angegeben.

Das Kultusministerium vertritt die Auffassung, daß die Übermittlung der vom Petenten angesprochenen Daten der Bewerberin an die an dem Besetzungsverfahren beteiligten Stellen zur rechtmäßigen Erfüllung von deren Aufgaben erforderlich war. Umfang und Adressaten des Übermittlungsvorganges sind durch Erlaß vom 20. Mai 1983 (SVBl. S. 216) geregelt. Dieser Auffassung kann ich vom Grundsatz her zustimmen.

Das Verfahren beim Schulträger erfolgte im Rahmen der Vorschriften des kommunalen Verfassungsrechts. Art. 28 Abs. 2 GG garantiert das Selbstverwaltungsrecht der Gemeinden. Es besteht weder seitens des Niedersächsischen Kultusministeriums noch des Niedersächsischen Innenministeriums die Möglichkeit, zu regeln, wie bei Kommunalbehörden und kommunalen Gremien mit den Daten aus Bewerbungen verfahren wird. Datenschutzrechtlich bindend sind jedoch die Vorschriften der Niedersächsischen Gemeindeordnung über die Pflicht der Ratsmitglieder und Ausschußmitglieder zur Amtsverschwiegenheit (§§ 39 Abs. 3, 25 NGO).

Aus der Eingabe war nicht ersichtlich, daß gegen diese Vorschriften verstoßen worden ist. Die Kommunalbehörden müssen zwar die nötige Vorsorge treffen, daß vertraulich zu behandelnde Unterlagen nur das betreffende Ratsmitglied erreichen. Daß die Mandatspost im Hause des Ratsmitglieds nicht in unbefugte Hände gelangt, liegt jedoch in dessen eigener Verantwortung. Auch kann es nach Auffassung des Innenministeriums den Verwaltungen nicht verwehrt werden, Beratungsunterlagen nicht nur dem Ausschußmitglied, sondern zugleich dessen Vertretung zuzusenden. Dies halte ich für problematisch.

Ich habe dem Petenten gegenüber zum Ausdruck gebracht, daß — auch in Anbetracht der Ausführungen des Niedersächsischen Innenministeriums — bei mir ein erhebliches Unbehagen bestehen bleibt. Nach meinem Dafürhalten hätte die Gemeinde ein Schreiben der in der Eingabe genannten Art zu-

mindest als vertrauliche Personalsache kennzeichnen, beim Adressaten den Zusatz „persönlich" hinzufügen und eine Regelung über den Verbleib der Unterlagen (Rückgabe? Vernichtung?) treffen sollen (vgl. Ehlers/Heydemann, DVBl. 1990, S. 1 ff., 8).

Mit diesem Ansatz bin ich mit der Arbeitsgemeinschaft der kommunalen Spitzenverbände Niedersachsens in Verbindung getreten. In einem Gespräch mit deren Vertretern habe ich vorgeschlagen, von dort aus an die niedersächsischen Kommunalverwaltungen bzw. deren Mitglieder in den kommunalen Selbstverwaltungsgremien zu appellieren, Unterlagen mit personenbezogenen Daten sorgsamer zu behandeln, als dies möglicherweise im einen oder anderen Bereich bisher der Fall ist. Die kommunalen Spitzenverbände haben sich bereit erklärt, zur Unterrichtung ihrer Mitglieder ein Rundschreiben zu erarbeiten und dies vor Veröffentlichung mit mir abzustimmen. Darin sollten einerseits Problembewußtsein vermittelt und andererseits konkrete Hinweise bzw. Empfehlungen für die Versendung von Unterlagen mit personenbezogenen Daten, deren Vernichtung bzw. Rückgabemöglichkeiten gegeben werden.

Im Frühjahr 1992 wurden entsprechende Rundschreiben vom Niedersächsischen Städtetag und vom Niedersächsischen Landkreistag verschickt, in denen die abgesprochenen Gesichtspunkte dargestellt wurden.

16.9 Aussiedlerdaten an Betreuungsorganisationen

In der Vergangenheit sind wiederholt Kommunalbehörden mit der Frage an mich herangetreten, ob die Weitergabe von Aussiedler-Daten (insbesondere auch in Listenform) an Betreuungsorganisationen im privaten Bereich zulässig ist.

In Niedersachsen besteht eine großzügige Regelung durch einen — nicht veröffentlichten — Erlaß des Ministeriums für Bundes- und Europaangelegenheiten vom 25. Mai 1981. Ich fordere seit längerem eine klare bereichsspezifische Befugnisnorm. Um einen Überblick über die bundesweite Praxis zu erhalten, habe ich eine Umfrage bei den (alten) Bundesländern durchgeführt. In einigen Ländern werden Anschriftenlisten nicht weitergegeben, offenbar auch, weil kein entsprechendes Bedürfnis gesehen wird. Zum Teil erfolgt eine Datenübermittlung aufgrund einer bereichsspezifischen Rechtsgrundlage. Teilweise werden die Daten mit Einwilligung bzw. unter Beachtung einer Widerspruchsmöglichkeit übermittelt.

Ich habe gegenüber dem Ministerium für Bundes- und Europaangelegenheiten zum Ausdruck gebracht, daß ich nach wie vor eine Regelung für sachdienlich halte, die eine Übermittlung von Aussiedlerdaten an präzise Voraussetzungen knüpft. In diesem Zusammenhang habe ich darauf hingewiesen, daß der Entwurf des künftigen Niedersächsischen Datenschutzgesetzes in § 13 im Gegensatz zu § 11 NDSG wesentliche Einschränkungen für die Übermittlung von personenbezogenen Daten an Stellen außerhalb des öffentlichen Bereiches vorsieht. Meinem Vorschlag, sich schon jetzt an dieser Regelung zu orientieren, ist das Ministerium bisher nicht gefolgt.

16.10 Registrator mißbraucht seine Zugriffsrechte

Ein Registrator des Ordnungsamtes der Landeshauptstadt Hannover mißbrauchte seine Zugriffsrechte auf gespeicherte Daten des Einwohnerwesens, der Kraftfahrtzulassung und des Ordnungswidrigkeitenwesens zum Telefon-

terror gegen Frauen. Durch den Zugang zur Altablage seines Amtes verschaffte er sich zusätzlich Einblick in Paßunterlagen, um so seine Opfer systematisch auszuwählen.

Ich bin dem Vorfall, der in der Presse ein lebhaftes Echo fand, sofort nachgegangen. Dabei stellte sich die Altablage — in nicht beaufsichtigten Kellerräumen untergebracht — als eine Schwachstelle der Datensicherung heraus. Durch gemeinsame Altablage mehrerer Ämter in offenen Regalen war eine zweckgebundene Verwendung nicht zu gewährleisten. Die übrigen von der Stadt getroffenen technischen und organisatorischen Maßnahmen zur Gewährleistung der Zugriffskontrolle waren vom Grundsatz nicht zu beanstanden, wenngleich diesem Mitarbeiter zu weitgehende Rechte eingeräumt waren. Durch verschließbare Behältnisse oder Teilarchive und eine regelmäßige Kontrolle der Protokolldateien wäre dieser Fall vermeidbar gewesen.

17. Natur- und Umweltschutz

17.1 Einsichtsrecht in Umweltakten

Sachliche Informationen sind im Umweltbereich notwendige Voraussetzung für eine Teilhabe an umweltpolitisch relevanten Entscheidungen und Maßnahmen des Staates. Nach dem deutschen Recht haben derzeit in der Regel nur die an einem konkreten Verfahren direkt Beteiligten die Möglichkeit, an Informationen heranzukommen (individueller Rechtsschutz). Es liegt nun eine Richtlinie des Rates der Europäischen Gemeinschaften vor, nach der ab 1. Januar 1993 alle Bürgerinnen und Bürger unabhängig von der konkreten Verfahrensbeteiligung ein Einsichtsrecht in Umweltakten haben. Die Ausgestaltung des Informationszugangsrechts ist Sache der einzelnen Staaten. Der Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit hat den zuständigen Länderressorts einen Referentenentwurf zur Umsetzung der Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt — Umweltinformationsgesetz (UIG) — zugeleitet (vgl. X 17.1). Ich teile die Auffassung des Niedersächsischen Umweltministeriums, wonach in Teilbereichen die Gesetzgebungszuständigkeit bei den Ländern liegt. Das beabsichtigte UIG des Bundes kann daher nur gelten, soweit das Informationszugangsrecht nicht durch Landesgesetz geregelt werden kann und auch geregelt wurde.

Bei der datenschutzrechtlichen Bewertung sind zwei zum Teil gegenläufige Interessen zu berücksichtigen. Auf der einen Seite wird das Recht eines jeden Menschen begründet, Informationen zu erhalten. Auf der anderen Seite kann das Interesse der Betroffenen bestehen, möglichst keine oder wenig personenbezogene Daten zu offenbaren. Oberstes Gebot muß aber die Beachtung des Ziels des Gesetzes sein, den freien Zugang zu Umweltinformationen zu gewährleisten.

Zum Schutz der Betroffenen habe ich im Hinblick auf das Verhältnismäßigkeitsprinzip gefordert, daß die Herausgabe anonymisierter Daten Vorrang haben müsse, sofern dadurch dem Antragsbegehren genügt wird. Auch sollten nur aufbereitete (gesicherte) personenbezogene Angaben weitergegeben werden dürfen. Es kann nicht im Interesse des Zugangsrechts einer Antragstellerin oder eines Antragstellers liegen, wenn eine Vorschrift des Entwurfs die Weitergabe von Angaben über individuelle Verantwortlichkeiten letztlich ausschließt

und wenn z. B. Betriebs- und Geschäftsgeheimnisse besonders geschützt werden. Die Beibehaltung solcher Bestimmungen würde das Zugangsrecht leerlaufen lassen. Für die genannten Fälle halte ich eine Interessenabwägung für sachgerecht. Für die Betroffenen wiederum kann es wichtig sein, die Gründe zu erfahren, die zu einer Auskunftserteilung geführt haben. Ich habe daher eine Regelung vorgeschlagen, nach der die maßgeblichen Gründe für die Auskunftserteilung zu dokumentieren sind. Auch halte ich es für geboten, die Betroffenen unverzüglich über die erteilte Auskunft zu unterrichten.

In meiner Stellungnahme gegenüber dem Umweltministerium habe ich auf die möglichen Gefahren eines Mißbrauchs des Zugangsrechts zu den Umweltinformationen hingewiesen. Meines Erachtens könnte dem dadurch begegnet werden, daß gesetzlich verboten wird, nach dem UIG erhaltene Daten mit Gewinnabsicht zu vermarkten. Für den Fall des Verstoßes hiergegen könnte eine Abführungspflicht der erlangten Gelder oder eine Sanktion vorgesehen werden.

17.2 Niedersächsisches Naturschutzgesetz

Das Niedersächsische Umweltministerium hatte den Entwurf eines Zweiten Gesetzes zur Änderung des Niedersächsischen Naturschutzgesetzes in das Anhörungsverfahren gegeben. Schwerpunktmäßig geht es um den Schutz wertvoller Grünlandflächen und um die Einführung der Verbandsklage. Die im Land Niedersachsen anerkannten Verbände sollen neben einem Klagerecht auch Beteiligungsrechte im Rahmen des Verwaltungsverfahrens eingeräumt bekommen.

Das Umweltministerium hat meine Anregung aufgegriffen, zum Schutz eventuell betroffener Bürgerinnen und Bürger den anerkannten Verbänden im Rahmen ihrer Mitwirkung nur die zur Beurteilung der Auswirkungen auf Natur und Landschaft erforderlichen Unterlagen zu überlassen.

17.3 Niedersächsisches Abfallgesetz

Das Niedersächsische Abfallgesetz enthält datenschutzrechtliche Bestimmungen zum Führen des Gülle-Katasters und des Verzeichnisses der im Lande festgestellten Altablagerungen und Altstandorte (vgl. X 17.2 u. 3). Eine allgemeine Regelung der Datenverarbeitung fehlt jedoch. Dies führt dazu, daß Maßnahmen unter Verwendung von personenbezogenen Daten ohne präzise Rechtsgrundlage durchgeführt wurden und werden. Dies kann nur mit Hilfe des „Übergangsbonus" im Interesse einer funktionsfähigen Umweltverwaltung datenschutzrechtlich hingenommen werden. Das Niedersächsische Umweltministerium hat jetzt eine 2. Novelle zum Niedersächsischen Abfallgesetz vorbereitet. Sachlich geht es im wesentlichen um die Entsorgung und Überwachung von Sonderabfällen, die Sanierung von Altlasten einschließlich Altlastenverzeichnis, Regelungen über ein Wirtschaftsdüngerverzeichnis und — in einem eigenständigen Teil — die Verarbeitung von personenbezogenen Daten.

Das Umweltministerium hat mich frühzeitig an den Vorbereitungen beteiligt. Ich habe im Bereich der Datenerhebung und -übermittlung der Regelung in einer Verordnung zugestimmt und geraten, eine Pflicht zur Protokollierung bzw. Dokumentation der Übermittlungen vorzusehen. Im Bereich der automatisierten Speicherung habe ich namentlich die Nachvollziehbarkeit personenbezogener Daten aus Akten (Aktenrückhalt) gefordert. Dieser Punkt, wie auch die Dokumentation von Übermittlungen, erscheint mir wichtig, weil zu

erwarten ist, daß die Dateien bundes- und EG-weit verknüpft werden. Es muß möglich sein, Daten auch nach mehreren Verarbeitungsschritten auf ihren ursprünglichen Aussagegehalt hin überprüfen zu können. Übermittlungen können aus meiner Sicht nur zulässig sein, wenn im Empfängerland der gleiche Datenschutzstandard gegeben ist wie in Niedersachsen. Weiterhin habe ich auf die Notwendigkeit der Unterrichtung der Betroffenen insbesondere bei Speicherung und Übermittlung und auf das Erfordernis fachspezifischer Löschungsregelungen hingewiesen.

In Anbetracht der zahlreichen Datentransfers im Abfallrecht bleibt nur zu hoffen, daß die 2. Novelle noch in dieser Legislaturperiode verabschiedet wird. Nur so werden die Bediensteten der Umweltverwaltung in die Lage versetzt, ihre Arbeit auf der Grundlage gebotener gesetzlicher Vorschriften durchzuführen.

17.4 Informationen über Rüstungsaltlasten aus Lastenausgleichsakten

Das Ministerium für Bundes- und Europaangelegenheiten trat an mich mit der Bitte heran, eine datenschutzrechtliche Prüfung zur Einsichtnahme in Lastenausgleichsakten für Zwecke der Gefährdungsabschätzung von Rüstungsaltlasten durchzuführen. Das zuständige Niedersächsische Landesamt hatte eine GmbH mit der Vorrecherche über den Standort „X" (Gelände eines früheren Eisenwerkes) beauftragt. Die wesentliche Aufgabe der Vorrecherche bestand im Zusammenstellen von Informationen und Unterlagen über Standort und Firma. Dabei interessierten insbesondere folgende Fragen: Eigentumsverhältnisse und Nutzungsfolge von 1914 bis heute, Betriebsgröße, besonders von 1936 bis 1945, Entsorgung der angefallenen Abfallstoffe bei der Produktion, Art der Produktion, Baubestand. Da die Anlagen dieser Firma während des 2. Weltkrieges stark zerstört wurden, bestand die Vermutung, daß seitens der Firma ein Antrag auf Entschädigung nach den Lastenausgleichsgesetzen gestellt wurde, aus dem sich Hinweise auf den ursprünglichen Gebäudebestand und die Art der Produktion ergeben könnten. Meine Prüfung hatte zum Ergebnis, daß die Einsichtnahme in die entsprechenden Unterlagen des Ausgleichsamtes datenschutzrechtlich nur mit Hilfe des Übergangsbonus zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Abwehr von Gefahren für Leib oder Leben zu rechtfertigen ist.

Dieser Vorgang wie auch weitere Eingaben und ministerielle Anfragen in diesem und ähnlichem Zusammenhang belegen einmal mehr, daß bereichsspezifische gesetzliche Grundlagen in einem Rüstungsaltlastengesetz erforderlich sind. Meine entsprechende Forderung hat das Niedersächsische Umweltministerium aufgegriffen. Im Bundestag wird derzeit der vom Bundesrat eingebrachte Entwurf eines Gesetzes über die Finanzierung der Sanierung von Rüstungsaltlasten in der Bundesrepublik Deutschland beraten (BT-Drs. 12/3257).

17.5 Niedersächsisches Wassergesetz

Das Niedersächsische Wassergesetz (NWG) enthält keine Regelungen zur Verarbeitung von personenbezogenen Daten. Ich habe gegenüber dem Umweltministerium gefordert, angemessene Rechtsgrundlagen im Bereich des NWG zu schaffen, und darauf aufmerksam gemacht, daß der datenschutzrechtliche „Übergangsbonus" die Verarbeitung personenbezogener Daten ohne normenklare Rechtsgrundlage nicht auf unbegrenzte Zeit erlaubt. Das Umweltministerium erwägt nun im Zusammenhang mit der Vorbereitung einer weiteren Novellierung des NWG die Aufnahme bereichsspezifischer Datenverarbeitungsvorschriften.

17.6 Datenverarbeitung zur Überwachung von Indirekteinleitern

Eine für die Erteilung von Genehmigungen nach der Verordnung über die Genehmigungspflicht für das Einleiten von Abwasser mit gefährlichen Stoffen in öffentliche Abwasseranlagen (Indirekteinleiterverordnung) vom 10. Oktober 1990 (Nieders. GVBl. S. 451) zuständige Behörde hatte im Zuge ihrer Überwachungs- bzw. Genehmigungsaufgaben nach der vorgenannten Verordnung die Zahnärztekammer um Übermittlung einer Auflistung der in ihrem Gebiet niedergelassenen Zahnärztinnen und Zahnärzte ersucht. Die bei der Zahnärztekammer vorhandenen Daten unterliegen jedoch der Zweckbestimmung entsprechend dem Kammergesetz für die Heilberufe. Für Datenübermittlungen zu den gewünschten Zwecken blieb somit kein Raum. Eine Datenübermittlung mit Einverständnis der Betroffenen war nicht praktikabel. Mittlerweile hat die Zahnärztekammer alle niedergelassenen Zahnärztinnen und -ärzte über die Genehmigungspflicht der Indirekteinleitung unterrichtet. Die Angehörigen dieser Berufsgruppe müssen sich also selbst bei den zuständigen Behörden melden. Dadurch ist eine Übermittlung nach dem eingangs dargestellten Verfahren entbehrlich.

17.7 Erhebungsbogen zum Abwasserkataster Arztpraxen

Eine Stadt hatte einen Vordruck „Erhebungsbogen zum Abwasserkataster Arztpraxen" erstellt und diesen an alle niedergelassenen Ärztinnen und Ärzte verschickt. Mit diesem Formular sollten Abwassereinleitungen in die öffentliche Kanalisation erfaßt werden. Hiervon versprach sich die Stadt umfassende Erkenntnisse über die Einleitung von Abwasser in ihre Kanalisations- und Abwasseranlagen und eine Reduzierung von Schadstoffen.

Der Vordruck enthielt einen umfangreichen Fragenkatalog, der nach Ansicht einer Einsenderin differenzierte Einblicke in Arbeitsweise, Spezialisierung, Größe, Mitarbeiterzahl und Anzahl der Patienten von Arztpraxen ermöglichte. Der Erhebungsbogen wies datenschutzrechtliche Mängel auf: Er enthielt weder am Anfang einen Hinweis auf die Freiwilligkeit zum Ausfüllen des Formulars noch war aus ihm die Rechtsgrundlage ersichtlich, auf die sich die Maßnahme stützte.

Meine datenschutzrechtlichen Ermittlungen ergaben, daß die Stadt für diesen Zweck den Runderlaß „Abwasserkataster" des Umweltministeriums vom 29. Oktober 1990 herangezogen hat. Der Erlaß erfüllt jedoch — als Verwaltungsvorschrift — nicht die rechtlichen Anforderungen an Eingriffe in das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG geschützte Recht auf informationelle Selbstbestimmung. Das Bundesverfassungsgericht hat in seinem Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 entweder normenklare gesetzliche Grundlagen oder die Einwilligung der Betroffenen verlangt. Aus datenschutzrechtlicher Sicht konnte mangels Rechtsgrundlage die Datenerhebung daher nur mit Einverständnis der Betroffenen erfolgen. Bei vorliegendem Einverständnis hat sich die Datenerhebung zudem am Grundsatz der Erforderlichkeit zu orientieren, d. h. es dürfen nur die Daten erhoben werden, die für die Erfüllung der jeweiligen Aufgabe unerläßlich sind. Die Stadt hat im übrigen mitgeteilt, daß die Daten ausschließlich zum Zwecke der Erstellung des Abwasserkatasters verarbeitet werden und die mit der Erhebung beauftragten Personen auf das Datengeheimnis verpflichtet worden sind. Das mit dem Kataster befaßte Tiefbauamt stelle sicher, daß die Angaben ausschließlich in diesem Amt zur Erstellung des Abwasserkatasters genutzt werden und keine anderen Stellen innerhalb der Stadtverwaltung Zugang zu den Daten erhielten. Dies entspricht dem Grundsatz der Zweckbindung.

Die Stadt hat veranlaßt, den Erhebungsbogen auf „freiwilliges" Ausfüllen umzustellen. Die Maßnahme dieser Stadt sowie die zunehmende Zahl der Kommunen, die zur Beurteilung ihrer Abwassersituation in ihrem Gebiet Abwasserkataster erstellen, zeigte erneut, wie dringend die Schaffung bereichsspezifischer gesetzlicher Grundlagen ist.

17.8 Übermittlung von Daten aus Abwasserkatastern

Ein Abwasserzweckverband, der ein Abwasserkataster erstellt hatte, erkundigte sich nach der datenschutzrechtlichen Zulässigkeit der Übermittlung von Daten aus diesem Kataster an einen Landkreis. Dieser beabsichtigte, die im Abwasserkataster des Zweckverbandes gespeicherten Daten zur Erfüllung seiner Aufgaben nach der Indirekteinleiterverordnung weiterzuverwenden. Ich halte die Datenübermittlung ohne ausreichende bereichsspezifische gesetzliche Grundlage datenschutzrechtlich nur für eine Übergangszeit für hinnehmbar.

18. Bau-, Wohnungs- und Vermessungswesen

18.1 Vollständige Kaufverträge für die Kaufpreissammlung

Jeder Vertrag, durch den sich jemand verpflichtet, Eigentum an einem Grundstück gegen Entgelt oder im Wege des Tausches zu übertragen oder ein Erbbaurecht zu begründen, ist nach § 195 Abs. 1 Baugesetzbuch (BauGB) von der beurkundenden Stelle in Abschrift dem Gutachterausschuß zur Führung der Kaufpreissammlung zu übersenden. Von Notaren kam die Anregung, im Hinblick auf das informationelle Selbstbestimmungsrecht anstelle vollständiger Vertragsabschriften auf einem besonderen Formblatt lediglich die Bezeichnung des Grundstücks nach Gemarkung, Flur- und Flurstücksnummer, die veräußerte Fläche, die Gegenleistung, den Tag der Beurkundung und die Nummer der Urkundenrolle des Notars mitzuteilen. Diese Daten könnten im Einzelfall durch die zusätzlichen Auskunfts-, Einsichts- und Betretungsrechte nach § 197 BauGB im erforderlichen Umfang ergänzt werden.

Das von mir befragte Sozialministerium lehnt eine für ein solches Vorgehen notwendige Änderung des BauGB ab und führt aus, daß der Verfahrensvorschlag die Belange einer „richtigen" Kaufpreissammlung nicht erfüllen könne und zudem unpraktikabel sei. Der Vorschlag verkürzter Vertragsinformationen führe zu Qualitätsverlusten der Kaufpreissammlung und gefährde die Arbeit der Gutachterausschüsse. Die besonderen Zahlungsbedingungen für den Gegenwert eines Kauffalles setzten sich häufig aus unterschiedlichen und unterschiedlich fälligen Leistungen zusammen, die sich nur sehr schwierig in eine (Geld-)Wertangabe umrechnen ließe. Hierzu seien umfassende Marktkenntnisse und Wertermittlungserfahrungen erforderlich. Der Gutachterausschuß mit seinen Fachkräften und der in vielen Fällen gewonnenen Erfahrung sei dazu am besten geeignet.

Ich teile diese Bewertung. Die gesetzliche Offenbarungspflicht gegenüber dem Gutachterausschuß liegt im überwiegenden Allgemeininteresse; der Eingriff in die Rechte der Betroffenen erscheint auch unter den Einschränkungen des § 195 Abs. 2 und 3 BauGB gerechtfertigt und aus datenschutzrechtlicher Sicht akzeptabel.

18.2 Vollständige Kaufverträge an die Gemeinden

Anders als im Falle der Kaufpreissammlung bewerte ich dagegen die bisherige Praxis, daß auch an die Gemeinden und Städte vollständige Abschriften der Kaufverträge geschickt werden. Die Gemeinden erhalten die Verträge als Mitteilung nach § 28 Abs. 1 Satz 1 BauGB, um über die Ausübung des Vorkaufsrechts zu entscheiden. Da das Vorkaufsrecht nur in einem geringen Prozentsatz der Kauffälle überhaupt besteht und es nur in einer noch weitaus geringeren Zahl von Fällen ausgeübt wird, ist die Übermittlung aller Kaufverträge und die Speicherung aller Daten bei den Gemeinden unverhältnismäßig.

Ich empfehle, die in Bayern bereits seit längerem praktizierte und bewährte „Zweistufenlösung" auch in Niedersachsen einzuführen. Danach übersendet der Notar der Gemeinde nicht den gesamten notariellen Kaufvertrag, sondern zunächst nur die für eine solche Grundentscheidung notwendigen Fakten. Erst wenn die Ausübung des Vorkaufsrechts in Betracht kommt, kann die Gemeinde in einem zweiten Schritt die Übermittlung des vollständigen Inhalts des Kaufvertrages verlangen. Diese Anwendung des § 28 Abs. 1 Satz 1 BauGB halte ich für sachgerecht.

18.3 Abbau der Fehlsubventionierung im Wohnungswesen

Auch Niedersachsen plant, die Fehlsubventionierung im Wohnungswesen durch die Einführung einer Fehlbelegungsabgabe abzubauen (LT-Drs 12/4110). Ich begrüße die Absicht, daß hierfür die erforderlichen Auskünfte bei den betroffenen Wohnungsinhabern, also der Mieterin oder dem Mieter, selbst eingeholt werden sollen. Es würde auch keinen datenschutzrechtlichen Bedenken begegnen, wenn der „andere Wohnungsinhaber", also Mitbewohnerin oder Mitbewohner einer Mietwohnung, die erforderlichen Auskünfte gegenüber der zuständigen Stelle gibt (so § 5 des Gesetzes zum Abbau der Fehlsubventionierung und der Mietverzerrung im Wohnungswesen), zumal die niedersächsische Regelung eine gegenseitige Hinweispflicht der Wohnungsinhaber vorsieht.

18.4 Vermietung an nicht-wohnberechtigte Personen

Bei der Vermietung einer der Wohnungsbindung unterliegenden Wohnung an eine Mietpartei, deren Einkommen die festgelegten Grenzen übersteigt, kann eine Ausgleichsabgabe nach den Vorschriften des Wohnungsbindungsgesetzes erhoben werden. Soweit sich die Höhe dieser Ausgleichszahlung nach der Höhe des individuellen Einkommens richtet, werden damit dem Vermieter die Einkünfte der Mietpartei offenbart. Der Vermieter kann aus der Höhe der Ausgleichszahlung Rückschlüsse auf die Höhe des Einkommens seiner Mieterin oder seines Mieters ziehen. Dieser Eingriff in das informationelle Selbstbestimmungsrecht der Mietpartei wäre vermeidbar, wenn die Ausgleichszahlungen direkt bei der nicht-wohnberechtigten Mieterin bzw. dem Mieter und nicht mehr beim verfügungsberechtigten Vermieter erhoben würden. Das Sozialministerium hat auf meine Anregung mitgeteilt, daß die Erörterung der Angelegenheit in der Fachkommission Wohnungsbindungs- und Berechnungsrecht der Arbeitsgemeinschaft der für das Bau-, Wohnungs- und Siedlungswesen zuständigen Minister der Länder ergeben habe, daß eine Rechtsänderung aus „systematischen Gründen" nicht möglich sei. Ich habe daraufhin den Bundesbeauftragten für den Datenschutz gebeten, sich beim Bundesminister für Raumordnung, Bauwesen und Städtebau für eine entsprechende Änderung der gesetzlichen Regelung einzusetzen.

19. Finanzverwaltung

19.1 Kontrollbefugnis des Landesbeauftragten

Erst nach massiver Kritik der Landesbeauftragten für den Datenschutz wurde im Referentenentwurf eines Gesetzes zur Änderung der Abgabenordnung (Stand 11. August 1992) durch eine Neufassung des § 31 b der Abgabenordnung so klargestellt, daß für Landesfinanzbehörden die Kontrollkompetenz der Landesbeauftragten für den Datenschutz gegeben ist. Auch weitere datenschutzrechtliche Anregungen wurden in den Gesetzentwurf eingearbeitet. Die in einer früheren Fassung vorgesehene Verpflichtung für die Finanzbehörden, einen Datenschutzbeauftragten zu bestellen, wurde allerdings bedauerlicherweise nicht übernommen. Auch einige andere Anregungen, wie z. B. die Einschränkung der Offenbarungsbefugnis gegenüber öffentlichen Stellen, eine Erweiterung der Regelungen über die Schweigepflicht öffentlicher Stellen um das Sozialgeheimnis und die ärztliche Schweigepflicht, eine Reduzierung von Daten bei der Mitteilung von festgesetzten Steuermeßbeträgen und eine Klärung der Befugnisse der Steuerfahndung, sind bisher nicht in dem Gesetzentwurf des Bundesministers der Finanzen aufgenommen worden. Nach erneuter Anmahnung beim Bundesminister der Finanzen durch den Bundesbeauftragten für den Datenschutz ist derzeit nicht absehbar, ob die vorgeschlagenen Änderungen aufgenommen werden und wann der Entwurf dem Bundestag zugeleitet werden wird.

Unter Hinweis auf das Steuergeheimnis lehnte ein Finanzamt in einem Beschwerdefall mein Auskunftsbegehren trotz der klaren Regelung in § 24 Abs. 2 in Verbindung mit § 24 Abs. 6 BDSG ab. Die von mir eingeschaltete Oberfinanzdirektion Hannover stellte in einer Verfügung an die Finanzämter vom Mai 1992 klar, daß diese Ablehnung zu Unrecht erfolgte und sich meine Kontrolle auch auf personenbezogene Daten erstreckt, die dem Steuergeheimnis unterliegen. Diese Klarstellung begrüße ich.

Unverständlich ist es dagegen, daß die Finanzämter in Niedersachsen verpflichtet sind, Antwortentwürfe auf Anfragen von mir jeweils vor Absendung der Oberfinanzdirektion vorzulegen. Nach Ansicht des Finanzministeriums ist dies erforderlich; zeitliche Verzögerungen müßten in Kauf genommen werden.

19.2 Verordnungen über Kontrollmitteilungen und Steuerdaten-Abruf

Noch immer fehlt die in § 93 a AO vorgesehene Rechtsverordnung, nach der Behörden verpflichtet werden sollen, zur Sicherung der Besteuerung den Finanzbehörden (Kontroll-)Mitteilungen zu übersenden. Das Niedersächsische Finanzministerium hat sich nunmehr meiner Rechtsauffassung angeschlossen, daß für die Kontrollmitteilungen eine spezielle Rechtsnorm erforderlich ist. Die Behörden wurden angewiesen, bis zum Erlaß der Rechtsverordnung von der Übersendung von Kontrollmitteilungen an die Finanzbehörden Abstand zu nehmen.

Auch eine Steuerdaten-Abrufverordnung wurde noch nicht erlassen. Zur Zeit wird die Erforderlichkeit einer Regelung über den Online-Zugriff der Rechnungsprüfungsbehörden auf Daten der Finanzämter erörtert.

19.3 Datenerhebung durch die Finanzämter

19.3.1 Datenanforderung des Finanzamtes beim Versorgungsamt

Die im X. Tätigkeitsbericht unter Ziffer 19.5 dargestellte Datenanforderung eines Finanzamtes beim Versorgungsamt wird auch vom Finanzministerium für unzulässig gehalten, weil die Voraussetzungen des § 71 Abs. 1 Nr. 3 SGB X für eine Offenbarung von Sozialdaten nicht vorliegen. Die Finanzämter wurden darauf hingewiesen, daß in den Fällen, in denen Schwerbehinderte die für die Weitergewährung der Kfz-Steuerermäßigung erforderlichen Nachweise nicht beibringen, von Auskunftsersuchen an Versorgungsämter abzusehen ist.

19.3.2 Auskunft über die Zahlung von Entschädigungen an Ratsmitglieder

In einem Auskunftsersuchen wurde eine Stadt von einem Finanzamt gebeten, alle in einem Jahr an die Ratsmitglieder gezahlten Entschädigungen namentlich mitzuteilen. Dies war unzulässig, weil gemäß § 93 AO zunächst die Beteiligten um Auskunft zu ersuchen sind. Diese Rechtsauffassung wurde vom Finanzministerium bestätigt; das Finanzamt zog sein Auskunftsersuchen zurück.

19.3.3 Nachweis von Aufwendungen für Fahrten zwischen Wohnung und Arbeitsstätte

Von einem Steuerpflichtigen wurde problematisiert, daß er zum Nachweis für Fahrten zwischen Wohnung und Arbeitsstätte in einem Fahrtenbuch nicht nur die tatsächlichen Fahrten und die Fahrten zwischen Wohnung und Arbeitsstätte explizit aufzeichnen, sondern auch die Privatfahrten unter Angabe von Ziel und Zweck angeben sollte. Die von mir hiergegen auch unter dem Grundsatz der Verhältnismäßigkeit geäußerten Bedenken wurden vom Finanzministerium geteilt. Bei Privatfahrten sind diese Angaben nur in Ausnahmefällen erforderlich.

19.3.4 Aufbewahrung/Rücksendung von Spendenbescheinigungen

Ich teile die von einem Steuerbürger geäußerte Befürchtung, daß durch die Aufbewahrung von Spendenbescheinigungen in den Steuerakten Rückschlüsse auf die soziale, religiöse oder politische Gesinnung der Betroffenen gezogen werden können. Bei meinen Bemühungen um Verfahrensänderung zeichnet sich ab, daß zukünftig Spendenbescheinigungen nur noch in Ausnahmefällen zu den Akten genommen werden sollen. Eine endgültige Entscheidung wird nach Abstimmung mit dem Landesrechnungshof getroffen werden.

19.4 Ausstellung von Lohnsteuerkarten für Gefängnisinsassen

In einigen Bundesländern wird bei Gefängnisinsassen, die unter der Anschrift einer Justizvollzugsanstalt (JVA) gemeldet sind, oder bei ehemaligen Gefangenen, die am Stichtag der Lohnsteuerkartenausgabe unter einer solchen Anschrift gemeldet waren, als Wohnanschrift auf der Lohnsteuerkarte grundsätzlich die JVA-Anschrift eingetragen. Dadurch erhalten das Finanzamt und ein späterer Arbeitgeber Kenntnis von dem JVA-Aufenthalt. Diese bedenkliche

Praxis wird in Niedersachsen nicht geübt. Bereits seit 1989 wird in einer jährlichen Rundverfügung der Oberfinanzdirektion Hannover darauf aufmerksam gemacht, daß die unter der Anschrift der JVA gemeldeten Gefängnisinsassen in geeigneter Weise darauf hinzuweisen sind, daß sie während ihrer Haft auf die Ausstellung einer Lohnsteuerkarte verzichten können. Die (nachträgliche) Ausstellung einer Lohnsteuerkarte kann dann nach der Haftentlassung beantragt werden. Hierbei wird dann als Wohnanschrift die neue Meldeadresse eingetragen.

19.5 Ausstellung von Lohnsteuerkarten bei Wechsel des Arbeitgebers

Bei einem Wechsel des Arbeitgebers innerhalb eines Kalenderjahres werden unnötigerweise die auf der Lohnsteuerkarte eingetragenen personenbezogenen Daten, z. B. der frühere Arbeitgeber, der von diesem gezahlte Lohn sowie eventuelle Arbeitsunterbrechungszeiträume, dem neuen Arbeitgeber bekannt. Ich habe dem Finanzministerium vorgeschlagen, daß eine zweite Lohnsteuerkarte mit derselben Steuerklasse, einem Gültigkeitsvermerk und einem Hinweis ausgestellt wird. Dieser Hinweis sollte beinhalten, daß eine ordnungsgemäße Besteuerung eines eventuellen sonstigen Bezuges und auch ein Lohnsteuer-Jahresausgleich durch den neuen Arbeitgeber nicht erfolgen kann. Das Finanzministerium hat meinen Vorschlag mit der Begründung abgelehnt, daß eine entsprechende Änderung des Einkommensteuergesetzes zu einer weiteren Komplizierung des Steuerrechtes führen würde.

19.6 Hinzuziehung von Zeugen bei Wohnungsdurchsuchungen in Abwesenheit des Vollstreckungsschuldners

In einigen Bundesländern sollen künftig Wohnungsdurchsuchungen in Abwesenheit des Vollstreckungsschuldners nicht mehr wie bisher mit zwei Vollziehungsbeamten, sondern unter Hinzuziehung von zwei Privatpersonen aus der Nachbarschaft als Zeugen durchgeführt werden. Ich habe erhebliche datenschutzrechtliche Bedenken geltend gemacht.

Im Bereich der niedersächsischen Finanzverwaltung wird, wenn der Vollziehungsbeamte den Vollstreckungsschuldner trotz wiederholter Versuche und Terminankündigung nicht antrifft, zunächst geprüft, ob andere Vollstreckungsmöglichkeiten bestehen. Erst wenn dieses nicht der Fall ist, werden Wohnungen durchsucht. Hierbei werden in der Regel Gemeinde- oder Polizeibeamte oder auch Finanzamts-Angehörige als Zeugen hinzugezogen. Nur in wenigen Ausnahmefällen werden Privatpersonen in Anspruch genommen. In diesen Ausnahmefällen erachte ich das Verfahren für datenschutzrechtlich hinnehmbar.

19.7 Zeichnungsrecht in den Finanzämtern

Die im IX. Tätigkeitsbericht unter Ziffer 19.9 dargestellte Problematik des Zeichnungsrechtes der Vorsteherin oder des Vorstehers eines Finanzamtes in Steuerangelegenheiten der eigenen Bediensteten wurde nochmals mit dem Finanzministerium erörtert. Dem Anliegen der Amtsangehörigen, ihre Steuerdaten Vorgesetzten nicht offenbaren zu müssen, wird nun Rechnung getragen. Allen Finanzamtsangehörigen wird es nunmehr ohne nähere Begründung ermöglicht, im Wege der Zuständigkeitsvereinbarung ein anderes Finanzamt mit ihren steuerlichen Angelegenheiten zu befassen. Dies ist zwar

eine Verbesserung der bisherigen Praxis, gleichwohl wäre es zu begrüßen, wenn § 27 AO so gestaltet würde, daß das entsprechende Recht der Finanzamtsangehörigen auch gesetzlich abgesichert wäre.

20. Sozialwesen

20.1 Krankenversichertenkarte

Nach § 291 SGB V sollten die Krankenkassen zum 1. Januar 1992 für alle Versicherten eine Krankenversichertenkarte ausstellen, die den Krankenschein ersetzt. Diese Karte darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen im Rahmen der kassen- oder vertragsärztlichen Versorgung sowie für die Abrechnung mit den Leistungserbringern verwendet werden.

Zugleich legt das Gesetz abschließend die Daten fest, die diese Karte enthalten darf. Es sind dies: Bezeichnung der ausstellenden Krankenkasse, Familienname und Vorname der Versicherten, Geburtsdatum, Anschrift, Krankenversichertennummer, Versichertenstatus, Tag des Beginns des Versicherungsschutzes und bei befristeter Gültigkeit der Karte das Datum des Fristablaufs. Die Einführung der Karte hat sich wohl infolge technischer Probleme und mangelnder Akzeptanz seitens der Ärztinnen und Ärzte verzögert. Die Spitzenverbände der Kassenärzte und der Krankenkassen haben nunmehr angekündigt, die Krankenversichertenkarte zum 1. Juli 1993 in einigen Regionen in Gestalt einer elektronischen Chipkarte einführen zu wollen. Chipkarten haben aus Sicht der Spitzenverbände gegenüber Magnetstreifenkarten den Vorteil, daß über die Grunddaten hinaus z. B. auch Verschreibungen, Befunde, Berichte, Gutachten, Krankenhausgeschichten gespeichert werden können.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung am 1./2. Oktober 1992 hierzu festgestellt, daß wegen der wachsenden Automatisierung bei allen Institutionen des Gesundheitswesens und der Erweiterung des Anteils maschinenlesbarer Datenträger eine Speicherung auf einer Chipkarte als elektronische Krankenversicherungskarte auf die gesetzlich festgelegten Grunddaten beschränkt bleiben muß und nicht auf Gesundheitsdaten ausgedehnt werden darf. Eine technische Sicherung dieser Beschränkung ist zu gewährleisten. In Niedersachsen wird nach Mitteilung der Kassenärztlichen Vereinigung Niedersachsen (KVN) der Modellversuch mit der Chipkarte nicht durchgeführt.

20.2 Medizinischer Dienst der Krankenversicherung (MDK)

Der Medizinische Dienst der Krankenversicherung ist der medizinische Beratungs- und Gutachterdienst der Krankenkassen. Nach dem Willen des Gesetzgebers (§ 275 Abs. 1 bis 4 SGB V) beauftragen die Krankenkassen für die Durchführung von Verwaltungsverfahren (§ 8 SGB X), die des medizinischen Sachverstandes bedürfen, den Medizinischen Dienst der Krankenversicherung. Rechtliche Außenbeziehungen zu den Versicherten und den Leistungserbringern entstehen dabei nur bei den Krankenkassen und nicht beim MDK. Die Krankenkassen bleiben auch dann „Herr" des Verwaltungsverfahrens, wenn sie den MDK einschalten. Allgemein gilt dies ebenso wie für die Aufklärung des Versicherten bezüglich seines Widerspruchsrechts nach § 277

Abs. 1 Satz 2 SGB V. Nach dem Wortlaut dieser Vorschrift ist der Begriff des Leistungserbringers nicht mit dem des Leistungsträgers gleichzusetzen. Aus der Fassung anderer SGB-Bestimmungen geht hervor, daß die Krankenkassen eindeutig als Leistungsträger im Sinne des SGB zu definieren sind. Insofern ist es zulässig, daß gem. § 277 Abs. 1 SGB V eine gutachterliche Stellungnahme der Krankenkasse übersendet wird.

Im Gegensatz zur Mitteilungspflicht gegenüber den Krankenkassen besteht gem. § 277 Abs. 1 Satz 2 SGB V seitens der Versicherten ein Widerspruchsrecht gegen die Mitteilung über den Befund an die Leistungserbringer, jedoch nicht gegen die Mitteilung des Ergebnisses der Begutachtung. Die Krankenkassen sind verpflichtet, den Versicherten auf die mit der Einladung zur sozialmedizinischen Beratung und Begutachtung verbundenen Mitwirkungspflichten und Widerspruchsrechte aufmerksam zu machen. Die Arbeitsgemeinschaft der Verbände der gesetzlichen Krankenkassen Niedersachsen hat mittlerweile den Krankenkassen empfohlen, die Versicherten in geeigneter Weise über die Widerspruchsmöglichkeiten aufzuklären.

20.3 Anforderung von Krankenhaus-Entlassungsberichten durch die Krankenkassen

In mehreren Eingaben ging es um die Frage, ob es zulässig ist, daß Krankenhaus-Entlassungsberichte an Krankenkassen übersandt werden. § 301 SGB V, der die Mitteilungspflichten und -befugnisse der Krankenhäuser regelt, sagt hierüber nichts aus. Deshalb haben sich die Spitzenverbände der gesetzlichen Krankenversicherung an das Bundesministerium für Arbeit und Sozialordnung (jetzt Bundesministerium für Gesundheit) gewandt. Ziel dieser Initiative ist es, den Katalog des § 301 SGB V zu erweitern.

Bis zu einer ausdrücklichen Regelung durch den Gesetzgeber halte ich die Anforderung von Krankenhaus-Entlassungsberichten unter Berücksichtigung des § 284 SGB V, der die Art der vom Krankenhaus zu verarbeitenden Daten genau beschreibt, für zulässig. Die Krankenkasse kann also unter strenger Beachtung des Verhältnismäßigkeitsgrundsatzes für Zwecke der Krankenversicherung und einem im einzelnen in § 284 SGB V genannten Zweck den jeweiligen Krankenhaus-Entlassungsbericht anfordern. Dies kann gem. § 284 Abs. 1 Nr. 4 zur Prüfung der Leistungspflicht, der Gewährung von Leistungen an Versicherte und damit auch zur versichertengerechten Aufklärung, Beratung und Auskunft geschehen. Die Notwendigkeit, den Entlassungsbericht anzufordern, ergibt sich für eine Kasse beispielsweise dann, wenn nach der Entlassung die weitere Vorgehensweise und einzuleitende Maßnahmen wie medizinische/berufliche Reha-Maßnahmen, Ernährungsberatung, Reha-Sport und andere ergänzende Leistungen zur Rehabilitation beurteilt werden sollen.

In der Regel wird die Kasse das Krankenhaus darum bitten, den Bericht unmittelbar an den Medizinischen Dienst der Krankenversicherung (MDK) zu senden. Der MDK berät die jeweilige Kasse (§ 275 SGB V). Dies führt dazu, daß Mitarbeiterinnen und Mitarbeiter einer Kasse den Bericht nicht zu Gesicht bekommen. Gleichwohl stehen dem MDK die für die Beratung bzw. Begutachtung notwendigen Unterlagen zur Verfügung.

Die Niedersächsische Krankenhausgesellschaft e. V. hat hierzu in einem Rundschreiben festgestellt, daß die Herausgabe des Entlassungsberichts — ohne Einverständnis der Patienten — einen Verstoß gegen die ärztliche Schweigepflicht darstellt. Dem MDK sei jedoch gem. § 276 SGB V Einsicht in die Krankenunterlagen zu gewähren. Das Krankenhaus solle bei Tätigwerden des MDK darauf bestehen, daß das gesetzliche Verfahren eingehalten

wird. Das bedeutet, daß dem MDK keine Unterlagen zugesandt werden. Er muß zur Einsichtnahme in das Krankenhaus kommen. Nach Auffassung der Niedersächsischen Krankenhausgesellschaft ist es ein Verstoß gegen die ärztliche Schweigepflicht, wenn die Krankenkassen für den MDK Entlassungsberichte anfordern. Dies entspricht auch meiner Auffassung.

In einem anderen Fall hat der Kostenträger (Landesversicherungsanstalt) einen Erklärungsvordruck zum ärztlichen Entlassungsbericht entwickelt. Hier sollen Patientinnen und Patienten ankreuzen, ob sie damit einverstanden sind, daß der vollständige ärztliche Entlassungsbericht der Krankenkasse, dem behandelnden Arzt, und soweit vom MDK eine Untersuchung in den letzten 12 Monaten vor Beginn der Heilbehandlung stattgefunden hat, auch diesem übersandt werden darf oder nicht.

Meines Erachtens ist diese Einverständniserklärung, die routinemäßig in jedem Fall ausgefüllt wird, problematisch. Nur dann, wenn die Krankenkasse im Einzelfall aufgrund der übersandten „Kurzfassung des Entlassungsberichts" zu der Auffassung gelangt, daß der vollständige Entlassungsbericht zur Aufgabenerfüllung erforderlich ist, sollte ein Einverständnis herbeigeführt werden. Eine vorgezogene Einverständniserklärung führt dazu, daß durchweg vollständige Entlassungsberichte an die Krankenkassen übermittelt werden. Die Patientin bzw. der Patient wird, um keine nachteiligen Rechtsfolgen zu erleiden, in der Regel zustimmen, obwohl die Kenntnis des vollständigen Entlassungsberichts für die Krankenkassen nicht erforderlich ist. Dies ist aus meiner Sicht datenschutzrechtlich bedenklich. Zudem hat der Gesetzgeber durch die Vorschrift des § 301 SGB V entschieden, daß in der Regel keine vollständigen Entlassungsberichte erforderlich sind. Diese gesetzliche Regelung wird durch das beschriebene Verfahren unterlaufen. Auch die Übersendung einer Kopie der „Erklärung zum ärztlichen Entlassungsbericht" an die Krankenkassen in den Fällen, in denen Versicherte der Übersendung des vollständigen Entlassungsberichts an die Krankenkasse widersprochen haben, halte ich für unzulässig. Ich sehe hierfür weder ein Erfordernis noch eine Rechtsgrundlage.

Was die Übermittlung der vollständigen Entlassungsberichte an den MDK angeht, so ist aus §§ 275, 276 SGB V zu entnehmen, daß die Krankenkassen verpflichtet sind, dem Medizinischen Dienst die für die Beratung und Begutachtung erforderlichen Unterlagen vorzulegen. Unterlagen, die die oder der Versicherte über die Mitwirkungspflicht nach §§ 60 und 65 SGB I hinaus der eigenen Krankenkasse freiwillig überlassen hat, dürfen an den MDK nur weitergegeben werden, soweit die Versicherten eingewilligt haben. Wegen dieser gesetzlichen Bestimmung halte ich es für bedenklich, daß die Versicherten generell eine Einverständniserklärung unterschreiben sollen. Vielmehr müßte im Einzelfall seitens der Krankenkasse geprüft werden, ob eine Übermittlung an den MDK erforderlich ist.

Die betroffene LVA hat mir hierzu mitgeteilt, daß das Formular „Erklärung zum ärztlichen Entlassungsbericht" in Kürze geändert wird. Künftig wird von den Versicherten zum Zeitpunkt ihrer Entlassung aus der stationären Heilbehandlung keine vorgezogene Einverständniserklärung für eine eventuelle Übersendung des Entlassungsberichts an die Krankenkasse verlangt. Die Krankenkassen sollen aber Kenntnis erhalten, wenn Versicherte auch der Übermittlung der Kurzfassung des Entlassungsberichts an die Krankenkasse widersprochen haben. Die Zustimmung der Versicherten zur Übersendung des vollständigen Entlassungsberichts an den MDK, wenn dieser die stationäre Heilbehandlung angeregt hat, wird künftig nicht mehr gefordert. Die Krankenkasse wird deshalb im Einzelfall zu prüfen haben, ob eine Übermittlung des Entlassungsberichts an den MDK erforderlich ist.

20.4 Amtshilfeersuchen an Krankenkassen in Vollstreckungsangelegenheiten

Eine Kommune teilte mir mit, daß Krankenkassen sich unter Hinweis auf § 67 ff. SGB X weigern, den Vollstreckungsbehörden Auskünfte über die Anschrift und den Arbeitgeber von Schuldnern zu erteilen, und bat mich um eine datenschutzrechtliche Bewertung.

§ 68 Abs. 1 Satz 1 SGB X läßt die Offenbarung von Namen und Anschrift des derzeitigen Arbeitgebers im Rahmen der Amtshilfe zu, soweit kein Grund zu der Annahme besteht, daß dadurch schutzwürdige Belange der Betroffenen beeinträchtigt werden. Letzteres ist bei einer Offenbarung zur Vollstreckung öffentlicher Geldforderungen — soweit es sich nicht um Bagatellbeträge handelt — regelmäßig nicht der Fall. Nachteile, die ein Schuldner als Folge der Offenbarung erleidet, muß er auf sich nehmen. Seine Interessen sind insoweit nicht als schutzwürdig anzusehen, denn die Rechtsordnung verpflichtet ihn, Forderungen zu begleichen und ggf. Vollstreckungsmaßnahmen zu dulden, wenn er seine Zahlungsverpflichtungen nicht erfüllt. Der Gesetzgeber ist deshalb — wie sich den parlamentarischen Beratungen zum Sozialgeheimnis entnehmen läßt — davon ausgegangen, daß Auskünfte der SGB-Stellen für Vollstreckungsfälle grundsätzlich zulässig sein sollen.

Eine Pflicht zur Auskunftserteilung besteht jedoch nicht, wenn sich die ersuchende Stelle die Angaben auf andere Weise beschaffen kann (§ 68 Abs. 1 Satz 2 SGB X). Das Subsidiaritätsprinzip verlangt, daß zunächst andere Kenntnismöglichkeiten genutzt werden, bevor das Sozialgeheimnis durchbrochen wird. Die ersuchende Stelle muß demnach einen größeren Verwaltungsaufwand und etwaige zeitliche Verzögerungen hinnehmen. Bei der Beurteilung der Frage, ob die Daten auf andere Weise ermittelt werden können, ist auch zu berücksichtigen, welche Belastungen sich hierdurch für die Betroffenen ergeben.

Ich hielte es für unangemessen, wenn eine Offenbarung von Arbeitgeberdaten in Vollstreckungsfällen mit dem Argument abgelehnt würde, die Vollstreckungsbehörde könne den Schuldner zur Abgabe einer eidesstattlichen Versicherung über seine Vermögensverhältnisse zwingen, um auf diese Weise den Arbeitgeber in Erfahrung zu bringen. Die Abgabe einer eidesstattlichen Versicherung führt zur Aufnahme des Schuldners in das Schuldnerverzeichnis. Da in dieses Verzeichnis ohne weiteres Einsicht genommen und über seinen Inhalt Auskunft verlangt werden kann (§ 915 Abs. 3 ZPO), belastet eine eidesstattliche Versicherung den Schuldner in einschneidender Weise. Aus diesem Grunde steht nach meiner Auffassung das Subsidiaritätsprinzip des § 68 Abs. 1 Satz 2 SGB X einer Offenbarung von Arbeitgeberdaten in den angesprochenen Fällen nicht entgegen.

20.5 Mitglieder von Zulassungsausschüssen

Eine Krankenkasse teilte mir mit, daß einer ihrer Geschäftsführer Mitglied eines Zulassungsausschusses ist. In diesem Zulassungsausschuß werden u. a. leitende Krankenhausärztinnen und -ärzte ermächtigt, an der kassenärztlichen Versorgung teilzunehmen. Gegen einen solchen Krankenhausarzt hat die Staatsanwaltschaft ein Verfahren wegen des Verdachts des Betruges eingeleitet. Gegenüber der Staatsanwaltschaft haben sich die beteiligten Ärzte auf ihre ärztliche Schweigepflicht berufen. Nunmehr begehrte die Kriminalpolizei von dem Geschäftsführer der Krankenkasse Auskünfte.

Es geht hier um die Frage, ob Informationen über Kassenärztinnen und -ärzte, über die die kasssenärztlichen Vereinigungen, Zulassungsausschüsse usw. ver-

fügen, Sozialgeheimnisse im Sinne des § 35 SGB I darstellen. Wenn dies so wäre, würde sich das Vorliegen einer Offenbarungsbefugnis nach den § 68 ff. SGB X richten. Aus diesen Vorschriften ergibt sich aber keine Offenbarungsbefugnis. Insbesondere ist § 69 Abs. 1 SGB X nicht einschlägig, weil das staatsanwaltschaftliche Ermittlungsverfahren noch kein gerichtliches Verfahren ist und darüber hinaus ein Zusammenhang mit der Erfüllung gesetzlicher Aufgaben zweifelhaft sein kann. Es stünde der Staatsanwaltschaft frei, einen gerichtlichen Beschluß nach § 73 Nr. 2 SGB X zu beantragen. Ein solcher Beschluß dürfte allerdings nur eine Offenbarung von Daten anordnen, die der Staatsanwaltschaft regelmäßig bereits bekannt sein dürften.

Ich bin jedoch gemeinsam mit dem Niedersächsischen Sozialministerium der Auffassung, daß es sich hier nicht um Sozialdaten handelt, da die Ärztinnen und Ärzte nicht Empfänger von Sozialleistungen sind und Angaben über diese auch in keinem direkten Zusammenhang mit der Inanspruchnahme von Sozialleistungen stehen. Insofern fallen die von der Kriminalpolizei bzw. Staatsanwaltschaft über den betreffenden leitenden Krankenhausarzt erbetenen personenbezogenen Daten nicht unter die Vorschriften des Sozialdatenschutzes.

20.6 Organmitglieder der Krankenkassen

Der Datenschutzbeauftragte einer AOK hat mich um einen datenschutzgerechten Lösungsvorschlag des von ihm wie folgt beschriebenen Problems gebeten: Die Mitglieder des Vorstandes auf der Versichertenseite sind — überwiegend freiwillig — bei der AOK versichert. Sie haben nach der Satzung über Anstellung, Beförderung, Versetzung in den Ruhestand, Kündigung oder Entlassung von dienstordnungsmäßigen Angestellten und Einstellung, Höhergruppierung und Kündigung von Tarifangestellten ab Vergütungsgruppe Vb BAT sowie über die Ausbildungsverträge zu entscheiden. Sämtliche Bediensteten der AOK (einschl. der Geschäftsführerinnen bzw. der Geschäftsführer) können Einsicht in die Versicherungs- und Leistungsdaten der Vorstandsmitglieder auf der Versichertenseite nehmen. Dies gilt nicht für die Mitglieder auf der Arbeitgeberseite im Vorstand, weil diese in der Regel nicht Mitglied der AOK sind. Die Mitglieder des Vorstandes auf der Versichertenseite begehren Datenschutz für ihre Daten. Sie wünschen, daß ihre Versicherungs- und Leistungsdaten im EDV-Verfahren ebenso wie bei Bediensteten der AOK gesperrt werden und die nötige Sachbearbeitung für ihre Leistungsanträge von einer kundigen Mitarbeiterin bzw. einem Mitarbeiter ihres Vertrauens durchgeführt wird (§ 284 Abs. 4 SGB V). Der Geschäftsführer der AOK möchte diesem Begehren nicht nachkommen.

Das Niedersächsische Sozialministerium vertritt zu diesem Problem folgende Auffassung: § 284 Abs. 4 SGB V stellt eine Schutzvorschrift dar, die verhindern soll, daß Personen, die mit kasseninternen Personalentscheidungen befaßt sind, Einblick in die Versicherungs- und Leistungsdaten der Mitarbeiterinnen und Mitarbeiter der Kasse nehmen können. Dabei soll ausgeschlossen sein, daß derartige Personalentscheidungen durch die Kenntnis solcher Daten in unzulässiger Weise beeinflußt werden könnten. Eine Vorschrift, die den speziellen Schutz von Vorstandsmitgliedern vor einer Einblicknahme von Kassenbediensteten in ihre Versicherungs- und Leistungsdaten sicherstellt, besteht nicht. Ein dem besonderen Schutzgedanken des § 284 Abs. 4 SGB V entsprechendes besonderes Schutzbedürfnis der Vorstandsmitglieder wird vom Gesetzgeber offenbar nicht gesehen; vielmehr wird offenbar die Beachtung der generellen Schutzvorschrift des § 284 Abs. 3 SGB V auch gegenüber Vorstandsmitgliedern für ausreichend gehalten. Eine analoge Anwendung des § 284 Abs. 4 SGB V auf Vorstandsmitglieder komme daher nicht in Betracht.

Dieser rechtlichen Bewertung der gegenwärtigen Rechtslage kann ich mich nicht verschließen. Ich würde es jedoch begrüßen, wenn bei Versicherungs- und Leistungsdaten von Vorstandsmitgliedern in gleicher Weise verfahren würde wie bei Daten von Kassenmitarbeiterinnen und -mitarbeitern.

20.7 Versorgungsverwaltung

Ein Petent rügte in seiner Eingabe die Verletzung datenschutzrechtlicher Bestimmungen durch ein Versorgungsamt. Er hatte die Feststellung des Nachteilsausgleichs „H" nach dem Schwerbehindertengesetz mit der Begründung beantragt, daß sich sein Gesundheitszustand rapide verschlechtert habe. In dem Antrag wurde auf verschiedene Ärzte verwiesen, bei denen der Petent in Behandlung war. Das Versorgungsamt zog daraufhin Befundberichte dieser Ärzte ein. Gegen diese Beiziehung der ärztlichen Unterlagen ohne sein Einverständnis wandte sich der Petent.

Das Versorgungsamt war zur Beiziehung der vorerwähnten Befundberichte nach Maßgabe des § 12 Abs. 2 Satz 2 des Verwaltungsverfahrensgesetzes der Kriegsopferversorgung, das gem. § 4 Abs. 1 des Schwerbehindertengesetzes auch für das Feststellungsverfahren nach dem Schwerbehindertengesetz anzuwenden ist, befugt. An dieser Stelle ist darauf hinzuweisen, daß mit dieser Befugnis eine korrespondierende Auskunftsverpflichtung der Ärzte nach Maßgabe des § 100 SGB X einhergeht.

Eine wirksame Einwilligung im Sinne dieser vorerwähnten Normen in die späterhin gerügte Beiziehung der Arztberichte lag vor.

Diese Vorgehensweise entspricht jedoch nicht ohne weiteres der gängigen Verwaltungspraxis in den Versorgungsämtern. Die Versorgungsämter sind bei Stellung formloser Neufeststellungsanträge nach dem Schwerbehindertengesetz gehalten, eine aktuelle, d. h. ausdrückliche Schweigepflichtsentbindung beizuziehen, um eventuellen Rügen bezüglich der Verletzung datenschutzrechtlicher Normen von vornherein die Grundlage zu entziehen. Im Falle der Verweigerung der Entbindungserklärung könnten die Neufeststellungsanträge gem. §§ 60 Abs. 1 Satz 1 Nr. 1, 66 Abs. 1, 3 SGB I ablehnend beschieden werden. Das Landesversorgungsamt Niedersachsen hat die Versorgungsämter hierauf nochmals hingewiesen.

Aus diesen Gründen erschien es dem Landesversorgungsamt Niedersachsen in diesem Einzelfall opportun, den Petenten zum Zwecke der Klarstellung und unter Hinweis auf die im Weigerungsfall zu besorgenden verfahrensrechtlichen Konsequenzen um Abgabe einer ausdrücklichen Entbindungserklärung zu bitten, wobei im Weigerungsfall die beigezogenen Befundberichte aus den Akten zu entfernen und zu vernichten wären.

In einer anderen Angelegenheit beauftragte ein Versorgungsamt einen Außengutachter, der kein Bediensteter der Versorgungsverwaltung ist, mit der Durchführung der Untersuchung und Begutachtung. Ihm wurden zu diesem Zweck Akten übersandt. Bei der postalischen Einbestellung zum Untersuchungstermin durch den Arzt war eine den Schwerbehindertenakten vorgeheftete Betreff-Etikette, die — jeweils in größerer Zahl gefertigt — neben der postalischen Adresse das Aktenzeichen sowie Geburtsdatum aufweisen und allein im internen Dienstgebrauch Verwendung finden sollte, als postalischer Adressenaufkleber verwandt worden. Die hier erfolgte bestimmungswidrige Verwendung der Betreff-Etikette war auf ein Versehen des bei dem Arzt beschäftigten Personals zurückzuführen. Das Landesversorgungsamt hat die Versorgungsämter angewiesen, entsprechende Vorkehrungen zu treffen, damit vergleichbare Vorkommnisse in Zukunft vermieden werden.

20.8 Förderung von Dauerarbeitsplätzen

Ein Arbeitgeber hat mich gefragt, inwieweit es mit dem informationellen Selbstbestimmungsrecht zu vereinbaren ist, wenn bei schwer vermittelbaren Arbeitslosen Merkmale wie „fehlender beruflicher Abschluß, gesundheitliche Einschränkung, 50 Jahre und älter, frühere Straffälligkeit oder Suchtgefährdung" mitgeteilt werden müßten. Insbesondere die Kriterien „frühere Straffälligkeit und Suchtgefährdung" stigmatisieren nach seiner Auffassung diese Arbeitslosen.

Nach den Richtlinien über die Gewährung von Zuwendungen zur Förderung von Dauerarbeitsplätzen in Sozialen Betrieben (RdErl. des Niedersächsischen Sozialministeriums vom 11. September 1991) wird die Schaffung von Dauerarbeitsplätzen in Sozialen Betrieben, die für die Produktion von Gütern oder für die Erstellung von Dienstleistungen Langzeitarbeitslose und sonstige schwer vermittelbare Arbeitslose sozialversicherungspflichtig beschäftigen, gefördert. Im Rahmen dieser Förderung kann u. a. ein Zuschuß zu den Personalausgaben für unbefristet beschäftigte Langzeitarbeitslose und schwer vermittelbare Arbeitslose gewährt werden. Sowohl für die grundsätzliche Förderung als auch für den als Individualförderung ausgestalteten Lohnkostenzuschuß müssen auf seiten der Beschäftigten die Kriterien Langzeitarbeitslosigkeit oder Schwervermittelbarkeit gem. Nr. 2.1 Abs. 3 der Richtlinie erfüllt sein. Danach müssen Langzeitarbeitslose länger als ein Jahr beim Arbeitsamt arbeitslos gemeldet sein. Bei schwer vermittelbaren Arbeitslosen haben mindestens zwei Merkmale, wie z. B. fehlender beruflicher Abschluß, gesundheitliche Einschränkung, 50 Jahre und älter, frühere Straffälligkeit oder Suchtgefährdung, vorzuliegen.

Bei der Beantragung der Zuschüsse zu den Personalausgaben der unbefristet beschäftigten Langzeitarbeitslosen und Schwervermittelbaren ist in den Antragsunterlagen für jede Person ein Personalbogen vorgesehen. Auf diesem Personalbogen war bisher neben der Angabe der individuellen Daten, die für die Ermittlung der Förderhöhe notwendig sind, ein Nachweis über die Gründe der Schwervermittelbarkeit zu erbringen. Weiterhin war vorgesehen, daß der Beschäftigte, für den die Förderung beantragt werden sollte, die Richtigkeit dieser Angaben bestätigte und sich mit der Weitergabe der Daten einverstanden erklärte.

Wegen meiner datenschutzrechtlichen Bedenken hat das Niedersächsische Sozialministerium zwischenzeitlich den Personalbogen für unbefristet beschäftigte Langzeitarbeitslose bzw. Schwervermittelbare dahingehend geändert, daß der Arbeitgeber mit Bezug auf die Förderrichtlinien generell erklärt, daß Schwervermittelbarkeit vorliegt. Die bisher notwendigen Einzelangaben entfallen. Zudem hat das Sozialministerium die Bezirksregierungen angewiesen, auf den schriftlichen Nachweis dieser Merkmale zu verzichten und das Vorliegen der Voraussetzung ggf. in Gesprächen mit dem sozialen Betrieb und bei der Verwendungsnachweisprüfung nachzuvollziehen.

20.9 Ausweis für Arbeit und Sozialversicherung aus der Ex-DDR

Ein Bürger hat hat bei mir angefragt, ob es zur Aufgabenerfüllung einer Landesversicherungsanstalt (LVA) erforderlich sei, den vollständigen Ausweis für Arbeit und Sozialversicherung der ehemaligen DDR vorzulegen. Aus diesem Ausweis ergeben sich nicht nur die Arbeitsrechts- und Sozialversicherungsverhältnisse, sondern auch ambulante und stationäre Heilbehandlungen und Angaben über Röntgengroßaufnahmen und Schirmbilder der Brustorgane sowie eventuelle Angaben über Tauglichkeitsuntersuchungen für Kraftfahrer und bestimmte Berufe.

Versicherte sind nach § 286 e SGB VI in diesem Fall berechtigt, in einer beglaubigten Abschrift des vollständigen Ausweises für Arbeit und Sozialversicherung oder von Auszügen dieses Ausweises die Daten unkenntlich zu machen, die für den Träger der Rentenversicherung nicht erforderlich sind, und diese Abschrift dem Träger der Rentenversicherung als Nachweis vorzulegen. Diese Regelung gilt auch für sonstige Beweismittel im Sinne des § 29 Abs. 4 SGB X.

Die Regelung berechtigt aber nicht dazu, die Daten im Original des Ausweises für Arbeit und Sozialversicherung unkenntlich zu machen. Für den Träger der Rentenversicherung sind insbesondere die Zeiträume der versicherungspflichtigen Beschäftigung, die Höhe der jeweils erzielten Arbeitsentgelte, die Anschriften der einzelnen Arbeitgeber, die Zeiten der Arbeitsunfähigkeit, die Mutterschutzfristen, die Zeiten des Mutterschaftsurlaubs und die Arbeitsausfalltage von Bedeutung. Nicht benötigt werden dagegen Angaben über die Verleihung von Auszeichnungen, über Röntgengroßaufnahmen und Schirmbilder sowie über ärztliche Diagnosen. Es bestehen daher keine Bedenken, wenn solche Angaben auf einer beglaubigten Abschrift des Ausweises oder dessen Auszügen unleserlich gemacht werden. Die Landesversicherungsanstalt hat mir mitgeteilt, daß in der nächsten Auflage der Antragsvordrucke ein entsprechender Hinweis auf § 286 e SGB VI aufgenommen werden wird.

20.10 Sozialhilfe

Ein Petent bat um Klärung der Frage, ob im Rahmen einer Rehabilitationsmaßnahme in einer Einrichtung, die von einem Kostenträger (hier: Landesversicherungsanstalt) bezahlt wird, bei der Taschengeldgewährung, für die ein Sozialamt zuständig ist, ärztliche Gutachten an den Sozialhilfeträger und — wenn ja — in welchem Umfang gesandt werden dürfen.

Hierzu stelle ich fest, daß Sozialhilfeleistungen (auch Nebenleistungen — hier: Barbetrag) während einer stationären Langzeittherapie in der Regel vom örtlichen Träger der Sozialhilfe im Namen des überörtlichen Trägers der Sozialhilfe gewährt werden. Diese Leistungen fallen jedoch nur dann gem. § 100 Abs. 1 Nr. 1 Bundessozialhilfegesetz (BSHG) in die sachliche Zuständigkeit des überörtlichen Trägers der Sozialhilfe, wenn Hilfe in besonderen Lebenslagen für die in § 39 Abs. 1 Satz 1 und Abs. 2 genannten Personen (Geisteskranke, Personen mit einer sonstigen geistigen oder seelischen Behinderung oder Störung, Anfallskranke und Suchtkranke) gewährt wird. Die Zugehörigkeit zum vorgenannten Personenkreis kann nur mit Hilfe einer ärztlichen Stellungnahme beurteilt werden. Dabei beantragt der örtliche Träger die Anerkennung der sachlichen Zuständigkeit nach § 100 Abs. 1 BSHG beim Landessozialamt Niedersachsen, das hier die Aufgaben des Landes durchführt. Das Landessozialamt macht die Anerkennung seiner sachlichen Zuständigkeit von der Vorlage einer ärztlichen Stellungnahme abhängig, aus der eindeutig das Vorliegen der genannten Voraussetzungen hervorgeht. Dies wird in der Regel durch den Arztbericht, der von den Rentenversicherungsträgern erstellt wird, erfüllt. Es genügt auch jede andere ärztliche Stellungnahme, die die Zugehörigkeit zum genannten Personenkreis und die Notwendigkeit der Maßnahme deutlich macht.

Darüber hinaus obliegt es in erster Linie dem Hilfesuchenden, im Rahmen seiner Mitwirkungspflicht nach § 60 ff. SGB I die erforderlichen Nachweise zu erbringen bzw. der Erteilung der erforderlichen Auskünfte zuzustimmen.

Wenn sich die ärztlichen Gutachten im Rahmen des oben beschriebenen halten und wenn eine Einverständniserklärung der oder des Hilfesuchenden sei-

tens des Sozialamtes vorgelegt wird, bestehen keine datenschutzrechtlichen Bedenken gegen die Offenbarung der entsprechenden Daten.

20.11 Heime, Heimaufsicht

20.11.1 Mitarbeiterlisten

Der Betreiber eines Altersruhesitzes hat mir mitgeteilt, daß ein Landkreis von ihm eine Liste der Mitarbeiterinnen und Mitarbeiter mit Namen, Vornamen, Geburtsdatum, Anschrift, Ausbildung und regelmäßiger Arbeitszeit gefordert hat. Nach seiner Auffassung sind diese detaillierten Daten nicht erforderlich.

Rechtsgrundlage für die Anforderung von Mitarbeiterlisten ist § 8 Abs. 1 des Heimgesetzes i. d. F. vom 23. April 1990 (BGBl. I S. 764). Danach hat der Träger eines Heimes nach den Grundsätzen einer ordnungsgemäßen Buchführung Aufzeichnungen über den Betrieb des Heimes zu machen, aus denen insbesondere ersichtlich sind: Name, Vorname, Geburtsdatum, Anschrift und Ausbildung der Beschäftigten, deren regelmäßige Arbeitszeit, die von ihnen in dem Heim ausgeübte Tätigkeit und die Dauer des Beschäftigungsverhältnisses. Nach § 8 Abs. 2 hat der Träger eines Heimes Aufzeichnungen nach dieser Vorschrift sowie sonstige Unterlagen und Belege über den Betrieb eines Heimes zur Einsichtnahme durch die zuständige Behörde fünf Jahre aufzubewahren. Die Überwachung der Heime selbst ist in § 9 des Heimgesetzes geregelt.

Neben der Buchführungspflicht besteht nach den weitergehenden Landesverordnungen — für Niedersachsen § 10 der Heimverordnung vom 3. Oktober 1968 (Nieders. GVBl.) — die Pflicht, Aufzeichnungen zu führen. Aus den Aufzeichnungen müssen nach § 10 Abs. 2 Nr. 1 Vor- und Zuname, Geburtsdatum, Geburtsort sowie letzter Wohnort und letzte Wohnung der Heimbewohner, der Tag ihres Einzugs, ihres Auszugs oder ihres Todes sowie Name und Anschrift eines der nächsten Angehörigen ersichtlich sein. Nach Nr. 5 dieser Bestimmung müssen weiter ersichtlich sein: Vor- und Zuname, Geburtsdatum, Geburtsort, Wohnort und Wohnung der im Heim Beschäftigten sowie der Ausbildungs- und Berufsweg des Pflegepersonals.

Die Übermittlung personenbezogener Daten stellt einen Eingriff in das Grundrecht auf informationelle Selbstbestimmung der Betroffenen dar, der nach der Rechtsprechung des Bundesverfassungsgerichts der Einwilligung der Betroffenen oder aber — jedenfalls in Fällen, in denen, wie bei der Heimaufsicht, staatlicher Zwang ausgeübt wird — einer präzisen gesetzlichen Befugnisnorm bedarf. Das Heimgesetz, das am 23. April 1990 neu gefaßt worden ist, enthält bereichsspezifische gesetzliche Befugnisnormen, die dem allgemeinen Datenschutzrecht vorgehen. Im Heimgesetz finden sich zahlreiche Verpflichtungen, die einer ordnungsgemäßen Heimaufsicht dienen, beispielsweise die Verpflichtung, Bücher zu führen und diese zur Einsicht und Kontrolle bereitzuhalten. Dagegen fehlt eine gesetzliche Befugnis zur regelmäßigen Übermittlung von Personallisten an die Aufsichtsbehörden.

Da eine regelmäßige Übermittlung von Personalaufstellungen an die Aufsichtsbehörden sich aus dem Heimgesetz und den einschlägigen Verordnungen nicht herleiten läßt, wäre eine entsprechende Forderung unzulässig. Dagegen ist es rechtmäßig, wenn im Einzelfall zur Sicherstellung einer sachgerechten Überwachung gem. § 9 des Heimgesetzes von den Heimaufsichtsbehörden die Vorlage entsprechender Personalaufzeichnungen gefordert wird.

20.11.2 Bewohnerakten und Taschengeldkonten

Eine Bezirksregierung hat sich an mich gewandt, um grundsätzliche Probleme hinsichtlich der Heimaufsicht zu klären. Dabei ging es darum, ob bei Nachschauen gem. § 9 Heimgesetz Einsicht in die Bewohnerakten und Taschengeldkonten der Heimbewohnerinnen und -bewohner genommen werden darf.

Nach § 18 Abs. 1 Heimgesetz bestimmen die Landesregierungen die für die Durchführung des Gesetzes zuständigen Behörden. Gemäß Nr. I.2. des Beschlusses des Niedersächsischen Landesministeriums über zuständige Behörden nach dem Heimgesetz vom 14. Januar 1992 (Nds. MBl. S. 197) sind die Bezirksregierungen für Entscheidungen nach §§ 12 Satz 2, 13 und 16 Heimgesetz zuständig, soweit die Landkreise, die kreisfreien Städte und die großen selbständigen Städte selbst Träger des Heimes oder der Einrichtung sind.

Die genannten Regelungen betreffen die Fälle, in denen eine Anordnung nach § 12 Satz 2 Heimgesetz zur Beseitigung einer eingetretenen oder zur Abwendung einer drohenden Beeinträchtigung oder Gefährdnung des Wohles der Bewohnerinnen und Bewohner oder zur Vermeidung eines Mißverhältnisses zwischen dem Entgelt und der Leistung des Heimes erforderlich wird, nach § 13 Heimgesetz dem Heimträger die weitere Beschäftigung der Leiterin bzw. des Leiters oder einer Mitarbeiterin bzw. eines Mitarbeiters wegen fehlender Eignung ganz oder teilweise untersagt werden muß oder eine Untersagung nach § 16 Heimgesetz ausgesprochen werden soll. Soweit hiernach die Bezirksregierungen für die Durchführung des Heimgesetzes in kommunalen Heimen zuständig sind, muß im Interesse der Einhaltung eines geordneten Verwaltungsverfahrens davon ausgegangen werden, daß sie auch die Befugnis zur erforderlichen Sachaufklärung besitzen. Diese Rechtslage bestand im Prinzip vor den genannten Zuständigkeitsregelungen in gleicher Weise aufgrund der Zuständigkeitsverordnung zur Durchführung des Heimgesetzes vom 25. Juni 1975 (Nieders. GVBl. S. 214). Unter Bezugnahme auf § 2 Abs. 2 dieser Verordnung hat das Niedersächsische Sozialministerium mit Erlaß vom 18. Dezember 1981 die Bezirksregierungen angewiesen, auch in kommunalen Einrichtungen eine regelmäßige Überwachung durchzuführen. Hierzu ist Bezug genommen worden auf den Erlaß des Niedersächsischen Sozialministeriums vom 30. September 1981, mit dem die Bezirksregierungen sowie das Landessozialamt Niedersachsen angewiesen worden sind, die Überwachung gem. § 9 Heimgesetz (damals noch: „Nachschau") regelmäßig einmal jährlich durchzuführen.

Diese Überwachung nach § 9 Heimgesetz hat dem in § 2 Heimgesetz genannten Gesetzeszweck zu dienen, nämlich die Interessen und Bedürfnisse der Heimbewohner und der Bewerber für die Aufnahme in ein Heim vor Beeinträchtigung zu schützen, insbesondere die Selbständigkeit und Selbstverantwortung der Bewohner im Heim zu wahren. Dieser Schutzbereich wird in § 6 Abs. 3 Heimgesetz konkretisiert; dort sind die umfangreichen Versagungsgründe für eine Erlaubnis aufgeführt. Vor dem Hintergrund dieser umfassenden Überwachungsaufgabe der mit der Durchführung des Heimgesetzes betrauten Behörden wird deutlich, daß diese nur bei entsprechenden umfangreichen Befugnissen ordnungsgemäß und das heißt nach dem Gesetzeszweck zum Schutze der Heimbewohnerinnen und -bewohner erfüllt werden kann.

Ich gehe — in Übereinstimmung mit dem Niedersächsischen Sozialministerium — davon aus, daß die mit der Durchführung der Heimaufsicht betrauten Behörden Einsicht in Bewohnerakten nehmen dürfen. Dieses Einsichtsrecht ist auch dann nicht ausgeschlossen, wenn in derartigen Bewohnerakten rein private Unterlagen aufbewahrt werden sollten. Es erstreckt sich aber nicht auf solche Unterlagen. Diese müssen vielmehr vor der Einsichtnahme entnommen werden. Nicht durch die Heimbetreuung veranlaßte persönliche Unterlagen

der Heimbewohnerinnen und -bewohner sind in einem von der Bewohnerakte getrennten Vorgang aufzubewahren.

Ich sehe auch keine durchgreifenden Bedenken gegen eine Überprüfung der ordnungsgemäßen Führung der sog. Taschengeldkonten durch die Heimaufsicht. Die Sicherstellung einer ordnungsgemäßen Taschengeldverwaltung dient nach der überzeugenden Darstellung des Niedersächsischen Sozialministeriums dem Schutz der Bedürfnisse der Heimbewohnerinnen und -bewohner, die mit dem ihnen zur Verfügung stehenden Barbetrag (Taschengeld) zu einem Teil ihre wirtschaftliche Selbständigkeit ausüben können (vgl. § 2 Heimgesetz).

20.12 Aktenübersendung an Gerichte und Dritte

In mehreren Petitionen wurde beanstandet, daß bei der Versendung von Akten an Dritte (Verwaltungsgerichte, Arbeitsgerichte, Sozialgerichte, andere Behörden) das in § 35 SGB I normierte Sozialgeheimnis verletzt worden sei. Hierzu hat das Niedersächsische Sozialministerium mit Erlaß vom 12. November 1991 für das Landessozialamt Niedersachsen und mit Erlaß vom 13. Februar 1992 für das Landesversorgungsamt Niedersachsen Regelungen getroffen. Aus datenschutzrechtlicher Sicht ist positiv hervorzuheben, daß für den Fall der vollständigen Übersendung einer Akte an ein Gericht die schriftliche Einwilligung der oder des Betroffenen gefordert wird. Schweigen wird nicht als Einwilligung anerkannt.

21. Gesundheitswesen

Nach der Koalitionsvereinbarung vom 19. Juni 1990 soll die Landesregierung prüfen, ob bereichsspezifische Regelungen zum Datenschutz in das Gesetz für den öffentlichen Gesundheitsdienst, in die Novellierung des Niedersächsischen Gesetzes über Hilfen für psychisch Kranke und Schutzmaßnahmen (PsychKG), in das Niedersächsische Maßregelvollzugsgesetz sowie in ein Krankenhausdatenschutzgesetz aufgenommen werden sollen oder ob ein Querschnittsgesetz zum Datenschutz im Gesundheitswesen erarbeitet werden soll. Ich hatte schon mehrfach auf die Notwendigkeit solcher bereichsspezifischer Regelungen hingewiesen (X 21.4). Schon am 15. Oktober 1987 hat der damalige Sozialminister im Niedersächsischen Landtag bekräftigt, daß „auch in Niedersachsen ein Landesgesundheitsgesetz geplant" sei (IX 21).

Mit Hilfe des sog. Übergangsbonus lassen sich informationelle Eingriffe im äußerst sensiblen Gesundheitsbereich heute schwerlich noch rechtfertigen. Die Übermittlung bzw. Offenbarung von dem Arztgeheimnis unterfallenden Daten ohne gesetzliche Rechtsgrundlage beinhaltet die Gefahr, daß die Mitarbeiterinnen und Mitarbeiter im Gesundheitswesen sich strafbar machen. Man hätte aufgrund der Aussage in der Koalitionsvereinbarung vermuten können, daß das zuständige Sozialministerium zumindest jetzt sofort daran gehen würde, die notwendigen Gesetzgebungsvorbereitungen zu treffen. Es hätte auch nahegelegen, daß das Ministerium derzeit schon verabschiedete oder in der Verabschiedung befindliche und teilweise gut gelungene Vorschriften anderer Länder zur Hand nimmt, um aus diesen Vorlagen einen ersten Arbeitsentwurf für die notwendigen Gesetze zu erstellen. Doch weit gefehlt: Zwei Jahre nach der Koalitionsvereinbarung bat das Sozialministerium mich sowie einige Ressorts um Mitteilung, „wo ... zur Informationsverarbeitung ein Bedarf an bereichsspezifischen Datenschutzvorschriften des Landes für den Gesundheitsbereich besteht".

Obwohl es nicht zu meinen Aufgaben gehört, gesetzgeberische Initiativen zu ergreifen, habe ich selbstverständlich versucht, in diesem Bereich, in dem es entweder überhaupt noch keine oder nur eine unzureichende Gesetzesgrundlage gibt, durch die Formulierung eigener Vorstellungen die Gesetzgebungsaktivitäten zu beschleunigen.

Folgende Punkte halte ich für den gesamten Gesundheitsbereich einer Regelung bedürftig und zugänglich:

Das Auskunfts- und Akteneinsichtsrecht bedarf einer den Erfordernissen des Gesundheitswesens angepaßten Regelung, die eine Einschränkung im Interesse der Patientin oder des Patienten vorsehen kann (vgl. § 25 SGB X). Bei der Einwilligung sollte eine Vertretungsregelung aufgenommen werden für den Fall, daß die Patientin oder der Patient nicht einwilligungsfähig ist. Unbedingt erforderlich ist eine Forschungsregelung, die der besonderen Sensibilität der Gesundheitsdaten Rechnung trägt. Derartige besondere Anforderungen können sein: Leitung des Vorhabens durch einen Arzt oder eine Ärztin, Reidentifizierung der anonymisierten Patientendaten nur über eine Treuhandstelle (entsprechend dem Michaelis-Modell bei Krebsregister-Projekten), Melde- und Protokollierungspflichten oder ein Verbot mit ministeriellem Genehmigungsvorbehalt. Die Auftragsdatenverarbeitung, die Mikroverfilmung und die Übermittlung mit Hilfe von Telefax kann nur unter Einhaltung klar definierter Voraussetzungen zugelassen werden. Löschungsregelungen und Aufbewahrungsfristen müssen vom Gesetzgeber vorgegeben werden.

21.1 PsychKG

Kurz nachdem ich meine Vorstellungen gegenüber dem Sozialministerium formuliert hatte, erhielt ich von einem Institut der Universität Hannover einen Formulierungsvorschlag zur Änderung des PsychKG zugesandt. Anläßlich dieses begrüßenswerten Vorschlages habe ich meine eigenen Vorstellungen für eine Überarbeitung des PsychKG konkretisiert. Die Notwendigkeit rechtlicher Änderungen ist hier besonders groß, da derzeit § 6 Abs. 5 PsychKG auf das Polizeirecht verweist. Dieses wird um weitgehende informationelle Eingriffsbefugnisse erweitert werden, die dann — der Problematik völlig unangemessen — auch im Rahmen des PsychKG Anwendung fänden.

Das PsychKG legt zwei unterschiedliche Zwecke fest: die Hilfeleistung zugunsten der psychisch Kranken und Schutzmaßnahmen vor diesen. Während die Hilfen freiwillig erfolgen, kommt den Schutzmaßnahmen Zwangscharakter zu. Insofern muß auch informationell eine saubere Trennung erfolgen. Anderenfalls könnte die Bereitschaft zur Inanspruchnahme freiwilliger Hilfen wegen der Gefahr, daß die freiwilligen Angaben zur Begründung von Zwangsmaßnahmen, insbesondere der Unterbringung, herangezogen werden, erheblich abnehmen. Die Zweckänderung darf nur unter eng und klar definierten Umständen zugelassen werden. Beim Offenbaren von Behandlungsdaten habe ich vorgeschlagen zu erwägen, ob nicht vollständig auf automatisierte Übermittlungen verzichtet werden kann. Es sollte enumerativ aufgezählt werden, in welchen Fällen eine Durchbrechung der ärztlichen Schweigepflicht zulässig ist. Anstelle eines Verweises auf den rechtfertigenden Notstand nach § 34 Strafgesetzbuch würde ich einer konkreteren Formulierung, z. B. „... zur Abwehr einer Gefahr für Leib und Leben", den Vorzug geben. Bei der Übermittlung an Verwaltungsbehörden ist zumeist nicht die Mitteilung aller Patientendaten nötig; es reicht oft die Mitteilung des Befundes. Daß hier nicht mehr als nötig übermittelt wird, muß gesetzlich festgelegt werden. Soweit die Betroffenen ein Widerspruchsrecht gegen Übermittlungen hat, muß gewährleistet sein, daß eine umfassende Unterrichtung hierüber erfolgt.

21.1.1 Aufbewahrungsfristen

Hinsichtlich der Aufbewahrungsfristen von Akten im Sozialpsychiatrischen Dienst haben mich mehrere Anfragen erreicht. Hierzu habe ich festgestellt, daß die Aufbewahrungsfrist nach § 11 der Berufsordnung der Ärztekammer Niedersachsen, nach der ärztliche Aufzeichnungen 10 Jahre nach Abschluß der Behandlung aufzubewahren sind, soweit nicht andere gesetzliche Vorschriften eine längere Aufbewahrungsfrist vorschreiben, sinngemäß anzuwenden sind. Diese „10 Jahre-Frist" schließt aber nicht aus, schon vor Fristablauf Unterlagen zu vernichten, die zur Aufgabenerfüllung nicht mehr erforderlich sind.

21.1.2 Waffenschein

Eine Eingabe beschäftigte sich mit der Frage, ob im Fall der Unterbringung einer Person nach den Vorschriften des Nds. PsychKG automatisch eine Überprüfung der betroffenen Personen im Hinblick auf den Besitz und ggf. den Entzug von Waffen zulässig ist. Hier gilt im Einvernehmen mit dem Niedersächsischen Innenministerium, dem Niedersächsischen Sozialministerium und dem Bundesminister des Innern folgendes:

Die automatische waffenrechtliche Überprüfung der betroffenen Personen ist nach denselben Kriterien vorzunehmen wie die Weitergabe personenbezogener Daten an Straßenverkehrsbehörden. Der Erlaß des Niedersächsischen Ministeriums vom 16. Januar 1987 (Gültigkeitsliste Nr. 151/11) ist auf diese Fälle sinngemäß anzuwenden. Eine Vergleichbarkeit der Problembereiche ist gegeben. Waffenrecht und Fahrerlaubnis unterliegen einem Prüfungs- und Genehmigungsverfahren. Die Ausübung stellt dabei durchaus eine gefahrgeneigte Tätigkeit dar. Eine automatische Überprüfung erscheint schon deshalb nicht sachgerecht, weil die Zahl der untergebrachten Personen, die einen Waffen- und Jagdschein besitzen, deutlich geringer sein dürfte als die Zahl der Führerscheininhaber. Die Vorschrift des § 5 Abs. 2 Nrn. 3 und 4 des Waffengesetzes, nach der die erforderliche Zuverlässigkeit in der Regel bei bestimmten Personen nicht gegeben ist, ist keine Befugnisnorm für die Übermittlung dieser Daten. Demzufolge ist die Übermittlung von Daten über erfolgte Unterbringungen hinsichtlich der Verwaltungsbehörden auch in waffenrechtlicher Hinsicht unzulässig und die Verwertung solcher Daten untersagt.

Nach Ansicht des Sozialministeriums ist es Aufgabe des die untergebrachte Person behandelnden Krankenhausarztes festzustellen, ob die Eignung zum Führen eines Fahrzeuges oder zum Besitz einer Waffe auch zukünftig gegeben ist. Hat die Ärztin oder der Arzt Bedenken, so sind diese der zuständigen Amtsärztin oder dem zuständigen Amtsarzt mitzuteilen. Von dort können diese Bedenken — wiederum durch § 34 StGB gerechtfertigt — der zuständigen Behörde mitgeteilt werden.

21.2 Öffentlicher Gesundheitsdienst

Immer wieder habe ich darauf hingewiesen, daß für den öffentlichen Gesundheitsdienst in Niedersachsen noch das Gesetz über die Vereinheitlichung des Gesundheitswesens vom 3. Juli 1934 Anwendung findet, in welchem von „Gesundheitspolizei", „Erbpflege" oder „gesundheitlicher Volksbelehrung" die Rede ist. Daß dieses Gesetz für die Praxis keine befriedigende Handlungsgrundlage darstellt, wurde mir im Rahmen von Gesprächen und Veranstaltungen auch von Mitarbeiterinnen und Mitarbeitern aus dem Gesundheitsbereich

immer wieder vorgetragen. Diese Gespräche haben mir ein Bild davon vermittelt, welche datenschutzrechtlichen Erfordernisse ein „Gesetz über den öffentlichen Gesundheitsdienst" erfüllen muß. Dazu einige wichtigen Stichworte:

Die Aufgaben des öffentlichen Gesundheitsdienstes müssen abschließend, differenziert und normenklar aufgeführt werden. Die Abschottung zwischen den Bereichen, welche verschiedene Zwecke verfolgen, von der Schulgesundheitspflege über die AIDS-Beratung bis hin zu den Einstellungsuntersuchungen, muß gewährleistet sein. Bei amtsärztlichen Untersuchungen darf nur das Untersuchungsergebnis mitgeteilt werden. Zentralkarteien, welche zu Zwecken der Postverteilung, der Regelung des Besucherverkehrs und der Aktenverwaltung geführt werden, dürfen keine diagnostischen und therapeutischen Angaben enthalten. Bei zwangsweiser Erhebung, die von der Wahrnehmung freiwilliger Aufgaben klar getrennt sein muß, sind der Datenkatalog und die weitere Verarbeitung in Verordnungen festzulegen. Schließlich bedarf es der Klärung, welche Informationen zu statistischen Zwecken zusammengetragen werden dürfen.

21.3 Landeskrankenhausgesetz

Schon vor zwei Jahren habe ich darauf hingewiesen, daß es für Datenschutzregelungen im Krankenhausbereich eine Vielzahl von Vorlagen in anderen Ländern gibt (X 24.4). Zu den von mir erwähnten Ländern Baden-Württemberg, Bayern, Berlin, Bremen, Hessen, Rheinland-Pfalz und Nordrhein-Westfalen sind inzwischen das Saarland und Hamburg hinzugekommen. Erwähnt werden müssen außerdem entsprechende Regelungen, welche für kirchliche Krankenhäuser erlassen worden sind. Ich bin gespannt, ob es das Land Niedersachsen schafft, zeitlich vor den neuen Bundesländern ein Gesetz zu erarbeiten, welches die Datenverarbeitung im Krankenhaus regelt. Ich habe mich mehrfach bereiterklärt, hierbei konstruktiv mitzuwirken.

21.4 Fast eine Unmöglichkeit: Die Auswertung von Todesbescheinigungen

Welche datenschutzrechtlichen Defizite im niedersächsischen Gesundheitswesen bestehen, zeigte sich anhand eines Forschungsprojektes, welches in mehreren Bundesländern, u. a. auch in Niedersachsen, durchgeführt wird. Das Projekt wird mit öffentlichen Mitteln gefördert. Ziel ist die Überprüfung der Richtigkeit und Verläßlichkeit von Todesbescheinigungen. Ärztinnen oder Ärzte, z. B. aus dem Notfalldienst, im hausärztlichen Dienst oder aus einem Krankenhaus, welche mit Verstorbenen zu tun hatten, werden vom Gesundheitsamt nochmals über Diagnose und vermutete Todesursache befragt. Die nacherhobenen Ergebnisse werden ebenso wie die Angaben aus den Todesbescheinigungen anonymisiert und in nicht mehr personenbezogener Form an das private Forschungsinstitut zur Auswertung weitergeleitet. Durch das Forschungsprojekt sollen Erkenntnisse gewonnen werden, wie die „Reliabilität" und „Validität" — also die Verläßlichkeit und die Aussagekraft der Todesbescheinigungen — erhöht und die Angabe falscher bzw. oberflächlich festgestellter Todesursachen verhindert werden kann.

Bei der datenschutzrechtlichen Überprüfung dieses aus fachlicher Sicht sicher zu begrüßenden Vorhabens, welches bei korrekter Durchführung kaum Gefahren für das Persönlichkeitsrecht in sich birgt, zeigt es sich, daß hierfür keinerlei Rechtsgrundlage vorhanden ist. Eine Aufgaben- und Befugnisnorm für die Gesundheitsämter besteht nicht. Auch eine Forschungsregelung fehlt. Die für das NDSG geplante Regelung ermächtigt nicht zum Umgang mit den Daten Verstorbener, schon gar nicht zum Umgang mit ärztlichen Angaben.

Anders als in Bremen, wo der Umgang mit Todesbescheinigungen vor kurzem in einem Gesetz über das Leichenwesen geregelt wurde, gibt es hierfür in Niedersachsen keine Ansätze. Auch die Nacherhebung bei den Hausärztinnen und Hausärzten sowie den Krankenhäusern ist gesetzlich nicht legitimiert.

Mein Kollege in Nordrhein-Westfalen sah in seinem Land keine Möglichkeit, das Projekt zu akzeptieren. Trotz schwerwiegender Bedenken habe ich mich schließlich entschlossen, die Durchführung des Forschungsvorhabens nicht zu beanstanden. Ich meine, die Säumigkeit des Gesetzgebers darf nicht zu Lasten der in Art. 5 Abs. 3 Grundgesetz gewährleisteten Forschung gehen, wenn, wie im konkreten Fall, die Forschungseinrichtungen sich alle Mühe geben, den datenschutzrechtlichen Erfordernissen Genüge zu tun. Der Beispielsfall ist dazu angetan, die zuständigen Ministerien und das Parlament an ihre vom Verfassungsgericht festgestellten Aufgaben nachdrücklich zu erinnern.

21.5 Blutspendedienst

Schon seit 1986 beschäftige ich mich aufgrund einer Eingabe mit dem Blutspendedienst der Medizinischen Hochschule Hannover (MHH). In der MHH wurden die Blutkonserven mit einem Aufkleber versehen, auf dem u. a. der vollständige Name der Spenderin bzw. des Spenders aufgedruckt war. Im September 1991 hat die MHH mitgeteilt, daß nunmehr der Spendername auf der Blutkonserve durch eine Zahlenidentifikation, die durch einen Barcode ergänzt wird, ersetzt worden ist. Ich halte dies für eine datenschutzgerechte Maßnahme, die leider viel zu spät kommt.

21.6 Gruppenbehandlung im Krankenhaus

Ein Petent hatte sich über eine Gruppenbehandlung in einer Augenklinik beschwert. Die Patienten waren gezwungen, vor den Mitpatienten ihre personenbezogenen Daten und die Krankheitsgeschichte zu offenbaren.

Im Anschluß an eine Besichtigung habe ich dem Krankenhaus vorgeschlagen, unter dem Gesichtspunkt des Datenschutzes und der ärztlichen Schweigepflicht eine Einwilligungserklärung der Patienten zu einer Gruppenbehandlung zu entwickeln und von diesen unterschreiben zu lassen. Der Text dieser Einwilligungserklärung wurde inzwischen vereinbart.

Dieses Verfahren scheint mir unter datenschutzrechtlichen wie unter Praktikabilitätsgesichtspunkten eine sinnvolle Lösung zu sein. Durch bauliche Maßnahmen war die Situation in dem Krankenhaus nicht zu verbessern.

21.7 Krankenhauswanderer

Krankenhäuser haben immer wieder mit dem Problem der „Krankenhauswanderung" zu tun: Personen, zumeist ohne festen Wohnsitz, melden sich mit einer vermeintlichen Krankheit und lassen sich stationär aufnehmen, Kost und Logis eingeschlossen. Nach zwei bis vier Tagen, nachdem sich evtl. herausgestellt hat, daß keine Behandlung notwendig und gerechtfertigt ist, verschwinden die Krankenhauswanderer wieder, um sich in einem anderen Krankenhaus unentgeltlich „einzumieten".

Die Medizinische Hochschule Hannover hat sich mit der Frage an mich gewandt, ob es zulässig sei, eine personenbezogene Datei über Krankenhauswanderer anzulegen. Bei diesem Problem sind folgende Fragen zu beantworten: Darf das Datum „Krankenhauswanderer" bei Patienten, die in der MHH behandelt worden sind, von dieser gespeichert werden? Darf das Datum „Krankenhauswanderer" bei Patienten, die in der MHH behandelt worden sind, von ihr an Dritte übermittelt werden? Dürfen Patientendaten, die der MHH von Dritten gemeldet worden sind, von dieser gespeichert werden?

Zu der ersten Frage ist festzustellen, daß die Speicherung des Merkmals „Krankenhauswanderer" aus meiner Sicht zur Aufgabenerfüllung erforderlich ist (§ 9 Abs. 1 NDSG). Eine Verpflichtung, die Patienten über die Speicherung dieses Datums zu unterrichten, gibt es z. Zt. nicht. Ob die Mitteilung über die Speicherung dieses Datums an den Patienten eine präventive Wirkung für das künftige Verhalten des Patienten hat, entzieht sich meiner datenschutzrechtlichen Beurteilung. Es gibt jedenfalls nach den Vorschriften des NDSG auch keinen Hinderungsgrund, die Patienten entsprechend zu informieren.

Eine bereichsspezifische Rechtsgrundlage, die eine Datenübermittlung an Dritte erlaubt, sehe ich z.Zt. nicht. Der niedersächsische Gesetzgeber könnte sie allerdings in einem Gesundheits- oder Krankenhausgesetz schaffen. Derzeit ist die Datenübermittlung in §§ 10 und 11 NDSG geregelt. Die Anwendung der allgemeinen Übermittlungsvorschrift des geltenden NDSG kommt aber nach meinem Dafürhalten nicht in Betracht. § 10 NDSG muß im Lichte des Urteils des Bundesverfassungsgerichts zum Volkszählungsgesetz interpretiert werden. Danach ist eine Übermittlung, die zu einer Zweckentfremdung führt, unzulässig, es sei denn, die Übermittlung wäre aufgrund einer Rechtsvorschrift vorgesehen. Sollte die Übermittlung dieser Daten (Krankenhauswanderer) unzulässig sein, so unterliegen sie einem Verwertungsverbot.

Das Niedersächsische Sozialministerium teilt meine Auffassung zur Frage, ob die Speicherung des Merkmals „Krankenhauswanderer" aus Sicht der Krankenhäuser zur Aufgabenerfüllung erforderlich ist. Allerdings bleibt die Umsetzung (Erfassung und Speicherung des Merkmals „Krankenhauswanderer") in das Ermessen des einzelnen Krankenhauses gestellt, wobei insbesondere wirtschaftliche Gesichtspunkte zu berücksichtigen sind.

Vor einer weitergehenden bereichsspezifischen Regelung der Datenübermittlung an andere Krankenhäuser und der damit verbundenen Verwertung in einer Datei, die präventiv in anderen Krankenhäusern aufgefallene Krankenhauswanderer registriert, wird eine Abwägung zwischen dem schützenswerten Recht auf informelle Eigenbestimmung und dem Abwehrinteresse des Gemeinwohls bezüglich einer finanziellen Benachteiligung durch betrügerische Handlungen vorzunehmen sein. Die Schaffung einer gesetzlichen Regelung, die eine Datenübermittlung an Dritte erlaubt, ist nach dem derzeitigen Stand im öffentlichen Gesundheitsdienst nicht vorgesehen.

Eine AOK hat in einer Fachzeitschrift für Krankenhäuser eine Warnung vor einem „Krankenhauswanderer" mit personenbezogenen Daten plaziert. Zu der Frage, ob die Veröffentlichung der Warnung vor einem „Krankenhauswanderer" in einer Zeitschrift zulässig ist, vertrete ich gemeinsam mit dem Niedersächsischen Sozialministerium folgende Auffassung: Es steht außer Frage, daß die Krankenkasse im Rahmen der Erfüllung ihrer gesetzlichen Aufgaben dazu befugt sein kann, personenbezogene Daten eines „Krankenhauswanderers" zu offenbaren. Der Umfang der preisgegebenen Daten ist so gering wie möglich zu halten und auf das Maß des zur Erreichung des Zieles Notwendigen zu beschränken. Als rechtlich problematisch muß jedoch die Art und Weise der gewählten Form der Offenbarung angesehen werden. Der Ver-

hältnismäßigkeitsgrundsatz erfordert, daß die erfolgte Durchbrechung des Sozialgeheimnisses unter Berücksichtigung der Umstände des Einzelfalles angemessen ist. Angemessenheit bedeutet wiederum, daß die Intensität des jeweiligen Eingriffs nicht größer ist, als es durch den jeweiligen Offenbarungszweck zu rechtfertigen wäre. Hierbei kommt etwaigen alternativen Mitteln zur Erreichung des Offenbarungszwecks besondere Bedeutung zu. Dieser Grundsatz ist um so gewichtiger, je intensiver der mit der Offenbarung erfolgte Eingriff ist. Bei der Veröffentlichung von Sozialdaten in Gestalt von Anzeigen in Zeitschriften handelt es sich um einen besonders intensiven Eingriff in das Sozialgeheimnis. Als Leitlinie für die Praxis gilt hier, sich nur wenig vom Prinzip des geringstmöglichen Eingriffs zu entfernen. In die Beurteilung der Verhältnismäßigkeit eines solchen Eingriffs sind auch etwaige Folgewirkungen der Offenbarung einzubeziehen.

Die Veröffentlichung der in Rede stehenden Anzeige in einer Krankenhaus-Zeitschrift grenzt den Personenkreis derer, die von ihrem Inhalt Kenntnis erhalten können, zwar von vornherein ein, jedoch ist m. E. in erster Linie darauf abzustellen, ob die Offenbarung bzw. Datenübermittlung erforderlich ist, um die betreffende Aufgabe ordnungsgemäß erfüllen zu können. Die Krankenhäusern obliegende Aufgabe der Behandlung von Patienten wird durch die Tatsache, daß eine geringe Anzahl von „Krankenhauswanderern" zu versorgen ist, nicht gravierend beeinträchtigt. Materielle Schäden in begrenztem Umfang gefährden die ordnungsgemäße Aufgabenerfüllung nicht.

Insoweit reicht meines Erachtens § 69 Abs. 1 Nr. 1 SGB X als Rechtsgrundlage für die Offenbarung personenbezogener Daten von „Krankenhauswanderern" nicht aus. Vielmehr bedarf es hierzu einer gesonderten Rechtsgrundlage.

Auch eine Offenbarung gem. § 71 Abs. 1 Nr. 1 SGB X ist unzulässig. Der Straftatbestand des Betruges (§ 263 StGB) ist in § 138 StGB nicht genannt. Aufgrund der aktuellen Rechtslage kann eine Mitteilung über „Krankenhauswanderer" an andere Krankenkassen und eine Speicherung bei diesen auch künftig nicht erfolgen. Aufgrund der Stellungnahme des Niedersächsischen Sozialministeriums gehe ich davon aus, daß aus fachlicher Sicht auch kein Bedürfnis für solche Unterrichtungen besteht.

21.8 Röntgenaufnahmen

Die Zielrichtung des § 16 Abs. 3 der Röntgenverordnung ist es, der oder dem Strahlenschutzverantwortlichen und der Ärztin bzw. dem Arzt Vorschläge zur Verringerung der Strahlenexposition zu machen. Die Röntgenaufnahmen werden von der Ärztin bzw. dem Arzt an die Zahnärzte- bzw. Ärztekammer gegeben. Auf den Aufnahmen befindet sich auch der Name der Patientin bzw. des Patienten. Ich bin der Auffassung, daß bei der Übersendung von Röntgenaufnahmen nur der Monat der Fertigung der Röntgenaufnahmen, das Geschlecht der Patienten und das Alter nach Dekade anzugeben ist. Dies habe ich den zuständigen Stellen mitgeteilt.

21.9 Bundesseuchengesetz

Eine Stadt hat bei mir angefragt, ob die Auffassung zutreffend sei, daß Kindergartenleiterinnen verpflichtet seien, Namen und Adressen krankheitsverdächtiger Personen dem Gesundheitsamt mitzuteilen, oder ob es ausreiche, anonyme Meldungen an das Gesundheitsamt zu geben.

Hierzu stelle ich fest, daß das Bundesseuchengesetz grundsätzlich nur die namentliche Meldung kennt. Das gilt sowohl für die Meldepflichten nach § 3 ff. als auch nach § 48 Abs. 2 Bundesseuchengesetz. Ausgenommen ist lediglich die Berichtspflicht nach der Laborberichtsverordnung für HIV-Befunde, die ausdrücklich für anonym erklärt worden ist. Zweck der namentlichen Meldepflicht ist es, das Gesundheitsamt in den Stand zu setzen, beim Auftreten übertragbarer Krankheiten sofort das Nötige zu veranlassen. Dies muß ohne zeitliche Verzögerung geschehen, um ggf. einem epidemischen Ausbreiten durch geeignete Maßnahmen rechtzeitig zuvorzukommen. Gerade in Kinderheimen, Kindergärten u. ä. Einrichtungen ist eine Verbreitungsgefahr von übertragbaren Krankheiten besonders hoch. Es gäbe wenig Sinn und würde zu unvertretbaren Verzögerungen führen, wenn der Kindergartenleitung lediglich eine anonyme Meldepflicht zugestanden würde. Das Gesundheitsamt müßte dann die erforderlichen personenbezogenen Daten durch eigene Ermittlungen erheben. Nach dem Wortlaut des § 48 Abs. 2 Bundesseuchengesetz wird eine eigenständige Meldepflicht für die Leiterinnen dieser Einrichtung statuiert, die im Hinblick auf den wichtigen Zeitfaktor, „unbeschadet der Meldepflicht anderer Personen nach § 4" gilt.

22. Kinder- und Jugendhilfe

22.1 Jugendgerichtshilfe

§ 62 Abs. 2 und 3 des Kinder- und Jugendhilfegesetzes — KJHG — (SGB VIII) regeln, daß die Datenerhebung — von den gesetzlich vorgesehenen Ausnahmefällen abgesehen — grundsätzlich bei den Betroffenen erfolgen muß.

Die Arbeitsgemeinschaft der obersten Landesjugendbehörden vertritt die Auffassung, daß diese Regelungen in vollem Umfang auch für die Jugendgerichtshilfe (JGH) gelten müssen. Das heißt, die JGH darf personenbezogene Daten, die sie in ihrem Bericht verwertet, grundsätzlich — vorbehaltlich des § 62 Abs. 3 Nr. 3 KJHG — nur beim Betroffenen erheben. Mit seiner Einwilligung können Daten auch bei Dritten erhoben werden. Diese Auslegung soll im Rahmen der Reform des Jugendgerichtshilfegesetzes (JGG) klargestellt werden.

22.2 Vorschlagsliste für die Bestellung als Vormünder oder Pfleger

Eine Gemeinde hatte einem Landkreis eine Vorschlagsliste für die Bestellung als Vormünder und Pfleger (seit 1. Januar 1992 Betreuer) übersandt, weshalb sich ein Petent beschwerte.

Aus datenschutzrechtlicher Sicht beurteilt sich die Sachlage wie folgt: Aufgrund des § 1849 BGB in Verbindung mit § 50 KJHG und § 1897 BGB besteht für das Jugendamt die Verpflichtung, dem Vormundschaftsgericht Personen vorzuschlagen, die geeignet und in der Lage sind, eine Pflegschaft oder Vormundschaft für Erwachsene zu führen. Rechtsgrundlage für Auskünfte aus dem Melderegister ist das Niedersächsische Meldegesetz (NMG). Die Übermittlung an andere Behörden oder sonstige öffentliche Stellen ist in § 29 NMG geregelt. Bei dem hier zu beurteilenden Sachverhalt ist eine Übermittlung nach § 29 NMG unter folgenden Voraussetzungen zulässig: Bei der Übermittlung der Daten ist § 10 Abs. 1 Satz 1 NDSG zu beachten. Werden Daten für eine Personengruppe listenmäßig oder in zusammengefaßter Form

übermittelt, dürfen für die Zusammensetzung der Personengruppe nur die in § 29 Abs. 1 Satz 1 genannten Daten zugrunde gelegt werden. Nach § 10 Abs. 1 Satz 1, 2. Alt. NDSG ist die Übermittlung personenbezogener Daten zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben erforderlich ist. Die von der Gemeinde übermittelten Daten überschritten den Rahmen des § 29 Abs. 1 NMG nicht. Darüber hinaus hat die Gemeinde die Auswahl der Personen automatisch durch die Datenverarbeitung mittels eines Zufallsgenerators vorgenommen. Ich halte daher die Übermittlung von Daten aus dem Melderegister für den beschriebenen Zweck im Rahmen des § 29 Abs. 1 NMG für zulässig.

22.3 Fragen an Unterhaltsverpflichtete

Mir wurde ein Fragebogen eines Landkreises für Unterhaltspflichtige vorgelegt, verbunden mit der Frage nach der Erforderlichkeit der darin abgefragten Angaben und nach dem Umfang der vorzulegenden Bescheinigungen.

Rechtsgrundlage für die Datenerhebung ist § 1605 BGB. Hier ist die Vorlage von Belegen, insbesondere Bescheinigungen des Arbeitgebers, geregelt. Ich halte die Vorlage von beglaubigten Fotokopien der Gehaltsabrechnung für ausreichend. Nur im Einzelfall kann es m. E. seitens des Jugendamtes erforderlich sein, eine Bescheinigung des Arbeitgebers zu fordern. Diese Bescheinigung sollte dann von den Unterhaltspflichtigen beigebracht werden. Eine Auskunft des Finanzamtes ist ebenfalls nur im Ausnahmefall erforderlich. Es reicht in vielen Fällen aus, wenn die Unterhaltspflichtigen selbst die Steuerbescheide einreichen.

22.4 Weitergabe von Kindergarten-Anmeldedaten

Vielfach wird von Kommunen verlangt, daß die einzelnen Kindergartenträger die jährlich neu aufgenommenen Kinder und die „Wartelistenkinder" namentlich mit Geburtsdatum und Adresse übermitteln. Begründet wird dies mit der gesetzlichen Verpflichtung nach dem KJHG zur Kindergartenbedarfsplanung. Von Interesse sind insbesondere die „Wartelistenkinder", weil die Erziehungsberechtigten ihre Kinder oftmals in mehreren Kindergärten anmelden.

Bei der Anforderung der Anmeldedaten von Kindern aus Kindertagesstätten handelt es sich um eine Datenerhebung seitens der Kommune. Gemäß § 62 Abs. 2 KJHG sind die Daten bei den Betroffenen zu erheben. Betroffene sind hier die Erziehungsberechtigten, die ihr Kind angemeldet haben. Ohne Mitwirkung der Betroffenen dürfen personenbezogene Daten nur unter den Voraussetzungen des § 62 Abs. 3 KJHG erhoben werden. Diese Ausnahmebestimmungen sind hier nicht erfüllt.

Zum anderen handelt es sich um eine Übermittlung (Offenbarung) der Daten der Betroffenen durch die Kindertagesstätten an die Kommune. Hierfür gilt bei kirchlichen Kindergärten kirchliches Datenschutzrecht, bei freien Trägern das Bundesdatenschutzgesetz. Das kirchliche Datenschutzrecht orientiert sich weitgehend am allgemeinen staatlichen Datenschutzrecht. Nach dem Bundesdatenschutzgesetz (§ 28 Abs. 2 Nr. 1 Buchst. b) wäre eine Übermittlung nur zulässig, wenn kein Grund zu der Annahme bestünde, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hätte. Ein schutzwürdiges Interesse könnte darin bestehen, daß Erziehungsberechtigte ihr Kind bewußt in kirchlichen oder freien Kindertagesstätten angemeldet haben und nicht wünschen, daß ihre Anmeldung an die Kommune übermittelt

wird. Jedenfalls ist im Einzelfall von der Kindertagesstätte festzustellen, ob ein schutzwürdiges Interesse der Übermittlung entgegensteht. Das heißt, letztlich ist eine Übermittlung der Daten nur bei Vorlage einer schriftlichen Einverständniserklärung unproblematisch.

Auf meinen Vorschlag hin beabsichtigt das Niedersächsische Kultusministerium, den vorgelegten Gesetzentwurf über Tageseinrichtungen für Kinder um eine entsprechende Regelung zu ergänzen. Hiernach soll § 13 Abs. 1 folgende Ergänzung erfahren: „Das Jugendamt kann zur Ermittlung des Bedarfs von den Trägern der Tageseinrichtungen für Kinder Angaben über die Anzahl der genehmigten Plätze, Umfang des Betreuungsangebots, Name, Anschrift und Alter der Kinder, die zur Aufnahme in der Einrichtung angemeldet wurden, verlangen."

Ich könnte mir vorstellen, daß für die Zukunft die Kindertagesstätten hiervon in Kenntnis gesetzt werden und darauf hingewiesen wird, daß bei der Anmeldung der Kinder eine Einverständniserklärung von den Erziehungsberechtigten einzuholen ist, die die Kindertagesstätten dann zu der Übermittlung der entsprechenden Daten berechtigt.

22.5 Unterbringungsgesuche für Behinderte

Jugendämter haben häufig die Aufgaben der Betreuungsbehörde nach dem Betreuungsgesetz auch für erwachsene Behinderte wahrzunehmen. In diesem Rahmen schreiben sie gleichzeitig, um diesen Personenkreis unterzubringen, gleichzeitig eine Vielzahl von möglichen Betreuungseinrichtungen an. Hierbei werden nicht nur die personenbezogenen Daten der Behinderten, sondern auch ärztliche Stellungnahmen bzw. Entwicklungsberichte übersandt.

Ich bin der Auffassung, daß dieses Verfahren in aller Regel in anonymer Form durchgeführt werden sollte. Das Niedersächsische Kultusministerium hat mittlerweile im Mitteilungsblatt der Arbeitsgemeinschaft der Jugendämter einen entsprechenden Hinweis veröffentlichen lassen. Der veröffentlichte Text lautet wie folgt:

„Die Datenschutzbeauftragten des Bundes und des Landes Niedersachsen haben sich aus verschiedenen Anlässen mit der Verfahrensweise vieler Jugendämter bei der Suche nach einem geeigneten Heim oder einer geeigneten Pflegefamilie für einen jungen Menschen befaßt. Verbreitet ist die Praxis, eine Beschreibung des jungen Menschen und seiner Probleme zu verfassen — teilweise in Fragebogenform, teilweise als ‚Kinderbogen' oder ähnlich bezeichnet — und an mehrere, mitunter viele in Frage kommende Einrichtungen oder Personen zu versenden.

Für die Beurteilung der datenschutzrechtlichen Zulässigkeit dieses Verfahrens ist § 69 Abs. 1 Nr. 1 SGB X maßgeblich. Die Offenbarung personenbezogener Daten ist danach zulässig, soweit sie für die Erfüllung einer gesetzlichen Aufgabe nach dem Sozialgesetzbuch erforderlich ist. Nach diesem Maßstab ist das Verfahren nicht grundsätzlich zu beanstanden, weil ein gleich effektives Verfahren, eine geeignete Unterbringungsmöglichkeit zu suchen, nicht ersichtlich ist. Es muß aber sorgfältig bedacht werden, dabei dem Datenschutz so weit wie möglich Rechnung zu tragen. Insbesondere sollte nach Auffassung der Datenschutzbeauftragten — und auch des Bundesministeriums für Familie und Jugend — die Darstellung anonym gehalten werden, also die Namen des Kindes und seiner Angehörigen, evtl. auch des Herkunftsortes, der Schule etc. nicht genannt werden. In der Regel kann das Ziel einer solchen Umfrage auch so erreicht werden."

Ich begrüße diese klarstellende Regelung. Außer Frage steht, daß das Jugendamt seine gesetzlichen Aufgaben erfüllen können muß. Wenn es unter den besonderen Umständen des Einzelfalles unerläßlich ist, den Namen des jungen Menschen zu nennen, vielleicht sogar ihn der Einrichtung vorzustellen, steht der Datenschutz dem nicht entgegen.

22.6 Sexueller Mißbrauch von Kindern

Ein Landkreis fragte an, ob Kindertagesstätten befugt sind, einen Verdacht, daß ein Kind sexuell mißbraucht oder körperlich oder seelisch mißhandelt wird, an das Jugendamt oder an eine Einrichtung zu übermitteln, die das Kind ebenfalls betreut oder es künftig betreuen wird.

Die Frage ist hinsichtlich der Kindertagesstätten datenschutzrechtlich relevant. Kommunale Kindertagesstätten sind Teil eines Sozialleistungsträgers; an diese richten sich die Vorschriften über den Schutz des Sozialgeheimnisses unmittelbar (vgl. § 35 i.V.m. § 12 SGB I). Kindertagesstätten freier Träger sind zwar nicht unmittelbar Adressaten des Sozialdatenschutzrechts, müssen nach § 61 Abs. 3 KJHG aber „den Schutz personenbezogener Daten in entsprechender Weise gewährleisten".

Die datenschutzrechtliche Relevanz für Kindertagesstätten ergibt sich weiter daraus, daß die Beobachtungen an einem Kind, die einen entsprechenden Verdacht begründen, personenbezogene Daten sind und die Übermittlung an das Jugendamt oder an eine andere Einrichtung eine Offenbarung im Sinne der §§ 35 SGB I, 67 ff. SGB X darstellt.

Die Weitergabe ist gem. § 69 Abs. 1 Satz 1 Nr. 1 SGB X datenschutzrechtlich legitimiert, wenn sie für die Erfüllung der eigenen gesetzlichen Aufgaben der Kindertagesstätte erforderlich ist. Eine Legitimation durch Einwilligung der Betroffenen (§ 67 SGB X) hingegen scheidet in den hier erörterten Fällen meist aus, zumal meist auch die Eltern oft nicht nur Betroffene, sondern „Angeschuldigte" sind und selbst einwilligen müßten.

Zu den gesetzlichen Aufgaben einer Kindertagesstätte gehört es auch, den Ursachen von ernsthaften Leiden oder Verletzungen beim Kind nachzugehen, die außerhalb der Kindertagesstätte liegen, wenn anzunehmen ist, daß die Eltern oder andere Stellen dies nicht ausreichend tun.

Die Weitergabe personenbezogener Daten ist zur Erfüllung dieser Aufgabe erforderlich, wenn die Kindertagesstätte nicht selbst in der Lage ist, die notwendigen Hilfen zu leisten, und angenommen werden kann, daß der Empfänger der Information dazu in der Lage ist. Die notwendige Hilfe wird nach Lage der Dinge in erster Linie in einer Beratung und Unterstützung der Familie des Kindes bestehen (§ 27 KJHG). Dieses Leistungsangebot knüpft an die bei dem Kind beobachteten Leiden und Verletzungen an, deren Ursachen beseitigt werden müssen. Es setzt eine Aufklärung des entstandenen Verdachts einer strafbaren Handlung nicht voraus; vielmehr ist es ein Teil der Hilfe, möglichst gemeinsam mit den Eltern die Ursachen festzustellen. Dabei müssen in der Regel außer einem möglichen sexuellen Mißbrauch auch andere denkbare Ursachen in Erwägung gezogen werden, da die festgestellten Symptome zumeist nicht eindeutig auf eine Ursache hinweisen. Zur notwendigen Hilfe können ggf. auch vormundschaftsgerichtliche Maßnahmen und eine Trennung des Kindes von den Eltern gehören.

Wenn Hinweise vorliegen, daß ein Kind in seiner Familie geschädigt wird, müssen die Bediensteten der Kindertagesstätte prüfen, ob sie Hilfe für das

Kind für notwendig halten und, wenn ja, ob sie selbst — etwa durch ein Gespräch mit den Eltern — das Nötige tun können. Wenn dies ihre Möglichkeiten übersteigt, ist eine Weitergabe der Daten — an das Jugendamt oder an eine andere entsprechende Einrichtung — zulässig.

Die Weitergabe an eine weiterbetreuende Einrichtung kann vor allem in Betracht kommen, wenn die Kindertagesstätte es für notwendig hält, die Auffälligkeiten bei dem Kind noch länger zu beobachten. Das gilt beim Verdacht von Mißbrauch, Mißhandlung und Vernachlässigung gleichermaßen.

23. Kulturgut- und Denkmalschutz

Die Besitzerin eines Baudenkmals führte Beschwerde u. a. darüber, daß der ehrenamtliche Beauftragte für die Denkmalpflege die bei der Unteren Denkmalschutzbehörde für das Objekt geführten Bauakten nach Hause zugesandt bekam. Das Niedersächsische Ministerium für Wissenschaft und Kultur vertritt hierzu die Auffassung, daß für die Aufgabenerledigung des Beauftragten für die Denkmalpflege nach § 22 des Niedersächsischen Denkmalschutzgesetzes ein unmittelbarer Zugriff auf Verwaltungsvorgänge nicht erforderlich ist. Ich habe daraufhin dem Landkreis mitgeteilt, daß ich die Aktenübersendung für datenschutzrechtlich unzulässig ansehe. Mit ihr wurden dem Beauftragten für die Denkmalpflege personenbezogene Daten übermittelt, die er für die Wahrnehmung seiner Aufgabe nicht benötigte.

24. Forschung

24.1 Keine datenschutzrechtlichen Unbedenklichkeitserklärungen

Wie in den vergangenen Berichtszeiträumen wurde mir auch in den letzten zwei Jahren eine Vielzahl von Forschungsvorhaben mit der Bitte vorgelegt, hierzu eine datenschutzrechtliche Unbedenklichkeitsbescheinigung abzugeben. Ich habe in jedem Fall anhand der mir verfügbaren Unterlagen eine datenschutzrechtliche Bewertung durchgeführt. Ich mußte aber immer wieder darauf hinweisen, daß ich für derartige „Unbedenklichkeitsbescheinigungen", mit denen die Auskunftsbereitschaft gegenüber dem jeweiligen Forschungsteam erhöht werden soll, nicht zuständig bin. Ich kann die Projekte auch nicht dauernd datenschutzrechtlich begleiten, so daß es vorkommen mag, daß sich ein Forschungsteam nicht an meine datenschutzrechtlichen Forderungen hält. Ebenso ist es möglich, daß bei der konkreten Durchführung Datenschutzverstöße erfolgen, welche bei der Projektierung nicht vorhersehbar waren.

Soweit mit einem wissenschaftlichen Vorhaben, bei welchem personenbezogene Daten erhoben und verarbeitet werden, öffentliche Stellen berührt sind, bin nicht ich für die datenschutzgerechte Planung und Durchführung verantwortlich, sondern die forschende Stelle bzw. das jeweils zuständige Ressort. So ist beispielsweise für die Klärung rechtlicher Fragen bei der Einholung von Auskünften aus dem Melderegister — einer oft verwendeten Datenquelle bei Forschungsprojekten — das Niedersächsische Innenministerium der erste Ansprechpartner. Das jeweilige Ressort hat bei seiner Prüfung auch die Belange des Datenschutzes mitzuberücksichtigen. Selbstverständlich bin ich gerne bereit, insoweit ergänzend Hilfestellung zu leisten.

24.2 Auswertung der Akten von Sexualstraftätern

Das Niedersächsische Sozialministerium hat mich um datenschutzrechtliche Prüfung eines Forschungsprojektes der Georg-August-Universität Göttingen über verurteilte erwachsene Sexualstraftäter zur Frage ihrer sexuellen Auffälligkeit im Kindes- und Jugendalter gebeten.

Im Rahmen der Untersuchung sollen äußerst sensitive Fragen aus dem Intimbereich der Gefangenen gestellt werden. Solche Befragungen stoßen erfahrungsgemäß (vgl. AIDS-Befragung in den niedersächsischen Vollzugsanstalten) nicht nur auf Widerstand der Betroffenen, sondern lösen auch Kritik und Angriffe von Verbänden oder Organisationen aus, sobald auch nur im geringsten Zweifel an einem datenschutzkonformen Vorgehen bestehen.

Bedeutsam war, daß das Projekt auf freiwilliger Teilnahme basiert. Ich habe darauf hingewiesen, daß die Zustellung des Hinweisblattes über das Projekt an eine bestimmte Auswahl von Strafgefangenen („die wegen Verstößen gegen die sexuelle Selbstbestimmung in einer forensisch-psychiatrischen Abteilung behandelt werden") über die Leitung bzw. die Mitarbeiterinnen und Mitarbeiter dieser Abteilungen die Akzeptanz der Probanden beeinträchtigen könnte. Daher habe ich empfohlen, schon im Hinweisblatt auf den Weg der Verteilung näher einzugehen und vor allem deutlich zum Ausdruck zu bringen, daß der Forschungsgruppe zum Zeitpunkt der Verteilung des Hinweisblattes keine der Personen bekannt ist, die das Hinweisblatt erhalten, und daß seitens der Anstaltsleitung, Abteilungsleitung usw. keinerlei Druck auf Teilnahme an der Befragung ausgeübt werden darf.

Außerdem habe ich angeregt, bereits im Hinweisblatt festzulegen, daß personenidentifizierende Angaben zwar bei der Befragung erhoben werden — was mit Einwilligung der Betroffenen auch zulässig ist —, daß die Angaben jedoch unverzüglich in den Computer eingegeben und dabei sämtliche Personenbezüge fortgelassen sowie die personenbezogenen Erhebungsbogen vernichtet werden. Soweit eine personenbezogene Durchführung (z. B. zur Ermöglichung späterer fortführender Interviews) beabsichtigt ist, muß auch dies, verbunden mit einem Hinweis auf die entsprechenden datenschutzrechtlichen Schutzvorkehrungen, bereits im Hinweisblatt mitgeteilt werden. Ich habe gebeten, die vorgenannten Schutzvorkehrungen bzw. die Selbstverpflichtung zur unverzüglichen Löschung aller Personenbezüge in die Projektbeschreibung aufzunehmen. Darüber hinaus war im Hinweisblatt aufzunehmen, daß die erhobenen Daten ausschließlich zur Durchführung dieses Forschungsprojekts benutzt und für keinen anderen Zweck verwendet werden. Auch sollten die Datenschutzvorkehrungen in der Prokjektbeschreibung detailliert festgehalten werden.

Meine nach Vorlage aller Unterlagen gestellte Frage, ob es nicht möglich oder gar sinnvoll ist, ganz auf eine personenbezogene Erhebung zu verzichten, so daß für die freiwilligen Teilnehmer absolute Anonymität gewährleistet ist, wurde von der Universität Göttingen wie folgt beantwortet:

„Es werden lediglich die Namen derjenigen, die sich freiwillig zu der Untersuchung bereiterklärt haben, zur Verabredung des Untersuchungstermines benötigt. Die von den Probanden auszufüllende Einverständniserklärung zu der Untersuchung soll gesondert aufbewahrt werden. Name, Vorname und Anschrift werden nicht mehr auf der Anleitung und Dokumentation zum strukturierten Interview aufgeführt. Auf den einzelnen Anleitungen und Dokumentationen zum strukturierten Interview wird lediglich eine laufende Nummer aufgeführt. Solange noch die Informationen von den Probanden selber oder die Befundberichte von den Probanden erwartet werden, sollen auf einer

gesonderten Liste Namen und Kontrollnummern notiert werden — diese Liste wird, sobald die betreffende Erhebung abgeschlossen ist, vernichtet werden."

Mit diesem Verfahren habe ich mich einverstanden erklärt.

24.3 Fall-Kontroll-Studie Leukämie Münchehagen

Das Niedersächsische Sozialministerium hat das Bremer Institut für Präventionsforschung und Sozialmedizin (BIPS) beauftragt, eine Inzidenz-Studie zur Erfassung der Häufigkeit von Erkrankungen an Leukämie und Malignen Lymphomen in den Landkreisen Nienburg und Schaumburg-Lippe durchzuführen. Hintergrund der Beauftragung waren Hinweise auf eine Häufung derartiger Erkrankungen in der weiteren Umgebung der Sonderabfalldeponie Münchehagen. Wegen der gesundheits- und umweltpolitischen Sensibilität des Untersuchungsvorhabens hat sich das Sozialministerium frühzeitig mit mir in Verbindung gesetzt.

Meine Prüfung hat ergeben, daß den Belangen des Datenschutzes bei der Durchführung des Projektes Rechnung getragen wird. Die bisherigen Ergebnisse der Inzidenz-Studie für die Landkreise Nienburg und Schaumburg-Lippe haben nachdrücklich den gesundheitspolitischen Handlungsbedarf dokumentiert. Im Rahmen der Erhebung für die Inzidenz-Studie sind Daten von 570 Personen (davon 250 Leukämie-Erkrankungen) angefallen.

Im einer zweiten Phase des Projektes soll nunmehr eine Kontrollstudie durchgeführt werden, für deren Durchführung Kontakte geknüpft werden müssen

a) zu den Betroffenen (Kranken),
b) zu den Angehörigen der inzwischen verstorbenen Kranken sowie
c) zu Vergleichspersonen aus der „übrigen Bevölkerung".

Die Kontaktaufnahme zu den betroffenen Patienten über die Krankenhäuser bzw. über die Arztpraxen erschien problemlos. Die Ärzte in den betroffenen Kliniken bzw. die behandelnden niedergelassenen Ärzte sollten vom BIPS vorgefertigte Informationsschreiben erhalten; dementsprechend sollten die Patientinnen und Patienten mit ihrer Einwilligung befragt werden.

Zu klären war die Übermittlung der Vergleichspersonen über eine Gruppenauskunft nach dem Melderecht. Dabei war zu beachten, daß das BIPS ein unselbständiges Institut des Bremer Vereins für wissenschaftliche Forschung und damit eine privatrechtliche Einrichtung ist. Auch die Kontaktaufnahme zu den Angehörigen der verstorbenen Patienten war nicht problemlos. Zu den beiden letztgenannten Punkten habe ich im einzelnen wie folgt Stellung bezogen:

Die Beschaffung der Angaben zu den Vergleichspersonen soll über das Melderegister durch das Gesundheitsamt erfolgen. In Niedersachsen besteht für das Gesundheitswesen bisher keine gesetzliche Grundlage, so daß es auch an einer gesetzlichen Befugnisnorm zur Datenerhebung mangelt. Als Befugnisnorm für die Übermittlung von Meldedaten an das Gesundheitsamt kommt § 29 NMG in Frage, wonach u.a. Name, Anschrift, Geburtstag und Geschlecht listenmäßig nach Maßgabe des § 10 Abs. 1 Satz 1 NDSG an andere Behörden übermittelt werden dürfen. Die Notwendigkeit der Meldedaten zur rechtmäßigen Erfüllung der in der Zuständigkeit des Empfängers liegenden Aufgaben wird unterstellt.

Eine Melderegisterauskunft direkt an das BIPS zur Feststellung von Vergleichspersonen als Gruppenauskunft wäre nach § 33 Abs. 3 NMG zulässig, soweit dies im öffentlichen Interesse liegt. Vom Vorliegen eines solchen öffentlichen Interesses kann bei dem Forschungsvorhaben ausgegangen werden. Als Suchkriterien sind Alter und Geschlecht zugelassen. Mitgeteilt werden dürfen u. a., wie geplant, Name und Adresse. Auch bei einer einengenden Auslegung des Begriffs ‚öffentliches Interesse' in § 33 Abs. 3 NMG durch das zusätzliche Erfordernis der Abwägung mit den Belangen des Betroffenen dürfte wohl von einer zulässigen Übermittlung der Meldedaten an das BIPS ausgegangen werden.

Aus datenschutzrechtlicher Sicht ist die Kontaktaufnahme mit den Vergleichspersonen durch das Gesundheitsamt der durch das BIPS vorzuziehen. Die Kontaktaufnahme zu Angehörigen verstorbener Patienten durch den ehemaligen behandelnden Arzt bzw. die Klinik ist datenschutzrechtlich problemlos möglich. Daten Verstorbener fallen nicht unter das Datenschutzrecht. Geschützt bleiben jedoch die Daten der Angehörigen. Über den allgemeinen Datenschutz hinausgehend ist das Arztgeheimnis, welches nach dem Tod des Betroffenen weitergilt (vgl. § 203 Abs. 4 StGB). Das Arztgeheimnis zwischen behandelndem Arzt und Patienten gilt auch gegenüber den Angehörigen dieses Patienten. Es stellt jedoch keine Verletzung des vertrauensvollen Arzt-Patienten-Verhältnisses dar, wenn nach dem Tod die Angehörigen ohne Willen des Patienten unterrichtet oder auch aus Gründen einer wissenschaftlichen Untersuchung angesprochen werden.

Für bedenklich halte ich die Feststellung der Adressen der Angehörigen verstorbener Patienten mit Hilfe der Todesbescheinigungen der Gesundheitsämter und die Abfrage der Meldedaten hierzu. Diese Todesbescheinigungen haben ausschließlich den Zweck der Todesfeststellung, nicht aber den der Identifizierung von Angehörigen (§ 1 ff. des Gesetzes über das Leichenwesen). Auf den Todesbescheinigungen sind die Namen der Angehörigen regelmäßig nicht vermerkt (Nds. MBl. 1990, S. 546). Eine gesetzliche Grundlage für die Verwendung der unter Umständen auf der Todesbescheinigung vorhandenen Angaben über die Angehörigen besteht nicht. Sollten sich die Angaben über Angehörige aus anderen Unterlagen der Gesundheitsämter ergeben, so wäre auch deren Verwendung problematisch, da damit eine Zweckänderung der Daten verbunden wäre, für welche keine Rechtsgrundlage besteht (vgl. 21.4).

24.4 Muttermilchuntersuchung

Die Abteilung Epidemiologie und Sozialmedizin der Medizinischen Hochschule Hannover (MHH) hat mich über einen geplanten Modellversuch zur Errichtung und Erprobung regionaler Beobachtungspraxen zwecks Erhebung umweltbezogener Gesundheitsstörungen unterrichtet. Im Forschungsvorhaben Morbus sollte eine Erhebung der Schadstoffbelastung in der Muttermilch erstgebärender Frauen durchgeführt werden. Durch niedergelassene Kinderärzte sollten insgesamt 200 stillende erstgebärende Frauen angesprochen und um ihre Mitarbeit gebeten werden. Die Teilnehmerinnen wurden durch ein von der MHH konzipiertes Informationsblatt über das Forschungsprojekt informiert. Darin wurde im einzelnen dargestellt, für welche Zwecke die erhobenen Daten verwendet werden. Die Teilnahme war freiwillig — eine entsprechende Einverständniserklärung wurde zur Unterzeichnung vorgelegt. Die Auswertung selbst erfolgt anonym. Die behandelnden Ärzte werden in die Lage versetzt, ihre Patientinnen über die Ergebnisse der Untersuchung zu unterrichten. Nur dem Arzt selbst sind Name und Adresse der Teilnehmerinnen bekannt.

Die Beschreibung der Untersuchungskonzeption zeigt, daß Forschungsprojekte bei entsprechendem Willen datenschutzgerecht durchgeführt werden können, ohne daß es zwischen dem Grundrecht der Forschungsfreiheit und dem Grundrecht auf informationelle Selbstbestimmung zu unauflösbaren Konflikten kommen müßte.

24.5 Erbgesundheitspflege als Forschungsthema

Ein niedersächsischer Landkreis fragte an, wie die beantragte Einsichtnahme in Sterilisierungsakten aus der Zeit des Nationalsozialismus zu Forschungszwecken datenschutzrechtlich zu beurteilen ist. Es handelte sich dabei um Akten eines Erbgesundheitsgerichtes, die vom Gesundheitsamt des Landkreises verwaltet werden. Das Forschungsvorhaben sollte der Aufklärung nationalsozialistischer Gewaltmaßnahmen gegen Heimbewohnerinnen und -bewohner einer Anstalt für Behinderte dienen und wurde von einem Angehörigen einer Kommission für kirchliche Zeitgeschichte durchgeführt.

Da nach der bisherigen Rechtslage keine bereichsspezifische gesetzliche Regelung für die Übermittlung personenbezogener Daten zu Forschungszwecken besteht, kommt grundsätzlich nur eine Datenverarbeitung mit vorheriger Einwilligung der Betroffenen in Frage. Dies wäre jedoch im konkreten Fall auf faktische Grenzen gestoßen, da die Personen bereits verstorben oder sehr alt sind und in letzterem Fall sicherlich auch die Ermittlung des Aufenthaltes nicht ohne Schwierigkeiten möglich war.

Der Entwurf eines neuen Niedersächsischen Datenschutzgesetzes beinhaltet in § 25 eine Forschungsklausel, die im wesentlichen folgenden Inhalt hat:

— Zweckbindung für das einzelne Forschungsvorhaben,
— frühestmögliche Anonymisierung,
— keine Veröffentlichung von Namen bzw. nur bei Personen der Zeitgeschichte,
— strenge Erforderlichkeitsprüfung,
— Erfordernis eines eindeutig überwiegenden Forschungsinteresses gegenüber dem privaten Geheimschutzinteresse.

Ich meine, daß trotz der bisherigen gesetzgeberischen Untätigkeit Forschungsprojekte nicht verhindert werden sollten, bei denen ein datenschutzkonformes Verfahren gewählt wird. Trotz Fehlens einer gültigen Eingriffsgrundlage nehme ich daher schon jetzt die geplante Forschungsklausel des NDSG-E zur Grundlage meiner datenschutzrechtlichen Bewertung. Im beschriebenen Fall war eine Zustimmung zur Akteneinsicht seitens des Landkreises vertretbar. Dabei mußte allerdings sichergestellt sein, daß nur der Forscher selbst die Akten für den bestimmten Zweck verarbeitet und aus den Veröffentlichungen keine Rückschlüsse auf einzelne Personen möglich sind.

25. Hochschulen

25.1 Hochschulgesetz

Anfang 1992 leitete mir das Ministerium für Wissenschaft und Kultur den Referentenentwurf für ein Fünftes Gesetz zur Änderung des Niedersächsischen Hochschulgesetzes (NHG) mit der Bitte um Stellungnahme zu. Dieser Ent-

wurf sieht unter anderem eine Überarbeitung der datenschutzrechtlichen Vorschriften im NHG vor. Der Entwurf wurde inzwischen dem Landtag zur Beschlußfassung zugeleitet (LT-Drs 12/3810). Nach intensiver Erörterung der Regelungen konnten einige wesentliche datenschutzrechtliche Verbesserungen gegenüber dem ursprünglichen Entwurf erreicht werden. Nicht durchsetzen konnte ich mich bei der Verarbeitungsgeneralklausel des § 44 a Abs. 1, welche die Zwecke der Daten über nicht-bedienstete Hochschulangehörige, also insbesondere Studierende, sehr weit faßt.

Massive Bedenken hatte ich zunächst gegenüber einer neuen Regelung, die pauschal die Erhebung und Verwendung von Daten zur Beurteilung (Evaluation) der Bewerbungssituation, der Lehr- und Forschungstätigkeit, des Studienangebots sowie des Ablaufs von Studium und Prüfungen zuließ. Als Begründung für die Regelung wurde vom Ministerium angegeben, die Daten würden gebraucht, um die Ursachen für ein ineffektives Studienangebot und für die teilweise sehr lange Studiendauer ausfindig zu machen. Es wurde versichert, daß aus den Ergebnissen der durchgeführten Evaluationen ausschließlich organisatorische und in keinem Fall personelle Konsequenzen gezogen werden sollten. Durch folgende Regelungen soll nun Datenschutzverstößen vorgebeugt werden:

— Der Kreis der Betroffenen wird auf Hochschulangehörige beschränkt.
— In einer Hochschulsatzung sind bei nicht-freiwilliger Datenerhebung zu regeln: Inhalt und Umfang einer eventuellen Auskunftspflicht, Zweck der Evaluation, Erhebungsmerkmale und Erhebungsverfahren.
— Durch Aufnahme eines Zweckentfremdungsverbots und einer frühestmöglichen Anonymisierungspflicht soll ausgeschlossen werden, daß die Untersuchungsergebnisse zu konkreten personellen Maßnahmen und zu Eingriffen in die Lehr- und Forschungstätigkeit verwendet werden.
— Die hochschulinterne Transparenz der Evaluationen ist durch den Erlaß der Satzung sowie durch eine Pflicht zur Rechenschaftslegung gesichert.

Es wird sich erweisen, ob diese Regelung, die datenschutzrechtlich zwischen den Regelungen zur Organisationskontrolle, zur Hochschulstatistik und zur Forschung steht, praktikabel ist.

Mit meiner Forderung, die Nutzung privater PC für dienstliche Zwecke einzuschränken, stieß ich in bezug auf die Verarbeitung von Hochschuldaten auf Verständnis: Datenverarbeitung nach dem NHG soll künftig nur auf Datenverarbeitungsanlagen der Hochschulen erfolgen. Davon unberührt bleibt die Notwendigkeit einer generellen Regelung, welche auch die Verarbeitung von Studentendaten durch das Lehrpersonal erfaßt.

25.2 Übermittlung von Studentendaten an eine Kommunalverwaltung

Eine Stadt ist an eine Hochschule mit der Bitte herangetreten, ihr die Namen und Adressen der immatrikulierten Studentinnen und Studenten zu überlassen. Dies wurde damit begründet, daß die Studierenden sich nach den Vorschriften des Melderechts mit Hauptwohnsitz in der Stadt anmelden müßten, dies aber in vielen Fällen nicht tun würden. Durch die Unvollständigkeit ihrer Einwohnermeldekartei würde der Stadt ein Einnahmeausfall im Rahmen des kommunalen Finanzausgleichs entstehen. Die Hochschule hat die Daten der Studierenden mit dem Hinweis auf datenschutzrechtliche Bedenken nicht herausgegeben. Beide Dienststellen haben mich eingeschaltet.

§ 44 a NHG sieht keine Datenübermittlung an andere Stellen vor. Eine entsprechende Regelung sollte nach dem Willen des Gesetzgebers auch nicht ge-

troffen werden. Wie aus dem schriftlichen Bericht zur Änderung des NHG vom 26. April 1989 (LT-Drs 11/3780) hervorgeht, „soll nach Ansicht des Wissenschaftsausschusses zunächst der Erlaß eines datenschutzrechtlichen Querschnittsgesetzes abgewartet werden, um überflüssige Normierung zu vermeiden und um feststellen zu können, ob und ggf. inwieweit neben dem künftigen allgemeinen Datenschutzrecht überhaupt noch ein Bedarf für eine hochschulspezifische Regelung zu diesem Thema besteht." Nach Erörterung der Problematik mit dem Niedersächsischen Innenministerium habe ich der Stadt mitgeteilt, daß ich die Bedenken der Hochschule hinsichtlich der Weitergabe der Daten der Studierenden für den angestrebten Zweck teile. Die Übermittlung von Daten aus dem Immatrikulationsregister würde im Ergebnis eine Art Kontroll- oder Vergleichsmitteilung darstellen, die die Meldebehörde in die Lage versetzen soll zu überprüfen, ob die Studentinnen und Studenten die ihnen nach dem Niedersächsischen Meldegesetz obliegenden Verpflichtungen ordnungsgemäß erfüllt haben. Hierfür enthält das Melderecht keine Rechtsgrundlage.

Zwar hat nach § 13 NMG der Meldepflichtige im Einzelfall die zur Führung des Melderegisters erforderlichen Auskünfte zu erteilen. Eine Datenerhebung von Dritten, um die es sich hier handeln würde, sieht das Melderecht in diesem Zusammenhang aber nur für den Wohnungsgeber und seine Beauftragten bzw. (bei Binnenschiffern und Seeleuten) für Schiffseigner und Reeder vor (§ 13 Abs. 3 NMG). Die hier in Rede stehende Erhebung/Übermittlung personenbezogener Daten zu Kontrollzwecken ist im Gesetz nicht vorgesehen. Die nach § 40 NMG im Anschluß an die Neuregelung des Hauptwohnungsbegriffs mögliche generelle Überprüfung von Meldefällen zur Berichtigung des Melderegisters hat der Gesetzgeber nur für eine befristete Zeit zugelassen.

Angesichts der bereichsspezifischen datenschutzrechtlichen Vorschriften über die Erhebung/Übermittlung von personenbezogenen Daten im NMG kann ein Rückgriff auf das Niedersächsische Datenschutzgesetz nicht erfolgen. Die Übermittlung von Daten aus dem Immatrikulationsregister ist damit unzulässig.

Aus verwaltungspraktischer Sicht kam nach meiner Auffassung in Betracht, daß die Stadt der Hochschule vorgefertigte Schreiben an die Studierenden zur Verfügung stellt und diese die Verteilung/Versendung an die bei ihr eingeschriebenen Studentinnen und Studenten übernimmt. Da auf diese Weise weder eine Datenerhebung durch die Stadt noch eine Datenübermittlung an sie erfolgt, wäre ein solches Verfahren aus Datenschutzgründen nicht zu beanstanden.

26. Niedersächsische Landesbibliothek

Ein Benutzer der Niedersächsischen Landesbibliothek in Hannover teilte mir mit, daß dort bei seiner Anmeldung die Nummer seines Personalausweises registriert worden ist. Sein Hinweis, daß diese Vorgehensweise in anderen öffentlichen Einrichtungen nicht mehr praktiziert werde, veranlaßte das Personal nicht zu einer anderen Vorgehensweise.

In ihrer Stellungnahme hat die Leitung der Landesbibliothek darauf hingewiesen, daß die Erhebung von Personaldaten der Benutzerinnen und Benutzer entsprechend der für die Einrichtung maßgeblichen Benutzungsordnung vom 6. November 1975 (Nds. MBl. S. 1708) i. d. F. vom 5. Juli 1978 (Nds. MBl. S. 995) erfolgt. Danach hat sich die Antragstellerin oder der Antragsteller durch einen amtlichen Ausweis mit Lichtbild auszuweisen. Die Feststellung

der persönlichen Identität und der Anschriften der Benutzerin oder des Benutzers wird für unentbehrlich gehalten, insbesondere um Mahnungen zuzustellen und Rückgabeansprüche geltend zu machen. Wie weiter ausgeführt, habe die Nummer des Personalausweises bei Nachfragen bei den Einwohnermeldeämtern die relativ häufig notwendige Ermittlung neuer Anschriften erleichtert.

Dennoch war die Leitung der Landesbibliothek sofort bereit, für die Zukunft (ab 15. Juli 1991) auf die Registrierung der Personalausweisnummer der Benutzer zu verzichten. Ich habe die Hoffnung, daß dieses Beispiel — sofern in anderen öffentlichen Einrichtungen noch erforderlich — Schule macht.

27. Schulen

27.1 Schulgesetz

Die von mir seit langem geforderte bereichsspezifische landesgesetzliche Grundlage (vgl. X 27) für Eingriffe in das informationelle Selbstbestimmungsrecht von Schülerinnen sowie Schülern und Erziehungsberechtigten hat das Niedersächsische Kultusministerium nunmehr mit dem Entwurf eines Vierten Gesetzes zur Änderung des Niedersächsischen Schulgesetzes (LT-Drs 12/3300) vorgelegt. Die erste Beratung hat in der Plenarsitzung des Niedersächsischen Landtages am 18. Juni 1992 stattgefunden. Der Entwurf sieht folgende Regelungen vor:

„§ 20 b — Verarbeitung personenbezogener Daten —

(1) Für die Verarbeitung personenbezogener Daten gelten die Bestimmungen des Niedersächsischen Datenschutzgesetzes, soweit sich aus den Absätzen 2 und 3 nichts anderes ergibt.
(2) Schulen, Schulbehörden, Schulträger, Schülervertretungen und Elternvertretungen dürfen personenbezogene Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten verarbeiten, soweit dies zur Erfüllung des Erziehungs- und Bildungsauftrages und der Fürsorgeaufgaben erforderlich ist; das gilt auch für Gesundheitsämter, soweit sie Aufgaben nach den §§ 40 und 41 wahrnehmen, und für Träger der Schülerbeförderung, soweit sie Aufgaben nach § 94 wahrnehmen.
(3) Das Recht auf Auskunft, Einsicht in Unterlagen, Berichtigung, Sperrung oder Löschung von Daten wird für minderjährige Schülerinnen und Schüler durch deren Erziehungsberechtigte ausgeübt. Die Einsicht in Unterlagen kann eingeschränkt oder versagt werden, soweit es zum Schutze Dritter erforderlich ist.
(4) Das Kultusministerium wird ermächtigt, durch Verordnung zu regeln, welche personenbezogenen Daten der Schülerinnen und Schüler und ihrer Erziehungsberechtigten von der Schule für Verwaltungsaufgaben verarbeitet und beim Übergang in eine andere Schule übermittelt werden dürfen."

Ein erster Entwurf einer Verordnung gemäß § 20 b Abs. 4 liegt mir mittlerweile vor. Über diesen Entwurf wird noch intensiv zu diskutieren sein.

Insgesamt kann ich feststellen, daß die vorgesehene bereichsspezifische Regelung zu einer Verbesserung des Datenschutzes in den Schulen beitragen wird.

Das Problem der Verarbeitung personenbezogener Daten auf privaten Rechnern von Lehrkräften wird bei der Beratung in den Ausschüssen des Niedersächsischen Landtages noch näher zu erörtern sein. Ich halte es für erforderlich, eine Verordnungsermächtigung hierzu in § 20 b aufzunehmen.

27.2 Schulgesundheitspflege

Darüber hinaus halte ich die Aufnahme von konkreten Bestimmungen zur Schulgesundheitspflege in das Schulgesetz für dringend erforderlich. Die bisherigen und geplanten Regelungen reichen nicht aus. Dies gilt auch für den Schulpsychologischen Dienst. Ich bin mir zwar bewußt, daß Vorschriften zur Schulgesundheitspflege auch in ein Gesundheitsgesetz aufgenommen werden könnten. Da aber für mich zur Zeit nicht erkennbar ist, daß ein solches Gesetz noch in dieser Legislaturperiode verabschiedet wird (vgl. 21.2), halte ich die Aufnahme von entsprechenden Bestimmungen in das Niedersächsische Schulgesetz für angebracht.

Ich habe dem Kultusministerium und dem Sozialministerium vorgeschlagen, folgende Gesetzesbestimmungen in das Niedersächsische Schulgesetz aufzunehmen:

„(1) Im Rahmen der Schulgesundheitspflege sind Schülerinnen und Schüler zur Teilnahme an den ärztlichen Untersuchungen zur Feststellung der Schulfähigkeit sowie vor Aufnahme in ein Berufsgrundbildungsjahr verpflichtet. Zur Schulgesundheitspflege gehören auch Folgeuntersuchungen sowie Maßnahmen der Schulzahnpflege. Die Teilnahme an diesen Maßnahmen ist freiwillig.
(2) Den Erziehungsberechtigten oder den volljährigen Schülerinnen und Schülern ist Gelegenheit zur Besprechung der Ergebnisse und zur Einsichtnahme in die Unterlagen zu geben. Die Einsicht in Akten soll durch einen Arzt vermittelt werden, soweit zu befürchten ist, daß diese den Beteiligten einen unverhältnismäßigen Nachteil, insbesondere an der Gesundheit, zufügen würde.
(3) Die Gesundheitsämter teilen der zuständigen Stelle nur die für deren Entscheidungen oder Maßnahmen erforderlichen Untersuchungsergebnisse mit. Wird das Gesundheitsamt nicht aufgrund besonderer gesetzlicher Vorschriften zur Vorbereitung schulischer Entscheidungen tätig, so bedarf die Unterrichtung der zuständigen Stelle der Einwilligung der volljährigen Schülerin bzw. des volljährigen Schülers oder der Erziehungsberechtigten. Dies gilt nicht, soweit dies zur Durchführung von gesundheitssichernden Maßnahmen im überwiegenden Interesse des Wohls der minderjährigen Schülerinnen bzw. Schüler erforderlich ist. Medizinische und psychologische Befunde dürfen nicht durch automatisierte Verfahren übermittelt werden.
(4) Das Sozialministerium regelt durch Verordnung, welche personenbezogene Daten für Zwecke der Schulgesundheitspflege verarbeitet werden dürfen."

Das Sozialministerium hat signalisiert, daß es diesen Vorschlag mit einigen kleinen Modifikationen dem Kultusministerium zur Aufnahme in das Schulgesetz empfiehlt.

Darüber hinaus sollte § 40 Abs. 5 des Niedersächsischen Schulgesetzes hinsichtlich der Bestimmungen über den Schulpsychologischen Dienst wie folgt geändert werden:

„Der Schulpsychologische Dienst teilt der zuständigen Stelle nur die für deren Entscheidung oder Maßnahmen erforderlichen Untersuchungsergebnisse mit. Eine Datenübermittlung bedarf des schriftlichen Einverständnisses der voll-

jährigen Schülerin bzw. des volljährigen Schülers oder der Erziehungsberechtigten. Dies gilt nicht, soweit dies im Interesse des Wohls der minderjährigen Schülerin bzw. des minderjährigen Schülers erforderlich ist."

27.3 Lernmittelfreiheit

Eine Vielzahl von Anfragen beschäftigte sich mit dem Niedersächsischen Gesetz über Lernmittelfreiheit vom 24. April 1991 (Nieders. GVBl. S. 174), der Verordnung zur Durchführung des Niedersächsischen Gesetzes über Lernmittelfreiheit vom 14. Mai 1991 (SVBl. S. 142) und dem Erlaß des Niedersächsischen Kultusministeriums vom 14. Mai 1991 zur Durchführung des Niedersächsischen Gesetzes über Lernmittelfreiheit und der Verordnung über Lernmittelfrei im Schuljahr 1991/92 (SVBl. S. 144).

In dem Erlaß ist u. a. vorgesehen, daß die Schülerinnen und Schüler in einem vorgeschriebenen Stempelaufdruck (für jedes Schulbuch) ihren Namen einzutragen haben. Das heißt, daß für mehrere Jahre erkennbar ist, wer dieses Buch benutzt hat. Eine Alternative wäre, nur die Inventarnummer des Buches zu vermerken. Aus einer korrespondierenden Liste ließe sich im Einzelfall der Name der Nutzerin bzw. des Nutzers feststellen.

Das Niedersächsische Kultusministerium hat hierzu mitgeteilt, daß nicht vorausgesetzt werden kann, daß sich jede Schülerin bzw. jeder Schüler die Inventarnummern ihrer bzw. seiner Bücher merkt, und daß ein Verbot individueller Kennzeichnung eingehalten wird. Zur Vermeidung von Verwechselungen ist für die Zeit, in der das Buch der Schülerin bzw. dem Schüler zur Leihe übergeben wird, der Vermerk des Namens und der Klasse sinnvoll.

Um jedoch dem Gedanken des Datenschutzes Rechnung zu tragen, zieht das Kultusministerium eine wirkungsvolle und praktikable Form der Anonymisierung in Erwägung:

1. Die Inventarnummer wird wie bisher als dauerhafte Kennzeichnung in den Stempeleindruck eingetragen.
2. Die Angabe des Namens und der Klasse erfolgt auf Klebeetiketten, die bei Rückgabe des Buches wieder entfernt werden.
3. Auf die Eintragung des Ausgabe- und Rückgabedatums wird an dieser Stelle verzichtet, da ein Vermerk darüber im Lernmittelleihschein erfolgt.

Eine entsprechende Regelung wird zusammen mit den Durchführungsbestimmungen für das Schuljahr 1992/93 veröffentlicht. Ich habe unter datenschutzrechtlichen Gesichtspunkten keine Bedenken gegen dieses Verfahren.

27.4 Förderunterricht

Ein Petent hat mir mitgeteilt, daß in der von seinem Kind besuchten Grundschule die Namen der Kinder, die am Förderunterricht teilnehmen, für jeden sichtbar an die Tafel geschrieben werden. Diese Auflistung bleibt ganzjährig an der Tafel und kann an Elternabenden, Elternsprechtagen und anderen Veranstaltungen mit den Eltern von diesen eingesehen werden.

Diese listenmäßige Aufzählung von Schülerinnen und Schülern fällt zwar nicht unter die Bestimmungen des gegenwärtig geltenden NDSG. Gleichwohl gebietet das Recht auf informationelle Selbstbestimmung, die für die Verarbeitung von personenbezogenen Daten in Dateien geltenden Grundsätze

auch auf personenbezogene Informationen außerhalb von Dateien anzuwenden. Hiernach sind personenbezogene Informationen so aufzubewahren, daß niemand unbefugt Einsicht nehmen kann.

Das eingangs geschilderte Verfahren trägt dieser Schutzabsicht — auch nach Meinung des Niedersächsischen Kultusministeriums — nicht Rechnung. Das Fachressort hält zudem eine Veröffentlichung in dieser Form auch für pädagogisch fragwürdig.

27.5 Suchtprävention und Verhalten bei Drogenproblemen an niedersächsischen Schulen

Durch Gemeinsamen Runderlaß des Kultusministeriums, des Sozialministeriums, des Innenministeriums und des Justizministeriums vom 26. Mai 1992 (SVBl. S. 201) ist mit Zustimmung des Landesbeauftragten für den Datenschutz hinsichtlich der Bestimmungen über das Verhalten bei Suchtmittelmißbrauch von Schülerinnen und Schülern die Suchtprävention und das Verhalten bei Drogenproblemen an niedersächsischen Schulen geregelt worden.

Wenn der begründete Verdacht besteht, daß eine Schülerin oder ein Schüler legale Drogen mißbraucht, illegale Drogen konsumiert oder an einer stoffungebundenen Suchtform leidet, hat die Lehrkraft die Schulleitung über diesen Verdacht und die geplanten und eingeleiteten pädagogischen Hilfen zu unterrichten. Davon kann im Einzelfall abgesehen werden, insbesondere, wenn sich die Schülerin oder der Schüler offenbart und um Verschwiegenheit bittet.

Handelt es sich um minderjährige Schülerinnen oder Schüler, ist grundsätzlich mit den Erziehungsberechtigten zusammenzuarbeiten. Wenn es dem Wohle des Kindes dient, kann zunächst davon abgesehen werden, die Erziehungsberechtigten zu informieren. Bei allen Entscheidungen gilt, daß pädagogische Maßnahmen der Lehrkräfte im Vordergrund stehen sollen. Ermittlungen mit strafrechtlicher Zielsetzung sind nicht Aufgabe der Schule.

27.6 Zusammenarbeit zwischen Kindergarten und Grundschule

Nach dem Erlaß des Niedersächsischen Kultusministeriums vom 27. September 1979 „Empfehlung zur Zusammenarbeit von Kindergarten und Grundschule" (SVBl. S. 291) sollen Kindergarten und Grundschule eng zusammenarbeiten. Wörtlich heißt es unter Ziffer 1.: „Dies erfordert eine enge Zusammenarbeit beider Institutionen, ihrer Erzieher und Lehrer sowie der Erziehungsberechtigten". Ziffer 3. betont, daß „die Zusammenarbeit nur dann auf Dauer wirksam werden kann, wenn sie von den Eltern mitgetragen wird. Deshalb ist bei allen konkreten Maßnahmen der Kooperation für die Beteiligung der Erziehungsberechtigten Sorge zu tragen."

Als Beispiel für eine Zusammenarbeit ist in diesem Erlaß des Kultusministeriums unter Ziffer 2.6 ausgeführt:

„Fragen der Einschulung:
z. B. Informationen über Anmeldung, amtsärztliche Untersuchung, Feststellung der Schulfähigkeit, Einschulungsgottesdienst; Vorschläge für die Klassenzusammensetzung; Einzelberatung von Eltern (z.B. vorzeitige Einschulung, Zurückstellung mit Empfehlung besonderer Hilfe)."

Das Niedersächsische Kultusministerium hat mir zugestimmt, daß der Erlaß bei allen konkreten Maßnahmen im Rahmen der Kooperation zwischen Kindergarten und Grundschule die Beteiligung der Erziehungsberechtigten verlangt. Im Widerspruch dazu steht in einigen Fällen das Verhalten von Kindergärten. In einem Fall sind z. B. die Erziehungsberechtigten noch nicht einmal darüber unterrichtet worden, daß der Kindergarten in einem Beobachtungsbogen eine — im einzelnen begründete — Empfehlung abgegeben hat, ein sogenanntes „Kann-Kind" nicht einzuschulen.

Datenschutzrechtlich wäre diese Datenübermittlung nach noch geltendem Recht — auch ohne Zustimmung der Erziehungsberechtigten — nur zulässig, wenn sie zur Wahrnehmung der Aufgaben der aufnehmenden Schule erforderlich wäre. Aus fachlicher Sicht ist aber eine solche Datenübermittlung ohne Zustimmung der Erziehungsberechtigten nicht erwünscht, wie sich aus dem zitierten Erlaß ergibt.

Ich bin gemeinsam mit dem Niedersächsischen Kultusministerium der Auffassung, daß eine Datenübermittlung vom Kindergarten an die Grundschule nur mit Zustimmung der Erziehungsberechtigten zulässig ist. Das Niedersächsische Kultusministerium hat deshalb mit Erlaß vom 6. August 1992 (SVBl. S. 253) die Ziffer 3 des Erlasses um eine entsprechende Aussage ergänzt.

27.7 Bedarfsermittlung für die Einrichtung von Schulen

Mehrere Eingaben beschäftigten sich mit der Zulässigkeit der von Kommunen vorgenommenen Bedarfsermittlung zur Einrichtung von Gesamtschulen, von vollen Halbtagsschulen und Schulen mit ganztägiger Betreuung von Kindern.

Zur Einrichtung von Gesamtschulen ist festzustellen, daß die Schulträger nach § 86 des Niedersächsischen Schulgesetzes (NSchG) berechtigt sind, Gesamtschulen zu errichten, soweit hierfür aufgrund von Schülerzahlen und des Interesses von Schülerinnen und Schülern oder Erziehungsberechtigten ein besonderes Bedürfnis besteht. Zur Feststellung eines solchen Bedürfnisses ist es erforderlich, daß die Erziehungsberechtigten einer hinreichenden Zahl von Kindern für eine solche Schule ein konkretes Interesse bekunden. In diesem Zusammenhang ist es unbedenklich, wenn Erziehungsberechtigte von Schülerinnen und Schülern, die sich an einer allgemeinen Fragebogenaktion über die Schulen — aus welchen Gründen auch immer — nicht oder nicht rechtzeitig beteiligt haben, gezielt angeschrieben und nochmals um eine konkrete Äußerung gebeten werden. Es gibt jedoch keine Rechtsverpflichtung, sich an einer solchen Umfrage zu beteiligen. Bedarfsermittlungen zur Einrichtung von vollen Halbtagsschulen und Schulen mit ganztägiger Betreuung der Kinder sind ebenfalls zulässig. Rechtsgrundlage ist § 18 Abs. 2 des NSchG, wonach die Kommunen verpflichtet sind, Schulentwicklungspläne aufzustellen.

Bei all diesen Fragebogenaktionen sollte jedoch in den Fragebogen ein Hinweis auf die Freiwilligkeit aufgenommen werden. Das Aufbringen von Schulstempeln sollte unterbleiben. Zulässig ist jedoch die Kennzeichnung der Fragebogen nach Schulbezirken.

27.8 Verarbeitung von Schülerdaten auf privaten Rechnern

Ich habe bereits unter X 27.5 festgestellt, daß für das Betreiben eines privaten Rechners ein vorgeschriebenes Genehmigungsverfahren festgelegt worden ist. Lehrkräfte, die auf einem privaten Rechner personenbezogene Daten von

Schülerinnen und Schülern verarbeiten wollen, bedürfen dazu der schriftlichen Genehmigung der Schulleitung. Eine Kopie des genehmigten Antrages leitet die Schule auf dem Dienstwege über das Kultusministerium dem Landesbeauftragten für den Datenschutz zu. Aus den bei mir eingegangenen Kopien schließe ich, daß das Verfahren nicht überall bekannt ist, anderenfalls müßte nach meiner Einschätzung die Anzahl der Meldungen deutlich höher liegen. Ich habe das Niedersächsische Kultusministerium darauf aufmerksam gemacht, daß es den Schulen nochmals mitteilt, daß diese Meldungen vorgeschrieben sind (vgl. 4.4, 4.6.14).

Nach dem Erlaß des Kultusministeriums vom 30. August 1990 (SVBl. S. 350) nehmen die Lehrkräfte im Rahmen einer Verpflichtungserklärung davon Kenntnis, daß sie mit einer datenschutzrechtlichen Überprüfung durch mich rechnen müssen. 1992 habe ich die bei mir gemeldeten Lehrer-PC von zwei Schulen überprüft. Die Akzeptanz bei den Lehrern war insgesamt positiv. Zu bemängeln hatte ich überwiegend einen fehlenden Paßwortschutz sowie die unsichere Lagerung der Datenträger. Weitere Prüfungen in diesem Bereich sind geplant.

27.9 EDV-gestützte Stunden- und Vertretungsplanerstellung auf privaten Rechnern

Eine Eingabe befaßte sich mit der Frage, ob ein stellvertretender Schulleiter einen Vertretungsplan oder einen Stundenplan mit seinem privaten Rechner im häuslichen Arbeitszimmer erstellen darf. Hierzu stelle ich fest, daß das Niedersächsische Kultusministerium in seinem Erlaß vom 30. August 1990 (SVBl. S. 350) unter Ziffer 1.3 die Verarbeitung personenbezogener Daten von Lehrkräften auf privaten Rechnern untersagt hat. Auch die Angaben über Lehrkräfte, die in ein Programm zur Erstellung eines Stundenplans oder eines Vertretungsplans eingegeben werden, sind personenbezogene Daten. Wie sich aus o. g. Erlaß eindeutig ergibt, kann die Verwendung privater Rechner zur Erledigung dienstlicher Aufgaben wegen der damit verbundenen datenschutzrechtlichen Risiken nur in Ausnahmefällen und nur mit Einschränkungen zugelassen werden. Diese Ausnahmen und Einschränkungen sind abschließend geregelt, so daß die Verarbeitung personenbezogener Daten der Lehrkräfte auf privaten Rechnern unabhängig von einer eventuellen Zustimmung der Betroffenen ausgeschlossen ist.

27.10 Übersicht über die Entlastungsstunden an den Personalrat

Ein Petent hat angefragt, ob es zulässig sei, daß die Schulleitung dem Personalrat eine namentliche Übersicht der den einzelnen Lehrkräften gewährten Entlastungsstunden zur Verfügung stellt, aus der auch die Berechnungs- bzw. Rechtsgrundlage hervorgehen. Insbesondere ging es um Entlastungsstunden für besondere unterrichtliche und Verwaltungsbelastungen wegen Schwerbehinderung, Fachleitertätigkeit, Koordinationstätigkeit und Erreichen einer bestimmten Altersgrenze.

Die Datenübermittlung richtet sich gemäß § 7 Abs. 2 NDSG nach § 24 BDSG in der Fassung vom 27. Januar 1977. Da der in dieser Vorschrift genannte Datenrahmen überschritten wird, wäre eine Datenübermittlung an den Personalrat nur unter den in § 24 Abs. 1 BDSG genannten Voraussetzungen zulässig, also zur Wahrung eines berechtigen Interesses, wenn schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. Über die Grundsätze für Stundenanrechnungen auf die Unterrichtsverpflichtungen der Lehrerinnen und Lehrer beschließt die Gesamtkonferenz. Die von der Gesamtkonferenz be-

schlossenen Grundsätze sind jedoch keine „Bestimmung" im Sinne des § 67 Abs. 1 Nr. 2 des Niedersächsischen Personalvertretungsgesetzes. Hiervon werden Gesetze, Verordnungen, Verwaltungsvorschriften sowie Tarifverträge und Dienstvereinbarungen erfaßt, nicht aber Beschlüsse eines Gremiums innerhalb einer Dienststelle. Im übrigen ist für die Ausführung der Beschlüsse der Gesamtkonferenz die Schulleiterin bzw. der Schulleiter verantwortlich.

Es gehört eindeutig nicht zum Aufgabenbereich des Personalrats einer Schule, die Ausführung der Beschlüsse der Gesamtkonferenz zu überwachen. Anhaltspunkte für eine derartige Kontrollfunktion des Personalrates ergeben sich weder aus dem Niedersächsischen Personalvertretungsgesetz noch aus dem Niedersächsischen Schulgesetz. Darüber hinaus gibt es jedoch Entlastungsstunden, die aufgrund von Bestimmungen im Sinne des § 67 Abs. 1 Nr. 2 des Niedersächsischen Personalvertretungsgesetzes gewährt werden (Altersgrenze, Schwerbehinderung). Nach der Rechtsprechung des Bundesverwaltungsgerichts zu § 68 Abs. 2 Satz 1 des Bundespersonalvertretungsgesetzes steht der Personalvertretung kein allumfassendes Informationsrecht zu, um eine allgemeine Kontrolle der Tätigkeit der Dienststelle vorzunehmen (vgl. auch den Beschluß des Bundesverwaltungsgerichts vom 29. August 1990, NJW 1991, 373). Allein der Hinweis auf allgemeine Überwachungsaufgaben reicht zur Begründung eines Informationsanspruches nicht aus.

Die Übermittlung der Daten an den Personalrat ist danach zur Wahrung berechtigter Interessen dieses Gremiums nicht erforderlich.

27.11 Weitergabe von Lehrerdaten an die Elternvertretung

Meine Ausführungen unter VII 27.6 und IX 27.13 beschäftigten sich mit der Weitergabe von Daten an Erziehungsberechtigte. In Übereinstimmung mit dem Niedersächsischen Kultusministerium halte ich diese Datenübermittlung auch weiterhin nicht für erforderlich. Anders verhält es sich bei der Weitergabe von Lehrerdaten an gewählte Elternvertreterinnen und -vertreter, die Vorsitzenden der Klassenelternschaften.

Gemäß § 7 Abs. 2 NDSG hat sich die Übermittlung von Lehrerdaten nach § 24 BDSG a. F. zu richten, da bestehende dienst- oder arbeitsrechtliche Rechtsverhältnisse betroffen sind. Die fragliche Datenübermittlung wäre hiernach zulässig. Die Erforderlichkeit der Datenübermittlung zur Wahrung berechtigter Interessen der Elternvertretung ist gegeben. Nach § 69 Abs. 1 des Niedersächsischen Schulgesetzes wirken die Erziehungsberechtigten u. a. durch die Klassenelternschaften in der Schule mit. Für die Erfüllung des gemeinsamen Erziehungsauftrages von Schule und Elternhaus sowie für das gewünschte enge Zusammenwirken von Lehrkräften und Elternvertretungen ist es erforderlich, daß die betroffenen Lehrkräfte für die Vorsitzenden der Klassenelternschaften auch außerhalb der Unterrichtszeit erreichbar sind. Selbstverständlich sollen die Elternvertreterinnen und -vertreter nur in begründeten Einzelfällen von diesen Daten Gebrauch machen. Sie sind auch nicht befugt, diese an Dritte weiterzugeben.

27.12 Lehrerdaten

Ein Lehrer eines niedersächsischen Schulzentrums, bestehend aus Haupt- und Realschule mit Orientierungsstufe, bat mich um datenschutzrechtliche Bewertung des Aushangs einer Personalentscheidung am „Schwarzen Brett". Gegenstand der Eingabe war eine Entscheidung der Schulleitung über die Gewährung von Sonderurlaub für die Teilnahme an einer internationalen Lehr-

mittelmesse. Der Petent brachte vor, daß der Leiter seiner Schule am allgemein zugänglichen „Schwarzen Brett" die Entscheidung veröffentlicht habe. Die Aushangstelle habe sich innerhalb des Verwaltungsbereichs vor dem Lehrerzimmer befunden, wo nach seiner Darstellung auch Schüler Zutritt gehabt haben.

Im Aushang waren aufgeführt:

— Vorgabe des zuständigen Schulaufsichtsamtes, daß 10 % eines Kollegiums teilnehmen können,
— Auswahlkriterien,
— Ablehnung des Sonderurlaub-Antrages des Petenten (darunter waren die Gründe für die Ablehnung aufgeführt),
— namentliche Aufführung der sechs ausgewählten Mitarbeiter, die zur Fachmesse fahren durften.

Die Schulleitung hatte den Aushang zwischenzeitlich entfernt. In ihrer Stellungnahme teilte sie mit, sie gehe davon aus, daß Schülerinnen und Schüler keine Kenntnis von den Petenten betreffenden Aushang erhalten hätten. Es wurde zugesichert, daß künftig derartige Aushänge mit persönlichen Daten nicht mehr am „Schwarzen Brett" erscheinen werden.

Ich habe die Schule darauf aufmerksam gemacht, daß auch ihr Hinweis, im Aushang getroffene Aussagen zu Erkrankungs- und Sonderurlaubstagen des Petenten seien im Kollegium ohnehin bekannt, nicht von einer vertraulichen Behandlung dieser Mitarbeiterdaten entbinden kann. Der Aushang an einem Mitteilungsbrett mit unkontrollierbarem Zugang stellt datenschutzrechtlich eine Übermittlung personenbezogener Daten an Personen und andere Stellen dar. Die Übermittlung ist auf das erforderliche Maß zu beschränken; die schutzwürdigen Belange der Betroffenen dürfen nicht unnötig beeinträchtigt werden.

27.13 Lehrerdatei an einer berufsbildenden Schule

Eine berufsbildende Schule hatte dem Niedersächsischen Kultusministerium eine Vereinbarung zwischen der Schulleitung und dem Lehrerpersonalrat der Schule über eine Lehrerdatei für Zwecke der Registermeldung vorgelegt. Das Kultusministerium hat mich hierüber unterrichtet und seine Bedenken gegen eine derartige Vereinbarung sowohl im Hinblick auf personalrechtliche als auch auf datenschutzrechtliche Vorschriften vorgetragen.

In der Lehrerdatei sollte eine Vielzahl von personenbezogenen Daten der beschäftigten Lehrkräfte gespeichert sowie die regelmäßige Übermittlung an bestimmte Stellen festgelegt werden. Die Übermittlung sämtlicher Personaldaten an den Lehrerpersonalrat hätte gegen den Erlaß des Niedersächsischen Kultusministeriums vom 26. Mai 1988 (SVBl. S. 25) verstoßen. Auch die regelmäßige Übermittlung bestimmter Daten der Lehrkräfte (u. a. Privatanschrift, Telefonnummer) an die Kolleginnen und Kollegen und den Festausschuß sowie die Schülervertretung wurde vom Kultusministerium als nicht unproblematisch angesehen.

In gleicher Angelegenheit ist mir auch die Eingabe eines betroffenen Lehrers zugegangen. Der Petent äußerte insbesondere Bedenken gegen eine Übermittlung der Lehrerdaten an den Schulelternrat und der Privatanschriften der Lehrerinnen und Lehrer an die Bezirksregierung. Das Kultusministerium hielt die vorgesehenen Datenübermittlungen aufgrund des Konsenses zwischen Schulleitung und Lehrerpersonalrat zunächst für hinnehmbar. Aufgrund der

Ausführungen des Petenten, die dem Ministerium anonym zugeleitet wurden, hat es seine Auffassung jedoch revidiert. Die berufsbildende Schule hat die Vereinbarung außer Kraft gesetzt — die Lehrerdatei ist nicht zum Einsatz gekommen.

27.14 Beurteilungserlaß

Bereits im November 1987 hatte ich das Niedersächsische Kultusministerium darauf hingewiesen, daß die Bezirksregierung Lüneburg — entgegen einer Anweisung des Fachressorts vom April 1984 — Abdrucke von Beurteilungen gem. § 101 Abs. 1 NBG den Betroffenen „auf dem Dienstweg" zusendet, so daß der Schulleiter Kenntnis erhält. Das Ministerium teilte mir mit, dort sei eine Arbeitsgruppe mit der Aufgabenstellung gebildet worden, Vorschläge für eine generelle, landesweite Beurteilungsregelung im Lehrerbereich zu konzipieren.

Die in Aussicht gestellte Regelung habe ich in der Folgezeit wiederholt angemahnt. Inhaltlich habe ich zum Ausdruck gebracht, daß die Bekanntgabe der Beurteilung gegenüber der Schulleiterin bzw. dem Schulleiter und die damit verbundene Datenübermittlung nur zulässig sein können, wenn sie zur rechtmäßigen Aufgabenerfüllung der Schulleitung erforderlich sind. An die Erforderlichkeitsprüfung sind enge Maßstäbe zu legen.

Nachdem es auch im Jahre 1992 nicht gelungen ist, eine Regelung zu treffen, habe ich das Niedersächsische Kultusministerium gebeten, die Bezirksregierungen unabhängig von der umfassenden Überarbeitung des Runderlasses auf die Rechtslage aufmerksam zu machen und auf eine Verfahrensweise hinzuwirken, die eine Einsichtsmöglichkeit der Schulleitung in Beurteilungsabdrucke von Lehrerinnen oder Lehrern ausschließt. Das Ministerium hat hierzu mitgeteilt, daß die Bezirksregierungen im Rahmen einer Dienstbesprechung am 28. April 1992 gebeten werden sollten, den Lehrkräften die Beurteilungen im verschlossenen Umschlag zuzuleiten.

Die jahrelange Verfahrensdauer ist mir unverständlich. Dies um so mehr, als mit dem 9. Gesetz zur Änderung dienstrechtlicher Vorschriften vom 11. Juni 1992 (BGBl. I S. 1030) Regelungen zum Personalaktenrecht (vgl. u.a. Art. 2 Nr. 3 — § 56 Abs. 3 BRRG) getroffen worden sind, die ab 1. Januar 1993 bereichsspezifische Einschränkungen für die Einsichtnahme in Personalunterlagen enthalten. Entsprechende Beschränkungen sieht auch der Entwurf des Niedersächsischen Innenministeriums für eine Verwaltungsvorschrift zum NBG vor.

28. Landwirtschaft und Forsten

28.1 Landwirtschaftliche Kontrollen per Satellit

Im Rahmen der tiefgreifenden strukturellen Umstellung im System der Landwirtschaftsförderung der EG sollen u.a. auch die Verfahren zur Anttragstellung und Bearbeitung bei den zuständigen Landesbehörden sowie zur Kontrolle der Angaben durch diese Stellen neu und weitgehend einheitlich gestaltet werden. Dies wird z. B. zur Folge haben, daß Landwirte für die Erzeugung von Feldfrüchten Beihilfen erhalten, die von der Anbaufläche und der Fruchtart abhängen. Dazu müssen nach der entsprechenden EG-Verordnung die

Flächen nicht nur mit der Größe, sondern auch mit der geographischen Lage angegeben werden. Die Angaben über die Aussaat sollen dann mit Satelliten und Luftbildaufnahmen (vgl. 6.5) abgeglichen und bei danach vermuteten Unstimmigkeiten kontrolliert werden. Nach Auffassung des Niedersächsischen Landwirtschaftsministers ist die Kontrolle per Satellit mit der Menschenwürde nicht zu vereinbaren (vgl. Hannoversche Allgemeine Zeitung vom 16. Dezember 1992). Die Flächenangaben werden außerdem daraufhin geprüft, ob für eine Fläche nicht mehrere Beihilfeanträge eingereicht wurden. Diese und andere Kontrollmöglichkeiten sind nach der EG-Verordnung von vornherein und ohne das Vorliegen eines besonderen Anlasses vorgesehen.

Bei der Realisierung der beabsichtigten Maßnahmen werden datenschutzrechtliche Belange eine erhebliche Rolle spielen. Ich habe mich deshalb bereits jetzt mit dem Niedersächsischen Ministerium für Ernährung, Landwirtschaft und Forsten in Verbindung gesetzt, um mit ihm die sich ergebenden datenschutzrechtlichen Fragestellungen zu erörtern.

28.2 Stützungsregelung für die Erzeuger von Ölsaaten

Die vom Bundesminister für Ernährung, Landwirtschaft und Forsten am 18. März 1992 erlassene Ölsaatenstützungsverordnung, welche die Durchführung der Rechtsakte des Rates und der Kommission der Europäischen Gemeinschaften zur Einführung einer Stützungsregelung für die Erzeuger von Sojabohnen, Raps- und Rübsensamen sowie Sonnenblumenkernen hinsichtlich der Gewährung einer Direktzahlung an die Erzeuger regelt, enthält in § 7 Aussagen über Aufbewahrungs-, Duldungs- und Mitwirkungspflichten.

Aus datenschutzrechtlicher Sicht war es dringend geboten, auch Vorschriften über die Verarbeitung personenbezogener Daten bei der Abwicklung der Fördermaßnahmen zu schaffen. Es hätte sich angeboten, solche Vorschriften in § 7 mit aufzunehmen. Datenschutzrechtliche Probleme (vgl. 6.5) hätten sich dadurch relativiert, da dann zumindest durch eine Rechtsverordnung des Bundes für die Betroffenen erkennbar gewesen wäre, wie und durch wen Eingriffe in ihr Recht auf informationelle Selbstbestimmung erfolgten.

Erfreulich ist, daß das Niedersächsische Ministerium für Ernährung, Landwirtschaft und Forsten mich bereits jetzt an Überlegungen für eine datenschutzgerechte Abwicklung der Ölsaatenbeihilfen für 1993 beteiligt hat.

29. Wirtschaft

29.1 Gewerbe- und Wirtschaftsverwaltungsrecht

Die seit sechs Jahren andauernden Arbeiten am Entwurf eines Gesetzes zur Änderung datenschutzrechtlich relevanter Vorschriften im Gewerberecht sind immer noch nicht zum Abschluß gekommen. Ob die von den Landesbeauftragten und dem Bundesbeauftragten für den Datenschutz vorgebrachten detaillierten Ergänzungs- und Änderungsvorschläge berücksichtigt werden, ist hier nicht erkennbar.

Verschiedentlich haben sich im Gewerberecht Probleme bei Datenübermittlungsvorgängen ergeben: Bei der Übersendung von Gewerbeakten im Gewerbeuntersagungsverfahren an die Industrie- und Handelskammern halte ich die

Überlassung kompletter Vorgänge nicht für erforderlich und daher für unzulässig. Für die Weiterleitung von Gewerbeanzeigen an die Sozialversicherungsträger erachte ich eine bereichsspezifische Regelung für erforderlich.

Zu den Entwürfen der Niedersächsischen Verwaltungsvorschriften zu den Titeln III (Reisegewerbe) und IV (Marktgewerbe) sowie den § 34 (Pfandleiher), 34 a (Überwachungsgewerbe) und 34 b (Versteigerer) wurde ich vom Niedersächsischen Ministerium für Wirtschaft, Technologie und Verkehr um Stellungnahme gebeten. Leider ist die zugrundeliegende gesetzliche Grundlage, die Gewerbeordnung, immer noch nicht an die Vorgaben des Volkszählungsurteils angepaßt worden. Zu den Entwürfen ist anzumerken, daß aus den verwendeten Formularen zwar die erhobenen Daten hervorgehen, die Verwendung dieser Formblätter jedoch nicht vorgeschrieben wird. Ich habe vorgeschlagen, statt der Sollvorschrift eine Mußvorschrift zu erlassen, damit der Datenkatalog abschließend festgelegt ist. Außerdem halte ich hinsichtlich der Beteiligung der Industrie- und Handelskammern eine Festlegung der zu übermittelnden Daten bzw. beizubringenden Unterlagen für erforderlich.

29.2 Handwerksrolle

Nach § 8 Abs. 3 und 4 der Handwerksordnung ist die Mitwirkung einer Handwerkskammer bei der Erteilung von Ausnahmebewilligungen zur Eintragung in die Handwerksrolle abschließend geregelt. In meinem vorherigen Bericht hatte ich darauf hingewiesen, daß die Anhörung einer Berufsvereinigung grundsätzlich nur dann erforderlich ist, wenn die Antragstellerin oder der Antragsteller dies ausdrücklich wünscht. Dieser Rechtsauffassung hat sich das Ministerium für Wirtschaft, Technologie und Verkehr nunmehr angeschlossen. Mit Erlaß vom 10. Juni 1991 wurde eine datenschutzgerechte Regelung getroffen. Danach ist eine Einverständniserklärung in den Antragsvordruck für Ausnahmebewilligungen nach § 8 der Handwerksordnung aufzunehmen.

29.3 Architektenliste

Wie unter X 29.4 ausgeführt, habe ich gegen den umfangreichen Fragenkatalog und die geforderten Unterlagen zur Eintragung in die niedersächsische Architektenliste erhebliche Bedenken. Die zwischenzeitlich dem Ministerium für Wirtschaft, Technologie und Verkehr von der Architektenkammer vorgelegten Neuentwürfe der Antragsvordrucke enthalten immer noch die von mir problematisierten Daten. Das Ministerium hat nun die Architektenkammer gebeten, die strittigen Angaben nochmals direkt mit mir ausführlich zu diskutieren. Das Problem wäre vermieden worden, wenn das Ministerium meiner Empfehlung nach normenklaren Regelungen im Architektengesetz gefolgt wäre.

29.4 Weitergabe von Einwendungen gegen eine Genehmigung nach dem Luftverkehrsgesetz

Ein Einwender in einem luftverkehrsrechtlichen Genehmigungsverfahren hatte die Bezirksregierung ausdrücklich darum gebeten, seine Stellungnahme zu einem schalltechnischen Gutachten, in dem es um die zu erwartenden Geräuschimmissionen beim Schleppbetrieb auf einem Segelfluggelände ging, nur ganz bestimmten Dritten zur Verfügung zu stellen. Die Bezirksregierung gab die Eingabe dann doch an andere Stellen weiter und unterrichtete den Einwender hiervon.

Ich habe der Bezirksregierung daraufhin mitgeteilt, daß der Einwender vor einer Weitergabe seiner Stellungnahme um sein schriftliches Einverständnis hätte gebeten werden müssen. Alternativ wäre auch eine Weitergabe in anonymisierter Form möglich und ausreichend gewesen.

29.5 Job-Ticket in Hannover

Der Großraumverkehr Hannover (GVH) bietet allen Firmen und Behörden Firmen-Abos zum halben Preis an. Bedingung ist, daß grundsätzlich für alle Mitarbeiter Jahresfahrausweise vom GVH abgenommen werden. Es bleibt dann der Firma/Behörde überlassen, wie viele Fahrausweise und zu welchen Bedingungen sie diese an ihre Mitarbeiterinnen und Mitarbeiter „los wird".

Das Land Niedersachsen beteiligt sich ab 1. April 1993 mit ca. 37.000 Bediensteten an dem Modellversuch. Das Job-Ticket wird dann zugleich Voraussetzung für die Benutzung von Parkplätzen der Landesbehörden in der Stadt Hannover sein. Der Abo-Preis wird durch die Bezügestelle monatlich von den Bezügen einbehalten. Hierfür ist eine schriftliche Einwilligung erforderlich.

Ich habe mich bereits 1991 in die Planungen zu diesem GVH-Angebot eingeschaltet, als mir bekannt wurde, daß alle Mitarbeiterdaten, gleich ob eine Teilnahme erfolgt, an den GVH übermittelt werden sollten. Meine Verfahrensvorschläge — vom Innenministerium unterstützt — wurden aufgegriffen. Dem GVH werden nur die Daten der Mitarbeiterinnen und Mitarbeiter, die ein Job-Ticket erwerben wollen, nach deren schriftlicher Einwilligung übermittelt. Darüber hinaus erhält der GVH die Gesamt-Mitarbeiterzahl der einzelnen Firma/Behörde. Das GVH-Angebot regelt auch einige Ausnahmen von der Abnahme- und Meldepflicht. Über diese Ausnahmen entscheidet die Firma/Behörde selbständig. Dem GVH wurde das Recht eingeräumt, die entsprechenden Antragsunterlagen bei der beantragenden Firma/Behörde einzusehen und sie zu prüfen. Dies ist im Einzelfall unter Beachtung des Erforderlichkeitsgrundsatzes datenschutzrechtlich vertretbar.

Nicht akzeptieren konnte ich dagegen die Vordruck-Gestaltung des „Antrages für einen Fahrausweis im Modellversuch Firmenabonnement". Die Antragsausfertigung für die ÜSTRA, die im Durchschreibeverfahren erstellt wird, enthält unzulässigerweise auch die Bezüge-Abrechnungsdaten „Kapitel, Titel, Empfängernummer". Dies hätte bei gleicher Herstellungs- und Vervielfältigungs-Technik allein durch einen Schwarz-Druck des Feldes „Aktenzeichen" verhindert werden können. Im Feld „Einwilligung" fehlt der Hinweis auf die Folgen bei fehlender Einwilligung, so wie dies § 9 Abs. 2 NDSG-E vorsieht. Unverständlich ist, warum ich nicht auch bei der Frage der Vordruckgestaltung beteiligt worden bin; die Vordruck-Panne hätte verhindert werden können, und zwar ohne einen Pfennig an Mehrkosten. Das Ministerium für Wirtschaft, Technologie und Verkehr hat das Versäumnis eingeräumt und bedauert. Das „Versehen" soll durch frühestmögliche Vernichtung der Erhebungsbogen nach Erfassen der erforderlichen Antragsdaten „geheilt" werden. Meine Kritik an einer an sich guten Lösung bleibt bestehen.

30. Verkehr

30.1 Verkehrsordnungswidrigkeiten

Die vom Niedersächsischen Innenministerium angekündigten Verwaltungsvorschriften zum Bußgeldverfahren wurden noch nicht erlassen. Die im X. Tätigkeitsbericht dargestellte Problematik bei den Sammelanzeigen soll nunmehr vorab in einem Rundschreiben an die Bußgeldbehörden geregelt werden. Es muß sichergestellt werden, daß bei Aktenanforderungen unter Verwendung von Vordrucken zu Sammelanzeigen nur die erforderlichen Daten übermittelt werden.

Ein Bürger kritisierte zu Recht, daß von ihm Geburtsdatum und -ort sowie die Adresse auf dem Formular zur Anhörung im Rahmen eines Verkehrsordnungswidrigkeiten-Verfahrens anzugeben seien, obwohl diese Daten der Bußgeldstelle bekannt und auch auf dem Anhörungsvordruck ausgedruckt waren. Fragen nach den im Fahrzeugregister gespeicherten Daten sind überflüssig, da sie gemäß § 35 Abs. 1 Ziffer 3 StVG zur Verfolgung von Ordnungswidrigkeiten übermittelt werden dürfen. Das Innenministerium hat zugesagt, künftig die Belehrung im Anhörungsbogen dahingehend zu fassen, daß die oder der Betroffene die Angaben zur Person nur noch ausfüllen muß, wenn die gespeicherten Daten unrichtig oder unvollständig sind.

Der Grund einer weiteren Eingabe war, daß Polizisten bei der Ermittlung einer Verkehrsordnungswidrigkeit den Nachbarn des nicht zu Hause angetroffenen Petenten Fotos über einen Rotlichtverstoß vorgelegt hatten, ohne daß zuvor ein Lichtbildvergleich mit dem Personalausweis- bzw. Paßregister vorgenommen worden war. Diese Vorgehensweise halte ich zumindest für unangemessen. Ich habe gegenüber dem Innenministerium angeregt, den Ordnungswidrigkeitenerlaß dahingehend zu ergänzen, daß bei der Ermittlung von Verkehrsordnungswidrigkeiten zunächst andere Möglichkeiten ausgeschöpft werden, wenn der Betroffene nicht erreichbar ist, bevor Ermittlungen bei den Nachbarn durchgeführt werden (vgl. 11.2).

30.2 Führerscheine

Auch im Berichtszeitraum 1991/1992 ist es wiederum nicht zum Erlaß bereichsspezifischer Regelungen zum Datenschutz im Fahrerlaubniswesen gekommen. Nach Mitteilung des Niedersächsischen Ministeriums für Wirtschaft, Technologie und Verkehr konnten die von einem Arbeitskreis begonnenen Erörterungen aus personellen Gründen nicht abgeschlossen und dem Bund-Länder-Fachausschuß „Fahrerlaubniswesen" vorgelegt werden.

Ich habe im Hinblick auf die von drogenabhängigen Kraftfahrern auf die übrigen Verkehrsteilnehmer ausgehenden Gefahren dem Erlaß zur Meldung von Drogenabhängigen und -konsumenten an die zuständige Straßenverkehrsbehörde für eine Übergangszeit zugestimmt, obwohl — bei Berücksichtigung der Unterscheidung zwischen Aufgaben- und Befugnisnormen — die § 1 Abs. 2 Satz 2 und 11 des Nds. SOG hierfür nicht als ausreichende Rechtsgrundlage angesehen werden können.

Die Praxis der regelmäßigen Übermittlung personenbezogener Daten an die örtliche Polizei nach der Entziehung von Fahrerlaubnissen durch die Verwaltungsbehörden wollte das Ministerium für Wirtschaft, Technologie und Verkehr durch einen Erlaß sanktionieren. Gegen diese Vorratsspeicherung bestehen grundsätzliche datenschutzrechtliche Bedenken. Ich habe daher das

Innenministerium aufgefordert, die Erforderlichkeit für die Datenübermittlung ausführlich darzulegen. Die Antwort steht noch aus.

30.3 Verwertung polizeilicher Auskünfte im Fahrerlaubnisverfahren

Eine Führerscheinstelle richtete im Rahmen der Überprüfung für eine Fahrerlaubnis zur Fahrgastbeförderung außer den Anfragen an das Bundeszentralregister und das Verkehrszentralregister auch regelmäßig Anfragen an die Kriminalpolizei. In einem Fall ging es um einen Antragsteller, der als Jugendlicher ohne Fahrerlaubnis gefahren war und gegen das Betäubungsmittelgesetz verstoßen hatte. Beide Verfahren waren gegen eine Geldbuße eingestellt und nur im Erziehungsregister vermerkt worden. Durch die Anfrage bei der Polizei hatte die Fahrerlaubnisbehörde eine Auskunft erhalten, die ihr normalerweise — da nicht im Bundeszentralregister vermerkt — nicht zugänglich gewesen wäre. Meine gegen diese Praxis vorgebrachten Bedenken wurden vom Niedersächsischen Ministerium für Wirtschaft, Technologie und Verkehr geteilt. Mit Erlaß vom 22. August 1991 wurden die Fahrerlaubnisbehörden angewiesen, von regelmäßigen Anfragen an die Polizei abzusehen und nur dann dort nachzufragen, wenn konkrete Anhaltspunkte dies geboten erscheinen lassen.

30.4 Beibringung von Gutachten einer medizinisch-psychologischen Untersuchungsstelle

Gleichzeitig mit der Aufforderung an einen Antragsteller, ein Gutachten von einer amtlich anerkannten medizinisch-psychologischen Gutachterstelle beizubringen, wurde von der Fahrerlaubnisbehörde eine Durchschrift der Anordnung an den TÜV Norddeutschland übersandt. Hierbei wurde übersehen, daß nach den Eignungsrichtlinien die Unterrichtung einer von dem Betroffenen gewählten Untersuchungsstelle erst nach seiner Zustimmung hätte erfolgen dürfen. Ich habe diesen Verstoß gegenüber der Fahrerlaubnisbehörde beanstandet. Diese hat mir daraufhin mitgeteilt, daß sie den Betroffenen zukünftig die in Betracht kommenden Untersuchungsstellen mitteilt und vor Übersendung der Akten die Zustimmung der jeweiligen Person einholt.

31. Rechtspflege

31.1 Bekämpfung der Organisierten Kriminalität

Am 22. September 1992 ist das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität in Kraft getreten (OrgKG, BGBl. I S. 1302). Inhaltlich geht es um Neuregelungen und Änderungen im Strafrecht und Strafverfahrensrecht. Im Bereich des Strafrechts betreffen die Neuregelungen im wesentlichen die Einführung einer zusätzlichen Geldstrafe (neben der Freiheitsstrafe), die Erweiterung der Möglichkeiten, Vermögensgegenstände zugunsten des Staates als verfallen zu erklären, und die Einarbeitung des neuen Straftatbestandes der „Geldwäsche". In der Strafprozeßordnung (StPO) wird der Zeugenschutz verbessert. Vor allem werden aber gesetzlich neu vier verdeckte Ermittlungsmethoden eingeführt. Ohne Wissen der Betroffenen dürfen eingesetzt werden: die Rasterfahndung (maschineller Abgleich der Daten eines mutmaßlichen Täters mit anderen Daten), technische Mittel zur akustischen und optischen Überwachung außerhalb von Wohnungen, verdeckte Ermittler (unter falscher Identität agierende Polizeibedienstete) und die beobachtende Fahndung (Ausschrei-

bungen zur bundesweiten Beobachtung anläßlich polizeilicher Kontrollen zur Erstellung von Bewegungsbildern). Das Land Niedersachsen hatte im Bundesrat wegen nicht genügend klarer Regelungen zur Rasterfahndung und zum verdeckten Ermittler gegen das Gesetz gestimmt.

Die Entstehungsgeschichte des OrgKG war von heftiger öffentlicher Kritik begleitet. Einig war man sich im Ziel, bestimmte Erscheinungsformen der Kriminalität in besonderer Weise zu bekämpfen. Gestritten wurde um den richtigen Weg, nämlich einen vertretbaren Kompromiß zu finden zwischen einer wirksamen Strafverfolgung und dem Schutz der einzelnen Menschen vor ungerechtfertigten staatlichen Eingriffen. Namhafte Verbände, wie die Strafverteidigervereinigungen und der Deutsche Richterbund sowie der Strafrechtsausschuß des Deutschen Anwaltvereins, haben u.a. kritisiert, daß mit dem OrgKG ein Weg beschritten wird, der den Ermittlungsbehörden Maßnahmen schon weit vor dem Vorliegen eines Anfangsverdachts auf eine konkrete Straftat (so die bisherige Rechtslage) erlaubt und damit in geschützte Rechtsstellungen der Bürgerinnen und Bürger eingreift. Auf der anderen Seite wird das Gesetz aus polizeilicher Sicht als eine einzige Enttäuschung angesehen, weil für notwendig erachtete Befugnisse, wie insbesondere die Begehung von milieubedingten Straftaten durch verdeckte Ermittler und das Abhören des nichtöffentlich gesprochenen Wortes in und aus Wohnungen (Lauschangriff), nicht erlaubt werden.

Die Datenschutzbeauftragten des Bundes und der Länder haben darauf aufmerksam gemacht, daß unter dem Deckmantel der Bekämpfung der Organisierten Kriminalität neue Ermittlungsmethoden gesetzlich zugelassen werden, die dann allgemein für die Strafverfolgung gelten. Die Kritikpunkte (vgl. Entschließung vom 27. Juni 1990, X Anlage 11 und Entschließung vom 25. Juni 1991 — gegen die Stimme Bayerns — in diesem Tätigkeitsbericht Anlage 3) sind im wesentlichen:

— der gesetzlich nicht präzisierte Begriff der „Straftaten von erheblicher Bedeutung" (ist Ausgangspunkt für bestimmte verdeckte Maßnahmen),
— der heimliche Einsatz von technischen Mitteln auch gegen unverdächtige Personen,
— die nicht durchgehend geregelte externe Kontrolle verdeckter Maßnahmen durch den Richter,
— die weitgehende Verwertung der aus heimlicher Überwachung gewonnenen Erkenntnisse über zufällig betroffene Dritte für die (allgemeine) vorbeugende Straftatenbekämpfung.

Ich habe noch kurz vor der abschließenden Entscheidung im Bundesrat die Landesregierung aufgefordert, dem OrgKG nicht zuzustimmen. Meine Warnung betraf die mögliche Entgrenzung der Polizei. Diese Möglichkeit ist ins Kalkül zu ziehen, wenn man bedenkt, daß das OrgKG die Zielrichtung heimlicher Ermittlungsmethoden — die Aufklärung der Straftaten von erheblicher Bedeutung — nicht näher definiert. Vor allem geht mit den verdeckten Maßnahmen die Erfassung Unverdächtiger einher. Mit Fug und Recht kann gesagt werden, daß mit den neuen Methoden „auf etwas (geschossen wird), von dem man nicht weiß, was man trifft" (vgl. Prof. Hassemer — mein hessischer Kollege — in der Frankfurter Rundschau vom 30. Juli 1992). Niemand kann nämlich genau sagen, was Organisierte Kriminalität eigentlich ist. Die die Zusammenarbeit von Staatsanwaltschaft und Polizei bei der Verfolgung der Organisierten Kriminalität regelnden Verwaltungsvorschriften benötigen knapp zwei DIN A4-Seiten, um Erscheinungsformen und Indikatoren der Organisierten Kriminalität zu beschreiben (vgl. Gem.RdErl. des Niedersächsischen Justizministeriums und des Niedersächsischen Innenministeriums vom 10. Juni 1992, Nds. Rpfl. S. 163). Ich habe mich auch deswegen an die Landesregierung gewandt, weil der im OrgKG angelegte Trend zu verdeckten Ermittlungen ge-

gen Unbeteiligte auch im Entwurf eines Niedersächsischen Gefahrenabwehrgesetzes (NGefAG) wiederzufinden ist (vgl. 12.4). Damit besteht die Gefahr, daß jede polizeiliche Maßnahme je nach Bedarf entweder auf Vorschriften der Strafverfolgung (StPO) oder solche der Gefahrenabwehr (NGefAG) gestützt werden kann.

Die Anwendung der neuen Bestimmungen des OrgKG ist jedenfalls mit einem gehörigen Vertrauensvorschuß an die Polizei verbunden, mit den eingeräumten Befugnissen sorgsam umzugehen.

Das noch im Gesetzentwurf eines OrgKG vorgesehene Abhören und Aufzeichnen des in der Wohnung gesprochenen nichtöffentlichen Wortes (Lauschangriff) wurde u. a. wegen schwieriger verfassungsrechtlicher Fragen im Hinblick auf den Schutz der Wohnung in Art. 13 GG wieder gestrichen. Der Deutsche Bundestag hatte jedoch bei der Verabschiedung des Gesetzes beschlossen, die Beratung hierüber nach der Sommerpause 1992 wiederaufzunehmen. Die quer durch die Parteien geführte derzeitige Diskussion um eine ggf. erforderliche Änderung des Art. 13 GG belegt, wie umstritten dieser Punkt ist. Leider sind mir Äußerungen zur näheren Ausgestaltung des dann verfassungsrechtlich Erlaubten nicht bekannt. Aus Sicht der Polizei ist der Lauschangriff notwendig, um an die Drahtzieher des organisierten Verbrechens heranzukommen. Es wird dabei auf Erfahrungen amerikanischer Ermittlungsbehörden verwiesen. Danach sollen ca. 80 % der geführten Ermittlungsverfahren letztendlich nur durch den Einsatz elektronischer Überwachungstechnik in Wohnungen erfolgreich und beweissicher zum Abschluß gebracht worden sein. Eine nachvollziehbare Dokumentation dieser Behauptung steht noch aus. Am Rande sei vermerkt, daß das (unbefugte) Abhören mit einer „Wanze" vor einiger Zeit erst ausdrücklich unter Strafe gestellt wurde. Die seinerzeitige Begründung stellte auf „spektakuläre Lauschangriffe auf den ehemaligen bayerischen Ministerpräsidenten Strauß" ab (vgl. Süddeutsche Zeitung vom 2. September 1992). Gegen den Lauschangriff hat eine große Anzahl von Staatsrechtlern, Strafrechtlern und Politologen Stellung bezogen. Sie halten den Lauschangriff auf den elementaren Lebensraum Wohnung für eine Verletzung des Kernbereichs der freien Entfaltung der Persönlichkeit, der Teil der Menschenwürde und daher nach Art. 1 GG unantastbar ist (vgl. Frankfurter Rundschau vom 12. November 1992).

Die Datenschutzbeauftragten des Bundes und der Länder haben — gegen die Stimme Bayerns — am 1./2. Oktober 1992 eine Entschließung gefaßt, in der sie ihre schwerwiegenden Bedenken gegen den Lauschangriff in oder aus Wohnungen betonen (vgl. Anlage 8). Ich habe die zuständigen Ressorts in Niedersachsen über die Entschließung der Datenschutzbeauftragten in Kenntnis gesetzt. Möglicherweise wäre man im Hinblick auf die schwierigen Fragen gut beraten, die Entscheidung des Bundesverfassungsgerichts zur erhobenen Verfassungsbeschwerde gegen die entsprechende Bestimmung für den im Bereich der Gefahrenabwehr im Hamburger Gesetz über die Datenverarbeitung der Polizei abzuwarten (1 BvR 1104/92).

Es steht außer Frage, daß die Erzielung hoher finanzieller Gewinne kennzeichnend für die Organisierte Kriminalität ist. Zur Verfolgung von Straftaten der Geldwäsche wird gegenwärtig in den Ausschüssen des Deutschen Bundestages der Gesetzentwurf über das Aufspüren von Gewinnen aus schweren Straftaten (Gewinnaufspürungsgesetz, BT-Drs. 12/2704) beraten. Der Entwurf verfolgt das Ziel, zur Bekämpfung der Organisierten Kriminalität Geldbewegungen insbesondere im Bankenverkehr transparent zu machen, Geldwäschevorgänge zu entdecken und für die Strafverfolgungsbehörden Ansatzpunkte für Ermittlungen zu liefern. Das Vorhaben dient der Umsetzung der EG-Richtlinie zur Verhinderung der Nutzung des Finanzsystems zum Zweck der Geldwäsche vom 10. Juli 1991. Danach sind die Mitgliedstaaten verpflichtet, bis zum

1. Januar 1993 entsprechende Vorschriften zu erlassen. In der Sache geht es um Identifizierungs- und Aufzeichnungspflichten sowie Verdachtsanzeigepflichten (daß eine Geldwäsche vorliegt), insbesondere der Banken bei Einzahlungen von DM 30 000,— oder mehr.

Aus datenschutzrechtlicher Sicht wird es darum gehen, das im Gesetzentwurf durch die Verpflichtung Privater als eine Art „Hilfssheriffs" vorgesehene umfassende Überwachungsnetz bezüglich Vermögensverschiebungen und die einhergehende Vorratsspeicherung mit einer strengen Zweckbindung zu versehen.

31.2 Genomanalyse im Strafverfahren

Der Bundesminister der Justiz hat einen Referentenentwurf einer gesetzlichen Regelung zum genetischen Fingerabdruck den Landesjustizverwaltungen vorgelegt. Es geht um die Feststellung von Identität und Abstammung zu strafprozessualen Zwecken. Mit dem genetischen Fingerabdruck kann eine Person — im Vergleich zu herkömmlichen Untersuchungsmethoden, wie z. B. Blutgruppenvergleich — mit einer wesentlich höheren Wahrscheinlichkeit als „Spurenleger" festgestellt oder ausgeschlossen werden. Der Bundesgerichtshof hat jüngst klargestellt, daß das Ergebnis eines genetischen Fingerabdrucks aber eine „statistische Aussage" bleibe und daher eine Verurteilung nicht ausschließlich auf dieses Beweismittel gestützt werden kann (vgl. Urteil v. 12. August 1992, NJW 1992, 2976 f.).

Der Referentenentwurf geht davon aus, daß die Gewinnung des zur Herstellung eines genetischen Fingerabdrucks erforderlichen Untersuchungsmaterials ihre Rechtsgrundlage in den § 81a und 81c StPO habe. Inhaltlich beschränkt sich der Entwurf daher im wesentlichen auf Vorschriften über den Einsatz der Untersuchungsmethode, das bei der Durchführung der Untersuchung zu beachtende Verfahren sowie Schutzvorkehrungen zugunsten der Betroffenen.

Die Erkenntnismöglichkeiten aus der Genomanalyse sind ungeheuer weitreichend. Durch gentechnische Verfahren können genetisch bedingte Eigenschaften des Menschen festgestellt werden. Mit anderen Worten: Der Mensch kann im Hinblick auf seine genetische Disposition klassifiziert werden. Bei solchen Möglichkeiten liegt es auf der Hand, daß die Gentechnik nicht nur gute Seiten hat, wie z. B. Früherkennung von Krankheiten, sondern auch erhebliche Befürchtungen verursacht. Im Mittelpunkt der Überlegungen müssen daher kontrollierbare Grenzziehungen stehen zum Schutz der Würde des Menschen, des allgemeinen Persönlichkeitsrechts wie auch des Rechts auf informationelle Selbstbestimmung. Aus datenschutzrechtlicher Sicht sind Untersuchungen dieser Art auf das zur erlaubten Zweckerreichung unabdingbare Maß zu beschränken. Die Untersuchung muß die „ultima ratio" sein. Für den Bereich des genetischen Fingerabdrucks bedeutet dies, daß nur diejenigen — gesetzlich festgelegten — Untersuchungsmethoden zur Identitätsfeststellung akzeptabel sind, die am wenigsten „Überschußinformationen" über die genetische Disposition eines Menschen erbringen (vgl. die Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26. Oktober 1989, X Anlage 17). Ich halte mithin nur eine Untersuchungstechnik für vertretbar, die ausschließlich nicht-codierende Bereiche der Desoxyribonukleinsäure untersucht. Leider läßt der Wortlaut des vorgelegten Referentenentwurfs einer gesetzlichen Regelung zum genetischen Fingerabdruck eine solche Grenzziehung vermissen.

In meiner Stellungnahme gegenüber dem Niedersächsischen Justizministerium habe ich weiter kritisiert, daß der Entwurf letztlich keine Zweckbindung

für das Untersuchungsmaterial enthält, da es auch zur Erforschung einer anderen prozessualen Tat verwendet werden kann. Nach meiner Auffassung sollte eine Verwertung nur im Rahmen des konkreten Strafverfahrens zulässig sein. Auch habe ich eine gesetzliche Regelung zur Anonymität der Untersuchung gefordert, so daß eine Zuordnung der Ergebnisse nur den Strafverfolgungsbehörden ermöglicht wird. Verfahrensrechtlich begrüßenswert ist die für den genetischen Fingerabdruck vorgesehene Anordnungskompetenz durch den Richter.

Im Bereich der Schutzvorkehrungen für die Betroffenen sieht der Referentenentwurf zwar die Vernichtung des Untersuchungsmaterials vor — „sobald (es für ein Strafverfahren) nicht mehr erforderlich (ist)". Die Befundunterlagen bleiben jedoch erhalten. Als weitere Schutzvorkehrungen für die Betroffenen habe ich zusätzlich ein Verwertungsverbot für rechtswidrig erhobene genomanalytische Befunde, ein Beschlagnahmeverbot für die entsprechenden Unterlagen und Ergebnisse sowie eine Strafandrohung für den Mißbrauch von Genomanalysen gefordert.

31.3 Nennung von Zeugenanschriften im Strafbefehl

Aus Gründen des Datenschutzes, die hier zugleich mit Gesichtspunkten des Zeugenschutzes einhergehen, halte ich es für sachgerecht, auf die Angabe der vollständigen Anschrift des Zeugen im Strafbefehl nach § 409 Abs. 1 StPO zu verzichten.

Das Niedersächsische Justizministerium hat mir mitgeteilt, daß es unbedenklich ist, wenn die Staatsanwaltschaften bis auf weiteres in begründeten Ausnahmefällen davon absehen, in einem Strafbefehl die Wohnanschrift von Zeugen anzugeben. Angesichts der seinerzeit aber noch nicht abgeschlossenen Beratungen zum Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) — mit Regelungen zur Verbesserung des Zeugenschutzes — wollte das Justizministerium zum damaligen Zeitpunkt von einer abschließenden, generellen Regelung in dem Sinne, wie von mir vorgeschlagen, absehen. Das nunmehr verabschiedete OrgKG enthält zwar Verbesserungen zum Zeugenschutz, bedauerlicherweise jedoch nicht zu § 409 StPO.

Über die angekündigte Prüfung hinsichtlich gegebenenfalls weiterer zu treffender Maßnahmen nach Abschluß der Beratungen zum OrgKG erwarte ich noch eine Stellungnahme des Justizministeriums.

31.4 Datenschutz im Zusammenhang mit der Einstellungsbegründung einer Staatsanwaltschaft

Ein Petent beschwerte sich darüber, daß in der Einstellungsbegründung einer Staatsanwaltschaft gegenüber einem Anzeigeerstatter Angaben gemacht wurden, die seiner Meinung nach nicht notwendig waren, nämlich zum Ort seiner Inhaftierung („JVA ..."), zur Dauer seiner Freiheitsstrafe („langjährige" Freiheitsstrafe) und dazu, daß „weitere Ermittlungsverfahren anhängig sind".

Nach meiner Auffassung war die Angabe des Ortes der Inhaftierung nicht erforderlich; hinsichtlich der weiteren Angaben hatte ich keine datenschutzrechtlichen Einwände zu erheben.

Dazu im einzelnen: Der Ort der Inhaftierung war nach Auffassung der Staatsanwaltschaft erforderlich, weil mit der Angabe deren Tatortzuständigkeit dargelegt werden sollte. Die Bekanntgabe des Aufenthaltsortes gegenüber dem rechtskundigen Anzeigeerstatter wurde als notwendig angesehen, weil er die Anzeige bei einer anderen Staatsanwaltschaft erstattet hatte. Zugunsten des mitgeteilten Ortes der Inhaftierung spricht zwar zunächst das in § 171 Satz 1 StPO strafprozessual verankerte Informationsrecht des Geschädigten. Dieses Recht gilt aber nicht grenzenlos. Es gewinnt seine inhaltliche Bedeutung erst im Zusammenhang mit der jeweiligen Einstellungsvorschrift. So muß der Anzeigeerstatter etwa bei § 154 Abs. 1 StPO anhand der dargestellten Gründe abwägen können, ob er mit einer Beschwerde in der Sache Erfolg hat. Maßgeblicher Prüfungsansatz ist demnach die Begründung für den Teilverzicht auf die Strafverfolgung der angezeigten Tat im Hinblick auf verhängte oder zu erwartende Strafen. Die Frage der örtlichen Zuständigkeit der einstellenden Staatsanwaltschaft spielt für die vorzunehmende Abwägung mithin keine Rolle. Nach meinem Dafürhalten war daher die Nennung des konkreten Aufenthaltsortes des Beschuldigten für die in § 154 Abs. 1 Nr. 1 StPO geforderte Abwägung ohne Belang. Dies schließt nicht aus, in Fällen dieser Art der anzeigeerstattenden Person einen allgemeinen Hinweis auf die sich nach den Ermittlungen ergebende Zuständigkeit der handelnden Staatsanwaltschaft zu geben. Insbesondere ein rechtskundiger Bescheidempfänger kann der Fertigung des Einstellungsbescheides entnehmen, daß die staatsanwaltschaftliche Prüfung auch die Frage des Tatortes umfaßt hat.

Im übrigen galt es nach Darstellung der beteiligten Stellen, dem rechtskundigen Anzeigeerstatter verständlich zu machen, daß der Beschuldigte nicht nur eine geringfügige Freiheitsstrafe oder gar Ersatzfreiheitsstrafe verbüßt, sondern eine langjährige und zudem noch in einem weiteren Verfahren eine empfindliche Strafe zu erwarten hatte. Dieser staatsanwaltschaftlichen Beurteilung habe ich mich in diesem Falle angeschlossen. Die Staatsanwaltschaft wird diese Fall zum Anlaß nehmen, in Dienstbesprechungen die Problematik zu erörtern und auf Zurückhaltung hinzuwirken.

31.5 Aufbewahrung von Beweismitteln nach Verfahrenseinstellung durch eine Staatsanwaltschaft

Ein Einsender rügte, daß sich Fotokopien seiner Briefe an seine Lebensgefährtin nach Verfahrenseinstellung noch in der Ermittlungsakte der Staatsanwaltschaft befanden. Der Inhalt war nach Angabe des Petenten höchst persönlicher, intimer Natur. Die Originalbriefe, die beschlagnahmt waren und im Verfahren zunächst als Beweismittel dienten, waren nach Darstellung des Beschwerdeführers der Empfängerin zurückgegeben worden. Der Einsender sah in dem Aufbewahren der Kopien einen Eingriff in das Briefgeheimnis sowie einen Verstoß gegen sein Recht auf informationelle Selbstbestimmung. Nach Einstellung des Verfahrens hätten die Kopien auch keinen Beweiswert mehr. Der Einsender forderte daher die Vernichtung der Kopien.

Ich habe gegenüber der Staatsanwaltschaft dargetan, daß es sich bei der Aufbewahrung von Kopien um eine Speicherung handelt, die nach der Entscheidung des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 — sofern keine Einwilligung vorliegt — einer Rechtsgrundlage bedarf (BVerfGE 65, 1 ff.). Verwaltungsvorschriften, wie etwa Nr. 76 RiStBV, sind keine Rechtsgrundlage. Ich habe allerdings darauf hingewiesen, daß auf die entsprechenden Bestimmungen in den Verwaltungsvorschriften für eine Übergangszeit — bis zum Inkrafttreten eines Gesetzes — zurückgegriffen werden könne. Während dieses Zeitraumes müsse allerdings die Datenverarbeitung auf das Unerläßliche beschränkt werden, d. h. auf das, was für die geordnete Weiterführung einer funktionsfähigen Verwaltung unverzichtbar sei.

Da die Staatsanwaltschaft Ansatzpunkte für weitere Ermittlungen nicht sah, hat sie die Vernichtung der Kopien veranlaßt. Die zuständige Generalstaatsanwaltschaft hat darüber hinaus mitgeteilt, daß die Problematik der Fertigung von Kopien beschlagnahmter Schriftstücke nach Einstellung des Verfahrens sowie der sicheren Aufbewahrung schriftlicher Aufzeichnungen höchstpersönlichen Inhalts bei der nächsten Dienstbesprechung mit den Leitenden Oberstaatsanwälten erörtert werde.

31.6 Austausch von Entscheidungen in Staatsschutzsachen

In X 31.4 habe ich meine datenschutzrechtlichen Bedenken gegen den Austausch von nicht anonymisierten Entscheidungen in Staatsschutzsachen bekundet und dargelegt, daß eine klare Rechtsgrundlage fehlt. Meine Bedenken gegen diesen Austausch der Entscheidungen bestehen fort. Ich habe meine Zweifel an der Erforderlichkeit des Datenaustauschs dem Niedersächsischen Justizministerium mitgeteilt und es für unerläßlich erachtet, für die beteiligten Stellen in Niedersachsen das Unterrichtungsverfahren einzustellen. Das Justizministerium hat sich zur sofortigen Einstellung des Austauschverfahrens nicht entschließen können. Ich bedauere diese Entscheidung. In Hessen wurde das Verfahren datenschutzfreundlicher geregelt. Dort werden Entscheidungen in Staatsschutzsachen nur noch anonymisiert übersendet.

31.7 Weitergabe von Gerichtsentscheidungen an Dritte

In einer Eingabe wurde gerügt, daß der an einen Dritten übersandte Abdruck eines Verwaltungsgerichtsbeschlusses nicht anonymisiert worden war. Meine Nachfrage beim Verwaltungsgericht ergab, daß die Übersendung der Entscheidung in nicht-anonymisierter Form auf einem Versehen beruhte und daß bei richtiger Sachbehandlung die Namen der Verfahrensbeteiligten, Zeugen, Sachverständigen sowie Ortsangaben und, soweit erforderlich, Zahlen und Zeitangaben durch Schwärzen unleserlich gemacht würden. Meine Prüfung hat bewirkt, daß die mit der Übersendung von Verfahrensabschriften betrauten Bediensteten nochmals auf sorgfältige Arbeitsweise hingewiesen wurden. Datenschutzrechtlich ebenfalls begrüßenswert ist die in diesem Zusammenhang gegebene Auskunft des Justizministeriums, nach der Urteilsabschriften an nicht verfahrensbeteiligte Dritte, die personenbezogene Daten der Verfahrensbeteiligten enthalten, nur in anonymisierter Form weitergegeben werden. Bei der Erfüllung von Mitteilungspflichten nach der Anordnung über Mitteilungen in Strafsachen (MiStra) würden die Personendaten, mit Ausnahme der Daten nichtbeteiligter anderer Beschuldigter, nicht geschwärzt. Bei Akteneinsicht zu Forschungszwecken werden die personenbezogenen Daten der Verfahrensbeteiligten ebenfalls unleserlich gemacht.

31.8 Justizmitteilungsgesetz

In meinen früheren Tätigkeitsberichten hatte ich Ausführungen zu damaligen Referentenentwürfen eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- und Strafsachen (Justizmitteilungsgesetz — JuMiG) gemacht (vgl. IX u. X 31.4). Nunmehr liegt ein Gesetzentwurf der Bundesregierung vor (vgl. BT-Drs. 12/3199).

Ich würde eine baldige Verabschiedung des JuMiG begrüßen. Dies schon deshalb, weil es den Justizbediensteten nun schon neun Jahre nach dem Volkszählungsurteil nicht mehr länger zugemutet werden kann, ohne gesetzliche

Grundlagen nur mit Hilfe des Übergangsbonus Mitteilungen an andere Stellen zu machen, die in das Recht auf informationlle Selbstbestimmung eingreifen. Auf der anderen Seite muß ich feststellen, daß der Gesetzentwurf mehrfach vorgetragene datenschutzrechtliche Kritik (vgl. X 31.4) nicht aufgegriffen hat. Zudem empfiehlt der Bundesrat in seiner Stellungnahme zum Gesetzentwurf, die aufgenommenen — auch datenschutzrechtlichen — Regelungen auf ihre Unabdingbarkeit hin zu überprüfen. Diese mit der Belastung der Justiz insbesondere in den neuen Ländern begründete Position veranlaßt mich wiederum zu fragen, ob das Problem nicht vielmehr im ausufernden Umfang der Mitteilungen liegt.

31.9 Mitteilungen an die Gemeinde

Mißglückte Verwaltungsvorschriften können die Ursache dafür sein, daß ein Betroffener bei der Wahl zum Deutschen Bundestag zu Unrecht nicht wählbar ist.

Wird jemand wegen eines Verbrechens zu einer Freiheitsstrafe von mindestens einem Jahr verurteilt, so verliert er von Gesetzes wegen u.a. das passive Wahlrecht für fünf Jahre (§ 45 Abs. 1 StGB). Die Staatsanwaltschaften sind nun nach Nr. 12 a der Anordnung über Mitteilungen in Strafsachen (MiStra) gehalten, die Tatsache der rechtskräftigen Verurteilung der zuständigen Gemeinde mitzuteilen, damit sie weiß, wer bei einer Wahl nicht wählbar ist (vgl. auch 16.5). Dementsprechend hatte eine Gemeinde zunächst zu Recht die Angabe „Ausschluß von der Wählbarkeit" gespeichert. Diese Information wurde aber auch dann noch vorgehalten — und führte im konkreten Fall zum Ausschluß von der Wählbarkeit —, als die fünfjährige Ausschlußfrist schon längst abgelaufen war. Grund hierfür ist die fehlende Vorgabe in Nr. 12 a MiStra für die Staatsanwaltschaften, der Gemeinde auch den ggf. kompliziert zu berechnenden Tag des Endes der Ausschlußfrist mit der Verurteilungsnachricht bzw. nachträglich mitzuteilen. Auf der anderen Seite bestehen für die Gemeinden keine Vorschriften, sich bei der jeweiligen Staatsanwaltschaft über den präzisen Fristablauf zu erkundigen.

Damit ein solcher Fall nicht noch einmal passiert, habe ich das Niedersächsische Justizministerium und den Niedersächsischen Landeswahlleiter gebeten, die Informationslücke zu schließen. Das Justizministerium hat die mitteilungspflichtigen Staatsanwaltschaften angehalten, den Gemeinden zukünftig die Zeit mitzuteilen, für die der Verlust der Wählbarkeit wirksam ist. Der Niedersächsische Landeswahlleiter wiederum hat die Gemeinden aufgefordert, in „Fristfällen" bei den Staatsanwaltschaften sicherheitshalber nachzufragen.

Die gebotene gesetzliche Regelung der hier angesprochenen Mitteilungen der Staatsanwaltschaften an die Gemeinden soll in dem geplanten Strafverfahrensänderungsgesetz (Gesetz zur Änderung der StPO) erfolgen.

31.10 Mitteilungen von Klagen, Vollstreckungsmaßnahmen u.a. gegen Angehörige rechtsberatender Berufe

Seit 1. Januar 1992 sind von den Gerichten Mitteilungen zu machen über Forderungsklagen, Räumungsklagen, die hierzu ergehenden Entscheidungen, die in diesen Sachen beschlossenen Vergleiche, den Erlaß von Vollstreckungsbescheiden, Arrestgesuche und die hierzu ergehenden Entscheidungen, Anträge im Rahmen der Zwangsvollstreckung u.ä., soweit sie sich gegen Rechtsanwälte, Mitglieder der Rechtsanwaltskammern, Notare, Notarassessoren und

Patentanwälte richten. Die Mitteilungen sind an die zuständigen Kammern sowie die Präsidenten des zuständigen Landgerichts, den Präsidenten des Deutschen Patentamts usw. zu richten.

Mit der die vorgenannten Regelungen enthaltenden bundeseinheitlich abgestimmten Allgemeinen Verfügung (AV) „Mitteilungen von Klagen, Vollstreckungsmaßnahmen o. a. gegen Angehörige rechtsberatender Berufe" vom 5. Dezember 1991 hat das Niedersächsische Justizministerium nunmehr Verwaltungsvorschriften erlassen, die datenschutzrechtlich eine Verbesserung der bisherigen Bestimmungen aus dem Jahre 1970 darstellen (Nds. Rpfl. S. 291). So sind beispielsweise die Gerichte verpflichtet, nicht nur Mitteilungen zu machen über Klagen usw., sondern auch über die hierzu ergehenden Entscheidungen und über die in diesen Sachen geschlossenen Vergleiche. Mitteilungen haben zu unterbleiben, wenn ein mitzuteilender Sachverhalt offensichtlich für Maßnahmen z. B. nach der Bundesrechtsanwaltsordnung, der Bundesnotarordnung oder der Patentanwaltsordnung ohne Bedeutung ist oder wenn besondere gesetzliche Verwendungsregelungen entgegenstehen. Mitteilungen sind ferner zu berichtigen, wenn sich herausstellt, daß sie unrichtig waren oder unrichtig geworden sind. Darüber hinaus treffen Entscheidungen über Mitteilungen nunmehr die Richter bzw. Rechtspfleger für ihren Zuständigkeitsbereich.

Die AV berücksichtigt nicht alle meine Forderungen (vgl. X 31.5); so fehlt eine Regelung zur Unterrichtung der von einer Mitteilung Betroffenen sowie eine Regelung zur Löschung von Mitteilungen. Der Hinweis des Justizministeriums, daß nach dem Entwurf eines Justizmitteilungsgesetzes (JuMiG) in vergleichbaren Fällen auf die Unterrichtung der Betroffenen verzichtet wird (die Landesjustizverwaltungen sind der Auffassung, daß die Kenntniserlangung unterstellt werden könne, weil die AV bekanntgemacht werde und die Betroffenen als Angehörige der rechtsberatenden Berufe damit rechnen müßten, daß die in der AV aufgezählten Vorgänge mitgeteilt würden), überzeugt nicht. Nach § 21 Abs. 2 Nr. 1 des geplanten JuMiG soll eine Unterrichtungspflicht dann nicht bestehen, „wenn damit zu rechnen ist, daß der Betroffene von der Übermittlung seiner Daten auf andere Weise Kenntnis erlangt". Eine solche Vorschrift entspricht nicht den datenschutzrechtlichen Anforderungen hinsichtlich der Normenklarheit von Rechtsvorschriften, wie sie im Urteil des Bundesverfassungsgerichts vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 gefordert wird.

Hinsichtlich der Löschung der Mitteilung ist seitens der Landesjustizverwaltungen angeregt worden, in den einzelnen Ländern jeweils in Anlehnung an die Vorschriften über die Personalaktenführung zu verfahren. Zu begrüßen ist, daß das Justizministerium es aus datenschutzrechtlichen Erwägungen für angebracht hält, im Rahmen eines Erlasses oder einer Rundverfügung diesbezüglich eindeutige Regelungen zu schaffen. Ein in Aussicht gestellter Regelungsvorschlag des Justizministeriums liegt allerdings noch nicht vor.

Insgesamt jedoch sind mit der nunmehr geltenden Vorschrift Bestimmungen geschaffen worden, die als datenschutzrechtlicher Fortschritt bewertet werden können.

31.11 Mitteilungen der Gerichte über Klagen auf Räumung von Wohnraum

Der Gesetzentwurf der Bundesregierung zum Justizmitteilungsgesetz (JuMiG) sieht eine Änderung des § 15 a des Bundessozialhilfegesetzes (BSHG) vor. Danach soll das Gericht, bei dem eine Klage auf Räumung von Wohnraum im Falle der Kündigung des Mietverhältnisses nach § 554 des Bürgerlichen Ge-

setzbuchs eingegangen ist, dem zuständigen örtlichen Träger der Sozialhilfe unverzüglich zur Wahrnehmung der im derzeitigen § 15 a BSHG bestimmten Aufgaben (Gewährung von Hilfe zum Lebensunterhalt, zur Sicherung der Unterkunft oder zur Behebung einer vergleichbaren Notlage) den Tag des Eingangs der Klage mitteilen, es sei denn, der Zahlungsverzug der Mieterin bzw. des Mieters beruht offensichtlich nicht auf Zahlungsunfähigkeit. Die Mitteilung soll ferner enthalten die Namen und die Anschriften der Parteien, die Höhe des monatlich zu entrichtenden Mietzinses, die Höhe des geltend gemachten Mietzinsrückstandes und der geltend gemachten Entschädigung und den Termin zur mündlichen Verhandlung, sofern dieser bereits bestimmt ist. Die übermittelten Daten sollen auch für entsprechende Zwecke der Kriegsopferfürsorge nach dem Bundesversorgungsgesetz verwendet werden dürfen.

Mir leuchtet nicht ein, eine Übermittlung „von Amts wegen" an Sozialhilfeträger bzw. Versorgungsämter vorzusehen. Meines Erachtens hätte eine mietergerechte Lösung so aussehen können, daß das Gericht die Betroffenen aufklärt. Mit der Zustellung der Klage könnte ein Hinweis übersandt werden, in dem die Betroffenen über die Möglichkeit unterrichtet werden, bei Mittellosigkeit Unterstützung durch den Träger der Sozialhilfe oder ggf. Leistungen der Kriegsopferfürsorge (Übernahme der Mietzahlung) zu erhalten.

31.12 Angabe personenbezogener Daten im Rubrum von Zivilurteilen

Gegenstand der Beschwerde eines Petenten war die Tatsache, daß das Rubrum des Urteils eines Amtsgerichts (Zivilsache) neben der Anschrift (Straße, Ort) auch die Angabe „Justizvollzugsanstalt ..." enthielt. Der Petent legte anhand von Beispielen dar, daß der Gläubiger den Titel in vielen Fällen benutzen darf. Damit erfolge eine Übermittlung der Angabe „Justizvollzugsanstalt ...", so daß die Inhaftierung des Schuldners offenbart werde.

Es steht außer Frage, daß Gerichte die Bezeichnung der Parteien so vorzunehmen haben, daß die Vollstreckung des Urteils ohne Schwierigkeiten möglich ist. Ich sehe jedoch nicht ein, daß dieser Zusatz die Vollstreckung des Urteils erschwert oder unmöglich macht.

Das Justizministerium hat seinen Geschäftsbereich über meine Auffassung unterrichtet. Es verweist darauf, daß in der Regel eine Notwendigkeit für die Anbringung des Zusatzes „Justizvollzugsanstalt" weder im Hinblick auf die Zustellbarkeit noch auf die Vollstreckbarkeit der Entscheidung gegeben ist.

31.13 Datenschutz bei der Zwangsvollstreckung

Datenschutzrechtlich problematisch ist die Zustellung von Pfändungs- und Überweisungsbeschlüssen vom Gerichtsvollzieher durch die Post an Drittschuldner, weil dabei der Inhalt der Beschlüsse einer Vielzahl von Bediensteten zur Kenntnis gelangen kann, bevor sie bei der sachbearbeitenden Stelle, z. B. Personal- oder Lohnbüro, vorliegen. Das auf dieses Problem von mir hingewiesene Niedersächsische Justizministerium betrachtet die Zustellungen in den einzelnen Verfahrensarten als gesetzlich geregelt (§ 166 bis 213 a ZPO — Allgemeine Zustellungsvorschriften, § 829 Abs. 2 ZPO — Verfahrensspezifische Vorschriften). Bei § 173 Gerichtsvollziehergeschäftsanweisung (GVGA) handele es sich um eine Beschreibung des gesetzlichen Zustellungsverfahrens. Im übrigen bezweifelt das Ministerium aufgrund der unterschiedlichen Organisationsstrukturen und der technischen Abläufe bei den Mitteilungsempfängern (z. B. Unternehmen) die Durchführbarkeit einer datenschutzrechtlich

angemessenen gesetzlichen Regelung. Neben den Problemen, die allgemein gültige Beschreibung des Adressatenkreises zu normieren, wären seiner Ansicht nach entsprechende Regelungen letztlich ein Eingriff in privatrechtliche oder öffentlich-rechtliche Organisationsstrukturen, dem erhebliche Bedenken entgegenstünden. Ich verkenne die hier zu lösenden Schwierigkeiten nicht, wenngleich eine datenschutzgerechtere Zustellungsform wünschenswert bzw. in vielen Fällen notwendig ist. Allerdings hoffe ich, daß bei der beabsichtigten Reform des Zustellungsrechts das Problem gelöst werden wird.

31.14 Bescheinigungen in Familiensachen (Sorgerecht)

Mir lag eine Beschwerde über folgenden Sachverhalt vor: Ein Amtsgericht hatte in einer Familiensache ein Urteil (Verbundentscheidung) verkündet. Es enthielt u. a. eine Regelung hinsichtlich des Sorgerechts der minderjährigen — über 14 Jahre alten — Tochter. Da Kinder über 14 Jahren ein eigenes Rechtsmittel bezüglich der sie betreffenden Sorgerechtsentscheidungen haben, muß ihnen das Urteil des Familiengerichts, soweit es sie betrifft (§ 624 Abs. 4 ZPO), zugestellt werden. In dem vorliegenden Fall erhielt die Tochter u. a. einen „Auszug" über den vollständigen — acht Punkte umfassenden — Urteilstenor mit Aussagen über Scheidung, Sorgerecht, Übertragung von Rentenanwartschaften, Ehegattenunterhalt und Zugewinnausgleich. Nach § 624 Abs. 4 ZPO hätte der Tochter aus der Urteilsformel aber nur die Entscheidung zum Sorgerecht (eine von acht Ziffern) mitgeteilt werden müssen.

Die Minderjährige benötigte die Sorgerechtsentscheidung zur Vorlage bei Dritten (z. B. Lehrherrn, Schule, Banken usw.). Der übersandte Komplettauszug der Urteilsformel hatte nun zur Folge, daß die Tochter den anfordernden Stellen auch Daten übermitteln mußte, die für die jeweiligen Zwecke überhaupt nicht erforderlich waren und bei denen es sich zudem um sehr sensible Daten handelte.

Das Gericht hat die Zustellung eines Urteilsauszuges veranlaßt, der nur den Sorgerechtsteils des Tenors enthält, und wird künftig in ähnlichen Fällen entsprechend verfahren.

31.15 Übersendung von Gerichtsakten an Sachverständige für die Erstellung von Gutachten

Mehrfach habe ich davon Kenntnis erlangt, daß Gerichte die gesamte Gerichtsakte übersenden, um Gutachten erstellen zu lassen. So führte der Auftrag eines Familiengerichts, ein Gutachten über den Mietwert eines Hauses zu erstellen, dazu, daß die komplette Akte — nahezu 200 Blatt mit sensiblen Angaben zu wirtschaftlichen und intimen familiären Verhältnissen, mit Behauptungen, Verdächtigungen und Erwiderungen der Parteien — einem Sachverständigen zugeleitet wurde.

Unbeschadet der in Art. 97 GG normierten richterlichen Unabhängigkeit haben Gerichte das Recht auf informationelle Selbstbestimmung bei der Anwendung zivilprozessualer Vorschriften zu beachten (Art. 1 Abs. 3 GG). Aus datenschutzrechtlicher Sicht ist es daher nicht zu akzeptieren, wenn bei der Vornahme und Umsetzung von Beweisbeschlüssen der Grundsatz der Erforderlichkeit keine Beachtung findet, indem zahlreiche Unterlagen, die für die Erstellung des Gutachtens nicht erforderlich sind, an die Gutachterin bzw. den Gutachter mitübersandt werden.

31.16 Datenerhebung bei der Eintragung einer Namensänderung im Grundbuch durch ein Amtsgericht

Kein Verständnis hatte ein Bürger dafür, daß vom Grundbuchamt ein — nach der Eheschließung neu ausgestellter — Personalausweis seiner Ehefrau als Urkunde für eine Grundbuchberichtigung nicht akzeptiert wurde. Die Ehefrau als im Grundbuch eingetragene Eigentümerin sollte, um die Gründe für die Namensänderung prüfen zu können, ihre Heiratsurkunde vorlegen, in der auch die Daten ihres Ehemannes vermerkt sind. Der Ehemann war hiermit nicht einverstanden. Nach seiner Auffassung reicht für die Änderung des Namens seiner Ehefrau im Grundbuch die Erkennbarkeit seines Vor- und Zunamens aus. Die Offenbarung weiterer Daten, wie Geburtsdatum/-ort und Wohnort, lehnte er ab. Bei der Vorlage der Heiratsurkunde sollten von seinen Daten allenfalls der Vor- und Familienname erkennbar, alle weiteren Daten aber unkenntlich sein.

Ich habe Verständnis für den Standpunkt des Petenten geäußert, da nach dem datenschutzrechtlichen Grundsatz der Erforderlichkeit nur die Daten verwendet werden dürfen, die für die jeweilige Aufgabenerfüllung unerläßlich sind. Danach wäre als Nachweis für die Namensänderung der Ehefrau des Petenten deren Personalausweis zu akzeptieren.

Ich mußte aber die auf § 29 Abs. 1 Satz 2 der Grundbuchordnung (GBO) gestützte Forderung des Grundbuchamtes nach Vorlage der Heiratsurkunde als rechtlich vertretbar akzeptieren. Die Offenlegung nur des Vor- und Familiennamens aus der Heiratsurkunde würde rechtlich einem Auszug gleichkommen. Nach dem Personenstandsrecht ist jedoch ein solcher Auszug nicht möglich. Die für eine Heiratsurkunde vorgesehenen Angaben sind in § 63 des Personenstandsgesetzes (PStG) geregelt. Ein Auszug aus der Heiratsurkunde ist in dem engen Rahmen des § 65 a PStG zulässig. Der Auszug nur über Vor- und Familienname ist hiernach nicht gestattet. Eine Heiratsurkunde, die nicht alle in § 63 PStG beschriebenen Daten enthält, ist wiederum eine unvollständige — öffentliche — Urkunde. Sie genießt nicht die vom Grundbuchamt geforderte Beweiskraft einer vollständigen Heiratsurkunde gemäß § 66 PStG.

Das von mir eingeschaltete Niedersächsische Innenministerium hat sich der Frage „Auszüge aus der Heiratsurkunde" angenommen. Es hat mich weiter über eine geplante Änderung und Ergänzung des Personenstandsgesetzes unterrichtet. Nach § 61 a des Entwurfs für ein 5. Personenstandsänderungsgesetz (Stand Oktober 1989) sollen Behörden Auskunft aus einem oder Einsicht in einen Personenstandseintrag sowie Erteilung von Personenstandsurkunden nur verlangen können, „soweit dies zur Erfüllung ihrer Aufgaben erforderlich ist" und die weiteren in der Vorschrift genannten Voraussetzungen erfüllt werden. Damit wäre sichergestellt, daß das Standesamt auch Auskünfte aus den Personenstandsbüchern geben könnte, die sich auf das für die Erfüllung der Aufgaben der empfangenden Behörde erforderliche Maß beschränkt.

31.17 Datenschutz bei Notaren

Notare unterliegen meiner datenschutzrechtlichen Kontrolle. Dies ist auch Auffassung des Justizministeriums (vgl. Allgemeine Verfügung vom 9. Januar 1987 — Nds. Rpfl. S. 29).

In einer Eingabe rügte eine Einsenderin, daß die Mitteilung des zuständigen Amtsgerichts über die Eintragung einer Grundschuld im Grundbuch von dem beurkundenden Notar nicht an sie direkt, sondern über die Rechtsbeistands- und amtliche Auktionatoren-Praxis, die zuvor das Hausgrundstücksgeschäft

vermittelt hatte, an die Petentin übersandt worden war. Datenschutzrechtlich bedeutete dies eine Datenübermittlung, für die weder eine Rechtsgrundlage noch eine Einwilligung vorlag. Meine Überprüfung ergab, daß die Weitrgabe über Dritte auf einem Versehen beruhte.

In einer anderen Angelegenheit hatte ein Notar bei der Beglaubigung der Unterschrift einer Petentin (Zustimmung zur Veräußerung einer Eigentumswohnung nach § 12 Wohnungseigentumgesetz) auch deren Geburtsdatum und die Anschrift aus dem Personalausweis in die Urkunde aufgenommen. Nach Auffassung der Beschwerdeführerin hätte es genügt, wenn Name und Vorname sowie der Zusatz „ausgewiesen durch Personalausweis Nr. ..." in die Urkunde aufgenommen worden wären. Die Daten wurden an alle Miteigentümer weitergegeben. Es ist fraglich, ob § 10 des Beurkundungsgesetzes insoweit eine normenklare Vorschrift ist. Danach sollen Beteiligte so genau bezeichnet werden, daß Zweifel und Verwechslungen über die Person ausgeschlossen sind. Der Vorgang ist noch nicht abgeschlossen.

31.18 Presse- und Öffentlichkeitsarbeit der Justiz

In meinen vorangegangenen Tätigkeitsberichten (vgl. X 31.21) habe ich die Notwendigkeit geäußert, die aus dem Jahre 1974 stammenden näheren Bestimmungen über die Öffentlichkeitsarbeit der Justizbehörden zu überarbeiten. Das Justizministerium ist mit mir der Auffassung, daß die aus dem Jahr 1974 stammenden Bestimmungen überarbeitungsbedürftig sind. Entsprechende Arbeiten sind eingeleitet.

31.19 Datenerhebungen durch Amtsgerichte

Private Arbeitgeber werden häufig von Amtsgerichten gebeten, Auskünfte über Mitarbeiterinnen und Mitarbeiter zu erteilen. In der Regel werden dabei sensible personenbezogene Daten übermittelt. Die Gerichte sind meines Erachtens verpflichtet, in ihren Anforderungen die jeweilige zur Auskunft verpflichtende Rechtsvorschrift zu nennen, damit der Arbeitgeber die Verpflichtung zur Datenübermittlung und deren zulässigen Umfang beurteilen kann.

Ich habe aus gegebenem Anlaß das Sozialministerium, das Finanzministerium und das Justizministerium darauf hingewiesen, entsprechende Maßnahmen zu ergreifen.

31.20 Einhaltung von Mitteilungsfristen

Nach Feststellungen des Bundesbeauftragten für den Datenschutz gehen Mitteilungen über den Straferlaß nach § 37 Abs. 2 Bundeszentralregistergesetz häufig mit Verzögerungen beim Bundeszentralregister (BZR) ein. Dies kann zur Herausgabe unrichtiger Führungszeugnisse führen. Ich habe das Niedersächsische Justizministerium auf diese Problematik hingewiesen. Aus datenschutzrechtlicher Sicht ist zu begrüßen, daß die mitteilungspflichtigen Stellen inzwischen vom Justizministerium gebeten worden sind, die Fristen für die Mitteilungen an das BZR unbedingt einzuhalten, und die Dienstaufsicht angehalten worden ist, im Rahmen der regelmäßigen Geschäftsprüfungen auf die Einhaltung der Fristen zu achten.

32. Strafvollzug

32.1 Strafvollzugsgesetz/Untersuchungshaftvollzugsgesetz

In Tätigkeitsberichten vergangener Jahre habe ich auf die Notwendigkeit zur Schaffung bereichsspezifischer Regelungen im Strafvollzugsgesetz hingewiesen (vgl. insbesondere IX 32.1). Der Vorläufige Referentenentwurf eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes (Stand: 25. März 1991) enthält Regelungen über den Schutz und die Verwendung personenbezogener Daten. Er wird dem Erfordernis bereichsspezifischer Konkretisierung jedoch noch nicht vollständig gerecht. Die Besonderheiten, die aus den rechtlichen und tatsächlichen Bedingungen des Strafvollzuges folgen, sollten in normenklare Regelungen über den Umgang mit personenbezogenen Daten von Gefangenen und anderen Personen noch besser berücksichtigt werden.

Ich habe dem Niedersächsischen Justizministerium eine umfangreiche Ausarbeitung „Datenschutzfragen im Strafvollzug" zugeleitet. Sie verdeutlicht datenschutzrechtliche Defizite des Strafvollzugs bei Datenerhebung, -speicherung, -übermittlung, -löschung und bei der Häftlingsüberwachung. Dieses Papier enthält im übrigen zahlreiche Beispiele für die Verarbeitung personenbezogener Daten Gefangener, die auf der Grundlage der Verwaltungsvorschrift Vollzugsgeschäftsordnung (VGO) erfolgen (Aufnahmeverfahren — Nr. 16 VGO, Ärztliche Untersuchung — Nr. 60 VGO, Erkennungsdienstliche Maßnahmen — Nr. 23 VGO, Behandlungsuntersuchung — Nr. 31 VGO, Auskünfte an Private — Nr. 5 VGO usw.). Ich habe das Justizministerium gebeten, das vorliegende Papier bei den weiteren Beratungen zur Novellierung des Strafvollzugsgesetzes zu berücksichtigen.

Wenig erfreulich ist auch, daß es noch immer an einem Untersuchungshaftvollzugsgesetz (vgl. X 32.4) fehlt. Derzeit bestehen für Eingriffe in das informationelle Selbstbestimmungsrecht von Untersuchungsgefangenen keine normenklaren gesetzlichen Grundlagen. Die Verarbeitung der personenbezogenen Daten von Gefangenen in Untersuchungshaft erfolgt auf der Grundlage von Verwaltungsvorschriften (Untersuchungshaftvollzugsordnung — UVollzO), deren Rechtsqualität unzureichend ist und nicht die Anforderungen erfüllt, die das Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983 zum Volkszählungsgesetz 1983 postuliert hat. Der vorliegende Arbeitsentwurf eines Untersuchungshaftvollzugsgesetzes (Stand: 24. Februar 1986) ist bis heute nicht bearbeitet worden. Im Hinblick auf die Rechtsprechung zum Übergangsbonus bedarf es dringender Arbeiten zur Schaffung der normenklarer gesetzlicher Grundlagen für die Verarbeitung personenbezogener Daten im Untersuchungshaftvollzug.

32.2 Verwendung veralteter Vordrucke in Justizvollzugsanstalten (Lebenslauf, Fragebogen)

Ein Gefangener beschwerte sich darüber, daß er nach seiner Verlegung in eine andere Justizvollzugsanstalt dort aufgefordert wurde, die Vordrucke „Lebenslauf" und „Fragebogen" (VG 16 und VG 17 — Nr. 31 VGO), auszufüllen. Diese Vordrucke enthielten keine Hinweise auf die Freiwilligkeit. Meine Überprüfung ergab, daß in dieser Justizvollzugsanstalt noch veraltete Vordrucke aus dem Jahre 1977 Verwendung fanden, die nicht die datenschutzrechtlichen Verbesserungen enthielten, die ich in Erörterungen mit dem Justizministerium im Jahre 1987 durchgesetzt hatte (vgl. IX 32.2). Meine Bemühungen hatten seinerzeit zum Ergebnis, daß die bundeseinheitlich neu gefaßten Vordrucke mit Wirkung vom 1. September 1987 eingeführt wurden. Sie enthielten im Kopf den Aufdruck: „Das Ausfüllen des Fragebogens ist freiwillig; ein

Nichtausfüllen hat keine disziplinarischen Folgen. Sie sollten jedoch die in § 6 des Strafvollzugsgesetzes geforderte Erforschung Ihrer Persönlichkeit und Ihrer Lebensverhältnisse durch Ausfüllen des Fragebogens unterstützen und dadurch in Ihrem eigenen Interesse wichtige Grundlagen für eine Ihnen gerechtwerdende Vollzugsplanung schaffen."

Bei meiner Prüfung erfuhr ich außerdem, daß mindestens in zwei Justizvollzugsanstalten seit drei Jahren noch immer diese veralteten Vordrucke an die Gefangenen ausgegeben wurden. Zu den weiteren Fragen wurde mir seitens des Justizministeriums erklärt, daß der Lebenslauf und der Fragebogen, unabhängig davon, ob sie ausgefüllt werden oder nicht, zur Gefangenenpersonalakte genommen werden. Dort seien sie allen mit der Behandlung des jeweiligen Gefangenen befaßten Bediensteten zugänglich, daneben in Einzelfällen auch Angehörigen der Aufsichtsbehörden

Ich habe die Verwendung der überholten Vordrucke beanstandet. Inzwischen hat das Justizvollzugsamt mit Rundverfügung vom 17. Dezember 1990 die Justizvollzugsanstalten und Jugendanstalten erneut darauf hingewiesen, daß ausschließlich die neu gefaßten Vordrucke VG 16 und VG 17 zu verwenden und die überholten Vordrucke unverzüglich auszusondern sind.

32.3 Aufbewahrung von psychiatrischen und psychologischen Gutachten über Gefangene

Durch Erlaß vom 25. April 1991 an das Niedersächsische Justizvollzugsamt hat das Justizministerium bestimmt, daß die psychiatrischen und psychologischen Gutachten über Gefangene bis zum Inkrafttreten der datenschutzrechtlichen Novelle zum Strafvollzugsgesetz nur der Anstaltsleitung, der zuständigen Abteilungsleitung sowie den Bediensteten des ärztlichen und des psychologischen Dienstes zugänglich zu machen sind. Dabei sind die Gutachten für die Dauer der Strafverbüßung in einem besonderen Ordner in der Vollzugsgeschäftsstelle unter Verschluß zu halten. Der Verbleib der Gutachten ist auf dem A-Bogen der Gefangenenpersonalakte zu vermerken. Nach der Entlassung sind die Gutachten wieder zur Gefangenenpersonalakte zu nehmen. Bei neu zugehenden Gefangenen sind die Gutachten ab sofort gesondert zu verwahren. Bei den übrigen Gefangenen sollten die Gutachten bis zum 31. Dezember 1991 aus den Gefangenenpersonalakten entfernt und in dem Sonderordner abgeheftet werden.

Aufgrund der von einigen Anstaltsleitern vorgebrachten Kritik sah sich das Justizministerium veranlaßt, die im April 1991 getroffenen Regelungen auf psychiatrische Gutachten sowie die dazu erstellten psychologischen und neurologischen Zusatzgutachten zu beschränken. Die Neufassung des Erlasses regelt nunmehr, daß neben dem vorbezeichneten Personenkreis auch der in der jeweiligen Vollzugsabteilung tätigen Abteilungshelferin bzw. dem Abteilungshelfer, den pädagogischen, sozialpädagogischen und soziologischen Fachkräften sowie den zuständigen Mitarbeiterinnen und Mitarbeitern der Aufsichtsbehörden die psychiatrischen Gutachten, soweit dies für die Wahrnehmung vollzuglicher Aufgaben im Einzelfall erforderlich ist, zugänglich zu machen sind. Darüber hinaus ist nach dieser Verwaltungsvorschrift die Überlassung der psychiatrischen Gutachten an andere öffentliche Stellen zulässig, wenn eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt. Alle übrigen nicht-ärztlichen Gutachten (z. B. psychologische Gutachten und Einweisungsgutachten) sind zur Gefangenenpersonalakte zu nehmen.

Ich werde wegen der Beschränkung auf psychiatrische Gutachten und der Erweiterung des zugangsberechtigten Personenkreises weitere Gespräche unter dem Gesichtspunkt der Erforderlichkeit mit dem Justizministerium führen.

32.4 Auskünfte einer Justizvollzugsanstalt über einen Gefangenen

Gegenstand der Beschwerde eines Strafgefangenen war die nach seiner Meinung unzulässige Auskunft einer Justizvollzugsanstalt an eine Wirtschaftsauskunftei, daß der Gefangene dort inhaftiert war, und die weitere Auskunft, daß der Gefangene in eine andere Justizvollzugsanstalt verlegt wurde, wobei diese Anstalt namentlich genannt worden ist. Die Auskunftei benötigte die ladungsfähige Anschrift des Gefangenen.

Das Niedersächsische Justizministerium vertritt mit der Justizvollzugsanstalt und dem Justizvollzugsamt die Auffassung, daß die Auskünfte in Anwendung von § 11 NDSG i.V.m. Nr. 5 der Verwaltungsvorschrift „Vollzugsgeschäftsordnung (VGO)" und i. V. m. den Rundverfügungen des Justizvollzugsamtes vom 23. Dezember 1983 und 27. November 1984 zu Recht erteilt wurden. Die Abwägung der Interessen des Gefangenen an der Geheimhaltung seines Aufenthaltsortes und der Wirtschaftsauskunftei an der Bekanntgabe einer ladungsfähigen Adresse durch die Justizvollzugsanstalt habe ergeben, daß zugunsten des Interesses der Auskunftei zu entscheiden sei. Das Justizministerium weist in diesem Zusammenhang außerdem darauf hin, daß sich die Anstalt bei ihrer Entscheidung auf die Begründung des Beschlusses des Oberlandesgerichts Celle vom 21. September 1984 (NStZ 1985, S. 44) habe stützen können, wonach bei Vorliegen eines rechtlichen Interesses der anfragenden Privatperson die Informationen mitgeteilt werden dürfen, die zur Verfolgung dieses Interesses notwendig sind. Die Auskunftserteilung müsse zur Erreichung des angestrebten Zweckes geeignet und erforderlich sein (vgl. VI 29.2). Ein rechtliches Interesse der Wirtschaftsauskunftei habe in diesem Falle vorgelegen. Ohne eine ladungsfähige Adresse des Schuldners könne z. B. eine titulierte Forderung nicht eingezogen werden.

Meines Erachtens hat die Justizvollzugsanstalt gegen das Recht auf informationelle Selbstbestimmung verstoßen. Ich vermag mich den vorstehenden Überlegungen nicht anzuschließen. Es kann dahinstehen, ob die Tatbestandsmerkmale des § 11 Satz 1, 2. Alt. NDSG vorliegen bzw. ob bei Heranziehung der Verwaltungsvorschriften Nr. 5 Abs. 3 VGO eine Begründung mit dem sog. Übergangsbonus erfolgen kann (mit dem Übergangsbonus argumentiert das OLG Hamm in seinem Beschluß vom 28. April 1988, vgl. NStZ 1988, 381).

Einen Rückgriff auf die allgemeine Rechtsgrundlage in § 11 Satz 1, 2. Alt. NDSG halte ich nicht für möglich. Mit dem Inkrafttreten des Niedersächsischen Meldegesetzes (NMG) vom 2. Juli 1985 sind melderechtliche Verfahren hinsichtlich durch das Melderegister erfaßter Personen — wozu auch Strafgefangene gem. § 17 Abs. 3 NMG gehören — nach den Vorschriften dieses Gesetzes zu beurteilen. Bei den Anfragen der Wirtschaftsauskunftei hat es sich in der Sache darum gehandelt, ob der Gefangene unter dieser Anschrift erreichbar ist. Für Auskünfte über die Anschrift ist nach § 2, 33 Abs. 1 NMG die Meldebehörde zuständig. Eine Zuständigkeit von Justizvollzugsanstalten ergibt sich aus dem NMG nicht. Da insoweit eine die gewünschte Rechtsfolge erlaubende Rechtsvorschrift vorliegt, ist für eine Anwendung der Nr. 5 Abs. 3 VGO i.V.m. dem Übergangsbonus kein Raum. Nach meiner Auffassung konnte sich die Justizvollzugsanstalt daher bei ihrer Auskunft an die Wirtschaftsauskunftei nicht auf eine die Übermittlung rechtfertigende Rechtsvorschrift berufen. Darüber hinaus hatte die Justizvollzugsanstalt nicht die Rundverfügung vom 25. April 1986 beachtet, in der die Zuständigkeit der Meldebehörde für Melderegisterauskünfte in den Fällen des § 17 Abs. 3 NMG klargestellt wird (vgl. VIII 32.2). In diesem Zusammenhang ist auch darauf hinzuweisen, daß § 128 Abs. 5 Satz 2 des Vorläufigen Referentenentwurfes eines Vierten Gesetzes zur Änderung des Strafvollzugsgesetzes (Stand 25. März 1991) ausdrücklich vom „Vorrang des Melderechts" ausgeht.

Der Beschwerdefall hatte jedoch eine positive Auswirkung: Die betreffende Justizvollzugsanstalt hat, nachdem ihr das Ergebnis meiner datenschutzrechtlichen Prüfung bekannt geworden war, umgehend in einer Anstaltsverfügung die Erteilung von Auskünften an private Dritte dahingehend geregelt, daß an die für die Justizvollzugsanstalt zuständige Meldebehörde verwiesen wird.

32.5 Ausgabe von Kontoauszügen an Strafgefangene

Ich habe wiederholt über die Praxis der Ausgabe von Kontoauszügen an Gefangene berichtet (vgl. X 32.2). Aufgrund weiterer Eingaben zu dieser Problematik habe ich mit dem Niedersächsischen Justizministerium diese Frage nochmals erörtert. Die Anstalten sind nunmehr gehalten, in Zukunft bei der Unterrichtung der Gefangenen über den Kontostand die Kontoauszüge geknickt und geklammert an die Gefangenen aushändigen zu lassen. Datenschutzrechtlich nichts einzuwenden ist gegen ein Verfahren, bei dem vor Wochenenden der jeweils aktuelle Kontostand als Liste den Stationen in den Justizvollzugsanstalten mitgeteilt wird, damit auch außerhalb der Geschäftszeiten der Zahlstelle (spontane) Ausgaben wie z. B. Telefonate und Fahrtkosten genehmigt werden können. Die Liste ist jedoch spätestens Montag vormittag der nächsten Woche zu vernichten.

32.6 Telefongespräche der Anstaltsseelsorger

Die Norddeutsche Konferenz der katholischen Seelsorger bei den Justizvollzugsanstalten in Bremen, Hamburg, Niedersachsen und Schleswig-Holstein hat die Erfassung von Telefongesprächsdaten von Anstaltsseelsorgern in Justizvollzugsanstalten problematisiert. So wurde ausgeführt, daß Seelsorger der Schweigepflicht unterliegen, die auch bei Telefongesprächen berührt sein kann. Beispiel: Bei einem Gespräch geht es um eine AIDS-Erkrankung. In diesem Zusammenhang werden telefonisch Informationen bei einer AIDS-Beratungsstelle eingeholt. Ein Vergleich der Telefonnummer der AIDS-Beratungsstelle mit dem Namen der Gesprächspartnerin oder des Gesprächspartners des Seelsorgers läßt den Rückschluß zu, daß die oder der Betroffene HIV-positiv ist — eine Information, welche durch das Seelsorgegeheimnis geschützt ist.

Zu dieser Problematik wurde im Niedersächsischen Landtag eine gleichgelagerte Anfrage gestellt. Das Niedersächsische Justizministerium hat daraufhin für seine Stellungnahmen an den Landtag und an mich umfangreiche Recherchen durchgeführt.

Als Ergebnis konnte der anfragenden Institution folgendes mitgeteilt werden:

„Nach den Ausführungen des Justizministeriums werden Telefongespräche der Anstaltsseelsorger in den Anstalten unterschiedlich erfaßt, weil diese mit unterschiedlichen Telefonanlagen ausgestattet bzw. an die Telefonanlage eines benachbarten Gerichts angeschlossen sind. In sieben niedersächsischen Anstalten werden lediglich die Gebühreneinheiten des Apparates des Anstaltsseelsorgers erfaßt, gegebenenfalls auch das Datum des Gesprächs. Eine Erfassung der angewählten Nummer erfolgt in diesen Anstalten nicht.

In einer Anstalt wird seit Juli 1989 bei Privatgesprächen und bei Ferngesprächen des Personalrats die angewählte Telefonnummer nicht mehr ausgedruckt. Dieses Verfahren sei nunmehr auf die von den Anstaltsseelsorgern geführten Gespräche ausgedehnt worden. In den übrigen Anstalten

werden über die Telefonzentrale bei dienstlichen Ferngesprächen Datum, Uhrzeit, die Nummer des Anstaltsapparates und des angewählten Telefons sowie die Zahl der Gebühreneinheiten erfaßt und ausgedruckt.

Das Justizministerium hat das Niedersächsische Justizvollzugsamt angewiesen, in Zukunft gemäß Ziffer 6 der Dienstanschlußvorschriften (RdErl. des Niedersächsischen Finanzministeriums vom 31. Juli 1989, Nds. MBl. Nr. 31/90) die Anstaltsgeistlichen den Personalräten hinsichtlich der Erfassung der dienstlichen Ferngespräche gleichzustellen, sofern dies ohne unverhältnismäßigen Aufwand möglich ist. Dies bedeutet:

— In den Anstalten, in denen die Telefonanlage die Möglichkeit bietet, die Telefonanschlüsse des Anstaltsgeistlichen automatisch von der Erfassung der angewählten Telefonnummern auszunehmen, ist so zu verfahren;

— in den Anstalten, in denen eine solche Ausnahme von der Erfassung technisch nicht möglich ist, sind die Telefonrechnungen den Anstaltsgeistlichen ungeprüft in verschlossenen Umschlägen zuzuleiten."

Die Dienstanschlußvorschriften des Niedersächsischen Finanzministeriums sind seinerzeit nach intensiver Einwirkung meiner Dienststelle erlassen worden (vgl. X 15.11).

32.7 Telefonate Gefangener im Strafvollzug

In einer Justizvollzugsanstalt (JVA) bestand am Eingang zum Zellenflur einer Station, auf der ca. 45 Gefangene untergebracht waren, für Gefangene die Möglichkeit, von einem dort unter einer Telefonhaube angebrachten Fernsprechapparat Telefongespräche entgegenzunehmen oder Telefonate nach außerhalb zu führen. An dieser Stelle des Stationsflurs herrschte jedoch ein ständiges Kommen und Gehen, insbesondere zur Telefonzeit zwischen 18.00 und 20.00 Uhr, wenn die Hafträume für die Freizeit geöffnet sind. So konnten die sich auf dem Flur aufhaltenden Gefangenen (mit)hören, was gesprochen wurde. Dabei wurden Telefonate mit Angehörigen ebenso wie mit Rechtsanwälten und Behörden geführt. Die Telefonbenutzer waren praktisch gezwungen, ihre Verhältnisse vor Dritten unfreiwillig offenzulegen. Hiergegen richtete sich die Beschwerde eines Gefangenen.

Die JVA hatte zunächst beabsichtigt, gebrauchte Telefonzellen aus Altbeständen der Bundespost, die im geschlossenen Zustand einen hinreichenden Schutz gegen ein unbefugtes Mithören gewährleistet hätten, aufzustellen. Leider ließ sich dieses Verfahren aus baulichen Gründen (wegen räumlicher Enge und der damit verbundenen Behinderung des Dienstbetriebes) nicht verwirklichen. Die JVA hat sich deshalb dafür entschieden, Teilbereiche von den Gemeinschaftsräumen auf verschiedenen Stationsfluren, die nicht mehr benutzt wurden, baulich abzutrennen und Fernsprechapparate in diesen Räumen zu installieren. Damit wird datenschutzrechtlichen Belangen in erfreulicher Weise Rechnung getragen.

32.8 Einkaufszettel für Zeitschriften und Schreibwaren pp.

„Dauerbrenner" sind die datenschutzrechtlichen Probleme beim Einkauf der Gefangenen. Auf dem Vordruck „Einkaufszettel für Zeitschriften und Schreibwaren pp." hatte ein Gefangener neben den Angaben zu seinen Einkaufswünschen seine personenbezogenen Daten Name, Vorname, Gefange-

nenbuchnummer, Kontonummer, Haus der Anstalt, Station und Zellennummer einzutragen. Danach wurde die Bestellung auf dem Einkaufszettel von der Zahlstelle mit dem Kontostand des Gefangenen überprüft. Der Einkaufszettel wurde dem Schreibwarenhändler ausgehändigt, der sodann den Betrag eintrug, der sich aus dem Auftrag ergab. Datenschutzrechtlich war die Aushändigung des Einkaufszettel mit den personenbezogenen Daten an den Schreibwarenhändler als unbefugte Datenübermittlung an Personen außerhalb des öffentlichen Bereichs nicht zu akzeptieren.

Auf meine Intervention hin hat die Justizvollzugsanstalt inzwischen eine Verfügung erlassen, nach der die Einkaufszettel mit dem Zusatz zu versehen sind: „Mit der Nennung meines Namens und Buch-Nr. bei der Bestellung von Waren bin ich einverstanden/nicht einverstanden". Dieser Zusatz gewährleistet das Recht des einzelnen, selbst über die Verwendung seiner personenbezogenen Daten zu bestimmen. Unberührt bleibt nach wie vor die Möglichkeit, daß der Betroffene persönlich Bestellungen vornimmt oder durch Dritte erledigen läßt. Dieses Verfahren trägt datenschutzrechtlichen Erfordernissen Rechnung.

32.9 Datenübermittlungen aus einer Bestandstafel

In X 32.4 stellte ich dar, daß in einer Vollzugsanstalt Daten von Untersuchungshäftlingen auf einer Bestandstafel aufgeführt waren, die in dem Stationszimmer angebracht war. Diese Angaben konnten von Dritten (Strafgefangene, Besucherinnen und Besucher) abgelesen werden. Ich habe darauf hingewiesen, daß es für diese Datenübermittlung keine Rechtsgrundlage gibt. Meine in diesem Zusammenhang durchgeführten Bemühungen um datenschutzrechtliche Verbesserungen führten zum Erfolg. Inzwischen wird der hinter dem Stationszimmer befindliche Haftraum, um den das Stationszimmer erweitert wurde, als Verwaltungsraum genutzt. Die fragliche Bestandstafel ist in diesem Zimmer angebracht. Sie kann von außen nicht mehr eingesehen werden. Zu diesem Raum haben nur zuständige Bedienstete der Justizvollzugsanstalt Zugang.

32.10 Schriftverkehr von Gerichten/Behörden mit Gefangenen

Mehrere Eingaben haben mich darauf aufmerksam gemacht, daß Gerichte und Behörden Schreiben an Gefangene z. T. an die Justizvollzugsanstalten adressieren und z. T. offen versenden. Diese Art des Schriftverkehrs führt zu einer nicht datenschutzgerechten und unnötigen Weitergabe von persönlichen Daten der Betroffenen an Dritte. Ich halte es für eine Selbstverständlichkeit, Schreiben an Gefangene auch nur an sie zu adressieren. Dies gebietet schon der in Art. 10 Abs. 1 GG verankerte Schutz des Briefgeheimnisses. Auch läßt sich dem § 30 des Verwaltungsverfahrensgesetzes der allgemeine Rechtsgedanke entnehmen, daß Schreiben mit persönlichen Daten oder Angaben, die Rückschlüsse auf persönliche Verhältnisse zulassen, grundsätzlich verschlossen zu übersenden sind.

Aus datenschutzrechtlicher Sicht bedarf jede Weitergabe von Daten an Dritte einer Rechtsgrundlage. In manchen Fällen haben nun die absendenden Stellen ihr Verhalten mit dem Hinweis zu rechtfertigen versucht, die Vorschriften des Strafvollzugsgesetzes über das Vermitteln der Post durch die Anstalt bzw. die mögliche Sicht- und Textkontrolle eingehender Briefe erlaube die eingangs dargestellten Übersendungsformen. Nach meiner Auffassung richten sich die Bestimmungen des Strafvollzugsgesetzes jedoch nur an die Justizvollzugsanstalten. Sie erlauben den absendenden Gerichten und Behörden nicht, an Gefangene gerichtete Schreiben an die Anstalt zu adressieren oder sie

— gleichsam im Vorgriff auf eventuelle Maßnahmen der Justizvollzugsanstalt — gleich offen zu versenden. Das Niedersächsische Justizministerium teilt meine Meinung. Im Bereich der Justiz liegt jetzt eine insoweit klarstellende Verwaltungsvorschrift vor (vgl. Allgemeine Verfügung v. 9. Juli 1992, Nds. Rpfl. S. 190).

32.11 Personenbezogene Daten in der Müllzelle einer Justizvollzugsanstalt

In einer Justizvollzugsanstalt war ein Raum nicht verschlossen, in dem sich u.a. alte „Wahrnehmungsbogen", also Berichte von Vollzugsbeamten zu bestimmten Vorkommnissen bei Gefangenen, und Akten mit Sozialgutachten befanden. So konnten sich Gefangene diese Unterlagen unkontrolliert beschaffen. Die Angelegenheit war seinerzeit Gegenstand einer Kleinen Anfrage im Landtag (vgl. X 32.2).

Obwohl ich aus diesem Grunde die ordnungsgemäße Aufbewahrung sensitiver Datensammlungen in allen Anstalten angemahnt und insbesondere verlangt hatte, solche Unterlagen vor dem Zugriff Unbefugter zu schützen, erreichte mich aus derselben Anstalt erneut eine Beschwerde darüber, daß personenbezogene Daten nicht datenschutzgerecht aufbewahrt wurden. In der Müllzelle einer Station dieser Anstalt hatte ein Gefangener mit anderen Strafgefangenen mehrere Schriftstücke gefunden, die Angaben über verschiedene Gefangene und verschiedene Maßnahmen enthielten (z. B. Kontostand, Anträge innerhalb des Vollzuges). U. a. befand sich bei den Schriftstücken eine längere Notiz mit diversen Angaben zur Person des Petenten und seiner Verlobten (Angabe zu bevorstehender Eheschließung, Staatsangehörigkeit der Verlobten usw.).

Meine datenschutzrechtliche Überprüfung der Angelegenheit ergab, daß ein Bediensteter der Justizvollzugsanstalt, der erst wenige Wochen dort beschäftigt war, in Unkenntnis über die Müllentsorgung und in vorweihnachtlicher Hektik es versäumt hatte, die Notizzettel in den Aktenvernichter zu geben. Beabsichtigt sei die Vernichtung der Notizzettel gewesen, nicht die Weitergabe an andere Personen. Aus datenschutzrechtlicher Sicht war diese Datenübermittlung unzulässig. Konsequenzen ergaben sich aus diesem Vorfall insoweit, daß durch eine Anstaltsverfügung nochmals darauf hingewiesen wurde, daß ausgesonderte Unterlagen der Vernichtung durch Aktenvernichter zugeführt werden müssen.

33. Öffentlich-rechtliche Religionsgesellschaften

Meinen Gedankenaustausch mit den kirchlichen Datenschutzbeauftragten über die Entwicklung der Datenverarbeitung und des Datenschutzrechts (vgl. X 33) habe ich während des Berichtszeitraumes in kollegialer Atmosphäre fortgeführt. Die Bischöfe der Bistümer Hildesheim, Osnabrück und des oldenburgischen Teils des Bistums Münster haben zum 1. Januar 1992 erstmalig einen gemeinsamen Datenschutzbeauftragten bestellt; Dienstsitz ist beim Katholischen Büro Niedersachsen in Hannover.

In den Gesprächen wurde deutlich, daß in bestimmten Bereichen die Notwendigkeit einer Überarbeitung der kirchenlichen Datenschutzvorschriften im Sinne einer Anpassung an den Standard der neuen Datenschutzgesetzgebung des Bundes und der Länder besteht. Dies gilt besonders für bereichsspezifische Regelungen, die für kirchenrechtliche Einrichtungen und solche unter kirch-

licher Trägerschaft erlassen wurden bzw. noch erlassen werden müssen. Der Datenschutzbeauftragte beim Katholischen Büro Niedersachsen kündigte an, daß die derzeit gültige, aus dem Jahr 1977 stammende Anordnung über den kirchlichen Datenschutz (KDO) Anfang 1993 in einer Fassung vorgelegt werde, die sich am Bundesdatenschutzgesetz von 1990 orientiert. Ich habe den Eindruck gewonnen, daß allseits guter Wille vorhanden ist, den Datenschutz im kirchlichen Bereich weiter zu verbessern.

In diesem Sinne bewerte ich auch eine Pressemeldung aus dem Monat August 1992, nach der der Präsident des Evangelisch-lutherischen Kirchenamtes in Hannover mitgeteilt hat, daß künftig Kirchenaustritte nicht mehr namentlich in den Gemeindebriefen veröffentlicht werden sollen. Gerade zu dieser Frage sowie zur Veröffentlichung von Jubiläumsdaten erreichen mich immer wieder Anfragen, die ich mangels Zuständigkeit an den hierfür zuständigen Beauftragten für den Datenschutz der betroffenen Kirchengliederung abgebe.

Im Frühjahr 1993 soll der Gedankenaustausch fortgesetzt werden — dabei soll auch der Vorschlag aufgegriffen werden, ein gemeinsames Gespräch mit den Beauftragten der evangelischen Kirche und der katholischen Kirche zu führen.

Datenschutz im nicht-öffentlichen Bereich

34. Zur Situation

34.1 Neu in der Obhut des LfD: Datenschutz im nicht-öffentlichen Bereich

Das neue Bundesdatenschutzgesetz (BDSG) vom 20. Dezember 1990, das am 1. Juni 1991 in Kraft getreten ist, hat für den nicht-öffentlichen Bereich zahlreiche Änderungen gebracht. Eine weitere wichtige Änderung ist durch Beschluß des Niedersächsischen Landesministeriums vom 20. Dezember 1991 eingetreten, der mich als zuständige Aufsichtsbehörde nach § 38 BDSG mit Wirkung vom 1. Januar 1992 an bestimmt (Nds. MBl. 1992 S. 230). Die vier niedersächsischen Bezirksregierungen wurden als Aufsichtsbehörde abgelöst (vgl. 3.2). Meine einjährigen Erfahrungen sind fast ausnahmslos positiv. So konnte ich die sehr unterschiedlichen Arbeitsweisen in der Registerführung und bei der Datenschutzkontrolle der vier Bezirksregierungen vereinheitlichen. Die langjährige Erfahrung aus dem öffentlichen Bereich konnte fruchtbar eingebracht werden. Trotz weiter Wege war eine Datenschutzkontrolle auch in den von meiner Geschäftsstelle weit entfernten Bereichen Niedersachsens möglich.

Bei der Durchführung von Kontrollen vor Ort werde ich — wie bislang die Bezirksregierungen — durch eine beim Niedersächsischen Landesverwaltungsamt eingerichtete Prüfgruppe unterstützt. Problematisch sind die geringe Verfügbarkeit der Prüfgruppe, die überwiegend für andere Aufgaben eingesetzt wird, und der hohe Abstimmungsaufwand. Dessenungeachtet möchte ich die Bereitschaft zur Zusammenarbeit bei der Behördenleitung und bei den Mitarbeitern hervorheben.

Ein Großteil der bislang angefallenen Arbeiten im nicht-öffentlichen Bereich diente der Einarbeitung in dieses neue Tätigkeitsgebiet und der Aufarbeitung aller Altunterlagen. Die Akten der Bezirksregierungen wurden nach Sichtung vor Ort fast vollständig in meine Geschäftsstelle übernommen. Alle zum Register gemeldeten Firmen (etwa 230) wurden von mir angeschrieben und auf die neue Kontrollzuständigkeit aufmerksam gemacht (vgl. 35.1). Der sie betreffende vorgefundene Registerinhalt wurde mit der Bitte um Überprüfung übersandt. Die schnellen Antworten und zahlreiche Informationsgespräche in meiner Geschäftsstelle und vor Ort belegen die begrüßenswerte Bereitschaft zur Zusammenarbeit. Die vielen Änderungsmeldungen zum Register haben aber auch den schlechten Zustand der übernommenen Unterlagen deutlich werden lassen.

Mein besonderes Anliegen wird es auch weiterhin sein, sowohl Eingaben von Bürgerinnen und Bürgern mit der notwendigen Aufmerksamkeit zügig zu bearbeiten als auch Kontrollen vor Ort im angemessenen Umfang durchzuführen.

34.2 Datenverarbeitung in der Wirtschaft: Nach wie vor ein schneller Wandel

Berichte über Absatzprobleme und Stellenkürzungen in renommierten Computerfirmen deuten scheinbar auf eine Abschwächung der stürmischen Entwicklung im IuK-Bereich hin. Meine Prüferfahrungen zeigen aber, daß die Entwicklung auch im nicht-öffentlichen Bereich ungebrochen weitergeht (vgl. 4.1). Allerdings hat die Wirtschaft gegenüber der öffentlichen Verwaltung

keinen Technologievorsprung, wie vielfach in der Verwaltung „befürchtet" wird. Auch in der Wirtschaft steigt die Ausstattung von Büroarbeitsplätzen mit Computern evolutionär, wächst die Informationsflut und wird zunehmend elektronische Kommunikation betrieben. „Downsizing" (Übergang zu kleineren Rechnereinheiten, vgl. 4.1) und Vernetzung sind bei vielen Wirtschaftsunternehmen anzutreffen. In einigen Bereichen der Wirtschaft werden zunehmend Rechnerleistungen für die Verarbeitung von Daten irgendwo in Deutschland oder Europa „gemietet" und auf einen vollständigen eigenen Rechnerpark verzichtet. Die eigentliche maschinelle Verarbeitung der Daten erfolgt dann in einem fast bedienerlosen Service-Rechenzentrum, dessen wenige Wartungsfachleute mit den eigentlichen Daten praktisch nicht mehr in Berührung kommen. Durch solche Auftragsformen erwachsen Probleme bei der Auslegung des BDSG.

Spezifisch für den nicht-öffentlichen Bereich sind neu eingeführte Abruf-Techniken, z. B. im Auskunfteiwesen, elektronische Kommunikation im Bankwesen und in der Kreditwirtschaft, Elektronische Zahlungsverfahren (EC-Cash), Videoüberwachung in Ladenzeilen, in Fußgängerpassagen, im Kassenraum von Banken und bei Bankautomaten oder die Einführung der Chip-Karten-Technologie.

Diese Techniken bringen neue Fragestellungen und Aufgaben für den Datenschutz mit sich. Sie erfordern vorausschauende Beobachtung, eine datenschutzrechtliche Bewertung und Vorschläge für einen datenschutzgerechten Umgang. Da mir auch im nicht-öffentlichen Bereich an präventivem Datenschutz gelegen ist, bin ich zu Beratungen bei der Erstellung von Datenschutz- und Datensicherungskonzepten bereit. Ich würde meine frühzeitige Beteiligung an Konzepten, Projekten und Versuchen sehr begrüßen.

35. Kontrolltätigkeit: Zahlen und Fakten

35.1 Datenverarbeitung als Dienstleistung: Meldepflicht nach § 32 BDSG

Das BDSG unterscheidet zwischen den Unternehmen, die Datenverarbeitung lediglich für eigene Zwecke durchführen, und denen, die personenbezogene Datenverarbeitung als Dienstleistung betreiben. Den ersteren wird eine weitreichende Eigenkontrolle in Datenschutzfragen übertragen, verkörpert durch den betrieblichen Datenschutzbeauftragten; nur bei „hinreichenden Anhaltspunkten" (§ 38 Abs. 1 BDSG) für eine Datenschutzverletzung wird die Aufsichtsbehörde tätig. Die EDV-Dienstleistungsunternehmen unterliegen neben der Eigenkontrolle zusätzlich meiner routinemäßigen Überwachung.

Nach § 32 BDSG sind die nicht-öffentlichen Stellen sowie ihre Zweigniederlassungen und unselbständigen Zweigstellen, die personenbezogene Daten geschäftsmäßig

— zum Zwecke der Übermittlung speichern,
— zum Zwecke der anonymisierten Übermittlung speichern oder
— im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen,

zu dem bei mir geführten Register meldepflichtig. Eine Speicherung zum Zweck der personenbezogenen Übermittlung erfolgt z. B. durch Auskunfteien und Adreßverlage. Markt- und Meinungsforschungsinstitute hingegen nehmen eine Speicherung zur anonymisierten Übermittlung vor. Eine Verarbei-

tung oder Nutzung von personenbezogenen Daten im Auftrag führen z. B. Service-Rechenzentren, Vernichtungs- und Mikroverfilmungsfirmen durch. Die Aufnahme und Beendigung einer meldepflichtigen Tätigkeit in Niedersachsen ist mir innerhalb eines Monats mitzuteilen.

Ich habe das Register nach § 32 BDSG mit Hilfe aller registrierten Firmen vollständig überarbeitet und in einer Datenbank automatisiert gespeichert (vgl. 34.1). Alle Firmen haben ihre aktuellen Datei-Ausdrucke erhalten. Seitdem erreichen mich häufig Schreiben von Firmen, die auf Änderungen der gemeldeten Daten hinweisen. Die im Gesetz festgelegte Mitteilungspflicht scheint somit besser als bisher befolgt zu werden.

Parallel zur Automatisierung des Registers wurde ein neues Meldeformular entwickelt, das eine schnelle und vollständige Übernahme der Meldedaten in das Register ermöglicht. Es erläutert auch den Meldeumfang zum Datum „Art der Datenverarbeitungsanlagen" (§ 32 Abs. 3 Nr. 1 BDSG), der nach § 32 Abs. 5 BDSG von mir genauer bestimmt werden kann. Ich halte folgende Angaben für erforderlich:

— Zentralrechner mit Typbezeichnung, Betriebssystem,
— andere größere selbständige Rechner, Workstations etc.,
— ungefähre Anzahl intelligenter Terminals, evtl. mit Typbezeichnung,
— ungefähre Anzahl der PC,
— Netzwerke mit Typbezeichnung,
— Datenfernübertragungsleitungen („DFÜ"; Typbezeichnung, z. B.: Datex-P),
— bei Mikroverfilmungs- oder Aktenvernichtungsfirmen: allgemeine Beschreibung ohne Typbezeichnung, z. B. „COM-Mikroverfilmungsgeräte", „Schredder".

Entbehrlich sind:
— Drucker, Lochkartenleser, Vorrechner, Steuereinheiten, Speicherungsgeräte usw.

Dieser neu festgelegte Umfang dient dazu, mir einen Überblick über Größe und Leistungsfähigkeit der jeweiligen Datenverarbeitung zu geben. Auch erhoffe ich mir, auf diese Weise Firmen in Zukunft gezielt auf Datensicherungsprobleme einzelner Hardware- oder Software-Komponenten hinweisen zu können. Außerdem geben mir die Angaben die Möglichkeit, Schwerpunkte bei Routineprüfungen zu setzen. Um jedoch den mit der Meldepflicht verbundenen Änderungsaufwand der Unternehmen niedrig zu halten, habe ich mich in vielen Punkten bewußt auf grobe bzw. ungefähre Angaben beschränkt. So sind auch die Fragen z. B. zum Betriebssystem oder Netzwerk-Typ gemeint. Es reicht die Bezeichnung „UNIX" oder „ Ethernet"; die Angabe der genauen Versionsnummer usw. ist nicht erforderlich, sie wird von mir unmittelbar vor einer Prüfung erfragt. Angaben zur Aktenvernichtung und Mikroverfilmung sind nur notwendig — wie die anderen Angaben auch —, soweit diese Tätigkeiten im Auftrage für Dritte durchgeführt werden.

Am 1. Dezember 1992 waren insgesamt 214 Firmen nach § 32 BDSG zum Register gemeldet. Im Laufe des Jahres 1992 wurden 33 Firmen, die teilweise schon längere Zeit keine meldepflichtige Tätigkeit mehr ausübten bzw. bereits nicht mehr existierten, gelöscht. Neu aufgenommen wurden 19 Firmen.

Größe und Geschäftszweck der gemeldeten Unternehmen variieren stark. Sie reichen von den großen EDV-Unternehmen für das Kreditwesen über mittelständische Unternehmen der unterschiedlichsten Branchen bis zum „Ein-Mann-" oder „Ein-Frau-Betrieb" am häuslichen PC. Abb. 1 zeigt die Grö-

ßenaufteilung der gemeldeten Firmen. Kleine Betriebe mit weniger als fünf Mitarbeitern und kleinen oder überhaupt keinen Datenverarbeitungsanlagen sind am häufigsten vertreten. Großbetriebe mit über 20 Mitarbeitern in der EDV bzw. mit Großrechenanlagen machen weniger als ein Viertel aus.

Abb. 1 Unterteilung der zum Register gemeldeten Firmen nach ihrer Größe.
Kleinbetriebe: weniger als 5 Mitarbeiter bzw. kleine DV-Anlagen.
Mittlere Betriebe: 5 bis 20 Mitarbeiter bzw. DV-Anlagen mittlerer Größe.
Großbetriebe: mehr als 20 Mitarbeiter bzw. Großrechenanlagen.

Von den insgesamt gemeldeten 214 Firmen
— speichern 30 Firmen personenbezogene Daten zum Zweck der Übermittlung (3 Adreßverlage und 27 Auskunfteien),
— beschäftigen sich 2 Firmen mit der Markt- und Meinungsforschung bzw. speichern personenbezogene Daten zum Zweck der anonymisierten Übermittlung,
— verarbeiten 182 Firmen personenbezogene Daten im Auftrag als Dienstleistungsunternehmen.

Am meisten vertreten sind Rechenzentren und Service-Rechenzentren, wobei hierzu auch Kleinbetriebe mit entsprechendem Geschäftsziel zählen (vgl. Abb. 2). Als Service-Rechenzentrum bezeichne ich dabei diejenigen Rechenzentren, die überwiegend Auftragsdatenverarbeitung betreiben. „Normale" Rechenzentren sind dagegen solche Unternehmen, die vorwiegend Datenverarbeitung für eigene Zwecke durchführen. Bei diesen macht der Anteil an Auftragsdatenverarbeitung oft nur wenige Prozent oder sogar Promille aus. Auffallend stark sind auch die Auskunfteien vertreten. Allerdings gehören oftmals mehrere Betriebe einer einzigen Vereinigung an. Die Vernichtungsunternehmen, in Abb. 2 als Aktenvernichter bezeichnet, sind zahlenmäßig schwach vertreten. Ich gehe davon aus, daß viele dieser Betriebe noch nicht gemeldet sind. Dies scheint daran zu liegen, daß die Aufnahme von Aktenvernichtern in das Register von den einzelnen Bezirksregierungen unterschiedlich gehandhabt wurde. Zum Teil wurden nur Betriebe registriert, die in der Lage

waren, Disketten, Platten oder Bänder mit Spezialgeräten zu vernichten. Fest steht aber, daß auch Aktenvernichter, die lediglich Computerausdrucke mit personenbezogenen Daten im Auftrage Dritter vernichten, meldepflichtig sind.

Abb. 2 Aufteilung der gemeldeten Firmen nach Betriebsarten (Service-Rechenzentren: überwiegend Auftragsdatenverarbeitung; Rechenzentren: überwiegend Datenverarbeitung für eigene Zwecke)

Auch in anderen Bereichen ist eine nicht unerhebliche Dunkelziffer zu vermuten. Viele Firmen sind sich nicht darüber im klaren, daß sie eine meldepflichtige Tätigkeit ausüben. Gelegentlich wird wohl auch ganz bewußt eine Meldung nach dem Motto: „Nur keine schlafenden Hunde wecken" unterlassen. Ein Schwerpunkt meiner Arbeit im nächsten Jahr wird daher sein, die Dunkelziffer der nicht gemeldeten Firmen zu reduzieren. Dabei ziehe ich auch in Betracht, daß nach § 44 Abs. 1 Nr. 2 BDSG für die Unterlassung der Meldung ein Bußgeld vorgesehen ist.

35.2 Kontrolle vor Ort

§ 38 BDSG regelt die Überwachung der nicht-öffentlichen Stellen durch die Aufsichtsbehörde. Es wird unterschieden zwischen „Anlaßprüfungen", also Prüfungen im Einzelfall beim Vorliegen hinreichender Anhaltspunkte (§ 38 Abs. 1 BDSG), und „Routineprüfungen", die ohne Anlaß bei meldepflichtigen Firmen durchgeführt werden können (§ 38 Abs. 2 BDSG).

Erfreulicherweise gab es im Jahr 1992 keinen Grund, Anlaßprüfungen mit einer umfangreichen Kontrolle vor Ort vornehmen zu müssen. Lediglich in drei Fällen mußten meine Mitarbeiter Firmen aufsuchen, um Anhaltspunkten in Informationsgesprächen nachzugehen.

Abb. 3 Aufteilung der in 1992 durchgeführten Prüfungen nach der Betriebsart. Zum Vergleich ist im unteren Teil des Bildes die entsprechende Aufteilung des Registers aufgeführt (vgl. Abb. 2).

1992 wurden von mir 21 Routineprüfungen vor Ort durchgeführt. Eine Aufteilung der Routineprüfungen nach Betriebsarten ist Abb. 3 zu entnehmen. Zum Vergleich sind die Aufsplittungen der zum Register gemeldeten Firmen (vgl. Abb. 2) im unteren Teil der Grafik mit aufgeführt. Wie aus dieser Abbildung ersichtlich, wurde die Prüftätigkeit auf nahezu alle Teilbereiche entsprechend der Häufigkeit im Register nach dem Motto „jeder kommt dran" verteilt. Service-Rechenzentren wurden überdurchschnittlich berücksichtigt, weil hier ein besonders hoher Anteil der Verarbeitung sensibler personenbezogener Daten zu vermuten ist.

Routineprüfungen im nicht-öffentlichen Bereich werden seit Inkrafttreten des alten Bundesdatenschutzgesetzes durchgeführt. Von den Bezirksregierungen wurde angestrebt, Prüfungen in regelmäßigen Abständen zu wiederholen. Abb. 4 zeigt, daß mittlerweile die Phase der zweiten Wiederholungsprüfung begonnen hat, 23 Firmen sind inzwischen drittgeprüft. Der größte Anteil an Firmen ist seit 1978 aber erst zweimal geprüft worden. Über ein Viertel aller Firmen war Anfang 1992 noch überhaupt nicht geprüft worden. Obwohl dies zum großen Teil Unternehmen sind, die erst vor kurzem zum Register gemeldet wurden, halte ich gerade diese Zahl für zu hoch. Die Prüftätigkeit im Jahr 1992 war vor allem darauf angelegt, die Zahl der Erstprüfungen zu verringern, was aus Abb. 4 b ersichtlich wird; es wurden aber auch Zweit- und Drittprüfungen bei wichtigen Firmen durchgeführt.

Abb. 4 Anzahl der Firmen im Register, die ungeprüft, erst-, zweit- oder drittgeprüft sind (Abb. 4a), sowie die Aufteilung der Prüfungen 1992 nach Erst-, Zweit- und Drittprüfung (Abb. 4 b).

Mit den im Jahr 1992 durchgeführten 21 Prüfungen ist bei der jetzigen Personalsituation die Grenze der Belastbarkeit erreicht. Berücksichtigt man die Gesamtzahl von 214 gemeldeten Firmen, so ergibt sich ein durchschnittlicher Zeitabstand zwischen zwei Prüfungen von etwa 10 Jahren, der wahrscheinlich noch wachsen wird, wenn die Dunkelziffer der nicht gemeldeten Firmen verringert werden kann. Dieser Prüfrhythmus ist leider viel größer, als die in den Verwaltungsvorschriften zum BDSG a. F. aufgeführten drei bis fünf Jahre.

Meine Prüferfahrungen zeigen, daß gerade kleine Unternehmen mit nur wenigen Mitarbeiterinnen und Mitarbeitern den Datenschutz — oft aus Unkenntnis — nicht genügend beachten. Andererseits bedeutet es einen überdurchschnittlich hohen Aufwand, Kleinbetriebe vor Ort zu prüfen. Diese Gegensätze haben meine Aufteilung von Prüfungen auf Klein-, Mittel- und Großbetriebe mitbestimmt (vgl. Abb. 5). Es wäre wünschenswert, auch kleinere Betriebe bei Kontrollen vor Ort entsprechend der Registeraufteilung zu berücksichtigen.

Abb. 5 Aufsplitterung der 1992 geprüften Firmen nach der Betriebsgröße. Zum Vergleich ist die entsprechende Aufteilung des Registers rechts mit aufgeführt (vgl. Abb. 1).

Die Prüfdauer bei den durchgeführten Kontrollen vor Ort betrug je nach Betriebsart und -größe zwischen zwei Stunden und zwei Tagen. Insbesondere folgende Mängel wurden während der Kontrollen festgestellt:

— Eingangstüren und Fenster zu sensiblen Bereichen waren oft schlecht abgesichert (Fenster nicht verschließbar, Notausgänge ungesichert). In einem Fall bestand die Eingangstür zu einer Auskunftei aus einer gewöhnlichen gläsernen „Wohnzimmertür".

— Der Zugang zu sensiblen Bereichen war oft auch organisatorisch mangelhaft gelöst (Schlüsselvergabe an unbeteiligte Mitarbeiterinnen und Mitarbeiter oder firmenfremde Personen, zu viele Generalschlüssel).

— Sicherungsdatenträger waren nicht sicher untergebracht bzw. nicht ausgelagert.

— Der Austausch von Datenträgern war nicht verbindlich geregelt.

— Der Zugriffsschutz auf Rechner mittels Paßwort war bei den meisten Stellen nicht ausreichend sicher (weniger als 6 Stellen, Vergabe durch die Systemverwaltung, keine Paßwort-Alterung). In einem Fall bestand das Systemverwalter-Paßwort nur aus drei Stellen, in einem anderen Fall bestand überhaupt kein Paßwortschutz.

— Bei Datenfernübertragungen mittels Wählleitung wurden keine Rückwählverfahren eingerichtet.

— Bestimmte Mitarbeiterinnen und Mitarbeiter, die Zugang zu sensiblen Datenbeständen haben, waren nicht auf das Datengeheimnis verpflichtet.

— Datenschutzbeauftragte zeigten zwar rechtliche Kenntnisse, aber keine EDV-Fachkunde.

— Registereintragungen zu § 32 BDSG waren des öfteren unkorrekt.

Insbesondere mangelhafte Paßwortregelungen wurden immer wieder festgestellt (vgl. 4.9). Gerade diesen Punkt werde ich im Jahr 1993 noch intensiver verfolgen.

Die Firmen wurden von mir aufgefordert, die bei den Kontrollen aufgezeigten Mängel zu beseitigen. Ich überwache in jedem Fall die Erledigung meiner Forderungen und Empfehlungen. Die entsprechenden Prüfvorgänge sind zum größten Teil noch nicht abgeschlossen. Anordnungen oder Bußgeldverfahren wurden bisher nicht eingeleitet.

35.3 Anfragen und Beschwerden

Nach Übernahme der Zuständigkeit für die Überwachung des Datenschutzes im nicht-öffentlichen Bereich wurden in der Zeit vom 1. Januar 1992 bis zum 31. Dezember 1992 insgesamt 78 Anfragen und Beschwerden bearbeitet. Die meisten Vorgänge betrafen die Bereiche Auskunfteien, Arbeitnehmerdatenschutz, Banken und Sparkassen sowie Versicherungen. Im einzelnen ergab sich folgende Verteilung:

Bereich	Anzahl
Adreßverlage, Adreßhandel	4
Arbeitnehmerdatenschutz	10
Auskunfteien	16
Banken und Sparkassen	9
Bausparkassen	2
Fahrschulen	1
Kinder-/Jugendhilfeeinrichtungen	1
Krankenhäuser	2
Markt- und Meinungsforschungsinstitute	1
Medizinische Heil- und Hilfsberufe	1
Mieter-/Vermieterorganisationen, Wohnungswirtschaft	7
Privatverrechnungsstellen	1
Rechtsanwälte	1
Sicherheitsdienste	1
Telefondatenerfassung	2
Vereine, Verbände	2
Versicherungen	10
Video	1
Volkshochschulen, Bildungseinrichtungen	1
Werbung für eigene Zwecke	3
Wohlfahrtsverbände	1
Zeitungs- und Zeitschriftenverlage	1

36. Datenschutzprobleme in Einzelbereichen

36.1 Werbepapierflut im Briefkasten: Direktwerbung und Datenschutz

Viele ärgern sich, daß Mengen von Werbematerial ihren Briefkasten überquellen lassen und sich die Privatpost darin verliert. Das beweisen eine ganze Reihe von Anfragen und Beschwerden an mich.

Ärger mit Werbung im Briefkasten ist dann ein Datenschutz-Thema, wenn mit Adressen oder persönlichen Anschreiben geworben wird. Viele beschleicht ein ungutes Gefühl, wenn sie von einer unbekannten Firma ein persönlich adressiertes Werbeschreiben erhalten: „Wie kommen die an meine Daten?" Viel Ärger könnte vermieden werden, wenn sich Adreßverlage und werbende Firmen dazu durchringen könnten, in Werbebriefen Hinweise auf die Herkunft der aufgeführten persönlichen Daten zu geben. In vielen Fällen sind solche Briefe nur ärgerlich, gelegentlich können aber auch massive Probleme entstehen, z. B. wenn angeschriebene Personen zu leichtgläubig auf den Inhalt der Briefe reagieren.

Die bei mir eingehenden Anfragen und Beschwerden sind sicherlich nur die Spitze eines massiven Eisbergs; vielfach unterbleibt wohl eine an mich gerichtete Bitte um Unterstützung. Oft ist auch nicht bekannt, daß Betroffene unmittelbar selbst gegen die Werbeflut im Briefkasten vorgehen können. Gelegentlich scheinen selbst werbende Unternehmen nicht auf dem laufenden zu sein. Aus diesem Grund bereite ich z.Zt. ein Merkblatt vor, in dem Hinweise zum Thema Direktwerbung und Datenschutz gegeben werden. Als besonders wichtige Hinweise seien bereits hier genannt:

— Nach § 34 BDSG besteht ein — freilich zu enger — Auskunftsanspruch über die zur eigenen Person gespeicherten Daten. Dabei sollte man allerdings berücksichtigen, daß in vielen Fällen nicht die Firma selbst die Adreßdaten speichert, sondern diese von Adreßverlagen oder anderen werbenden Firmen „gemietet" hat. Oftmals ist daher ein Durchfragen über mehrere Stellen notwendig, um die gewünschte und gesetzlich zustehende Auskunft zu erhalten.

— In § 28 Abs. 3 BDSG ist ausdrücklich ein Nutzungsverbot für Werbezwecke bei erklärtem Widerspruch durch den Betroffenen festgeschrieben: „Widerspricht der Betroffene bei der speichernden Stelle der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- und Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig."

— Viele Direktwerbungsunternehmen richten sich nach der sog. „Robinsonliste" des Deutschen Direkt-Marketing-Verbands. In diese Liste können sich diejenigen eintragen lassen, die keine Direktwerbung wünschen. Hierfür ist eine neue Adresse eingerichtet worden:

  DDV, Robinsonliste, Postfach 1401, 7257 Ditzingen

  Ein entsprechender Eintrag kann neuerdings auch telefonisch (Anrufbeantworter) erfolgen unter der Nummer: (0 71 56) 95 10 10

— Neben diesen „offiziellen" Punkten gibt es noch Tips und Tricks, mit denen der Werbepapierflut begegnet werden kann. So sollte man auf Zusatzangaben im Telefonbuch verzichten, da diese eine der wichtigsten Quellen der Adreßverlage sind. Natürlich werden oft auch Antworten auf Werbebriefe — teilweise getarnt als Preisausschreiben — für die Bestimmung

des Konsumverhaltens und die Einordnung in eine entsprechende Adreßdatei verwendet. Solche Reaktionen auf Werbebriefe sollten deshalb gut überlegt sein. Um den Quellen von Werbebriefadressen auf die Spur zu kommen, kann man in den Fällen, in denen die Angabe der eigenen Adresse notwendig ist, auch leichte Variationen an den Angaben vornehmen und darauf achten, wo diese leicht variierten Daten wieder auftauchen.

— Auch gegen unadressiert verteiltes Werbematerial kann man vorgehen. Ist auf dem Briefkasten ein Aufkleber „keine Werbung bitte" oder „Werbung einwerfen verboten" angebracht, so müssen sich Verteilerinnen und Verteiler von Werbematerial daran halten.

36.2 Bitte mehr Sorgfalt: Übermittlungen durch Auskunfteien

1992 erhielt ich 16 Beschwerden von Betroffenen, die die Praxis von niedersächsischen Auskunfteien kritisierten. Die Institution Auskunftei oder die Art und Weise der Datenerhebung wurde dabei nicht angezweifelt, vielmehr der Inhalt von Eintragungen zur eigenen Person, der ja durch das Recht auf Eigenauskunft für Betroffene zugänglich ist. Meine Untersuchungen ergaben, daß die Kritik an unkorrekten Angaben zumeist zu Recht bestand. Der Wettbewerb mit niedrigen Auskunftspreisen läßt offenbar nur eine flüchtige Recherche zu. Oft lassen sich Auskunfteien auch auf subjektive und damit aus Datenschutzsicht bedenkliche Aussagen ein.

Interventionen von mir halfen in vielen Fällen schnell weiter. Dennoch muß ich fordern, daß die Datenerhebung, -speicherung und -übermittlung durch Auskunfteien bzw. ihnen zuarbeitende Unternehmen mit größerer Korrektheit als bisher vorgenommen werden, um berechtigte Kritik an den gespeicherten Daten gar nicht erst aufkommen zu lassen. Das müßte auch für die Unternehmen wirtschaftlicher als zeitaufwendige Nachuntersuchungen und Berichtigungen sein.

36.3 SCHUFA: ein Informationssystem der kreditgebenden Wirtschaft

36.3.1 SCHUFA-Verfahren und SCHUFA-Klausel

Die SCHUFA beschreibt sich selbst als Schutzgemeinschaft für allgemeine Kreditsicherung. Es ist eine Gemeinschaftseinrichtung der kreditgebenden deutschen Wirtschaft; Gesellschafter sind Banken, Sparkassen, Volksbanken und Raiffeisenbanken und Ratenkreditbanken. Vertragspartner der SCHUFA sind Kreditinstitute, Leasinggesellschaften, Einzelhandelsunternehmen einschließlich des Versandhandels, Kreditkartengesellschaften und sonstige Unternehmen, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben. Konsumenten in diesem Sinne sind natürliche Personen, die Kredite für private, nicht aber für berufliche oder gewerbliche Zwecke aufnehmen.

Die SCHUFA unterscheidet bei der Zusammenarbeit mit Vertragspartnern das:

A-Verfahren: Es berechtigt zur uneingeschränkten Auskunft und verpflichtet umgekehrt zur uneingeschränkten Meldung.

B-Verfahren: Es berechtigt nur zur Auskunft über Negativmerkmale (z. B. fruchtlose Pfändung, Lohn- und Gehaltspfändung, Wechselprotest, uneinbringliche ausgeklagte Forderung, erlassener Vollstreckungsbescheid, Zwangsvollstreckung). Es verpflichtet zur Meldung dieser auch als „harte" Negativmerkmale bezeichneten Informationen.

Ein einschneidendes Ereignis für das SCHUFA-Verfahren war das Urteil des Bundesgerichtshofs vom 19. September 1985 (NJW 1986, 46). Das Urteil hat neben der Neufassung der SCHUFA-Klausel eine ganze Reihe von Verbesserungen für den Datenschutz der Betroffenen gebracht:

— Die Zahl der SCHUFA-Vertragspartner wurden durch Kündigung bestehender Verträge deutlich reduziert (Wohnungsunternehmen, Makler, Bauträger, Automatenhändler, Brauereien und Getränkegroßhandel sowie Dienstleistungsunternehmen wie Lesezirkel und Fernschulen).
— Die Informationen der Kunden wurde verbessert (das SCHUFA-Merkblatt enthält umfangreiche Erläuterungen des gesamten Auskunftsverfahrens; es wird auf Wunsch den Kunden ausgehändigt).
— Aus dem Merkmals-Katalog der an die SCHUFA zu meldenden Angaben wurden solche gestrichen, die einseitige Maßnahmen der Banken und Sparkassen gegen ihre Kunden betreffen, z. B. „Klageerhebung", „letzte außergerichtliche Mahnung".
— Die Betroffenen erhalten jetzt von der SCHUFA bei einer Eigenauskunft neben den Angaben, die zur Person gespeichert werden, auch Angaben, wer diese Daten übermittelt hat, und den Hinweis, wer in den letzten Monaten eine Anfrage an die SCHUFA gerichtet und wer eine Auskunft erhalten hat.
— Die SCHUFA-Vertragspartner sind jetzt zur Nachmeldung verpflichtet, wenn die oder der Betroffene Widerspruch gegen einen Mahnbescheid eingelegt hat.
— Vor der Übermittlung „weicher" Negativmerkmale (z. B. Klageerhebung, beantragter Mahnbescheid) an die SCHUFA unterrichtet der SCHUFA-Vertragspartner seinen Kunden über die Übermittlungsabsicht. Der Kunde erhält die Möglichkeit, notfalls dagegen vorzugehen, um so die eigenen Belange noch vor der Meldung an die SCHUFA geltend zu machen.
— Die SCHUFA-Vertragspartner müssen vor der Übermittlung an die SCHUFA eine Abwägung zwischen den Belangen des Kreditnehmers und den Interessen der speichernden Stelle und der angeschlossenen Kreditgeber in jedem Einzelfall vornehmen.
— Die SCHUFA löscht Negativ-Merkmale am Ende des dritten vollen, auf die Einspeicherung folgenden Kalenderjahres.

Das neue SCHUFA-Verfahren und die neue SCHUFA-Klausel sind am 1. Juli 1986 eingeführt worden. Alle Kreditinstitute haben ihre Alt-Kunden, mit denen sie schon Geschäftsbeziehungen unterhielten, mit individuellen Schreiben oder in Mitteilungsblättern über die neuen SCHUFA-Klauseln und das neue Auskunftsverfahren unterrichtet. Durch diese Information wurde den Kunden Gelegenheit zum Widerspruch gegen die Datenübermittlung an die SCHUFA gegeben. Den Kunden wurde mitgeteilt, das Kreditinstitut werde vom Einverständnis mit dem neuen Verfahren ausgehen, wenn sie nicht ausdrücklich widersprächen.

Mehr als sechs Jahre nach dem BGH-Urteil erhalte ich noch immer Anfragen und Beschwerden von Bürgerinnen und Bürgern, die nicht verstehen können, daß sie noch immer in SCHUFA-Dateien gespeichert sind, obwohl sie die neue SCHUFA-Klausel nicht unterschrieben hätten. Sie verlangen deshalb, aus den SCHUFA-Dateien mit allen Alt-Eintragungen gelöscht zu werden. In sämtlichen Beschwerdefällen wurde mir von den kritisierten Kreditgebern dar-

gelegt, daß vor jeder SCHUFA-Meldung eine Interessenabwägung der schutzwürdigen Schuldner-Belange und der berechtigten Interessen der Kreditwirtschaft vorgenommen werde und dies in den konkreten Fällen auch geschehen sei. Der Nachweis, daß ein Unterrichtungschreiben den Alt-Kunden zugegangen war, konnte nur allgemein geführt werden. Wohl konnte belegt werden, daß Informationsblätter an alle Kunden versandt worden waren. In keinem Beschwerdefall lag ein belegbarer Widerspruch gegen die neue SCHUFA-Klausel vor. Somit hatte ich keine Möglichkeit, die Konsequenzen eines Widerspruchs im Einzelfall überprüfen zu können.

Nach einem Jahr Prüferfahrung kann ich feststellen, daß — gemessen am großen SCHUFA-Datenbestand und bei 1,7 Mio. Auskünften pro Jahr durch die SCHUFA Hannover — die Zahl von sieben Beschwerden sehr gering war. Der Geschäftsführer der SCHUFA Hannover hat mich bei der Aufklärung der Beschwerde-Vorgänge in vorbildlicher Weise unterstützt. Auch auf meine allgemeinen Fragen erhielt ich stets umgehend Antwort.

36.3.2 SCHUFA-Auslandskonzept

Die SCHUFA hat für die Übermittlung personenbezogener Daten an ausländische Kreditinstitute ein Auslandskonzept entwickelt. Der ausländische Vertragspartner der SCHUFA schließt mit der zuständigen SCHUFA-Gesellschaft einen Vertrag zu Gunsten Dritter. Der zukünftige Kunde des ausländischen Kreditinstituts erhält so vertraglich einen Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Beurteilungsmaßstab für die Zulässigkeit von Speicherung und Übermittlung ist das Bundesdatenschutzgesetz. Der Rahmenvertrag enthält zudem eine allgemeine Verpflichtung des Vertragspartners, die Grundsätze des „Übereinkommens zum Schutze des Menschen bei der automatischen Verarbeitung personenbezogener Daten" des Europarates vom 28. Januar 1981 einzuhalten.

Nach Auskunft der SCHUFA Hannover gibt es einige wenige Verträge mit Kreditinstituten in den Niederlanden und in Österreich. Probleme seien nicht bekannt geworden.

36.3.3 Eigen-Auskünfte aus SCHUFA-Dateien

Die SCHUFA-Gesellschaften haben im ersten Halbjahr 1992 bundesweit insgesamt rund 10,8 Mio. Einzelauskünfte erteilt; davon waren 174.000 Eigenauskünfte nach § 34 BDSG. Bei einer Anlaß-Überprüfung der SCHUFA Hannover hat sich die Kritik eines Bürgers bestätigt, daß ihm bei der Eigen-Auskunft nach § 34 BDSG nicht alle über ihn gespeicherten Daten mitgeteilt worden waren. Bei der sogenannten „Norm-Auskunft" wurden dem Betroffenen die Datumsangaben zum Girokonto und Voranschriften nicht mitgeteilt. Die SCHUFA begründete die verkürzte Auskunft damit, daß einerseits schutzwürdige Belange des Betroffenen nicht verletzt seien und andererseits der Betroffene jederzeit Gelegenheit habe, die Girodaten bei seinem kontoführenden Institut in Erfahrung zu bringen. § 34 BDSG läßt für eine derartige Einschränkung keinen Raum. Vielmehr erstreckt sich das Auskunftsrecht auf alle zur Person der Betroffenen oder des Betroffenen gespeicherten Daten. Das Auskunftsrecht umfaßt selbst gesperrte Daten, da auch diese gespeichert sind. Ziel der Selbstauskunftsregelung des § 34 BDSG ist es primär, der Betroffenen oder dem Betroffenen eine Möglichkeit zu geben, die Richtigkeit der gespeicherten Daten zu überprüfen. Das praktizierte Norm-Auskunftsverfahren der SCHUFA-Organisation erfüllt diesen Zweck nicht hinreichend und ist deshalb mit § 34 BDSG nicht vereinbar. Ich habe die SCHUFA Hannover aufgefor-

dert, das Auskunftsverfahren zu ändern und auskunftsbegehrende Bürgerinnen und Bürger umfassend über alle ihre Daten zu informieren. Weiter habe ich eine bundesweite Abstimmung der Aufsichtsbehörden initiiert.

36.3.4 Überprüfung des berechtigten Interesses nach SCHUFA-Anfragen

Nach § 29 Abs. 2 Nr. 1 a) BDSG hat der Empfänger von Daten, die geschäftsmäßig zum Zwecke der Übermittlung gespeichert werden, ein „berechtigtes Interesse" an ihrer Kenntnis glaubhaft darzulegen. Die Gründe für das Vorliegen eines „berechtigten Interesses" und die Art und Weise ihrer glaubhaften Darlegung sind von der übermittelnden Stelle aufzuzeichnen. Daraus leite ich die Pflicht ab, dies zumindest stichprobenweise zu überprüfen. Die Pflicht zur Überprüfung setzt nicht erst dann ein, wenn sich Betroffene beschweren, noch wird die Prüfungspflicht dadurch ersetzt, daß die SCHUFA weitere Meldungen von Vertragspartnern entgegennimmt und dies pauschal als „Bestätigung" der Rechtmäßigkeit der Anfragen wertet. Die Praxis der SCHUFA, lediglich 10 Stichproben im Monat durchzuführen, kann nicht als ausreichende Kontrolle hingenommen werden; darin sind sich alle Aufsichtsbehörden bundesweit einig. Sie fordern eine Erhöhung der Quote auf 1 0/00. Der Ansicht der SCHUFA, daß bei Online-Auskünften ihrer Vertragspartner keine Stichproben durchzuführen wären, muß ebenfalls widersprochen werden. Hier gilt § 10 Abs. 4 Satz 3 BDSG. Auch wenn dort nicht mit der wünschenswerten Klarheit gesagt ist, daß stichprobenweise Überprüfungen durchzuführen sind und wer die Stichproben durchzuführen hat, so ist nach meiner Auffassung hierfür die SCHUFA verantwortlich. Andernfalls würde die Ungleichheit entstehen, daß die immer weniger werdenden konventionellen Einzelauskünfte überprüft, das Massengeschäft der Online-Abfragen ohne direkte Kenntnisnahme der SCHUFA jedoch ungeprüft bliebe.

36.3.5 Unzulässige Weitergabe einer SCHUFA-Auskunft

In einem Fall ist mir bekannt geworden, daß eine unzulässige SCHUFA-Auskunft erteilt worden war. Über eine Freundschaftswerbung sollte ein Mitglied eines Buch-Clubs geworben werden. Die anwerbende Vertriebsfirma versprach, die Freundschaftswerbeprämie dem Neumitglied zukommen zu lassen. Ihr wäre dann ein Pachtzins gekoppelt am Umsatz des Mitgliedes zugefallen. Dafür hätte sie jedoch die Aufnahmekosten tragen müssen. Da jedoch Zweifel an der Bonität des Neumitgliedes bestanden, bat der Werber den Buch-Club um Vermittlung einer ihm nicht selbst zustehenden SCHUFA-Auskunft. Die SCHUFA-Auskunft wurde dem Werber unzulässigerweise übermittelt und in einer anderen Vertragsangelegenheit verwendet. Der Buch-Club bedauerte das „einmalige" Versehen und erklärte, daß SCHUFA-Auskünfte grundsätzlich nur dann eingeholt würden, wenn hinreichende Anhaltspunkte vorlägen, die Zweifel an der Bonität eines Neumitgliedes rechtfertigen. Vertriebsfirmen erhielten lediglich bei Negativ-Informationen die Mitteilung, daß eine Clubmitgliedschaft nicht in Frage komme. Die Ablehnung müsse den Vertriebsfirmen mitgeteilt werden, da ihnen im Falle der erfolgreichen Mitgliedschaft der Pachtzins zustehe.

36.4 Videoüberwachung bei Bankautomaten

Die Technisierung schreitet besonders im Bereich der Banken und Sparkassen schnell voran. Eine der neueren Errungenschaften sind die Bankautomaten, an denen liquide Kunden mit Hilfe einer Scheckkarte auch außerhalb der Geschäftszeiten etwas gegen die Ebbe im Geldbeutel tun können. Nicht nur das

Vergessen der „Persönlichen-Identitäts-Nummer (PIN)" läßt dabei neue Probleme entstehen. Mißbrauch mit gestohlenen Karten oder Vandalismus in den Geldausgaberäumen sind bittere Erkenntnisse der Betreiber. Was liegt da näher, als gegen diesen Mißbrauch und Vandalismus mit Videoüberwachungsanlagen vorzugehen?

Doch Vorsicht! Mit der Videoüberwachung kann auch weit über das eigentliche Ziel hinausgeschossen werden (vgl. 12.5). Videoaufzeichnungen bei Bankautomaten lassen umfangreiche personenbezogene Bilddateien entstehen, die zusammen mit den Buchungsvorgängen personenbezogen ausgewertet werden können. „Was wird gespeichert?", „Wer erhält diese Aufnahmen?", „Was geschieht mit den Aufzeichnungen?", „Wer wertet aus und kontrolliert?", das sind die Datenschutzfragen dieser Überwachungstechnik.

Um diese und andere Probleme bei Videoaufnahmen zu klären, habe ich mich mit einer Umfrage an eine Auswahl hannoverscher Banken und Sparkassen gewandt. Es wurden 27 Kreditinstitute angeschrieben und um Ausfüllung eines Fragebogens gebeten, der allgemeine Fragen zur Videoüberwachung, Fragen zu baulichen Maßnahmen, zum Aufzeichnungsverfahren und zur Organisation enthält.

22 Unternehmen haben geantwortet; davon hatten 5 Firmen Videoanlagen im Zusammenhang mit Bankautomaten installiert. Diese relativ geringe Zahl erklärt sich daher, daß die meisten angeschriebenen Banken oder Sparkassen noch keine Bankautomaten besitzen. Da angenommen werden kann, daß sich die Anzahl an Bankautomaten erhöhen wird, wird die Zahl der Videoüberwachungsanlagen bei Bankautomaten bald zunehmen.

In einigen Punkten variieren Aufbau und Verfahren der Videoüberwachung stark. So sind die Kameras im Bankautomatenraum mal sichtbar, mal versteckt aufgestellt. Der Hinweis auf die Videoaufnahme ist nicht generell vorhanden. Im Grundprinzip sind sich die Techniken aber sehr ähnlich. Ohne Ausnahme werden die Aufnahmen aufgezeichnet; hierfür wird jeweils ein weitgehend handelsüblicher Videorecorder verwendet. Es werden Zeitrafferaufnahmen durchgeführt. Eine Zuordnung der aufgenommenen Personen zu den Belegen der Bankautomaten erfolgt über Datum und Uhrzeit auf dem Videofilm. Da diese Angaben auch auf den Protokollen der Bankautomaten vorhanden sind, besteht eine direkte Auswertbarkeit. Diese Videoaufzeichnungen sind personenbezogene Dateien im Sinne des § 3 BDSG; die Bestimmungen des BDSG sind anzuwenden.

Nach § 28 Abs. 1 Satz 1 Nr. 2 ist das Speichern und Nutzen der Videoaufnahmen zulässig, soweit es zur Wahrung berechtigter Interessen der Banken und Sparkassen erforderlich ist und kein Grund zur Annahme besteht, daß das schutzwürdige Interesse der Betroffenen an dem Ausschluß der Verarbeitung oder Nutzung überwiegt. Aus dem Erforderlichkeitsgrundsatz folgt, daß Videofilme nur im Bedarfsfall ausgewertet werden dürfen. Das Umfrageergebnis belegt, daß dies von den befragten Unternehmen so gehandhabt wird. Unklar bleibt dabei allerdings, was als Bedarfsfall anzusehen ist.

Unterschiedlich ist die Auswertungspraxis. Sie erfolgt nämlich entweder direkt vor Ort, bei der Firmenzentrale oder bei der Polizei. Problematisch im Zusammenhang mit der Auswertung ist, daß es bei der jetzigen Technik praktisch unumgänglich ist, daß auch Bilder von unbeteiligten Personen auf der Suche nach dem richtigen Bild eingesehen werden.

Nach § 28 Abs. 1 Satz 2 BDSG müssen die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Ich leite daraus die Verpflichtung ab, daß Kameras deutlich sichtbar angebracht werden müssen oder ein entsprechendes Hinweisschild auf die Überwachung notwendig ist.

Bei der Aufzeichnung und der Auswertung von Videoaufzeichnungen müssen technische und organisatorische Maßnahmen getroffen werden, die einen datenschutzgerechten Ablauf ermöglichen. Hierzu gehören angemessene bauliche Maßnahmen, schriftliche Dienst- oder Arbeitsanweisungen, eine verbindliche Regelung der Zuständigkeit für Betreuung, Wartung und Auswertung sowie eine Protokollierung von Aufzeichnung und Auswertung. Meine Umfrage hat gezeigt, daß noch gravierende Defizite bestehen. Eine ausreichende Dienstanweisung war nur in einem Fall vorhanden, Protokollierungen wurden nur teilweise vorgenommen, Hinweise auf die Videoaufzeichnungen waren nicht generell vorhanden.

Insgesamt bleibt also für die kommende Zeit noch einiges zu tun. Vor allem müssen die Banken und Sparkassen auf die notwendigen technischen und organisatorischen Maßnahmen hingewiesen werden. Deren Umsetzung bedarf der Überwachung.

36.5 Mietkataster

Das Gesetz zur Regelung der Miethöhe (MHG) fordert in § 2 vom Vermieter zur Begründung einer Mieterhöhung die Benennung von konkreten Vergleichsmieten. Kriterien für die Vergleichbarkeit von Wohnungen sind die Größe, Ausstattung, Beschaffenheit und Lage der Wohnung. Hierzu werden in verschiedenen Großstädten Mietkataster geführt, zu dem Mieter und Vermieter freiwillig Vergleichsdaten anliefern. In Hannover führt der Verein zur Ermittlung und Auskunftserteilung über die ortsüblichen Vergleichsmieten (MEA e. V.) ein solches Mietkataster.

Nach übereinstimmender Meinung der Datenschutzaufsichtsbehörden der Länder werden in Mietkatastern, in denen Angaben zur Lage, Größe, Ausstattung einer Wohnung und zur Miete enthalten sind, personenbezogene Daten von Mietern und Vermietern gespeichert, auch wenn deren Namen nicht festgehalten werden. Die Übermittlung der im Mietkataster enthaltenen Daten an Auskunftssuchende, z. B. zur Begründung von Mieterhöhungsverlangen, wird als Auskunfteitätigkeit im Sinne des § 29 BDSG angesehen. Sie ist nur zulässig, wenn der Empfänger ein berechtigtes Interesse an ihrer Kenntnis glaubhaft dargelegt hat und kein Grund zur Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Speicherung oder Veränderung seiner personenbezogenen Daten hat. Die Kenntnis von personenbeziehbaren Einzelangaben bedeutet in vielen Fällen das Eindringen in den privaten Lebensbereich, der einen besonderen Schutz genießt. Insbesondere und gerade durch die Möglichkeiten der automatisierten Datenverarbeitung erhöht sich die Betroffenheit der Mieter, deren Lebensverhältnisse jederzeit, beliebig und lückenlos offenbart werden können und die infolgedessen mit unverhältnismäßigen Belastungen rechnen müssen.

Entsprechend dieser Bewertung ist nach § 33 Abs. 1 BDSG die Mieterin oder der Mieter zumindest von der erstmaligen Übermittlung und der Art der übermittelten Daten zu benachrichtigen, sofern er nicht auf andere Weise Kenntnis von der Speicherung oder der Übermittlung seiner Daten erlangt hat. Bei Auskünften an Dritte sollten nach Auffassung der Datenschutzaufsichtsbehörden der Länder keine adressenbezogenen Daten über Vergleichsobjekte übermittelt werden. Es sollten lediglich die Vermieter, die die Daten über ein Vergleichsobjekt gemeldet haben, und allgemeine Merkmale der Vergleichsmietobjekte (z. B. Größe der Wohnung, Ausstattungsmerkmale der Wohnung, Qualität der Wohnlage, Stadtteil) mitgeteilt werden.

Ich habe den MEA e. V. über diese grundsätzliche Auffassung unterrichtet und um Information über das in Hannover praktizierte Verfahren gebeten. Der MEA e. V. hält die Weitergabe von adressenbezogenen Daten über Vergleichsobjekte im Hinblick auf die vom Bundesverfassungsgericht geforderte Identifizierbarkeit bzw. Auffindbarkeit der Vergleichswohnung für erforderlich. Ein auskunftssuchender Vermieter erhält z. Zt. folgende Daten:

— die Lage des Objekts nach Stadtteil, Straße und Hausnummer, die Lage innerhalb des Hauses (Stockwerk) und die Lage innerhalb der Etage,
— die Anzahl der zur Wohnung gehörenden Räume,
— die Wohnfläche sowie
— der Nettomietpreis pro Quadratmeter Wohnfläche.

Die Namen der Mietvertragspartner werden nicht mitgeteilt.

Der MEA e. V. versucht durch regelmäßige Informationen über seine Tätigkeit über den örtlichen Mieter- und Haus-, Wohnungs- und Grundbesitzerverein den Betroffenen von der Speicherung und Übermittlung Kenntnis zu geben. Außerdem hat er eine Klausel in die Erfassungsbögen zum Mietkataster und in die überwiegend von den Vermietern genutzten Mietverträge zur Speicherung und Übermittlung der Daten aufgenommen. Damit ist jedoch nicht sichergestellt, daß alle Betroffenen Kenntnis von der Speicherung der Daten über ihre Wohnung erhalten. Ich habe den MEA e. V. aufgefordert, in die Erhebungsbogen auch eine Einwilligungsklausel der bei der Erhebung nicht direkt beteiligten dritten Partei (Mieterin bzw. Mieter oder Vermieterin bzw. Vermieter) aufzunehmen, um so eine ausreichende Unterrichtung sicherzustellen.

36.6 Vereine

Mitglieder und Vorstände von Vereinen haben mich gefragt, ob Mitgliederdaten dem BDSG unterliegen und ob diese Daten automatisiert verarbeitet und genutzt werden dürfen, z.B. mit einem PC. Bei Beratungswünschen versuche ich, praktikable Vorschläge für die Umsetzung der rechtlichen sowie der technisch-organisatorischen Regelungen für den nicht-öffentlichen Bereich zu geben.

Anlagen

Entschließungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Anlage 1

Beschluß der Sonderkonferenz am 29. Januar 1991 zum Vorschlag der EG-Kommission für eine Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

I.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem „informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.

Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarates zum Datenschutz von 1980 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.

Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedsstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.

Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in „Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.

2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet: die Transparenz des Datenumgangs geht für den einzelnen verloren.

3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.

4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur „nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.

5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem „angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in Drittländer übersichtlich und praktikabel auszugestalten.

6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten" erfüllt — betrachtet man ihre Struktur, Aufgaben und Kompetenzen — diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser — aus den nationalen Datenschutzorganen zusammengesetzten — „Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der „Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der „Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.

7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.

Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.

Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

Anlage 2

Beschluß der 41. Konferenz am 8. März 1991 zu Telekommunikation und Datenschutz

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderungen des Datenschutzes, das „Grundrecht auf unbeobachtete Kommunikation" zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, „Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden — auch Arbeitgeber — auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das

Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle — durch die computergesteuerte Vermittlungstechnik entstehenden — Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur Erstellung eines Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von „Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen — zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen — müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5. Oktober 1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Art. 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung — schon aus Gründen der Normenklarheit — in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

Anlage 3

Entschließung der Konferenz vom 25. Juni 1991 — gegen die Stimme Bayerns — zum Bundesratsentwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität

Schon seit Jahren haben Datenschutzbeauftragte von Bund und Ländern eine angemessene gesetzliche Regelung zu den in die Freiheitsrechte der Bürger eingreifenden Strafverfolgungsmaßnahmen, wie der Rasterfahndung, des Einsatzes Verdeckter Ermittler und des Einsatzes besonderer technischen Observationsmittel gefordert. Sie bedauern, daß hierzu die Bundesregierung nicht schon längst einen Entwurf vorgelegt hat. Der Bundesrat mit seinem Ende April 1991 beschlossenen Gesetzentwurf wird diesem Anliegen ebenfalls nicht gerecht.

Zum Schutz der Persönlichkeitsrechte der Bürger wie im Interesse wirksamer Aufgabenerfüllung durch die Strafverfolgungsorgane bedarf es klarer Rechtsgrundlagen. Der Datenschutz stellt sich Bemühungen nicht entgegen, den zunehmenden Herausforderungen, denen die Bürger unseres Staates durch die organisierte Kriminalität, insbesondere durch die Drogenkriminalität ausgesetzt sind, in erforderlicher Weise zu begegnen. Über dieses Ziel schießt der Bundesratsentwurf aber hinaus. Zwar enthält der Entwurf gegenüber früheren Vorschlägen des Bundesrates insofern eine Verbesserung, als nunmehr die Rasterfahndung und der Einsatz Verdeckter Ermittler an einen Straftatenkatalog gebunden werden sollen. Es bestehen aber weiterhin Bedenken, daß schwerwiegende Eingriffe in die Privatsphäre, wie der Einsatz von Peilsendern, schon bei „Straftaten von erheblicher Bedeutung" möglich sind.

Mit diesem schwammigen Begriff statt eines präzisen Kataloges von Straftaten wird der Einsatz der geheimen Ermittlungsmethoden weit über den Bereich der organisierten Kriminalität hinaus ausgedehnt. Diese Mittel werden damit für sämtliche Straftaten außerhalb der Bagatell- und Kleinkriminalität verfügbar.

Nach dem Gesetzentwurf wären auch über völlig unbeteiligte Personen heimliche Bild- und Filmaufnahmen zulässig, wenn es „der Erforschung des Sachverhalts" oder der „Aufenthaltsermittlung des Täters" dient. Gegen unverdächtige Personen sollen Wanzen und Peilsender eingesetzt werden können, wenn eine „Verbindung" — was immer darunter verstanden werden soll — mit dem Täter vermutet wird.

Selbst in privaten Wohnungen sollen Gespräche, die im Beisein eines Verdeckten Ermittlers geführt werden, heimlich abgehört und aufgezeichnet werden.

Es ist außerdem problematisch, daß derart schwerwiegende Eingriffe wie der Einsatz Verdeckter Ermittler nach dem Gesetzentwurf nicht in allen Fällen vom Richter angeordnet werden müssen, sondern weitgehende Eilkompetenzen für Polizei und Staatsanwaltschaft vorgesehen sind.

Ein weiteres Problem liegt darin, daß durch den Einsatz geheimer Ermittlungsmethoden gewonnene Informationen in zu weitem Umfang für andere Zwecke verwendet werden können. Offen bleibt insbesondere, ob die gewonnenen Erkenntnisse der Polizei für eine jahrelange Speicherung zur vorbeugenden Straftatenbekämpfung überlassen werden dürfen. Dies sieht der Gesetzentwurf undifferenziert nicht nur für Tatverdächtige, sondern sogar für andere Personen wie Begleiter oder zufällig betroffene Dritte vor.

Die Datenschutzbeauftragten halten es deshalb für dringend geboten, daß Bundestag und Bundesrat im weiteren Gesetzgebungsverfahren diese Probleme aufgreifen und die — wiederholt geäußerten — datenschutzrechtlichen Vorschläge berücksichtigt werden. Die Stellungnahme der Bundesregierung zu dem Entwurf des Bundesrates sollte diese Bemühungen unterstützen.

Anlage 4

Entschließung der 42. Konferenz am 26./27. September 1991 zum Datenschutz im Recht des öffentlichen Dienstes

I.

Die Daten von Arbeitnehmern werden im Laufe ihres beruflichen Lebens in vielfältiger Weise vom Arbeitgeber verarbeitet. Allein schon im Hinblick auf die große Zahl der über Arbeitnehmer erhobenen Daten und mit Rücksicht auf die Abhängigkeit des Arbeitnehmers vom Arbeitgeber ist eine gesetzliche Regelung der Verarbeitung von Personaldaten zwingend erforderlich. Auch gegenüber Beamten und anderen im öffentlichen Dienst Tätigen kann die Verarbeitung ihrer Daten nicht allein auf die hergebrachten Grundsätze des Berufsbeamtentums gestützt oder in Verwaltungsvorschriften geregelt werden. Vielmehr ist eine gesetzliche Grundlage vonnöten. Sie muß um so konkreter sein, je tiefer in das Persönlichkeitsrecht der Betroffenen eingegriffen wird.

II.

In der Auseinandersetzung um das Recht des öffentlichen Dienstes beeinträchtigen zwei grundlegende Fehleinschätzungen eine angemessene Regelung des Datenschutzes. Es trifft nicht zu, daß die Kenntnis des Dienstherrn über seine Bediensteten alle persönlichen Lebensumstände vollständig und lückenlos umfassen muß. Es ist ferner unrichtig, daß gesetzliche Regelungen überflüssig sind, weil stets die Einwilligung der Betroffenen eingeholt werden kann.

Zum einen wäre es mit der Würde des Menschen unvereinbar, wollte man ihn in seiner ganzen Persönlichkeit registrieren. Zwar ist der Angehörige des öffentlichen Dienstes dem Staat gegenüber besonders eng verpflichtet; er bleibt aber auch gegenüber seinem Dienstherrn Grundrechtsträger: Auch seine personenbezogenen Daten dürfen nur erhoben und verarbeitet werden, soweit das für die Begründung und Abwicklung des Dienstverhältnisses erforderlich ist.

Zum anderen macht der Rückgriff auf die Einwilligung gesetzliche Regelungen keineswegs überflüssig. Zwar ist die Erhebung und Verarbeitung personenbezogener Daten mit Einwilligung des Betroffenen grundsätzlich auch dann zulässig, wenn eine gesetzliche Grundlage fehlt. Die Einwilligung wird jedoch zur Farce, wenn sie faktisch erzwungen wird, weil z. B. eine Bewerbung ohne Einwilligung nicht berücksichtigt wird. Soweit bestimmte Angaben verfügbar sein müssen, sind sie gesetzlich präzise vorzuschreiben, aber zugleich auf den erforderlichen Umfang zu begrenzen.

III.

Neben der Neuordnung des Personalaktenrechts bedürfen auch andere Teilbereiche des öffentlichen Dienstrechts der datenschutzgerechten gesetzlichen Regelung. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält insbesondere die Lösung folgender Probleme für vorrangig:

1. Bewerbung um Einstellung in den öffentlichen Dienst

   Es ist — für den Bewerber transparent — festzulegen,
   - welche personenbezogenen Informationen von ihm verlangt bzw. über ihn eingeholt, wie sie genutzt werden dürfen und wann sie zu löschen sind,
   - ob und unter welchen Voraussetzungen und in welchem Stadium des Verfahrens der Bewerber sich Tests, Untersuchungen und Überprüfungen zu unterziehen hat,

— ob und inwieweit private Institutionen daran mitwirken und welche vertraglichen Sicherungen zum Schutz personenbezogener Daten zu vereinbaren sind,
— daß die Daten jeweils erst zu dem Zeitpunkt, in dem sie für das Verfahren erforderlich werden, und mit dem geringstmöglichen Eingriff erhoben werden.

2. Sicherheitsüberprüfung

Es ist bereichsspezifisch gesetzlich festzulegen,
— wer im öffentlichen Dienst einer Sicherheitsüberprüfung unterzogen wird,
— welche personenbezogenen Daten dafür erhoben und verarbeitet werden,
— wie das Verfahren gestaltet wird, insbesondere welche Stellen mit welchen Befugnissen am Verfahren beteiligt sind, und unter welchen Voraussetzungen Sicherheitsbedenken anzunehmen sind,
— daß die im Rahmen der Sicherheitsüberprüfung erhobenen Daten grundsätzlich nur für diesen Zweck verwendet werden dürfen,
— daß der Betroffene über das Ergebnis der Sicherheitsüberprüfung zu unterrichten ist. (Auf ihre Forderungen zur Sicherheitsüberprüfung [Geheimschutzgesetz] in den Entschließungen vom 13. September 1985, 18. April 1986 und 22. März 1990 nimmt die Konferenz Bezug.)

3. Ärztliche Untersuchung

Es ist durch Gesetz oder ergänzende Rechtsverordnung festzulegen,
— unter welchen Voraussetzungen die ärztliche Untersuchung eines Bewerbers oder Bediensteten angeordnet werden kann,
— daß jede ärztliche Untersuchung einen präzisen Untersuchungsauftrag voraussetzt, der Anlaß und Gegenstand der Untersuchung möglichst exakt definiert und den Umfang der Untersuchung eingrenzt,
— wie das Arztgeheimnis und der Datenschutz sicherzustellen sind,
— wann und in welchem Umfang Versicherungen und früher behandelnde Ärzte über frühere Untersuchungen und Maßnahmen befragt werden und diese offenbaren dürfen,
— daß Ärzte und Versicherungen Daten nicht ohne Kenntnis des Betroffenen und nur mit Einwilligung des Bewerbers offenbaren dürfen,
— daß die Unterlagen der ärztlichen Untersuchungen nicht für andere Zwecke verwendet werden und nicht mit solchen vermengt werden dürfen, die anderen Zwecken dienen, und daß sie zu vernichten sind, sobald sie nicht mehr benötigt werden,
— daß der Arzt der personalverwaltenden Stelle nur das Endergebnis seiner Untersuchung und — soweit erforderlich — nur tätigkeitsbezogene Risiken mitzuteilen hat,
— daß dem Betroffenen ein Recht auf Einsicht in die beim Arzt verbliebenen Untersuchungsunterlagen zusteht.

4. Beihilfen

Gesetzlich festzulegen sind Grundlagen eines datenschutzgerechten Beihilfeverfahrens, insbesondere die Abschottung der Beihilfestelle, das Verbot automatisierter Speicherung von Diagnosedaten und anderen medizinischen Einzelangaben, die Zweckbindung der Daten sowie ein eigener Beihilfeanspruch der Angehörigen.

5. Personalinformationssysteme

Es muß dienstrechtlich gewährleistet sein, daß
— automatisierte Systeme zur Verarbeitung von Personaldaten zu unterschiedlichen Zwecken (z. B. Urlaubsdatei, Telefondatenerfassung, PC-Betriebsdaten) nicht zu umfassenden Persönlichkeitsprofilen verknüpft werden,
— alle vorgesehenen Auswertungen von Personaldaten in einer Übersicht, die dem Betroffenen zugänglich sein muß, zusammengefaßt werden,

— Kontrollen der Bediensteten mit Hilfe automatisierter Systeme unzulässig sind; Ausnahmen bedürfen einer gesetzlichen, insbesondere personalvertretungsrechtlichen Regelung.

IV.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die für das Personalrecht zuständigen Minister und den Gesetzgeber auf, die auf der Grundlage der Rechtsprechung des Bundesverfassungsgerichts verfassungsrechtlich notwendigen Vorschriften zu erlassen.

Anlage 5

Entschließung der 43. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 23./24. März 1992 in Stuttgart zum Arbeitnehmerdatenschutz

I.

Im Rahmen des Arbeitsverhältnisses werden personenbezogene Daten aus ganz unterschiedlichen Lebensbereichen des Arbeitnehmers erhoben und gespeichert. Diese Daten verwendet der Arbeitgeber nicht nur für eigene Zwecke. Aus dem Arbeitsverhältnis ergeben sich auch Auskunfts-, Bescheinigungs- und Meldepflichten, die der Arbeitgeber gegenüber öffentlichen Stellen zu erfüllen hat. Durch die Möglichkeit, im Arbeitsverhältnis anfallende personenbezogene Daten miteinander zu verknüpfen und sie — losgelöst vom Erhebungszweck — für andere Verwendungen zu nutzen, entstehen Gefahren für das Persönlichkeitsrecht des Arbeitnehmers. Mit der Intensität der Datenverarbeitung, insbesondere durch Personalinformationssysteme und digitale Telekommunikationsanlagen, nehmen die Kontroll- und Überwachungsmöglichkeiten des Arbeitgebers zu.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb bereits seit 1984 bereichsspezifische und präzise gesetzliche Bestimmungen zum Arbeitnehmerdatenschutz. Bundestag, Bundesrat und Bundesregierung haben ebenfalls eine Regelungsnotwendigkeit bejaht; gleichwohl stehen bundesgesetzliche Regelungen über den allgemeinen Arbeitnehmerdatenschutz immer noch aus.

Die Notwendigkeit zur gesetzlichen Regelung besteht unabhängig davon, ob Arbeitnehmerdaten in automatisierten Dateien, in Akten oder in sonstigen Unterlagen verarbeitet werden. Der erhöhten Gefährdung durch die automatisierte Datenverarbeitung ist durch spezifische Schutzvorschriften Rechnung zu tragen.

Angesichts der besonderen Abhängigkeit des Arbeitnehmers im Arbeitsverhältnis und während der Phase einer Bewerbung um einen Arbeitsplatz ist durch Gesetz zu untersagen, daß Rechte, die dem Arbeitnehmer nach einschlägigen Datenschutzvorschriften zustehen, durch Rechtsgeschäft, Tarifvertrag und Dienst- oder Betriebsvereinbarung ausgeschlossen werden. Außerdem ist durch Gesetz festzulegen, daß eine Einwilligung des Arbeitnehmers oder Bewerbers nur dann als Grundlage einer Datenerhebung, -verarbeitung oder -nutzung in Frage kommt, wenn die Freiwilligkeit der Einwilligung sichergestellt ist, also die Einwilligung ohne Furcht vor Nachteilen verweigert werden kann. Deshalb dürfen allein aufgrund einer Einwilligung z.B. keine Gesundheitszeugnisse, Ergebnisse von Genomanalysen u.ä. angefordert werden, wenn sie den Rahmen des Fragerechts des Arbeitgebers überschreiten.

II.

Die gesetzliche Ausgestaltung des Arbeitnehmerdatenschutzes muß insbesondere folgende Grundsätze beachten:

1. Die Datenerhebung muß grundsätzlich beim Arbeitnehmer erfolgen.

2. Der Arbeitgeber darf Daten des Arbeitnehmers — auch durch Befragen des Arbeitsnehmers oder Bewerbers — nur erheben, verarbeiten oder nutzen, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgesehen ist. Dabei ist der Grundsatz der Zweckbindung zu beachten. Auch ist zwischen der Bewerbungs- und Einstellungsphase zu unterscheiden.

3. Der Arbeitgeber darf Daten, die er aufgrund gesetzlicher Vorgaben für andere Stellen (z. B. Sozialversicherungsträger) erheben muß, nur für diesen Zweck verwenden.

4. Eine Datenauswertung und -verknüpfung, die zur Herstellung eines umfassenden Persönlichkeitsprofils des Arbeitnehmers führen kann, ist unzulässig.

5. Beurteilungen und Personalauswahlentscheidungen dürfen nicht allein auf Informationen gestützt werden, die unmittelbar durch automatisierte Datenverarbeitung gewonnen werden.

6. Notwendige Datenübermittlungen zwischen Arzt und Arbeitgeber sind eindeutig zu regeln. Dem Arbeitgeber darf grundsätzlich nur das Ergebnis der ärztlichen Untersuchung zugänglich gemacht werden. Darüber hinaus dürfen ihm — soweit erforderlich — nur tätigkeitsbezogene Risikofaktoren mitgeteilt werden. Medizinischen und psychologische Befunde sind getrennt von den übrigen Personalunterlagen aufzubewahren. Die Ergebnisse medizinischer oder psychologischer Untersuchungen und Tests des Beschäftigten dürfen automatisiert nur verarbeitet werden, wenn dies dem Schutz des Beschäftigten dient.

7. Dem Arbeitnehmer sind umfassende Auskunfts- und Einsichtsrechte in die Unterlagen einzuräumen, die sein Arbeitsverhältnis betreffen. Diese Rechte müssen sich auch auf Herkunft, Verarbeitungszwecke und Empfänger der Daten sowie die Art und Weise ihrer Auswertung erstrecken.

8. Dem Personal-/Betriebsrat muß ein Mitbestimmungsrecht bei der Einführung, Anwendung und der wesentlichen Änderung von automatisierten Dateien mit personenbezogenen Daten der Arbeitnehmer für Zwecke der Personalverwaltung zustehen. Das gilt auch bei sonstigen technischen Einrichtungen, mit denen das Verhalten und die Leistung der Beschäftigten überwacht werden kann.

9. Gesetzlich festzulegen ist, welche Daten der Arbeitnehmervertretung für ihre Aufgabenerfüllung zugänglich sein müssen und wie der Datenschutz bei der Verarbeitung von Arbeitnehmerdaten im Bereich der Arbeitnehmervertretung gewährleistet wird. Regelungsbedürftig ist auch das Verhältnis zwischen dem Personal-/Betriebsrat und dem behördlichen/betrieblichen Datenschutzbeauftragten.

10. Die Befugnis des Personal-/Betriebsrats, sich unmittelbar an die Datenschutzkontrollinstanzen zu wenden, ist gesetzlich klarzustellen.

11. Arbeitnehmerdaten dürfen nur dann ins Ausland übermittelt werden, wenn dort ein dem deutschen Recht vergleichbarer Datenschutzstandard gewährleistet ist oder wenn der Betroffene nach den oben genannten Grundsätzen (vgl. Abschnitt I Abs. 4) eingewilligt hat.

Anlage 6

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum Grundrecht auf Datenschutz vom 28. April 1992

1. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 ist allgemein anerkannt, daß die Grundrechte auch die Befugnis des einzelnen umfassen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu entscheiden. Die Datenschutzbeauftragten treten dafür ein, dieses Recht ausdrücklich im Grundgesetz zu verankern. Damit würde

   — für die Bürger deutlicher erkennbar, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte,
   — der wachsenden Bedeutung des Datenschutzes für das Funktonieren der freiheitlichen Demokratie Rechnung getragen und auf die negativen Erfahrungen der DDR-Geschichte reagiert,
   — der Grundrechtskatalog dem technologischen Wandel angepaßt und
   — die Konsequenz aus den positiven Erfahrungen gezogen, die in mehreren Ländern des Bundes und im Ausland mit ähnlichen Verfassungsbestimmungen gemacht wurden.

   Die Konferenz begrüßt deshalb die Vorstellungen, die in der Verfassungskommission des Bundesrates entwickelt worden sind.

   Die Datenschutzbeauftragten empfehlen der Gemeinsamen Verfassungskommission des Bundestages und Bundesrates im Zusammenhang mit Art. 1 und Art. 2 GG den nachfolgenden Text zur Beratung:

   „Jeder hat das Recht, über die Preisgabe und Verwendung seiner persönlichen Daten selbst zu bestimmen. Dazu gehört das Recht auf Auskunft und Einsicht in amtliche Unterlagen. Dieses Recht darf nur durch Gesetz oder aufgrund eines Gesetzes eingeschränkt werden, soweit überwiegende Interessen der Allgemeinheit es erfordern."

2. Darüber hinaus empfiehlt die Konferenz, die unabhängige Datenschutzkontrolle, die für die Verwirklichung des Grundrechts auf Datenschutz im Alltag von entscheidender Bedeutung ist, in der Verfassung zu verankern.

3. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält es zusätzlich für erforderlich, in die Verfassungsdiskussion folgende Punkte miteinzubeziehen, die sich aus der Entwicklung der Informationstechnik ergeben:
   — Stärkung der Grundrechte aus Art. 10 und 13 im Hinblick auf neue Überwachungstechniken,
   — Recht auf Zugang zu den Daten der Verwaltung (Aktenöffentlichkeit, Informationsfreiheit),
   — Instrumente zur Technikfolgenabschätzung.

Anlage 7

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuregelung des Asylverfahrens (BT-Drs. 12/2062) vom 28. April 1992

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält Änderungen des Gesetzentwurfs zur Neuregelung des Asylverfahrens für erforderlich, insbesondere der geplanten Regelungen

1. über die erkennungsdienstliche Behandlung von Asylbewerbern zur Sicherung der Identität (§ 16 Abs. 1) und
2. über die Nutzung der dabei gewonnenen erkennungsdienstlichen Unterlagen zur Strafverfolgung und zur Gefahrenabwehr (§ 16 Abs. 5).

Zu 1.:
Nach dem geltenden Recht sind Lichtbilder und Fingerabdrucke bei Asylbewerbern nur dann zu fertigen, wenn deren Identität nicht eindeutig bekannt ist. Demgegenüber sieht der Gesetzentwurf zur Neuregelung des Asylverfahrens vor, daß von sämtlichen Asylbewerbern — bis auf wenige Ausnahmen — Lichtbilder und Fingerabdrucke zu fertigen sind. Dies ist mit dem Verfassungsgrundsatz der Verhältnismäßigkeit nicht vereinbar:
Der Staat hat selbstverständlich das Recht zu wissen, mit wem er es zu tun hat. Jeder — gleichgültig ob Deutscher oder Ausländer — muß sich deshalb durch Dokumente ausweisen können; nur wenn Zweifel an der Identität bestehen, kommen erkennungsdienstliche Maßnahmen in Betracht. Dieser Grundsatz unserer Rechtsordnung muß auch im Rahmen der Neuregelung des Asylverfahrens beachtet werden. Nur wenn feststeht, daß die Identität eines hohen Anteils der Asylbewerber — also nicht bloß diejenige einzelner oder bestimmter Gruppen — zweifelhaft ist, wäre eine erkennungsdienstliche Behandlung aller Asylbewerber gerechtfertigt. Gerade dies aber ist bisher nicht hinreichend belegt: In der amtlichen Begründung des Gesetzentwurfs ist allein davon die Rede, daß nach Feststellung niederländischer Behörden 20 % der Asylbewerber unter falschem Namen einen weiteren Asylantrag stellen. Aussagekräftige Angaben, in welchem Umfang in der Bundesrepublik Deutschland Asylbewerber unter Täuschung über ihre Identität gleich bei der ersten Antragstellung oder nach dessen Ablehnung erneut versuchen, Asyl zu erhalten, fehlen bislang.

Zu 2.:
Bei der zentralen Auswertung der Fingerabdrucke von Asylbewerbern durch das Bundeskriminalamt muß — ungeachtet dessen, ob das Bundeskriminalamt dabei in eigener Zuständigkeit oder für das Bundesamt für die Anerkennung ausländischer Flüchtlinge tätig wird — unbedingt folgendes sichergestellt sein:

— Fingerabdrucke von Asylbewerbern, die unter Beachtung des zu Nr. 1 Gesagten gefertigt wurden, dürfen nur gespeichert werden, soweit dies zur Sicherung der Identität unbedingt erforderlich ist. Dazu reicht die bisher vom Bundeskriminalamt angewandte Methode der sog. Kurzsatzverformelung der Fingerabdrucke aus. Gerade aber dabei soll es nicht bleiben: Mit der bevorstehenden Einführung von AFIS — einem neuen automatisierten Fingerabdruckverfahren — sollen künftig auch die Fingerabdrucke von Asylbewerbern, die allein zur Feststellung deren Identität gefertigt wurden, genauso erfaßt und ausgewertet werden wie die Fingerabdrucke mußmaßlicher oder tatsächlicher Straftäter. Asylbewerber würden damit von vornherein wie Straftäter behandelt. Eine solche Verfahrensweise wird dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot nicht gerecht. Zudem unterläuft sie die in § 16 Abs. 4 des Gesetzentwurfs vorgesehene Trennung der erkennungsdienstlichen Unterlagen von Asylbewerbern und Straftätern. Um die gebotene Differenzierung sicherzustellen, sollte — über das Trennungsgebot des § 16 Abs. 4 hinaus — die Verformelung auf den Abdruck eines Fingers des Asylbewerbers beschränkt werden, da dies zur eindeutigen Feststellung seiner Identität genügt.

— Die Datenschutzbeauftragten verkennen nicht, daß es unter Umständen im überwiegenden Allgemeininteresse notwendig sein kann, im Rahmen asylrechtlicher Identitätsfeststellung gefertigte Fingerabdrucke für Zwecke der Strafverfolgung zu nutzen. Weil eine solche Verwendung einen neuen und zudem erheblichen Eingriff in das Grundrecht auf Datenschutz darstellt, darf sie nicht — wie es der Gesetzentwurf aber vorsieht — praktisch voraussetzungslos erfolgen. Notwendig ist vielmehr, die Voraussetzungen in einem abschließenden Straftatenkatalog aufzuführen; darin könnten auch die in der amtlichen Begründung des Gesetzentwurfs erwähnten Fälle des Sozialhilfebetrugs enthalten sein.
— Ein entsprechender Maßstab ist an die Regelung anzulegen, wann zur Identitätssicherung gefertigte Fingerabdrucke von Asylbewerbern zur polizeilichen Gefahrenabwehr genutzt werden dürfen. Eine solche Nutzung sollte nur zugelassen werden, soweit dies zur Abwehr einer gegenwärtigen erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist.

Anlage 8

Entschließung der Konferenz der Datenschutzbeauftragten vom 1./2. Oktober 1992 (zum heimlichen Abhören in und aus Wohnungen — bei Gegenstimme Bayerns)

Nachdem erst vor kurzem mit dem Gesetz zur Bekämpfung der organisierten Kriminalität die Befugnisse der Strafverfolgungsbehörden erheblich erweitert worden sind und obwohl über den Erfolg dieser Maßnahme noch keine Erfahrungen gesammelt werden konnten, wird gegenwärtig parteiübergreifend vielfach die Forderung erhoben, der Polizei in bestimmten Fällen das heimliche Abhören und Herstellen von Bild- und Tonaufzeichnungen in und aus Wohnungen (sog. „Lauschangriff") zu ermöglichen. Hierzu erklären die Datenschutzbeauftragten des Bundes und der Länder:

1. Das Grundgesetz gewährt jedem einen unantastbaren Bereich privater Lebensgestaltung, der der Einwirkung der öffentlichen Gewalt entzogen ist. Dem einzelnen muß um der freien und selbstverantwortlichen Entfaltung seiner Persönlichkeit willen ein „Innenraum" verbleiben, in dem er „sich selbst besitzt" und „in den er sich zurückziehen kann, zu dem die Umwelt keinen Zutritt hat, in dem man in Ruhe gelassen wird und ein Recht auf Einsamkeit genießt" (BVerfGE 27, 1 ff.). Jedem muß ein privates Refugium, ein persönlicher Bereich bleiben, der obrigkeitlicher Ausforschung — insbesondere heimlicher — entzogen ist. Dies gilt gegenüber Maßnahmen der Strafverfolgung vor allem deshalb, weil davon auch unverdächtige oder unschuldige Bürger betroffen sind. Auch strafprozessuale Maßnahmen dürfen nicht den Wesensgehalt eines Grundrechts, insbesondere nicht das Menschenbild des Grundgesetzes verletzen.

2. Die Datenschutzbeauftragten nehmen die Gefahren, die das organisierte Verbrechen für die Opfer und auch für die Demokratie und den Rechtsstaat heraufbeschwört, sehr ernst. Sie sind allerdings der Meinung, daß eine angemessene Abwägung zwischen der Verfolgung der organisierten Kriminalität und dem Schutz der Persönlichkeitsrechte der Bürger geboten und möglich ist und es eine Wahrheitsforschung um jeden Preis auch künftig im Strafprozeßrecht nicht geben darf. Daraus folgt, daß der Lauschangriff auf Privatwohnungen für Zwecke der Strafverfolgung auch in Zukunft nicht erlaubt werden darf.

3. Eine andere Frage ist, ob und unter welchen Voraussetzungen der Gesetzgeber für Räume, die allgemein zugänglich sind oder beruflichen oder geschäftlichen Tätigkeiten dienen (z. B. Hinterzimmer von Gaststätten, Spielcasinos, Saunaclubs, Bordelle), einen Lauschangriff zulassen kann. Hierfür sind Mindestvoraussetzungen ein eng begrenzter abschließender Straftatenkatalog, die Verwendung der gewonnenen Erkenntnisse ausschließlich zur Verfolgung dieser Straftaten, ein strikter Richtervorbehalt sowie die Wahrung besonderer Amts- und Berufsgeheimnisse.

Anlage 9

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1./2. Oktober 1992

zum

Entwurf eines Gesetzes zur Sicherung und Strukturverbesserung der gesetzlichen Krankenversicherung — Gesundheits-Strukturgesetz 1993 — (BR-Drs 560/92)

Die Bundesregierung will mit dem Gesundheits-Strukturgesetz dem Kostenanstieg in der gesetzlichen Krankenversicherung entgegenwirken. Dieses begrüßenswerte Ziel soll nach dem vorgelegten Gesetzentwurf u.a. auch durch eine verstärkte automatisierte Datenverarbeitung erreicht werden. Die damit verbundenen Eingriffe in die Persönlichkeitsrechte der Versicherten und in die sie schützende ärztliche Schweigepflicht müssen auf das unbedingt Notwendige beschränkt werden. Die Datenschutzkonferenz hält vor allem folgende Verbesserungen des Gesetzentwurfs für notwendig:

— Der Gesetzentwurf sieht vor, daß die Krankenhäuser den Krankenkassen mehr Versichertendaten zur Verfügung stellen müssen als bisher. Es sollte deshalb eingehend geprüft werden, ob die Krankenkassen tatsächlich alle geforderten Angaben benötigen; die Aufgabenteilung zwischen Krankenkassen und Medizinischem Dienst muß aufrechterhalten bleiben.

— Für das Modellvorhaben zur Überprüfung des Krankenhausaufenthalts müssen die Erhebung, Verwendung und Löschung von Versichertendaten durch den Medizinischen Dienst präziser als bisher vorgesehen geregelt werden.

— Bei Einzug der Vergütung der Krankenhausärzte für Wahlleistungen durch Krankenhäuser sollte die Einschaltung privater Abrechnungsstellen ohne Einwilligung der Patienten nicht zugelassen werden, da dabei Abrechnungsdaten an Dritte offenbart werden. Die Daten sind gegen unbefugte Offenbarung und Beschlagnahme rechtlich besser geschützt, wenn sie — auch zur Abrechnung — im Krankenhaus verbleiben. Die Krankenhäuser sind zudem selbst in der Lage, die Vergütung einzuziehen.

— Für die neu vorgesehenen Patienten-Erhebungsbogen zur Ermittlung des Bedarfs an Pflegepersonal im Krankenhaus sollte eine strikte Zweckbindung sowie eine frühestmögliche Löschungs- oder Anonymisierungspflicht festgelegt werden. Eine Überlassung der Patienten-Erhebungsbogen in der im Gesetzentwurf vorgesehenen Fassung an die Krankenkassen ist abzulehnen.

Anlage 10

Entschließung der Konferenz der Datenschutzbeauftragtren des Bundes und der Länder vom 1./2. Oktober 1992

zum

Datenschutz bei internen Telekommunikationsanlagen

Der zunehmende Einsatz von digitalen Telekommunikationsanlagen (TK-Anlagen) in Wirtschaft und Verwaltung birgt Datenschutzrisiken in sich, denen durch eine datenschutzfreundliche Ausgestaltung der Technik und durch geeignete bereichsspezifische Regelungen entgegengewirkt werden muß. Telefongespräche stehen — auch wenn sie von einem Dienstapparat aus geführt werden — unter dem Schutz des Grundgesetzes. Dies hat das Bundesverfassungsgericht in seiner neueren Rechtsprechung hervorgehoben.

Der Schutz des Fernmeldegeheimnisses und des nichtöffenlich gesprochenen Wortes ist gerade bei Arbeitnehmern bedeutsam, da diese sich in einem besonderen Abhängigkeitsverhältnis befinden; aber auch das informationelle Selbstbestimmungsrecht Dritter, die anrufen oder angerufen werden, muß gewahrt werden.

Entsprechende bundesrechtliche Regelungen für interne TK-Anlagen sind überfällig, da in diese Anlagen — insbesondere wenn sie digital an das öffentliche ISDN angeschlossen sind — umfangreiche Sammlungen sensibler personenbezogener Daten entstehen können, die sich auch zur Verhaltens- und Leistungskontrolle eignen und zudem Hinweise auf das Kommunikationsverhalten aller Gesprächsteilnehmer geben.

Die Regelungen sollten verbindliche Vorgaben für die technische Ausgestaltung von TK-Anlagen geben und den Umfang der zulässigen Datenverarbeitung festzulegen:

— Es müssen die technischen Voraussetzungen gewährleistet sein, daß Anrufer und Angerufene die Rufnummernanzeige fallweise abschalten können.

— Die automatische Speicherung der Rufnummern von externen Anrufern nach Beendigung des Telefongesprächs ist auszuschließen, es sei denn, eine sachliche Notwendigkeit besteht hierfür (z. B. bei Feuerwehr und Retttungsdiensten).

— Die Weiterleitung eines Anrufs an einen anderen als den gewählten Anschluß sollte dem Anrufer so rechtzeitig signalisiert werden, daß dieser den Verbindungsaufbau abbrechen kann.

— Das Mithören und Mitsprechen weiterer Personen bei bestehenden Verbindungen sollten nur nach eindeutiger und rechtzeitiger Ankündigung möglich sein.

— Verbindungsdaten einschließlich der angerufenen Telefonnummern sollten nach Beendigung der Gespräche nur insoweit gespeichert werden, als dies für Abrechnungszwecke und zulässige Kontrollzwecke erforderlich ist. Die Nummern der Gesprächspartner von Arbeitnehmervertretungen, internen Beratungseinrichtungen und sonstigen auf Vertraulichkeit angewiesenen Stellen dürfen nicht registriert werden.

— Die TK-Anlagen müssen durch geeignete technische Maßnahmen gegen unberechtigte Veränderungen der Systemkonfiguration und unberechtigte Zugriffe auf Verbindungs- und Inhaltsdaten geschützt werden.

Da TK-Anlagen geeignet sind, das Verhalten und die Leistung der Arbeitnehmer zu kontrollieren, und sie überdies häufig die Arbeitsplatzgestaltung beeinflussen, löst ihre Einführung in Betrieben und Behörden Mitbestimmungsrechte der Betriebsräte und überwiegend auch der Personalräte aus. Sie dürfen daher nur betrieben werden, wenn

unter Beteiligung der Arbeitnehmervertretungen verbindlich festgelegt wurde, welche Leistungsmerkmale aktiviert und unter welchen Bedingungen sie genutzt werden, welche Daten gespeichert, wie und von wem sie ausgewertet werden. Die Nutzer der TK-Anlage sind über den Umfang der Datenverarbeitung umfassend zu unterrichten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, daß umgehend datenschutzrechtliche Regelungen für den Einsatz und die Nutzung von internen TK-Anlagen mit einer bereichsspezifischen Rechtsgrundlage für die Verarbeitung von Arbeitnehmerdaten geschaffen werden.

Anlage 11

Schreiben des Landesbeauftragten für den Datenschutz Niedersachsen an den Präsidenten des Niedersächsischen Landtages vom 6. November 1991 zur Umgestaltung der Vorläufigen Niedersächsischen Verfassung in eine endgültige Niedersächsische Verfassung

DER LANDESBEAUFTRAGTE FÜR DEN DATENSCHUTZ
NIEDERSACHSEN

Landesbeauftragter für den Datenschutz · Postfach 221 · 3000 Hannover 1

Präsident
des Niedersächsischen Landtages
- Landtagsverwaltung -

3000 Hannover 1

Ihr Zeichen, Ihre Nachricht vom	(Bitte bei Antwort angeben) Mein Zeichen	☎ (05 11) 120-	Hannover
	4 - 10	68 41	06.11.1991
			11 15 bl

Umgestaltung der Vorläufigen Niedersächsischen Verfassung in eine endgültige Niedersächsische Verfassung

Sehr geehrter Herr Landtagspräsident,

hiermit erlaube ich mir, in der o.a. Angelegenheit einen Vorschlag zu unterbreiten. Dieser Vorschlag soll allerdings nur für den Fall gelten, daß eine Grundsatzentscheidung erfolgt, die derzeitige Landesverfassung, ein bloßes Organisationsstatut, um Grundrechte zu ergänzen.

Das Grundrecht auf informationelle Selbstbestimmung ist fester Bestandteil der Rechtsprechung des Bundesverfassunsgerichts - vom Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65,1) bis zum Beschluß vom 11. Juni 1991 in einer Mietrechtsangelegenheit (NJW 1991, 2411) - und anderer Gerichte. Gleichwohl ist es angebracht, die bloße Herleitung aus Art. 2 Abs. 1 in Verbindung mit Art.1 Abs. 1 GG aufzugeben und ein eigenständiges Grundrecht sowohl im Grundgesetz als auch in den Landesverfassungen zu verankern. Die Gründe sehe ich in gewissen Unwägbarkeiten der Rechtsprechung und in der außerordentlichen Bedeutung, die der Information derzeit in Staat und Gesellschaft zukommt ("Informationsgesellschaft"); vgl. insoweit z.B. Büllesbach, Das neue Bundesdatenschutzgesetz, NJW 1991, 2593 (2594 f.).

Erfreulicherweise finden sich Regelungen bereits in den Verfassungen des Landes Nordrhein-Westfalen (Art. 4), des Saarlandes (Art. 2) und von Berlin (Art. 21 b). In den Verfassungsentwürfen einiger neuer Bundesländer sind entsprechende Weichenstellungen erfolgt. Von den vier Sachverständigen, die am 7. Februar 1991 von dem Sonderausschuß "Niedersächsische Verfassung" angehört wurden, sprachen sich drei - die Herren Prof. Dr. Schneider, Prof. Dr. Schmidt-Jortzig und Bäumer - für die Aufnahme eines Rechts auf Datenschutz bzw. informationelle Selbstbestimmung in unsere Landesverfassung aus.

Im Hinblick auf den genannten Beschluß des Bundesverfassungsgerichts vom 11. Juni 1991 sollte eine Festlegung, daß das Recht auf informationelle Selbstbestimmung allein gegen den Staat gerichtet sei, vermieden werden.

Unter weitgehender Übernahme einer Formulierung, die Herr Prof. Dr. Simitis - der kürzlich aus dem Amt geschiedene Hessische Datenschutzbeauftragte - anläßlich des vom Hessischen Landtag und von der Hessischen Landesregierung am 30. und 31. Oktober 1991 veranstalteten Verfassungssymposions vorlegte, schlage ich folgenden neuen Artikel ("Recht auf informationelle Selbstbestimmung") in der Landesverfassung vor:

(1) Jeder Mensch hat das Recht, über die Verarbeitung der auf seine Person bezogenen Daten selbst zu bestimmen.

(2) Jeder Mensch hat das Recht auf Information über die Verarbeitung der auf seine Person bezogenen Daten und Einsicht in die Akten, die Daten zu seiner Person enthalten.

(3) Einschränkungen dieser Rechte dürfen nur durch Gesetz oder aufgrund eines Gesetzes erfolgen.

Angemerkt sei, daß Herr Prof. Dr. Simitis auch einen Vorschlag zur Aufnahme eines "Rechts auf Informationsfreiheit" - im Sinne eines Rechts auf Zugang zu den Daten der Behörden ("Aktenöffentlichkeit") - in das Grundgesetz machte. Da hier Neuland beschritten wird - allerdings in zwingend notwendiger Weise -, sollte nach meiner Auffassung die Entwicklung auf Bundesebene abgewartet werden.

Eine Durchschrift dieses Schreibens darf ich der Niedersächsischen Staatskanzlei und dem Niedersächsischen Innenministerium zukommen lassen.

Mit vorzüglicher Hochachtung

Dr. Dronsch

Anlage 12

Auszug aus „Normen, Standards und Empfehlungen für den IuK-Technikeinsatz in der Landesverwaltung"

7. Datenschutz und Datensicherung

7.1 Aufgabe

Datenschutzvorschriften haben die Aufgabe, das Recht auf informationelle Selbstbestimmung zu gewährleisten und damit das Persönlichkeitsrecht zu schützen. Zulässigkeit und Umfang der Datenverarbeitung richten sich im Einzelfall nach den einschlägigen bereichsspezifischen gesetzlichen Bestimmungen oder, wenn solche nicht vorhanden sind, nach den Bestimmungen der Datenschutzgesetze. Datenschutz-Grundsätze gelten unabhängig davon, wo und auf welche Weise die Datenverarbeitung geschieht (Akte, Kartei, Textverarbeitung, Graphik, Groß-ADV, Mehrplatzsystem, PC usw.). Für den Umgang mit personenbezogenen Daten — gleich welcher Verarbeitungsform — gilt das Prinzip: „Verboten ist, was nicht ausdrücklich erlaubt wurde!" Informationen, die zur Durchführung technischer oder organisatorischer Kontrollen gespeichert werden, dürfen nicht zu Zwecken der Verhaltens- oder Leistungskontrolle genutzt werden.

Unter Datensicherung sind im Rahmen der IuK-Technik-Empfehlungen die technischen und organisatorischen Maßnahmen zu verstehen, die eine störungsfreie und gegen Mißbrauch gesicherte Datenverarbeitung zum Ziel haben. Dabei ist von folgenden Gefahren auszugehen:

— unbefugter Informationsgewinn (Verlust der Vertraulichkeit)
— unbefugte Modifikation von Informationen (Verlust der Integrität)
— unbefugte Beeinträchtigung der Funktionalität (Verlust der Verfügbarkeit).

Um einen sicheren Umgang mit personenbezogenen Daten und informationsverarbeitenden Systemen zu gewährleisten, ist es erforderlich, der jeweiligen Gefährdungslage entsprechende Sicherheits-Standards einzuhalten. Zur Beurteilung der Sicherheit sind die „IT-Sicherheitskriterien" als Weiterentwicklung des sogen.„Orange Book" erarbeitet worden (Bek.d.BMI v. 09.05.1989, GMBl. S. 278). Vor Einsatz neuer automatisierter Informationssysteme, in denen personenbezogene Daten verarbeitet werden, sollte sich die verarbeitende Stelle vom Software-Hersteller ein Sicherheitszertifikat nach § 6 BSIG vorlegen lassen.

Die systemseitigen Möglichkeiten zur Datensicherheit sollten ausgeschöpft werden. Sofern die Datensicherheit mit den verfügbaren Maßnahmen für eine sensitive Anwendung nicht gewährleistet werden kann, soll hierfür auf den Einsatz von informationsverarbeitenden Systemen verzichtet werden.

7.2 Grundsätze

7.2.1 Paßwörter

Jedes DV-System, mit dem ein Zugriff auf personenbezogene Daten möglich ist, ist zur Benutzer-Identifikation und -Authentifikation mindestens mit einem Paßwort-Schutz zu versehen. Das Paßwort-Verfahren ist hierfür das am

meisten verwendete Kontroll-Verfahren. Um Ausforschungs-Versuchen zu begegnen und unbefugte Zugriffe zu verhindern, sollten bei Auswahl und Verwendung von Paßworten folgende Grundsätze beachtet werden:

— Mindestlänge 6 Zeichen, die möglichst aus einer Kombination von Buchstaben, Ziffern und Sonderzeichen bestehen, nur dem Benutzer bekannt.
— Für den Benutzer leicht zu merken, für einen Fremden schwer zu erraten!
— Automatischer Ausschluß von Trivialwörtern (z. B. 08/15, Vornamen, Geburtsdaten,
— Fehlversuchszähler unter Einbeziehung des Tagesdatums,
— Reaktionsverzögerung des Rechners bei wiederholter Fehleingabe,
— verschlüsselte Speicherung von Paßworten,
— automatischer Änderungszwang nach Zeitablauf, jedoch nicht zu oft!

7.2.2 Protokolldateien

Durch automatisierte Aufzeichnung von Protokolldaten wird die DV nachprüfbar und transparent gemacht; zugleich wird damit einer mißbräuchlichen Verwendung vorgebeugt, weil keiner darauf vertrauen kann, daß Verstöße unentdeckt bleiben. Protokollierung ist jedoch kein Selbstzweck, sondern ist nur sinnvoll und datenschutzrechtlich vertretbar, wenn die Protokolldaten auch tatsächlich ausgewertet werden. Eine totale Registrierung aller Benutzer-Aktivitäten kann aus Sicht des Datenschutzes sogar bedenklich sein, da auf diese Weise eine neue Sammlung personenbezogener Daten über betroffene Bürger und über Mitarbeiter entsteht, die zu zweckfremder Nutzung reizt.

Protokoll-Umfang, Kontroll-Dichte und Löschungsfristen sind von der Sensitivität der jeweiligen Anwendung abhängig. Folgende Grundsätze sollten beachtet werden:

1. Protokolle müssen die Aktionen erfassen, die auf mögliche Datenschutzverstöße hinweisen, wie z. B. nicht erfolgreiche Login-Versuche, Hoch- und Runterfahren des Systems usw. Bei sensitiven Daten sind weitergehende Protokollierungen erforderlich (z. B. sämtliche Paßwortänderungen, alle Login-Versuche, Aktivitäten über DFÜ).

2. Protokollierungen sollten im jeweiligen Anwendungsverfahren selbst erfolgen, nur so sind ausreichende Differenzierungen nach Daten, Feldern, Masken, Auswertungen, Ausdrucken u. ä. möglich.

3. Grundsätzlich ist jeder schreibende Zugriff aufzuzeichnen, evtl. mit Inhalt des neu eingegebenen oder geänderten Datensatzes; bei sensitiven Daten sollten jedoch nur Feldbezeichnungen protokolliert werden. Darüber hinaus sollten lesende Zugriffe sensiblerer Anwendungen, alle Abruf-Zugriffe sowie per Dialog veranlaßte Übermittlungen aufgezeichnet werden.

4. Für jede aufzuzeichnende Aktivität sollten mindestens Geräte-Identifikation, Datum und Uhrzeit, Veranlasser, Grund, Ordnungs-Nr. des Datensatzes und Programm festgehalten werden. Untauglich sind Protokolle, die lediglich das Starten und Beenden des Betriebssystems oder eines peripheren Gerätes aufzeichnen. Bei Massenprotokollierungen kann eine Stichproben-Aufzeichnung nach dem Zufallsverfahren in Frage kommen.

5. Protokolle sind regelmäßig auszuwerten. Je nach Sensitivität kann eine tägliche bis vierteljährliche Kontrolle angemessen aber auch erforderlich sein. Die großen Datenmengen der Protokolle erfordern eine automatisierte Auswertung zur zeitnahen und effizienten Kontrolle und erzwingen kurze Aufbewahrungsfristen.

Protokolldateien müssen nach angemessener Zeit möglichst automatisch gelöscht werden. Die Speicherungsdauer sollte 1 Jahr nicht übersteigen. Für kürzere Aufbewahrungsfristen sprechen der geringere Speicheraufwand und deutlich reduzierte Mißbrauchs-Gefahren.

7.2.3 Verschlüsselung von Daten

Sensitive personenbezogene Daten sollten bei Speichung in DOS- und UNIX-Systemen sowie bei Übertragungen in einem Kommunikationssystem grundsätzlich verschlüsselt werden. Da eine Verschlüsselung standardmäßig nicht verfügbar ist, muß hierfür Zusatz-Software beschafft werden. Die gängigsten Methoden der Verschlüsselungstechnik sind:

XOR
ein relativ einfacher, dafür schneller Verschlüsselungsalgorithmus, für Experten jedoch nicht allzu sicher;

DES
ein symmetrisches Schlüsselverfahren, das beim Verschlüsseln und beim Entschlüsseln den gleichen Schlüssel verwendet, weitaus sicherer als XOR, jedoch sehr zeitaufwendig, problematisch ist die Geheimhaltung des Schlüssels.

RSA
ein asymmetrisches Schlüsselverfahren, das mit Schlüsselpaaren arbeitet, einem öffentlichen Schlüssel (public key), der zum Verschlüsseln dient, und einem geheimen Schlüssel zum Entschlüsseln, der nur dem Berechtigten bekannt ist, wobei jeder Benutzer sowohl einen öffentlichen wie einen geheimen Schlüssel hat, die zueinander invers sind.

7.2.4 Virenschutz

Als Computervirus wird ein nicht eigenständiges Programm bezeichnet, das sich selbst vervielfältigen, sich in Wirtsprogramme einnisten und Schaden anrichten kann. Typische Anzeichen von Virenbefall sind z. B. Veränderung von Programmen im Vergleich zu ihren Sicherungskopien, deutliche Verringerung der Verarbeitungsgeschwindigkeit, scheinbare Hardware-Fehler (z. B. „Bildschirmverschmutzung") und unerklärliche Systemabstürze. Computervieren haben sich zu einer realen Gefährdung ordnungsgemäßer Datenverarbeitung entwickelt. Nicht nur der Einsatz illegaler Software kann zum Virenbefall führen, sondern Viren sind bereits in von Händlern gelieferten neuen PC-Systemen und in Originalsoftware aufgetreten. Den Befall seines Rechners kann niemand völlig ausschließen. Daher sind abgestimmte Maßnahmen zum Virenschutz und zur Schadensbegrenzung unerläßlich.

Alle Mitarbeiter sollen über die Gefährdung durch Computerviren und über die Bedeutung vorbeugender Maßnahmen unterrichtet sein. Erstbestände sind durch schreibgeschützte Sicherungskopien zu sichern und gesondert aufzubewahren. Der Einsatz von nicht autorisierter Software sowie von Demo-Disketten und -Programmen, public domain-Software und shareware-Programmen ist zu untersagen.

Bei Verdacht von Virenbefall sollten alle vorhandenen PC mit dem Virus-Suchprogramm überprüft werden. Bei Datenaustauschverfahren sollten „Schleusen" eingerichtet werden, damit Disketten nicht ungeprüft in den Geschäftsgang gelangen können. Die Prüfungstätigkeit sollte einer zentralen Stelle in der Behörde zugewiesen werden, deren Mitarbeiter tiefergehende

IuK-Technik-Kenntnisse haben, z. B. dem Benutzer-Service. Die Ergebnisse aller Überprüfungen sind zu dokumentieren.

Wird ein Virusbefall festgestellt, sind unverzüglich die Sicherungsmaßnahmen einzuleiten und das Meldeverfahren durchzuführen (Anlage 1). Das NLVwA-D2 leistet auf Anforderung fachliche Unterstützung. Die Beschaffung eines Viren-Suchprogramms (Vieren-Scanner) sowie seine ständige Aktualisierung wird empfohlen, z. B. TNT Turbo Antivirus (EPG GmbH, Hans-Stießberger-Straße 3, 8013 Haar), McAffee (NOVIER Datentechnik GmbH, Hochofenstraße 19-21, 2400 Lübeck 14), Dr. Solomons Anti-Viren-Werkzeuge (S&S International Ltd., Chesham).

In der Anlage 2 wird ein „Merkblatt zum sicheren Umgang mit PC am Arbeitsplatz" abgebildet, das weitgehend dem vom „Bundesamt für Sicherheit in der Informationstechnik — BSI" entwickelten Merkblatt entspricht.

7.2.5 Einsatzvoraussetzungen für Applikationen aus Standardsoftware

Die folgenden Regeln gelten für Programme auf der Basis von Standardsoftware Applikationen):

— Entwicklung
Sollen Applikationen landeseinheitlich eingesetzt werden, empfiehlt es sich, die Entwicklung und Pflege dem NLVwA-D6 (vgl. 6.4) zu übertragen.

— Testverfahren
Applikationen sind auf die ordnungsgemäße Erledigung der Fachaufgabe zu überprüfen. Bei personenbezogenen Anwendungen und bei komplexen oder umfangreichen Applikationen sollen eigens dafür Testdaten erstellt werden. Verantwortlich für das Testverfahren ist die freigebende Stelle. Sie soll die Stelle, die die Applikation entwickelt hat, und die anwendende Stelle beteiligen.

— Freigabeverfahren
Die freigebende Stelle ist durch Anweisung der Behördenleitung festzulegen. Landeseinheitliche Applikationen sollen durch die zuständige oberste Landesbehörde freigegeben werden.

— Dokumentation
Die wesentlichen Funktionen der Applikation, die Ergebnisse des Testverfahrens und die Freigabe sollen dokumentiert werden.

7.2.6 Dienstanweisung

In einer Dienstanweisung sollten alle datenschutz- und datensicherheits-relevanten Maßnahmen, sowie die Pflichten und Verantwortlichkeiten festgehalten werden. Zum Regelungsumfang gehören insbesondere Verhaltensregeln wie das Verschließen der Geräte auch bei kurzfristiger Abwesenheit, Verschließen der Räume, Kennzeichnung der Datenträger und deren Verschluß, Aufgaben des Systemverwalters, Paßwortregeln, Dokumentationspflichten, Programm-Prüfung und -Freigabe, Datenschutz-Kontrolle.

7.3 DOS-Systeme

7.3.1 Organisatorische Maßnahmen

PC unter dem Betriebssystem MS-DOS sind offene Systeme, solange der Benutzer Zugang zur Betriebssystemebene hat. Dies führt bei einer Nutzung durch mehrere Personen zu unkontrollierbaren Verarbeitungs-Zuständen. Vor einem geplanten DOS-Einsatz mit personenbezogenen Daten ist daher ein angemessenes Sicherungskonzept zu entwickeln, das nur die unabdingbar benötigten DOS-Befehle und die Fachanwendungen verfügbar und das eine Kontrolle der Benutzung möglich macht.

7.3.2 Technische Maßnahmen

Bei Speicherung sensitiver Daten wird nach einer Entscheidung des IMA-IuK der Einsatz der Sicherheits-Soft- und Hardware „Safe-Guard-Professional" (Utimaco Software GmbH, Dornbachstraße 30, Postfach 2026, 6370 Oberursel 1) gefordert. Zur Beschaffung dieser Sicherheits-Technik sollte auf den Rahmenvertrag zwischen dem Land Niedersachsen und dem Hersteller zurückgegriffen werden.

7.3.3 Bauliche Maßnahmen

Zur physischen Absicherung bieten sich u.a. mechanische Verriegelung der Geräte (Sicherungseisen), Aufbewahrung der PC in Sicherheitsschränken, Einsatz in einem eigenen abgesicherten Baukörper, Zugangsüberwachung, zentrale Benutzung eines Datensafes an.

7.4 UNIX-Systeme

7.4.1 Organisatorische Maßnahmen

Das Standard-UNIX V.3 und die entsprechenden Derivate bieten im Gegensatz zum Betriebssystem MS-DOS einige datenschutzrelevante Sicherungsmöglichkeiten. Sie werden in den meisten Fällen den Benutzern lediglich optional angeboten, nicht jedoch erzwungen. Auch folgt aus der UNIX-Struktur, daß sicherheitsrelevante Mechanismen schnell unübersichtlich werden, so daß Schwachstellen und „menschliches Versagen" leicht möglich sind. Aus der Sicht der Verfahrenssicherheit und des Datenschutzes ist die Allmacht des UNIX-Systemverwalters (USVw) die entscheidende Sicherheits-Schwachstelle. Deren Zugriffs- und Nutzungsrechte sollten wie folgt konsequent begrenzt und kontrolliert werden:

- — der USVw ist nicht zugleich Anwender bzw. interner Datenschutzbeauftragter,
- — der USVw wird sorgfältig ausgewählt und gut geschult,
- — der USVw hat einen gleichwertig geschulten Vertreter,
- — das Super-User-Paßwort ist zweigeteilt und wird nach Tresorverfahren verwendet,
- — USVw-Funktionen sind nur von gesicherten Arbeitsplätzen aus möglich
- — Anwender haben grundsätzlich keine Shell-Berechtigung,
- — wenn überhaupt wird eine Shell-Berechtigung nur eingeschränkt eingerichtet.

7.4.2 Technische Maßnahmen

Datenschutzrechtlich vertretbar sind nur UNIX-Systeme mit erhöhtem Sicherheits-Standard. Bei einer System-Auswahl sollte zur Grundlage der Entscheidung ein Zertifizierungsnachweis gemacht werden, der mindestens der Funktionsklasse F2 und der Qualitätsstufe Q3 des IT-Kriterienkataloges entspricht.

Das UNIX-System muß vom USVw unter Beachtung der oben beschriebenen Grundsätze zum Paßwortverfahren, zur Protokollierung und zur Verschlüsselung konfiguriert werden. Darüber hinaus sind insbesondere die Zugriffsberechtigungen auf sämtliche sicherheitsrelevanten Dateien sorgfältig einzurichten und zu pflegen. Besonderes Augenmerk ist auf Dateien mit s-bit und auf Verweise („links") zu richten.

„Admin Tools" von Quantum ist ein Werkzeug zur UNIX-Systemverwaltung, das u. a. eine Protokolldatenaufbereitung, Daten-Integritätsprüfung und andere Sicherheitskriterien enthält.

7.4.3 Bauliche Maßnahmen

UNIX-Rechner mit besonderen Funktionen (Server, Datensicherungseinrichtungen, zentrale Speicher mit sensitiven Daten, zentral eingesetzte, automatische Ein-/Ausgabegeräte) sind in ständig verschlossenen Räumen oder Schränken unterzubringen, die nur autorisierten Mitarbeitern zugänglich sind. Die Stromzufuhr darf nicht ohne weiteres unterbrechbar sein, da sonst u. U. ein ungeschützter Single-User-Mode mit Datei-Zugriffen ohne Paßwortschutz möglich ist. Manipulationen an den Rechnern (z. B. Öffnen des Gehäuses) ist nur dem USVw bzw. seinem Vertreter oder von ihnen autorisierten Personen gestattet.

7.5 Kommunikationssysteme

In zunehmendem Maße kommen vernetzte Rechnersysteme zum Einsatz. Da ein Netzwerk zumindest theoretisch eine Vielzahl von Angriffspunkten bietet, ist die Netzwerk-Architektur und die Kommunikations-Überwachung von besonderer Bedeutung für Datenschutz und Datensicherheit.

Ethernet ist für UNIX-LAN zur Quasi-Standard-Übertragungstechnik geworden. Im PC-Bereich sind auch andere Netz-Technologien üblich (z. B. Token Ring, ARCnet, u. a.). Bei Ethernet ist nicht festgelegt, wann eine Station auf das Netz zugreifen darf. Auch wird die gesendete Information physikalisch allen Netzwerk-Teilnehmern zugeleitet. Erst ein Vergleich der Kennungen im empfangenden Rechner entscheidet, ob die Daten verarbeitet werden oder nicht. Auch andere LAN-Technologien arbeiten ähnlich.

Paßworte werden überwiegend unverschlüsselt über das Netz gesendet. Um möglichen Ausforschungsversuchen zu begegnen, sollte zumindest die Inhouse-Verkabelung verdeckt installiert sein, so daß Kabel nicht öffentlich zugänglich sind. Sensitive Daten — auch Paßwörter — sind nur verschlüsselt im Kommunikationsnetz zu übertragen.

Bei Datenfernübertragungen außerhalb eines LAN ist eine Dokumentation über alle Kommunikationspartner und die gesamte Übertragungstechnik zu führen. Alle DFÜ-Aktivitäten sollten protokolliert werden (Quelle, Ziel, Datum und Uhrzeit, Anlaß, Veranlasser).

In Abhängigkeit von der Sensitivität der Anwendung sind darüber hinaus folgende technische und organisatorische Maßnahmen zu treffen:

— Authentizitätsprüfung (Paßwort, Rückruf, Chipkarte)
— Zugangskontrolle
— Verschlüsselung (Private Key, Public Key)
— Digitale Unterschrift
— Routingkontrollen
— Überwachung der Abhörsicherheit von Übertragungswegen (z. B. bei Telefax)
— Installation von Direktruffunktionen
— Notariatsfunktionen
— Journalfunktionen
— Abstrahlsichere Endgeräte oder Vermittlungseinrichtungen
— Überwachung und Alarmierung
— Logbücher.

Hinweise zur Übertragungssicherung können ferner den „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT-Sicherheitskriterien) entnommen werden, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) herausgegeben hat (Bekanntmachung vom 9. Mai 1989, GMBl. 1989 S. 278; BAnz Nr. 99a vom 1. Juni 1989).

Die DBP Telekom stellt für bestimmte Dienste bzw. Netze technische Maßnahmen (Anschlußkennung, Teilnehmerkennung, Geschlossene Benutzergruppen) zur Verfügung, die die Sicherheit der Kommunikation erhöhen.

Ergänzung
(zu Drs 12/4400)

Der Präsident
des Niedersächsischen Landtages
— Landtagsverwaltung —

Hannover, den 12. 2. 1993

Betr.: **Elfter Bericht über die Tätigkeit des Niedersächsischen Datenschutzbeauftragten**

Der o. a. Bericht ist auf den Seiten 199 bis 203 um die nachfolgend abgedruckten Abbildungen zu ergänzen:

Abb. 1

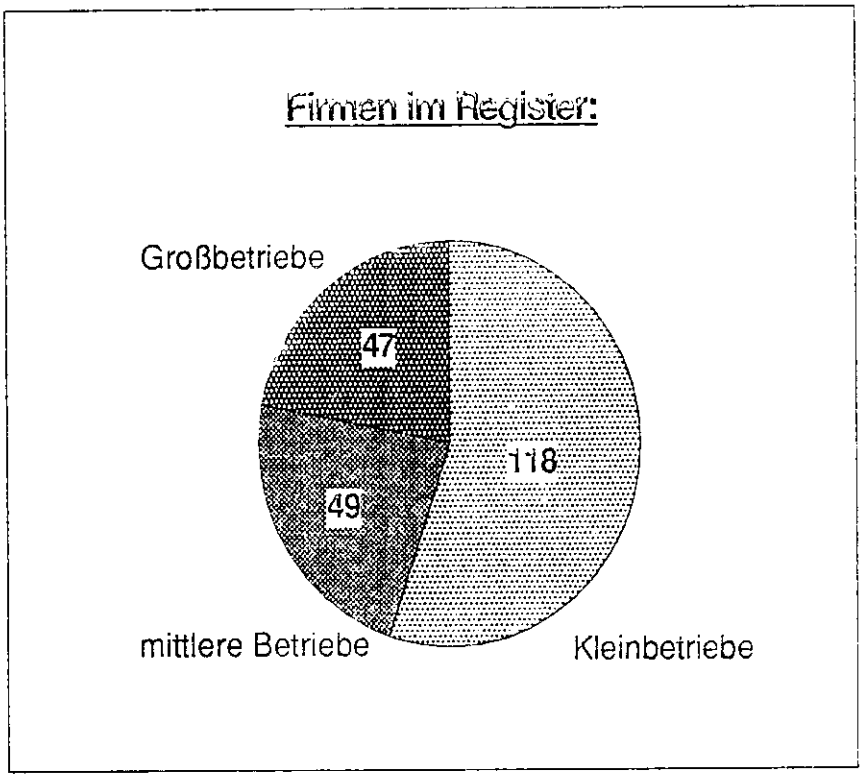


Abb. 2

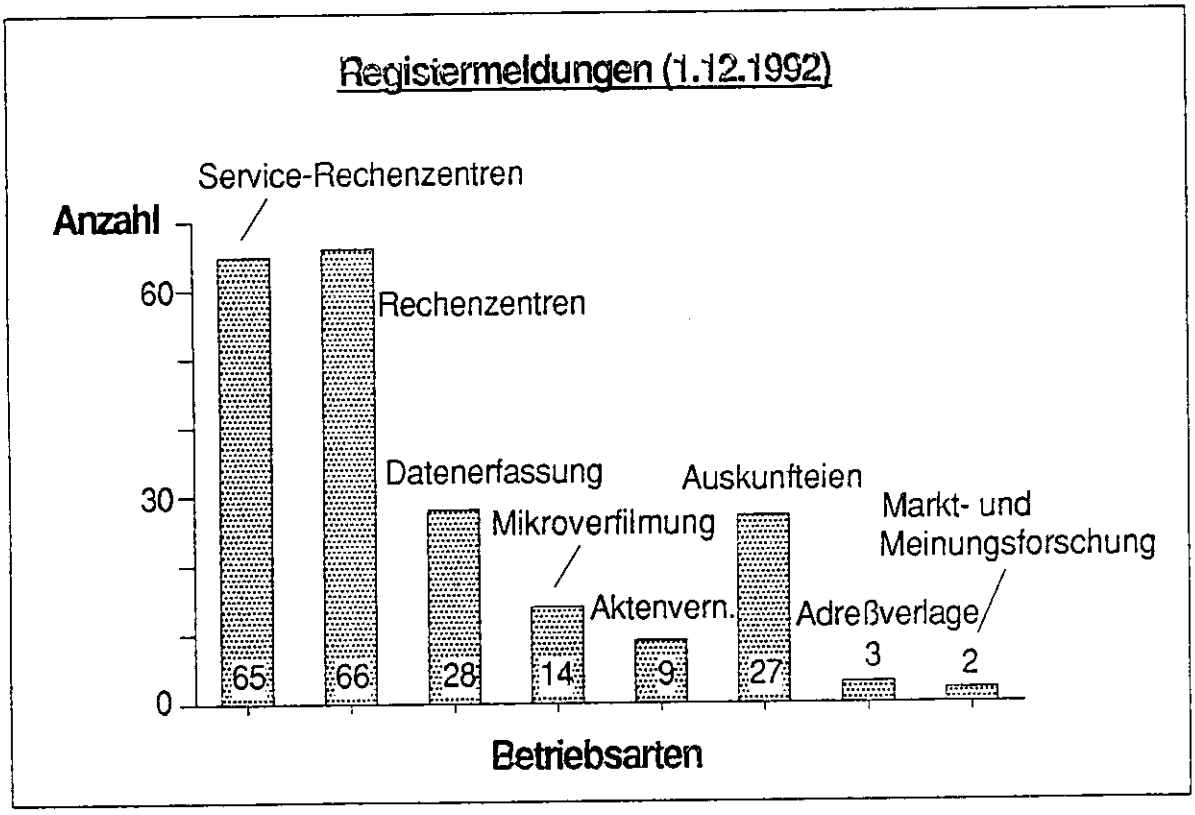

Registermeldungen (1.12.1992)
Anzahl
60
30
0
Service-Rechenzentren
Rechenzentren
Datenerfassung
Mikroverfilmung
Aktenvern.
Auskunfteien
Adreßverlage
Markt- und Meinungsforschung
65
66
28
14
9
27
3
2
Betriebsarten

Abb. 3

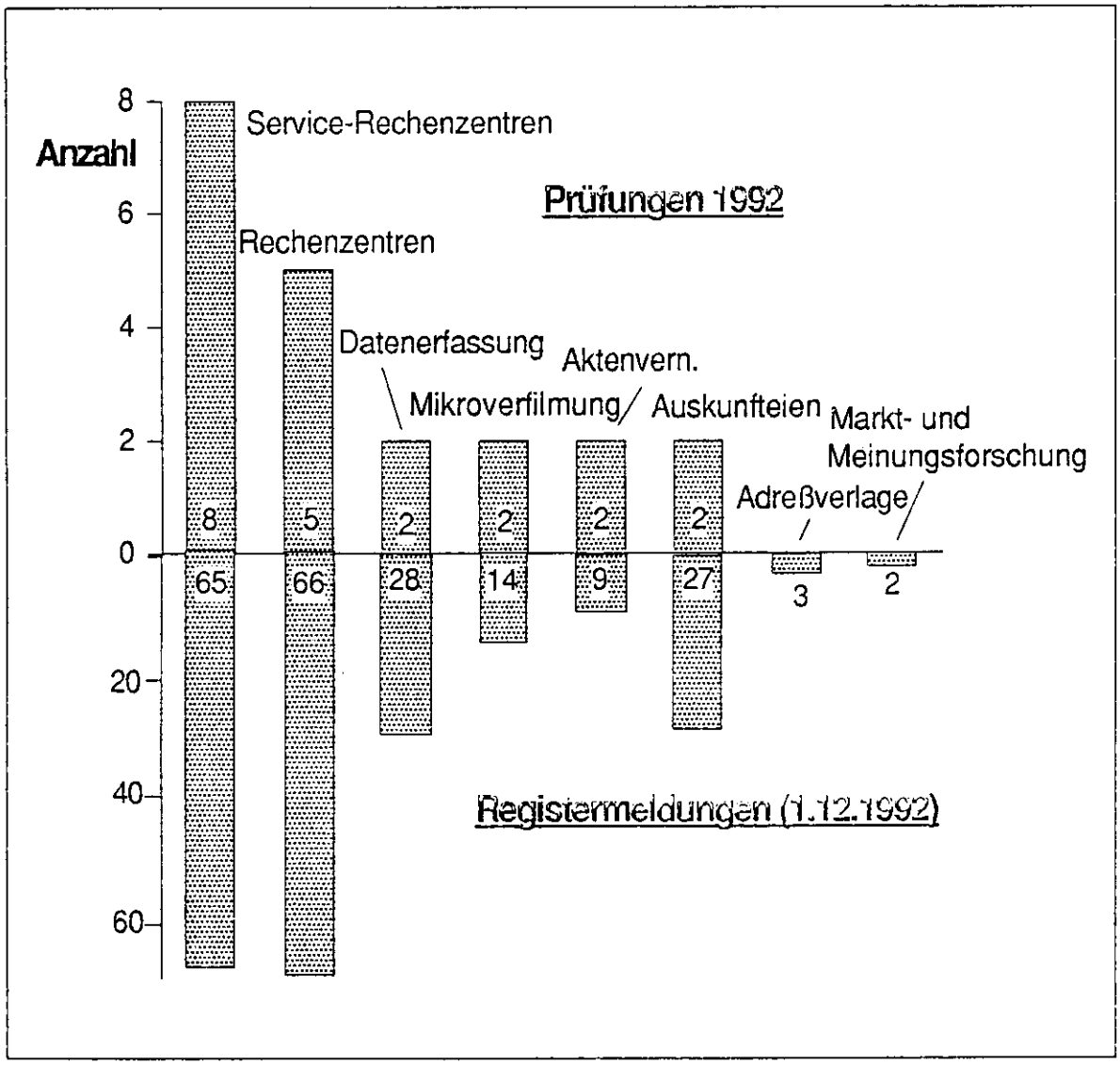

Anzahl
8
6
4
2
0
20
40
60
Service-Rechenzentren
Rechenzentren
Datenerfassung
Aktenvern.
Mikroverfilmung
Auskunfteien
Markt- und Meinungsforschung
Adreßverlage
Prüfungen 1992
8
5
2
2
2
2
Registermeldungen (1.12.1992)
65
66
28
14
9
27
3
2

Abb. 4

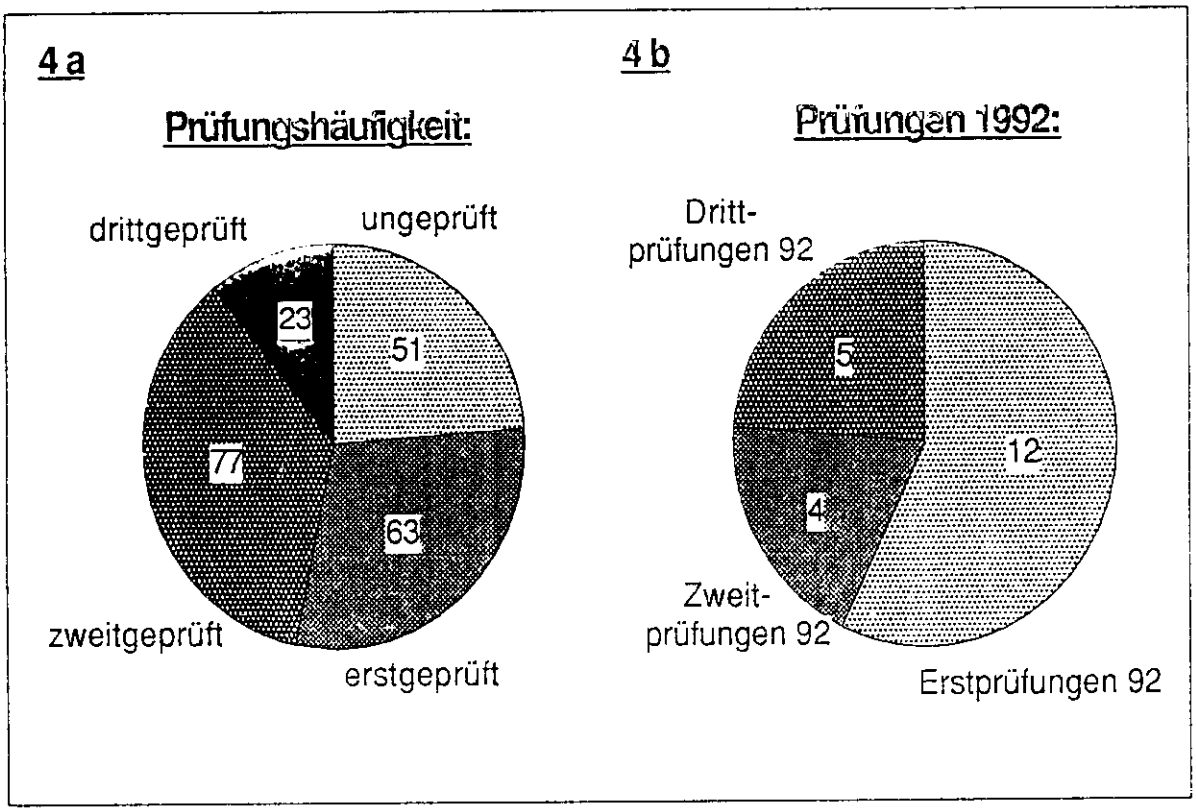
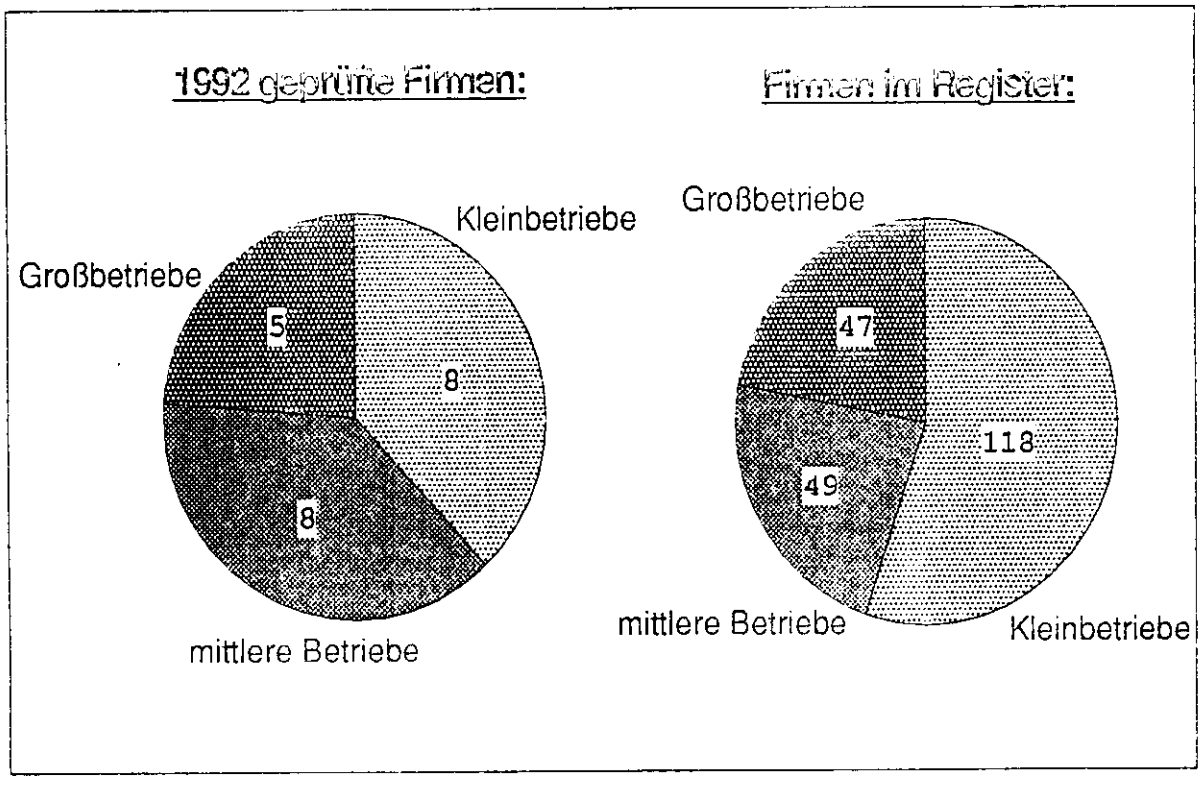

4a
Prüfungshäufigkeit:
drittgeprüft
ungeprüft
23
51
77
63
zweitgeprüft
erstgeprüft
4b
Prüfungen 1992:
Dritt-
prüfungen 92
5
12
4
Zweit-
prüfungen 92
Erstprüfungen 92

Abb. 5


1992 geprüfte Firmen:
Kleinbetriebe
Großbetriebe
5
8
8
mittlere Betriebe
Firmen im Register:
Großbetriebe
47
118
49
mittlere Betriebe
Kleinbetriebe