13. Wahlperiode

Drucksache **13/5813**

Ca. 95 Seiten

11. 02. 94

HESSISCHER LANDTAG

Zweiundzwanzigster Tätigkeitsbericht des Hessischen Datenschutzbeauftragten

vorgelegt zum 31. Dezember 1993
nach § 30 des Hessischen Datenschutzgesetzes vom 11. November 1986

Eingegangen am 11. Februar 1994 · Ausgegeben am 1. März 1994

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

INHALTSVERZEICHNIS

Anlagen

KERNPUNKTE DES 22. TÄTIGKEITSBERICHTS

1. Der vom Hessischen Ministerium des Innern und für Europaangelegenheiten erarbeitete Entwurf eines Gesetzes über Sicherheitsüberprüfungen von Angehörigen des öffentlichen Dienstes (HSÜG, Stand 21. September 1993) enthält gegenüber dem Entwurf der Bundesregierung unter datenschutzrechtlichen Gesichtspunkten eine Reihe von Verbesserungen (Ziff. 2).

2. Der Gesetzentwurf der Landesregierung für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOG) nimmt die rechtsstaatlich gebotene Eingrenzung der Befugnis der Polizei zur Erhebung personenbezogener Daten durch Observation und den Einsatz technischer Mittel sowie durch den Einsatz von V-Personen und verdeckt ermittelnden Personen vor (Ziff. 4.2).

3. Der Fall eines Darmstädter Taxifahrers, der sich vergeblich um die Verlängerung seines Fahrgastbeförderungsscheins bemühte, ist ein typisches Beispiel dafür, daß Verwaltungen gesetzliche Verwertungsverbote mißachten (Ziff. 6.2)

4. Bei der Prüfung der Staatsanwaltschaften wurden Mängel festgestellt, die auch bei strukturellen Kontrollen anderer Verwaltungen immer wieder auffallen (Ziff. 7.1).

5. Bei der Prüfung des Universitätsklinikums Frankfurt wurde festgestellt, daß die Patienten entsprechend der Neuregelung im Krankenhausgesetz bei ihrer Aufnahme gefragt werden, ob an der Pforte Auskunft über ihren Aufenthalt im Krankenhaus gegeben werden soll. Die im Gesetz vorgeschriebene Abschottung der Datenbestände der Fachabteilungen untereinander wird umgesetzt. Einige Mängel bei den technischen und organisatorischen Datensicherungsmaßnahmen müssen beseitigt werden (Ziff. 9.2).

6. Erklärungen der Patienten zur Entbindung von der ärztlichen Schweigepflicht sind nur rechtswirksam, wenn die Patienten vorher korrekt und konkret über die vorgesehene Verwendung ihrer Daten informiert wurden. Entbinden dann die Patienten ihren Arzt aufgrund der ihnen gegebenen Informationen von der Schweigepflicht, so dürfen die Daten nicht später auf andere Weise verwendet werden (Ziff. 9.3).

7. In das Hessische Beamtengesetz (HBG) wurden in Anpassung an das Beamtenrechtsrahmengesetz (BRRG) gesetzliche Regelungen zum Umgang mit Personalakten aufgenommen, deren Umsetzung in der Praxis noch Probleme bereitet (Ziff. 10.1).

8. Das Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms (FKPG) ermöglicht den Sozialhilfeträgern umfangreiche Datenabgleiche. Dadurch entsteht für die Mehrzahl der gesetzestreuen Bürger die Gefahr, zum „gläsernen Leistungsbezieher" zu werden (Ziff. 11.1).

9. Das Hessische Kultusministerium hat den Entwurf einer Rechtsverordnung zum Schulgesetz vorgelegt, die den Umfang und die Einzelheiten personenbezogener Datenverarbeitung im Schulbereich regelt (Ziff. 12.1).

10. Der Einsatz von Bürokommunikationsmitteln in den Verwaltungen nimmt ständig zu. Es sind Wege zu suchen, die das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger wahren, ohne den Fortschritt der Kommunikationstechnologie zu hindern (Ziff. 14.2).

11. Auch bei Staffelung der Beiträge oder Gebühren für die Kindergartenbenutzung nach dem Einkommen darf die Kommune nicht die Vorlage des vollständigen Einkommensteuerbescheids verlangen (Ziff. 14.5).

12. Der von der Landesregierung vorgelegte Entwurf für ein Hessisches Umweltinformationsgesetz (HUIG) verspricht Informationsfreiheit und ein Recht auf Akteneinsicht, ohne das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger zu verletzen (Ziff. 18.1).

13. Das durch EG-Verordnungen eingeführte integrierte Verwaltungs- und Kontrollsystem (InVeKoS) führt zu einer lückenlosen Erfassung der Landwirte zum Zweck der Kontrolle im Bereich landwirtschaftlicher Förderungsmaßnahmen und verstößt mit seinem Sammeln personenbezogener Daten auf Vorrat und zu unbestimmten bzw. noch nicht bestimmbaren Zwecken gegen den Grundsatz der Verhältnismäßigkeit (Ziff. 19).

14. Aus der zunehmenden Vernetzung von Rechnern ergeben sich erhebliche Risiken für die Datensicherheit (Ziff. 21.1).

1. Vorwort

Das Jahr 1993 war in Staat und Gesellschaft der Bundesrepublik von Sorgen geprägt. Diese Sorgen haben auch den Datenschutz erreicht und beeinträchtigt. Auf zwei Feldern vor allem konnte man spüren, daß sich das Klima geändert hat: in der Wirtschaft und bei der Inneren Sicherheit.

Die wirtschaftlichen Probleme und die Angst vor dem Verbrechen bewirken für den Datenschutz am Ende dasselbe: Sie erhöhen die Kontrollbedürfnisse des Staates.

Mißbrauch von Sozialleistungen oder Steuerverkürzung werden – auch in den Augen der Bevölkerung – in schlechten Zeiten zu einem unerträglichen Anschlag auf die gemeinsamen Ressourcen. Also wächst das Bedürfnis, solches zu unterbinden, mit der Tendenz, es möglichst lückenlos zu kontrollieren und aufzuklären. Der Tätigkeitsbericht belegt diese Tendenz (Ziff. 8.1, 11.1).

Auf dem Gebiet der Inneren Sicherheit hat sich die öffentliche Diskussion um die „Organisierte Kriminalität" so entwickelt und zugespitzt, daß eine Analyse unter Gesichtspunkten des Datenschutzes an der Zeit war. Die Instrumente, welche zur Ermittlung und Bekämpfung dieser Kriminalitätsform bereits gesetzlich vorgesehen sind oder noch eingefordert werden, berühren den Datenschutz, denn sie richten sich fast ausschließlich auf die Verarbeitung persönlicher Daten von Beschuldigten, Verdächtigen oder Dritten: Telefonüberwachung, langfristige polizeiliche Beobachtung, Rasterfahndung, verdeckte Ermittlungen, „Lauschangriff".

Das zweite öffentliche Forum Datenschutz, das am 1. Juli 1993 – wiederum unter gemeinsamer Leitung des Präsidenten des Hessischen Landtags und des Hessischen Datenschutzbeauftragten – im Plenarsaal des Hessischen Landtags stattfand, hatte deshalb das kontrovers formulierte Thema: „Organisierte Kriminalität – geschützt vom Datenschutz?"

In Referaten sowie in spontanen Diskussionsbeiträgen aus dem Publikum wurden den zahlreichen Zuhörern im Plenarsaal des Hessischen Landtags und den Zuschauern des Hessischen Fernsehens vor allem die folgenden Schwerpunkte und Sichtweisen vorgestellt: Reformvorstellungen von Strafrichtern, von Staatsanwaltschaft, Polizei und Verfassungsschutz; Formen von Kriminalität und Möglichkeiten von Ermittlungen in einem Bundesland wie Hessen und einer Großstadt wie Frankfurt; Datenschutz als Menschenrecht und Konsequenzen für die staatliche Reaktion auf Kriminalität; langfristige gesellschaftliche Einstellungen gegenüber allgemeinen Bedrohungen und einschlägige ausländische Erfahrungen mit Kriminalität und Kriminalitätsbekämpfung; Hintergründe der Kriminalitätsentwicklung. Die Referate und Diskussionsbeiträge dieses zweiten Forums Datenschutz sind wiederum in Buchform erschienen.

Der Datenschutz nimmt an den langfristigen Entwicklungen in Staat und Gesellschaft teil. Er kann sie hie und da beeinflussen, er kann sie aber nicht umdrehen: Daß wir auf absehbare Zeit mit wirtschaftlichen Schwierigkeiten und in Verbrechensfurcht leben müssen, führt zu Einschränkungen bei der Gewährleistung der informationellen Selbstbestimmung der Bürger. Die Datenschützer können das beklagen und monieren, sie können es aber, wie sich zeigt, nicht verhindern. Darauf müssen sie sich theoretisch und pragmatisch einstellen.

Was bleibt, sind der Kampf um Kontrollfreiheit im Kernbereich des Rechts auf Privatheit, etwa bei der Wohnung, und der Versuch, die Kontrollbedürfnisse ansonsten so zu lenken, daß sie die Persönlichkeitsrechte der Bürgerinnen und Bürger möglichst wenig beschädigen. Ob dieser Versuch gelingt, hängt freilich nicht nur von globalen Entwicklungen in Staat und Gesellschaft, sondern häufig auch von scheinbaren Nebensächlichkeiten ab, wie etwa der frühzeitigen Beteiligung des Datenschutzbeauftragten an Entscheidungen und Planungen, die auch den Datenschutz betreffen. Datenverarbeitung in der Schule (Ziff. 12.2) und Korruptionsbekämpfung in der Landesverwaltung (Ziff. 20) sind Beispiele dafür, wie der Datenschutz, wenn richtig geplant und entschieden wird, Zielerreichung nicht bremst, sondern fördert.

W.H.

2. Verfassungsschutz: Entwurf eines Gesetzes über Sicherheitsüberprüfungen von Angehörigen des öffentlichen Dienstes

Nach meinen Erfahrungen mit der Prüfung von Akten über die Sicherheitsüberprüfung von Angehörigen des öffentlichen Dienstes beim Landesamt für Verfassungsschutz, von der ich im letzten Tätigkeitsbericht (21. Tätigkeitsbericht, Ziff. 2) berichtet habe, hatte ich erneut eine gesetzliche Grundlage für die Sicherheitsüberprüfung angemahnt. Erfreulicherweise begann das Hessische Ministerium des Innern und für Europaangelegenheiten im März 1993 mit der Erarbeitung eines Gesetzentwurfs. Ich wurde dabei von Anfang an beteiligt.

Grundlage der Diskussion war der Entwurf der Bundesregierung für ein Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes (SÜG, BRDrucks. 97/93 v. 12. Februar 1993), den ich im letzten Tätigkeitsbericht (21. Tätigkeitsbericht, Ziff. 2.2) erwähnte, sowie die im Bundesrat gestellten Anträge des Landes Hessen zu diesem Entwurf.

Der nunmehr vorliegende Entwurf des Ministeriums (Hessisches Sicherheitsüberprüfungsgesetz (HSÜGE), Stand 5. November 1993) enthält gegenüber dem Entwurf der Bundesregierung unter datenschutzrechtlichen Gesichtspunkten eine Reihe von Verbesserungen. Einige sollen hier genannt werden:

– Nach dem Gesetzentwurf des Bundes ist die Erhebung von Informationen über eine Vielzahl von Personen vorgesehen, die zum Umfeld der zu überprüfenden Person gehören, z. B. des Ehegatten, Verlobten, Lebenspartners, der leiblichen Eltern, Stief- und Pflegeeltern sowie der im Haushalt lebenden Personen über 18 Jahren. Dieser Personenkreis ist im hessischen Entwurf erheblich reduziert worden; beibehalten wurde er nur noch für die Sicherheitsüberprüfung von Bewerbern und Mitarbeitern des Landesamts für Verfassungsschutz. Nach dem Entwurf des Hessischen Sicherheitsüberprüfungsgesetzes ist der Betroffene (soweit es nicht um eine Tätigkeit beim Landesamt für Verfassungsschutz geht) nunmehr nur noch zur Angabe von Daten über den Ehegatten, also nicht des Verlobten und Lebenspartners, verpflichtet (§ 13 Abs. 1, 2 HSÜGE). Zu dem Ehegatten führt das Landesamt für Verfassungsschutz – vorausgesetzt, er stimmt zu – eine Abfrage des nachrichtendienstlichen Informationssystems der Verfassungsschutzbehörden (NADIS) durch. Nur für den Fall, daß in NADIS Informationen zum Ehegatten enthalten sind, können über ihn – wiederum unter der Voraussetzung seiner Zustimmung – weitere Informationen bei einzelnen im Gesetz genannten Stellen erhoben werden (§ 2 Abs. 2,3 HSÜGE).

Darüber hinaus bleibt es dabei – wie im Bundesentwurf vorgesehen –, daß der Betroffene ab der Überprüfungsart „Geheim" zwei Auskunftspersonen zur Identitätsüberprüfung und ab „Streng Geheim" drei Referenzpersonen anzugeben hat (§ 13 Abs. 1 Nrn. 15, 16 HSÜGE). Auch zu diesen Personen erfolgt – mit deren Zustimmung – ein Abgleich mit NADIS. Weitere Maßnahmen dürfen gegenüber diesen Personen nicht ergriffen werden.

– Im hessischen Entwurf werden die Rechte des Betroffenen verbessert, sich zu den vom Landesamt für Verfassungsschutz zusammengetragenen Anhaltspunkten, die ein Sicherheitsrisiko begründen, zu äußern. Neu ist auch, daß dieses Anhörungsrecht auf den Ehegatten, bei dem derartige Anhaltspunkte bestehen, erstreckt wird (§ 6 Abs. 1, 2 HSÜGE).

– Erweitert wird gegenüber dem Bundesentwurf das Recht des von der Sicherheitsüberprüfung Betroffenen, Angaben zu verweigern, wenn dies für ihn oder nahe Angehörige bestimmte Nachteile, wie z. B. eine strafrechtliche Verfolgung, begründen würde (§ 13 Abs. 5 HSÜGE).

– Der Entwurf der Bundesregierung geht bei der Speicherung von Daten, die im Rahmen der Sicherheitsüberprüfung gewonnen worden sind, in automatisierten Dateien über den status quo hinaus. Automatisierte Dateien sind dort sowohl für die Speicherung bei der zuständigen Behörde, also der Stelle, die dem Betroffenen die sicherheitsempfindliche Tätigkeit zuweist, als auch bei der mitwirkenden Behörde, nämlich dem Landesamt für Verfassungsschutz, vorgesehen. Die Verfassungsschutzbehörden dürfen neben der bereits jetzt erfolgenden Speicherung von Daten des Betroffenen und des in die Sicherheitsüberprüfung einbezogenen Ehegatten in NADIS eigene Amtsdateien führen. Im Unterschied zu NADIS, das einen begrenzten Datensatz enthält und hauptsächlich als Aktennachweissystem dient, handelt es sich nach dem Bundesentwurf um sog. Textdateien, in die z. B. auch über den Betroffenen gesammelte „sicherheitserhebliche Erkenntnisse" aufgenommen werden können. Das Landesamt für Verfassungsschutz Hessen verfügt derzeit nach meinen Informationen nicht über derartige Textdateien im Bereich der Sicherheitsüberprüfung. Die Erforderlichkeit derartiger Dateien wurde bisher auch nicht vom Landesamt für Verfassungsschutz dargelegt. Deshalb habe ich zumindest darauf gedrungen, daß im Gesetz selbst noch nicht die Entscheidung über derartige Dateien getroffen wird, sondern es dazu einer Rechtsverordnung des Ministeriums bedarf.

– Nicht durchgesetzt habe ich mich mit der Forderung, die im Rahmen der Sicherheitsüberprüfung gesammelten Informationen einer strengen Zweckbindung zu unterwerfen. Nach meiner Auffassung dürfen Informationen, die im Unterschied zu den anderen Aufgabenbereichen des Verfassungsschutzes zu vollkommen unverdächtigen Personen erhoben werden, über die Sicherheitsüberprüfung hinaus nur für eng umgrenzte Zwecke, z. B. die Spionageabwehr, genutzt werden. Dabei ist zu berücksichtigen, daß es keinesfalls nur um solche Daten geht, die vom Betroffenen selbst stammen, sondern im großen Umfang um Informationen, die bei anderen Stellen erhoben werden und die dem Betroffenen im einzelnen nicht bekannt sind. Der hessische Gesetzentwurf läßt Nutzung und Übermittlung für Zwecke der Verfolgung bestimmter Straftaten, der disziplinarrechtlichen Verfolgung sowie dienst- und arbeitsrechtlicher Maßnahmen sowie praktisch für alle Zwecke, die der Verfassungsschutz von seiner Aufgabenstellung her verfolgt, zu. Positiv anzumerken ist, daß der hessische Entwurf den im Entwurf der Bundesregierung verwandten Begriff der „Straftaten von erheblicher Bedeutung" jedenfalls präzisiert. Auch bei meiner Forderung, daß die Aufbewahrung von beispielsweise strafrechtlichen Verurteilungen beim Landesamt für Verfassungsschutz nicht zu einer Umgehung des in § 51 BZRG vorgesehenen Verwertungsverbots führen darf, kam man mir ein Stück entgegen (§ 21 Abs. 4 Satz 5 HSÜGE):

Nach Ablauf der im Bundeszentralregister festgelegten Fristen dürfen derartige Unterlagen nicht mehr für andere Zwecke als die der Sicherheitsüberprüfung genutzt werden.

3. Ausländerrecht

3.1
Automatisierte Datenverarbeitung bei den Ausländerbehörden (LADIVA)

Im letzten Tätigkeitsbericht (vgl. 21. Tätigkeitsbericht, Ziff. 3.1.2) hatte ich darauf hingewiesen, daß in den Ausländerbehörden die Verwaltung der Ausländerdaten zunehmend automatisiert erfolgt. Mittlerweile bieten alle fünf Kommunalen Gebietsrechenzentren (KGRZ) in Hessen unter Federführung des KGRZ Frankfurt das sog. LADIVA an. Dieses Verfahren haben die hessischen Kommunalen Gebietsrechenzentren von der Datenzentrale Baden-Württem-

berg fast unverändert übernommen. Ein großer Teil der Ausländerbehörden der hessischen Städte bzw. Kreise sind bereits an LADIVA angeschlossen und arbeiten damit.

Mit LADIVA können verschiedene bei den Ausländerämtern anfallende Aufgaben automatisationsunterstützt abgewickelt werden. Das Verfahren erfüllt beispielsweise folgende Funktionen:

- Es ersetzt die Karteikarte bei der Ausländerbehörde;
- es erledigt den Mitteilungsdienst zum Ausländerzentralregister;
- durch den Anschluß an das Einwohnerwesen sichert es die maschinelle Aufnahme von Mitteilungen der Meldebehörden;
- es gewährleistet die Terminüberwachung durch maschinelle Fristenkontrolle;
- es erleichtert die Abwicklung von Wiedervorlagen;
- es sorgt bundesweit für die Erledigung von Aktenanforderungsschreiben;
- es erstellt Gebührenbescheide durch den Anschluß an das automatisierte Finanzwesen.

Die Ausländerakte, in der z. B. Verfügungstexte abgelegt werden und die bei Bedarf an eine andere Ausländerbehörde verschickt werden muß, wird nicht ersetzt.

Im letzten Tätigkeitsbericht (vgl. 21. Tätigkeitsbericht, Ziff. 3.1.2) hatte ich das Problem angesprochen, daß im Rahmen von LADIVA Daten gespeichert werden, die nicht in der zu § 80 Ausländergesetz (AuslG) ergangenen Ausländerdateienverordnung (AuslDatVO) enthalten sind.

Ich halte dies deshalb für problematisch, weil es sich bei den ausländerrechtlichen Vorschriften um abschließende Regelungen handelt. Dafür spricht zweifelsfrei der Wortlaut der Vorschrift, aber auch die Begründung zur Ausländerdateienverordnung.

Der Bundesminister des Innern sowie die Ausländerreferenten der Länder vertreten hingegen die Auffassung, daß die ausländerrechtlichen Vorschriften nur die Verpflichtung der Länder zur Führung der gesamten Dateien mit dem in der Verordnung geregelten Mindestdatensatz bezwecken.

Anläßlich eines Informationsbesuchs beim KGRZ Wiesbaden habe ich zwischenzeitlich feststellen können, daß ein Teil der – aus meiner Sicht ohne Rechtsgrundlage erfolgenden – Datenspeicherungen anders als noch im Anwenderhandbuch zu LADIVA vorgesehen, nicht mehr vorgenommen wird.

Bedenken habe ich nach wie vor hinsichtlich des für verschiedene Datensätze vorgesehenen Freifelds für „Bemerkungen". Hier kann immerhin über zwei Zeilen hinweg ein beliebiger Text eingefügt werden; beispielsweise die Aussage „Achtung, schwieriger Fall".

Abgesehen davon, daß für diese Speicherung keine Rechtsgrundlage existiert, halte ich die Zulassung derartiger Freitexte für problematisch. Diese nach dem subjektiven Empfinden des Bearbeiters vorgenommenen Speicherungen können in verkürzter Form negative Aussagen über den Betroffenen enthalten, die zu einer Voreingenommenheit des Bearbeiters gegenüber dem Ausländer führen können. Der mit diesem Text verfolgte Zweck, den Bearbeiter auf bestimmte Umstände aufmerksam zu machen, kann auch auf andere Weise erfüllt werden, beispielsweise durch den Zusatz: „Akte hinzuziehen". Auf diese Weise würde jedenfalls sichergestellt, daß der Bearbeiter den gesamten Akteninhalt zur Kenntnis nimmt und sich nicht mit subjektiven – evtl. verkürzten – Wertungen zufrieden gibt. Ich werde mich deshalb dafür einsetzen, daß die Speicherung von „Bemerkungen" ausgeschlossen oder aber auf einen festgelegten Zusatz beschränkt wird.

3.2
Verwaltungsvorschriften zu §§ 75 bis 77 Ausländergesetz

In den letzten beiden Tätigkeitsberichten (20. Tätigkeitsbericht, Ziff. 5.1; 21. Tätigkeitsbericht, Ziff. 3.1.1) hatte ich kritisiert, daß der Bundesminister des Innern – entgegen der Verpflichtung nach § 104 Ausländergesetz (AuslG) – keine allgemeinen Verwaltungsvorschriften zur Konkretisierung des Gesetzes geschaffen hat. Daran hat sich bis heute, mehr als drei Jahre nach Inkrafttreten des Ausländergesetzes, nichts geändert. Für die Datenverarbeitungsregelungen in § 75 ff. AuslG ist das Bundesministerium des Innern über einen ersten Entwurf für „vorläufige Anwendungshinweise" vom 25. Februar 1991 nicht hinausgekommen.

Um so wichtiger erschien es deshalb, daß das Hessische Ministerium des Innern und für Europaangelegenheiten – solange der Bundesminister des Innern untätig bleibt – eigene Verwaltungsvorschriften für Hessen in Kraft setzt.

Alles begann erfolgversprechend: Das Amt für multikulturelle Angelegenheiten in Frankfurt berief im Sommer 1991 eine Arbeitsgruppe ein, an der neben Richtern, Anwälten und Vertretern von Ausländerberatungseinrichtungen auch ein Vertreter des Hessischen Ministeriums des Innern und für Europaangelegenheiten und meiner Dienststelle teilnahmen. Der Vertreter des Ministeriums versprach, die in der Arbeitsgruppe zusammengetragenen Anforderungen

in einen Erlaß umzusetzen. Nachdem fast ein Jahr lang nichts geschah, formulierten Mitglieder der Arbeitsgruppe im Juni 1992 einen Entwurf für Verwaltungsvorschriften, der dem Hessischen Ministerium des Innern und für Europaangelegenheiten mit der Bitte übersandt wurde, die Umsetzung alsbald zu veranlassen. Auf meine wiederholten Nachfragen versicherte mir der zuständige Vertreter des Ministeriums immer wieder, der Entwurf würde alsbald ohne große Änderungen als Verwaltungsvorschrift in Kraft gesetzt. An diese Zusage hielt sich das Ministerium allerdings in zweifacher Hinsicht nicht:

Zum einen dauerte es noch einmal fast ein Jahr, bis das Ministerium im Juli 1993 überhaupt aktiv wurde.

Zum anderen weicht der nun vorgelegte Entwurf in wichtigen Positionen von dem Ergebnis der Arbeitsgruppe ab. Einige dieser Änderungen sollen hier genannt werden:

- Der Grundsatz, daß Erkenntnisse, die öffentliche Stellen ausschließlich im Rahmen einer Auskunfts- und Beratungstätigkeit gewinnen, nicht zu übermitteln sind, wird aufgegeben.
- Eine Übermittlungspflicht ist nicht mehr dann ausgeschlossen, wenn es Anhaltspunkte dafür gibt, daß die Aufgabenerfüllung der öffentlichen Stelle gefährdet wird. Gedacht ist hier an Fälle, in denen der Ausländer – wenn er mit der Weitergabe von Informationen durch die Stelle, an die er sich wendet, rechnen muß – dieser nicht mehr das erforderliche Vertrauen entgegenbringen kann.
- Die Mitteilung bestimmter Ausweisungsgründe an die Ausländerbehörde erfolgt auch dann, wenn abzusehen ist, daß der Ausländer aus anderen Gründen, beispielsweise weil er eine Aufenthaltsberechtigung besitzt oder wenn er mit einem deutschen Familienangehörigen in familiärer Gemeinschaft lebt (§ 48 AuslG), im Einzelfall überhaupt nicht mehr ausgewiesen werden kann.

Das Hessische Ministerium des Innern und für Europaangelegenheiten vertritt nunmehr die Auffassung, daß die früher erarbeiteten Regelungen nicht mit den Vorschriften des Ausländergesetzes vereinbar sind. Ich bin hingegen der Meinung, daß die Datenverarbeitungsregelungen des Ausländergesetzes einen derartigen Spielraum zulassen, der auch ausgeschöpft werden sollte.
In den Gesprächen mit dem Ministerium habe ich mich mit dieser Auffassung nicht durchsetzen können. Werden die Verwaltungsvorschriften – so wie im Entwurf vorgesehen – in Kraft gesetzt, ergeben sich unter datenschutzrechtlichen Gesichtspunkten keine wesentlichen Verbesserungen gegenüber den „vorläufigen Anwendungshinweisen" des Bundesministers des Inneren.

3.3
Höhere Kontrolldichte für Ausländer

Neben den großen Gesetzgebungen der letzten Jahre, den Novellierungen des Ausländergesetzes und des Asylverfahrensgesetzes, die sich nachhaltig auf die Stellung der ausländischen Bürger in der Bundesrepublik auswirken, finden sich in anderen, ganz unterschiedliche Materien betreffenden, Gesetzen Sonderbestimmungen für Ausländer. Diese führen u.a. dazu, daß die öffentliche Verwaltung an das Verhalten von Ausländern höhere Anforderungen stellt als an das Verhalten von deutschen Bürgern. Gerade auch in diesen weniger spektakulären Bereichen verfolge ich kritisch, inwieweit das ausländischen Bürgern in gleicher Weise garantierte Recht auf informationelle Selbstbestimmung gewahrt wird. Ich möchte zwei Beispielsfälle aus dem Berichtszeitraum herausgreifen:

3.3.1
Zusammenschluß von Ausländern in Vereinen

Deutsche Bürger genießen in vollem Umfang das in Art. 9 Abs. 1 Grundgesetz (GG) verankerte Recht, Vereine zu bilden, und können dies unterhalb der Schwelle einer Verbotsverfügung, die allein unter den Voraussetzungen des Art. 9 Abs. 2 GG in Frage kommt, frei von staatlicher Reglementierung tun.

Vereine, in denen sich Ausländer zusammenschließen, können nach den §§ 14, 15 Vereinsgesetz (VereinsG) zusätzlich zu den Voraussetzungen des Art. 9 Abs. 2 GG auch dann verboten werden, „wenn sie durch politische Betätigung die innere oder äußere Sicherheit, die öffentliche Ordnung oder sonstige erhebliche Belange der Bundesrepublik Deutschland oder eines ihrer Länder verletzen oder gefährden". Hinzu kommt, daß die Durchführungsverordnung zum Vereinsgesetz (VereinsG-DVO) für Ausländervereine (Vereine, deren Mitglieder oder Leiter sämtlich oder überwiegend Ausländer sind) und ausländische Vereine (Vereine mit Sitz im Ausland, deren Organisation oder Tätigkeit sich auf den Geltungsbereich des Vereinsgesetzes erstreckt) Anmelde- und Auskunftspflichten vorsieht (§§ 19 bis 21). Danach sind in der Anmeldung derartiger Vereine beispielsweise Angaben zu machen über die Satzung, den Namen und die Anschriften der Vorstandsmitglieder oder zur Vertretung berechtigter Personen. Diese Vereine haben den zuständigen Behörden Auskunft zu geben über ihre Tätigkeit und, soweit sie sich politisch betätigen, über die Namen und Anschriften ihrer Mitglieder und über die Herkunft und Verwendung ihrer Mittel.

Ich habe festgestellt, daß die Regierungspräsidien als zuständige Behörden Durchschriften dieser Anmelde- und Auskunftsformulare sowohl an das Bundesverwaltungsamt als auch an das Landeskriminalamt (LKA) übermitteln. Beide Behörden erhalten damit detaillierte Angaben über alle Vereine, die in Hessen von Ausländern gegründet wurden oder deren Organisation oder Tätigkeit sich auf Hessen erstreckte. Ich kann nicht erkennen, weshalb das LKA derartige Informationen zur Erfüllung seiner Aufgaben benötigen sollte. Allein die Möglichkeit, daß eine

derartige Information im Einzelfall einmal von Interesse sein könnte, reicht jedenfalls nicht aus. Für die Übermittlung an das LKA besteht – anders als für die Übermittlung an das Bundesverwaltungsamt – auch keine ausreichende Rechtsgrundlage.

Das Hessische Ministerium des Innern und für Europaangelegenheiten teilte meine Auffassung und wies mit Datum vom 13. April 1993 die Regierungspräsidien und das LKA an, die bisherige Praxis einzustellen. Die bereits beim LKA gesammelten Anmelde- und Auskunftsformulare wurden vernichtet.

3.3.2
Zulassung von Kraftfahrzeugen durch Ausländer

Bei der Zulassung eines Kraftfahrzeuges benötigt die Kraftfahrzeugzulassungsstelle für ihre Aufgabenerfüllung verschiedene Auskünfte und Nachweise vom Fahrzeughalter. Er muß beispielsweise Angaben machen, die es der Zulassungsstelle ermöglichen, ihr Zulassungsregister zu führen (§ 33 Straßenverkehrsgesetz (StVG)) sowie zur Durchführung des Kraftfahrzeugsteuergesetzes mit Finanzämtern (§ 9 FRV) oder des Gesetzes über die Pflichtversicherung für Kfz-Halter (PflVG) mit Kraftfahrzeugversicherungen (§ 8 FRV) Daten auszutauschen. Dabei Unterschiede zu machen zwischen Deutschen und Ausländern, ist sachlich nicht geboten; die Straßenverkehrsvorschriften sehen auch solche Unterscheidungen nicht vor.

Der Verband der Kraftfahrzeugzulassungsdienste e.V. Wiesbaden wandte sich an mich, weil ihm von seinen Mitgliedern berichtet worden war, einige Zulassungsstellen würden von Ausländern mehr Daten erheben und speichern als von Deutschen. Teilweise würden Zusatzformulare verwendet, auf denen die Staatsangehörigkeit, Aufenthaltsgenehmigung und Heimatanschrift sowie die Paßnummer, Paßausstellungsdatum und Paßausstellungsbehörde erhoben würden.

Ich teilte dem Verband die Rechtslage mit: § 34 StVG regelt die Erhebung von Daten bei der Zuteilung oder Ausgabe von Kraftfahrzeugkennzeichen. Er bestimmt u.a., daß derjenige, der die Zuteilung oder die Ausgabe eines Kennzeichens für ein Fahrzeug beantragt, der zuständigen Stelle hierfür die nach § 33 Abs. 1 Satz 1 Nr. 2 StVG zu speichernden Halterdaten mitzuteilen und auf Verlangen nachzuweisen hat. § 33 Abs. 1 Satz 1 Nr. 2 StVG nennt die Daten, welche die Zulassungsstelle in ihrem Fahrzeugregister speichern darf. Diese sind bei natürlichen Personen: Familienname, Geburtsname, Vorname, vom Halter für die Zuteilung oder die Ausgabe des Kennzeichens angegebener Ordens- oder Künstlername, Tag und Ort der Geburt, Geschlecht und Anschrift. Keine Bedenken habe ich, wenn die Zulassungsstellen noch über die genannten Daten hinaus, zur Dokumentation, wie die gespeicherten Daten nachgewiesen wurden, die Paßnummer (bei Ausländern wie Deutschen) notiert. Weitere Daten dürfen weder erhoben noch gespeichert werden.

Kurz darauf erhielt ich einen Brief vom Oberbürgermeister der Stadt Frankfurt. Er bezog sich auf mein Schreiben an den Verband und verteidigte die Ungleichbehandlung zwischen Deutschen und Ausländern. Der Nachweis einer gültigen Aufenthaltserlaubnis sei zwingend notwendig, um zu verhindern, daß eine Zulassung an eine Person erfolgt, die sich illegal oder mit Touristenvisum in der Bundesrepublik aufhält. Denn solche Fälle endeten in der Regel damit, daß die Zulassungsstelle Fahndungsmaßnahmen wegen nicht entrichteter Steuern und Versicherungsbeiträge einleiten müsse. Der Nachweis der Meldeanschrift genüge in diesen Fällen nicht, da zumindest in Großstädten von vielen Scheinanmeldungen ausgegangen werden müsse. Auch bei Asylbewerbern sei eine Einsichtnahme in die Aufenthaltserlaubnis zur Prüfung der Gültigkeit und des Aufenthaltsbereichs erforderlich.

Diese Auffassung ist falsch. Zwar ist nichts dagegen einzuwenden, wenn Ausländer, die ihre Wohnanschrift nicht, wie Deutsche, durch Vorlage eines Personalausweises nachweisen können, der Zulassungsstelle Einsicht in die Aufenthaltsgenehmigung gewähren. Wahlweise ist es aber auch immer möglich, statt der Gewährung der Einsicht in die Aufenthaltserlaubnis den Wohnsitz durch Vorlage einer Meldebescheinigung nachzuweisen. Außerdem können die Zulassungsstellen, sofern sie über die entsprechenden technischen Einrichtungen verfügen, die erforderlichen Daten aus dem Melderegister direkt abrufen (§ 15 Meldedatenübermittlungsverordnung) und auf die Vorlage einer Wohnsitzbescheinigung bei Deutschen wie Ausländern verzichten.

Es ist nicht Aufgabe der Zulassungsstelle, im Zusammenhang mit einer Kraftfahrzeugzulassung bei Ausländern die Gültigkeit der Aufenthaltserlaubnis zu prüfen. Weshalb sollten Asylbewerber keine Kraftfahrzeuge zulassen dürfen? Selbstverständlich dürfen auch Touristen unter bestimmten Bedingungen Fahrzeuge zulassen. Der Status eines Ausländers, selbst dessen Staatsangehörigkeit, ist für die Zulassung eines Kraftfahrzeuges unerheblich.

Nachdem ich den Hessischen Minister für Wirtschaft, Verkehr und Technologie eingeschaltet hatte, stellte dieser in einem Erlaß vom 2. April 1993 (IV b 2-66 l 06.111.02 n.v.) an alle hessischen Zulassungsstellen u.a. klar, daß eine Erhebung oder Speicherung von Daten, wie etwa die Heimatanschrift, Staatsangehörigkeit und Aufenthaltserlaubnis, durch die Zulassungsstellen nicht erfolgen darf.

4. Polizei

4.1
Datenverarbeitung bei der Polizei; das Projekt HEPOLAS

4.1.1
Der bisherige Projektablauf von HEPOLAS

Vor mehreren Jahren hat die hessische Polizei Überlegungen angestellt, wie ihre Datenverarbeitung in der Zukunft aussehen soll. Als ein wesentlicher Baustein wurde die Automatisierung der polizeilichen Vorgangsbearbeitung in

Angriff genommen. Hierzu wurde das Projekt HEPOLAS (Hessisches Polizeiarbeitsplatzsystem) begonnen. Als Generalunternehmer wurde im Dezember 1989 die Firma Siemens ausgewählt.

Nachdem das Projekt nicht die gewünschten Ergebnisse zeigte, wurde die Zusammenarbeit mit der Firma Siemens 1992 beendet, und die hessische Polizei übernahm die alleinige Projektleitung. Die Gründe hierfür sollen an dieser Stelle nicht dargestellt werden; weitergehende Informationen sind der LTDrucks. 13/2462 zu entnehmen.

Am 6. Juli 1993 wurde der Grundausbau HEPOLAS in Hofheim als erstem Polizeirevier in Betrieb genommen. Weitere Polizeidienststellen werden in rascher Folge ebenfalls entsprechend ausgestattet. Die derzeit gültige Konzeption geht von einer schrittweisen Einführung von HEPOLAS aus. Nach dem Grundausbau soll, beginnend ab Mitte 1994, mit den Stufen 1.1 und 1.2 die Vorgangsbearbeitung von Strafsachen den ersten Polizeidienststellen zur Verfügung stehen. Die programmtechnische Realisierung dieser Stufen findet z.Zt. statt.

4.1.2
Konzeption des Grundausbaus HEPOLAS

4.1.2.1
Technik

Die eingesetzte Technik entspricht der des Gesamtsystems HEPOLAS. Im Endausbau sollen ca. 200 Dienststellen mit etwa 3000 Arbeitsplätzen ausgestattet sein.

An den Arbeitsplätzen werden X-Terminals (Bildschirme mit besonderen Fähigkeiten im Bereich der Grafik) und Laserdrucker installiert.

Das Rechnernetz soll 3-stufig hierarchisch gegliedert werden. Die unterste lokale Ebene bilden Standortrechner, an denen die Terminals angeschlossen werden. Die Standortrechner sind mit dem zugeordneten Regionalrechner der nächsten Ebene verbunden. Die Regionalrechner sind schließlich an den Zentralrechner des Landeskriminalamts angeschlossen.

Auf lokaler und regionaler Ebene wird als Betriebssystem UNIX eingesetzt. Die eingesetzte UNIX-Version ist System V Release 4 mit der Option, auf eine Version mit einer höheren Sicherheitsstufe zu wechseln. Die Vernetzung soll über ein privates X-25-Netz erfolgen.

4.1.2.2
Funktionalität

Im Grundausbau besteht HEPOLAS aus den Komponenten „Textverarbeitung" und „Formularerfassung und -ausgabe". Die Komponenten basieren auf der Bürokommunikationssoftware UNIPLEX. Zur Gewährleistung der Zugriffskontrolle wird eine spezielle Schutzsoftware eingesetzt.

Grundsätzlich werden bei der Formularbearbeitung die Daten zu einem Vorgang, die bisher manuell in mehrere Formulare eingetragen werden mußten, am Arbeitsplatz einmal erfaßt. Es erfolgt sofort der Ausdruck aller zugehörigen Formulare mit anschließender Löschung der Daten. Eine Speicherung findet nur temporär während der Erfassung und des Drucks statt.

Eine Zwischenspeicherung von Daten ist vorgesehen, wenn ein Formular nicht vollständig ausgefüllt werden konnte. In diesem Fall werden die bekannten Daten erfaßt. Nach Ergänzung der fehlenden Angaben werden die Formulare wie gewohnt ausgedruckt und die Daten gelöscht. Um eine dauerhafte Speicherung unvollständiger Angaben zu verhindern, wurde eine maximale Speicherdauer festgelegt. Wird diese überschritten, so kommt es zur zwangsweisen Löschung der Daten.

Eine Datenspeicherung erfolgt daher nur zeitlich befristet in wenigen Fällen. Es findet, außer für den Formulardruck, keine Verarbeitung statt.

Im Rahmen der Textverarbeitung ist die Speicherung personenbezogener Daten wahrscheinlich. Durch die Schutzsoftware werden unberechtigte Zugriffe soweit möglich unterbunden. Da nach dem Ausdruck die Schriftstücke gelöscht oder anonymisiert werden, ist das Risiko tolerierbar.

4.1.2.3
Datenschutzrechtliche Bewertung

Die Beschreibung der Funktionalität läßt klar erkennen, daß der Grundausbau von HEPOLAS noch kein Vorgangsbearbeitungssystem ist. In Anbetracht der einfachen Funktionen und der nur eingeschränkten Speicherung personenbezogener Daten hatte ich keine Bedenken gegen den HEPOLAS-Grundausbau.

4.1.2.4
Gründe für den Einführung des Grundausbaus

Obwohl der Grundausbau HEPOLAS mit dem ursprünglich geplanten System zur Vorgangsbearbeitung erst wenige Funktionen gemeinsam hat, gibt es gute Gründe für die Einführung mit dem jetzigen Funktionsumfang:

- Die tägliche Arbeit wird erleichtert (vgl. 4.6).
- Die Mitarbeiter werden an die Technik herangeführt, so daß sie sich in den späteren Phasen auf die neue Anwendung konzentrieren können.
- Probleme aus dem Aufbau der technischen Infrastruktur werden von anwendungsspezifischen Problemen getrennt.

Dieser Ansatz ist begrüßenswert.

4.1.3
Einbeziehung des Hessischen Datenschutzbeauftragten in das Projekt HEPOLAS

Im Laufe der letzten Jahre fanden mehrere Informationsgespräche statt, in denen ich bereitwillig und offen über den Stand des Projekts informiert wurde. Um das Bild der Planungen zu vervollständigen, wurde mir Anfang 1992 auch die aktuell vorhandene Dokumentation zugeleitet.

Die Dokumentation, nach der die Stufen 1.1 und 1.2 von HEPOLAS endgültig realisiert werden, erhielt ich einen Monat vor dem Redaktionsschluß zu diesem Tätigkeitsbericht im Oktober 1993. Meine Prüfung wird anhand dieser Unterlagen erfolgen. Ich gehe davon aus, daß Anforderungen des Datenschutzes an das Verfahren, falls solche erhoben werden, trotz des schon fortgeschrittenen Projektstandes umgesetzt werden.

Im Bereich des technischen Datenschutzes wird derzeit mit Unterstützung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) ein Datensicherheitskonzept erarbeitet. Die Umsetzung des Konzepts soll dann die Anforderungen des § 10 Hessischen Datenschutzgesetzes bezüglich der Datensicherungsmaßnahmen erfüllen. Ich begleite dieses Teilprojekt direkt in der Projektgruppe.

4.2
Novellierung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung

Die Furcht vor organisierter Kriminalität, aber auch die Zunahme der Alltagskriminalität haben unser Polizeirecht in letzter Zeit entscheidend verändert und verschärft. Fundamentale Prinzipien gelten nicht mehr oder nur noch eingeschränkt:

- die Trennung von Polizeiarbeit und Strafverfolgung, d.h. von Prävention und Repression;
- die Konzentration von Maßnahmen auf den Störer;
- die grundsätzliche Offenheit von Ermittlungen.

Gerade in der letzten Zeit hat die Polizei in großem Umfang die gesetzlichen Zwangsmittel bekommen, die sie zuvor jahrelang vergeblich eingefordert hatte: Datenerhebung durch langfristige polizeiliche Observation und den Einsatz technischer Mittel, Datenermittlung durch Einsatz von V-Personen und verdeckten Ermittlern, Datenabgleich oder Rasterfahndung und Ausschreibung zur polizeilichen Beobachtung.

Die genannten Verschärfungen der polizeilichen Eingriffsrechte haben zu entscheidenden Veränderungen unserer rechtsstaatlichen Tradition in diesem Bereich geführt. Die vorbeugende Verbrechensbekämpfung als Ziel polizeilichen Handelns ebnet den Unterschied von Prävention und Repression, von Gefahrenvorsorge und Verbrechensbekämpfung ein, der bislang Polizei- und Strafprozeßrecht auseinandergehalten hat. Die neuen Ermittlungsmethoden erstrecken sich zwangsläufig auf unbeteiligte Dritte, was bislang nur ausnahmsweise der Fall war. Die Einbeziehung sog. „Kontaktpersonen" zielt sogar darauf ab. Alle diese Mittel werden heimlich eingesetzt; bislang waren Ermittlungen grundsätzlich offen, schon damit der Betroffene sich rechtzeitig zur Wehr setzen konnte. Gerade vor diesem Hintergrund ist es von äußerster Wichtigkeit, daß die Fälle, in denen diese Mittel zum Einsatz kommen, klar eingegrenzt sind und daß die auf diese Weise erhobenen Daten strengen Zweckbindungen unterliegen. Bereits im 19. Tätigkeitsbericht (Ziff. 7.1.1, 7.2.2) hat mein Vorgänger im Amt kritisiert, daß das geltende Recht diesen Anforderungen nicht entspricht.

Der Entwurf der Landesregierung für ein Gesetz zur Änderung des Hessischen Gesetzes über die öffentliche Sicherheit und Ordnung (HSOGE, LTDrucks. 13/4670) versucht nunmehr, die rechtsstaatlich gebotene Eingrenzung der Befugnis der Polizei zur Erhebung personenbezogener Daten durch Observation und die Verwendung technischer Mittel sowie durch den Einsatz von V-Personen und verdeckt ermittelnden Personen zu erreichen.

4.2.1
Positive Ansätze

Der Entwurf ersetzt den Begriff der „Straftat mit erheblicher Bedeutung", bei der die genannten Ermittlungsmethoden zum Einsatz kommen dürfen, durch einen Straftatenkatalog (§§ 15 Abs. 2 Nr. 2 HSOGE). Aus verfassungsrechtlichen Gründen und unter Gesichtspunkten der Normenklarheit halte ich dies für eine wesentliche Verbesserung.

Für den Einsatz von verdeckt ermittelnden Personen mit einer auf Dauer angelegten Legende sieht der Entwurf die richterliche Anordnung vor (§ 16 Abs. 5 HSOGE). Die Datenerhebung durch verdeckte Ermittler stellt einen beson-

ders intensiven Eingriff in das Recht auf informationelle Selbstbestimmung dar. Das im Nachhinein wirkende Korrektiv der Unterrichtung des Betroffenen wird in diesen Fällen wegen der Gefährdung der Person oder des weiteren Einsatzes des verdeckten Ermittlers häufig nicht praktisch werden. Daher halte ich den Richtervorbehalt für ein wichtiges Mittel sicherzustellen, daß die Belange des Betroffenen hinreichend berücksichtigt werden.

Zu begrüßen ist außerdem die Regelung, daß Daten, die mittels Abhören zum Zweck der Eigensicherung einer V-Person oder einer verdeckt ermittelnden Person erhoben wurden, in Zukunft zu vernichten sind, falls sie nicht zur Verfolgung einer in § 100a Strafprozeßordnung bezeichneten Straftat erforderlich sind (§ 15 Abs. 6 HSOGE).

4.2.2
Kritische Punkte

Der Entwurf sieht vor, daß für eine Observation über einen Zeitraum von mehr als drei Monaten die Zustimmung des Ministeriums des Inneren und für Europaangelegenheiten oder einer von ihm benannten Stelle erforderlich ist (§ 15 Abs. 3 HSOGE). Da hier über erhebliche Grundrechtseingriffe entschieden wird, sollte das Ministerium die Zustimmung für Observationen von mehr als drei Monaten Dauer in eigener Verantwortung treffen und nicht auf andere Stellen delegieren können, zumal wegen der geringen Zahl dieser Fälle auch keine praktische Notwendigkeit dafür besteht.

Nach dem Entwurf bedarf das Abhören zur Eigensicherung von Personen bei einem polizeilichen Einsatz auch in Wohnungen nicht der richterlichen Anordnung (§ 15 Abs. 6 HSOGE). Ich sehe keinen sachlichen Grund, in diesem Fall von dem Erfordernis der richterlichen Anordnung abzusehen.

4.3
Neue Richtlinien für kriminalpolizeiliche personenbezogene Sammlungen

Nachdem das Hessische Gesetz über die öffentliche Sicherheit und Ordnung (HSOG) mit der Datenschutznovelle vom 18. Dezember 1989 um bereichsspezifische datenschutzrechtliche Bestimmungen ergänzt worden war und aufgrund der darin enthaltenen Ermächtigung (jetzt § 27 Abs. 4 HSOG) eine Verordnung über Prüffristen bei vollzugspolizeilicher Datenspeicherung (Prüffristenverordnung vom 28. August 1990 – GVBl. 1990 S. 553ff.) in Kraft trat, hat das Landeskriminalamt (LKA) die durch Erlaßbereinigung außer Kraft getretenen KpS-Richtlinien (Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen – StAnz. 1981 S. 881ff.) neu gefaßt.

Waren früher die jetzt in der Prüffristenverordnung enthaltenen Fristen, nach denen in Dateien oder Akten gespeicherte personenbezogene Daten daraufhin zu überprüfen waren, ob eine weitere Speicherung erforderlich ist, Kernstück dieser Richtlinien, so sind es jetzt die Modalitäten über die Aufnahme und Aussonderung von Informationen in Akten und Dateien, über Datenübermittlungen an Dritte sowie Auskunfts- und Löschungsanträge der Betroffenen.

4.3.1
Aufnahme von Daten im Hessischen Polizeiinformationssystem (HEPOLIS)

– Nach § 20 Abs. 4 Nr. 4 HSOG ist eine Datenspeicherung im HEPOLIS nur zulässig, wenn die Besorgnis besteht, daß die Person, die verdächtig ist, eine Straftat begangen zu haben, weitere Straftaten begehen werde. Diese Negativprognose ist nach Ziff. 8.1 der KpS-Richtlinien nur begründet, wenn der festgestellte Sachverhalt nach kriminalistischer Erfahrung angesichts aller Umstände des Einzelfalls Anhaltspunkte für die Annahme bietet, daß die betroffene Person künftig weitere Straftaten begehen wird. Bei der Prognose sind insbesondere Art, Schwere und Begehungsweise der Straftaten, welche dieser Person zur Last gelegt werden, ihre Persönlichkeit sowie der Zeitraum, während dessen sie strafrechtlich nicht (mehr) in Erscheinung getreten ist, zu berücksichtigen.

  Kann eine Negativprognose nicht gestellt werden, z. B. weil der Verdächtige erstmals mit Strafgesetzen in Konflikt kam, erfolgt neben der Speicherung von Vorgangsverwaltungsdaten (§ 20 Abs. 8 HSOG) lediglich eine Datenspeicherung über den Fall (z. B. Tatort, Tatzeit, Delikt usw.). Statt des Namens und Vornamens des Verdächtigen wird festgehalten, welche Dienststelle zuständig ist und daß es sich um einen Ersttäter handelt.

  Wird nach dieser Person im HEPOLIS gefragt, so werden die Falldaten nicht erschlossen. Die abfragende Stelle erhält lediglich die Information, welcher Polizeibehörde Vorgangsverwaltungsdaten vorliegen. Um welche Informationen es sich dabei handelt und welcher Sachverhalt zur Anlage des Vorganges führte, darüber gibt HEPOLIS in diesem Falle keine Auskunft.

  Ich habe Zweifel, ob eine solche Verfahrensweise, die dem Abfrager diese – zugegebenermaßen erheblich verkürzte – Information zur Verfügung stellt, mit dem Gebot, Vorgangsverwaltungsdaten ausschließlich für diesen Zweck oder zur befristeten Dokumentation behördlichen Handelns zu verwenden (§ 20 Abs. 8 HSOG) noch vereinbar ist. Denn die Information über die Vorgangsverwaltungsdaten bedeutet für den Bearbeiter das Angebot, bei der zuständigen Stelle die Vorgänge anzufordern und zu dem gleichen Zweck zu verwenden wie im Fall einer Negativprognose. Ich habe das Verfahren bisher nicht beanstandet, weil ich mich dem Argument der Polizei, daß eine Bewertung, ob ein Täter ein „Episodentäter" oder ein Täter ist, der weitere Straftaten begeht, in aller Regel bei der Ersttat nicht möglich ist, verschließen kann (so der Direktor des Landeskriminalamts in der öffentlichen Anhörung zu den Gesetzentwürfen der Fraktionen für ein Gesetz zur Änderung des HSOG, Hessi-

scher Landtag, UID-12/9 vom 22. Februar 1989). Verzichtet man gänzlich auf die Speicherung der Ersttat, so stellt sich naturgemäß jedes weitere Tätigwerden immer wieder als Ersttat dar. Die Wiederholungstat ist dann als solche nicht zu erkennen. Trotzdem halte ich es für möglich, durch technische oder organisatorische Maßnahmen, z. B. differenzierte Zugriffsbefugnisse, eine bessere Berücksichtigung des Zweckbindungsgebotes des § 20 Abs. 8 HSOG zu erreichen.

- Nach Ziff. 9.1 der Richtlinien erfolgt bei festgestellt fahrlässiger Tatbegehung keine Anlage einer Kriminalakte, in bereits vorhandene Kriminalakten werden diese Vorgänge nicht aufgenommen.
- Bei Antragsdelikten ist die Anlage von Kriminalakten bzw. die Aufnahme in bereits vorhandene Kriminalakten nur zulässig, wenn die angezeigte Straftat durch die polizeilichen Feststellungen oder Ermittlungen bestätigt und entweder Strafantrag gestellt wurde oder die Staatsanwaltschaft das besondere öffentliche Interesse an der Strafverfolgung bejaht hat.
- Unterlagen über Verkehrsordnungswidrigkeiten werden nicht in kriminalpolizeiliche Sammlungen aufgenommen.

4.3.2
Datenübermittlungen aus kriminalpolizeilichen Sammlungen

Wann, zu welchen Zwecken und unter welchen Bedingungen Daten aus kriminalpolizeilichen Sammlungen übermittelt werden dürfen, regeln die §§ 20 bis 22 HSOG. Die KpS-Richtlinien übertragen die Zuständigkeit zur Übermittlung personenbezogener Daten an die Behördenleiter des Hessischen Landeskriminalamts, des Hessischen Wasserschutzpolizeiamtes, der Polizeipräsidien und -direktionen sowie bei den Regierungspräsidien an die Leiter der Dezernate Polizei bzw. Einsatzleiter der Kriminalpolizei. Zur Datenübermittlung an bestimmte Empfänger können sie die Befugnis an bestimmte Funktionsträger innerhalb der Polizeibehörde übertragen.

4.3.3
Aussonderung von Datenspeicherungen

Werden die nach der Prüffristenverordnung festgelegten Fristen erreicht, so sind die Daten zu löschen und die damit korrespondierenden Akten zu vernichten, wenn kein Anlaß für eine erneute Aufnahme in die Datei oder die Akte entstanden ist. In Ausnahmefällen kann die Frist verlängert werden; dann sind die Gründe für die Verlängerung aktenkundig zu machen. Spätestens nach zwei Jahren muß eine erneute Prüfung erfolgen.

Die KpS-Richtlinien sehen folgendes Verfahren vor: Jeder Datensatz muß – dies ist durch technische Vorkehrungen gesichert – ein nach der Prüffristenverordnung festzulegendes Aussonderungsprüfdatum enthalten. Bei mehreren Datenspeicherungen zur gleichen Person gilt das höchste Aussonderungsprüfdatum. Drei Monate vor Erreichen des höchsten Aussonderungsprüfdatums wird den aktenführenden Dienststellen vom LKA eine Liste der zu überprüfenden Datensätze übersandt. Liegen keine Gründe für die Verlängerung der Prüffristen vor, bleiben die Aussonderungsprüfdaten unverändert. Diese Datensätze werden nach drei Monaten im HEPOLIS automatisch gelöscht. Den Dienststellen werden Listen der gelöschten Datensätze übersandt. Die zugehörigen Kriminalakten sind nebst evtl. vorhandenen erkennungsdienstlichen Unterlagen zu vernichten. Vor Ablauf des Aussonderungsprüfdatums ist eine Bereinigung möglich, wenn die Polizei aus Anlaß einer Einzelfallbearbeitung feststellt, daß die Kenntnis der Daten für die speichernde Stelle zur Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist. Diese Einzelfallbearbeitung kann von den Betroffenen jederzeit veranlaßt werden.

4.4
Neukonzeption des bundesweiten Informationssystems der Polizei (INPOL)

Als Zentralstelle für das polizeiliche Auskunfts- und Nachrichtenwesen verarbeitet das Bundeskriminalamt (BKA) in bundesweiten Informationssystemen der Polizei (INPOL) personenbezogene Daten, die es in der Regel nicht selbst erhoben hat, sondern die ihm von den Polizeibehörden der Länder übermittelt worden sind.

Die Speicherung und Nutzung von Daten im INPOL-System greift in das Recht auf informationelle Selbstbestimmung vieler Bürger ein. Die Entscheidung, welchen Umfang das Informationssystem haben und wie es ausgebaut werden soll, war bisher weitgehend der Exekutive unter Ausschluß der parlamentarischen und öffentlichen Kontrolle überlassen. Denn das Gesetz über das Bundeskriminalamt enthält keine bereichsspezifischen Vorschriften über die Datenverarbeitung im INPOL-System. Trotz dieses gesetzlichen Regelungsdefizits hat eine beim BKA federführend eingesetzte Projektgruppe eine Neukonzeption des INPOL-Systems erarbeitet, die eine wesentliche Erweiterung des Systems vorsieht. Einzelheiten liegen noch nicht fest.

Bei der beabsichtigten Neustrukturierung des Systems sind aber mindestens folgende Grundsätze zu berücksichtigen:

- Zweck der Einrichtung des INPOL-Systems beim BKA ist es, die Strafverfolgungs- und Polizeibehörden bei ihrer Aufgabenerfüllung zu unterstützen. Die Verfolgung und die vorbeugende Bekämpfung von Straftaten sind grundsätzlich Sache der Länder. Also muß auch die Verantwortung für die Zulässigkeit, Richtigkeit und Dauer der Speicherung der Daten im INPOL-System bei den Ländern verbleiben.
- Die bereichsspezifischen Regelungen zur Datenverarbeitung der Polizei in der Strafprozeßordnung und in den Ländergesetzen dürfen nicht unterlaufen werden. Insbesondere dürfen die unterschiedlichen Regelungen zu

Erhebungsmethoden (z. B. Einsatz technischer Mittel, Einsatz verdeckter Ermittler) und Verwendungsbeschränkungen (z. B. Katalogtaten) nicht ausgehöhlt werden.

- Es ist genau festzulegen, wann eine Nutzung des INPOL-Systems erfolgen soll. Maßgeblich sollten die Kriterien „Schwere und überregionale Bedeutung einer Straftat" sein.
- Es müssen differenzierende Zugriffsbefugnisse, bezogen auf den Aufgabenbereich, geschaffen werden. Insbesondere Recherchen dürfen nur im Rahmen der Aufgabenerfüllung unter strikter Beachtung bestehender Zweckbindungsregelungen durchgeführt werden.
- Die automatisierte Verarbeitung gespeicherter personenbezogener Daten muß hinreichend protokolliert werden, so daß eine nachträgliche Kontrolle durch die Datenschutzbeauftragten des Bundes oder der Länder möglich ist.

4.5
Datenübermittlung der Polizei an die Führerscheinstelle

Nicht selten kommt es vor, daß die Polizei Personen auch ohne deren ausdrücklich erklärten Willen ärztlicher Behandlung zuführt. Sei es, daß sie verwirrten oder bewußtlosen Menschen hilft oder daß sie Personen, die sich selbst oder andere gefährden, zwangsweise in eine Klinik bringt. Dabei ist es unerläßlich, daß sie auch personenbezogene Daten der betroffenen Personen verarbeitet. Teilweise muß sie auch wegen evtl. vorliegender Straftaten ermitteln und andere Behörden über ihre Maßnahmen informieren. Erfolgt z. B. eine Verwahrung nach § 10 Hessisches Freiheitsentziehungsgesetz (HFEG) und steht die Anordnung in direktem Zusammenhang mit dem Führen eines Kraftfahrzeuges, dann kommt die Information der Straßenverkehrsbehörde in Betracht. Rechtsgrundlage dafür ist § 22 Abs. 1 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG). Danach dürfen Polizeibehörden personenbezogene Daten an andere für die Gefahrenabwehr zuständige Behörden übermitteln, soweit die Kenntnis dieser Daten zur Erfüllung der Aufgaben des Empfängers erforderlich erscheint. Doch längst nicht alle Maßnahmen nach dem Hessischen Freiheitsentziehungsgesetz stehen im direkten Zusammenhang mit dem Führen eines Kraftfahrzeuges. Das Hessische Ministerium des Innern und für Europaangelegenheiten hat im Einvernehmen mit dem Hessischen Ministerium für Jugend, Familie und Gesundheit, dem Hessischen Ministerium der Justiz und dem Hessischen Ministerium für Wirtschaft, Verkehr und Technologie durch Erlaß vom 16. April 1991 (StAnz. 1991 S. 1213), das Verfahren der Unterrichtung der Straßenverkehrsbehörden über Maßnahmen nach dem Hessischen Freiheitsentziehungsgesetz geregelt und die Anwendung von § 22 Abs. 1 HSOG damit konkretisiert.

Da in erster Linie medizinisch-psychologische Befunde und Prognosen für eine Unterrichtung der Straßenverkehrsbehörde entscheidungserheblich sind, wurde die Verantwortung für diese Entscheidung weitgehend in den ärztlichen Bereich verlagert. Nur wenn die Klinik bzw. der behandelnde Arzt eine Unterrichtung der Straßenverkehrsbehörde grundsätzlich ablehnt, entscheidet die HFEG-Behörde – das ist die Ordnungsbehörde – unter Beteiligung des Gesundheitsamtes über die Mitteilung. Mitteilungen durch die Polizeibehörden erfolgen grundsätzlich nicht, es sei denn, die Anordnung über die Maßnahme stand in direktem Zusammenhang mit dem Führen eines Kraftfahrzeuges.

Einem Bürger, der zweimal kurz hintereinander in ein psychiatrisches Krankenhaus eingewiesen werden mußte, weil von ihm eine erhebliche Gefahr für sich und andere Personen ausging, wurde von der Führerscheinstelle mit sofortiger Wirkung die Fahrerlaubnis entzogen und für den Fall der Wiederbeantragung die Vorlage eines medizinisch-psychologischen Gutachtens verlangt. Er hatte randaliert, Fensterscheiben zerschlagen, die herbeigerufenen Polizeibeamten bedroht und bei seiner vorläufigen Festnahme verletzt. Ein Zusammenhang mit der Teilnahme am Straßenverkehr bestand nicht. Grundlage für den Führerscheinentzug war eine Mitteilung der Polizei: Sie informierte die Führerscheinstelle in einer 21 Seiten umfassenden Mitteilung (Strafanzeige der Geschädigten, Polizeibericht, Anordnungen über die HFEG-Maßnahmen nebst ärztlichen Attesten, Erklärungen der verletzten Polizeibeamten, Vermerke, Beschuldigtenvernehmung) über den Vorgang. Ich bat die Polizeibehörde um Mitteilung, nach welcher Rechtsgrundlage diese Datenübermittlung erfolgte. Sie sah die Information der Führerscheinstelle als eine durch die §§ 1 Abs. 6, 22 Abs. 1 HSOG gebotene Erkenntnis- und Datenübermittlung an. Diese Bewertung des Sachverhaltes ist nicht gerechtfertigt.

§ 1 Abs. 6 HSOG, der alle Behörden zur Zusammenarbeit bei der Gefahrenabwehr verpflichtet, stellt keine selbständige Rechtsgrundlage zur Übermittlung personenbezogener Daten dar. Satz 2 dieser Vorschrift stellt dies ausdrücklich klar. § 22 Abs. 1 Satz 3 HSOG käme zwar als Rechtsgrundlage in Frage, der bereits erwähnte Erlaß schließt aber die Datenübermittlung durch die Polizeibehörden – von Ausnahmefällen abgesehen – aus. Ich habe die Datenübermittlung gegenüber dem Hessischen Ministerium des Innern und für Europaangelegenheiten gemäß § 27 Hessisches Datenschutzgesetz beanstandet und darum gebeten sicherzustellen, daß in künftigen Fällen der Erlaß vom 25. April 1991 Beachtung findet.

Das Ministerium wies meine Beanstandung zurück. Es schrieb, die Straßenverkehrsbehörde sei von den Maßnahmen der Polizeibehörde nicht unterrichtet worden. Der Betroffene sei wegen des Verdachts der Sachbeschädigung, des Widerstands gegen die Staatsgewalt sowie der Körperverletzung als Beschuldigter vernommen worden. Der Eindruck, den der vernehmende Beamte in dieser Vernehmung gewonnen habe, sei für die Unterrichtung der Straßenverkehrsbehörde entscheidend gewesen.

Meiner Ansicht nach trat die Beschuldigtenvernehmung – dort war von einer Teilnahme des Betroffenen am Straßenverkehr keine Rede – in der umfassenden Mitteilung an die Führerscheinstelle in den Hintergrund. Im

Vordergrund standen die unmittelbaren Anlässe, die zu den HFEG-Maßnahmen führten. Auf diese bezog sich auch die Führerscheinstelle in ihrem Bescheid über die Entziehung der Fahrerlaubnis.

Mir kommt es nicht darauf an, Personen, bei denen begründete Bedenken gegen ihre Teilnahme am Straßenverkehr bestehen, vor Maßnahmen der Straßenverkehrsbehörde zu schützen, jedoch soll in solchen Fällen die Initiative zu einer Mitteilung an die Führerscheinstelle grundsätzlich von einem Arzt ausgehen, so jedenfalls die Verständigung in dem erwähnten Erlaß der Fachministerien. Der Erlaß berücksichtigt, daß nicht jeder Person, die krankheitsbedingt kurzfristig kein Kraftfahrzeug führen sollte, sofort die Fahrerlaubnis entzogen wird, die sie nur nach einer medizinisch-psychologischen Begutachtung, die einen intensiven Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, wiedererteilt bekommen kann. Schließlich kommt bei einer nicht psychiatrisch bedingten Krankheit, die ebenso einen übergangsweisen Verzicht auf das Führen eines Kraftfahrzeuges verlangt, z.B. bei einem längeren Krankenhausaufenthalt, niemand auf den Gedanken, dem Patienten die Fahrerlaubnis zu entziehen, um sie nur nach einer medizinischen Begutachtung wiederzuerteilen.

4.6
Prüfung der DV-Nutzung einer Polizeidienststelle

1993 habe ich eine größere Polizeidienststelle geprüft, um einen Überblick über die eingesetzten Geräte und Programme sowie deren Nutzung zu erhalten. Die geringe Ausstattung mit DV-Geräten hatte im Fall der geprüften Dienststelle zu Konsequenzen geführt, die ich zuvor nicht erwartet hatte.

Dadurch, daß der weitaus größte Teil der Schreibarbeiten noch mit mechanischen Schreibmaschinen gemacht wurde, fühlten sich die Polizeibeamten in ihrer Arbeit stark benachteiligt. Durch die private Nutzung von PC's hatten sie sich an die Annehmlichkeiten dieser Technik gewöhnt. Um auch an ihrem Arbeitsplatz neuere Technik zur Verfügung zu haben, hatten einige der Beamten private PC's mitgebracht. Es ergab sich das für mich erstaunliche Bild, daß fast ein Drittel der vorhandenen PC's Privatgeräte waren.

Zeitgleich mit der Prüfung wurde ich informiert, daß das Hessische Ministerium des Innern und für Europaangelegenheiten den Entwurf einer PC-Rahmendienstanweisung erarbeitet, in der u.a. der Einsatz privater PC's zu dienstlichen Zwecken geregelt wird. Diese wurde mir kurz vor Redaktionsschluß übersandt. Die bei der Prüfung festgestellten Schwachstellen dürften bei einer konsequenten Umsetzung der Rahmendienstanweisung nicht auftreten. Es wird daher wesentlich sein, deren Umsetzung zu prüfen.

4.6.1
Prüfergebnisse

4.6.1.1
Zulässigkeit der Datenverarbeitung

Auf allen geprüften PC's wurden personenbezogene oder personenbeziehbare Daten gespeichert. In den geprüften Fällen war die Verarbeitung nicht zu beanstanden.

In den Fällen, in denen die Geräte zur Textverarbeitung genutzt wurden, wurden die Schriftstücke im Regelfall nach dem Ausdruck gelöscht. Konnte ein Schriftstück nicht an einem Arbeitstag beendet und ausgedruckt werden, so wurde es auf einer Diskette gespeichert. Die Disketten wurden in Stahlschränken sicher verschlossen aufbewahrt.

Die privaten Rechner wurden in der Regel zur Textverarbeitung benutzt. In einem Fall führte ein Polizeibeamter auf seinem Rechner eine kleine Datenbank mit Raubdelikten inkl. aller Opfer- und, soweit bekannt, Täterdaten. Zu der Anwendung gab es eine Errichtungsanordnung.

4.6.1.2
Technische Sicherungsmaßnahmen

Hinsichtlich der getroffenen Datensicherungsmaßnahmen gab es Unterschiede zwischen dienstlich beschafften und privaten PC's.

Bis auf drei Geräte waren alle dienstlichen PC's mit einer Datenschutzsoftware ausgestattet. Die restlichen PC's sollten in Kürze damit ausgerüstet werden.

Stichprobenhaft habe ich die Implementierung geprüft. Es ergaben sich keine Beanstandungen.

Die Sicherungsmaßnahmen der privaten PC's waren von der Fantasie und vom Engagement ihrer Eigentümer abhängig. In mehreren Fällen war es erforderlich, Paßwörter einzugeben, um mit dem jeweiligen Rechner arbeiten zu können. Um die oben genannte Anwendung über Raubdelikte zu schützen, waren die Daten zusätzlich verschlüsselt. Man kann feststellen, daß die Beamten generell Sicherungsmaßnahmen ergriffen hatten, von denen sie annahmen, daß ein Mißbrauch dadurch ausgeschlossen war. Der Standard der dienstlich beschafften PC's war nicht erreicht.

Die Geräte wurden nur als Stand-alone PC's eingesetzt. Zusätzliche Probleme durch eine Vernetzung entstanden nicht.

4.6.1.3
Organisatorische Regelungen

Es waren ein PC-Administrator und ein Stellvertreter bestimmt, die in Fragen des Einsatzes von PC's beteiligt wurden. Zu den Aufgaben gehört u.a. die Implementierung der Datenschutzsoftware.

Eine Aufstellung der dienstlich eingesetzten privaten PC's lag vor. Bei der Prüfung wurde ein privater PC vorgefunden, der in der Aufstellung noch nicht aufgeführt war und für den auch keine Anmeldung vorlag. Nach Aussage der Mitarbeiter war er erst wenige Tage vor der Prüfung aufgestellt worden.

Die Nutzung privater PC's ist dem Ministerium bekannt. Es erhält einmal jährlich eine Statistik der eingesetzten privaten PC's.

Weiterhin haben die Polizeibeamten in gewissem Umfang selbst Anwendungen programmiert. Es erfolgte keine ausreichende Dokumentation, was zu Problemen führen kann.

4.6.1.4
Zusammenfassung

Ich habe einige Defizite gefunden, die insbesondere im Bereich der organisatorischen und technischen Sicherungsmaßnahmen lagen. Es ist unbedingt erforderlich, durch die PC-Dienstanweisung für die Polizei einheitliche Rahmenbedingungen vorzugeben und deren Umsetzung zu kontrollieren.

4.6.2
Anforderungen an einen datenschutzgerechten Einsatz privater PC's am dienstlichen Arbeitsplatz

Bei der Prüfung stellte sich als ein Schwachpunkt heraus, daß private PC's wie dienstliche genutzt wurden, ohne daß die technischen und organisatorischen Rahmenbedingungen vergleichbar waren. Der Entwurf der Rahmendienstanweisung sieht vor, daß personenbezogene Daten auf privaten PC's nicht gespeichert werden dürfen. Trotzdem möchte ich an dieser Stelle allgemeine Anmerkungen zum Einsatz privater PC's machen.

Im Grundsatz ist es für die Tätigkeit am dienstlichen Arbeitsplatz unerheblich, wem ein DV-Gerät gehört, solange identische Anforderungen von dienstlichen und privaten Geräten erfüllt werden. Wegen der Schwierigkeit, gewisse organisatorische Vorkehrungen, wie z.B. Löschregelungen, konsequent durchzuführen, sollten an die Nutzung privater PC's zu dienstlichen Zwecken strenge Anforderungen gestellt werden.

- Der Einsatz privater PC's muß erforderlich sein.

  Es muß ausgeschlossen sein, zu dem gewünschten Zweck dienstlich beschaffte Geräte einzusetzen.

- Der Einsatz privater PC's ist auf die Verarbeitung weniger sensibler Daten zu beschränken.

  Anwendungen mit verbindlicher Verarbeitungslogik und solche, die personenbezogene Daten oder für den Dienstbetrieb wesentliche Daten verarbeiten, müssen vorrangig auf dienstlichen PC's betrieben werden.

  Sollen besonders sensible Daten verarbeitet werden, ist der Einsatz privater PC's abzulehnen. Die anderen Anwendungen sind in eine Rangfolge zu bringen, nach der die Nutzung von dienstlichen PC's erfolgt. Es bleiben nur die weniger sensiblen Daten, die auf privaten PC's verarbeitet werden.

- Die gespeicherten Daten sind auf das im Einzelfall erforderliche Mindestmaß zu beschränken.

  Nicht mehr benötigte Daten müssen umgehend physisch gelöscht werden.

- Dienstliche und private PC's müssen mit vergleichbaren Schutzmaßnahmen gesichert werden.

  Dienst-PC's, auf denen personenbezogene Daten verarbeitet werden, sind mit einer Schutzsoftware ausgestattet. Dies muß auch für private PC's gelten, die entsprechend genutzt werden.

- Es muß sichergestellt werden, daß private PC's, die die Diensträume verlassen, in den Zustand versetzt werden, in dem sie aufgestellt wurden.

  Hieraus folgt insbesondere, daß Daten physisch gelöscht werden müssen und dienstlich beschaffte Programme oder Hardwarekomponenten zu entfernen sind. Dies sicherzustellen ist nicht einfach. So speichern einige Textverarbeitungsprogramme Texte während der Erfassung in Abständen weniger Minuten auf der Festplatte, damit im Fehlerfall die Arbeit vieler Stunden nicht verloren geht. Auch diese Daten müßten physisch gelöscht werden.

  Kann dies nicht garantiert werden, so muß man von dem Einsatz absehen.

4.6.3
Ausblick

Die Prüfung hat deutlich gemacht, daß der Ansatz, den Grundausbau HEPOLAS (Hessisches Polizeiarbeitsplatzsystem) so schnell wie möglich einzuführen, für den polizeilichen Alltag richtig ist. In dem Grundausbau HEPOLAS wird den Benutzern eine Textverarbeitung zur Verfügung gestellt. Dadurch werden dienstlich beschaffte PC's für andere Anwendungen frei. Private PC's werden dann ebenfalls nicht mehr für Schreibarbeiten benötigt, und es könnte

möglich sein, die verbleibenden Anwendungen auf dienstlich beschaffte Rechner zu verlagern. Vielleicht gelingt es, ganz auf private Rechner zu verzichten oder diese tatsächlich nur noch so einzusetzen, daß keine personenbezogenen Daten gespeichert werden. Die Durchsetzung von Datensicherungsmaßnahmen für dienstliche Rechner ist in jedem Fall problemloser als bei privaten PC's.

Sollte die Datenverarbeitung in Polizeidienststellen weiterhin in einer Art und Weise erfolgen, wie ich es bei der Prüfung festgestellt habe, so wäre dies ein Grund zur Sorge. Ich gehe aber davon aus, daß das Zusammenspiel zwischen HEPOLAS und der neuen PC-Rahmendienstanweisung zu einer datenschutzgerechten Nutzung der Datenverarbeitung führt. Dies werde ich im nächsten Jahr prüfen.

5. Ordnungswidrigkeiten: Zeugenangabe im Bußgeldbescheid

Frau B. aus Hammersbach fuhr auf der Autobahn A 45 vom Autobahndreieck Langenselbold zur Autobahnraststätte Langen-Bergheim. Plötzlich sah sie im Innenspiegel, wie das hinter ihr fahrende Auto ins Schleudern kam und die Leitplanke berührte. An der Raststätte hielt sie an und rief die Polizei an, da sie nicht wußte, ob der Autofahrer verletzt wurde. Nach einer Weile kam die Polizei und nahm ihre Aussage auf, danach setzte sie ihre Fahrt fort. Einige Wochen später war sie Repressalien einer Verwandten des Autofahrers ausgesetzt, die sie dazu veranlassen wollte, ihre Anzeige zurückzunehmen. Name und Anschrift der Bürgerin waren dem Bußgeldbescheid, der gegen den Autofahrer erging, zu entnehmen. Sie stellte nun die Frage, warum der Name des Zeugen im Bußgeldbescheid enthalten sein muß. Sie meinte, es genüge, wenn dem Bußgeldbescheid zu entnehmen sei, daß „eine Zeugenaussage" vorliege.

Die Praxis stellt sich wie folgt dar: Die weitaus meisten bei den Bußgeldbehörden eingehenden Ordnungswidrigkeitenanzeigen tragen als Zeugenangabe den Namen eines Vollzugs- oder Hilfspolizeibeamten, dessen Dienstbezeichnung und die Dienststelle als ladungsfähige Anschrift. Soweit Privatpersonen als Zeugen benannt sind, ist die Praxis der anzeigenden Stellen unterschiedlich. Teilweise wird nur der Name, teilweise werden Name und Wohnort und zu einem weiteren Teil Name und vollständige Anschrift der Zeugen angeführt.

§ 66 Ordnungswidrigkeitengesetz (OWiG) schreibt den Inhalt des Bußgeldbescheides vor. Nach Abs. 1 Nr. 4 dieser Vorschrift gehört die Angabe der Beweismittel zum wesentlichen Inhalt des Bußgeldbescheides. Der Vorschlag, dazu nur anzugeben „eine Zeugenaussage", stößt auf Widerspruch in der Literatur und Rechtsprechung (vgl. Göhler, OWiG, 9. Aufl. 1990, Rdnr. 18 zu § 66). Nach einigen – wenn auch schon älteren – Gerichtsurteilen stellt das Weglassen von Name und Anschrift des Zeugen im Bußgeldbescheid einen Gesetzesverstoß dar (BayObLG MDR 1970, 440; OLG Celle NJW 1970, 580; OLG Hamm VM 1972, 30).

Meiner Ansicht nach genügt es, wenn im Bußgeldbescheid der Name des Zeugen – ohne weitere Angaben – aufgeführt ist. Ich habe dazu das Hessische Ministerium des Innern und für Europaangelegenheiten um Stellungnahme gebeten und auf das Urteil des Bundesgerichtshofs vom 5. April 1990 (NJW 1990, 1860) verwiesen, wonach die Bekanntgabe des Wohnortes und der Anschrift von Zeugen einen Eingriff in deren geschützten Persönlichkeitsbereich darstellt, der nur im überwiegenden Allgemeininteresse im Rahmen der Verhältnismäßigkeit hinzunehmen ist.

Das Ministerium teilt meine Ansicht nur „ein Stück". Es hält zwar Straßen- und Hausnummernangabe für entbehrlich, die Angabe des Wohnortes aber für unerläßlich. Der landeseinheitlich zu verwendende Vordrucksatz für die manuelle Bearbeitung von Bußgeldverfahren sei auch entsprechend gestaltet. Er sehe lediglich Name und „Wohnort" von Zeugen vor. Da nach § 222 Abs. 1 Strafprozeßordnung (StPO) auch das Gericht bei der Namhaftmachung von Zeugen deren Wohn- oder Aufenthaltsort anzugeben habe und die Vorschriften der StPO nach § 46 Abs. 1 OWiG sinngemäß für das Bußgeldverfahren gelten, wenn das Ordnungswidrigkeitengesetz keine eigene Regelung enthält, müsse zur Angabe des Namens auch die Angabe des Wohnortes von Zeugen hinzukommen. Es führte weiterhin aus, Sinn und Zweck der Regelung in § 66 Abs. 1 Nr. 4 OWiG sei es, dem Betroffenen die Prüfung zu ermöglichen, ob der gegen ihn im Bußgeldbescheid erhobene Vorwurf beweisbar sei. Da die Einlegung des Einspruchs für den Betroffenen mit Kosten verbunden sein könne, solle er die Erfolgsaussichten des Rechtsbehelfs abschätzen können. Dies sei ihm aber nur möglich, wenn er wisse, was die Verwaltungsbehörde gegen ihn in der Hand hat. Beim Zeugenbeweis könne es daher im Verteidigungsinteresse des Betroffenen liegen, Nachforschungen über die Person des Zeugen, insbesondere für dessen Glaubwürdigkeit beachtliche Umstände, anzustellen. Mein Vorschlag, nur den Namen des Zeugen anzugeben, würde gegen die in § 222 Abs. 1 Strafprozeßordnung (StPO) normierte Pflicht zur Namhaftmachung von Zeugen verstoßen. Zudem könnte der Betroffene einwenden, sein legitimes Verteidigungsinteresse sei ohne ersichtlichen Grund eingeschränkt worden. Außerdem verwies es auf die Regelung in § 68 StPO, wonach lediglich gefährdeten Zeugen gestattet werden könne, ihren Wohnort nicht anzugeben. Ferner habe der Betroffene nach der mit dem Justizmitteilungsgesetz geplanten Änderung des Ordnungswidrigkeitengesetzes ohnehin die Möglichkeit, Einsicht in die Akte seines Bußgeldverfahrens zu nehmen.

Ich bleibe dabei: Die regelmäßige Angabe des Wohnorts berücksichtigt nicht hinreichend den Grundsatz der Verhältnismäßigkeit, insbesondere im Hinblick auf die Bedeutung des Vorwurfs bei Verkehrsordnungswidrigkeiten, die überwiegend geringfügige Verfehlungen im Straßenverkehr betreffen. Das Gebot der Verhältnismäßigkeit verlangt in diesen Fällen eine Abstufung gegenüber den im Strafverfahren gebotenen Mitteln. Grundsätzlich halte ich bei Verkehrsordnungswidrigkeiten aufgrund von Anzeigen von Privatpersonen die Bekanntgabe lediglich des Namens des Anzeigeerstatters in dem Bußgeldbescheid für erforderlich, aber auch für ausreichend. Lehnt der Betroffene die

Rechtsfolgen des Bußgeldbescheides ab, soll seinem Informationsinteresse – abgesehen von den Fällen des § 68 Abs. 2 StPO – nichts entgegenstehen. Erfolgt jedoch die Bezeichnung des Wohnorts des Zeugen bereits im Bußgeldbescheid, werden in einer Vielzahl von Fällen Angaben offenbart, ohne daß dies erforderlich ist.

6. Verkehrswesen

6.1
Zuverlässigkeitsprüfung bei der Ausgabe „roter Kfz-Kennzeichen zur wiederkehrenden Verwendung"

Der Begriff der Zuverlässigkeit findet sich immer dort, wo einzelne behördliche Erlaubnisse unter der Bedingung erteilt werden, daß ihr bisheriges Verhalten bestimmten Anforderungen entspricht. Diese Anforderungen sind oft gesetzlich nicht definiert. So gibt es beispielsweise den Begriff der Zuverlässigkeit im Gaststättenrecht (§ 4 Abs. 1 GastG), im Waffenrecht (§ 30 Abs. 1 WaffG), an zahlreichen Stellen des Gewerberechts (z. B. § 30 Abs. 1 Nr. 1, § 33c Abs. 2 GewO), aber auch im Gesundheitsrecht (z. B. in der 1. DVHeilprG – § 2 Abs. 1f). Im Straßenverkehrsrecht sieht § 28 Abs. 3 Straßenverkehrszulassungsordnung (StVZO) u. a. vor, daß rote Kfz-Kennzeichen zur wiederkehrenden Verwendung nur an zuverlässige Kfz-Händler ausgegeben werden. Rote Kfz-Kennzeichen werden z. B. verwendet, um (noch) nicht zugelassene Kraftfahrzeuge zu überführen.

Im Gegensatz zu neueren Vorschriften (z. B. § 5 WaffG) geben ältere oft keine Hinweise darauf, was unter der „Zuverlässigkeit" zu verstehen ist, wie sie geprüft wird und welche personenbezogenen Daten dabei erhoben werden dürfen (vgl. auch Ziff. 9.6). Es leuchtet ein, daß vor Erteilung der Erlaubnis zum Führen einer Waffe geprüft wird, ob der Antragsteller schon einmal mit dem Waffengesetz in Konflikt geraten ist. Nicht einleuchtend ist, wenn bei der Zuteilung roter Kfz-Kennzeichen zur wiederkehrenden Verwendung ein unbegrenzter Informationsaustausch mit Ordnungs-, Polizei- und Justizbehörden stattfindet und beispielsweise die dabei in Erfahrung gebrachte Information, daß einem Kfz-Händler das Sorgerecht für sein minderjähriges Kind zugesprochen wurde, eine Rolle spielt.

Im Zusammenhang mit der Prüfung nach § 28 Abs. 3 StVZO bat die Kraftfahrzeugzulassungsstelle Frankfurt den Feldschutz-, Ermittlungs- und Außendienst ihres Ordnungsamtes um Mitteilung, ob Tatsachen bekannt sind, die gegen die Zuverlässigkeit des Antragstellers sprechen, und ob er, wie in seinem Antrag angegeben, tatsächlich Oldtimerfahrzeuge besitzt. Die befragte Stelle antwortete, der Betroffene sei wie angegeben wohnhaft und gemeldet. Er könne nicht positiv beurteilt werden, da er schon öfter wegen Ordnungswidrigkeiten und Straftaten negativ in Erscheinung getreten sei, besonders zu erwähnen seien Anzeigen nach § 29c StVZO (Anzeige eines Kfz-Versicherers über abgelaufenen Versicherungsschutz) und die Auferlegung der Führung eines Fahrtenbuches. Er besäße einige alte Feuerwehrfahrzeuge und einen alten Traktor.

Auf welche Weise der Feldschutz-, Ermittlungs- und Außendienst die Angaben ermittelt hat, ist unklar. Offenbar fanden ein Informationsaustausch mit der Meldebehörde, der Führerscheinstelle, der Polizei, der Abteilung Ordnungswidrigkeiten des Ordnungsamtes sowie eine Ortsbesichtigung statt. Nachdem der Antrag abgelehnt wurde und der Kfz-Händler gegen die ablehnende Entscheidung Widerspruch eingelegt hatte, wandte sich die Zulassungsstelle erneut an den Feldschutzdienst und bat um Konkretisierung der Angaben. Der Feldschutzdienst antwortete, ihm sei durch Polizeibeamte mitgeteilt worden, der Kfz-Händler sei in sieben Fällen „negativ in Erscheinung getreten". Hinsichtlich der Anzeige nach § 29c StVZ0 wurde eine konkrete Angabe gemacht, bezüglich der Fahrtenbuchauflage stützte sich der Feldschutzbeamte auf die Aussage eines Kollegen. Nun richtete die Zulassungsstelle eine Anfrage an die Polizei.

Das Polizeipräsidium teilte vier Aktenzeichen und den jeweiligen Tatvorwurf mit. Es folgte eine Anfrage an die Amtsanwaltschaft nach dem Ausgang der Verfahren. Diese antwortete, das erste Verfahren sei nach § 170 Abs. 2 Strafprozeßordnung eingestellt worden, im zweiten sei auf den Weg der Privatklage verwiesen worden, das dritte sei an die Staatsanwaltschaft abgegeben worden und das vierte sei noch anhängig. Der Kfz-Händler sei also nicht vorbestraft. Nun übersandte die Zulassungsstelle die Akte an die Aufsichtsbehörde und bat um Entscheidungshilfe. Das Regierungspräsidium empfahl, die Ablehnung zurückzunehmen. Da über den Kfz-Händler im Verkehrszentralregister und im Bundeszentralregister keine Einträge vorlägen, könne die Ablehnung lediglich auf ein angebliches Verfahren nach § 29c StVZO gestützt werden. Außerdem habe man in Erfahrung bringen können, daß Ermittlungsverfahren wohl teilweise von der geschiedenen Ehefrau initiiert worden seien und dem Widerspruchsführer das Sorgerecht für seine Tochter zugesprochen worden sei.

Meiner Ansicht nach stellt die Zuverlässigkeitsprüfung nach § 28 Abs. 3 StVZO keine ausreichende Rechtsgrundlage dar, um – wie im vorliegenden Fall – grenzenlos Recherchen über einen Kraftfahrzeughändler anzustellen. Außerdem wurde bei den Ermittlungen gegen die §§ 11 Abs. 1 und 12 Abs. 2 Ziff. 2 Hessisches Datenschutzgesetz (HDSG) verstoßen. Ich wandte mich daher an das Hessische Ministerium für Wirtschaft, Verkehr und Technologie. Das Ministerium teilt meine Ansicht, daß die Ordnungsbehörde bei den Nachforschungen im Zuge der Prüfung der Zuverlässigkeit „zu weit" gegangen ist und für ihre Ermessensentscheidung Informationen herangezogen hat, die nicht entscheidungsrelevant sind. Es forderte das Regierungspräsidium auf, der ausufernden Praxis der Zulassungsstelle Frankfurt, ggf. auch anderer Zulassungsstellen, bei der Prüfung der Zuverlässigkeit der Antragsteller Einhalt zu gebieten. Ob eine Veränderung der Praxis eintritt, werde ich 1994 beobachten.

6.2
Unzulässige Verwertung von Informationen bei der Erteilung von Fahrgastbeförderungsscheinen

Ein Darmstädter Taxifahrer hatte bei der Stadtverwaltung die Verlängerung seines 1982 ausgestellten Fahrgastbeförderungsscheines um drei Jahre beantragt. Die Behörde lehnte seinen Antrag ab und gewährte, weil sie Bedenken an seiner persönlichen Zuverlässigkeit hatte, die Verlängerung nur um ein Jahr.

Zur Begründung führte sie an, daß im Jahre 1982 gegen den Taxifahrer wegen Beleidigung und Anwendung körperlicher Gewalt ermittelt worden war, er in der Zeit von 1983 bis 1988 vier Ordnungswidrigkeiten begangen hatte und im Jahre 1992 gegen ihn ein Verfahren wegen Widerstandes gegen Vollstreckungsbeamte und gefährlichen Eingriffs in den Straßenverkehr geführt wurde.

Mit Ausnahme des letzten Falles, der wegen geringer Schuld gegen Zahlung einer Geldbuße eingestellt worden war, unterlagen sämtliche Vorwürfe einem Verwertungsverbot. Schon 1977 stellte das Bundesverwaltungsgericht (NJW 1977, 1075) fest, daß sich das Verbot, im Verkehrszentralregister getilgte Eintragungen noch zu verwerten, aus dem Sinne des Verkehrszentralregisters ergibt. Denn das Verkehrszentralregister ist die allein maßgebende Erfassungs- und Auskunftsstelle der für die Belange der Verkehrssicherheit bedeutsamen gerichtlichen und verwaltungsbehördlichen Entscheidungen. Da die Ordnungswidrigkeiten schon länger zurücklagen und im Verkehrszentralregister getilgt waren, hätten sie dem Taxifahrer bei der Verlängerung seines Personenbeförderungsscheins nicht vorgehalten werden dürfen. Das gleiche gilt für den schon über zehn Jahre zurückliegenden Fall der Beleidigung. Damals war es während einer Taxifahrt zu einem Zwischenfall mit einem anderen Verkehrsteilnehmer gekommen, der den Taxifahrer der Beleidigung und der Anwendung körperlicher Gewalt beschuldigte. Ein schuldhaftes Verhalten des Taxifahrers konnte jedoch nicht festgestellt werden, so daß keine weiteren Schritte gegen ihn eingeleitet wurden. Es erfolgte also weder eine Eintragung im Verkehrszentralregister noch im Bundeszentralregister, so daß auch dieser Vorfall nicht gegen ihn verwertet werden durfte.

Der Taxifahrer legte Widerspruch gegen die Verwaltungsentscheidung ein. Die Widerspruchsbehörde bestätigte zwar in ihrem Bescheid das Verwertungsverbot, war aber der Ansicht, der Schuldvorwurf aus dem Jahre 1992 genüge, um an der persönlichen Zuverlässigkeit des Taxifahrers zu zweifeln. Eine verwaltungsgerichtliche Entscheidung über diese Beurteilung steht noch aus.

Wegen der unzulässigen Verwertung der Informationen wandte sich der Betroffene an mich. Ich wies den Oberbürgermeister der Stadt Darmstadt auf das Verwertungsverbot hin und bat ihn um Mitteilung, ob es sich in dem konkreten Fall um einen Einzelfall handele oder ob er grundsätzlich bei der Erteilung von Fahrgastbeförderungsscheinen alle ihm zur Verfügung stehenden und ggf. ganz oder teilweise auch einem Verwertungsverbot unterliegenden Informationen verwerte. Ggf. bat ich ihn zu prüfen, wie sichergestellt werden könne, daß in künftigen Fällen solche Informationen nicht mehr verwertet würden. Bei dieser Prüfung bat ich ihn zu erwägen, die Akten in einem bestimmten Rhythmus oder bei der laufenden Erfüllung von Aufgaben auf das Vorhandensein solcher Informationen durchzusehen mit dem Ziel, sie dann auszusondern.

Der Oberbürgermeister der Stadt Darmstadt antwortete mir, daß er die Ansicht, im Verkehrszentralregister getilgte Ordnungswidrigkeiten nicht mehr verwerten zu dürfen, nicht teile. Er sei berechtigt, bei der Beurteilung der Gesamtpersönlichkeit des Betroffen alle ihm aus seinen Unterlagen zur Verfügung stehenden Informationen, auch wenn sie bereits im Verkehrszentralregister getilgt seien, zu berücksichtigen.

Ich schaltete die Aufsichtsbehörde ein, schilderte ihr den Sachverhalt und bat sie, den Oberbürgermeister der Stadt Darmstadt zu bewegen, seine, das Verwertungsverbot ignorierende Haltung, aufzugeben. Sie teilte mir mit, sie habe ihn aufgefordert, die Rechtsprechung des Bundesverwaltungsgerichts in seiner Verwaltungspraxis zu beachten. Der Oberbürgermeister hat mir zwischenzeitlich zugesagt, das Verwertungsverbot künftig zu beachten. Im konkreten Fall habe es sich um einen Einzelfall gehandelt. Bei der laufenden Bearbeitung der Anträge auf Erteilung von Personenbeförderungsscheinen würden in Zukunft die Unterlagen über getilgte Vorgänge aus den Akten entfernt.

7. Justiz

7.1
Datenschutz bei den Staatsanwaltschaften

1993 habe ich verschiedene Staatsanwaltschaften geprüft und dabei einige typische Mängel festgestellt.

7.1.1
Zugang und Sicherung der Dienstgebäude und Diensträume

Die Sicherung der Dienstgebäude und Diensträume war in den meisten Fällen nicht zu beanstanden; vorgefundene Mängel können durch einzelne technische oder organisatorische Maßnahmen behoben werden. Aus dem Rahmen fiel hier allerdings eine der größeren Staatsanwaltschaften. Sie ist in einem Gebäude untergebracht, dessen Zugangstüren und Fenster lediglich einfach verglast sind. Sonstige Sicherungsmaßnahmen (z. B. Diebstahlmeldeanlage usw.) sind nicht vorhanden.

Das Gebäude ist abends bis 19.00 Uhr geöffnet. Zwar ist der Zugang ständig mit einem Pförtner besetzt, der jedoch zum Zeitpunkt meiner Prüfung keine Zugangskontrolle vornahm, sondern lediglich als Auskunftsstelle zur Verfügung stand. Die Türen zu den einzelnen Diensträumen, die ohnehin nur mit einfachen Schlössern gesichert sind, werden zwar beim Verlassen abgeschlossen, die Schlüssel bleiben aber auch nach Dienstende und während des Urlaubs der Bediensteten von außen stecken. So war es mir nach Dienstschluß ohne weiteres möglich, unbehelligt die Diensträume zu betreten. Ich hatte freien Zugang zu den offen aufbewahrten Akten und den PC's.

Zwar gibt es bei dieser Staatsanwaltschaft Hausverfügungen, welche die Sicherung der Diensträume detailliert regeln. Die Hausverfügungen werden auch wiederkehrend in Umlauf gebracht, ihre Einhaltung aber offensichtlich nicht hinreichend überwacht.

Die Dienstgebäude sollten zumindest durch doppelt verglaste Fenster und Außentüren und – abhängig von der Lage des Gebäudes – Alarmanlagen gesichert sein.

Die Diensträume der Staatsanwaltschaften sollten grundsätzlich mit Sicherheitsschlössern ausgestattet sein. Die Türen sind, auch bei nur kurzfristiger Abwesenheit, unbedingt zu verschließen, denn die Akten werden bei den Staatsanwaltschaften, insbesondere bei den Geschäftsstellen, im Regelfall in nicht verschließbaren Regalen aufbewahrt. Schließlich sollte es auch im Interesse der Staatsanwaltschaft liegen, einem Mißbrauch von Daten wirksam vorzubeugen.

7.1.2
Manuelle Datenverarbeitung

7.1.2.1
Mitteilung über den Verfahrensausgang an die Polizei

Die Aussagekraft kriminalpolizeilicher personenbezogener Sammlungen hängt auch davon ab, daß eine Rückmeldung der Staatsanwaltschaft an die Polizei über den Ausgang des Verfahrens erfolgt. Denn die Kenntnis des Verfahrensausgangs ist ausschlaggebend für die Entscheidung der Polizei, ob und wie lange die Daten des Betroffenen gespeichert und Unterlagen zu dem Verfahren aufbewahrt werden. Die Polizei sendet daher gleichzeitig mit der Abgabe des Ermittlungsverfahrens einen Vordruck an die Staatsanwaltschaft, der zu den Handakten zu nehmen und nach Beendigung des Verfahrens ausgefüllt zurückzusenden ist. Trotz dieser Erleichterung gerät die Rückmeldung immer wieder in Vergessenheit.

7.1.2.2
Einhaltung der Aufbewahrungsbestimmungen

Die Frage, wie lange Akten, gerichtliche Entscheidungen, Register, Karteien usw. im Bereich der Staatsanwaltschaften aufzubewahren sind, haben die Landesjustizressorts einheitlich in den „Aufbewahrungsbestimmungen für das Schriftgut der ordentlichen Gerichtsbarkeit der Staatsanwaltschaften und der Justizvollzugsbehörden" geregelt. Stichproben in den Archiven haben ergeben, daß die Aussonderung nicht immer rechtzeitig erfolgt. Nicht nur die Akten bleiben mitunter bis zu mehreren Jahren über die Frist hinaus liegen, ich habe sogar Aktenregister mit den dazugehörigen Namensverzeichnissen aus den zwanziger Jahren gefunden.

In einem – zudem nicht verschlossenen – Archiv lagerten unter den Strafakten die Personalakten ausgeschiedener Mitarbeiter. Personalakten sind in jedem Fall getrennt von den übrigen Akten aufzubewahren und dürfen nur den Mitarbeitern, die für Personalangelegenheiten zuständig sind, zugänglich sein.

7.1.3
Automatisierte Datenverarbeitung

7.1.3.1
Automatisierte Datenverarbeitung in den Dezernaten

Die Dezernenten der von mir geprüften Staatsanwaltschaften setzen zunehmend dienstliche oder auch private PC's ein. Die PC's werden überwiegend zur Textverarbeitung benutzt, in geringerem Umfang werden zur Unterstützung der Ermittlungen in umfangreichen Verfahren auch Datenbanken aufgebaut.

Dabei fiel auf, daß trotz unzureichender räumlicher Sicherungsmaßnahmen (vgl. 7.1.1) nicht nur keine Datenschutzsoftware eingesetzt wurde, sondern nicht einmal die in den verwendeten Programmen vorgesehenen Datensicherungsmaßnahmen aktiviert waren. Gefertigte Sicherungskopien wurden offen aufbewahrt. Schriftliche Dienstanweisungen, die den Einsatz und die Benutzung der PC's, insbesondere auch die Löschung der gespeicherten Daten, näher regelten, waren entweder unzureichend oder überhaupt nicht vorhanden.

Es ist unbedingt erforderlich, entsprechende Dienstanweisungen zu erarbeiten, die einheitliche Rahmenbedingungen für die Staatsanwaltschaften vorgeben, und deren Umsetzung zu kontrollieren.

7.1.3.2
Automatisierte Datenverarbeitung beim Schreibdienst

Auf Datensicherungsmaßnahmen ist jedoch nicht nur bei den Dezernenten der Staatsanwaltschaften, sondern auch bei den Schreibkräften zu achten. Bei einer Staatsanwaltschaft war ein PC-Netz für den Schreibdienst installiert.

Gearbeitet wurde mit dem Textverarbeitungsprogramm PRSIMA-Office. Der Zugang zum Netz war paßwortgeschützt. Allerdings war es möglich, die Funktion „Benutzerwechsel" zu nutzen und dadurch Dateien anderer Mitarbeiter abzurufen. So führte mich die Eingabe der Buchstabenkombination „sch" zu den Dateien einer Mitarbeiterin der Personalabteilung. Die Möglichkeit der Nutzung dieser Funktion ist zu unterbinden.

Bei dieser Gelegenheit stellte ich fest, daß in den Dateien der Personalabteilung dienstliche Beurteilungen gespeichert waren. Das ist ein Verstoß gegen § 34 Abs. 6 Hessisches Datenschutzgesetz, der ausdrücklich untersagt, daß dienst- und arbeitsrechtliche Beurteilungen automatisiert verarbeitet werden. Daher müssen dienstliche Beurteilungen, unmittelbar nachdem die endgültige Fassung erstellt ist, aus dem Textverarbeitungssystem gelöscht werden.

7.1.3.3
REFAS

Zwei Staatsanwaltschaften arbeiten mit dem EDV-Verfahren REFAS (Registerführung an Amts- und Staatsanwaltschaften), das die Geschäftsstellen- und Kanzleitätigkeit unterstützt. In das Verfahren einbezogen sind die Eingangserfassung der Verfahren, die Abschlußmitteilung über den Ausgang des Verfahrens nach der „Anordnung über Mitteilungen in Strafsachen" sowie Mitteilungen an und von und die Anfragen an Bundes- und Verkehrszentralregister. Die Statistikzwecken dienenden Zählkarten werden ebenfalls automatisationsgestützt geführt und über eine Schnittstelle an das Hessische Statistische Landesamt übergeben.

Das Verfahren wurde nach Vorgaben der Staatsanwaltschaft von der Hessischen Zentrale für Datenverarbeitung (HZD) entwickelt. Die Eingaben und Ausgaben erfolgen bei der Staatsanwaltschaft menügeführt an Bildschirmen und Druckern, die über eine Poststandleitung und einen Vorortrechner an den HZD-Großrechner angebunden sind, wo alle Daten zentral verarbeitet und gespeichert werden. Zugriffsmöglichkeiten der Staatsanwaltschaften untereinander auf die jeweils „fremden" Datenbestände sind nicht eingeräumt. Eine Schnittstelle zu anderen Auskunftssystemen, z. B. der Polizei, besteht bisher nicht.

Bei einer Staatsanwaltschaft ist REFAS seit dem Jahr 1984 im Einsatz. Gespeichert sind dort ca. 750.000 bis 800.000 Datensätze. Zu meinem Erstaunen mußte ich feststellen, daß trotz der relativ langen Laufzeit die Funktionalität „löschen" noch nicht realisiert ist. D.h., Daten, die nach den „Bestimmungen über die Aufbewahrungsfristen für das Schriftgut der ordentlichen Gerichtsbarkeit, der Staatsanwaltschaften und der Justizvollzugsbehörden" nicht länger gespeichert werden dürfen, können in absehbarer Zeit nicht gelöscht werden. Dieser Mangel ist umgehend zu beheben.

7.1.4
Telefax-Geräte

Bei zwei Staatsanwaltschaften ist mir folgendes aufgefallen:

Vor Jahren wurde jeweils ein Telefax-Gerät angeschafft, das als zentrales Fax-Gerät der Justizbehörden diente. Es gehen dort sehr häufig Telefaxe ein, die für das Amtsgericht, Landgericht oder weitere Justizbehörden bestimmt sind. Dabei müssen Bedienstete der Staatsanwaltschaft personenbezogene Daten zur Kenntnis nehmen, um sie der richtigen Justizbehörde zuordnen und an sie weiterleiten zu können.

Dies war sicherlich für eine Übergangszeit hinzunehmen. Mittlerweile verfügen aber auch die anderen Justizbehörden über eigene Fax-Geräte. Meiner Ansicht nach bilden die „Justizbehörden" keine informationelle Einheit, so daß der jetzt eingetretenen Situation, daß ständig personenbezogene Daten von der „falschen" Justizbehörde zur Kenntnis genommen werden, um sie der „richtigen" Justizbehörde zuleiten zu können, gegengesteuert werden sollte. Ich habe deshalb den Dienststellenleitungen empfohlen, die Absender von Telefaxen, die nicht an sie gerichtet sind, auf die korrekte Telefax-Nummer hinzuweisen.

7.2
Reform der Strafprozeßordnung

Durch den Landesbeauftragten für den Datenschutz Schleswig-Holstein wurde ich zuerst auf den Arbeitsentwurf eines Strafverfahrensänderungsgesetzes 1993 (StVÄG 1993) – Stand 12. Juli 1993 – aufmerksam. Der Entwurf, der mir zwischenzeitlich auch vom Hessischen Ministerium der Justiz zur Verfügung gestellt wurde, beruht offenbar auf dem von der Bundesregierung vorgelegten „Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts – StVÄG 1989 – Stand 26. Juni 1989 –" (vgl. 18. Tätigkeitsbericht, Ziff. 18.1). Erarbeitet wurde er von einer Unterarbeitsgruppe des Strafrechtsausschusses der Justizministerkonferenz, an der u.a. auch Hessen beteiligt ist.

Leider wurden die vergangenen Jahre nicht dazu genutzt, Formulierungen zu suchen, die eine sorgfältige Abwägung zwischen den Interessen des Staates und seiner Bürger und der Heranziehung der vom Bundesverfassungsgericht aufgestellten Grundsätze zum Recht auf informationelle Selbstbestimmung erkennen lassen. Im Gegenteil – die im jetzigen Entwurf vorgesehenen Datenschutzregelungen bleiben weit hinter denen des StVÄG 1989 zurück. Da mir noch keine Begründung für den Entwurf vorliegt, kann ich hier keine Bewertung verantworten, sondern vorab nur auf einige generelle Mängel hinweisen:

7.2.1
Auskünfte aus Akten und Akteneinsichtsrecht

In Strafakten sind in der Regel nicht nur die Daten des Beschuldigten, sondern einer Vielzahl weiterer Personen, wie beispielsweise des Opfers, der Zeugen usw. enthalten. Dabei kann es sich auch um äußerst sensible Daten handeln, beispielsweise die Untersuchungsergebnisse und Gutachten, die das Opfer einer Sexualstraftat betreffen, oder die Einkommensverhältnisse des Opfers eines Anlagebetrügers, das Anteile an einem angeblichen Steuersparmodell erworben hat. Aufgrund dieser Tatsache hat das Hessische Ministerium der Justiz erst im Jahre 1992 in einem „Erlaß zur Datenweitergabe im Strafrechtlichen Ermittlungsverfahren" (Runderlaß des Ministeriums der Justiz vom 14. Oktober 1992, JMBl. S. 554) genau geregelt, wer in welchem Umfang Akteneinsicht erhält. Um so mehr überrascht es, in dem auch von Hessen mitgetragenen Entwurf nunmehr ganz undifferenzierte Regelungen in diesem Bereich zu finden.

So war im StVÄG 1989 noch vorgesehen, daß Behörden und andere öffentliche Stellen Auskünfte aus Akten erhalten, soweit dies 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. Nach dem StVÄG 1993 hingegen sollen derartige Auskünfte bereits dann zulässig sein, wenn dies zur Erfüllung der in der Zuständigkeit der anfragenden Stelle liegenden Aufgabe erforderlich ist. Ist die Erteilung der Auskunft mit „unverhältnismäßig hohem Aufwand" verbunden, soll sogar Akteneinsicht gewährt werden können. Letzteres dürfte bei der seit Jahren unter Überlastung leidenden Justiz der Regelfall werden. Damit wird ein ungehinderter Zugriff aller öffentlichen Stellen auf sämtliche in einem Strafverfahren zusammengetragenen Informationen ermöglicht.

Nicht besser sieht es mit der Auskunft aus Akten und dem Akteneinsichtsrecht für Privatpersonen und sonstige Stellen aus. Darunter sind Nichtbeschuldigte, Privatkläger, Nebenkläger, Opfer oder Einziehungsbeteiligte zu verstehen, deren Akteneinsichtsrecht schon seit längerer Zeit gesondert geregelt ist. Gemeint sind hier auch Versicherungsunternehmen, Interessenverbände und so weiter. Während das StVÄG 1989 in diesen Fällen noch die Glaubhaftmachung eines berechtigten Interesses verlangte, gibt sich der jetzige Entwurf mit der Darlegung, also dem bloßen Vortrag eines berechtigten Interesses zufrieden. Und auch hier gilt wieder, daß im Falle eines „unverhältnismäßig hohen Aufwands" die Entlastung der Verwaltung über das Recht auf informationelle Selbstbestimmung gestellt wird.

Der Entwurf kehrt das Prinzip um, daß Datenübermittlungen nur in gesetzlich bestimmten Fällen zulässig sind, indem er eine Vielzahl von Übermittlungen von Daten aus Strafverfahren an andere Stellen zuläßt, soweit keine anderen gesetzlichen Regelungen einer solchen Übermittlung entgegen stehen. Spezifische Regelungen, die einer solchen Übermittlung entgegen stehen könnten, gibt es indes nur in wenigen Bereichen.

7.2.2
Dateienregelungen

Die Dateienregelungen des StVÄG 1989 hatten noch zwischen Beschuldigten, Zeugen, Opfern, Kontakt- und Begleitpersonen, Hinweisgebern und sonstigen Auskunftspersonen unterschieden. Ferner war differenziert worden zwischen Speicherung, Veränderung und Nutzung von Daten zu Zwecken des anhängigen Strafverfahrens, künftiger Strafverfahren und Vorgangsverwaltung. Außerdem wurden verbindliche Löschungsfristen festgelegt. Nach dem StVÄG 1993 können Informationen über jeden gespeichert werden, wenn es für „erforderlich gehalten wird", gleichgültig, welche Stellung der Betroffene in dem jeweiligen Verfahren einnimmt. Gespeichert, verändert und genutzt werden können somit alle Daten, die für Gerichte, Staatsanwaltschaften und andere Justizbehörden sowie sonstige Strafverfolgungsbehörden zur Aufgabenerfüllung erforderlich sind und das auch in gemeinsamen und verbundenen Dateien. Statt auf der Grundlage des StVÄG 1989 differenzierte Vorschriften zur Regelung der einzelnen Schritte der Datenerhebung und -verarbeitung durch die Staatsanwaltschaft und die Polizei zu Zwecken des Strafverfahrens und der Strafrechtspflege auszuarbeiten, sieht der Entwurf also nur weitgefaßte Generalklauseln vor. Dies führt zu erheblicher Rechtsunsicherheit und Unklarheit der Normen. Der vom Bundesverfassungsgericht in seinem Volkszählungsurteil erhobenen Forderung, daß jeder Bürger erkennen können muß, wer wann was über ihn weiß, kommt der Entwurf nicht mehr nach. Gegen die vorgesehenen Regelungen bestehen daher erhebliche verfassungsrechtliche Bedenken.

Immerhin sieht der Entwurf noch eine Löschungspflicht für Daten vor, deren Speicherung unzulässig oder deren Kenntnis nicht mehr erforderlich ist. Auf bestimmte Fristen legt er sich jedoch nicht fest.

Mit Befremden habe ich folgende Regelung zur Kenntnis genommen: Stellt die speichernde Stelle fest, daß unrichtige, zu löschende oder zu sperrende personenbezogene Daten übermittelt worden sind, so ist dem Empfänger die Berichtigung, Löschung oder Sperrung mitzuteilen, wenn dies zur Wahrnehmung schutzwürdiger Interessen des Betroffenen erforderlich ist. Jedoch kann die Mitteilung unterbleiben, wenn sie einen unverhältnismäßigen Aufwand erfordern würde. Auch hier spielen die schutzwürdigen Belange des Betroffenen gegenüber dem Aufwand der Verwaltung — wie so oft — keine Rolle.

7.3
Datenschutz im Zusammenhang mit der Eintragung in das Vereinsregister

Aufgrund einer Eingabe wurde ich auf folgenden Fall aufmerksam:

Eine Bürgerin hatte als Vorstandsmitglied bei einem südhessischen Amtsgericht die Eintragung eines Vereins in das Vereinsregister beantragt. Sie wunderte sich, als sie im Zusammenhang mit der Vereinsgründung eine Vorladung der

Industrie- und Handelskammer (IHK) erhielt. Noch größer war ihre Verwunderung, als sie in Gegenwart eines weiteren Vorstandsmitgliedes zu einem an das Amtsgericht gerichteten denunzierenden Schreiben ihres geschiedenen Ehemannes Stellung nehmen sollte. Außerdem lag der IHK ein unbeschränkter Auszug aus dem Bundeszentralregister vor, der eine Eintragung enthielt, die nicht in ein Führungszeugnis aufzunehmen war. Ich bin der Angelegenheit nachgegangen und habe den Ablauf des Verfahrens rekonstruiert.

Das Amtsgericht hatte die Vereinsanmeldung dem Landratsamt zur Stellungnahme zugeleitet. Das Landratsamt nahm Kontakt mit der Polizei auf. Dort erfuhr es, daß bei der Kriminalpolizei Informationen zu der Betroffenen existieren sollen. Dies stellte sich nach weiteren Recherchen als falsch heraus. Das Landratsamt teilte dem Amtsgericht mit, keine Bedenken gegen die Eintragung in das Vereinsregister zu erheben. Kurz danach gab das bei Gericht eingegangene Schreiben des geschiedenen Ehemannes der Betroffenen dem zuständigen Richter Veranlassung, einen unbeschränkten Bundeszentralregisterauszug anzufordern. Nach dessen Eingang sollte die Akte dem Landratsamt erneut zur Stellungnahme vorgelegt werden. Die Akte wurde aber durch ein Versehen der Gerichtspoststelle – so das Amtsgericht – der IHK zugeleitet. Diese erkannte die fehlerhafte Aktenzuleitung nicht, sondern meinte, aufgefordert zu sein, zu der Frage Stellung zu nehmen, ob der Verein auf einen wirtschaftlichen Geschäftsbetrieb ausgerichtet ist. Zwar kam sie zu dem Ergebnis, daß dies nicht der Fall ist, doch blieben Zweifel. Sie regte an, die Ein- und Ausgänge des Vereinskontos zu überprüfen, weil die Betroffene in Fernsehen und Presse unter dem noch nicht in das Vereinsregister eingetragenen aber mittlerweile vom Finanzamt als gemeinnützig anerkannten Verein auftrat und um Spenden bat.

Die Einschaltung des Landratsamtes durch das Amtsgericht war korrekt. Denn § 61 Bürgerliches Gesetzbuch (BGB) regelt u.a., daß die Verwaltungsbehörde gegen eine Eintragung in das Vereinsregister Einspruch erheben kann, wenn der Verein nach dem öffentlichen Vereinsrecht unerlaubt ist oder verboten werden kann. Für die Einschaltung der Polizei durch das Landratsamt aber gab es keine Veranlassung. Im Vordergrund der Prüfung, ob die Verwaltungsbehörde von ihrem Einspruchsrecht Gebrauch macht, steht nicht die persönliche Zuverlässigkeit der Vorstandsmitglieder, sondern „ob der Verein nach dem öffentlichen Vereinsrecht unerlaubt ist oder verboten werden kann", also der Zweck und die Tätigkeit des Vereines. Das Hessische Ministerium des Innern und für Europaangelegenheiten hat mit Erlaß vom 24. Januar 1991 (StAnz. 1991 S. 369) näheres zu dem Verfahren bei der Verwaltungsbehörde geregelt. Danach kommt ein Informationsaustausch mit der Polizei über die Vorstandsmitglieder erst dann in Frage, wenn Anhaltspunkte dafür vorliegen, daß der tatsächliche Zweck und die tatsächlichen Ziele des angemeldeten Vereins einen der Verbotsgründe erfüllen könnten. Verbotsgründe liegen vor, wenn der Zweck oder die Tätigkeit des Vereins den Strafgesetzen zuwiderlaufen, wenn der Verein sich gegen die verfassungsmäßige Ordnung richtet oder gegen den Gedanken der Völkerverständigung. Ich bat das Landratsamt um Stellungnahme, worin es solche Anhaltspunkte sah. Es teilte mir mit, daß es nach einer subjektiven Auslegung des VereinsG es für notwendig gehalten habe, bei Satzungsüberprüfungen auch die Person des ersten und zweiten Vorsitzenden mit einzubeziehen. Nach nochmaliger Kenntnisnahme des Erlasses stellte das Landratsamt jedoch fest, daß eine solche Überprüfung nicht erforderlich ist, und sagte zu, die Bestimmungen künftig genauestens beachten zu wollen.

Die Anforderung des unbeschränkten Auszuges aus dem Bundeszentralregister durch den Richter am Amtsgericht möchte ich nicht bewerten, da die Ausübung der richterlichen Tätigkeit nicht meiner Kontrolle unterliegt. Jedenfalls sind die Gerichte durch die Regelung in § 41 Abs. 1 des Bundeszentralregistergesetzes (BZRG) privilegiert. Ihnen darf für Zwecke der Rechtspflege eine unbeschränkte Auskunft aus dem Bundeszentralregister erteilt werden. Allerdings hätte bei der beabsichtigten Übersendung der Akte an das Landratsamt der unbeschränkte Registerauszug entnommen werden müssen. Solche Auskünfte müssen besonders vertraulich behandelt werden. Sie dürfen nur den mit der Entgegennahme und Bearbeitung der Auskunft betrauten Bediensteten zur Kenntnis gebracht werden (§ 44 BZRG).

Die IHK ging davon aus, daß ihr der Vorgang im Rahmen einer Anhörung nach § 12 Gesetz über Angelegenheiten der freiwilligen Gerichtsbarkeit (FGG) übersandt worden war. Danach hat das Gericht von Amts wegen die zur Feststellung der Tatsachen erforderlichen Ermittlungen zu veranstalten und die geeignet erscheinenden Beweise aufzunehmen. Auch wenn die IHK die fehlerhafte Aktenübersendung nicht zu vertreten hat und nicht erkannte oder erkennen konnte (denn sie erfolgte nicht nach § 12 FGG, sondern versehentlich und war damit unzulässig), war jegliche Weiterverarbeitung der Daten durch die IHK unzulässig. Die Betroffene hat gemäß § 19 Abs. 4 Hessisches Datenschutzgesetz einen Löschungsanspruch.

Gemäß § 79 BGB hat „jedermann" das Recht, in das Vereinsregister sowie in die von einem Verein bei dem Amtsgericht eingereichten Schriftstücke einzusehen. Dieses Recht bezieht sich nicht auf Schriftstücke, die nicht von dem Verein eingereicht wurden. Im Zusammenhang mit der Eintragung in das Vereinsregister können, wie der vorliegende Fall aufzeigt, zahlreiche weitere Schriftstücke anfallen. So bezieht sich das Einsichtsrecht nicht auf die Stellungnahme der Verwaltungsbehörde, die Stellungnahme der IHK, den unbeschränkten Auszug aus dem Bundeszentralregister und das unaufgefordert eingegangene denunzierende Schreiben des früheren Ehemannes des Vorstandsmitgliedes. Bei den Amtsgerichten sind, soweit ich dies feststellen konnte, keine organisatorischen Vorkehrungen getroffen, um sicherzustellen, daß eine Einsichtnahme in solche Schriftstücke nicht gewährt wird. Das Hessische Ministerium der Justiz habe ich zu diesem Sachverhalt um Stellungnahme gebeten.

8. Finanzwesen

8.1
Änderung der Abgabenordnung

Bereits in meinem 17. (vgl. Ziff. 11.1) und in meinem 20. Tätigkeitsbericht (vgl. Ziff. 10) habe ich von der beabsichtigten Reform der Abgabenordnung (AO) berichtet.

Der 1988 vom Bundesfinanzministerium vorgelegte Entwurf zur Änderung der Abgabenordnung wurde in den vergangenen Jahren mehrfach überarbeitet, nicht zuletzt aufgrund der Anregungen der Datenschutzbeauftragten des Bundes und der Länder. Erklärte Ziele der Änderung waren die Reform des außergerichtlichen Rechtsbehelfsverfahrens nach der Abgabenordnung sowie die Anpassung an den neuesten Stand der Datenschutzgesetzgebung. Im Mittelpunkt stand dabei die Neufassung des § 30 AO, der das Steuergeheimnis regelt.

Im Juli 1993 überraschte das Bundesfinanzministerium mit der Nachricht, daß aus heutiger Sicht weder eine rechtliche noch eine praktische Notwendigkeit für eine Änderung der Abgabenordnung im Hinblick auf datenschutzrechtliche Vorschriften bestehe.

Trotz ausführlicher Gegendarstellungen seitens der Datenschutzbeauftragten gegen diese Vorgehensweise steht zwischenzeitlich fest, daß der Entwurf für ein Abgabenordnungsänderungsgesetz 1994 nicht weiterverfolgt werden wird. Einige Vorschriften der Abgabenordnung wurden jedoch im Gesetz zur Bekämpfung des Mißbrauchs und zur Bereinigung des Steuerrechts (Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz (StMBG)) vom 29. Dezember 1993 (BGBl. I S.2310) geändert bzw. neu hinzugefügt, dadurch sind aus datenschutzrechtlicher Sicht keine Verbesserungen eingetreten. Im Gegenteil, es wurden gesetzliche Grundlagen geschaffen, die den Steuerbehörden umfangreiche Berechtigungen zugestehen, Daten von Steuerpflichtigen zu sammeln, weiterzugeben und zu verwenden, z. B.:

- Die für die Verwaltung der Grundsteuer zuständigen Behörden sind berechtigt, die aufgrund des Steuergeheimnisses (§ 30 AO) geschützten Namen und Anschriften von Grundeigentümern, die bei der Verwaltung der Grundsteuer bekanntgeworden sind, zur Verwaltung anderer Abgaben sowie zur Erfüllung sonstiger öffentlicher Aufgaben zu verwenden. Sie dürfen diese Daten den hierfür zuständigen Gerichten, Behörden oder juristischen Personen des öffentlichen Rechts auf Ersuchen mitteilen. Dies gilt nicht, soweit überwiegend schutzwürdige Interessen des Betroffenen entgegenstehen (§ 31 Abs. 3 AO).
- Die Finanzbehörden dürfen Sozialleistungsträgern und Subventionsgebern Tatsachen mitteilen, die zur Aufhebung von deren Leistungsbescheiden und zu Erstattungen von Sozialleistungen und Subventionen führen können (§ 31 Abs. 3 AO).
- Die Finanzbehörden dürfen die durch das Steuergeheimnis (§ 30 AO) geschützten Daten auch für Zwecke künftiger Steuerverfahren und Steuerstrafverfahren in Dateien oder Akten sammeln und verwenden (§ 88a AO).

Für mich bleibt festzuhalten, daß zehn Jahre nach Erlaß des Volkszählungsurteils des Bundesverfassungsgerichtes vom 15. Dezember 1983 die Vorgaben des Urteils noch immer keinen Niederschlag in der Abgabenordnung gefunden haben. Die Novellierung ist und bleibt überfällig.

8.2
Telefonkosten als Werbungskosten

Telefonkosten sind als Werbungskosten steuerlich berücksichtigungsfähig, wenn sie ausschließlich beruflich veranlaßt sind. Es obliegt dem Steuerpflichtigen, den von ihm behaupteten Umfang der beruflichen Telefonate gegenüber dem Finanzamt darzulegen.

Zum Nachweis verlangte das Finanzamt Wiesbaden I von einer Lehrerin, daß diese drei Monate lang jedes Gespräch aufzeichnet: den Gesprächsteilnehmer, die Dauer des Anrufs und den Inhalt. Andernfalls könne eine Berücksichtigung des beruflichen Anteils an den Gesamttelefonaten nur nach Maßgabe der Verwaltungsanweisungen geschätzt werden.

Mit dem Finanzamt Wiesbaden I konnte ich klären, daß die Angabe zum Inhalt des Gesprächs weder erforderlich noch verhältnismäßig ist und deshalb nicht mehr aufgeführt werden muß.

Zur Frage, ob und inwieweit die Angabe des Namens eines Gesprächsteilnehmers notwendig ist, um die berufliche Veranlassung des Telefongespräches nachzuweisen, hat sich die Oberfinanzdirektion Frankfurt geäußert. Sie verweist auf eine Verwaltungsanweisung des Bundesfinanzministeriums, wonach der beruflich veranlaßte Anteil von Telefongesprächen durch „geeignete Aufzeichnungen" glaubhaft zu machen ist; hierzu gehöre auch der Name des Gesprächsteilnehmers.

Die von mir vorgeschlagenen Alternativen, den Gesprächspartner entweder mit einer neutralen Bezeichnung (z. B. „Vater eines Schülers, Jugendamt") anzugeben oder eine Bestätigung der Gespräche durch die Schulleitung ausreichen zu lassen, hielt die Oberfinanzdirektion für ungeeignet. Meine Bedenken hinsichtlich der Erforderlichkeit, die Namen unbeteiligter Dritter aufzuzeichnen, konnten hierdurch jedoch nicht ausgeräumt werden.

8.3
Versendung von Kontrollmitteilungen

Im Rahmen von Zuwendungen zur Projektförderung des Landes Hessen in der Jugendpflege war eine Kreisverwaltung verpflichtet, dem Finanzamt Honorarzahlung an Referenten bzw. Betreuer mitzuteilen. Dieser Mitteilungsverpflichtung ist die Kreisverwaltung nachgekommen, indem sie jährlich dem Finanzamt eine Liste zukommen ließ, in der die einzelnen Honorarempfänger sowie der jeweilige Betrag aufgeführt waren.

Ein Betreuer hatte die Kreisverwaltung darauf aufmerksam gemacht, daß er von seinem Finanzamt eine Kopie dieser Liste erhalten hatte. Der Betreuer konnte dieser Liste zu seinem Erstaunen nicht nur entnehmen, welches Honorar er selbst erhalten hat. Auch die Honorare der anderen Referenten und Betreuer waren, zusammen mit deren Anschriften, in der Liste aufgeführt.

Ich habe das zuständige Finanzamt um Aufklärung gebeten. Der Sachverhalt bestätigte sich. Das Finanzamt räumte die Verletzung datenschutzrechtlicher Bestimmungen ein und sicherte zu, organisatorische Vorkehrungen zu treffen, um derartige Vorfälle in Zukunft zu vermeiden.

Darüber hinaus waren für die auf der Liste genannten Personen verschiedene Finanzämter zuständig. Ich habe daher mit der Kreisverwaltung vereinbart, daß sie die für die Einkommensbesteuerung erforderlichen Daten den jeweils für die Personen örtlich zuständigen Finanzämter gesondert übermittelt.

9. Gesundheit

9.1
Maschinenlesbare Patientenkarten mit medizinischen Daten

Maschinenlesbare Karten gibt es in den verschiedensten Formen, insbesondere als Prägekarte oder Magnetstreifenkarte, Chipkarte (einfache Speicherkarte, intelligente Speicherkarte mit Bereichen, auf die nach vorangegangener Prüfung zugegriffen werden kann, multifunktionale Prozessor Chipkarte mit CPU, die Rechenfunktionen und Speicherschutz ermöglichen, sog. „Smart-Cards"), optische Karten (reine Speicherkarten für Anwendungen, die viel Speicherplatz benötigen wie z. B. für Röntgenaufnahmen, Kardiogramme etc.) oder auch als Kombination verschiedener Typen.

Die ab 1993/94 in Chipkartenform bundesweit als Krankenscheinersatz vorgesehene Krankenversichertenkarte (vgl. 21. Tätigkeitsbericht, Ziff. 9.2), die ebenfalls keine medizinischen Daten enthält, ist eine einfache Speicherkarte. Der Umfang der auf der Krankenversichertenkarte gespeicherten Daten ist in § 291 Sozialgesetzbuch V (SGB V) abschließend geregelt (ausstellende Krankenkasse, Name, Geburtsdatum und Anschrift des Versicherten, Krankenversichertennummer, Versichertenstatus, Zeit des Versicherungsschutzes), ebenso der Zweck der Karte. Die Karte darf nur für den Nachweis der Berechtigung zur Inanspruchnahme von Leistungen sowie für die Abrechnung mit den Leistungsträgern verwendet werden. Die mit dem Einsatz der Krankenversichertenkarte verbundenen Fragen betreffen – neben der Datensicherheit – in erster Linie den Gesamtkontext der Verarbeitung der personenbezogenen Versichertendaten: Die Krankenversichertenkarte ist ein Teil der im Gesundheitsreformgesetz und im Gesundheitsstrukturgesetz vom Gesetzgeber vorgesehenen Maßnahmen, mit denen der Gesetzgeber „Transparenz des Leistungsgeschehens" und Kostenbegrenzung im Gesundheitswesen erreichen will.

Unter Verwendung der Krankenversichertenkarte und maschinenlesbarer Formulare werden den Kassenärztlichen Vereinigungen und den Krankenkassen arzt- und patientenbezogene Daten auf Magnetbändern oder anderen maschinell verwertbaren Datenträgern übermittelt, und die Daten können bei diesen Stellen maschinell ausgewertet werden. Umfang und Zweck solcher Auswertungen waren vor Verabschiedung des Gesundheitsstrukturgesetzes Gegenstand intensiver datenschutzrechtlicher Diskussionen, die auch zu einer Reihe von Änderungen des ursprünglichen Gesetzentwurfs geführt haben, insbesondere zu einer strikten Zweckbindung der Versichertendaten. Die datenschutzrechtlichen Fragen betreffen somit weniger den Einsatz der Krankenversichertenkarte selbst als die Speicherung und Weiterverwendung der Versichertendaten bei den Kassenärztlichen Vereinigungen und den Krankenkassen.

Inzwischen zeichnen sich darüber hinausgehend immer mehr Möglichkeiten und Ziele der Verwendung maschinenlesbarer Karten für die Speicherung medizinischer Patientendaten ab. In der Regel geht es hierbei um Smart-Cards, da Präge- oder Magnetstreifenkarten eine zu geringe Speicherkapazität haben und einfache Chipkarten für die Speicherung sensibler Daten auch keine hinreichenden Sicherheitsvorkehrungen gegen einen Mißbrauch der Daten durch Unbefugte ermöglichen. Die bei einfachen Speicherkarten möglichen Sicherheitsvorkehrungen entsprechen in etwa denen einer Magnetstreifenkarte; die Sicherheitsvorkehrungen werden mit den Lesegeräten getroffen, die Karte hat keine eigene Sicherheitslogik.

International werden zahlreiche Pilotstudien zum Einsatz solcher Patientenkarten geplant bzw. durchgeführt, zum Teil existieren auch bereits Routineanwendungen. Die Speicherkapazität der Chipkarten wird sich in absehbarer Zeit so vergrößern, daß technisch gesehen auch die Speicherung der gesamten Krankengeschichte eines Menschen realisierbar sein wird. In Deutschland wird die Krankenversichertenkarte vielfach als Wegbereiter für den Einsatz umfassender Patientenkarten betrachtet, da durch die Einführung der Krankenversichertenkarte eine technische Infrastruktur geschaffen wird, die grundsätzlich auch für den Einsatz weiterer Karten genutzt werden kann.

Dies gibt Anlaß, sich mit den Chancen und Risiken dieser Entwicklung für das Recht auf informationelle Selbstbestimmung der Patienten auseinanderzusetzen.

9.1.1
Notfallkarten, Karten für besondere Patientengruppen, Karten für alle Patienten

Mit den Projekten zum Einsatz von Patientenkarten mit medizinischen Daten werden in den verschiedenen Ländern unterschiedliche Ziele verfolgt. Die Einzelheiten hängen u.a. auch von der jeweiligen nationalen Ausgestaltung des Gesundheitssystems ab. Geht man von den Projekten aus, die – jedenfalls in erster Linie – eine Verbesserung der medizinischen Versorgung der Patienten anstreben, so sind vor allem zu nennen:

- Notfallkarten für eine schnelle und einfache Verfügbarkeit von Notfalldaten (Blutgruppe, Rhesusfaktor, Allergien, Impfungen, für den Notfall wichtige Krankheiten etc.) im Notfall;
- Patientenkarten für besondere Patientengruppen zum Zweck einer verbesserten Kommunikation unter den (mit-) behandelnden Ärzten (Hausarzt, Fachärzte, Fachabteilungen eines Krankenhauses etc.) im Zusammenhang mit der Behandlung chronisch Kranker bzw. solcher Patienten, die intensiver Betreuung und Nachsorge bedürfen, an der regelmäßig verschiedene Ärzte bzw. Institutionen beteiligt sind, sowie
- Patientenkarten zur generellen Verwendung mit einer standardisierten, normierten, strukturierten Behandlungsdokumentation, die dem Arzt einen Überblick über die gesamte Krankengeschichte ermöglicht und die Diagnosestellung und Behandlung erleichtern soll.

Ein Beispiel für eine Karte für Patienten, die intensiver Betreuung bedürfen, ist der in der Medizinischen Hochschule Hannover und verschiedenen Nachsorgestellen getestete Einsatz einer Smart-Card bei der Überwachung von implantierten Defibrillatoren (eine Notfallmaßnahme bei Herz-Kreislauf-Stillstand), die sog. Defi-Card. Betroffen sind hier Patienten, die intensiver Nachsorge nach einem festen zeitlichen Schema bedürfen. Sie erhalten von der Medizinischen Hochschule Hannover nach der Implantation die Defi-Card mit ihren medizinischen Behandlungsdaten und nehmen diese Karte zu allen Nachsorgeuntersuchungen bei den Kliniken ihres Wohnortes mit. Die Daten der Nachsorgeuntersuchungen werden von den diese Untersuchungen durchführenden Ärzten auf der Karte eingetragen. Wenn der Patient wegen einer erneuten Untersuchung, Reimplantation etc. zur Medizinischen Hochschule Hannover kommt, bringt er die aktuelle vollständige Dokumentation seiner Behandlung mit. Die Medizinische Hochschule Hannover aktualisiert und vervollständigt dann wiederum ihren Datenbestand und die Daten auf der Karte.

Ein weiteres Beispiel ist die ab Herbst 1993 mit dem Deutschen Krebsforschungszentrum als Projektkoordinator durchgeführte sog. Machbarkeitsstudie zum Einsatz der Smart-Card in der Krebsnachsorge. Beteiligt sind an der Studie u.a. niedergelassene Ärzte (Hausarzt, Radiologe, Internist etc.), verschiedene Krankenhausabteilungen sowie etwa 150 Patienten. Die Patienten erhalten zu Beginn der Nachsorge die Patientenkarte mit ihren Krankenhausbehandlungsdaten und bringen diese Karte zu jeder Nachsorgeuntersuchung mit. Die Daten sollen beim Arzt in seinen Datenbestand übernommen und aktualisiert und dann auch auf der Karte aktualisiert werden. Die Karte enthält neben Angaben zur Person, zum Versicherungsstatus etc. medizinische Informationen über Dauerdiagnosen (z.B. Diabetes, Allergien usw.), Tumordokumentation und Nachsorgeverlauf. Das Vorlegen der Karte durch den Patienten soll im Regelfall die Versendung eines Arztbriefs ersetzen. Auf jeden Fall enthält die Karte auch Angaben über das letzte Untersuchungsdatum und den behandelnden Arzt, so daß ggf. kurzfristig zusätzlich benötigte Informationen dort erfragt werden können.

Ein Beispiel für ein internationales Projekt ist die für 1994 geplante Pilotinstallation für die DIABCARD. Im Rahmen des AIM-Projektes (AIM = Advanced Informatics in Medicine) der EG-Kommission wird das Projekt DIABCARD unter Beteiligung von Italien, Spanien, Österreich und Deutschland geplant, das auf eine verbesserte Versorgung von Diabetikern abzielt. Die Karte soll eine detaillierte Dokumentation von Testergebnissen und Therapiedaten (Medikation etc.) enthalten, die dann jedem (mit-)behandelnden Arzt zur Verfügung steht.

Für allgemeine Patientenkarten werden z.B. auf europäischer Ebene im Rahmen der Commission Européenne de Normalisation in verschiedenen technischen Kommissionen Standards einer Patientenkarte (insbesondere Beschriftung, Identifikation, Chip-Technik, Struktur der Inhalte, Inhalte der Karte) diskutiert. In den Diskussionen wird gegenwärtig überwiegend nicht davon ausgegangen, daß es sinnvoll ist, die Krankengeschichte vollständig auf einer Patientenkarte zu dokumentieren. Angestrebt wird eine – mehr oder weniger ausführliche – sog. „Basisdokumentation", die auch Angaben zu den jeweiligen behandelnden Ärzten enthält, so daß weitere Details dann ggf. bei diesen erfragt werden können.

Über den Umfang einer solchen Basisdokumentation ist noch keine Einigung erzielt worden. In der Diskussion waren bisher z.B. Angaben zur Identität des Patienten (Geburtsdatum, Adresse, Beruf, Versicherung etc.), Datum des Kontaktes mit den behandelnden Ärzten und Namen der Ärzte, Anlaß des Kontaktes, allgemeine Gesundheitsmerkmale (Größe/Gewicht, Sehfähigkeit, Hörfähigkeit, Blutgruppe, Unverträglichkeiten, Allergien, Risikofaktoren, Impfungen, chronische Krankheiten, Zusammenfassung der klinischen Vorgeschichte, Früherkennungsuntersuchungen etc.), Angaben zur gegenwärtigen Krankheit, Anzahl der Kontakte mit Ärzten hierzu, durchgeführte diagnostische und therapeutische Maßnahmen, Haupt- und Nebendiagnosen, Überweisungen, Ergebnisbewertungen.

9.1.2
Freiwilligkeit bei Verwendung der Karte durch den Patienten

Da § 291 Sozialgesetzbuch V, wie gesagt, eindeutig vorgibt, daß die Krankenversichertenkarte lediglich eine begrenzte Anzahl von persönlichen Angaben über den Versicherten enthalten darf, dürfen auf diese Pflichtkarte keine weiteren, insbesondere keine medizinischen Daten aufgenommen werden. Nach der derzeitigen Gesetzeslage in der gesetzlichen Krankenversicherung ist die Verwendung einer Karte mit medizinischen Daten nur auf freiwilliger Basis zulässig. Hierüber besteht auch grundsätzlich Einigkeit.

Aus datenschutzrechtlicher Sicht bedarf es jedoch einer näheren Betrachtung, was mit „Freiwilligkeit" bei Verwendung der Karte gemeint ist. Hierzu gehören insbesondere auch die Fragen, wieviel Entscheidungsfreiheit der Patient tatsächlich hat und worüber genau der Patient entscheiden kann (welche Daten auf die Karte aufgenommen werden, wer welche Daten auf der Karte lesen darf, wer Daten auf der Karte eintragen, wer die auf der Karte gespeicherten Daten in seinen Datenbestand überspielen darf?). Angesprochen sind hier zentrale Fragen des Arzt-Patientenverhältnisses, die einer Klärung bedürfen.

Grundsätzlich ist die Einwilligung eines Bürgers in die Verarbeitung seiner personenbezogenen Daten nur dann rechtswirksam, wenn er zuvor konkret über den vorgesehenen Umfang und Zweck der Verarbeitung seiner Daten informiert wurde (§ 7 Abs. 2 Hessisches Datenschutzgesetz (HDSG)). Eine Einwilligung des Bürgers kann sich daher nicht auf die generelle Verwendung einer Patientenkarte beziehen, sondern lediglich auf die Verwendung der Patientenkarte in einem konkreten Behandlungskontext; der Bürger muß also in jedem Einzelfall frei entscheiden können, ob er die Karte verwenden will.

Diese Gesichtspunkte sprechen nicht grundsätzlich gegen die Verwendung einer Patientenkarte, sie zeigen jedoch, daß mit einem pauschalen Hinweis auf die „Freiwilligkeit" der Verwendung die mit dem Einsatz einer Patientenkarte verbundenen datenschutzrechtlichen Fragen alleine keineswegs beantwortet sind.

9.1.3
Mehr Transparenz und Selbstbestimmung für den Patienten?

Mit der Patientenkarte werden zum Teil weitgehende Erwartungen hinsichtlich einer Stärkung der Patientenrechte verknüpft. So wird z. B. davon ausgegangen, daß der Patient durch eine Patientenkarte unabhängig wird von den Informationssystemen des Gesundheitswesens, daß er erstmalig „Herr seiner Gesundheitsdaten" wird und frei darüber entscheidet, wer seine Daten einspeichern, lesen und weiterverarbeiten darf.

Richtig ist daran sicherlich, daß die Aushändigung der Daten an den Patienten grundsätzlich die Chance eröffnet, die Patientenrechte in diese Richtung auszugestalten. Eine praktische Umsetzung derartiger Forderungen bzw. Annahmen zeichnet sich bisher allerdings nur sehr begrenzt ab.

Was den Inhalt der Karte anbelangt, so ist er in vielen Projekten, z. B. auch bei der Krebsnachsorgekarte, standardisiert und damit für den Patienten vorgegeben. Offen ist beispielsweise die Frage, was passiert, wenn ein Patient ein Datum – z. B. eine Aidsinfektion – nicht auf der Karte gespeichert haben will, insbesondere nicht auf einem Zugriffsbereich, der für jeden Arzt zugänglich ist, der behandelnde Arzt aber gerade eine Speicherung dieses Datums als Information für andere Ärzte als notwendig ansieht.

Wenn ein Patient darüber entscheiden können soll, welcher Arzt auf welche Daten von ihm zugreifen darf, so setzt dies zunächst technisch voraus, daß auf der Karte differenzierte Zugriffsbereiche eingerichtet sind, sonst läuft nämlich die Entscheidungsfreiheit des Patienten ins Leere. Grundsätzlich ermöglicht die technische Entwicklung der Smart-Cards die Einrichtung differenzierter Zugriffsbereiche. In den derzeitigen Pilotprojekten ist vielfach z. B. zwischen den Bereichen administrative Daten (Name, Adresse, Versicherungsstatus etc.), Notfalldaten und sonstige medizinische Daten unterschieden. Dies wird freilich nicht immer ausreichend sein.

Die Frage ist, wie die Zugriffsbereiche so ausgestaltet werden können, daß das Recht auf informationelle Selbstbestimmung der Patienten und die ärztliche Schweigepflicht hinreichend berücksichtigt sind. Bei der Krebsnachsorgekarte wird z. B. davon ausgegangen, daß jeder behandelnde Arzt sämtliche Behandlungsdaten des Patienten bezüglich der Krebserkrankung lesen können soll, Zugriffsbereiche sind hier insoweit nicht unterschieden. Dies entspricht der Ausgestaltung der Klinischen Krebsregister in Hessen, bei denen jeder (mit-)behandelnde Arzt im onkologischen Schwerpunktkrankenhaus auf sämtliche Daten seiner Patienten zugreifen darf (vgl. 19. Tätigkeitsbericht, Ziff. 5.1; 20. Tätigkeitsbericht, Ziff. 16.4). Die Kenntnis aller Daten ist für jeden Arzt für die Behandlung des Patienten erforderlich, der konkrete Behandlungszusammenhang ist hier gegeben.

Aus datenschutzrechtlicher Sicht problematischer wird die Frage der Ausgestaltung der Zugriffsberechtigung z. B. dann, wenn eine standardisierte, normierte umfassendere Krankengeschichte des Patienten auf der Karte dokumentiert wird. Es erscheint als zweifelhaft, daß tatsächlich bei jedem Arztbesuch die gesamte Patientenhistorie (sämtliche frühere Erkrankungen, Krankenhausaufenthalte, Behandlungsmaßnahmen etc.) eingesehen werden muß, unabhängig vom konkreten Behandlungszusammenhang.

Grundsätzlich besteht Konsens darüber, daß der Patient seine auf der Karte gespeicherten Daten lesen können muß. Dies kann z. B. durch einen aktuellen schriftlichen Ausdruck oder durch ein eigens beim Arzt dafür bereitgestelltes

Terminal realisiert werden. Auch unabhängig von der Verwendung einer Patientenkarte hat der Patient nach der gegenwärtigen Rechtslage grundsätzlich das Recht, seine Krankengeschichte einzusehen. In Hessen ist dies für die Krankenhäuser gesetzlich festgelegt (§§ 12 Hessisches Krankenhausgesetz, 18 HDSG). Im übrigen ist dies durch die Rechtsprechung des Bundesgerichtshofs schon vor einigen Jahren entschieden worden (BGH NJW 1983, 328; NJW 1983, 330; NJW 1985, 674). In der Praxis ist dieses Recht allerdings bisher nur teilweise realisiert worden. Es kommt keineswegs selten vor, daß sich Patienten an mich wenden, weil ihnen mit unzutreffender rechtlicher Begründung eine Einsicht in ihre Krankengeschichte verwehrt wurde. Die Verwendung einer Patientenkarte könnte folglich möglicherweise zu mehr Transparenz führen.

Zur Herstellung von Transparenz für den Patienten gehört jedoch nicht nur die Frage, welche Daten jeweils aktuell auf der Karte über ihn gespeichert sind, sondern auch die Frage, wer diese Daten in welchem Umfang zu welchem Zweck weiterverarbeitet, insbesondere, in welchem Umfang und zu welchem Zweck die auf seiner Karte gespeicherten Daten vom Arzt in dessen Datenbestand übernommen werden. Die Vorstellung, daß der Patient mit Hilfe der Patientenkarte Herr seiner Gesundheitsdaten wird und nunmehr selbst entscheidet, wer welche Informationen erhält, setzt im Grunde voraus, daß der Patient alleine Inhaber seiner Daten ist (für den Fall des Verlustes oder des Diebstahls der Karte muß der Datenbestand allerdings an irgendeiner Stelle – z. B. beim Hausarzt – parallel gespeichert sein, damit er ggf. rekonstruiert werden kann). Infolge der technischen Infrastruktur ist es jedoch technisch ohne Aufwand möglich, daß jeder Arzt alle Daten des Patienten von der Karte in seinen Datenbestand übernimmt und dann wiederum Ärzte ohne Beteiligung des Patienten diese Daten untereinander austauschen, z. B. über Kommunikationsnetze.

Die Frage, ob durch die Einführung einer Patientenkarte mehr Transparenz für den Patienten hergestellt wird, hängt daher maßgeblich von den Einzelheiten der Verwendung der Karte ab. Der Einsatz der Karte kann auch dazu führen, daß für den Patienten immer schwieriger überblickbar wird, wer welche Daten über ihn vorhält, weil die Karte die technische Möglichkeit bietet, seine Krankengeschichte ohne einen konkreten Behandlungskontext zu übernehmen und weiterzuverarbeiten. Mit der Chipkarte kann auch die Verwendung der Daten nicht mehr kontrolliert werden, wenn die Daten an den Computer des Arztes weitergegeben wurden. Eine Kontrolle der Verwendung wäre z. B. in der Weise denkbar, daß der Arzt nur eine speziell zugelassene Software verwendet und von der Chipkarte überprüft wird, ob das Programm verändert wurde.

9.1.4
Fazit

In Deutschland ist bisher noch nicht absehbar, in welchem Umfang und auf welche Weise maschinenlesbare Patientenkarten mit medizinischen Informationen künftig eingesetzt werden.

Die voranstehenden Überlegungen zeigen, daß das technische Medium maschinenlesbare Karte in sehr verschiedener Weise eingesetzt werden kann. Für die datenschutzrechtliche Bewertung sind die Einzelheiten des Inhalts und der Verfahrensweise mit der Karte entscheidend.

Jeder Bürger hat selbstverständlich das Recht, sich eine Patientenkarte zu verschaffen, wenn er dies wünscht. Die rechtlichen Rahmenbedinungen der Verwendung von Patientenkarten bedürfen jedoch weiterer Diskussion. Aus meiner Sicht geht es darum, bei der Diskussion um künftige Einsatzmöglichkeiten datenschutzrechtliche Aspekte rechtzeitig zu berücksichtigen.

Die Einführung medizinischer Patientenkarten macht es notwendig, die Rechte und Pflichten von Patienten und Ärzten bzw. medizinischem Personal klarer festzulegen und umzusetzen. Transparenz muß für den Patienten sichergestellt werden. Die verfassungsgerichtliche Forderung, jeder Bürger müsse wissen, wer wann welche Daten über ihn hat, muß auch und gerade für die Verarbeitung sensibler medizinischer Daten gelten. Dies gilt allerdings nicht nur im Zusammenhang mit dem Einsatz der Patientenkarte. Bereits der Aufbau komplexer Krankenhauskommunikationssysteme macht es schwierig für den Patienten zu überblicken, in welchem Umfang und zu welchem Zweck im Krankenhaus Daten über seine Person verarbeitet werden. Ich habe mich daher in den letzten Jahren dafür eingesetzt, durch die Ausgestaltung der Aufnahmeformulare mehr Transparenz für die Patienten im Krankenhaus sicherzustellen (vgl. 9.8). Auch die Entwicklung präzise formulierter Schweigepflichtentbindungserklärungen ist ein wichtiger Schritt zu mehr Transparenz (vgl. 9.3).

Bei der Diskussion um die Patientenkarten kommt auch Aspekten der Datensicherheit zentrale Bedeutung zu. Selbstverständlich muß eine Patientenkarte mit sensiblen medizinischen Daten umfangreiche Sicherheitsmaßnahmen vorsehen gegenüber einem Mißbrauch der Daten, insbesondere Schutzmechanismen gegen unerlaubtes Lesen (Identifikation und Authentifikation des Arztes als Zugriffsvoraussetzung, Freigabe bestimmter Zugriffsbereiche durch den Patienten z. B. durch Eingabe einer PIN (Personal Identification Number) oder durch Prüfung biometrischer Merkmale, Verschlüsselung des Dateninhalts), gegen unerlaubtes Schreiben (z. B. Einfügen eines MAC (Message Authentication Code), durch den eine nachträgliche Veränderung des geschriebenen Wertes erkannt werden kann; Verwendung eines Datenspeichers, der nur einmal beschreibbar ist), gegen unerlaubtes Löschen (bei wiederbeschreibbarem Speicher ist die Eingabe eines Schlüssels für das Löschen von Daten denkbar) sowie gegen unerlaubtes Duplizieren der Chipkarte.

Als Hessischer Datenschutzbeauftragter sehe ich es als meine Aufgabe an, mich an der Diskussion um die künftige Verwendung von Patientenkarten zu beteiligen. Konkrete Lösungen können jedoch nicht isoliert aus datenschutzrechtlicher Sicht, sondern nur im Dialog zwischen allen Beteiligten gewonnen werden.

9.2
Prüfung Universitätsklinikum Frankfurt

1993 habe ich die Verarbeitung personenbezogener Patientendaten im Universitätsklinikum Frankfurt geprüft. Gegenstand der Prüfung war das Verfahren bei der Patientenaufnahme, die Umsetzung der neuen Vorschriften des Gesundheitsstrukturgesetzes, die vom Hessischen Krankenhausgesetz (HKHG) vorgeschriebene Abschottung der Datenbestände der Fachabteilungen untereinander und die Verarbeitung personenbezogener Daten in zwei – stichprobenhaft ausgewählten – Fachabteilungen.

9.2.1
Patientenaufnahme

Wöchentlich werden im Universitätsklinikum etwa 600 Patienten stationär aufgenommen. Die Aufnahme erfolgt – mit Ausnahme der Notfälle, die direkt in den Behandlungseinheiten aufgenommen werden – zentral für alle Behandlungseinheiten in der Aufnahme- und Abrechnungsabteilung der Verwaltung. Zum Zeitpunkt der Prüfung war die Aufnahme- und Abrechnungsabteilung aus baulichen Gründen provisorisch im Zentrum für Innere Medizin untergebracht.

Bei der Prüfung der räumlichen und organisatorischen Sicherungsmaßnahmen habe ich trotzdem keine gravierenden Mängel vorgefunden.

Die räumlichen Sicherungsmaßnahmen können für dieses Provisorium als ausreichend bezeichnet werden.

Der Zugang ist mit einer Stahltür, die mit einem Sicherheitsschloß ausgestattet ist, gesichert. Die Schlüsselvergabe wird restriktiv gehandhabt. Die Fensterfront befindet sich im ersten Stock des Gebäudes.

Die neuen Patienten werden zunächst im vorderen Teil der Patientenaufnahme, einem Großraumbüro, das mit ca. 20 Mitarbeitern besetzt ist, an vier Bildschirmarbeitsplätzen bedient.

Diese Bildschirmarbeitsplätze sind relativ nahe aneinander plaziert, so daß ein Mithören von unberechtigten Personen nicht ausgeschlossen werden kann. Mir wurde versichert, daß die Mitarbeiter der Patientenaufnahme sich dessen bewußt sind und versuchen, die notwendigen Gespräche so zu führen, daß ein Mithören nach Möglichkeit vermieden wird.

In den Fällen, in denen nach der Erfassung der Daten noch Fragen zur Krankenversicherung bzw. zur Kostenübernahme zu klären sind, werden die Patienten zu den für ihren Namen zuständigen Mitarbeitern im hinteren Teil des Raumes verwiesen. Dort sind jeweils zwei Mitarbeiter an aneinander gestellten Schreibtischen für jeweils eine „Buchstabengruppe" zuständig.

Es konnte nicht ausgeschlossen werden, daß gleichzeitig zwei Patienten an diesen Arbeitsplätzen bedient werden. In diesen Fällen ist es den Patienten zum einen möglich, die Gesprächsinhalte Dritter zur Kenntnis zu nehmen, und zum anderen die auf den Schreibtischen liegenden Unterlagen zu lesen, den dort installierten Bildschirm einzusehen und die Telefonate der Mitarbeiter zu verfolgen.

Nach meiner Beratung wurde mir zugesagt, diese Praxis sofort zu ändern. Zukünftig wird auch bei größerem Andrang in der Patientenaufnahme nur noch ein Patient pro „Buchstabengruppe" bedient.

Die Patientenakten werden auf den Schreibtischen der Sachbearbeiter bis zur Rechnungstellung offen in Karteikästen aufbewahrt. Die Aufstellung von Aktenschränken, in denen diese Unterlagen nach Dienstschluß aufbewahrt werden können, ist aus räumlichen Gründen nicht möglich.

Ein Zugriff auf die Patientendaten über die an den Zentralrechner angeschlossenen Bildschirme ist nur durch Eingabe einer Benutzeridentifikation und eines Paßwortes zu erreichen. Wird innerhalb von ca. drei Minuten an diesen Bildschirmen keine Eingabe getätigt, erfolgt durch das System automatisch eine Inaktivierung, d.h. daß die Sachbearbeiter erst nach erneuter Eingabe des Paßwortes Daten abrufen oder erfassen können.

Zwei „Stand-alone PC's" in der Patientenaufnahme waren nicht durch eine Datensicherungssoftware geschützt. Dies habe ich bemängelt. Mir wurde die Installation einer entsprechenden Schutzsoftware zugesagt.

Eine Besichtigung der sich z.Zt. im Bau befindlichen neuen Räumlichkeiten der Patientenaufnahme zeigte, daß zukünftig gewährleistet werden kann, daß die von mir in der „provisorischen" Patientenaufnahme festgestellten Mängel z.B. durch Einbau von sog. Besprechungskabinen und Aufstellung von Aktenschränken und Raumteilern nicht mehr relevant sein werden.

Bei der Aufnahme in der Verwaltung muß der Patient zunächst das Krankenhaus-Aufnahmeformular ausfüllen. In meinen beiden letzten Tätigkeitsberichten hatte ich darüber berichtet, daß die Aufnahmeformulare zahlreicher Krankenhäuser noch nicht den Anforderungen des Hessischen Krankenhausgesetzes entsprechen und daß als Hilfestellung für die Kliniken gemeinsam von der Hessischen Krankenhausgesellschaft und meiner Dienststelle ein Muster-

formular entwickelt wurde (21. Tätigkeitsbericht, Ziff. 18.5). Das vom Universitätsklinikum Frankfurt verwendete Aufnahmeformular war bereits in neuerer Zeit überarbeitet, entsprach aber noch nicht vollständig den rechtlichen Vorgaben. Die durch §§ 12 Abs. 1 HKHG, 12 Abs. 4, 18 Abs. 2 Hessisches Datenschutzgesetz (HDSG) vorgeschriebene Information und Benachrichtigung der Patienten (vgl. hierzu 9.8) über die Verarbeitung ihrer Daten im Krankenhaus war unzureichend. Mir wurde mitgeteilt, daß der Vorrat an Formularen nur noch bis zum Frühjahr 1994 reicht und derzeit ein Entwurf für ein neues Formular von allen Universitätskliniken gemeinsam erstellt wird, das mir zur Stellungnahme übersandt wird.

In dem zum Zeitpunkt der Prüfung verwendeten Formular war – entsprechend den datenschutzrechtlichen Forderungen – bereits vorgesehen, daß der Patient bei der Aufnahme darüber entscheiden kann, ob seine Daten an der Pforte an Dritte weitergegeben werden. Der Patient kann hierzu auf dem Aufnahmeformular seine Einwilligung erteilen. Der Pförtner erhält täglich eine aktualisierte Liste der im Klinikum befindlichen stationären Patienten. Sofern ein Patient bei der Aufnahme nicht in die Weitergabe seiner Daten an der Pforte eingewilligt hat, ist auf der Liste eine Auskunftssperre vermerkt.

In der Aufnahme- und Abrechnungsabteilung werden die in dem Aufnahmeformular erhobenen sog. „Patientenstammdaten" auch automatisiert erfaßt. Hinsichtlich Umfang und Dauer der Datenspeicherungen habe ich keine datenschutzrechtlichen Probleme festgestellt. Konkret handelt es sich um insgesamt 43 Datensätze, insbesondere die Patienten-Aufnahmenummer, Name, Geburtsdatum, Geschlecht, Adresse, Behandlungseinheit, Aufnahme- und Entlassungsdatum, Angaben zum Hauptversicherten und zur Abrechnungsart. Ein Teil dieser Patientenstammdaten wird in regelmäßigen Zeitabständen (etwa zwei bis drei Jahre) archiviert und ist für die Mitarbeiter in der Aufnahme- und Abrechnungsabteilung nicht mehr abrufbar. Im Direktzugriff bleibt für die Mitarbeiter dann nur ein sog. „Rumpfdatensatz", aus dem bei einer Neuaufnahme des Patienten insbesondere ersichtlich ist, in welcher Behandlungseinheit sich die bereits zu einem früheren Zeitpunkt angelegte Krankenakte befindet. Bei der Neuaufnahme wird dann dieser „Rumpfdatensatz" um die vom Patienten aktuell angegebenen weiteren Daten ergänzt.

9.2.2
Umsetzung des Gesundheitsstrukturgesetzes

Mit den Neuregelungen des Gesundheitsreformgesetzes vom 20. Dezember 1988 (BGBl. I S. 2477) und des Gesundheitsstrukturgesetzes vom 21. Dezember 1992 (BGBl. I S. 2266), durch die der Gesetzgeber „Transparenz des Leistungsgeschehens" und Kostenbegrenzung im Gesundheitswesen erreichen will, sind u.a. die Leistungserbringer verpflichtet worden, den Krankenkassen zusätzliche medizinische Daten über die Versicherten zu übermitteln. So sieht die Neufassung des § 301 Sozialgesetzbuch V (SGB V) einen erheblich erweiterten Datenkatalog für die routinemäßige Übermittlung von den Krankenhäusern an die Krankenkassen in jedem Behandlungsfall vor. Die Daten müssen künftig auch maschinenlesbar übermittelt werden, damit sie von den Krankenkassen umfassender ausgewertet werden können. Bei meiner Prüfung habe ich festgestellt, daß das Universitätsklinikum wegen der notwendigen Umstellungen der EDV-Programme die Vorschriften bisher noch nicht vollständig umsetzen konnte. Nach mir vorliegenden Informationen ist dies auch in anderen Krankenhäusern der Fall.

9.2.3
Abschottung der Fachabteilungen untereinander

Das Krankenhaus ist keine Einheit, innerhalb der personenbezogene Patientendaten beliebig weitergegeben werden dürfen. Der Grundsatz der Zweckbindung der Daten ist zu beachten (§ 12 Abs. 1 HKHG, §§ 13, 12 HDSG). Die ärztliche Schweigepflicht i.S.v. § 203 Strafgesetzbuch gilt grundsätzlich auch innerhalb des Krankenhauses, auch im Verhältnis der Ärzte untereinander. Das Hessische Krankenhausgesetz regelt daher, daß die Vorschriften über die Übermittlung von Patientendaten vom Krankenhaus an externe Stellen in Krankenhäusern mit Behandlungseinrichtungen verschiedener Fachrichtungen (Fachabteilungen) auch zwischen diesen gelten (§ 12 Abs. 3 HKHG).

Bei meiner stichprobenhaften Überprüfung der Ausgestaltung der Direktzugriffe auf die automatisiert gespeicherten medizinischen Patientendaten in den Fachabteilungen habe ich festgestellt, daß diese rechtlichen Vorgaben beachtet werden. In verschiedenen Fachabteilungen wird das Verfahren „Befunddokumentation und Arztbriefschreibung in Krankenhäusern (BAIK)" eingesetzt. Zugriff auf die medizinischen Patientendaten hat jeweils nur die behandelnde Fachabteilung selbst.

Da das Verfahren der abteilungsübergreifenden Weitergabe von Patientendaten zu Forschungszwecken während der Prüfung nicht geklärt werden konnte, habe ich zu diesem Punkt noch um eine schriftliche Auskunft gebeten.

9.2.4
Verarbeitung von Patientendaten in der Abteilung Thorax-, Herz- und Gefäßchirurgie des Zentrums der Chirurgie

1983 wurde in der Abteilung Thorax-, Herz- und Gefäßchirurgie des Zentrums der Chirurgie begonnen, Patientendaten – Patientenstammdaten, ausgewählte Diagnose- und Therapiedaten – parallel zur herkömmlichen Krankenakte mit dem Einsatz des Verfahrens zur „Befunddokumentation und Arztbriefschreibung in Krankenhäusern (BAIK)" zu speichern. Zum Zeitpunkt der Prüfung waren die Daten von etwa 12.000 Patienten in der BAIK-Datei gespeichert. Die Anwendung ist auf zwei vernetzten PC's implementiert. Auf einem PC sind die Daten gespeichert, auf dem

anderen PC werden Teile des Datenbestandes zur Sicherung gegen Ausfall gespiegelt. Die Fachabteilung erhält die in der zentralen Aufnahme- und Abrechnungsabteilung ausgedruckten Patientenetiketten. Diesen Etiketten entnimmt die Fachabteilung die Aufnahmenummer, gibt diese in den PC ein und läßt sich sodann von der Aufnahme- und Abrechnungsabteilung einen Teil der dazugehörigen Patientenstammdaten überspielen. Die medizinischen Daten werden in der Fachabteilung in die BAIK-Datei eingegeben. Der Umfang der gespeicherten Daten wirft keine datenschutzrechtlichen Probleme auf, jedoch sind noch Fragen zum Zweck und zur Dauer der automatisierten Speicherung der Daten zu klären.

Die automatisierte Verarbeitung der Patientendaten soll der Routineunterstützung der Dokumentation, der automatischen Erstellung von Arztbriefen, Patientenanschreiben und OP-Berichten sowie statistischen und wissenschaftlichen Auswertungen dienen. Fristen für die Löschung von Patientendaten in der BAIK-Datei sind bisher nicht festgelegt worden und auch nicht geplant. Die Speicherung der Patientendaten soll „dauerhaft" erfolgen.

Ich habe Zweifel, daß es erforderlich ist, die personenbezogenen Daten sämtlicher Patienten im Direktzugriff auf unbegrenzte Zeit – also sogar noch über die Aufbewahrungsfristen für die Krankenakten hinaus, vorzuhalten. (Nach § 11 der Berufsordnung für Ärztinnen und Ärzte in Hessen sind ärztliche Aufzeichnungen zehn Jahre nach Abschluß der Behandlung aufzubewahren, soweit nicht nach anderen Vorschriften eine längere Aufbewahrungsfrist besteht. Eine längere Aufbewahrung ist auch dann erforderlich, wenn sie nach ärztlicher Erfahrung geboten ist.) Über die Länge der Fristen einer Speicherung kann sicherlich diskutiert werden, die automatisiert geführte BAIK-Datei darf jedoch nicht völlig losgelöst vom Behandlungszusammenhang verwendet werden.

Soll die BAIK-Datei für wissenschaftliche Zwecke weiterverwendet werden, muß sie entsprechend strukturiert und muß auch so weit wie möglich mit anonymisierten Daten gearbeitet werden. Zu diesem Punkt habe ich das Universitätsklinikum um Stellungnahme gebeten, auch im Hinblick auf die in den anderen Fachabteilungen entsprechend vorhandene Problematik.

Die Fachabteilung beteiligt sich seit dem 1. Januar 1992 an bundesweit durchgeführten Qualitätssicherungsmaßnahmen in der Herzchirurgie. Mit diesen Maßnahmen werden die gesetzlichen Vorgaben der §§ 137, 112 SGB V für externe Qualitätssicherungsmaßnahmen erfüllt. Für die organisatorische und fachliche Durchführung dieser Maßnahmen hat die Ärztekammer Nordrhein in Düsseldorf eine Projektgeschäftsstelle unter ärztlicher Leitung eingerichtet. Bestimmte in der Herzchirurgie vorgenommene Eingriffe unterliegen der Dokumentationspflicht. Aufgrund der erhobenen Daten muß die Projektgeschäftsstelle mindestens einmal jährlich pro Klinik eine Gesamtstatistik mit einem Vergleich der Gesamtheit aller Kliniken herausgeben. Daran kann jede Klinik erkennen, inwieweit sie von den Werten der Gesamtstatistik abweicht. Eine vom Bundeskuratorium eingesetzte Fachkommission hat die Möglichkeit, die Gesamtstatistik zu kontrollieren und bei evtl. vorhandenen statistischen Abweichungen beratend in einer Klinik tätig zu werden.

Die Landesärztekammer erhält von der Fachabteilung nicht die vollständigen Patientenstammdaten, sondern lediglich die Kliniknummer, die Fallnummer, das Geburtsdatum, Geschlecht, Aufnahme- und Entlassungsdatum bzw. Todesdatum der Patienten und medizinische Angaben zu den durchgeführten Operationen. Diese Angaben habe ich im konkreten Verwendungszusammenhang als hinreichend anonymisiert angesehen.

Trotz einer Reihe von technischen und organisatorischen Datensicherungsmaßnahmen zeigten sich Schwachstellen, die beseitigt werden müssen.

Die PC's sind in einem separaten Raum installiert, dessen Tür mit einem Sicherheitsschloß versehen ist. Schlüssel besitzen nur die Erfassungskräfte, der zuständige Arzt und der EDV-Betreuer. Es gilt die Anweisung, den Raum abzuschließen, wenn keine berechtigte Person anwesend ist. Diese Maßnahmen sind grundsätzlich geeignet, die Zugangskontrolle zu gewährleisten. Es war jedoch zweifelhaft, ob auch der EDV-Betreuer als zutrittsberechtigte Person anzusehen ist. Aufgabe des EDV-Betreuers ist es, Fehler zu beheben und sporadisch neue Anwendungsfunktionen nach den Wünschen der Anwender zu erstellen. Die PC's in der Herz-Thorax-Klinik sind für die medizinische Anwendung bestimmt; die Programmierung und der Test neuer Anwendungsfunktionen darf nur auf einem getrennten Rechner mit Testdaten erfolgen. Die Nutzung der beiden PC's zur Anwendungsentwicklung ist somit nicht zulässig. Stellen Benutzer Fehler fest, rufen sie den Betreuer, der dann in Anwesenheit der berechtigten Person den Fehler behebt. Folglich benötigt der EDV-Betreuer auch für diesen Fall keinen Schlüssel zu dem Raum. Ich habe daher gefordert, den Kreis der zutrittsberechtigten Personen auf die Erfassungskräfte und den zuständigen Arzt zu beschränken. Dies wurde mir inzwischen zugesagt.

Die PC's sind durch Hardware-Paßwörter geschützt. Um mit der Anwendung arbeiten zu können, mußte zusätzlich eine Anmeldeprozedur durchlaufen werden, in der Benutzerkennungen und Paßwörter abgefragt wurden. Defizite ergaben sich dadurch, daß die Standardanforderungen an eine Paßwortverwaltung nicht erfüllt waren und durch Booten von den Diskettenlaufwerken die Anmeldeprozedur umgangen werden konnte. Eine Protokollierung, wer wann mit der Anwendung gearbeitet hat, erfolgt nicht. Da alle berechtigten Personen umfassende Zugriffsrechte auf die Daten haben, geht es vorrangig darum, die Nachvollziehbarkeit der Datenverarbeitung zu erreichen. Hierzu sollten die PC's mit einer Datenschutzsoftware ausgestattet werden. Damit könnten die Daten außerdem verschlüsselt werden, so daß weitere Risiken für den Datenschutz minimiert würden.

9.2.5
Verarbeitung von Patientendaten im Zentrum der Radiologie

Im Zentrum der Radiologie, Abteilung für Allgemeine Röntgendiagnostik, werden seit März 1987 alle Patientendaten auf dem DV-System RADOS, einem modular strukturierten Informationssystem für die Radiologie im Krankenhaus/Röntgeninstitut, das in zahlreichen Krankenhäusern eingesetzt wird, gespeichert. Es dient insbesondere der Patientenadministration, dem Ausdruck von Patientenpapieren (Etiketten, Formularen, Bestrahlungsplänen etc.), der Befundschreibung, Leistungskontrolle, Abrechnung, Erstellung von Listen, Statistiken und medizinischen Auswertungen sowie der Filmtüten-Verwaltung. Außerdem wird RADOS eingesetzt für die in § 28 Röntgen-Verordnung vorgeschriebene Dokumentation jeder Anwendung von Röntgenstrahlen. Eine Dokumentation in Papierform bzw. in einer manuellen Kartei ist in der Fachabteilung nicht mehr vorhanden. Zum Zeitpunkt der Prüfung waren die Daten von etwa 80.000 Patienten in RADOS gespeichert.

9.2.5.1
Die Technik von RADOS

- Betriebssystem
  RADOS ist eine unter MUMPS programmierte Anwendung. Bei MUMPS handelt es sich um eine offene Datenverarbeitungstechnologie, die aus Programmiersprache, Daten-Speicherungs- und Retrievalsystem, Transaktionsmonitor (multiuser, multitasking), Dialogmonitor, Netzwerkmanagement und Grafik-Interface besteht. MUMPS ist ein ISO-Standard und auf viele Rechnerplattformen portiert. Im Fall des Uniklinikums läuft RADOS auf einem PC mit MS-DOS als Basis-Betriebssystem.

Wenn MUMPS gestartet wird, verwandelt sich der PC in einen Rechner mit einem multiuser, multitasking Betriebssystem. Aus einem Rechner, an dem nur eine Person arbeiten kann, wird so ein Rechner, an dem viele Personen mit ihren Terminals gleichzeitig arbeiten können. Dabei ist dieser PC leistungsfähiger als z. B. PDP-11 Rechner, auf denen vor einigen Jahren die ersten RADOS-Installationen erfolgten.

- Vernetzung
  Im Rechenzentrum des Uniklinikums gibt es keinen Zentralrechner, sondern die Anwendungen sind auf mehrere Rechner verteilt. Welches Terminal mit welchem Rechner und daher mit welchen Anwendungen arbeiten kann, wird über einen Vermittlungsrechner gesteuert.

Die Terminals sind an den Vermittlungsrechner angeschlossen, der über Terminalserver die Verbindung zu den verschiedenen Rechnern herstellen kann. An der physischen Leitung, über die eine Anfrage erfolgt, erkennt der Verbindungsrechner ein Terminal.

Wenn ein Benutzer mit verschiedenen Rechnern arbeiten darf, muß er sich mit einem eigenen Paßwort ausweisen. Anschließend kann er seinen Verbindungswunsch angeben.

Wenn, wie im Fall der RADOS-Terminals, nur mit einem Rechner gearbeitet werden darf, wird die Verbindung direkt hergestellt. Ein Zugriff auf andere Rechner oder ein Verbindungswunsch anderer Terminals wird unterbunden. Auf dem RADOS-Rechner sind die Terminals im MUMPS als sog. „Tied-Terminals" definiert. Das bedeutet, die Terminals werden nur mit der Anwendung verbunden. Es ist nicht möglich, auf die Betriebssystemebene zu gelangen oder andere Anwendungen aufzurufen. Ein Zugriff auf RADOS ist daher nur von den zugelassenen Terminals aus möglich und von diesen Terminals, mit Ausnahme des Terminals des Systemverwalters, kann nur mit RADOS gearbeitet werden.

9.2.5.2
Schutzfunktionen bei RADOS

Benutzerkontrolle
Um mit RADOS arbeiten zu können, muß ein Benutzer eine gültige Benutzerkennung besitzen, mit der er sich unter RADOS anmeldet. Jede Benutzerkennung ist an eine Benutzergruppe gekoppelt, der gewisse Zugriffsrechte gegeben sind.

Ohne eine Anmeldung an RADOS ist es nicht möglich, mit der Anwendung zu arbeiten. Hierzu müssen die Benutzerkennung und das zugehörige Paßwort eingegeben werden. Im Bereich der Paßwortverwaltung gibt es dabei Schwachstellen. In der neuesten Version, die im Uniklinikum Frankfurt zum Zeitpunkt der Prüfung unmittelbar vor dem Einsatz stand, sind diese teilweise behoben. Es soll daher dieser Stand geschildert werden.

In weiten Teilen entspricht die Paßwortverwaltung den von mir im 19. Tätigkeitsbericht (Ziff. 15.5.4) dargelegten Vorstellungen. Dies gilt z. B. für den Ablauf bei der Vergabe von Paßwörtern, der verschlüsselten Speicherung oder der Mindestlänge von sechs Stellen. Auch erfolgt ab der dritten Fehleingabe eines Paßwortes eine Zwangspause von mehreren Sekunden vor der nächsten Anmeldung. Trotz der Verbesserungen zum alten Stand sind noch einige Anpassungen vorzunehmen:

- Es muß möglich sein, eine maximale Gültigkeitsdauer von Paßwörtern festzulegen.
- Es sollte eine Historie von Paßwörtern existieren, damit nicht nur zwischen zwei Paßwörtern gewechselt wird.

- Es sollte eine Mindestgültigkeit einstellbar sein, damit nicht, wenn ein neues Paßwort verlangt wird, so lange neue Paßwörter vergeben werden, bis das alte wieder gültig ist.
- Es sollte eine Anzeige erfolgen, wann die letzte Anmeldung mit dieser Kennung erfolgte.

Speicherkontrolle
Wenn fünf Minuten lang keine Eingaben über das Terminal erfolgen, wird die Anwendung mit einem Zwangs-Logoff beendet. Die Modularisierung der Anwendung würde es allerdings auch gestatten, in Abhängigkeit von der jeweiligen Funktion das Zeitintervall festzulegen. Ob und welche Anforderungen zu stellen sind, wird in der Universitätsklinik geklärt.

Zugriffskontrolle
Die Anwendung ist in Form eines Menü-Baumes aufgebaut. Hinter jedem Menüpunkt steht entweder ein Untermenü oder ein Anwendungsprogramm. Einer Benutzergruppe kann der Zugriff auf einen Menüpunkt, d.h. auf die Anwendung oder die Untermenüs, erlaubt oder verwehrt werden. So werden für jede Benutzergruppe spezifische Sichten der Anwendung geschaffen.

Es ist möglich, diese Anwendungssicht noch für jede Benutzergruppe nach dem Terminal, von dem aus der Zugriff erfolgt, unterschiedlich zu gestalten.

Eine Differenzierung der Zugriffe auf Daten innerhalb der Anwendungsfunktion ist nicht möglich. Eine Ausnahme bilden Befunde. Hier kann der Zugriff explizit für jeden Befund geregelt werden. Dazu wird für den Befund ein Paßwort vergeben. Ein Zugriff ist nur möglich, wenn dieses eingegeben wird.

Protokollierung
Es gibt derzeit keine Systemprotokolle, mit denen die Revision der Datenschutzmaßnahmen unterstützt wird. Welche Protokolle sinnvoll eingesetzt werden können, muß im Einzelfall geklärt werden. Anhaltspunkte habe ich im 20. Tätigkeitsbericht (Ziff. 15.2.2.2) gegeben.

Reaktion des Herstellers
Ich habe dem Uniklinikum die Schwachstellen genannt. Parallel dazu ist es zu Kontakten mit dem Hersteller von RADOS gekommen. Nach dem jetzigen Stand der Dinge ist zu erwarten, daß die Schwachstellen schnell behoben werden.

Zugangskontrolle
Neben den aus der Anwendung kommenden Schutzfunktionen gibt es Maßnahmen baulicher Art, die das Klinikum zu treffen hat. Der PC steht im Rechenzentrum der Universitätsklinik. Es gelten daher die gleichen Zugangsbeschränkungen wie für die anderen Zentralrechner der Verwaltung.

Die Sicherheit des PC's selbst ist analog dem Vorgehen bei Stand-alone PC's zu erreichen.

9.2.5.3
Ergebnisse

Datenschutzrechtliche Probleme habe ich hinsichtlich der Ausgestaltung der Zugriffsberechtigungen festgestellt. Nahezu alle eingerichteten Benutzergruppen (Sekretariate, Professoren, Oberärzte, Ärzte, Leitende medizinisch-technische Röntgenassistenten, Vertretung Leitende medizinisch-technische Röntgenassistenten, medizinisch-technische Röntgenassistenten, Patientenanmeldung, Schreibkräfte, Hilfskräfte) haben Zugriff auf die Funktionen Archivauskunft, d.h. auf die Grunddaten sämtlicher bisher in der Abteilung behandelten – derzeit ca. 80.000 – Patienten, und alle in RADOS zu diesen Patienten gespeicherten Befunde. Die gegebene technische Möglichkeit, den Zugriff auf einzelne Befunde einzuschränken, wird in der Regel nicht genutzt. Ferner hat die überwiegende Anzahl der Benutzergruppen Zugriff auf die Funktion Terminbuchung, die alle detaillierten Angaben zu sämtlichen jemals in der Abteilung behandelten Patienten anzeigt. Den Umfang dieser Berechtigungen zum jederzeitigen Direktzugriff auf die Daten aller in dieser Abteilung in der Vergangenheit behandelten Patienten sehe ich als zu weitgehend an. Während meiner Prüfung wurde mir bereits zugesagt, daß eine Eingrenzung der Berechtigungen vorgenommen und mir ein schriftlicher Vorschlag hierzu übersandt wird.

Da auch hinsichtlich der Speicherung von Patientendaten in RADOS keine Speicherungsfristen festgelegt werden, die Patientendaten vielmehr dauerhaft gespeichert werden sollen, habe ich auch zu diesem Punkt noch um schriftliche Stellungnahme gebeten.

Ferner müssen noch technische und organisatorische Datenschutzmaßnahmen ergriffen werden. Für die Anwendung RADOS ist insbesondere der Hersteller gefordert. Im Bereich der organisatorischen Maßnahmen muß das Klinikum aktiv werden. Es muß ein Datenschutzkonzept erstellt werden, in dem Schutzmaßnahmen festgelegt werden. Beim Einsatz von PC's (vgl. 9.2.4) gehört beispielsweise die Datenverschlüsselung als Stand der Technik zu den in Betracht kommenden Mechanismen. Als weiterer regelungsbedürftiger Punkt ist die Revision der Datenverarbeitung zu nennen. So muß bei RADOS im Rahmen einer Revision die korrekte Implementierung der „Tied-Terminals" kontrolliert werden, damit die Anwendung gesetzeskonform eingesetzt wird.

Unter RADOS werden Teile der Patientenakte elektronisch gespeichert. Solange ein Ausdruck der Daten in der normalen Patientenakte abgelegt wird, gibt es qualitativ keine Änderung zu den bisherigen Abläufen.

Die ausschließliche Speicherung der Patientendaten in RADOS wirft Fragen hinsichtlich der Fälschungssicherheit auf. In der Anwendung ist es nicht mehr möglich, archivierte Daten zu ändern. Personen, die Zugriff auf die Systemebene von MUMPS oder MS-DOS haben, also an RADOS vorbei auf Daten zugreifen, können aber archivierte Informationen durchaus ändern. Derartige Änderungen sind dann kaum nachweisbar.

Unter welchen Voraussetzungen elektronisch gespeicherte Informationen als echt anzusehen sind, muß noch allgemein festgelegt werden. Das Problem wird immer drängender, da rechtswirksame Informationen verstärkt elektronisch gespeichert werden, mit dem Ziel, auf Originaldokumente, auf Papier oder andere dokumentenechte Speichermedien zu verzichten.

9.3
Probleme mit der Entbindung von der ärztlichen Schweigepflicht

Daten, die der ärztlichen Schweigepflicht i.S.d. § 203 Strafgesetzbuch unterliegen, dürfen nur „befugt" an andere Personen oder Stellen weitergegeben werden. Eine Befugnis zur Offenbarung der Daten kann sich aus einer Rechtsvorschrift ergeben oder aus einer Einwilligung der Patienten. Die Einwilligung der Patienten ist nur dann rechtswirksam, wenn die Patienten vorher über die vorgesehene Verwendung ihrer Daten informiert wurden. Entsprechendes gilt auch für die in vielen Fällen gleichzeitig einzuholende Einwilligung in die Verarbeitung personenbezogener Daten i.S.d. Hessischen Datenschutzgesetzes (HDSG) (§ 7 Abs. 1 Nr. 2 HDSG). In der Praxis habe ich in diesem Jahr vielfach Probleme hinsichtlich der Verfahrensweise bei der Einholung der Einwilligung festgestellt.

1. Sind die Daten nicht hinreichend anonymisiert, ist eine Einwilligung der Patienten notwendig.

   Ärzte bzw. Kliniken gehen immer wieder fälschlich davon aus, daß umfangreiche Datenkataloge, die nicht den Namen und die vollständige Adresse der Patienten enthalten, als anonymisierte Daten einzustufen sind und ihre Übermittlung an Dritte daher ohne eine Entbindung von der ärztlichen Schweigepflicht durch die Patienten erfolgen darf.

   So wurde z.B. bei der Kerndokumentation zur Erfassung rheumakranker Menschen in der Modellregion Rhein-Main im Rahmen eines vom Bundesminister für Gesundheit geförderten Projekts zur besseren Versorgung chronisch Kranker ein standardisiertes Anschreiben an die Patienten verwendet, in dem den Patienten mitgeteilt wurde, daß nur anonymisierte Daten über sie weitergegeben werden. Tatsächlich war es jedoch so, daß im Rahmen des Projekts ein umfangreicher Datenkatalog an das Universitätsklinikum Frankfurt weitergegeben wurde, der neben detaillierten medizinischen Informationen auch soziale Angaben (Schulbildung, Berufsausbildung, berufliche Tätigkeit, Familienstand, Anzahl der im Haushalt lebenden Personen) und insbesondere auch Angaben zum Wohnort (Gemeinde mit Postleitzahl bzw. in Großstädten Stadtteil) enthielt. Zumindest bei Patienten aus kleineren Gemeinden war die Möglichkeit einer Identifizierung aufgrund der auf dem Fragebogen enthaltenen detaillierten Informationen nicht auszuschließen. Die Daten mußten daher als personenbezogen eingestuft werden. Erst im Universitätsklinikum Frankfurt wurde der Fragebogen vollständig anonymisiert und dann an das Deutsche Rheuma-Forschungszentrum weitergegeben. Aufgrund meiner Beratung wurde das Anschreiben an die Patienten entsprechend geändert.

2. Konkrete Information über Umfang und Zweck der vorgesehenen Verwendung der Daten ist notwendig.

   Ein Gesundheitsamt hatte ein Formular für eine Einverständniserklärung entworfen, in dem u.a. der folgende Text enthalten war:

   „Ebenso bin ich damit einverstanden, daß evtl. vorhandene hausinterne Befunde des Gesundheitsamtes in die Begutachtung einbezogen werden dürfen, und entbinde die Beteiligten insoweit von ihrer Schweigepflicht ...".

   Wenn man bedenkt, daß das Gesundheitsamt eine Vielzahl sehr unterschiedlicher Aufgaben wahrnimmt, in deren Rahmen ärztliche Daten über die Betroffenen dort gespeichert sein können (z.B. amtsärztliche Untersuchungen, Tuberkulosebekämpfung, Schwerbehindertenberatung, sozialpsychiatrische Beratung etc.), so muß die Einwilligungserklärung die betroffenen Patienten darüber aufklären, welche Informationen grundsätzlich in Betracht kommen, und ihnen damit auch ermöglichen, einzelne Informationen, z.B. diejenigen, die aufgrund einer freiwilligen sozialpsychiatrischen Beratung im Gesundheitsamt vorliegen, von einer Einbeziehung in das Gutachten auszuschließen. Mit dem Gesundheitsamt habe ich besprochen, daß der Formularentwurf überarbeitet wird.

   Ein Krankenhaus bat mich um Stellungnahme zu dem Entwurf einer Einwilligungserklärung, die jedem Patienten bei der Aufnahme ins Krankenhaus ausgehändigt werden sollte. Er enthielt den folgenden Text:

   „... Zur Weitergabe Ihrer persönlichen Daten an die Institute für Radiologie und Nuklearmedizin benötigen wir Ihre vorherige schriftliche Zustimmung. Aus betriebsorganisatorischen Gründen möchten wir Sie deshalb bitten, bereits zum Aufnahmezeitpunkt Ihre schriftliche Einwilligung durch Ankreuzen auf diesem Formular zu erteilen und zurückzureichen. Sollten Sie aber mit einer Weitergabe Ihrer persönlichen Daten ... nicht einverstanden sein, so entsteht Ihnen deshalb kein Nachteil ...".

In diesem Fall war der Zweck der vorgesehenen Datenweitergabe für die Patienten nicht verständlich. Insbesondere war nicht klar, ob denn alle Patienten in den genannten Instituten behandelt werden (was nicht der Fall ist). Aufgrund meiner Beratung wurde der Zweck der Datenweitergabe in dem Formular genauer erläutert.

3. Den Patienten müssen korrekte Informationen gegeben werden.

Selbstverständlich müssen die tatsächlichen und rechtlichen Informationen, die den Patienten gegeben werden, korrekt sein. Daß dies nicht immer der Fall ist, zeigte das Formular eines Krankenhauses für die Einwilligung in die Durchführung eines Aids-Tests. Auf diesem Formular, von dem ich durch eine Beschwerde Kenntnis erhielt, war der folgende Passus enthalten:

„... Eine namentliche Weitergabe des Testergebnisses an Personen oder Institutionen außerhalb ... der Kliniken erfolgt nicht, es sei denn auf Ihren ausdrücklichen Wunsch hin ...".

Meine Nachfragen ergaben, daß sich in dem Krankenhaus niemand Gedanken darüber gemacht hatte, wie denn diese Zusicherung rechtlich und tatsächlich realisiert werden kann. Das Ergebnis des Aids-Tests wird in die übliche Krankenakte aufgenommen – die Durchführung des Tests unterliegt ja auch der ärztlichen Dokumentationspflicht. Eine Übermittlung der Diagnose Aids an die Krankenkasse (§ 301 Sozialgesetzbuch V (SGB V)) und eine Einsichtnahme des Medizinischen Dienstes in die Krankenakte (§§ 275, 276 SGB V) sind im Einzelfall weder rechtlich noch praktisch ausgeschlossen. Ebensowenig ist ausgeschlossen, daß Informationen über das Vorliegen einer Aids-Infektion des Betroffenen an das Gesundheitsamt gelangen, z. B. wenn das Gesundheitsamt im Rahmen der Tuberkulosebekämpfung auf der Grundlage der Bestimmungen des Bundesseuchengesetzes den Krankenhausentlassungsbericht oder einen Arztbrief über diesen Patienten anfordert (§§ 31 Abs. 1, 32 Abs. 1, 10 Abs. 2 Bundesseuchengesetz). Aufgrund meiner Beratung wurden die den Patienten auf dem Formular gegebenen Informationen entsprechend abgeändert.

4. Datenanforderungen müssen konkret formuliert sein.

Werden bei Ärzten, Gesundheitsämtern, Kliniken etc. vorhandene ärztliche Unterlagen von anderen Stellen angefordert, so muß die anfordernde Stelle konkret darlegen, welche Unterlagen sie benötigt, und daß eine Entbindung von der ärztlichen Schweigepflicht durch die betroffenen Patienten in diesem Umfang und für diesen Zweck vorliegt. Leider wird dies in der Praxis nicht immer beachtet.

So forderte z. B. ein Gericht ärztliche Unterlagen bei einem Gesundheitsamt an mit einem allgemeinen Anschreiben, in dem der Arzt um Übersendung „der Akten des Klägers" gebeten und ihm zugleich mitgeteilt wurde, daß der Kläger „der Beiziehung seiner Akten zugestimmt hat". Einem solchen Anschreiben kann der Arzt keine Informationen darüber entnehmen, in welchem Umfang und zu welchem Zweck der Patient ihn von der ärztlichen Schweigepflicht entbunden hat und er daher zur Offenbarung ärztlicher Daten berechtigt ist. Der Arzt muß dies aber wissen, andernfalls er nicht verantwortlich entscheiden kann, welche Informationen er offenbart. Eine (teilweise) unbefugte Offenbarung ärztlicher Informationen kann strafrechtliche Konsequenzen für ihn haben.

Selbstverständlich kann eine andere Stelle auch keine ärztlichen Daten anfordern mit der allgemeinen Begründung „Amtshilfe". Leider kommt auch dies gelegentlich immer noch vor. Ist keine Rechtsgrundlage für eine Übermittlung ärztlicher Daten vorhanden, muß die anfordernde Stelle eine Einwilligung der Patienten einholen.

5. Die den Patienten erteilten Informationen sind verbindlich.

In diesem Jahr bin ich von mehreren Stellen um Stellungnahme gebeten worden zu der Frage, ob die onkologischen Schwerpunktkrankenhäuser einen Teil ihrer Patientendaten, die sie in ihren klinischen Krebsregistern gespeichert haben, an die Kassenärztliche Vereinigung Hessen weitergeben dürfen, damit die Patientendaten künftig dort gespeichert und ausgewertet werden können. Dies führte zu Diskussionen über die Frage, inwieweit die Informationen, die den Patienten mitgeteilt werden, bevor sie ihre Einwilligung in die Weitergabe ihrer Daten erteilen, verbindlich sind.

Die onkologischen Schwerpunktkrankenhäuser haben bisher nicht nur ihre eigenen Patientendaten, sondern zum Teil – im Rahmen sogenannter „kooperativer Nachsorge" – auch die Patientendaten niedergelassener Ärzte in ihrem klinischen Krebsregister gespeichert. In diesen Fällen hatten die Patienten keinen Behandlungsvertrag mit dem registerführenden Krankenhaus, sondern mit dem niedergelassenen Arzt. Speichernde Stelle i.S.d. § 23 Bundesdatenschutzgesetz war der niedergelassene Arzt, das registerführende Krankenhaus verarbeitete die Patientendaten in seinem Auftrag. Zwischen dem niedergelassenen Arzt und dem registerführenden Krankenhaus wurde in einem standardisierten Vertrag geregelt, welche Daten zu welchem Zweck im Register verarbeitet werden. Der niedergelassene Arzt holte die Einwilligung der Patienten in die Weitergabe ihrer Daten an das jeweilige registerführende Krankenhaus ein. Der mit meiner Beratung von der Kassenärztlichen Vereinigung Hessen entworfene standardisierte Text der Einwilligungserklärung enthielt Informationen für die Patienten darüber, an welche registerführende Klinik ihre Daten weitergegeben werden und in welchem Umfang und zu welchem Zweck (vgl. 17. Tätigkeitsbericht, Ziff. 5.3.; 18. Tätigkeitsbericht, Ziff. 8.3.; 19. Tätigkeitsbericht, Ziff. 5.1.).

Ich habe die Auffassung vertreten, daß eine Verlagerung des Datenbestandes von dem registerführenden Krankenhaus zur Kassenärztlichen Vereinigung Hessen ohne Einschaltung der Patienten nicht zulässig ist. Die Patienten

treffen ihre Entscheidung, ob sie ihre Einwilligung in die Offenbarung ihrer Daten gegenüber einer anderen Stelle (hier: dem jeweiligen onkologischen Schwerpunktkrankenhaus) geben wollen, aufgrund der ihnen gegebenen Informationen und des Vertrauens, das sie der konkret genannten datenverarbeitenden Stelle entgegenbringen. Daher halte ich es nicht für zulässig, daß aufgrund einer solchen Einwilligungserklärung die Patientendaten zu einem späteren Zeitpunkt bei einer anderen, in der Einwilligungserklärung nicht genannten datenverarbeitenden Stelle ohne erneute Einschaltung der betroffenen Patienten gespeichert werden. Im konkreten Fall hat mir die Kassenärztliche Vereinigung Hessen inzwischen mitgeteilt, daß sie meinen Rechtsstandpunkt teilt und bei einer (teilweisen) Verlagerung der Register die Patientenrechte gewährleistet werden.

9.4
„Rechtfertigender Notstand"
Rechtsgrundlage für die Weitergabe von Sozialdaten?

Ich wurde um Stellungnahme zu folgendem Fall gebeten:

Der Versicherungsnehmer einer Krankenkasse hatte mit einem Mitarbeiter Auseinandersetzungen über den Umfang der Kassenleistungen. Der Streit ging so weit, daß der Versicherungsnehmer drohte, er werde sich das Leben nehmen und den Mitarbeiter sowie weitere Personen mit in den Tod nehmen. Der betroffene Mitarbeiter war aufgrund der konkreten Umstände der Auffassung, daß diese Drohung ernst zu nehmen war, und wandte sich an eine Polizeibehörde, die dann prüfte, ob und ggf. welche polizeilichen Schutzmaßnahmen zu treffen waren. Auf diese Weise erhielt die Polizeibehörde Kenntnis der bei der Krankenkasse vorhandenen Sozialdaten i.S.d. § 35 Abs. 1 Sozialgesetzbuch I (SGB I) über den Versicherten.

Die Krankenkasse führte als Rechtsgrundlage für die Weitergabe der Sozialdaten des Versicherten an die Polizeibehörde den in § 34 Strafgesetzbuch (StGB) geregelten Rechtfertigungsgrund „Rechtfertigender Notstand" an. Nach dieser Vorschrift handelt derjenige nicht rechtswidrig, der in einer gegenwärtigen, nicht anders abwendbaren Gefahr für Leben oder Leib oder ein anderes Rechtsgut eine Tat begeht, um die Gefahr von sich oder einem anderen abzuwenden, wenn bei Abwägung der widerstreitenden Interessen, namentlich der betroffenen Rechtsgüter und des Grades der ihnen drohenden Gefahren, das geschützte Interesse das beeinträchtigte wesentlich überwiegt.

Sicherlich war es verständlich, daß der betroffene Mitarbeiter der Krankenkasse sich und die weiteren Personen schützen wollte. Dennoch kann die von der Krankenkasse genannte Rechtsgrundlage aus datenschutzrechtlicher Sicht nicht akzeptiert werden. Dies würde eine grundsätzliche und weitreichende Relativierung des gesetzlich geregelten Sozialdatenschutzes bedeuten.

In § 35 Abs. 1 SGB I wurde eine besondere Regelung über die Geheimhaltung der Sozialdaten getroffen, im SGB X eine abschließende Aufzählung der Gründe für eine Offenbarung von Sozialdaten festgelegt. Hintergrund dieser Spezialregelung ist, daß die Bürger im Zusammenhang mit Sozialleistungen den Behörden in besonders weitem Umfang persönliche Informationen offenlegen müssen und der Gesetzgeber daher einen möglichst weitgehenden und klar geregelten Schutz der Sozialdaten für unumgänglich hielt (BTDrucks. 7/868, S. 45).

Für die Übermittlung von Sozialdaten gelten die §§ 67 ff. SGB X. Eine Offenbarung der personenbezogenen Daten ist nur zulässig, soweit der Betroffene im Einzelfall eingewilligt hat oder eine gesetzliche Offenbarungsbefugnis nach den §§ 68 – 77 SGB X vorliegt (§ 67 SGB X). Ob § 34 StGB grundsätzlich auf staatliches Handeln anwendbar ist und als Rechtsgrundlage für grundrechtseinschränkende hoheitliche Maßnahmen angesehen werden kann, ist sehr umstritten. Vieles spricht dafür, es allein als Aufgabe des Gesetzgebers anzusehen, die Handlungsmöglichkeiten der öffentlichen Stellen zu regeln, und es nicht den öffentlichen Stellen zu überlassen, sich Handlungsspielräume in eigener Verantwortung zu gestalten, da sonst das Recht des Staates, in Grundrechte einzugreifen, in unüberschaubarer und kaum kontrollierbarer Weise ausgedehnt würde. Ganz überwiegend besteht die Rechtsauffassung, daß in den Fällen, in denen ein bestimmter Interessenkonflikt durch öffentlich-rechtliche Sondervorschriften konkret und abschließend geregelt ist, ein Rückgriff auf § 34 StGB als Rechtsgrundlage für staatliches Handeln versperrt ist.

Eine solche Situation liegt hier vor. Es steht außer Zweifel, daß der Gesetzgeber mit der Konkretisierung der Offenbarungsbefugnisse der Sozialleistungsträger im zweiten Kapitel des SGB X eine abschließende Regelung schaffen wollte. Unter dem Gesichtspunkt des rechtfertigenden Notstandes i.S.d. § 34 StGB kann daher allenfalls der einzelne Mitarbeiter von strafrechtlichen Sanktionen wegen der Weitergabe geschützter Sozialdaten freigestellt, nicht aber der Leistungsträger zu einer Weitergabe sensibler personenbezogener Informationen an Dritte ermächtigt werden, zu der er weder nach den §§ 68 bis 77 SGB X noch aufgrund der Einwilligung des Betroffenen berechtigt ist.

Im konkreten Fall habe ich das Vorliegen der Voraussetzungen des § 71 Abs. 1 Nr. 1 SGB X bejaht, demzufolge eine Offenbarung personenbezogener Sozialdaten zulässig ist, soweit sie erforderlich ist für die Erfüllung der gesetzlichen Mitteilungspflicht zur Abwendung geplanter Straftaten nach § 138 StGB. Nach dem mir mitgeteilten Sachverhalt konnte der Mitarbeiter der Krankenkasse davon ausgehen, daß konkrete Anhaltspunkte für eine geplante Tat i.S.d. § 138 StGB vorlagen. Die Regelung des § 71 Abs. 1 Nr. 1 SGB X zielt darauf ab, eine Offenbarung von Sozialdaten zuzulassen zum Schutz der in den § 138 StGB genannten Rechtsgüter. Die Information der Polizeibehörde über den Sachverhalt ermöglichte es der Polizeibehörde, darüber zu entscheiden, ob und ggf. welche Maßnahmen zur Gefahrenabwehr getroffen werden mußten.

9.5
„Liste der fragwürdigen Patienten" im Krankenhaus

Wie wird aus einem zehn Monate alten Säugling ein fragwürdiger Patient? Die Frage läßt sich anhand einer Liste, erstellt aus der automatisierten Datei der Patientenaufnahme eines Krankenhauses, das ich geprüft habe, beantworten:

Das Kind wurde 1992 in den Kliniken geboren. Da kein Kostenträger für die Übernahme der Entbindungs- bzw. Pflegekosten zuständig war, die Eltern die Kosten ebenfalls nicht bezahlten, wurde aus dem Säugling bereits im Alter von nur wenigen Monaten ein fragwürdiger Patient. In der Liste und damit auch in der automatisierten Datei der Patientenaufnahme wurde er mit seinem Namen, Vornamen, Geburtsdatum und dem Kommentar „Pflegekosten offen" gespeichert.

Aber auch andere in den Kliniken behandelte Patienten fanden sich in der Liste wieder. Die Kommentare zu weiteren Patienten lauteten: „Ausweis noch hier"; „Eigenanteil noch offen"; „Kostenträger falsch angegeben"; „Telefonrechnung offen"; „Strafanzeige gestellt"; „Keine Zusage vom Sozialamt".

Die im August 1993 erstellte Liste umfaßte insgesamt 61 Datensätze und – die doppelt eingegebenen Datensätze abgerechnet – immerhin noch 55 namentlich aufgeführte Patienten, die vom Krankenhaus als fragwürdig eingestuft wurden. Die in der Patientenaufnahme des Krankenhauses erfaßten und automatisiert gespeicherten Daten betrafen nur die im Krankenhaus selbst behandelten Patienten. Eine Übermittlung der Daten an Dritte außerhalb der Klinik war nicht vorgesehen. Von der Klinik konnte nicht dargelegt werden, welcher Zweck mit der Datenverarbeitung verfolgt wird. Selbst die Mitarbeiter, die die Daten in die Datei eingegeben hatten, wußten z. B. nicht, wie sie weiter zu verfahren hatten, wenn einer der „fragwürdigen Patienten" erneut im Krankenhaus aufgenommen wurde. Auch die Rechnungsstelle der Klinik, die den Einzug von Forderungen bei Patienten überwacht, konnte nicht erklären, welche Konsequenzen die Neuaufnahme eines „fragwürdigen Patienten" hat. Für die Führung der Datei gab es in der Klinik keine Dienstanweisung, in der beispielsweise die Fristen für die Sperrung und Löschung der gespeicherten Daten festgelegt waren. Es war daher nur folgerichtig, daß die Mitarbeiter der Klinik die Frage, ob der Datensatz eines Patienten, dessen Pflegekosten nachträglich bezahlt wurden, im System gelöscht wird, verneint haben.

Nach §§ 12 Hessisches Krankenhausgesetz, 11 Hessisches Datenschutzgesetz dürfen personenbezogene Daten nur verarbeitet werden, soweit sie für die Aufgabenerfüllung des Krankenhauses und für den jeweils damit verbundenen Zweck erforderlich sind. Da der Zweck der automatisiert geführten „Liste der fragwürdigen Patienten" nicht ersichtlich war, habe ich gegenüber dem Krankenhaus die Auffassung vertreten, daß die weitere Speicherung der Daten nicht zulässig ist.

Der Datenschutzbeauftragte des Krankenhauses hat mir inzwischen mitgeteilt, daß die Liste gelöscht wurde.

9.6
Datenerhebung des Ordnungsamts Wiesbaden im Rahmen des Heilpraktikergesetzes

Wer die Heilkunde ausüben will, ohne als Arzt bestallt zu sein, bedarf dazu der Erlaubnis (§ 1 Abs. 1 Heilpraktikergesetz (HeilprG)).

Probleme, die Erlaubnis zu erhalten, schilderte mir ein Antragsteller in einer Eingabe. Zu den mir von dem Eingeber vorgelegten Unterlagen gehört auch ein Schreiben des Ordnungsamtes Wiesbaden, in dem das Ordnungsamt dem Antragsteller darlegt, aus welchen Gründen beabsichtigt sei, den Zulassungsantrag abzulehnen. Als Begründung für die beabsichtigte Ablehnung ist in dem Schreiben des Ordnungsamtes u. a. folgendes zu lesen:

„Die Erlaubnis zur Ausübung der Heilkunde wird auf Antrag erteilt. Über den Antrag entscheidet nach § 1 Abs. 1 HeilprG i.V.m. § 3 Abs. 1 der 1. Durchführungsverordnung Heilpraktikergesetz (DVO-HPG) vom 18. Februar 1939 (RGBl. I S. 259) die Untere Verwaltungsbehörde im Benehmen mit dem Gesundheitsamt unter Berücksichtigung der Versagungsgründe nach § 2.1 DVO-HPG.

Nach § 2 Abs. 1f und g der 1. DVO-HPG wird die Erlaubnis nicht erteilt, wenn sich aus Tatsachen ergibt, daß dem Antragsteller die sittliche Zuverlässigkeit fehlt, insbesondere, wenn schwere strafrechtliche oder sittliche Verfehlungen vorliegen, sowie aufgrund eines körperlichen Leidens oder wegen Schwäche seiner geistigen oder körperlichen Kräfte oder wegen einer Sucht die für die Berufsausbildung erforderliche Eignung fehlt.

Aufgrund Ihrer Vorstrafe bestehen seitens des Amtsarztes an Ihrer persönlichen und geistigen Zuverlässigkeit erhebliche Zweifel. Gemäß den Richtlinien zur Durchführung des Heilpraktikergesetzes des Hessischen Sozialministers vom 19. Januar 1978 (StAnz. S. 815) ist zu prüfen, ob ein Bewerber vorbestraft ist und ob die der Verurteilung zugrunde liegenden Sachverhalte zu negativen Rückschlüssen auf persönliche Zuverlässigkeit und Eignung eines Bewerbers zwingen.

Der hier vorliegende Sachverhalt der rechtskräftigen Verurteilung läßt zweifelsohne negative Rückschlüsse auf die persönliche und damit auch sittliche Zuverlässigkeit zu."

Die Begründung für die beabsichtigte Ablehnung enthält allerdings einen gravierenden Fehler. Der Antragsteller ist nicht vorbestraft. Dies hatte er gegenüber dem Ordnungsamt durch Vorlage eines Führungszeugnisses aus dem Bundeszentralregister dokumentiert. Auch wurde der Antragsteller vom Gesundheitsamt auf seine gesundheitliche Eignung untersucht und zur berufsmäßigen Ausübung der Heilkunde ohne Bestallung für geeignet befunden.

Wie konnte es aber dazu kommen, daß der Antragsteller dennoch nicht zum Beruf des Heilpraktikers zugelassen werden sollte? Diese Frage hat mir das Ordnungsamt folgendermaßen beantwortet:

„Da, wie im Falle des Antragstellers, das vorgelegte Führungszeugnis keine Eintragungen ausgewiesen hat und eingestellte Verfahren nicht eingetragen werden, sind wir auf die Erkenntnisse der Polizei angewiesen.

Da in Führungszeugnissen nur abgeschlossene Verfahren (Verurteilungen) eingetragen werden, ist es erforderlich, bei der Polizeibehörde nachzufragen, ob dort Erkenntnisse über schwebende Verfahren vorliegen.

Die Polizei teilt dort vorliegende Erkenntnisse in Form von Aktenzeichen der anfragenden Behörde mit.

Aufgabe der zuständigen Verwaltungsbehörde ist es dann, bei der zuständigen Staatsanwaltschaft um Akteneinsicht nachzusuchen. Werden danach Erkenntnisse gewonnen, die in bezug auf die Ausübung der Heilkunde ohne Bestallung (Heilpraktiker) relevant werden, müssen diese natürlich in die Entscheidung der Verwaltungsbehörden einfließen.

... Auf die polizeiliche Überprüfung wird der Bewerber nicht hingewiesen."

Im vorliegenden Fall lag der Polizei ein Hinweis auf ein Ermittlungsverfahren bei der Staatsanwaltschaft vor. Das Ordnungsamt forderte bei der Staatsanwaltschaft die Strafakte an und übermittelte die daraus gewonnenen Erkenntnisse dem Gesundheitsamt. Daraufhin wurde der Antragsteller ein zweites Mal amtsärztlich untersucht. Das Gesundheitsamt hielt außerdem eine fachpsychiatrische Zusatzbegutachtung für erforderlich.

In der von mir erbetenen Stellungnahme führt das Gesundheitsamt aus, daß die „Vorstrafe" bei der Beurteilung der Eignung des Antragstellers nicht im Vordergrund gestanden habe. Vielmehr lasse es die nun aufgedeckte Persönlichkeitsstruktur des Antragstellers nicht zu, ihn für den verantwortungsvollen Beruf des Heilpraktikers als geeignet anzusehen.

Das Gesundheitsamt hat also zunächst eine positive und danach eine negative Stellungnahme abgegeben. Die vom Gesundheitsamt behauptete „Vorstrafe" konnte in der Tat nicht im Vordergrund der Entscheidungsfindung stehen, weil der Antragsteller eben nicht vorbestraft ist. Zwar hatte die Staatsanwaltschaft gegen den Antragsteller wegen des Verdachts des Verstoßes gegen das Betäubungsmittelgesetz ermittelt. Das Verfahren wurde jedoch nach Erfüllung einer Auflage vom Gericht im Jahre 1986 eingestellt.

Unter datenschutzrechtlichen Gesichtspunkten war das Ordnungsamt gemäß § 12 Abs. 2 Ziff. 2 und 3 des Hessischen Datenschutzgesetzes befugt, bei Polizei und Staatsanwaltschaft die erforderlichen Daten für die Entscheidung über den gestellten Antrag zu erheben. Vor der Datenerhebung, d.h. bereits bei Stellung des Antrages, war das Ordnungsamt aber auch verpflichtet, den Antragsteller darauf hinzuweisen, bei welchen öffentlichen Stellen Daten erhoben werden. Diese Information stellt Transparenz für die Betroffenen her und ermöglicht es dem Antragsteller, seinen Antrag ggf. noch vor der Datenerhebung zurückzuziehen.

Auf meine Anregung hin hat das Ordnungsamt Wiesbaden in das Merkblatt über die vom Antragsteller beizubringenden Nachweise einen entsprechenden Hinweis aufgenommen.

Diese Regelung kann jedoch nur für eine Übergangszeit gelten. Weder das Heilpraktikergesetz vom 17. Februar 1939 noch die Durchführungsverordnung vom 18. Februar 1939 regeln bisher die Datenerhebung. Eine dahingehende Änderung des Gesetzes ist längst überfällig. Solange jedoch noch keine gesetzliche Regelung besteht und es für erforderlich gehalten wird, Informationen über eingestellte oder laufende Strafverfahren einzuholen, muß die Verfahrensweise in den Richtlinien zur Durchführung des Heilpraktikergesetzes präzise festgelegt sein.

Ich habe daher das zuständige Hessische Ministerium für Jugend, Familie und Gesundheit informiert und um Stellungnahme gebeten.

9.7
Aufgaben des Medizinischen Dienstes der gesetzlichen Krankenversicherung bei der Durchführung von „ambulanter Psychotherapie" im Erstattungsverfahren

9.7.1
Rechtliche Einordnung des Erstattungsverfahrens

Nach § 15 Abs. 1 Satz 1 Sozialgesetzbuch V (SGB V) wird ärztliche Behandlung, zu der auch die psychotherapeutische Behandlung gehört, von Ärzten erbracht. Zur Durchführung einer Psychotherapie sind aber nur Ärzte berechtigt, die eine abgeschlossene Weiterbildung mit dem Erwerb der Zusatzbezeichnung „Psychotherapie" und „Psychoanalyse"

nachweisen können. Nach § 15 Abs. 1 Satz 2 SGB V dürfen psychotherapeutische Hilfeleistungen auch von anderen Personen erbracht werden, wenn sie vom Arzt angeordnet und von ihm verantwortet werden. In diesem Fall erfolgt die Hinzuziehung von Diplom-Psychologen oder Kinder- und Jugendlichen-Psychotherapeuten im Delegationsverfahren. Sinn dieser Regelung ist es, die ambulante psychotherapeutische Versorgung der Bevölkerung sicherzustellen. Weil diese durch die Ärzte und Vertragsbehandler allein aber nicht gewährleistet ist, wird zur Verbesserung der Versorgungssituation auf der Grundlage des § 13 Abs. 3 SGB V die Durchführung ambulanter Psychotherapien durch Nicht-Vertragstherapeuten im (Kosten-) Erstattungsverfahren von den Krankenkassen anerkannt. Zu den Besonderheiten des Erstattungsverfahrens gehört, daß zwischen dem behandelnden Therapeuten und der gesetzlichen Krankenkasse kein Vertragsverhältnis besteht.

9.7.2
Gesundheitliche Versorgung und Qualitätssicherung

Der Medizinische Dienst der Krankenversicherung in Hessen (MDK) ist eine Körperschaft des öffentlichen Rechts. Aufgaben und Organisation des MDK sind im Neunten Kapitel des SGB V festgelegt. Zu den Aufgaben des MDK gehört es, im Auftrag einer gesetzlichen Krankenkasse die Qualifikation von Behandlern, welche die psychotherapeutische Versorgung im Erstattungsverfahren durchführen, zu überprüfen. Um diese Aufgabe erfüllen zu können, ist die Erhebung personenbezogener Daten von Behandlern erforderlich. Bis Ende 1992 wurden die jeweiligen Behandler vom MDK direkt aufgefordert, Qualifikationsnachweise vorzulegen. Da es jedoch Aufgabe der gesetzlichen Krankenkassen ist, im Einzelfall den MDK einzuschalten, fordert der MDK selbst seit Anfang 1993 keine Unterlagen mehr bei den Behandlern an.

9.7.3
Qualifikationsanforderungen an Psychotherapeuten im Erstattungsverfahren

Weder die Ausbildung noch die Zulassung zum Beruf der Psychotherapeuten wurden bisher gesetzlich geregelt. Die Bundesregierung hat dem Deutschen Bundestag am 13. Oktober 1993 den „Entwurf eines Gesetzes über die Berufe des Psychologischen Psychotherapeuten und des Kinder- und Jugendlichen-Psychotherapeuten und zur Änderung des Fünften Buches Sozialgesetzbuch" zur Beschlußfassung vorgelegt (Drucks. 12/5890). Bis zum Inkrafttreten des Gesetzes müssen Psychotherapeuten, die keine Ärzte sind und im Delegationsverfahren nach § 15 SGB V tätig werden, die Qualifikationsanforderungen der Psychotherapie-Richtlinien des Bundesausschusses der Ärzte und Krankenkassen i.d.F. vom 3. Juli 1987 (Beilage zum BAnz. Nr. 156), zuletzt geändert am 9. April 1991 (BArbBl. 6 S. 86), erfüllen. Die Hauptverwaltung des MDK in Oberursel hat am 5. Januar 1993 auf der Grundlage der Psychotherapie-Richtlinien einen „Kriterienkatalog für die Begutachtung ambulanter Psychotherapie im Erstattungsverfahren" erstellt und diesen an die gesetzlichen Krankenkassen verschickt. Nach diesem Kriterienkatalog sind folgende Anforderungen an die Qualifikation der psychologischen Psychotherapeuten zu stellen:

a) Diplom-Zeugnis.

b) 3-jährige klinische Tätigkeit.

c) a) und b) können durch den vom Berufsverband Deutscher Psychologen vergebenen Titel eines „Klinischen Psychologen (BDP)" abgedeckt werden.

d) Es ist ein Zertifikat mit dem Abschluß der Fortbildung in einer der drei genannten Psychotherapie-Richtungen vorzulegen.

e) Es wird empfohlen, daß die psychologischen Psychotherapeuten in Fotokopie ihre Zulassung als Heilpraktiker im Bereich Psychotherapie beifügen.

f) Hinsichtlich der Ausbildungskandidaten gilt die Regelung, daß diese nur dann in Einzelfällen akzeptiert werden, wenn sie mindestens die Hälfte ihrer Ausbildung durchschritten haben und eine Bescheinigung vorlegen, daß die fallbezogene Supervision jeder vierten Behandlungsstunde bei der jeweiligen Behandlung gewährleistet ist. Die Supervisionsbescheinigung kann nur von einem für die Therapierichtung qualifizierten und zugelassenen Supervisor erteilt werden.

Bei den zu d) genannten drei Psychotherapie-Richtungen handelt es sich um die Psychoanalyse, die tiefenpsychologisch fundierte Psychotherapie sowie die Verhaltenstherapie. Die Krankenkassen verlangen von den Behandlern im Erstattungsverfahren die gleichen Qualifikationen, wie sie die Behandler im Delegationsverfahren nachweisen müssen.

9.7.4
Transparenz der Datenverarbeitung

Unter datenschutzrechtlichen Gesichtspunkten ist es nicht zu beanstanden, daß die Qualifikationen von Behandlern durch den MDK im Auftrag der Krankenkassen überprüft werden, da dies zur Aufgabenerfüllung der Krankenkassen erforderlich ist. Durch die Eingabe einer Therapeutin (Behandlerin) wurde ich allerdings darauf aufmerksam gemacht, daß ihr weder die Krankenkassen noch der MDK das Verfahren der Datenerhebung sowie der weiteren Datenverwendung plausibel erläutern konnten. Die Behandlerin hat mir ein an sie gerichtetes Schreiben der Krankenkasse übersandt, in dem die Krankenkasse der Behandlerin mitteilt, daß sie sich, bedingt durch den nicht vorhandenen Vertragsstatus mit den gesetzlichen Krankenkassen, nicht in der Lage sieht, eine rechtliche Basis zu der Behandlerin

herzustellen bzw. die aufgeworfenen Fragen ihr gegenüber zu beantworten. Die Behandlerin wollte insbesondere von der Krankenkasse wissen, nach welcher Rechtsgrundlage ihre Daten von der Krankenkasse erhoben und in welcher Form die Daten beim MDK weiterverarbeitet werden. Dem vorausgegangenen war die telefonische Anforderung zur Vorlage von Unterlagen bei der Behandlerin.

Die Behandlerin ist rechtlich nicht verpflichtet, der Krankenkasse bzw. dem MDK Qualifikationsunterlagen vorzulegen. Dies hätte der Behandlerin auch klar mitgeteilt werden müssen.

Die Krankenkasse ist jedoch gegenüber einem Antragsteller im Erstattungsverfahren nur dann leistungspflichtig, wenn die Qualifikation eines Behandlers im Erstattungsverfahren der Qualifikation der Diplom-Psychologen oder Kinder- und Jugendlichen-Psychotherapeuten im Delegationsverfahren entspricht und nachgewiesen wird. Wenn also ein Behandler im Erstattungsverfahren die Behandlung übernehmen und der Versicherte die Behandlungskosten von seiner Krankenkasse erstattet haben will, so muß der Behandler den Nachweis seiner Qualifikation erbringen. Ist ein Behandler nicht bereit, die erforderlichen Unterlagen vorzulegen, oder ist er hierzu nicht in der Lage, weil er eine erforderliche Qualifikation nicht besitzt, lehnt die Krankenkasse die Kostenübernahme der Behandlung ab und verweist den Patienten an einen Vertragstherapeuten mit freien Therapieplätzen.

Da die Qualifikation der Behandler vom MDK im Auftrag der gesetzlichen Krankenkassen geprüft wird, ist die Kenntnis des Inhalts der Qualifikationsunterlagen durch die Krankenkasse nicht erforderlich. Es besteht also für die Behandler grundsätzlich die Möglichkeit, ihre Unterlagen im verschlossenen Umschlag der Krankenkasse zur Weiterleitung an den MDK zu übersenden. Der MDK prüft die eingereichten Unterlagen und teilt das Ergebnis der Prüfung der Krankenkasse mit, die danach ihre Kostenentscheidung trifft. Für die Mitteilung an die Krankenkasse benutzt der MDK einen Vordruck. Wird ein Antrag vom MDK nicht befürwortet, ist als Begründung hierfür vorgesehen: „Die beantragte therapeutische Methode entspricht nicht den Psychotherapie-Richtlinien" und „Die Qualifikation des/der Behandlers/in entspricht nicht den Psychotherapie-Richtlinien". In diesen Verfahren ist die Unterrichtung der Behandler nicht vorgesehen.

Es ist auch bisher für die Behandler im Erstattungsverfahren nicht transparent, in welcher Form ihre Daten bzw. Unterlagen vom MDK verarbeitet werden.

Ich habe im September 1993 mit Vertretern der Hauptverwaltung des MDK zur Durchführung der Qualifikationsprüfungen und der Notwendigkeit, alle Behandler umfassend über die Datenverarbeitung zu informieren, ein Gespräch geführt. Ergebnis des Gesprächs war, daß im Rahmen einer Überarbeitung des Kriterienkatalogs zum Begutachtungsverfahren die Behandler in geeigneter Form über die Verwendung ihrer Daten informiert werden. Die Unterlagen hierfür, so die Auskunft des MDK, werden spätestens Anfang 1994 fertiggestellt sein und mir dann zur Abstimmung vorliegen.

9.8
Aufnahmeformulare der Krankenhäuser

Die Datenerhebung bei der Patientenaufnahme in Krankenhäusern habe ich schon mehrfach kritisiert (vgl. 20. Tätigkeitsbericht, Ziff. 9.2 und 21. Tätigkeitsbericht, Ziff. 18.5).

Obwohl inzwischen bereits vier Jahre seit Inkrafttreten des Hessischen Krankenhausgesetzes am 1. Januar 1990 vergangen sind, gibt es immer noch Kliniken, die Daten in unzulässigem Umfang erheben und die Patienten nicht oder nicht ausreichend über die Verarbeitung und die Verwendungszwecke der erhobenen Daten informieren. Ich habe zudem festgestellt, daß verschiedene Kliniken ihrer gesetzlichen Verpflichtung gemäß § 18 Abs. 2 Hessisches Datenschutzgesetz (HDSG), die Patienten schriftlich zu benachrichtigen, wenn ihre personenbezogenen Daten in einer automatisierten Datei gespeichert werden, immer noch nicht nachgekommen sind. Konkrete Gründe für die mangelnde Umsetzung der rechtlichen Vorgaben konnte mir keine der Kliniken, die ich um Stellungnahme gebeten habe, nennen.

Nicht ganz einfach war der Schriftwechsel mit dem Stadtkrankenhaus Rüsselsheim. Die von mir bei der Klinik angeforderten Aufnahmeanträge sind am 11. Mai 1993 in meiner Dienststelle eingegangen. In dem Begleitschreiben der Klinik war angegeben: „Sollten wir bis zum 25. Mai 1993 von Ihnen nichts hören, gehen wir davon aus, daß obiger Antrag den Bestimmungen entspricht und wir ihn dann in Druck geben können." Es mußten also rund 3 1/2 Jahre für ein Tätigwerden des Krankenhauses vergehen, um mir eine Frist von 14 Tagen zu setzen. Leider war es nicht so, daß die Aufnahmeanträge den datenschutzrechtlichen Bestimmungen entsprachen. So beabsichtigte die Klinik z. B., die Personalausweisnummer aller aufzunehmenden Patienten zu erheben. Die Notwendigkeit dieser Datenerhebung wurde damit begründet, daß die Personalausweisnummer aus Gründen der Beweispflicht registriert werde, damit bei Einsprüchen der Patienten, Kostenträger bzw. Rechtsanwälte dokumentiert werden könne, daß ein Patient in der Klinik behandelt worden sei.

Die routinemäßige Erhebung der Personalausweisnummer bei der Aufnahme des Patienten ist für die Durchführung der Behandlung nicht erforderlich und somit unzulässig. Inzwischen hat das Stadtkrankenhaus Rüsselsheim auf die Erhebung dieses Datums verzichtet und den Aufnahmeantrag (auch in anderen Punkten) den datenschutzrechtlichen Erfordernissen angepaßt.

Eine abschließende Prüfung der Aufnahmeunterlagen des Kreiskrankenhauses Heppenheim und des Kreiskrankenhauses in Bad Homburg war mir noch nicht möglich, da beide Kliniken meiner Bitte um Übersendung der Unterlagen bisher nicht nachgekommen sind. Meine Anfrage an das Kreiskrankenhaus Heppenheim datiert vom 30. September 1992, die an das Kreiskrankenhaus Bad Homburg vom 8. März 1993. (Zu den Aufnahmeformularen des Universitätsklinikums Frankfurt, vgl. Ziff. 9.2.)

Nachfolgend abgedruckt (siehe Anlage) sind der Aufnahmebeleg (Vorder- und Rückseite) der Orthopädischen Klinik Kassel sowie die Benachrichtigung nach § 18 Abs. 2 HDSG des Zentrums für Rheumatologie in Schlangenbad. Beide Beispiele sind geeignet, aufzuzeigen, wie die gesetzlichen Anforderungen vernünftig umzusetzen sind.

10. Personalwesen

10.1
Neuregelungen des Personalaktenrechts

10.1.1
Neuordnung des Hessischen Beamtengesetzes

Schon wiederholt habe ich über die Novellierung des Beamtenrechtsrahmengesetzes berichtet, mit der gesetzliche Regelungen zum Umgang mit Personalakten als bereichsspezifische Rechtsgrundlagen geschaffen wurden (vgl. etwa 21. Tätigkeitsbericht, Ziff. 18.4).

Ende 1993 ist auch die notwendige Anpassung des Hessischen Beamtengesetzes (HBG) erfolgt. Dabei hat sich der Landesgesetzgeber entschieden, im wesentlichen die Regelungen des Beamtenrechtsrahmengesetzes zu übernehmen. Diese gelten unmittelbar jedoch nur für Beamte. Von der Möglichkeit, diese Regelungen auch für Angestellte und Arbeiter für anwendbar zu erklären, wurde ausdrücklich kein Gebrauch gemacht. Allerdings bedeutet dies nicht, daß für diesen Personenkreis ein wesentlich anderer oder schlechterer Schutz der Personaldaten bestünde. § 34 Abs. 1 Hessisches Datenschutzgesetz (HDSG) gilt weiterhin für alle Angaben, die nicht Personalaktendaten im Sinne des § 107 HBG sind, und für die Daten der Arbeiter und Angestellten. Danach ist eine Verarbeitung von Personaldaten für den Arbeitgeber möglich, soweit dies zur Eingehung, Durchführung, Beendigung oder Abwicklung des Dienst- oder Arbeitsverhältnisses oder zur Durchführung innerdienstlicher organisatorischer, sozialer und personeller Maßnahmen erforderlich ist. Diese Anforderungen entsprechen denen des § 107 HBG an die Zulässigkeit der Verwendung von Personalaktendaten. Bei der Beurteilung, ob eine bestimmte Verwendung erforderlich ist, kann daher als Maßstab das Hessische Beamtengesetz herangezogen werden, da in aller Regel kein sachlicher Grund vorhanden ist, Arbeiter und Angestellte anders zu behandeln als Beamte.

In einem Punkt unterscheiden sich nach dem Wortlaut die Regelungen des HDSG und des HBG, nämlich bei der Verarbeitung von Gesundheitsdaten. § 34 Abs. 6 HDSG verbietet die automatisierte Verarbeitung von medizinischen und psychologischen Befunden, § 107g Abs. 3 HBG läßt sie hingegen zu, soweit sie die Eignung betreffen und ihre Verarbeitung oder Nutzung dem Schutz des Beamten dient. In der Sache wird jedoch auch dies nicht zu unterschiedlichen Ergebnissen führen. Der von § 34 Abs. 6 HDSG angestrebte Zweck, vor allem einen Kontextverlust der Daten durch spätere, andere Verwendungen zu verhindern und die besondere Sensibilität medizinischer Angaben zu berücksichtigen, ist auch im Rahmen des Hessischen Beamtengesetzes gewährleistet. Andererseits ist damit klargestellt, daß z. B. eine Automatisierung der Beihilfeberechnung möglich ist. Das besondere Gefährdungspotential besteht hier nicht in diesem Umfang, da eine solche automatisierte Verwendung der medizinischen Daten nach den Vorgaben des § 107a HBG getrennt von der sonstigen Personalverwaltung erfolgen muß.

10.1.2
Auswirkungen der Neuregelungen auf die Praxis der Personalverwaltung

Die Mehrzahl der Neuregelungen stellt an die Personalverwaltungen keine neuen Anforderungen, sondern enthält eine Klarstellung der bestehenden Rechtslage, geprägt durch die Rechtsprechung zum Begriff der Personalakte sowie die Regelungen des § 34 HDSG. Allerdings sollte dies Anlaß sein, die tägliche Praxis des Umgangs mit Personalangelegenheiten zu überdenken. Ich habe den Eindruck, daß häufig die Organisation der Verwaltungsabläufe in der Personalverwaltung nicht auf ihre Notwendigkeit hin hinterfragt wird. In letzter Zeit hatte ich wiederholt Anlaß zur Kritik an der Handhabung von Personalunterlagen. Dazu gehörte beispielsweise die Aufnahme von Unterlagen in Personalakten, die auch Daten anderer Mitarbeiter enthielten (vgl. z. B. 18. Tätigkeitsbericht, Ziff. 12.1).

Ich beabsichtige, in der nächsten Zeit verstärkt die Praxis von Personalverwaltungen zu überprüfen. Erste Stichproben zur Information über Verfahrensweisen in unterschiedlich großen Verwaltungen haben gezeigt, daß in vielen Fällen mehrere Komplexe zu überdenken sind:

- Ordungsgemäße Führung von Haupt- und Nebenakten;
- klare Regelungen, welche Kompetenzen nachgeordnete Dienststellen haben und, daran anknüpfend, Festlegungen für die Organisation der Personalaktenführung,
- Umsetzung des § 107f HBG hinsichtlich der unterschiedlichen Aufbewahrungsfristen.

So habe ich z. B. in einem Fall festgestellt, daß die Nebenakte nochmals sämtliche Unterlagen enthielt, die auch die übergeordnete Dienststelle in der Personalakte führte, nur ergänzt um Urlaubs- und Krankmeldungen. Nur für die letzteren war die Dienststelle selbst zuständig.

§ 107 Abs. 4 HBG regelt auch die Datenerhebung. Unter Zugrundelegung der Neuregelung muß die Mehrzahl der im Personalbereich verwendeten Formulare überarbeitet werden. Dies gilt für die Personalbögen ebenso wie für die Unterlagen zum Besoldungsrecht. Der landeseinheitliche Personalbogen wird derzeit schon neu erstellt. Dabei ist m.E. klar zu trennen zwischen Daten, die von allen Beschäftigten benötigt werden, und Daten, die nur in Einzelfällen relevant sein können. Darüber hinaus sind nicht nur der Umfang der Fragen, sondern auch der Zeitpunkt der Datenerhebung zu berücksichtigen. Häufig wird schon von Bewerbern, die in die engere Wahl kommen, verlangt, den Personalbogen auszufüllen. Damit werden dann aber Daten erfragt, die für die Einstellungsentscheidung überhaupt nicht relevant sein können.

10.1.3
Hessisches Personalinformationssystem (HEPIS)

Gleichzeitig mit der Novellierung des Hessischen Beamtengesetzes ist die von mir schon seit mehr als sieben Jahren angemahnte Rechtsgrundlage für das beim Landespersonalamt (LPA) geführte HEPIS-System geschaffen worden. In § 111 Abs. 2 HBG ist nunmehr bestimmt, daß das LPA eine solche Datei führt und dazu die Daten von den Besoldungsstellen erhält. Klargestellt ist jetzt auch, daß neben Auswertungen zu Zwecken der Personalplanung jeweils für die Ressorts personenbezogene Auswertungen zur Unterstützung der Personalverwaltung möglich sind. Dies sind z. B. Wählerlisten, Personallisten, Auswertungen zu Dienstjubiläen usw.

10.2
Zugang der Frauenbeauftragten zu Personalakten

Seit es vermehrt Frauenbeauftragte in den Dienststellen gibt, bin ich wiederholt danach gefragt worden, welche Rechte die Frauenbeauftragte im Umgang mit Personalakten hat. Dies hängt natürlich entscheidend davon ab, wie sie bestellt worden ist und welche Rechte ihr zugewiesen sind.

Eine Frauenbeauftragte, die von der Dienststelle berufen wird, nimmt eine Aufgabe der Dienststelle wahr. Sie ist u.a. an Personalentscheidungen beteiligt. Damit gehört sie zu dem Personenkreis, der gemäß § 107a Hessisches Beamtengesetz im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten befaßt ist, und hat somit ein Zugangsrecht zu Personalakten. Einer ausdrücklichen gesetzlichen Regelung, etwa wie für die Personalvertretung, bedarf es daher nicht.

Dies bedeutet im Ergebnis nicht, daß die Frauenbeauftragte von sich aus Zugang zu allen Personalakten in der Dienststelle hat. Ihr Einsichtsrecht ist – wie das aller mit Personalangelegenheiten betrauter Mitarbeiter – durch den Grundsatz der Erforderlichkeit beschränkt. Sie hat daher nur Zugang zu jeweils den Unterlagen, die Grundlage für die entsprechenden Entscheidungen bzw. Vorgänge sind, bei denen sie beteiligt ist. Soweit für solche Sachverhalte von der Dienststelle komplette Personalakten beigezogen werden, hat auch die Frauenbeauftragte ein entsprechendes Einsichtsrecht.

10.3
Zugang des Personalrats zu Personalverwaltungssystemen

Immer mehr Dienststellen setzten Personalverwaltungssysteme ein. Dabei ist der Umfang der gespeicherten Daten sehr unterschiedlich. § 107g Hessisches Beamtengesetz legt den Rahmen fest, innerhalb dessen Personalaktendaten automatisiert verarbeitet werden dürfen. Für alle diese Verfahren gilt, daß jeweils derjenige Personenkreis Zugang zu Daten haben kann, der mit dem Aufgabenbereich innerhalb der Personalverwaltung betraut ist, für den das Verfahren eingerichtet ist (z. B. Urlaubsdatei, Reisekostenabrechnung usw.). Das kann bei Systemen, die verschiedene Bereiche der Personalverwaltung abdecken, auch bedeuten, daß einzelne nur auf Teile der Daten zugreifen können.

In diesem Zusammenhang ist zu prüfen, ob auch dem Personalrat ein Zugangsrecht zu solchen Systemen eingeräumt werden kann. Nach den Regelungen des Personalvertretungsrechts hat der Personalrat ohne Einwilligung des Beschäftigten kein eigenes Zugangsrecht zur Personalakte. Ihm sind jedoch alle Unterlagen zur Verfügung zu stellen, die zu seiner Aufgabenerfüllung erforderlich sind. D.h. die Entscheidungsgrundlagen, die der Dienststelle für ihre Meinungsbildung zur Verfügung gestanden haben, sind ihm zugänglich zu machen. Nur dann kennt er alle entscheidenden Gesichtspunkte, um sein Mitbestimmungsrecht sachgerecht ausüben zu können. Über das Beteiligungsrecht in Einzelfällen hinaus hat der Personalrat aber auch allgemeine Aufgaben gemäß § 62 Hessisches Personalvertretungsgesetz, beispielsweise Maßnahmen zur beruflichen Förderung Schwerbehinderter zu beantragen, die Eingliederung ausländischer Beschäftigter zu fördern usw. Um diese Pflichten sinnvoll ausfüllen zu können, benötigt der Personalrat einen Überblick, wen er vertritt. Diese Daten sind ihm daher zur ständigen Verwendung zur Verfügung zu stellen. Dazu gehören Angaben wie Name, Organisationseinheit, Eingruppierung, letzte Beförderung, Beurlaubung, Ermäßigung der Arbeitszeit. In welchem Rhythmus diese Aufstellungen aktualisiert werden, müssen die Beteiligten miteinander vereinbaren.

Das gleiche gilt für das Verfahren, wie die Daten zur Verfügung gestellt werden. Grundsätzlich ist es möglich, dem Personalrat ein Leserecht für diese Datenfelder im Personalverwaltungssystem einzuräumen, unter der Bedingung,

daß sichergestellt ist, daß er nur auf die entsprechenden Felder zugreifen kann. Eine Rahmenbedingung, die für jeden anderen Nutzer des Systems ja ebenfalls gilt.

Der Personalrat ist im übrigen genauso an die Regelungen des Hessischen Datenschutzgesetzes gebunden. Auch er hat z. B. die Zweckbindung zu beachten, Löschungsfristen festzulegen und die entsprechenden Datensicherungsmaßnahmen zu treffen bzw. die zentral für die Benutzer des Systems vorgegebenen einzuhalten.

11. Sozialwesen

11.1
Mißbrauchskontrolle beim Sozialhilfebezug

11.1.1
Das neue Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms

Immer wenn aus wirtschaftspolitischen Gründen über Einsparungen im Sozialleistungsbereich diskutiert wird, ist dies mit einer intensiven Debatte um den Mißbrauch von Sozialleistungen und der Forderung nach mehr Kontrolle verbunden. Ein Ansatz dazu findet sich jetzt u.a. im Gesetz über Maßnahmen zur Bewältigung der finanziellen Erblasten im Zusammenhang mit der Herstellung der Einheit Deutschlands, zur langfristigen Sicherung des Aufbaus in den neuen Ländern, zur Neuordnung des bundesstaatlichen Finanzausgleichs und zur Entlastung der öffentlichen Haushalte (Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms (FKPG)) vom 23. Juni 1993, BGBl. I S. 944. Neben dem Bereich der Arbeitsförderung sind hier vor allem die Sozialhilfeträger angesprochen. Ihnen soll durch umfangreiche Datenabgleiche ein Instrumentarium an die Hand gegeben werden, Doppelbezug von Leistungen oder unkorrekte Angaben zu den Einkommensverhältnissen aufzudecken.

Unbestritten ist es notwendig, vorhandenen Mißbrauch von Sozialleistungen gerade auch durch unberechtigten Doppelbezug aufzudecken bzw. zu verhindern. Eine Grenze sehe ich jedoch da, wo für die Mehrzahl der gesetzestreuen Bürger die Gefahr nicht auszuschließen ist, zum „Gläsernen Leistungsbezieher" zu werden. An den verfassungsrechtlichen Vorgaben für einen Eingriff in das Recht auf informationelle Selbstbestimmung ist festzuhalten. Dies gilt insbesondere bezüglich der Normenklarheit, der Zweckbindung sowie des Grundsatzes, daß bei der Überprüfung von Anträgen Auskünfte, Nachweise und Bescheinigungen zunächst beim Antragsteller selbst einzuholen sind, bevor Überprüfungen bei dritten Stellen erfolgen. Daß die Tatsache allein, daß ein Bürger eine Sozialleistung beantragt, ohne nähere Berücksichtigung des Einzelfalles zum Abgleich mit einer Fülle von anderen Leistungsträgern führen soll und damit quasi die Bemühung, unrechtmäßig Leistungen zu erhalten, unterstellt wird, halte ich unter dem Gesichtspunkt der Verhältnismäßigkeit für sehr bedenklich. Den Gesetzentwurf zum FKPG (BTDrucks. 12/4401) habe ich daher entsprechend kritisiert. Ein Teil dieser Kritik, die auch von anderer Seite vorgetragen wurde, ist im Laufe des Gesetzgebungsverfahrens aufgegriffen worden. Insbesondere wurden der Umfang der abzugleichenden Daten und der beteiligten Stellen konkretisiert.

Das Bundessozialhilfegesetz i.d.F. des Art. 7 FKPG gibt nunmehr den Sozialhilfeträgern drei Überprüfungsmöglichkeiten:

- Regelmäßig im Wege des automatisierten Datenabgleichs ist es möglich zu überprüfen, ob und welche Leistungen bei der Bundesanstalt für Arbeit oder bei Trägern der Renten- oder Unfallversicherung bezogen wurden bzw. ob Versicherungspflicht besteht oder eine geringfügige Beschäftigung ausgeübt wird (§ 117 Abs. 1 Bundessozialhilfegesetz (BSHG)). Der dabei zu verwendende Datensatz ist festgelegt, ebenso die Zweckbindung und die Verpflichtung zur unverzüglichen Löschung der Daten aller Personen, für die keine Feststellungen getroffen sind. § 117 Abs. 1 BSHG sieht vor, daß in einer Rechtsverordnung das Verfahren des Abgleichs näher bestimmt wird. Bis dahin ist ein solcher Abgleich nicht zulässig.
- Zulässig ist künftig auch ein Abgleich der Sozialhilfeträger untereinander; diese dürfen alle erforderlichen Daten für einen solchen Abgleich übermitteln. Für den regelmäßigen Abgleich ist aber auch hier zunächst noch eine Rechtsverordnung erforderlich (§ 117 Abs. 2 BSHG).
- Im Einzelfall ist es den Sozialämtern möglich, bei anderen Stellen ihrer Verwaltung, also z. B. beim Meldeamt oder der Kfz-Zulassungsstelle, Daten zu überprüfen (§ 117 Abs. 3 BSHG).

11.1.2
Erste Anwendungserfahrungen mit der Neuregelung

In der Praxis ist der Umfang der neuen Befugnisse nicht immer klar. So wurde ich von einem Landkreis gefragt, ob es jetzt wieder möglich sei, den Wohnsitzgemeinden eine Kopie des Sozialhilfebescheides zu übersenden (vgl. 16. Tätigkeitsbericht, Ziff. 7.1). Dies ist jedoch weder für die Aufgabenerfüllung der Sozialhilfeträger noch für die Wohnortgemeinden erforderlich und daher weiterhin unzulässig.

§ 117 Abs. 3 BSHG regelt sehr konkret, welche Daten „soweit erforderlich" bei anderen Stellen überprüft werden dürfen. Die Überprüfung setzt zwingend voraus, daß vor einer Entscheidung die Angaben des Antragstellers überprüft werden. Dies ist bei der Übersendung des Sozialhilfebescheides, d.h. nach der Entscheidung von der Sache her nicht möglich. Darüber hinaus legt § 117 Abs. 3 BSHG aber auch einen konkreten Katalog fest, welche Angaben auf diese

Weise überhaupt überprüft werden dürfen. Auch hier geht der Sozialhilfebescheid mit seinem Inhalt weit über diesen Katalog hinaus.

In einem anderen Fall war der Umfang der zulässigen Nachfragen bei der Kfz-Zulassungsstelle zu klären. Ein Sozialamt hatte dazu ein Formblatt entwickelt, das u.a. für einen Antragsteller bzw. sämtliche Mitglieder seines Haushaltes Auskünfte zum amtlichen Kennzeichen, dem Fabrikat und Typ des Kraftfahrzeugs sowie den Tag der ersten Zulassung und das Datum einer eventuellen Umschreibung erfragte. Dies war vom Rahmen des § 117 Abs. 3 Ziff. f BSHG nicht gedeckt. Bisher durften die Kfz-Zulassungsstellen gar keine entsprechenden Auskünfte erteilen.

Zulässig ist daher nur die Übermittlung der Daten, zu denen § 117 Abs. 3 BSHG ausdrücklich verpflichtet. Dies ist lediglich die Eigenschaft als Kfz-Halter. Zusätzliche Angaben zum einzelnen Fahrzeug sind nicht möglich.

Wenn es für die Beurteilung des Sozialhilfeträgers nicht nur auf den Zeitpunkt der Anfrage, sondern auch auf Verhältnisse in der Vergangenheit ankommt, ist der genaue Zeitrahmen, für den gefragt wird, anzugeben. Dabei ist zu berücksichtigen, daß Angaben für die Vergangenheit in der Regel nur dann in Betracht kommen, wenn über die Ansprüche für diesen Zeitraum noch nicht entschieden ist. Auf jeden Fall halte ich es für unzulässig, bei jeder Anfrage den Tag der Erstzulassung sowie den Tag einer Umschreibung des Fahrzeugs zu erfragen.

11.2
Ermittlung zur Gestaltung der Haushaltsführung von Wohngeldantragstellern durch die Wohngeldstelle

Wer Wohngeld beantragt, hat im Rahmen des Wohngeldgesetzes und der §§ 60 bis 65 Sozialgesetzbuch I Mitwirkungspflichten, die darauf zielen, der zuständigen Wohngeldstelle alle Tatsachen anzugeben, die für die zu gewährende Leistung erheblich sind. Darüber hinaus hat der Antragsteller der Einholung von erforderlichen Auskünften bei Dritten zuzustimmen, wenn die Wohngeldstelle dies verlangt.

Die Datenerhebung erfolgt mittels eines Vordrucks „Antrag auf Wohngeld (Mietzuschuß)". U.a. hat der Antragsteller in diesem Vordruck seine und die Einkünfte der zu seinem Haushalt gehörenden Personen detailliert anzugeben. Was zu den Einnahmen gehört, ist in den Hinweisen zum Ausfüllen des Vordrucks beispielhaft beschrieben: Gehälter, Löhne, Gratifikationen, Tantiemen, Trinkgelder, Ruhegelder, Witwen- und Waisengelder, Renten aller Art, Einnahmen aus selbständiger Tätigkeit, aus Gewerbebetrieb, aus Land- und Forstwirtschaft, aus Kapitalvermögen, aus Vermietung und Verpachtung (ohne Einnahmen aus Untervermietung), Unterhalt, Sachbezüge, Arbeitslosengeld, Arbeitslosenhilfe. Die Einnahmen sind zudem gegenüber der Wohngeldstelle durch entsprechende Nachweise zu belegen.

Die Daten zu den Einkünften sowie die ebenfalls in dem Wohngeldantrag vorgesehenen Angaben zu den monatlichen Mietbelastungen einschließlich der Nebenkosten waren für eine hessische Wohngeldstelle offenbar nicht ausreichend. Diese Wohngeldstelle hatte, wie mir durch die Beschwerde einer Bürgerin bekannt wurde, einen zusätzlichen Vordruck verwendet, der abfragen sollte, welche konkreten Beträge die Antragstellerin und ihre zum Haushalt rechnenden Personen im Laufe eines Jahres verbraucht hatten. Dieser Vordruck war dem Wohngeldantrag ohne nähere Erläuterungen durch die Wohngeldstelle beigefügt und verlangte: „Ergänzende Angaben zu meinem Wohngeldantrag vom ...". Nicht nur, daß, wie bereits im Wohngeldantrag selbst, nach den Kosten der Unterkunft gefragt wurde, die Wohngeldstelle wollte zudem wissen, welche Beträge die Antragstellerin und die zum Haushalt gehörenden Personen durchschnittlich im Monat für die Bestreitung des Lebensunterhaltes aufwenden. Folglich fanden sich in dem Vordruck Fragen zu den Aufwendungen für Ernährung (Frühstück, Mittag- und Abendessen); Neuanschaffung für Bekleidung; Telefon, Rundfunk, Fernsehen; Reinigung und Reparaturen von Schuhen, Kleidung, Wäsche usw.; Versicherungen; persönliche Dinge des täglichen Lebens (einschließlich Kosmetik, Körperpflege, Bücher, Zeitschriften, Vereine, Hobby usw.).

Die Antragstellerin sollte mit ihrer Unterschrift versichern, daß ihre Angaben der Wahrheit entsprechen und daß sie darüber informiert wurde, daß falsche oder unvollständige Angaben zur Rücknahme des Wohngeldbescheides und zur Rückforderung des bereits gezahlten Wohngeldes führen können. Der Hinweis auf die Möglichkeit eines Verfahrens wegen Betruges nach § 263 Strafgesetzbuch fehlte ebenfalls nicht in dem Vordruck.

Die Wohngeldstelle begründete ihr Vorgehen damit, daß auf diese Weise erkennbare Differenzen zwischen den schon bekannten Angaben zu Einnahmen und Ausgaben auszuräumen seien und so Nachfragen und der damit verbundene Ärger mit den Antragstellern vermieden werden könnten.

Diese Datenerhebung ist jedoch unzulässig. Im Wohngeldgesetz ist konkret geregelt, welche Daten zur Entscheidung über einen Wohngeldantrag erhoben werden dürfen. Der Nachweis täglicher oder monatlicher Ausgaben gehört keinesfalls dazu. Die Formulierungen des Vordruckes und das gewählte Verfahren suggerierten zudem eine Verpflichtung der Antragstellerin, diese Angaben zu machen, die eben nicht im Rahmen der gesetzlichen Mitwirkungspflichten erforderlich sind.

Die Wohngeldstelle wird den Vordruck künftig nicht mehr verwenden.

11.3
Verdienstanfrage des Sozialamts bei dem Arbeitgeber eines Unterhaltsverpflichteten

Der Datenschutzbeauftragte der Sozialverwaltung einer hessischen Stadt hatte mir im Frühjahr drei von Fachverlagen erstellte Vordrucke „Verdienstanfrage beim Arbeitgeber", „Verdienstanfrage an Arbeitgeber" und „Anfrage über Arbeitsverdienst" zur datenschutzrechtlichen Prüfung übersandt.

Die Formulare wurden vom städtischen Sozialamt benutzt, um im Rahmen des § 116 Abs. 2 BSHG bei Arbeitgebern von Unterhaltspflichtigen Daten zu erheben, die als Grundlage für die Berechnung und Festsetzung von Ersatzansprüchen des Sozialamtes gegen die Unterhaltspflichtigen dienten. Der Verwaltungsablauf zur Verwendung der Vordrucke durch das Sozialamt wurde mir so geschildert, daß es ständige Praxis des Sozialamtes sei, Unterhaltspflichtige nach § 116 Abs. 1 BSHG aufzufordern, ihre Einkommens- und Vermögensverhältnisse gegenüber dem Sozialamt darzulegen und gleichzeitig mit der Aufforderung einen der o.g. Vordrucke zu übersenden. Dieser sei vom Arbeitgeber auszufüllen und zusammen mit den eigenen wirtschaftlichen Angaben dem Sozialamt vorzulegen.

Diese Verwaltungspraxis ist grundsätzlich unzulässig. Im Rahmen des § 116 Abs. 1 BSHG müssen Unterhaltspflichtige Angaben zu ihren Einkommens- und Vermögensverhältnissen machen, soweit sie zur Durchführung des Bundessozialhilfegesetzes erforderlich sind. Wenn Unterhaltspflichtige dieser Verpflichtung nachkommen und keine substantiellen Verdachtsmomente vorliegen, die gegebenen Auskünfte könnten wahrheitswidrig sein, dürfen zusätzliche Auskünfte bei Arbeitgebern im Rahmen des § 116 Abs. 2 BSHG vom Sozialamt nicht eingeholt werden. Hieraus folgt, daß ein Unterhaltspflichtiger, wenn er bereit ist, die erforderlichen Auskünfte zu erteilen, nicht vom Sozialamt verpflichtet werden darf, die Bescheinigung „Verdienstanfrage beim Arbeitgeber" seinem Arbeitgeber vorzulegen.

Das Sozialamt hat aber auch sicherzustellen, daß in den verwendeten Fragebogen die einzelnen Fragen die gesetzlichen Grenzen nicht überschreiten. Die mir übersandten Vordrucke zur Auskunftseinholung bei Arbeitgebern erfüllen diese Voraussetzung nicht.

Die in den Vordrucken enthaltenen Datenerhebungen gehen zum Teil weit über die zulässige Datenerhebung nach § 116 Abs. 2 BSHG hinaus. In § 116 Abs. 2 BSHG ist klar festgelegt, welche Daten vom Sozialamt beim Arbeitgeber zu erheben sind. Es handelt sich hierbei im einzelnen um Angaben über die Art und Dauer der Beschäftigung, die Arbeitsstätte und den Arbeitsverdienst. Die Datenerhebung durch das Sozialamt muß sich auf die konkret aufgeführten Sachverhalte beschränken. Keinesfalls dürfen vom Arbeitgeber zum Beispiel Angaben über Versicherungsverhältnisse (Name und Anschrift der Krankenkasse) eines Unterhaltsverpflichteten oder Einkünfte von Familienangehörigen verlangt werden. Auch die Frage nach Entlassungsgründen eines Arbeitnehmers oder den Namen der Gläubiger bei eventuellen Lohnpfändungen ist unzulässig.

Ich habe die Stadt aufgefordert, die Verwaltungspraxis und die Formulare entsprechend zu ändern.

12. Schulen

12.1
Neue Rechtsverordnung für den Datenschutz in Schulen

Am 1. August 1993 ist das neue Schulgesetz (SchulG, GVBl. I (1992) S. 233) in Kraft getreten. Seine besondere Bedeutung für die Entwicklung des Datenschutzes in der gesamten hessischen Schulverwaltung hatte ich bereits im 21. Tätigkeitsbericht ausführlich erläutert (Ziff. 11.1). Es bietet erstmals eine ausreichende gesetzliche Grundlage für eine verfassungsgemäße Verarbeitung der personenbezogenen Daten im Schulbereich, die ich seit Jahren angemahnt hatte (vgl. 19. Tätigkeitsbericht, Ziff. 6.3.1).

Allerdings enthält das Gesetz nicht abschließende und erschöpfende Regelungen für alle denkbaren Fragestellungen im Datenschutzbereich, es hat sich vielmehr auf wesentliche Grundsätze beschränkt und nur dort Einzelregelungen getroffen, wo Leitentscheidungen des Gesetzgebers notwendig waren. Im übrigen hat es die weitere notwendige Konkretisierung ausdrücklich einer ergänzenden Rechtsverordnung überlassen (§ 83 Abs. 7 SchulG).

Der mir zwischenzeitlich vom Hessischen Kultusministerium vorgelegte Entwurf einer solchen Rechtsverordnung mit zahlreichen Anlagen beschränkt sich allerdings auf den Betrieb der Schule selbst, wie er auch in § 83 Abs. 1 SchulG in bewußter Differenzierung von dem Bereich des Schulträgers und der Schulaufsichtsbehörden angesprochen wird. Der Entwurf entspricht weitestgehend dem seit Jahren vorliegenden Text eines Erlaßentwurfes zum Datenschutz in Schulen, zu dem ich bereits 1990 ausführlich Stellung genommen hatte (vgl. 19. Tätigkeitsbericht, Ziff. 6.3.2). Erfreulicherweise hat das Kultusministerium in dem ganz überwiegenden Teil meine damaligen Änderungsvorschläge berücksichtigt, so daß sich die weiteren Änderungswünsche auf wenige Fragestellungen beschränkten. Wegen der immer wiederkehrenden Streitfragen möchte ich hier folgende Punkte herausgreifen:

12.1.1
Einsatz privater PC's

Soweit die Lehrkraft für schulische Zwecke den eigenen PC einsetzen will – diese Tendenz nimmt fortlaufend zu –, bestimmt bereits § 83 Abs. 5 Satz 3 SchulG, daß der Schulleiter dies in begründeten Ausnahmefällen genehmigen

kann. Nach § 83 Abs. 7 SchulG muß die Rechtsverordnung auch festlegen, welche schulischen Daten hier überhaupt nur verarbeitet werden dürfen. Der in § 2 Abs. 3 des Entwurfs genannte Katalog erwähnt lediglich: Name, Vorname, Jahrgangsstufe, Klassen-, Kurs- und Lerngruppenbezeichnung, Unterrichtsfächer und Ergebnisse schriftlicher Arbeiten. Weitere Daten von Schülern und Eltern können zwar auch auf dem privaten PC maschinell verarbeitet werden, aber nur mit Einverständnis der Betroffenen i.S.d. § 7 Hessisches Datenschutzgesetz (HDSG). Die Schule bleibt dabei speichernde Stelle i.S.v. § 6 Abs. 1 HDSG mit allen sich daraus ergebenden Pflichten, etwa der Dateibeschreibung. Auch muß die den privaten PC einsetzende Lehrkraft in dem Genehmigungsantrag ausreichende Datensicherheitsmaßnahmen nach § 10 HDSG nachweisen.

12.1.2
Klassenbuch

Anlaß zahlreicher Anfragen sind immer wieder die Unklarheiten über die Daten, die ausschließlich im Klassenbuch vermerkt werden dürfen. Übereinstimmung besteht mit Datenschutzregelungen anderer Bundesländer und mit dem Vorschlag des Hessischen Kultusministeriums, sowohl Leistungsdaten als auch Vermerke über grobes Fehlverhalten der Schüler aus dem Klassenbuch zu verbannen. Die Notwendigkeit der Dokumentation dieser Daten soll nicht bestritten werden, sie kann jedoch problemlos auf eine Weise vollzogen werden, die sicherstellt, daß nur diejenigen Lehrkräfte von den Daten Kenntnis erlangen, welche die Daten benötigen. Im übrigen entfällt damit einer der Gründe, warum Klassenbücher oft verschwinden.

12.1.3
Schulischer Datenschutzbeauftragter

Schließlich bringt die nach § 5 Abs. 2 HDSG vorzunehmende Bestellung eines schulischen Datenschutzbeauftragten immer wieder Probleme mit sich. Insbesondere der im Gesetz genannte Interessenkonflikt ist bei der Bestellung zu vermeiden. Selbstredend sind damit Schulleiter und ihre Vertreter auszuschließen. Gleiches soll nach meinem Vorschlag auch gelten für Lehrer, „die für die Entscheidung über die Einführung, Anwendung, Änderung oder Erweiterung der automatisierten Verarbeitung personenbezogener Daten zuständig sind". Bei Schulen mit nur einer oder zwei hauptamtlichen Lehrkräften muß ein Mitarbeiter des Staatlichen Schulamtes bestellt werden. Im übrigen enthält die Anlage 4 des Entwurfs eine umfangreiche Aufstellung der zahlreichen Aufgaben des schulischen Datenschutzbeauftragten.

12.1.4
Datensicherheitsmaßnahmen

Die Anlage 5 beschreibt ausführlich den Katalog notwendiger Maßnahmen zur Datensicherheit i.S.d. § 10 HDSG. Mit Zunahme der Automation der schulischen Datenverarbeitung, damit verbundener technischer Gefahren – wie etwa Computerviren – und mit vermehrtem Diebstahl schulischer PC's erhält auch die technische Datensicherheit einen besonderen Stellenwert. Selbstverständlich sollte jede Schule einen Papierzerkleinerer besitzen.

Kurz vor Redaktionsschluß teilte mir das Hessische Kultusministerium mit, daß meine Änderungswünsche fast ausnahmslos berücksichtigt würden und die Rechtsverordnung vor der Verkündung stehe. Es bleibt zu hoffen, daß auch die Rechtsverordnung für den Bereich der Schulaufsichtsbehörden nicht lange auf sich warten läßt, zumal dort wichtige Regelungen anstehen wie etwa die zum Tätigkeitsfeld der Schulpsychologen. Nach letzten Mitteilungen des Hessischen Kultusministeriums wird dieser Forderung ausreichend Rechnung getragen werden.

12.2
Automatisierung von Verwaltungs- und Planungsaufgaben im Schulbereich

Bereits im Sommer 1993 informierte mich das Hessische Kultusministerium über die Absicht, die hessische Schulverwaltung künftig in großem Umfang zu automatisieren. Ähnliche Bestrebungen gibt es auch in anderen Bundesländern, etwa in Nordrhein-Westfalen. Kurz vor Redaktionsschluß legte mir dann das Ministerium den endgültigen Text des umfangreichen Gesamtkonzeptes der Automatisierung zur Stellungnahme vor. Das Konzept schließt an das bereits seit Jahren bestehende Hessische Schulinformationssystem (HESIS) an, das jedoch nur auf Teilen der Automatisierung von administrativen Aufgaben und Planungsaufgaben beruht. In das dichte Netz des Informationsflusses von Daten der Lehrkräfte und Schüler sind zahlreiche Schulbehörden eingebunden, von der Schule selbst über das Staatliche Schulamt, das Regierungspräsidium bis hin zum Ministerium selbst. Daneben erhalten verschiedene Daten auch das Hessische Statistische Landesamt, die Schulträger, die Zentrale Besoldungsstelle usw. Der Informationsaustausch erfolgt bisher jedoch überwiegend auf herkömmliche Weise.

12.2.1
Planungsziele

Zur Verbesserung der Einheitlichkeit der Datenstrukturen sowie der Aktualität der Daten und zur Vermeidung identischer Arbeitsabläufe in verschiedenen Behörden ist nun beabsichtigt, eine zentrale Datei zu schaffen, an welche die verschiedenen Schulbehörden sowie das Hessische Staatistische Landesamt im Online-Verfahren unmittelbar angeschlossen sind. Die genannten Behörden sollen ihre Verwaltungs- und Planungsaufgaben zwar mit eigener Hard- und Software eigenverantwortlich erledigen, sie bedienen sich jedoch zum Datenaustausch dieser zentralen Datei, die

u.a. sowohl schulverwaltungsbezogene Daten der Lehrkräfte als auch der Schüler aus ganz Hessen in der aktuellen Fassung enthält. Die angeschlossenen Behörden sollen, je nach Zuständigkeit, die exakt bezeichneten Daten nach einheitlichen Vorgaben und Bedingungen eingeben, löschen, erfragen oder aktualisieren können. Von diesem Datenbestand sollen sie nach ihrem Bedürfnis, im Rahmen noch festzulegender Zugriffsbeschränkungen, Teile kopieren und weiterbearbeiten können.

12.2.2
Fragestellungen

Dieses Konzept wirft eine Fülle von datenschutzrechtlichen Problemen auf, deren Lösung mangels detaillierter Angaben im Konzept noch nicht absehbar ist. Da es sich hier um ein automatisiertes Abrufverfahren handelt, steht in formeller Hinsicht die Forderung im Mittelpunkt, vor Realisierung zumindest eine Rechtsverordnung nach § 15 HDSG zu erlassen. Dabei hat die Landesregierung im Rahmen des Grundsatzes der Verhältnismäßigkeit abzuwägen, ob im Interesse der Allgemeinheit ein ausreichender Grund für einen schnellen Datenaustausch besteht. Auch unter Berücksichtigung der ab dem 1. Dezember 1993 geltenden neuen Regelung des § 107g Abs. 1 Hessisches Beamtengesetz (GVBl. 1993, S. 473) ist eine besondere Rechtsvorschrift für den automatisierten Abruf von Personalaktendaten zu fordern. Völlig ungeklärt ist das Rechtsverhältnis der verschiedenen angeschlossenen Behörden zueinander und zu der Zentraldatei, die einen hohen Grad von Eigenständigkeit erhalten soll, auch wenn sie von der Hessischen Zentrale für Datenverarbeitung verwaltet werden wird.

12.3
Übermittlung schulischer Daten italienischer Grundschüler an das Italienische Generalkonsulat Frankfurt

Oftmals kann ich bei grundsätzlichen datenschutzrechtlichen Fragestellungen erst dann beratend tätig werden, wenn der Verwaltungsvollzug bereits begonnen hat und die ersten Beschwerden erhoben werden. Als Beispiel sinnvoller, viel Verdruß und Aufwand ersparender Zusammenarbeit mit Behörden ist eine rechtzeitige Anfrage zu erwähnen, die ich vom Hessischen Kultusministerium erhielt und die zu einem gemeinsamen und praktikablen Arbeitsergebnis führte.

Das Italienische Generalkonsulat Frankfurt hatte das Ministerium über die Absicht informiert, im Rahmen eines vom italienischen Staat aufgelegten Förderprogramms italienische Grundschüler in Hessen außerschulisch mit besonders beauftragten Lehrkräften zu fördern, soweit erhebliche Anpassungsprobleme an deutsche Schulen und allgemeine Lebensverhältnisse erkennbar geworden sind. Ähnliche Vorhaben werden bereits in anderen Bundesländern durchgeführt. Sinnvoll und erfolgversprechend ist die Förderung nur, wenn die eingesetzten Lehrkräfte umfassend über die schulischen Leistungen und Probleme des Kindes unmittelbar durch die Schule informiert sind. Diese vom Generalkonsulat erbetene Übermittlung schulischer Daten ist nach § 17 Abs. 1 HDSG jedoch nur zulässig, wenn sie in einem Gesetz oder einer internationalen Vereinbarung ausdrücklich geregelt ist. In Ermangelung dieser Voraussetzung käme zwar auch § 17 Abs. 2 HDSG in Betracht, wonach der Drittstaat „gleichwertige Datenschutzregelungen" geschaffen haben muß. Da zur Zeit in Italien Datenschutzgesetze überhaupt fehlen, kann nur eine Einwilligung i.S.d. § 7 Abs. 1 Nr. 2 HDSG die gewünschte Übermittlung ermöglichen.

12.3.1
Probleme der ausreichenden Aufklärung

In den der Anfrage folgenden Gesprächen und Verhandlungen mit dem Italienischen Generalkonsulat und dem Ministerium stellte sich bald heraus, daß die Probleme insbesondere bei der umfassenden Aufklärung der betroffenen Eltern und Kinder i.S.d. § 7 Abs. 2 HDSG liegen; diese Aufklärung hat notwendigerweise der schriftlichen Einwilligungserklärung vorauszugehen und läßt diese erst rechtswirksam werden. Sowohl die nicht einfach gelagerten Abläufe des Informationsflusses von der Schule über das Generalkonsulat und den von diesem zwischengeschalteten „Schulausschuß" bis hin zum konkret eingesetzten Förderlehrer sind darzustellen als auch die rechtliche Tragweite der Einwilligung und der Verwendungszweck. Als datenschutzrechtlich nicht ganz unproblematisch war dabei der Umstand zu würdigen, daß eine maschinelle Verarbeitung der Schuldaten vorgesehen ist und meine datenschutzrechtliche Kontrolle außerhalb des Schulbereichs entfällt. Ein diesbezüglicher Hinweis ist unverzichtbar, um den betroffenen Eltern und Kindern eine Abschätzung aller Vor- und Nachteile der Einwilligungserklärung zu ermöglichen.

12.3.2
Zusagen des Generalkonsulats

Es konnte allerdings die Zusage des italienischen Generalkonsuls erreicht werden, im Rahmen seiner Möglichkeiten zu gewährleisten, daß die Daten ausschließlich für den Förderunterricht benutzt und nach seinem Abschluß gelöscht werden. Auch wurde zugesagt, den jeweils eingesetzten Förderlehrer auf Geheimhaltung, Zweckbindung der Daten, ihre rechtzeitige Löschung und notwendige technische Datensicherheitsmaßnahmen ausdrücklich zu verpflichten. Das gemeinsam erarbeitete, in deutsch-italienischer Sprache ausgefertigte Informationsblatt hat alle diese Anforderungen und Auflagen zum Inhalt, so daß die formularmäßige Einwilligungserklärung eine gesicherte Basis für die Datenübermittlung darstellt. Das Land Rheinland-Pfalz hat sich zwischenzeitlich diese Vorarbeiten, wie ich erfahren habe, zunutze gemacht.

12.4
Bescheid unter Verwendung eines Briefes an einen Dritten

Der Fantasie öffentlich Bediensteter, behördliche Tätigkeiten und Abläufe zu vereinfachen und zu verkürzen und damit Zeit für kreative Arbeit zu gewinnen, sind keine Grenzen gesetzt. Ein gut dotiertes Verbesserungsvorschlagswesen kann dem Dienstherrn gelegentlich erheblichen Gewinn an Arbeitsinhalten oder Aufwandsersparnis bescheren. Doch manchmal überschreitet der gute Wille rechtliche Grenzen, wenn auch meistens nicht bösgläubig.

Ein hessischer Lehrer konfrontierte mich mit folgendem Sachverhalt: Er hatte sich bei der oberen Fachaufsichtsbehörde über eine Entscheidung des Schulamtes beschwert, das eine von ihm erteilte Mathematiknote aufgehoben und gegen sein Votum und das des Abiturprüfungsausschusses den betroffenen Schüler zum mündlichen Abitur zugelassen hatte. In der gleichen Sache hatte die eingeschaltete Fachaufsichtsbehörde auch anläßlich einer Beschwerde des genannten Prüfungsausschusses darüber zu befinden, daß sein Votum zur Nichtzulassung zum Abitur übergangen worden sei. Die Aufsichtsbehörde betrachtete beide Beschwerdeverfahren als sachliche und rechtliche Einheit, so daß sie die Kopie der Beschwerdeentscheidung gegenüber dem betroffenen Lehrer dem Prüfungsausschuß übersandte und ihn damit beschied.

Personal- und Sachaufwand wurden hier zweifellos erspart, aber rechtmäßig war dies nicht. Denn der Bescheid an den betroffenen Lehrer enthielt zahlreiche Hinweise und Einschätzungen bezüglich seiner Notengebung sowie seiner Aufgabenerfüllung in diesem Einzelfall. Die durchaus sensiblen Daten wurden dem Prüfungsausschuß vermittelt, ohne daß sie irgendeine erkennbare rechtliche Bedeutung in der ihn betreffenden Beschwerdeentscheidung entfalteten. Sie waren somit nicht erforderlich, die Übermittlung war unzulässig. Die für beide Beschwerdeverfahren geltende, gleiche bzw. ähnliche Rechtslage und ihre einheitliche Darstellung konnten die Verwendung eines Bescheides in zwei unterschiedlichen Verfahren nicht rechtfertigen. In Zeiten zunehmender Texterstellung durch Textautomaten und PC's dürfte es zudem immer weniger aufwendig sein, Textbausteine in Schreiben unterschiedlichster Funktion und verschiedener Adressaten mehrfach zu verwenden.

12.5
Die Beschwerde nach § 28 Hessisches Datenschutzgesetz und der Dienstweg

Der Schulpersonalrat eines hessischen Gymnasiums wandte sich unmittelbar an mich mit einer Frage, deren Beantwortung durch das zuständige Staatliche Schulamt ihn nicht überzeugt hatte: Müssen persönliche Aufzeichnungen eines Schulleiters über dienstliche Gespräche mit Kollegen als rein private Unterlagen angesehen werden, oder sind sie als amtliche Dokumente zu bewerten? Entgegen der Auffassung des Staatlichen Schulamtes betrachte ich diese Aufzeichnungen als Dokumentation von Daten der Lehrkräfte; denn sie dienen ausschließlich dienstlichen Zwecken des Schulleiters. § 34 HDSG ist also zu beachten.

Der Leiter des genannten Staatlichen Schulamtes beschwerte sich allerdings beim Hessischen Kultusministerium darüber, wie der Schulpersonalrat dazu komme, mich „unter Umgehung aller Dienstwege" und unmittelbar einzuschalten, und wie es möglich sei, daß meine Stellungnahme „seine dienstlichen Feststellungen relativieren" dürfe. Besonders nachdenklich stimmte mich die erste Fragestellung deshalb, weil die Regelung des § 28 Abs. 2 HDSG an Klarheit nichts zu wünschen übrig läßt. Jeder öffentlich Bedienstete kann sich – ohne Einhaltung des Dienstweges – mit Datenschutzproblemen aus seiner Dienststelle unmittelbar an mich wenden. Er braucht also seinen Vorgesetzten vorher nicht darüber zu informieren. Dies gilt selbst dann, wenn das Datenschutzproblem ihn nicht persönlich betrifft. Die zahlreichen Anfragen aus hessischen Behörden belegen auch, daß die Regelung sich eines recht großen Bekanntheitsgrades erfreut und erfolgreich praktiziert wird. Zu erwähnen bleibt natürlich, daß nach § 28 Abs. 2 Satz 2 HDSG der Beschäftigte seinen Vorgesetzten über die Anfrage ggf. unterrichten muß, soweit der Vorgesetzte dies anordnet. Nicht verlangt werden kann jedoch, daß die Unterrichtung des Vorgesetzten vor der Anfrage erfolgen soll oder daß sie gar sein Einverständnis voraussetze.

Soweit der genannte Leiter des Staatlichen Schulamtes sein Befremden darüber kundtat, daß meine Stellungnahme seinen Äußerungen ausdrücklich widersprach, läßt dies auf ein falsches Verständnis der Aufgaben und der Stellung meiner Behörde schließen. Es bedarf keiner weiteren Ausführung, daß meine Stellungnahmen zu datenschutzrechtlichen Anfragen zwar auf Rechtsauffassungen betroffener Behörden eingehen sollen, in der Sache jedoch unabhängig und neutral erstellt werden müssen.

12.6
Weitergabe von Abiturientennamen an die Presse

Fehlende Sensibilität, Unkenntnis, alte Verwaltungsgewohnheiten, Überforderung durch Fluten von Reglements, was auch immer es sein mag: Der datenschutzrechtliche Lernprozeß der Schulverwaltung ist oft sehr träge. Ein banal wirkendes Beispiel:

Bereits 1990 erhielt ich Kenntnis davon, daß eine Darmstädter Schule die Namen der Abiturienten der örtlichen Presse mitgeteilt hatte, ohne die Einwilligung der Betroffenen dazu einzuholen. Nach § 16 Abs. 1 HDSG ist eine solche Übermittlung nur zulässig, wenn der Empfänger ein berechtigtes Interesse an den Daten glaubhaft gemacht hat und keine Anhaltspunkte dafür bestehen, daß schutzwürdige Belange des Betroffenen beeinträchtigt werden können. Letzteres ist bei Abiturienten nicht ausnahmslos anzunehmen, so daß jedenfalls eine Einwilligung i.S.d. § 7

HDSG erforderlich ist. Auf diese Rechtslage wies ich den betroffenen Schulleiter hin und bat auch das Hessische Kultusministerium, alle Schulen entsprechend zu informieren. Bereits ein durch Zeitablauf erledigter Erlaß vom 10. Oktober 1977 hatte in diesem Punkt eine ähnliche klare Aussage getroffen.

Mit Erlaß vom 2. Oktober 1990 an die Hessischen Regierungspräsidien wies das Ministerium wunschgemäß nochmals auf die Rechtslage hin. 1992 übersandte man mir erneut Darmstädter Presseberichte, welche die Namen aller Abiturienten verschiedener Darmstädter Schulen wiedergaben. Anfragen bei den Schulen ergaben, daß ein Teil von ihnen die Abiturienten vorher nicht um Einwilligung gebeten hatte. Ein Schulleiter äußerte sogar, dies interessiere ihn nicht. Ich gehe davon aus, daß solch krasse Einstellungen im Laufe der Zeit verschwinden werden. Ihre Äußerung zeigt jedoch die Notwendigkeit, wesentliche Eckpunkte schulischen Datenschutzrechts aus der Flut schulrechtlicher Richtlinien und Einzelerlasse herauszuheben und der Schulpraxis über Gesetze und Rechtsverordnungen näher zu bringen. Das ab 1. August 1993 geltende Schulgesetz enthält dazu die notwendigen Rahmenbedingungen (§ 83 ff.). Die Anlage 6 der vor der Veröffentlichung stehenden Rechtsverordnung zum Datenschutz in Schulen bringt auch für den vorliegenden Fall eine klare Vorgabe: Grundsätzlich dürfen die Daten der Schüler an Dritte nur mit Einwilligung übermittelt werden. Dies gilt natürlich auch für Abiturienten.

12.7
Die Umfrage an Europaschulen

Demoskopische Untersuchungen und Studien über Einstellungen ausgewählter Bevölkerungsgruppen zu aktuellen politischen Themen sind zweifellos sinnvoll, um der Politik und der Verwaltung eine Orientierung in planerischen Entscheidungen zu vermitteln. Gerade das Thema „Europa" hat im Wege der Öffnung des Europäischen Binnenmarktes Anfang des Jahres 1993 an Bedeutung zugenommen und beschäftigt auch Schulen.

So plante das Hessische Kultusministerium in Zusammenarbeit mit der Bundeszentrale für politische Bildung eine Umfrage zum „Bild eines vereinten Europa" und zur „Schule der Zukunft" an den fünf hessischen Europaschulen. Zu befragen waren bestimmte Schülerjahrgänge und die Lehrkräfte. Allerdings wurde mit der Entwicklung des mehrseitigen Fragebogens, der Abwicklung der Befragung selbst und der Auswertung ein privates Forschungsinstitut beauftragt. Dieses verteilte die Fragebögen im Frühjahr 1993 an den Schulen und wies in einem Vorblatt auf den Ablauf der Umfrage hin. Die ausgefüllten und in verschlossenen Umschlägen befindlichen Fragebögen sandten die Schulsekretariate dem Institut zur Auswertung zu. Erst nach Abwicklung der Umfrage bat mich der Hauptpersonalrat der Lehrer und Lehrerinnen beim Ministerium, dem Verdacht datenschutzrechtlicher Verstöße nachzugehen. Meine Nachforschungen deckten im Ablauf der Umfrage einige Schwachpunkte auf. Der Aufwand des darauf bezogenen internen Streits stand in keinem angemessenen Verhältnis zum Aufwand, den gesetzlichen Anforderungen an solche Umfragen Folge zu leisten.

12.7.1
Bestimmbarkeit der befragten Lehrkräfte

Das Forschungsinstitut und das Ministerium gingen davon aus, die Umfrage erfolge „anonym", d.h. eine Bestimmbarkeit der befragten Lehrkräfte bei Auswertung der Fragebögen sei zu keinem Zeitpunkt gegeben gewesen. Diesem Standpunkt liegt ein falsches Verständnis des Begriffes „bestimmbare natürliche Person" (§ 2 Abs. 1 HDSG) zugrunde. Zwar sah der Fragebogen als Hilfsmerkmale nur vor: Name der Schule, grobe Altersgruppe, Geschlecht, Nationalität und drei Gruppen von Unterrichtsfächern. Die Kenntnis weiterer schulischer Personaldaten der Lehrkräfte hätte es jedoch mühelos ermöglicht, einen Teil von ihnen zu individualisieren, denn hier kommt es nicht darauf an, wer dieses Zusatzwissen hat. Das Problem hätte allerdings leicht entschärft werden können, wenn z. B. die Angabe der Schule entfallen wäre. Die spätere Auswertung erfolgte auch nicht mehr schulbezogen; insoweit vollzog sich – wenn auch erst später – die sonst gesetzlich vorgesehene, frühzeitige Anonymisierung (§§ 33 Abs. 2 HDSG, 40 Abs. 2 Bundesdatenschutzgesetz).

12.7.2
Die Aufklärung nach § 7 Abs. 7 Hessisches Datenschutzgesetz

Ein leicht vermeidbarer Streit entstand weiter bei der Frage, ob die befragten Lehrkräfte umfassend i.S.d. § 7 Abs. 2 HDSG über die Bedeutung der mit der Abgabe des Fragebogens verbundenen Einwilligungserklärung und vor allem über die Freiwilligkeit des Mitwirkens aufgeklärt worden waren, soweit die genannte Vorschrift hier Anwendung findet. Ohne diese Aufklärung ist die Einwilligungserklärung rechtsunwirksam (ab 1. August 1993 gilt § 84 Abs. 2 S. 5 Schulgesetz (SchulG)). Ein schriftlicher Hinweis auf die Freiwilligkeit im Vorblatt fehlte gänzlich. Vorgetragen wurde, daß Mitarbeiter des Instituts beim Verteilen der Fragebögen mündlich auf die Freiwilligkeit verwiesen hätten. Zwar hatte auch das Ministerium die betroffenen Schulleiter gebeten, alle Lehrkräfte unter anderem über die Freiwilligkeit mündlich zu unterrichten. Aufwendige spätere Befragungen hatten ergeben, daß teils der Personalrat, teils die Dienstversammlung oder die Gesamtkonferenz entsprechend informiert worden waren. Dies konnte jedoch nur die jeweils anwesenden Lehrkräfte erreichen. Die Information des Personalrats allein kann nicht ausreichen, da die Aufklärung sich nur an den Betroffenen höchst persönlich richten kann.

Der Ärger und der Verwaltungsaufwand in diesem Punkte wären allerdings allen erspart geblieben, wenn das Vorblatt des Fragebogens den schlichten Satz enthalten hätte: „Wir weisen ausdrücklich darauf hin, daß die erbetene Beantwortung der Fragen vollkommen freiwillig erfolgt." Die Moral aus der Geschichte: Die Forschungseinrichtung

sollte sich der jederzeit entstehenden Beweisnot einer ausreichenden Aufklärung immer mit der Schriftform entziehen, selbst wenn diese nicht zwingend vorgeschrieben ist. § 7 Abs. 2 S. 2 HDSG spricht nur von „in geeigneter Weise". Dies gilt um so mehr, als eine Umfrage sensiblere Daten erfragen kann.

12.7.3
Geltung des § 33 Abs. 1 S. 3 Hessisches Datenschutzgesetz

Streit entzündete sich auch bei der Frage, ob für das Forschungsvorhaben eine ministerielle Genehmigung nach § 33 Abs. 1 S. 3 HDSG notwendig war. Diese Vorschrift war jedoch u.a. deshalb nicht anwendbar, weil die Lehrkräfte ihre Daten im Rahmen einer Einwilligung offenbarten, während § 33 Abs. 1 HDSG immer die Offenbarung ohne Einwilligung vorsieht. Ab 1. August 1993 gilt § 84 Abs. 1 SchulG, der eine Genehmigung des Ministeriums bei wissenschaftlichen Forschungsvorhaben in Schulen immer erfordert. Der Vorschrift ist der ministerielle Erlaß über „Wissenschaftliche Untersuchungen im Schulbereich" vom 29. September 1987 (ABl. S. 765/87) anzupassen. Klarzustellen ist dabei, daß der Genehmigungsvorbehalt unabhängig davon gilt, welche private oder öffentliche Stelle Auftraggeber des Forschungsvorhabens ist und welche Stelle das Vorhaben durchführt. Dies gilt selbst dann, wenn ein Ministerium ein Forschungsvorhaben durch ein privates Institut eigenständig durchführen läßt.

13. Hochschulen und Forschung

13.1
Inhalt des amtsärztlichen Attestes bei Prüfungsunfähigkeit

Eine hessische Fachhochschule bat mich um Stellungnahme zu einer Frage, die keinen Einzelfall betraf, sondern für alle Hochschulprüfungsverfahren und ähnliche Prüfungssituationen von Bedeutung ist:
Muß das vom Prüfling, der sich auf eine krankheitsbedingte Prüfungsunfähigkeit beruft, meist geforderte amtsärztliche Attest auch detailliert Auskunft über die Art der Erkrankung geben?

Die Suche nach einschlägigen Regelungen in Prüfungsordnungen hessischer Hochschulen oder in hessischen Gesetzen mündete in der Feststellung: Die meisten Vorschriften legen zwar fest, ob zur Feststellung der Prüfungsunfähigkeit lediglich ein privatärztliches oder ein amtsärztliches Attest gefordert werden kann. Über seinen Inhalt fehlen aber Aussagen. Lediglich § 17 Abs. 7 Juristenausbildungsgesetz (JAG) fordert ausdrücklich: „Eine Erkrankung ist unverzüglich anzuzeigen und durch Vorlage eines amtsärztlichen Zeugnisses über Art und voraussichtliche Dauer der Erkrankung nachzuweisen." Interessanterweise hat das Hessische Sozialministerium in einem Erlaß vom 7. Juli 1988 (Az.: III/III A3 18a 04.11) die Notwendigkeit der Dokumentation der Krankheit unterstrichen. Bekannt wurde mir jedoch, daß seitens des Justizprüfungsamtes in verschiedenen Fällen der Verzicht des Amtsarztes auf die Wiedergabe der Diagnose im Attest widerspruchslos hingenommen wurde.

Ich habe der Fachhochschule mitgeteilt, daß ich die Rechtspflicht des Prüflings, für die Feststellung der Prüfungsunfähigkeit durch das Prüfungsgremium seine Krankheit durch das vorzulegende amtsärztliche Attest zu offenbaren, für unzulässig halte.

Ausschlaggebend waren dabei folgende Überlegungen: Sicherlich kommt als eine Krankheit, welche die Prüfungsfähigkeit ausschließt, nur eine gesundheitliche Beeinträchtigung in Betracht, die im Einzelfall konkrete, erhebliche und prüfungsrelevante, d.h. objektivierte leistungsmindernde Beschwerden verursacht oder sie mit hinreichender Sicherheit erwarten läßt. Es muß also eine außergewöhnliche und deshalb den Aussagewert der Prüfung verfälschende Beeinträchtigung des Leistungsvermögens gegeben sein. Auch mag es rechtlich im Ergebnis unproblematisch sein, regelmäßig das Attest eines Amtsarztes statt eines Privatarztes zu verlangen.

13.1.1
Die Selbständigkeit des Amtsarztes

Die Pflicht zur Offenbarung der Krankheit greift jedoch unzulässig in das Recht auf informationelle Selbstbestimmung ein, unabhängig davon, ob eine ausreichende gesetzliche Grundlage dazu überhaupt vorliegt oder – wie häufig der Fall – fehlt. Denn zum einen fehlen dem Prüfungsgremium regelmäßig die medizinischen Fachkenntnisse, um erhobene medizinische Daten daraufhin zu bewerten, ob ein ausreichendes Krankheitsbild vorliegt. Dem Amtsarzt kann es in Kenntnis der rechtlichen Tragweite des Begriffs der Prüfungsunfähigkeit deshalb uneingeschränkt überlassen werden, seine Anamnese daraufhin abschließend und verläßlich zu bewerten. Langjährige, gefestigte Rechtsprechung und einschlägige Erlasse vermitteln dem Amtsarzt problemlos den entscheidenden Inhalt des Begriffs der Prüfungsunfähigkeit. Die unabhängige gutachterliche Bewertung medizinischer Daten auf der Grundlage unbestimmter Rechtsbegriffe ist dem Amtsarzt auch nicht fremd. Er muß in zahlreichen ähnlichen Zusammenhängen verläßliche Aussagen treffen, die teilweise erhebliche Folgen haben (z. B. Schwerbehinderung, Dienstunfähigkeit usw.). Ein Blick auf neuere Regelungen in ähnlichen Zusammenhängen zeigt auch, daß dieser durch das Arztgeheimnis geschützte, besonders sensible Lebensbereich des Bürgers informativ abgeschottet werden kann, ohne daß – etwa im Dienstrecht dem Arbeitgeber oder im Schulbereich der Schulaufsichtsbehörde – unmittelbare Nachteile entstehen. So erhält der Dienstherr bei amtsärztlichen Gutachten lediglich das dienstrechtlich relevante Ergebnis der Untersuchung, nicht jedoch den Befund selbst (§ 18a der Zweiten Hessischen Durchführungsverordnung zum Gesetz über die Vereinheitlichung des Gesundheitswesens). § 83 Abs. 4 des seit 1. August 1993 geltenden Hessischen Schulgesetzes beschränkt

die Mitteilungen des schulärztlichen und schulpsychologischen Dienstes an die Schule auf das Ergebnis der Pflichtuntersuchung.

13.1.2
Die Anpassung des § 17 Abs. 7 Juristenausbildungsgesetz

Mit gleicher Begründung hatte ich den Rechtsausschuß des Hessischen Landtags im Rahmen einer Anhörung zur anstehenden Änderung des Juristenausbildungsgesetzes gebeten, in dem unverändert gebliebenen Text des § 17 Abs. 7 JAG den Hinweis auf die „Art der Erkrankung" zu streichen.

Der Hessische Landtag hat bei der im Dezember 1993 beschlossenen Änderung des Juristenausbildungsgesetzes diesem Wunsch Rechnung getragen. Konsequenterweise muß auch der o.g. Erlaß des Hessischen Sozialministeriums entsprechend geändert werden.

13.2
Forschung und Datenschutz

Regelmäßig erreichen mich Anfragen zu wissenschaftlichen Forschungsvorhaben, die sich im Planungsstadium befinden. Diese Anfragen, aber auch ministerielle Mitteilungen über Genehmigungen nach § 33 Abs. 1 Satz 3 HDSG vermitteln immer wieder den Eindruck, daß sowohl der Überblick über die zahlreichen einschlägigen formellen und materiellen Datenschutzanforderungen an solche Vorhaben als auch die Umsetzung der Bedingungen in einzelnen Vorhaben teilweise erhebliche Probleme bereiten. Im Mittelpunkt steht dabei neben ergänzenden bereichsspezifischen Bestimmungen (z. B. § 84 Schulgesetz) die Anwendung des § 33 HDSG, der die Datenverarbeitung für wissenschaftliche Zwecke regelt. Seine genaue Prüfung wirft die Frage auf, ob eine dem Hessischen Datenschutzgesetz unterliegende datenverarbeitende Stelle, etwa eine Behörde, einer Forschungseinrichtung, sei sie öffentlich oder privat, überhaupt personenbezogene Daten übermittelt.

Dies ist beispielsweise nicht der Fall, wenn die Forschungseinrichtung öffentlich Bedienstete zu rein persönlichen Einschätzungen befragt und der Dienstherr dazu lediglich Räume und Arbeitszeit zur Verfügung stellt, wie etwa bei Umfragen in Schulen während des Schulbetriebes. Ist eine Veröffentlichung des Forschungsergebnisses beabsichtigt, die auch personenbezogene Daten erfaßt, hat dieser Umstand zweifellos eine ganz erhebliche Bedeutung für die Frage, ob schutzwürdige Belange i.S.d. § 33 Abs. 1 S. 2 HDSG des Betroffenen beeinträchtigt werden. Wann tritt der frühestmögliche Zeitpunkt ein, in dem die Hilfsmerkmale von den übrigen erhobenen Daten getrennt werden müssen (§ 33 Abs. 2 HDSG)? Ist eine Behörde an bestimmten Forschungsergebnissen interessiert, überläßt sie aber die Durchführung des Forschungsvorhabens weitgehend privaten Forschungsinstituten, dann stellt sich die Frage nach der Anwendung des § 33 Abs. 5 HDSG. Die Vorschrift ist sicher dann anzuwenden, wenn die Behörde an der forschungsbezogenen Verarbeitung der personenbezogenen Daten direkt beteiligt ist und etwa nur Hilfstätigkeiten an einen Auftragnehmer vergibt. In diesem Falle ist § 4 HDSG zu beachten.

Meine frühzeitige Beteiligung an datenschutzrechtlichen Prüfungen von Forschungskonzepten begrüße ich. Sie hat sich auch bewährt, da Mängel und damit verbundene Folgeprobleme schon in der Planungsphase ausgeschaltet werden können. Dabei hat sich oftmals gezeigt, daß Lösungswege für bestimmte Verfahrensschritte, die sich bei vielen Forschungsvorhaben wiederholen, als „Musterlösung" übernommen und empfohlen werden können. Dies betrifft etwa die Frage, ob nicht das Versenden von Fragebögen an ausgewählte Personengruppen einer bestimmten Institution überlassen werden kann, während Empfang und Auswertung der gänzlich anonym gestalteten Fragenbögen in der Hand einer anderen Einrichtung liegen, ohne den Aufwand damit wesentlich zu erhöhen. Die hier geschilderten Erfahrungen haben mich veranlaßt, die inhaltlichen und formellen Zusammenhänge der einzelnen datenschutzrechtlichen Bestimmungen für Forschungsvorhaben in einem Merkblatt zusammenzustellen und auf typische Fragestellungen auch entsprechende Hinweise zu geben. Das Merkblatt soll die Forschungseinrichtung in die Lage versetzen, schon frühzeitig eine datenschutzgerechte Ablaufplanung zu entwickeln.

Dies ersetzt natürlich nicht die ggf. notwendige ministerielle Genehmigung nach § 33 Abs. 1 Satz 2 HDSG, die mir – was leider immer wieder in Vergessenheit gerät – mitzuteilen ist.

13.3
Teilnahmebescheinigungen für Lehrveranstaltungen an Hochschulen

Zahlreiche datenschutzrechtliche Fragestellungen an Hochschulen entwickeln sich nicht nur im Bereich ihrer Zentralverwaltungen, die in großem Umfang die verschiedensten Daten der Studierenden und Hochschulmitarbeiter, überwiegend automatisiert, verarbeiten. Der Zwang, sich in Massenverfahren für einfach gelagerte Schriftstücke der automatisierten Textverarbeitung zu bedienen, nimmt stetig zu.

So entstand für den juristischen Fachbereich einer Hochschule die Frage, unter welchen datenschutzrechtlichen Rahmenbedingungen die automatisierte Erstellung von Teilnahmebescheinigungen für Lehrveranstaltungen zulässig ist. In der rechtlichen Beurteilung ist dabei von Bedeutung, daß der einzusetzende PC nicht nur als komfortabler Schreibautomat benutzt wird, sondern auch die in Frage kommenden studentischen Daten über eine gewisse Zeit speichern soll. Die Erörterung mit der betroffenen Fachbereichsleitung ergab abschließend folgende Verarbeitungskonditionen:

Die verarbeiteten Daten werden beschränkt auf den Zweck der Bescheinigung, einen Nachweis über die Teilnahme an einer Lehrveranstaltung zu erhalten, nämlich auf Namen, Vornamen, Anschrift, Semester, Bezeichnung der Lehrveranstaltung und ggf. Note. Des weiteren dürfen die Daten nicht an Dritte weitergegeben werden. Endgültig gelöscht werden sie jeweils nach Beendigung des Semesters bzw. des Abschlusses der Veranstaltung. Vor der Löschung werden die Daten in Listen ausgedruckt, die in verschlossenen Schränken der betroffenen Lehrkraft sicher aufbewahrt werden. Zugriff haben nur bestimmte Personen. Der Fachbereich bereitet für alle betroffenen Professuren unter Mitwirkung des internen Datenschutzbeauftragten die notwendige Registermeldung vor, die mir über das zuständige Wissenschaftsministerium zuzuleiten ist (§ 26 Abs. 1 HDSG). Die Studierenden erhalten bereits bei ihrer Anmeldung zu einer Lehrveranstaltung einen Hinweis nach § 18 Abs. 2 HDSG auf die automatisierte Verarbeitung der genannten Daten. Damit ist den Bestimmungen des Hessischen Datenschutzgesetzes ausreichend Rechnung getragen.

14. Kommunen

14.1
INTEBS/PARLIS – Parlamentsinformationsystem

Bereits in meinem 19. Tätigkeitsbericht (Ziff. 11) hatte ich über die Entwicklung von sog. Ratsinformationssystemen berichtet und entsprechende Verfahren aus Kassel und Wiesbaden beschrieben.

In Frankfurt wird jetzt etwas Vergleichbares installiert. Bei diesem Verfahren handelt es sich um ein Parlamentsinformationssystem, das es verschiedenen Benutzergruppen ermöglichen soll, möglichst leicht Informationen aus dem Geschäftsbereich der Stadtverordnetenversammlung sowie der Ortsbeiräte zu erlangen. Im Unterschied zu den beiden oben angesprochenen Verfahren handelt es sich hier allerdings um ein Verfahren, das ausschließlich Materialien enthält, die aus den Gremien der kommunalen Vertretungskörperschaften stammen und nicht aus der Verwaltung bzw. aus dem Magistrat. Damit entfallen einige Rechtsprobleme im Zusammenhang mit Zugriffsrechten nach der Hessischen Gemeindeordnung (HGO), die im 19. Tätigkeitsbericht (Ziff. 11.2) angesprochen wurden.

Hinterlegt werden sollen Dokumente der Stadtverordnetenversammlung, der Ausschüsse und der Ortsbeiräte; dabei handelt es sich um Tagesordnungen, Niederschriften, Fragestunden, Wortprotokolle. Des weiteren werden erfaßt Vorlagen, Beschlußausfertigungen, Rechtsgrundlagen (z. B. Hessische Gemeindeordnung), Terminübersichten, Mitgliederlisten (z. B. Ausschüsse/Stadtverordnetenversammlung) sowie allgemeine Informationen, wie etwa Auszüge aus dem Handbuch der Stadtverordnetenversammlung oder Wahlergebnisse.

Das Verfahren INTEBS (Informations- und Textverarbeitungssystem für das Büro der Stadtverordnetenversammlung) unterstützt den Sitzungsdienst der Stadtverordnetenversammlung, der Ausschüsse, der Ortsbeiräte und sonstiger Gremien; datenschutzrechtliche Probleme ergeben sich insoweit nicht. Das Verfahren PARLIS (Parlamentsinformationssystem) ist als Auskunftssystem für die Öffentlichkeit, für die Mandatsträger und für Mitarbeiter des Büros der Stadtverordnetenversammlung gedacht. Beide Verfahren stützen sich auf dieselbe Datenbasis.

Das Büro der Stadtverordnetenversammlung und das Referat Datenschutz der Stadt Frankfurt haben meine Dienststelle hinsichtlich der Berücksichtigung datenschutzrechtlicher Fragen im Zusammenhang mit den Nutzungsmöglichkeiten des Auskunftssystem „PARLIS" durch die verschiedenen Benutzergruppen intensiv beteiligt. Gegen den jetzt für die Stadtverordnetenversammlung formulierten Beschlußvorschlag zum Einsatz des Parlamentsinformationssystem PARLIS habe ich daher keinen datenschutzrechtlichen Bedenken.

Wesentlich war vor allem die Frage, welche der im System eingestellten Unterlagen welchen Berechtigungsgruppen unter welchen Bedingungen zur Verfügung gestellt werden dürfen. Hier ist insgesamt zwischen vier Gruppen zu unterscheiden:

- Öffentlichkeit
- Mandatsträger (Stadtverordnete und Ortsbeiratsmitglieder) und Mitarbeiter der Fraktionsgeschäftsstellen
- Mitarbeiter des Büros der Stadtverordnetenversammlung
- PARLIS-Administration

Die Öffentlichkeit soll in Zukunft an öffentlich aufgestellten Terminals die Möglichkeit erhalten, Informationen aus dem Bereich der Stadtverordnetenversammlung abzurufen, die ihr auch bisher in Papierform zur Verfügung standen. Beispielhaft können hier die Tagesordnungen für die Stadtverordnetenversammlung und die Ausschußsitzungen sowie Informationen über Mitglieder in den einzelnen Gremien genannt werden, soweit die betroffenen Mandatsträger einer Veröffentlichung zugestimmt haben.

Die Mandatsträger und Fraktionsmitarbeiter sollen darüber hinaus Zugriff auf die Tagesordnungspunkte, Niederschriften und Protokolle erhalten, die nicht öffentlich behandelt worden sind bzw. so zu behandeln sind. Soweit es um die Zugriffsrechte der Ortsbeiratsmitglieder ging, habe ich verdeutlicht, daß diese nur auf personenbezogene Daten zugreifen dürfen, welche den jeweiligen Ortsbezirk betreffen. Ein entsprechender Passus hat Eingang in den Beschlußvorschlag gefunden.

Da die Fraktionsmitarbeiter auch Zugriff auf nichtöffentliche Daten erhalten sollen, sie aber nicht den in der Hessischen Gemeindeordnung geregelten Verschwiegenheitspflichten unterliegen, ist als Anlage zum Beschlußentwurf über den Einsatz des Parlamentsinformationssystems PARLIS eine Verpflichtungserklärung der Fraktionsmitarbeiter aufgenommen worden. Danach haben sich die Mitarbeiter der Fraktionsgeschäftsstellen zu verpflichten, die Bestimmungen des Hessischen Datenschutzgesetzes und die Vorschriften der Hessischen Gemeindeordnung zur Verschwiegenheit (§§ 36a Abs. 1 Satz 6, 24 HGO) einzuhalten.

Die Mitarbeiter des Büros der Stadtverordnetenversammlung haben darüber hinaus Zugriffsrechte auf verwaltungsinterne Daten der Stadtverordnetenversammlung.

Soweit es nicht um Daten geht, die auch der Öffentlichkeit zugänglich sind, müssen sich die Anwender von PARLIS durch Eingabe einer Benutzerkennung und eines Paßworts identifizieren. Die Paßwörter sind regelmäßig zu ändern; dies wird von Seiten des Systems vorgegeben. Alle Daten stehen nur im Lesezugriff und können lediglich ausgedruckt werden, überschrieben werden können sie nicht.

Der Beschluß der Stadtverordnetenversammlung zum Einsatz des Parlamentsinformationssystems PARLIS soll vermutlich zu Beginn dieses Jahres gefaßt werden.

14.2
Bürokommunikation

Der Einsatz moderner Bürokommunikationsmittel in den Stadt- und Gemeindeverwaltungen nimmt in erheblichem Umfang zu. So ist im letzten Jahr auch das Referat Datenschutz der Stadt Frankfurt an mich herangetreten, um gemeinsam mit mir datenschutzrechtliche Rahmenbedingungen für den Einsatz zu erarbeiten.

14.2.1
Umfang des Einsatzes von Bürokommunikationsmitteln

Die Stadt Frankfurt beabsichtigt, alle Ämter der Stadt umfassend mit Datenverarbeitungsanlagen zu versorgen. Ziel ist es, möglichst jeden Arbeitsplatz mit einer „Work-Station" auszustatten. In einigen Ämtern ist dieses Ziel bereits annähernd realisiert. Innerhalb der einzelnen Ämter sind die DV-Arbeitsplätze miteinander vernetzt bzw. sollen miteinander vernetzt werden; als weiteres Ziel ist angestrebt, auch verschiedene Ämter miteinander zu verbinden und damit einen Datenaustausch per Elektronic-Mail zu ermöglichen.

Die eingesetzte Software bietet die folgenden Nutzungsmöglichkeiten:

- Textverarbeitung,
- Elektronische Post,
- Kalenderfunktion,
- Telefonbuchfunktion,
- Notizbuch.

14.2.2
Beabsichtigte Vernetzung verschiedener Ämter

Die beabsichtigte Vernetzung der städtischen Ämter untereinander wirft natürlich erhebliche datenschutzrechtliche Probleme auf. Ich habe wiederholt darauf hingewiesen, daß die Kommunalverwaltung nicht als informationelle Einheit zu betrachten, sondern nach Aufgabenbereichen zu unterscheiden ist. Diese Unterscheidung darf nicht durch die Vernetzung mehrerer Ämter aufgehoben werden. D.h., daß der Einsatz von Elektronic-Mail auch nur in dem Umfang erfolgen darf, in dem eine „normale" Datenübermittlung zulässig wäre. Eine Fortsetzung des Dialogs mit der Stadt Frankfurt ist, was diesen Aspekt betrifft, dringend erforderlich.

14.2.3
Weitere datenschutzrechtliche Anforderungen

Bei der Einführung der DV-Möglichkeiten tritt ein weiteres Problem auf: Die Nutzung der Bürokommunikationsmittel eröffnet die Möglichkeit, eigenständig Dateien anzulegen. Fraglich ist, ob die Mitarbeiter der einzelnen Ämter diese Möglichkeit überhaupt nutzen dürfen und wenn ja, in welchem Umfang, denn sie geht weit über das hinaus, was bisher an Datenverarbeitung betrieben wurde.

Ist das Anlegen von Dateien im Einzelfall zulässig, so ist des weiteren zu klären, ob – bezogen auf jeden einzelnen Arbeitsplatz – eine Verpflichtung zur Registermeldung nach § 26 HDSG sowie zur Benachrichtigung nach § 18 Abs. 2 HDSG besteht. Wir haben in gemeinsamer Arbeit versucht, einen für die Verwaltung praktikablen Lösungsansatz zu entwickeln, der auch den im Hessischen Datenschutzgesetz formulierten datenschutzrechtlichen Anforderungen gerecht wird.

Zugrundezulegen ist zunächst, daß das jeweilige konkrete Amt, in dem die Daten durch die einzelnen Mitarbeiter verarbeitet werden, datenverarbeitende Stelle i.S.d. § 2 Abs. 3 HDSG ist. Das Amt zeichnet demzufolge verantwortlich für die Einhaltung der datenschutzrechtlichen Bestimmungen. Es regelt im einzelnen den Umfang zulässiger Datenverarbeitung. Die jeweilige Dienststellenleitung ist aufgefordert zu beschreiben, was die Mitarbeiter zulässigerweise im Rahmen der angebotenen technischen Ausstattung zu Zwecken einer „Arbeitserleichterung" an Dateien erstellen dürfen. Grundsätzlich dürfen die Mitarbeiter dabei nur diejenigen Daten verarbeiten, die sie im Rahmen ihrer konkreten Aufgabenerfüllung benötigen. Das Amt muß sich demnach der Aufgabe unterziehen, einen Katalog von benötigten Dateien zu erstellen.

Jeder Mitarbeiter einer Dienststelle muß zudem verpflichtet werden, die von ihm gefertigten Dateien der Dienststellenleitung anzuzeigen. Die Dienststelle ist dann verpflichtet, in einer zusammenfassenden Dateibeschreibung dem Hessischen Datenschutzbeauftragten eine Meldung über die in der Dienststelle geführten Dateien zu machen. Des weiteren ist nur die Dienststelle verpflichtet, die Betroffenen nach § 18 Abs. 2 HDSG darüber zu informieren, daß ihre Daten in einer automatisierten Datei gespeichert sind. Ist die Benachrichtigung erfolgt und erhalten die Mitarbeiter einen Extrakt dieser Daten, so entfallen weitere Meldungen, auch wenn mit diesen Daten andere Dateien erstellt werden. Nicht unter eine Meldepflicht – auch gegenüber der Dienststellenleitung – fallen reine Textverarbeitungsprozesse, d.h. ein Schreibmaschineneinsatz ohne die Speicherung von Daten. Das setzt voraus, daß die gespeicherten Texte gelöscht werden, wenn der Schreibvorgang abgeschlossen ist; dies ist in der Regel dann der Fall, wenn der entsprechende Schriftsatz ausgedruckt, unterschrieben und versandt worden ist.

Als Fazit bleibt festzuhalten, daß beim Einsatz von Bürokommunikationsmitteln jeweils die einzelne Dienststellenleitung für die Einhaltung der im HDSG vorgegebenen datenschutzrechtlichen Anforderungen verantwortlich ist. Nur die Dienststellenleitung also muß die in § 18 Abs. 2 und § 26 HDSG normierten Pflichten erfüllen. Auf diese Weise ist ein Weg gefunden worden, den rechtsstaatlichen Zweck der Dateimeldung und der Information der Bürger zu wahren, ohne den Fortschritt der Kommunkationstechnologie zu verhindern.

14.3
Fragwürdige Zusammenarbeit zwischen Fremdenverkehrsamt und Arbeitsamt

Durch eine Beschwerde des Arbeitskreises der Gästeführerinnen und Gästeführer im Landkreis Marburg-Biedenkopf wurde ich auf eine unrechtmäßige Datenübermittlung zwischen einem Fremdenverkehrsamt und einem Arbeitsamt aufmerksam.

Die Mitglieder des genannten Arbeitskreises führten im Auftrag der Stadt Marburg Gästeführungen auf Honorarbasis durch. Als Vermittler war jahrelang das Fremdenverkehrsamt tätig und verfügte daher auch über Namen, Anschrift und Telefonnummer der einzelnen Arbeitskreismitglieder. Im Laufe des Jahres 1993 traf das Fremdenverkehrsamt eine Vereinbarung mit dem Arbeitsamt, welches die Vermittlung der Fremdenführer an Gäste oder Gästegruppen in Zukunft übernehmen sollte. Zu diesem Zweck gab das Fremdenverkehrsamt die genannten Daten der Arbeitskreismitglieder an das Arbeitsamt weiter. Eine Einwilligung der Betroffenen hatte das Fremdenverkehrsamt zuvor nicht eingeholt. Aufgrund meiner Anfrage bei der Stadt Marburg wurde das Verfahren der Vermittlung der Gästeführer unter datenschutzrechtlichen Gesichtspunkten neu überdacht. Die Zusammenarbeit zwischen dem Fremdenverkehrs- und dem Arbeitsamt wurde so geregelt, daß die Daten der Gästeführer in Zukunft nur mit deren Einwilligung übermittelt werden und das Arbeitsamt diese Daten ausschließlich für die Vermittlungstätigkeit von Gästeführungen einsetzt.

14.4
Information des Dienstherrn statt Einleitung eines Ordnungswidrigkeitenverfahrens?

Ein Bürger konnte sich mit einer Stadtverwaltung über die Rechtmäßigkeit eines Verwarnungsgeldes für eine Verkehrsordnungswidrigkeit nicht einigen. Es wurden Briefe ausgetauscht, deren Form und Inhalt ich nicht zu beurteilen habe. Nachdem man zu keiner Einigung kam, wäre der übliche Weg die Einleitung eines Ordnungswidrigkeitenverfahrens durch den Regierungspräsidenten gewesen.

Der Bürger hatte aber das Pech, daß er gleichzeitig Bediensteter beim Landratsamt ist. Kurzerhand wurde der gesamte Vorgang von der Stadt an seinen Dienstherrn übersandt. Die Reaktion erfolgte prompt, der Landrat untersagte seinem Bediensteten ein solches Vorgehen gegen die Stadtverwaltung und kündigte bei einer Fortsetzung des Schriftwechsels dienstrechtliche Schritte an.

Die von dem Bürgermeister der Stadt mir gegenüber geäußerten Rechtfertigungen, wie z. B. die vom Bürger angedrohte Information der Presse bzw. die vom Bürger vorgeschlagene Erarbeitung eines Lösungsansatzes für die Verkehrsprobleme auf politischer Ebene ergaben allerdings keinen rechtmäßigen Grund für die Weitergabe des Schriftverkehrs an den Landrat. Hier wurde eindeutig zum Nachteil eines Bürgers gegen die Bestimmungen des Hessischen Datenschutzgesetzes verstoßen.

14.5
Kindergartengesetz

Am 1. September 1993 ist eine auch datenschutzrechtlich bedeutsame Änderung im Kindergartengesetz (KiGaG) in Kraft getreten. In § 10 KiGaG ist nunmehr geregelt, daß Beiträge oder Gebühren für die Kindergartenbenutzung gestaffelt nach dem Einkommen der Erziehungsberechtigten erhoben werden können.

Die Grundlage für die Möglichkeit einer gesetzlichen Regelung, die Beiträge für die Kindergartenbenutzung nach Einkommensgruppen zu staffeln, bildet § 90 Abs. 1 Nr. 3 Sozialgesetzbuch VIII (SGB VIII – Kinder- und Jugendhilfegesetz). Der Bundesgesetzgeber hat mit dieser Vorschrift ausdrücklich keine Unterscheidung zwischen Beiträgen und Gebühren vorgenommen, so daß die Grundsätze des Kommunalen Abgabengesetzes, das von einer solchen Unterscheidung ausgeht, hier nicht herangezogen werden können. Die nun geltende Fassung des § 10 des KiGaG setzt diese Regelung um.

Bereits im Vorfeld hatte eine Kommune bei mir angefragt, in welcher Form die Einkommensnachweise zu erbringen sind, denn dies ist weder im SGB VIII noch im Hess.KiGaG geregelt.

Zur Klärung dieser Frage habe ich mit Vertretern des Hessischen Ministeriums für Jugend, Familie und Gesundheit ein Gespräch geführt. Es bestand Einigkeit darüber, daß die Betreiber der Kindergärten von den Eltern bzw. den Erziehungsberechtigten nicht die Vorlage eines Steuerbescheides fordern dürfen. Zwar kann grundsätzlich ein Einkommensnachweis verlangt werden, wenn die Beiträge nach Einkommenshöhe gestaffelt erhoben werden sollen. Einem Einkommensteuerbescheid kann jedoch eine Vielzahl von weiteren Informationen aus dem persönlichen Lebensbereich der Erziehungsberechtigten entnommen werden, die für die Bemessung des Kindergartenbeitrages völlig ohne Belang sind. Es darf deshalb den Nachweispflichtigen überlassen bleiben, ob sie den Steuerbescheid teilweise geschwärzt vorlegen oder den Einkommensnachweis in anderer Form führen.

14.6
Datenschutz im Planfeststellungsverfahren

In einem Beschluß aus dem Jahre 1990 hat sich das Bundesverfassungsgericht mit dem Thema Datenschutz im Planfeststellungsverfahren auseinandergesetzt (CR 1990, 798).

Das Bundesverfassungsgericht führt in diesem Beschluß aus, daß Daten, die ein Einwendungsführer der Planfeststellungsbehörde preisgibt, um ihr eine sachgerechte Beurteilung der geltend gemachten Einwendungen zu ermöglichen, einer besonderen Zweckbindung unterlägen. Diese Zweckbindung werde durch eine öffentliche Bekanntmachung der nicht anonymisierten Daten unterlaufen und im Ergebnis aufgelöst.

Das Gericht sieht in der Veröffentlichung der Daten der Einwendungsführer eine Datenübermittlung auf Vorrat, da weder vorhersehbar noch bestimmbar sei, wer von diesen Daten Kenntnis erlangen werde und wie diese Daten verwendet werden könnten. Dieser Beschluß wendet damit konsequent die Grundsätze des Volkszählungsurteils zum Recht auf informationelle Selbstbestimmung auch auf das Planfeststellungsverfahren an.

Meine Nachfrage bei einigen hessischen Kommunen hat ergeben, daß vielfach Einwendungen, die im Planfeststellungsverfahren vorgetragen werden, nichtanonymisiert in öffentlichen Sitzungen der Gemeindevertretungen diskutiert werden. Dieses Vorgehen widerspricht den erwähnten, vom BVerfG aufgestellten Grundsätzen. Soweit Daten über Einwendungsführer in Planfeststellungsbeschlüssen in nichtanonymisierter Form erscheinen bzw. ihre Einwendungen in öffentlicher Sitzung personenbezogen diskutiert werden, ist dieses Verfahren unter Beachtung der Rechtsprechung des Bundesverfassungsgerichts zu ändern.

15. Meldewesen

15.1
Gesetz zur Änderung des Hessischen Meldegesetzes

15.1.1
Ziel des Gesetzentwurfs

Bereits zu Beginn des Jahres 1992 hatte die Landesregierung einen Entwurf zur Änderung des Hessischen Meldegesetzes vorgelegt. In Kraft getreten ist das geänderte Meldegesetz am 28. Juli 1993.

Die hessischen Meldebehörden verfügen entweder über eine eigene ADV oder sind einem der Kommunalen Gebietsrechenzentren angeschlossen.

Erklärtes Ziel des Gesetzentwurfs war vor allem die rechtliche Absicherung eines landeseinheitlichen ADV-Verfahrens im Einwohnerwesen. Hauptsächliches Anliegen war, je Einwohner nur einen Datensatz für alle beteiligten Meldebehörden zu speichern. Auf diesen Datensatz sollten alle beteiligten Meldebehörden zugreifen und ihn auch verändern können. Daneben sollten aber noch zahlreiche Vorschriften des Gesetzes geändert werden, die teilweise datenschutzrechtliche Verbesserungen enthielten, teilweise allerdings auch Verschlechterungen.

Der Innenausschuß des Hessischen Landtags hatte mir die Möglichkeit gegeben, zu dem Gesetzentwurf Stellung zu nehmen (vgl. Ausschußvorlage INA 13/30). Ich hatte die Gelegenheit genutzt, über die Vorschläge der Landesregierung hinaus selbst einige Änderungen anzuregen. Das jetzt in Kraft getretene Gesetz berücksichtigt die von mir eingebrachten Änderungswünsche zum Teil.

15.1.2
Positive Aspekte der Gesetzgebung

Zentrale Vorschrift für das oben erläuterte Gesetzgebungsziel ist § 37a Hessisches Meldegesetz (HMG). Hier ist nunmehr ausdrücklich geregelt, daß bei einem Kommunalen Gebietsrechenzentrum die Daten eines Bürgers nur einmal in einem gemeinsamen Datensatz geführt werden. Schreibt eine Meldebehörde die Daten eines Einwohners fort, steht die aktualisierte Fassung auch anderen Meldebehörden im Rahmen ihrer Zuständigkeit zur Verfügung.

Wechselt z. B. ein Einwohner innerhalb des Zuständigkeitsbereichs eines Rechenzentrums den Wohnsitz, so werden die Daten der Wegzugsgemeinde auf Veranlassung der Zuzugsgemeinde geändert. Betrifft ein Datum mehrere Familienangehörige (z. B. Familienstand), werden auch deren Daten fortgeschrieben. Nimmt die Meldebehörde der Nebenwohnung Datensatzänderungen vor, so ist gleichzeitig der der Hauptwohnung zur Verfügung stehende Datensatz geändert. Durch differenzierte Zugriffsrechte, Protokoll- und Unterrichtungspflichten wird den Belangen des Datenschutzes Rechnung getragen.

Allerdings war neben der Schaffung eines gemeinsamen Datensatzes beabsichtigt, die §§ 3 Abs. 3, 18 Abs. 1 HMG, welche die (eingeschränkte) Datenerhebung bei Anmeldung einer Nebenwohnung regeln, zu ändern und damit die Unterscheidung des Datensatzes nach Haupt- und Nebenwohnung aufzuheben. Dies wurde damit begründet, daß das bisherige Speicherungsverbot bestimmter Daten durch die für die Nebenwohnung zuständige Meldebehörde zu einem erheblichen Arbeitsaufwand bei den Kommunalen Gebietsrechenzentren, den Meldebehörden und den Einwohnern führe. So müßten z. B. beim Statuswechsel von Wohnungen (Änderung Hauptwohnung in Nebenwohnung) Daten gelöscht oder bei den Einwohnern nacherhoben werden. Auch sei aus rechtssystematischen und praktischen Gründen eine unterschiedliche Behandlung von Gemeinden, die den Kommunalen Gebietsrechenzentren angeschlossen seien, und Gemeinden, die eigene ADV-Verfahren hätten, und ihre Datensätze je nachdem, ob bei ihnen eine Haupt- oder Nebenwohnung gemeldet sei, unterschiedlich ausgestalten müßten, nicht angezeigt.

Dagegen hatte ich eingewandt, daß beide Argumente keine stichhaltige Begründung dafür sein können, nicht erforderliche Daten zu erheben und zu speichern. Gemeinsame Aufgabe aller Meldebehörden ist es, die in ihrem Zuständigkeitsbereich wohnhaften Einwohner zu registrieren, um deren Identität und Wohnung feststellen und nachweisen zu können (§ 1 Abs. 1 HMG). Die Meldebehörde, bei der ein Einwohner seine Hauptwohnung angemeldet hat, hat darüber hinaus eine Reihe weiterer Aufgaben zu erfüllen, beispielsweise die Vorbereitung von Wahlen, die Mitwirkung bei der Ausstellung von Lohnsteuerkarten usw.. Für die Erfüllung dieser Aufgaben benötigt die Meldebehörde des Hauptwohnsitzes Daten, deren Kenntnis für die Meldebehörde, bei der ein Einwohner lediglich eine Nebenwohnung gemeldet hat, nicht erforderlich ist. Dabei kann es sich – zumindest teilweise – um äußerst sensible Daten handeln, wie z. B. die Tatsache, daß ein Einwohner vom Wahlrecht und von der Wählbarkeit ausgeschlossen ist. Der Gesetzgeber hat sich letztlich meiner Argumentation angeschlossen und auf eine Änderung der §§ 3 Abs. 3, 18 Abs. 1 HMG verzichtet.

Weiterhin war beabsichtigt, den öffentlich-rechtlichen Religionsgemeinschaften einen erweiterten Auskunftsanspruch über Familienangehörige ihrer Mitglieder einzuräumen. Die Religionsgemeinschaften hatten in einer schriftlichen Anhörung ausgeführt (vgl. Ausschußvorlage UID/13/8), daß es für die seelsorgerische Arbeit hilfreich sei, auch Informationen über das familiäre Umfeld der Kirchenmitglieder zu erhalten. Aus meiner Sicht ging diese Regelung zu weit. Daß die Kenntnis dieser Daten die Arbeit der Kirchen möglicherweise erleichtern könnte, ist unter dem Gesichtspunkt der Erforderlichkeit der Datenverarbeitung nicht ausreichend. Insoweit ist es bei der alten Regelung geblieben.

Eine im Melderegister eingetragene Auskunftssperre kann im Einzelfall widerrufen werden, wenn ein glaubhaft gemachtes rechtliches Interesse an der Melderegisterauskunft offensichtlich das Interesse des Betroffenen an der Auskunftssperre überwiegt (§ 34 Abs. 6 HMG). Der Gesetzentwurf sah ergänzend dazu vor, daß die Aufhebung der Auskunftssperre auch bei Vorliegen eines „wirtschaftlichen Interesses" einzuräumen sei. Da das Institut „Auskunftssperre" insgesamt in Frage gestellt und ausgehöhlt worden wäre, hat der Gesetzgeber von der Erweiterung der Widerrufsmöglichkeit abgesehen. In diesem Zusammenhang möchte ich darauf hinweisen, daß die Auskunftssperre nicht mehr unbefristet eingetragen wird, sondern mit Ablauf des dritten auf die Eintragung folgenden Kalenderjahres endet und nur auf Antrag verlängert wird (§ 34 Abs. 7 HMG).

Zu begrüßen ist die Einführung des neuen Absatz 7 in § 35 HMG. Danach ist die Meldebehörde künftig verpflichtet, einmal jährlich und zusätzlich zwei Monate vor der Datenübermittlung an Adreßbuchverlage die Einwohner durch einen öffentlichen Hinweis über die Auskunftssperren nach diesem Gesetz zu unterrichten. Schon in der Vergangenheit hatte ich den Meldebehörden empfohlen, so zu verfahren, da vielen Einwohnern die Möglichkeit des Widerspruchsrechts gegen Meldedatenübermittlungen gar nicht bekannt war. Mit der Neuregelung wird den Bürgerinnen und Bürgern die Möglichkeit gegeben, dieses Recht wirksamer auszuüben.

15.1.3
Unberücksichtigte Anregungen

Nach § 35 Abs. 1 HMG darf die Meldebehörde Parteien, anderen Trägern von Wahlvorschlägen und Wählergruppen im Zusammenhang mit Wahlen Auskünfte aus dem Melderegister erteilen, „für deren Zusammensetzung das Lebens-

alter der Betroffenen bestimmend ist". Damit hat der Gesetzgeber m.E. die zulässigen Auswahlkriterien für Gruppenauskünfte zu Wahlzwecken stark eingeschränkt. Er hat ein öffentliches Interesse nur insoweit anerkannt, als die Parteien usw. bestimmte Altersgruppen unter den Wahlberechtigten gezielt ansprechen wollen.

Das Hessische Ministerium des Inneren und für Europaangelegenheiten hat sich in der Vergangenheit jedoch auf den Standpunkt gestellt, der Wortlaut des Gesetzes lasse zwar das Lebensalter als Auswahlkriterium für eine (begrenzte) Datenübermittlung zu. Nach diesen Auswahlkriterien müsse aber nicht vorgegangen werden; grundsätzlich sei auch eine Übermittlung der Daten aller Altersgruppen zulässig. Ich hatte daher vorgeschlagen, Satz 1 des § 35 Abs. 1 in Anlehnung an § 22 des Entwurfs eines ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes (MRRG, BTDrucks. 12/2376) klarstellend wie folgt zu formulieren. „..., soweit für deren Zusammensetzung das Lebensalter der Betroffenen bestimmend ist". Diese Anregung soll nach dem Vorliegen des Melderechtsrahmengesetzes noch einmal zur Diskussion gestellt werden.

Des weiteren hatte ich angeregt, in das Meldegesetz eine Vorschrift einzubringen, die dem Betroffenen, der durch unzulässige Datenverarbeitung geschädigt wurde, nach dem Vorbild des § 20 Hessischen Datenschutzgesetzes einen Schadensersatzanspruch gewährt. Auch dieser Punkt soll nach Erlaß des Melderechtsrahmengesetzes wieder aufgegriffen werden.

Außerdem hätte ich es begrüßt, wenn der Datensatz des § 3 Abs. 1 HMG der im Melderegister zu führenden Daten um die Daten „akademische Grade" und „erwerbstätig/nicht erwerbstätig" reduziert worden wäre. Für die Erfüllung der Aufgaben der Meldebehörde sind diese Daten nicht erforderlich. Der Gesetzgeber sah sich jedoch an die Vorgaben des Melderechtsrahmengesetzes gebunden, auch wenn dies, wie ich ausgeführt habe, nicht zwingend geboten ist. Denn das Melderechtsrahmengesetz besagt lediglich, daß die Meldebehörden einen in § 2 MRRG näher bezeichneten Datensatz speichern dürfen, d.h. sie dürfen über diesen Datensatz hinaus keine weiteren Daten speichern. Es bleibt ihnen jedoch unbenommen, weniger als diesen Maximaldatensatz zu speichern.

§ 31 HMG regelt die Datenübermittlung der Meldebehörde an andere Behörden oder sonstige öffentliche Stellen. Nach § 31 Abs. 7 HMG darf die Meldebehörde innerhalb der Gemeinde, der sie angehört, sämtliche der in § 3 Abs. 1 HMG genannten Daten weitergeben. Die einschränkende Regelung des § 37 Abs. 4 HMG, nach der regelmäßige Datenübermittlungen an andere Behörden oder sonstige öffentliche Stellen nur zulässig sind, soweit dies durch Bundes- oder Landesrecht unter Festlegung des Anlasses und des Zwecks der Übermittlungen, der Datenempfänger und der zu übermittelnden Daten bestimmt ist, gilt insoweit nicht. Daher hatte ich die folgende Ergänzung vorgeschlagen: Im Falle der Einrichtung von Online-Anschlüssen an das Melderegister innerhalb der Gemeinden sollte geregelt werden, welcher Stelle zu welchem Zweck aus welchem Anlaß Zugriff auf Daten eröffnet wird. Dies hätte z. B. in der Form erfolgen können, daß die Gemeinden verpflichtet werden, Zugriffsrechte durch Organisationsverfügung des Gemeindevorstands zu regeln. Der Gesetzgeber sah hierin einen zu weit gehenden Eingriff in das Recht der kommunalen Selbstverwaltung und nahm meinen Vorschlag nicht auf.

15.2
Einzelfälle aus dem Meldewesen

15.2.1
Mietverträge in den Akten des Einwohnermeldeamts

In einer Eingabe an meine Dienststelle wurde der folgende Sachverhalt berichtet:

Eine Bürgerin wollte sich nach ihrem Zuzug in eine hessische Gemeinde ordnungsgemäß anmelden. Als sie beim Einwohnermeldeamt vorsprach, wurde von ihr die Vorlage ihres Mietvertrages verlangt. Als sie erneut beim Einwohnermeldeamt erschien und den Mietvertrag vorlegte, machte sich der Bearbeiter von dem Mietvertrag eine Kopie und nahm sie zu den Akten. Da die Bestätigung des Wohnungsgebers über den Einzug von Mietern bereits seit der Neufassung des Meldegesetzes am 14. Juni 1982 entfallen ist, habe ich die Gemeinde angeschrieben und ihr mitgeteilt, daß eine solche Vorgehensweise von den Vorschriften des Hessischen Meldegesetzes nicht gedeckt ist.

Die Meldebehörde darf Angaben zum Mietverhältnis nicht im Melderegister führen, da der Katalog des § 3 Hessischen Meldegesetzes (HMG) eine abschließende Aufzählung der zulässigerweise im Melderegister zu speichernden Daten enthält. Daten und Angaben zum Mietverhältnis gehören nicht dazu.

Bei der Anmeldung darf die Meldebehörde zwar zur Überprüfung der Angaben des Anmeldenden nach dem Wohnungsgeber fragen. Dies ergibt sich aus § 19 HMG. Außerdem darf die von der Meldebehörde ausgestellte Meldebestätigung gemäß § 18 Abs. 3 Nr. 6 HMG den Namen und die Anschrift des Wohnungsgebers enthalten. Insofern kann auch die Meldebehörde, die eine Durchschrift der amtlichen Meldebestätigung bei ihren Akten behält, dieses Datum in ihren Unterlagen haben. In einzelnen Zweifelsfällen mag auch die Vorlage des Mietvertrages zur Kontrolle der Angaben des Mieters zulässig sein, wobei die Meldebehörde lediglich berechtigt ist, die Angaben zu Name und Anschrift des Wohnungsgebers zu überprüfen.

Die Einbehaltung einer Kopie des Mietvertrages aber ist nach den Vorschriften des Hessischen Meldegesetzes unzulässig. Die Einzelheiten mietvertraglicher Regelungen z. B. über Größe der Wohnung, Mietzins und andere Absprachen sind für die Aufgabenerfüllung der Meldebehörde nicht erforderlich, so daß Informationen darüber auch nicht in ihren Unterlagen sein dürfen.

Bei einer Überprüfung der betroffenen Meldebehörde wurde mir mitgeteilt, daß es in der Gemeinde üblich sei, eine Kopie der ersten Seite des Mietvertrages an die Anmeldung zu heften. Aufgrund der Beschwerde der Bürgerin und meiner Darlegungen zur Rechtslage wird diese Vorgehensweise nicht mehr praktiziert. Bei Durchsicht der neuen Anmeldungen konnte ich feststellen, daß keine Kopien von Mietverträgen mehr an die Anmeldungsbescheinigungen angeheftet worden waren.

15.2.2
Überflüssige Datenerhebung bei getrennt lebenden Ehegatten

Ein Bürger wurde von der Stadt Neu-Isenburg im Rahmen des Vollzugs von Melderecht und Lohnsteuerrecht mit einem Fragebogen angeschrieben und um Ergänzung des zu seiner Person gespeicherten Datensatzes gebeten. Der Betroffene lebte zu diesem Zeitpunkt seit einigen Jahren von seiner Ehefrau getrennt. Neben Angaben zu seiner Person und der Person seiner Ehefrau wurde er gefragt, ob sich das Getrenntleben auf die eheliche Gemeinschaft, den gemeinsamen Haushalt, die Wirtschaftsprüfung oder die gemeinsame Wohnung erstrecke und auf längere Zeit beabsichtigt sei.

Zwar darf die Meldebehörde nach § 3 Abs. 2 Hessisches Meldegesetz aufgrund ihrer Mitwirkung bei der Ausstellung von Lohnsteuerkarten steuerrechtliche Daten, u.a. auch über das dauernde Getrenntleben von Ehegatten, erheben und speichern.

Jedoch ist die Nachfrage, auf welche Bereiche sich das Getrenntleben erstreckt, für die Entscheidung, in welche Lohnsteuerklasse i.S.d. § 38b Einkommensteuergesetz der Betroffene einzureihen ist, nicht erheblich.

Die Stadt Neu-Isenburg hat daher nach einem entsprechenden Hinweis von mir den Vordruck gesetzeskonform gestaltet und das dazugehörige Anschreiben mit einer für den Bürger verständlichen Begründung versehen.

16. Rundfunk: PC-Verfahren Rundfunkgebührenbefreiung

Das Kommunales Gebietsrechenzentrum (KGRZ) Kassel hat in Zusammenarbeit mit dem Sozialamt des Schwalm-Eder-Kreises in Homberg (Efze) ein Verfahren entwickelt, das – installiert auf einem PC – von den Sozialämtern als Verwaltungshilfe bei der Gewährung von Rundfunkgebührenbefreiungen sowie Telefongebührenermäßigungen eingesetzt werden kann. U.a. unterstützt das Verfahren die Erfassung der Antrags- und Änderungsdaten für die Bearbeitung der Befreiungsanträge, führt spezielle Berechnungen bei Personen mit geringem Einkommen aus (§ 1 Abs. 1 Nr. 7 der Verordnung über die Befreiung von der Rundfunkgebührenpflicht (BefrVO) vom 31. August 1992, GVBl. I S. 377) und erstellt alle erforderlichen Schreiben.

Das KGRZ Kassel hatte mich gem. § 29 Abs. 3 Hessisches Datenschutzgesetz über das PC-Verfahren unterrichtet. Sowohl die Verfahrensbeschreibung über die automatisierte Verarbeitung von Sozialdaten als auch die Zielsetzung des Kommunalen Gebietsrechenzentrums, das Programm hessenweit und darüber hinaus auch in anderen Bundesländern zu vertreiben – das funktioniert dann, wenn die sog. „Regelsatztabelle" (für jedes Bundesland gelten in der Sozialhilfe besondere Regelsätze) vor dem Einsatz angepaßt worden ist –, hatten mich veranlaßt, eine intensive datenschutzrechtliche Prüfung vorzunehmen.

16.1
Rechtsgrundlagen für die Datenverarbeitung

Nach § 5 Abs. 2 BefrVO ist der Antrag auf Befreiung von der Rundfunkgebührenpflicht an den zuständigen örtlichen Träger der Sozialhilfe, in dessen Bezirk das Rundfunkgerät zum Empfang bereitgehalten wird, zu richten. Das Sozialamt prüft das Vorliegen der Voraussetzungen, entscheidet im Auftrag des Hessischen Rundfunks über den Antrag und händigt dem Antragsteller den Befreiungsbescheid aus. Der Umfang der erfaßten Merkmale ergibt sich aus der BefrVO bzw. dem Bundessozialhilfegesetz. Nach § 5 Abs. 4 BefrVO hat der Antragsteller die Voraussetzungen für eine Gebührenbefreiung glaubhaft zu machen. Dabei kann es sich beispielsweise um die Vorlage des Schwerbehindertenausweises im Zusammenhang mit einer Sehbehinderung oder Blindheit i.S.v. § 1 Abs. 1 der BefrVO oder Einkommensbescheinigungen im Rahmen einer Antragstellung wegen geringen Einkommens nach § 1 Abs. 1 Nr. 7 BefrVO handeln.

16.2
Zuviel erfragte Merkmale

Zwar ist das Erheben von Daten, die für den eigentlichen Zweck gar nicht benötigt werden durchaus nicht ungewöhnlich, aber datenschutzrechtlich gleichwohl unzulässig. Diese Feststellung mußte ich auch bei dem vom Schwalm-Eder-Kreis verwendeten Formular zur Feststellung des Einkommens machen; und mit dem DV-Programm des KGRZ Kassel wurde ebenfalls mehr erfaßt als notwendig war. So wurde in dem Antragsformular (dessen Daten im übrigen ebenfalls automatisiert erfaßt und verarbeitet werden) nach dem z.Zt. ausgeübten Beruf gefragt. Dieses Merkmal war für die Bearbeitung des Antrages und der Entscheidungsfindung des Sozialamtes ebensowenig erforderlich wie das im DV-Programm enthaltene Datenfeld „alleinerziehend". Entsprechend meiner Forderung verzichtete das KGRZ Kassel auf diese Merkmale. Das vom Sozialamt verwendete Formular veranlaßte mich, mich mit dem

Hessischen Rundfunk in Verbindung zu setzen, um eine inhaltliche Abstimmung und landeseinheitliche Verwendung zu erreichen. Mittlerweile hat die Abteilung Rundfunkgebühren des Hessischen Rundfunks mit meiner Beteiligung ein Formblatt entwickelt, das nunmehr landeseinheitlich in allen hessischen Sozialämtern verwendet wird, die mit der Bearbeitung von Anträgen auf Befreiung von der Rundfunkgebührenpflicht befaßt sind.

16.3
Probleme des Zugriffsschutzes

Das vom KGRZ Kassel entwickelte PC-Verfahren Rundfunkgebührenbefreiung wurde mit dem Anwendungsentwicklungspaket „Open Access" erstellt. Dieses Paket bietet neben vielen anderen Optionen auch die Möglichkeit, eigene Schutzmechanismen in die zu erstellende Anwendung zu integrieren. Das KGRZ hatte sich diese Optionen zunächst zu Nutze gemacht und beispielsweise den Zugriff auf die Dateien des Verfahrens über die Eingabe eines Paßwortes gesteuert. Den Anwendern stand aber nicht nur das entwickelte Verfahren, sondern auch das gesamte Programmpaket „Open Access" zur Verfügung, da sie einige Optionen zwar nicht im Verfahren, aber doch im Rahmen ihrer Aufgabenstellung sinnvoll einsetzen können (z.B. integrierte Textverarbeitung). Mit einer dieser Optionen war es ihnen nun möglich, das vorgenannte Paßwort nicht nur zu ändern, sondern es ganz aufzuheben. Darüber hinaus bietet das Programmpaket weitere Einsatzmöglichkeiten, die über den im Rahmen der Anwendung erforderlichen Bedarf hinausgehen und unzulässige Zugriffe auf den Datenbestand erlauben.

Weitere erhebliche Probleme ergaben sich dadurch, daß die Betriebssystem-Ebene des PC zugänglich war, ohne daß die in diesem Bereich vorgenommenen Aktivitäten Einschränkungen unterworfen waren oder wenigstens durch eine Protokollierung registriert wurden. Insgesamt wurde das Verfahren in der zunächst vorliegenden Konstellation den Forderungen an den Zugriffsschutz, die sich nach § 10 HDSG bei den hier verarbeiteten Sozialdaten stellen, nicht gerecht.

Die Verwaltung des Schwalm-Eder-Kreises hat zwar weitgehend alle organisatorischen Voraussetzungen geschaffen, um eine derartige Anwendung im Rahmen eines PC-Verfahrens betreiben zu können, aber ein Zugriff auf die Sozialdaten muß jenseits der Anwendung weitestgehend ausgeschlossen werden. Dies ist jedoch bei PC-Verfahren insbesondere dann problematisch, wenn sich das Umfeld in Form neuer Benutzer oder zusätzlicher Anwendungen ändert.

16.4
Lösungsansätze

Eine zunächst denkbare Alternative, lediglich eine lauffähige Version des Anwendungsprogrammes auf dem PC zu installieren, ist nicht nur deshalb abzulehnen, weil damit erhebliche Einschränkungen hinsichtlich der Nutzung von Standardprogrammen verbunden wären. Im weiteren müßte jeder denkbare Anwendungsschritt in das Verfahren integriert werden, und jede künftige Änderung der Anwendungskonstellation würde sich nur durch neuerlichen Programmieraufwand abbilden lassen.

Um den Zugriffsschutz in der geschilderten Konstellation zu gewährleisten und möglichen Veränderungen im Umfeld des Verfahrens und des eingesetzten PC Rechnung zu tragen, ist der Einsatz einer Schutzsoftware auf dem PC daher unumgänglich (vgl. schon den 17. Tätigkeitsbericht, Ziff. 12 ff.).

Ich habe daher dem KGRZ Kassel empfohlen, das Verfahren Rundfunkgebührenbefreiung im allgemeinen immer in Verbindung mit einer Schutzsoftware anzubieten und die weitere Verfahrensentwicklung auf die sich daraus ergebenden Möglichkeiten abzustimmen. Das KGRZ hat diese Anregung aufgegriffen und auf den PCs, auf denen das Verfahren RGB-PC zum Einsatz kommt, eine Schutzsoftware installiert.

Künftig wird das Verfahren in einer neueren Version, die den Datenträgeraustausch mit dem Hessischen Rundfunk bzw. der Gebühreneinzugszentrale vorsieht, nur noch in Verbindung mit einer Schutzsoftware angeboten. Das Kommunale Gebietsrechenzentrum wird dabei die integrierte Option des Schutzprodukts nutzen, die Datenträger zu verschlüsseln, um die Daten für den Transportweg zu schützen.

Am Beispiel des Verfahrens Rundfunkgebührenbefreiung wird deutlich, daß es nicht sinnvoll ist, bei der Entwicklung von PC-Anwendungen Schutzfunktionen zu realisieren, die auch durch den Einsatz eines leistungsfähigen und spezialisierten Schutzprodukts gewährleistet werden können. Vielmehr ist es – wie die Entwicklung gezeigt hat – zweckmäßig, das Verfahren auf den Einsatz mit einer geeigneten Schutzsoftware abzustimmen und die damit verbundenen Vorteile einer größeren Flexibilität sowohl für das einzelne Verfahren als auch für das gesamte Nutzungsspektrum eines PC in Anspruch zu nehmen.

17. Sparkassen, Banken

17.1
Prüfung des Schufa-Online-Verfahrens (SCDA) für die hessischen Sparkassen

Im vergangenen Jahr konnte eine bereits 1992 begonnene Prüfung des von der Schufa (Schutzgemeinschaft für allgemeine Kreditsicherung) ihren Vertragspartnern, zu denen auch die hessischen Sparkassen zählen, zur Verfügung gestellten automatisierten Abruf- und Meldeverfahrens SCDA (Schufa Computer Dialog Anwendung) abgeschlossen werden.

17.1.1
Die Schufa-Datenbank

Wer einen Konsumentenkredit aufnehmen möchte, ein Girokonto eröffnen will, eine Kreditkarte beantragt, eine Stereoanlage auf Raten kaufen möchte oder beispielsweise bei einem Versandhandelsunternehmen Waren gegen Rechnung bestellt, kann in der Regel davon ausgehen, daß die Bank, die Kreditkartengesellschaft, das Kaufhaus bzw. das Versandhaus seine Bonität durch eine Anfrage bei der Schufa überprüfen. Die Schufa ist eine Einrichtung der kreditgebenden deutschen Wirtschaft und besteht aus 13 regionalen privatrechtlichen Gesellschaften, deren Gesellschafter Banken, Sparkassen sowie Einzelhandelsunternehmen sind. Sie registriert neben den Angaben zur Person z.B.: Informationen zu Girokonten und Kreditkarten, beantragte und gewährte Kredite, Bürgschaften, Leasingverträge, Versandhauskonten, Scheckrückgabe mangels Deckung, Scheckkartenmißbrauch, Kündigungen von Krediten wegen Rückzahlungsverzug, Lohnpfändungen, Mahnbescheide bei unbestrittener Forderung usw. Die Arbeitsweise beruht auf dem Prinzip der Gegenseitigkeit: Auskünfte erhält nur, wer seinerseits bereit ist, Informationen zu liefern.

17.1.2
Direktzugriff auf die Datenbank

Die Vertragspartner konnten und können die Angaben telefonisch oder per Telefax, Telex oder gewöhnlichem Brief abfragen. Seit ca. zwei Jahren bietet die Schufa den Unternehmen auch die Möglichkeit, direkt, d.h. ohne Kontaktaufnahme mit den Geschäftsstellen, auf die zentrale Schufa-Datenbank zuzugreifen. Dies kann entweder auf der Basis eines Rechner-Rechner-Verbundes oder mit einem Personal-Computer mittels Datex-P geschehen.

Das Online-Verfahren bietet sowohl für die Teilnehmer als auch die Schufa-Vorteile: Es entfallen telefonische Anfragen und das damit verbundene Problem der Identifizierung des Anrufers. Beleggebundene Anfragen werden überflüssig. Anfragen und Auskünfte müssen nicht mehr mit der Post versandt werden. Durch die zeitnahen Neu-, Änderungs- und Ergänzungsmeldungen gewinnt der Datenbestand eine größere Aktualität. Der Kreditsachbearbeiter hat die benötigten Informationen ohne Zeitverzögerung unmittelbar am Arbeitsplatz zur Verfügung.

17.1.3
Anlaß und Verfahren der Prüfung

Da die hessischen Sparkassen ihre Teilnahme an diesem Verfahren von einem positiven Ergebnis einer Überprüfung durch den Hessischen Datenschutzbeauftragten abhängig gemacht hatten, war auch der Schufa an der Prüfung gelegen. Ohne ihre Kooperation hätte ich ohnehin nicht prüfen können, denn als privatrechtliche Einrichtung unterliegt die Schufa nicht meiner Kontrollkompetenz. Weil die Datenverarbeitung im öffentlichen und privaten Bereich (Sparkassen und Schufa) erfolgt, war darüber hinaus zeitweise das Regierungspräsidium Darmstadt, die zuständige Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, eingeschaltet. Außer Gesprächen mit Vertretern der Bundes-Schufa (Bundesverband der Schufa-Gesellschaften), der regionalen Schufa-Gesellschaften Hamburg und Hannover, die u.a. für das Rhein-Main-Gebiet und den Kasseler Raum zuständig sind, Unterredungen mit Vertretern des Sparkassen- und Giroverbandes Hessen-Thüringen und des Rechenzentrums der Hessischen Sparkassenorganisation GmbH fand ein Prüfbesuch bei der Stadtsparkasse Kassel statt, bei dem eine Pilotinstallation der „Schufa Computer Dialog Anwendung" von mir überprüft wurde. Von einem Vertreter der Firma Debis-Systemhaus MGI GmbH, die in ihrem Eschborner Rechenzentrum für die Schufa die Datenverarbeitung durchführt und die gleichfalls nicht meiner Kontrolle unterliegt, habe ich mir das Sicherheitskonzept des Rechenzentrums für das Online-Verfahren schildern lassen und mich im übrigen auf eine Prüfung gestützt, die das Regierungspräsidium dort kurze Zeit vorher vorgenommen hatte.

17.1.4
Datensicherungsmaßnahmen im Eschborner Rechenzentrum der Debis-Systemhaus MGI GmbH

Die Schufa bietet für den direkten Zugriff auf ihre Daten zwei Kommunikationsformen an:

- Terminal-Kopplung, d.h. das Netzwerk des Vertragspartners mit Datensichtgeräten/PC's wird mit dem Schufa-System so gekoppelt, daß ein berechtigtes Terminal arbeitet, als sei es am Schufa-System angeschlossen. Der Rechner des Vertragspartners funktioniert wie eine Steuereinheit, die Daten lediglich weiterleitet. Der Teilnehmer nutzt die im Schufa-Rechenzentrum ablaufende Anwendungssoftware.
- Programmkopplung, d.h. eine Anwendungssoftware des Teilnehmers, die unter einem Transaktionsmonitor abläuft, kommuniziert mit einem Partner-Programm des Schufa-Systems.

Für die hessischen Sparkassen ist die „Terminal-Lösung" vorgesehen. Die Verwaltung der Sicherheitssoftware RACF (Resource Access Control Facility) erfolgt dezentral durch die Schufa. Alle Subsysteme sind mit der Schutzsoftware über Schnittstellen gekoppelt. Beim TP (Teleprocessing)-Monitor CICS (Customer Information Control System der Fa. IBM) gehen die Prüfungen beispielsweise bis auf die Transaktionsebene. Die Schufa-Anwendung ist mit eigener Benutzer- und Zugriffskontrolle ausgestattet. Es werden alle Eingaben, besonders solche, die zu Abfragen führen, protokolliert. Dabei werden Benutzerkennung, ggf. Terminal, Datum, Uhrzeit und die Eingaben gespeichert. Die Protokolle werden ein Jahr aufbewahrt, ihre Auswertung erfolgt auf Anweisung der Schufa. Es gibt außerdem die

Möglichkeit, Online-Abfragen schriftlich bestätigen zu lassen. Insgesamt können die auf Seiten der Schufa getroffenen technischen und organisatorischen Maßnahmen als ausreichend angesehen werden.

17.1.5
Pilotinstallation bei der Stadt- und Kreissparkasse Kassel

Installiert waren dezentral Steuereinheiten, die im Verbund mit dem in Frankfurt befindlichen Rechenzentrum der Hessischen Sparkassenorganisation (RHSO) standen und an die Terminals oder PC's angeschlossen waren. Anträge auf Zugriffsberechtigungen wurden an das RHSO weitergeleitet. Dort wurde für das betroffene Terminal oder den PC die Berechtigung eingetragen, SCDA aufzurufen. Es gab keine Möglichkeit zwischen Anwendungen zu wechseln, der Benutzer befand sich entweder in SCDA oder in einer anderen Anwendung.

Im RHSO wurde sofort die Verbindung zum Debis-Rechner aufgebaut. Eine Zwischenspeicherung erfolgte nicht, der RHSO-Rechner funktionierte nur als Steuereinheit. Die Zugangsberechtigung wurde mittels User-Identifizierung und Paßwort überprüft. Die zusätzliche persönliche Identifizierung mußte die Sparkasse freilich besonders beantragen, denn das System läßt einen Verbindungsaufbau auch ohne User-Identifizierung zu. Außerdem wurden eine Kennziffer, die das Kreditinstitut identifizierte, und ein für die Sparkasse geltendes Kennwort abgefragt.

Soweit ersichtlich, entspricht die Benutzerkontrolle der Schufa-Anwendung dem Stand der Technik, allerdings nur, wenn der Anwender SCDA mit zusätzlicher persönlicher User-Identifizierung angefordert hat. Andernfalls wird die Eingabe- und die damit verbundene Übermittlungskontrolle problematisch. Darüber hinaus ist es ohne User-Identifizierung nicht möglich, in einer Einrichtung mit einer großen Zahl von Mitarbeitern wie der Stadt- und Kreissparkasse Kassel, die Zugriffsbeschränkungen wirksam umzusetzen. Denn angesichts der vielen Terminals, die dort zur Abfrage zur Verfügung standen, hätten Unberechtigte ohne große Schwierigkeiten auf Schufa-Daten zugreifen können, da ca. 150 Beschäftigte das Institutskennzeichen kannten.

Die Protokollierung der Datenübermittlungen erfolgte bei der Schufa. Die Schufa stellt die Daten, die sie zur Eingabekontrolle nutzt, den Teilnehmern für Übermittlungskontrollen zur Verfügung. Begründet wurde das damit, daß die erforderlichen Daten an keiner anderen Stelle automatisiert vorlägen. Von der Sparkasse habe ich in diesem Zusammenhang gefordert, durch Namenskürzel oder ähnliches auf den Originalunterlagen zu kennzeichnen, wer wann welche Daten an die Schufa übermittelt hat. Für eine detaillierte Nachprüfung stünden dann immer noch zusätzlich die Schufa-Protokolle zur Verfügung.

17.1.6
Dienstanweisung

Unter meiner Mitwirkung wurde von der Stadtsparkasse Kassel und dem RHSO eine Dienstanweisung entworfen, die das Schufa-Auskunftsverfahren für die Sparkassenmitarbeiter detailliert regelt. Festgelegt wird u.a. der Kreis der Zugriffsberechtigten, in diesem Fall Kundenberater, Sachbearbeiter des Geschäftsstellenbereichs und Kreditsachbearbeiter; wer die konkrete Zugriffsberechtigung erteilt und wie dies zu erfolgen hat. Geregelt ist auch die Beendigung der Zugriffsberechtigung. Ausführlich erläutert werden die Form der Anfragen und Meldungen, die einzelnen Meldepflichten, die Zuständigkeiten für die jeweiligen Meldungen und die Aufbewahrung der Unterlagen. Die Dienstanweisung soll den übrigen Sparkassen als Musterdienstanweisung vom Sparkassen- und Giroverband Hessen-Thüringen ausgehändigt werden.

17.2
Der verlorene Scheck

Eine Kundin kaufte in einem Kinderbekleidungshaus Waren im Wert von 230,00 DM und bezahlte mit einem Euroscheck. Einige Zeit später rief die Inhaberin des Geschäfts bei ihr an und verlangte den Betrag erneut. Der Scheck, so die Begründung, sei abhanden gekommen; wahrscheinlich habe ihn eine inzwischen ausgeschiedene Mitarbeiterin veruntreut.

Die Kundin wunderte sich, daß die Inhaberin sie ausfindig machen konnte, denn sie war in dem Geschäft nicht bekannt und wohnte darüber hinaus an einem anderen Ort. Als sie herausfand, daß die Sparkasse, auf die der Scheck bezogen war, ihre Anschrift und Telefonnummer weitergegeben hatte, bat sie mich um Überprüfung der Angelegenheit.

Bei meinen Recherchen stellte sich heraus, daß die Volksbank, das Kreditinstitut der Geschäftsinhaberin, in deren Auftrag bei der Sparkasse Namen und Anschrift der Kundin erfragt hatte. Rechtlich gesehen handelte es sich somit um eine Datenübermittlung von der Sparkasse an die Inhaberin des Bekleidungshauses. Als Rechtsgrundlage dafür kam nur § 28 Bundesdatenschutzgesetz (BDSG) in Betracht. Danach ist eine Datenweitergabe u.a. zulässig, soweit sie zur Wahrung berechtigter Interessen Dritter erforderlich ist und kein Grund zu der Annahme besteht, daß der Betroffene ein schutzwürdiges Interesse an dem Ausschluß der Übermittlung hat (§ 28 Abs. 2 Nr. 1a BDSG).

Entscheidend für das berechtigte Interesse war hier, ob die Inhaberin des Bekleidungshauses weiterhin einen Anspruch auf Kaufpreiszahlung gegen die Kundin hatte (§ 433 Abs. 2 Bürgerliches Gesetzbuch (BGB)). Ein Scheck dient zwar der Zahlung, ist aber kein gesetzliches Zahlungsmittel. Mit der Übergabe des Schecks an den Verkäufer erlischt die

Kaufpreisforderung nicht, sondern es entsteht eine zusätzliche Forderung des Verkäufers aus dem Scheck. Der Verkäufer, der statt Barzahlung einen Scheck angenommen hat, ist allerdings verpflichtet, zunächst Erfüllung aus dem Scheck zu suchen. Die Kaufpreisforderung gilt so lange als gestundet. Die Hingabe eines Schecks zur Begleichung einer Kaufpreisforderung bedeutet also grundsätzlich eine Leistung erfüllungshalber und nicht an Erfüllungs Statt (§ 364 Abs. 2 BGB). Die Kaufpreisforderung erlischt erst, wenn der Scheck von der bezogenen Bank eingelöst worden ist, etwa durch Barauszahlung oder Gutschrift. Aus der Eingabe war zu entnehmen, daß der Scheck noch nicht eingelöst worden war, so daß die Kaufpreisforderung noch bestand. Die Inhaberin des Bekleidungshauses hatte danach also nicht nur ein berechtigtes, sondern sogar ein rechtliches Interesse an der Übermittlung der Daten, dem auf Seiten der Kundin keine schutzwürdigen Belange entgegenstanden. Die Auskunft der Sparkasse war somit zulässig.

In zwei Kommentaren zum Bürgerlichen Gesetzbuch wird allerdings die Auffassung geäußert, daß bei Übergabe eines ordnungsgemäß ausgefüllten Euroschecks bereits mit Scheckübergabe der Kaufpreis gezahlt sei. Dies läßt sich gut vertreten. Im täglichen Geschäftsverkehr wird der Euroscheck von den Beteiligten wie ein gesetzliches Zahlungsmittel behandelt. Soweit der Ausstellungsbetrag innerhalb der Garantiesumme bleibt, ist die Sicherheit der Erfüllung einer Bargeldübergabe gleichzusetzen. Folgt man dieser Ansicht, wäre die Kaufpreisforderung des Bekleidungshauses mit der Scheckübergabe erloschen. Bei Verlust des Schecks würde der Empfänger so behandelt, als hätte er Bargeld erhalten und dies verloren. Die Auskunft der Sparkasse wäre demzufolge unzulässig gewesen.

Es ließ sich allerdings weder in der übrigen einschlägigen Literatur noch in der Rechtsprechung eine Bestätigung dieser Meinung zur Erfüllungswirkung eines Euroschecks finden. Daher war es nicht möglich, eine abschließende datenschutzrechtliche Bewertung zu treffen. Denn die Entscheidung über die Zulässigkeit oder Unzulässigkeit der Datenweitergabe der Sparkasse hing ab von einer rein zivilrechtlichen Vorfrage, der Erfüllungswirkung der Scheckübergabe. Hierüber könnte jedoch nur ein ordentliches Gericht verbindlich entscheiden.

18. Umwelt

18.1
Entwurf eines Hessischen Umweltinformationsgesetzes

Es ist erfreulich, berichten zu können, daß eine alte Forderung des Hessischen Datenschutzbeauftragten zum Thema Informationsfreiheit (freedom of information – vgl. 14. Tätigkeitsbericht, Ziff. 11.1; 15. Tätigkeitsbericht, Ziff. 10) inzwischen ihrer Verwirklichung durch die Gesetzgebung entgegengeht: Im Hinblick auf die – durch die EG-Richtlinie Nr. 90/313/EWG (Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt, ABl. EG Nr. L 158/56) festgelegte – Frist bis Jahresende 1992 zwar mit gut einem Jahr Verspätung, aber immer noch mit der Möglichkeit, als erstes Bundesland seine Verwaltung für die Bürgerinnen und Bürger transparenter zu machen, hat die Hessische Landesregierung den Entwurf für ein Hessisches Umweltinformationsgesetz (HUIG) vorgelegt.

Dieser Entwurf hat das Ziel, „... jeder Person Informationsmöglichkeiten über Art und Ausmaß von Umwelteinwirkungen zu verschaffen, das umweltbedeutsame Handeln der Verwaltung durch die Öffentlichkeit kontrollierbarer zu machen und dem Schutz der Umwelt zu dienen" (§ 1 HUIGE). Das Gesetz soll gelten „für alle Informationen über die Umwelt, die bei den in § 3 Abs. 2 bestimmten Behörden des Landes, bei den Gemeinden und Gemeindeverbänden sowie den sonstigen, der Aufsicht des Landes unterstehenden juristischen Personen des öffentlichen Rechts vorhanden sind..." (§ 2 HUIGE). Bezüglich dieser Informationen über die Umwelt kann jede Person Auskunft sowie Einsicht in Umweltakten verlangen, auch über solche Informationen, „die in sonstigen Informationsträgern" enthalten sind (§ 4 Abs. 1 HUIGE) – also beispielsweise auf Datenträgern gespeicherte Daten.

An dieser Stelle berührt das Akteneinsichtsrecht den Datenschutz, soweit es sich nämlich um Einsicht in personenbezogene Daten handelt. Allerdings braucht sich niemand deshalb zu beunruhigen. Das Grundprinzip aller bisher bekannten oder geplanten Regelungen über Aktenzugang bzw. Informationsfreiheit ist: „Informationsfreiheit bzw. Aktenzugangsrecht nur insoweit, als der Datenschutz dadurch nicht verletzt wird". Das gleiche gilt für den Schutz von Betriebs- und Geschäftsgeheimnissen. Dementsprechend sieht das geplante Hessische Umweltinformationsgesetz vor, daß der Anspruch auf Zugang zu Informationen über die Umwelt nach § 4 Abs. 1 nicht besteht, „... soweit durch die Erteilung der Auskunft oder die Einsichtnahme unbefugt personenbezogene Daten oder Betriebs- oder Geschäftsgeheimnisse offenbart werden" (§ 5 Abs. 1 HUIGE). Es betont ausdrücklich, daß nur dann personenbezogene Daten und Betriebs- oder Geschäftsgeheimnisse offenbart werden dürfen, „wenn keine schutzwürdigen Belange der Betroffenen entgegenstehen" (§ 5 Abs. 2 Satz 1 HUIGE). Wie wichtig dem Gesetzgeber der Schutz der Betroffenen in diesem Zusammehang ist, ergibt sich aus der Bestimmung in § 5 Abs. 2 Sätze 2, 3:

„Vor ihrer Offenbarung sind die Betroffenen anzuhören. Die Behörde hat in der Regel von der Betroffenheit eines Dritten auszugehen, soweit dieser übermittelte Informationen als Betriebs- und Geschäftsgeheimnisse kennzeichnet und die Gründe hierfür im einzelnen dargelegt hat".

Aus der Sicht des Datenschutzes erscheint die Regelung hinreichend klar, um zu gewährleisten, daß auch bei Ausübung des neuen Einsichtsrechts in Umweltakten das Grundrecht auf informationelle Selbstbestimmung (Datenschutz) unberührt bleibt.

Wenn es Probleme bei Anwendung des neuen HUIG geben sollte, dann werden diese weniger im Theoretischen und Grundsätzlichen liegen als vielmehr in der Praxis der Anwendung, d.h. im richtigen Verständnis der verschiedenen Rechtsbegriffe wie z.B. „Umweltinformationen", „Behörden", „Umweltakten" und in der Subsumtion der entsprechenden Sachverhalte. Hier wird – wie aus Erfahrungen mit „freedom of information" aus anderen Ländern bekannt ist – wahrscheinlich nicht unerheblicher Beratungsbedarf bei den betroffenen Behörden bestehen, insbesondere wenn sie nicht selbst über Mitarbeiter mit entsprechender juristischer Schulung verfügen. Es steht zu befürchten, daß die zu erwartende Unsicherheit in der Abwägung von Anträgen auf Akteneinsicht mit Datenschutzrechten oder dem Schutz von Betriebs- oder Geschäftsgeheimnissen in einer großen Zahl von Fällen zu einer Ablehnung durch die Behörde und – als Folge davon – zu einer Flut von Prozessen vor den Verwaltungsgerichten führen wird.

Aus diesem Grunde ist es zu begrüßen, daß die Landesregierung hier eine Neuerung eingeführt hat, die sich in Frankreich und Kanada bereits seit Jahren bewährt hat: Die Institution eines Beauftragten für den freien Zugang zu Umweltinformationen. Diese Institution berät die zuständigen Behörden bei der Ausführung des Gesetzes, ebenso die betroffenen natürlichen und juristischen Personen. Jede Person kann sich an sie wenden, „wenn sie annimmt, daß ihr Umweltinformationen nach diesem Gesetz zu Unrecht verweigert werden oder daß solche zu Unrecht übermittelt wurden oder werden sollen" (§ 6 Satz 3 HUIGE).

Jedoch wird hier keine neue Bürokratie geschaffen, sondern die neue Aufgabe soll dem Hessischen Datenschutzbeauftragten übertragen werden. Da beim Hessischen Datenschutzbeauftragten ohnehin über 20-jährige Erfahrung in der Abwägung von Rechten des einzelnen mit den Interessen der Allgemeinheit – wie es bei Datenschutzproblemen die Regel ist – vorliegen, bot sich eine solche Lösung, nicht nur unter Gesichtspunkten der Sparsamkeit, an. Hinzu kommt, daß sich die französischen Erfahrungen mit zwei verschiedenen Kontrollinstanzen für Datenschutz (CNIL) und Aktenzugangsrecht (CADA) nicht befriedigend entwickelt haben und in unserem Nachbarland Überlegungen im Gange sind, beide Institutionen zu einer einzigen zu verschmelzen (vgl. 15. Tätigkeitsbericht, Ziff. 10.5). Es ist zu erwarten, daß die in § 6 des Gesetzentwurfs vorgesehene Beratung von Behörden und Bürgern die meisten der befürchteten Verwaltungsstreitverfahren wird verhindern können. Der Beauftragte für Informationsfreiheit soll – wie schon in seinem Amt als Hessischer Datenschutzbeauftragter – keinerlei Exekutivfunktionen haben, also gegenüber den betroffenen Behörden und Personen keine Weisungen erteilen können. Wer also mit seiner Empfehlung nicht einverstanden ist, kann selbstverständlich eine Klage vor dem Verwaltungsgericht einreichen.

Für die Aufgaben und die Stellung des Beauftragten für Informationsfreiheit gilt im übrigen das Hessische Datenschutzgesetz entsprechend (§ 6 letzter Satz HUIGE).

Für die Zeit ab 1. Januar 1993 bis zum Inkrafttreten des neuen HUIG ist das Einsichtsrecht in Umweltakten unmittelbar aufgrund der EG-Richtlinie gewährleistet: Das Hessische Ministerium für Umwelt, Energie und Bundesangelegenheiten hat mit Erlaß vom 14. Dezember 1992 (Az.: I B 1-70 16-11/92; StAnz. 1992, 3306) alle Umweltbehörden angewiesen, den Bürgern Auskunft aus bzw. Einsicht in Umweltakten zu gewähren. Bisher hielt sich die Anzahl entsprechender Anträge im Bereich von mehreren Dutzend; danach wird eine Überlastung der Behörden durch das neue Umweltakteneinsichtsrecht zunächst nicht zu erwarten sein.

18.2
Erfassung der Lagerorte privater Heizöltanks

Ein typisches Beispiel dafür, wie eine wichtige Umweltschutzaufgabe durch mißverstandenen Datenschutz behindert werden könnte, zeigt ein Fall, auf den ich durch eine Anfrage aufmerksam wurde.

Aus dem Schreiben des Umweltamtes des Magistrats der Stadt Frankfurt an das Regierungspräsidium Darmstadt ergibt sich das Problem:

> „Die im Rahmen der Umweltüberwachung gebotene Vorsorge zur Verhinderung etwaiger Schadensfälle macht es notwendig, sämtliche Lagerorte privater Heizöltanks zu erfassen und anschließend auf die Erfüllung der Anforderungen gemäß der Verordnung über Anlagen zum Lagern, Abfüllen und Umschlagen wassergefährdender Stoffe und die Zulassung von Fachbetrieben – Anlagenverordnung (VAwS) vom 23. März 1982 (GVBl. I 1982 S. 74) – hin zu überprüfen. Dadurch soll ein potentieller Risikofaktor bezüglich Grundwasser- und Bodenverunreinigung wesentlich minimiert werden.
>
> Um die Standorte der Heizöltanks komplett registrieren und die jeweiligen Betreiber anschreiben zu können, ist die Mithilfe der Schornsteinfegerinnung dringend angeraten."

Ein Brief ähnlichen Inhalts des Landkreises Offenbach ergänzt den Sachverhalt:

> „Durch den täglichen Dienstbetrieb wird immer wieder klar, daß es ‚Schwarzbestände' an Öllagerungen gibt, die prüfpflichtig sind und bis zum heutigen Tag nicht einmal durch den TÜH/TÜV geprüft wurden. Solche uns nicht bekannte Altanlagen stellen eine erhebliche Gefahr für das Grundwasser dar, da gerade solche Anlagen teilweise mit einwandigen und nach heutigem Wasserrecht mit nicht mehr bestandskräftigen Bauartzulassungen ausgerüstet sind.
>
> Zum Schutze des Grundwassers ist es unerläßlich, Daten zu beschaffen, die es ermöglichen, diese Gefahr zu beseitigen."

Die Schornsteinfegerinnung war grundsätzlich zur Zusammenarbeit mit der Unteren Wasserbehörde bereit, wenn auch unter der Voraussetzung, daß eine entsprechende Datenübermittlung datenschutzrechtlich unbedenklich sei.

Die Rechtslage ist eindeutig: Ausgangspunkt ist die Vorschrift von § 105 Abs. 1 Hessisches Wassergesetz (HWG) vom 22. Januar 1990 (GVBl. I S. 114), da diese als „bereichsspezifische" Datenschutzvorschrift nach § 3 Abs. 3 Satz 1 Hessisches Datenschutzgesetz diesem vorgeht.

Die Erhebung von Namen und Adressen der Betreiber von Heizölanlagen durch die Untere Wasserbehörde bei den jeweils zuständigen Bezirksschornsteinfegermeistern bzw. der Schornsteinfegerinnung, bzw. die entsprechende Datenübermittlung von diesen Stellen an die Untere Wasserbehörde ist nach § 105 Abs. 2 HWG zulässig: Es handelt sich dabei um eine Aufgabe der „Durchführung der Wasseraufsicht" (§ 5 Abs. 1 Ziff. 1 HWG). Dazu gehört nämlich die Gefahrenabwehr nach § 74 Abs. 1 HWG hinsichtlich genehmigungsbedürftiger oder anzeigepflichtiger Anlagen. Heizölanlagen sind anzeigepflichtig nach § 31 Abs. 1 HWG i.V.m. § 19g Abs. 1 Wasserhaushaltsgesetz vom 23.09.1986 (BGBl. I S. 1529; ber. S. 1654).

19. Landwirtschaft (InVeKoS)

Schon in früheren Tätigkeitsberichten (vgl. z.B. 21. Tätigkeitsbericht, Ziff. 13.2) habe ich darauf hingewiesen, daß EG-Vorschriften auf dem Gebiet der Landwirtschaft immer wieder schwierige datenschutzrechtliche Probleme verursachen. Dies ist auch der Fall bei einem neuen, durch zwei EG-Verordnungen eingeführten „Integrierten Verwaltungs- und Kontrollsystem – InVeKoS", das dazu führen soll, eine mißbräuchliche Verwendung von EG-Fördermitteln festzustellen und zu verhindern. Vom angestrebten Ziel her gesehen ist dieses Projekt ohne jeden Zweifel zu begrüßen.

19.1
Probleme bei der Umsetzung der EG-Verordnungen zu InVeKoS

Probleme gibt es jedoch bei der Umsetzung der EG-Vorschriften, insbesondere bei einzelnen ihrer Bestimmungen.

Nach einem Hinweis des Bundesbeauftragten für den Datenschutz an die Landesbeauftragten für den Datenschutz über das Projekt InVeKoS und die unzureichenden Datenschutzvorschriften für seine Umsetzung hat der rheinland-pfälzische Datenschutzbeauftragte als erster die Öffentlichkeit in einer kritischen Stellungnahme auf die Gefahr des InVeKoS-Projekts hingewiesen. Er schreibt u.a.:

> „Von der Öffentlichkeit unbemerkt ist es der EG-Bürokratie gelungen, die Mitgliedstaaten auf die Errichtung einer Datenbank zu verpflichten, die – zusammen mit den vorgesehenen Überwachungsmaßnahmen – bislang beispiellos ist ... Ziel ... ist, daß jedes Mitgliedsland eine Datenbank nach einheitlichen Kriterien errichtet, in der alle Landwirte erfaßt werden, die an bestimmten Förderungsmaßnahmen teilnehmen. Bestandteil dieser Datenbank ist insbesondere eine lückenlose Erfassung der Flächen der betroffenen Landwirte und der Flächennutzungsart; weiterhin ist beabsichtigt, Daten zur wirtschaftlichen Situation der Betriebe zu erfassen; alle förderungsrelevanten Informationen sind automatisiert zu speichern. Die Grundstücke sollen nach einheitlichen Kriterien so bezeichnet werden, daß eine Kontrolle der angegebenen Nutzungsarten durch einen Vergleich mit Satellitenaufnahmen möglich wird. Die Überwachung mit Hilfe der Satellitentechnik ist ein wesentlicher, integraler Bestandteil des Konzepts ... Nur Staaten, die zu den für 1993 festgelegten Terminen die Datenbank realisiert haben, erhalten Mittel für die genannten landwirtschaftlichen Fördermaßnahmen ...

Da im Bereich der EWG wohl kaum ein Landwirt, sei er nebenberuflich oder sei er hauptberuflich tätig, ohne Beteiligung an irgendeiner Förderungsmaßnahme existieren kann (und sei es nur die Inanspruchnahme der Milchquotenregelung), ist die Erfassung fast aller Landwirte in der landwirtschaftlichen Betriebsdatenbank unausweichlich ... Das integrierte Verwaltungs- und Kontrollsystem ist also nichts anderes als eine lückenlose Erfassung der Landwirte zum Zweck der Kontrolle im Bereich landwirtschaftlicher Förderungsmaßnahmen." („Das integrierte Verwaltungs- und Kontrollsystem der EG (InVeKoS) – kommt der ‚Gläserne Landwirt'?" in: Datenschutz und Datensicherung 2/93 S. 72).

Mehrere Landwirte haben sich im Frühjahr 1993 mit Beschwerden an mich gewandt. Sie sind der Ansicht, daß der Umfang der geforderten Angaben weit über das Maß des Erforderlichen hinausgehe. Ich habe mich sofort der Angelegenheit angenommen und festgestellt, daß in Hessen die Verwirklichung des InVeKoS-Projekts zu den gleichen Problemen führt wie im Nachbarland Rheinland-Pfalz. Die hessische Landwirtschaftsverwaltung bis hin zum Ministerium hat mich bei meinen Ermittlungen unterstützt. Sie ergaben folgendes:

Die Agrarförderung „Flächen" 1993 Hessen ist ein Teil des Integrierten Verwaltungs- und Kontrollsystems für bestimmte gemeinschaftliche Beihilferegelungen – InVeKoS. Maßgeblich sind die Verordnung (EWG) Nr. 3508/92 des Rates vom 27. November 1992 (ABl. EG L 355/1 vom 5. Dezember 1992) und die Verordnung (EWG) Nr. 3887/92 der Kommission vom 23. Dezember 1992 mit Durchführungsbestimmungen zum Integrierten Verwaltungs- und Kontrollsystem für bestimmte gemeinschaftliche Beihilferegelungen (ABl. EG Nr. 93/36 vom 31. Dezember 1992). Art. 6 Abs. 1 der Verordnung vom 27. November 1992 bestimmt, daß ein Betriebsinhaber Beihilferegelungen nur in Anspruch nehmen kann, wenn er für jedes Jahr einen „Beihilfeantrag Flächen" abgibt; dieser Beihilfeantrag muß

nach Art. 4 der Verordnung vom 23. Dezember 1992 „alle erforderlichen Informationen enthalten, insbesondere die Identifizierung des Betriebsinhabers" und „die zweckdienlichen Angaben zur Identifizierung aller landwirtschaftlich genutzten Parzellen des Betriebs, ihre Fläche, Lage und Nutzung, ggf. mit Hinweis darauf, ob es sich um eine bewässerte Parzelle handelt, sowie die jeweilige Beihilferegelung".

Aus den beiden EG-Verordnungen geht eindeutig hervor, daß hier eine Datenerhebung auf Vorrat betrieben wird, da – wie auch im Falle der vorliegenden Beschwerden – dem Beihilfeantrag Daten beigefügt werden müssen, die für dessen Bearbeitung konkret irrelevant sind. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65,1) ausdrücklich die Sammlung personenbezogener Daten „auf Vorrat zu unbestimmten oder noch nicht bestimmbaren Zwecken" als unzulässig bezeichnet (vgl. BVerfG a.a.O. S. 46). Objektiv gesehen, bestehen also die Beschwerden der Landwirte zu Recht, da für den Beihilfeantrag mehr Daten erhoben werden als zu seiner Bearbeitung erforderlich sind.

Darüber hinaus bestehen erhebliche Zweifel, ob die genannten EG-Verordnungen den grundsätzlichen Forderungen des Volkszählungsurteils entsprechen: Nach diesem sind Beschränkungen des Grundrechts auf informationelle Selbstbestimmung nur zulässig auf „einer (verfassungsmäßigen) gesetzlichen Grundlage, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben und die damit dem rechtsstaatlichen Gebot der Normenklarheit entspricht ... Bei seinen Regelungen hat der Gesetzgeber ferner den Grundsatz der Verhältnismäßigkeit zu beachten". Die EG-Verordnungen erfüllen keine der genannten Voraussetzungen: Sie sind weder normenklar, da die entsprechenden Beschränkungen nur sehr allgemein formuliert sind, noch sind sie verhältnismäßig, da hier mehr Daten gefordert werden als zur Aufgabenerfüllung erforderlich.

Darüber hinaus weist der rheinland-pfälzische Datenschutzbeauftragte darauf hin: „In diesem Zusammenhang ist erneut zu bedauern, daß EG-Rechtsetzungsakte häufig an nationalen Institutionen vorbei wirksam werden. So ist eine grundsätzliche datenschutzrechtliche Erörterung der genannten Aspekte vor Erlaß der hier maßgeblichen EG-Verordnung nicht erfolgt. Die Landesbeauftragten für den Datenschutz sind sämtlich vor vollendete Tatsachen gestellt worden ... Die Schaffung des „Gläsernen Landwirts" als Objekt der Agrarbürokratie ist unter datenschutzrechtlichen Gesichtspunkten nicht akzeptabel" (a.a.O. S. 227).

Auf meine Anregung hin wurde die im vergangenen Jahr gebildete „Ad hoc-Arbeitsgruppe Umweltschutz und Datenschutz" (vgl. 21. Tätigkeitsbericht, Ziff. 12.1) um den Aufgabenbereich „Landwirtschaft" erweitert und in einen festen Arbeitskreis der Datenschutzbeauftragten-Konferenz umgewandelt. Dieser hat sich in mehreren Sitzungen mit dem Projekt InVeKoS befaßt und einen Vorschlag für eine Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet. Die Konferenz der Datenschutzbeauftragten hat in ihrer 46. Sitzung in Berlin am 26./27. Oktober 1993 die entsprechende Entschließung verabschiedet. Sie ist in den Materialien zu diesem Tätigkeitsbericht (Ziff. 23.8) im Wortlaut wiedergegeben.

Sollte diese Entschließung nicht zu wesentlichen Veränderungen bei der Verwirklichung des InVeKoS-Projekts im Sinne der Forderungen der Datenschutzbeauftragten führen, so hat sich inzwischen durch das sog. „Maastricht-Urteil" des Bundesverfassungsgerichts vom 12. Oktober 1993 (Az.: 2 BvR 2134/92; 2 BvR 2159/92) die Aussicht auf eine verfassungsgerichtliche Kon trolle der EG-Verordnungen erheblich gebessert: „Das Bundesverfassungsgericht prüft, ob Rechtsakte der europäischen Einrichtungen und Organe sich in den Grenzen der ihnen eingeräumten Hoheitsrechte halten oder aus ihnen ausbrechen" (Leitsätze zum Urteil des 2. Senats vom 12. Oktober 1993, Ziff. 5, letzter Satz).

Hinsichtlich der mir vorliegenden Beschwerden der Landwirte war das Ergebnis meiner Bemühungen unbefriedigend: Das Hessische Landwirtschaftsministerium hatte mich darauf hingewiesen, daß – nach Erfahrungen aus den Bundesländern Bayern und Baden-Württemberg – mit Kürzungen der Beihilfen zu rechnen sei, wenn die hessischen Landwirte in entsprechenden Anträgen für EG-Beihilfen nur „reduzierte" Angaben machen würden – also nur die Angaben, die tatsächlich für den gegenwärtigen Antragszweck benötigt würden. Nach Ansicht der EG-Behörden seien solche Anträge „unvollkommen" ausgefüllt und zögen eine Verminderung oder gänzliche Ablehnung der Beihilfen nach sich. Ich konnte daher – trotz der oben dargestellten Rechtsprobleme – den Beschwerdeführern nicht raten, die Angabe der entsprechenden personenbezogenen Daten zu verweigern.

Nach dem Maastricht-Urteil des Bundesverfassungsgerichts besteht allerdings eine gewisse Hoffnung darauf, daß die Antragspraxis im Rahmen von InVeKoS in Zukunft so wird geändert werden können, daß sie dem deutschen Verfassungs- und Datenschutzrecht entspricht.

19.2
Probleme bei der Einführung der für InVeKoS notwendigen DV-Programme

Mit der Einführung von InVeKoS sah sich das Hessische Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz mit der Aufgabe konfrontiert, den sich ständig ändernden Randbedingungen für die Zuteilung von landwirtschaftlichen Fördermitteln (im wesentlichen neue Förderprogramme) mit einer wirkungsvollen DV-Struktur begegnen zu müssen, da die Flut von Anträgen sonst nicht fristgerecht hätte bearbeitet werden können.

Fristgerecht bedeutet im Zusammenhang mit den durch EG-Beschlüsse zu verteilenden Fördermitteln, daß die jeweiligen Stichtage zur Antragsannahme und Bearbeitung von der Landwirtschaftsverwaltung einzuhalten sind, da sonst Kürzungen der Leistungen für die Antragsteller befürchtet werden müssen.

Dies führt dazu, daß die notwendige programmtechnische Umsetzung geänderter oder neuer Förderprogramme in einer für die Entwicklung und Einführung von Software unüblich kurzen Zeitspanne erfolgen muß. Die bisherigen DV-Strukturen der Landwirtschaftsverwaltung waren diesen Anforderungen nicht gewachsen.

19.2.1
Die Einführung von einheitlichen Netzwerken in den Ämtern für Regionalentwicklung, Landschaftspflege und Landwirtschaft

In der Vergangenheit wurden einzelne Förderbereiche sowohl auf Stand-alone PCs in den Ämtern für Regionalentwicklung, Landschaftspflege und Landwirtschaft bzw. im Landesamt, als auch zentral durch die Hessische Zentrale für Datenverarbeitung (HZD) verarbeitet. Diese Struktur schien nicht länger geeignet, um für einzelne, zum Teil kurzfristig eingeführte, Förderprogramme die notwendige Software zur Erfassung, Prüfung, Verwaltung und Weiterverarbeitung bereitzustellen. Im Hessischen Ministerium für Landesentwicklung, Wohnen, Landwirtschaft, Forsten und Naturschutz und dem Hessischen Landesamt für Regionalentwicklung und Landwirtschaft kam man daher zu dem Ergebnis, daß sich einzelne Bearbeitungspakete am schnellsten in den Ämter für Regionalentwicklung, Landschaftspflege und Landwirtschaft einführen lassen, wenn dort eine weitgehend identische vernetzte PC-Umgebung existiert und die neuen Programm-Module lediglich wie Updates einer Standardsoftware eingespielt werden müssen. Diese Module können dann nach Vorgaben des Hessischen Landesamtes für Regionalentwicklung und Landwirtschaft je nach Bedarf von der HZD, anderen professionellen Softwareentwicklern oder, in besonderen Fällen, auch im Hessischen Landesamt für Regionalentwicklung und Landwirtschaft selbst entwickelt werden.

19.2.2
Das Technik-Konzept und der Datenschutz

Als Basis für die PC-Vernetzung wurde das Netzwerkbetriebssystem Novell Netware ausgewählt, das nach zentralen Vorgaben durch das Hessische Landesamt für Regionalentwicklung und Landwirtschaft in den einzelnen Ämtern für Regionalentwicklung, Landschaftspflege und Landwirtschaft installiert wurde. Bei meinen Gesprächen mit dem Hessischen Landesamt für Regionalentwicklung und Landwirtschaft konnte ich feststellen, daß nahezu alle wesentlichen Fragen des Datenschutz bei der technischen Konzeption bereits berücksichtigt waren.

Insbesondere die Fragen des Zugriffsschutzes, der Benutzerverwaltung, Dokumentation und Protokollierung hatte man bedacht. Für die Übermittlung der Daten von den Ämtern für Regionalentwicklung, Landschaftspflege und Landwirtschaft an das Hessische Landesamt für Regionalentwicklung und Landwirtschaft hatte man auch eine Verschlüsselung der Datenträger vorgesehen. Diese können somit dem Postweg anvertraut werden, ohne daß bei Verlust der Datenträger befürchtet werden muß, daß die Daten unbefugten Dritten zugänglich werden.

Die Konzeption sieht vor, daß dem Systembeauftragten vor Ort bei der Rechtevergabe nur eingeschränkte Funktionen (Workgroup Manager) übertragen werden. Sie berechtigen nur zum Eingriff in dem vom Hessischen Landesamt für Regionalentwicklung und Landwirtschaft vorausbestimmten Umfang. Weitergehende Möglichkeiten haben nur die Mitarbeiter des Hessischen Landesamts für Regionalentwicklung und Landwirtschaft, die auch die Funktion des Notfall-Supervisors und die Anwendungsbetreuung übernehmen. Damit wird in einem gewissen Umfang sichergestellt, daß die Netzwerke auch künftig die gleichen einheitlichen Randbedingungen für die vom Landesamt geplanten Anwendungen beibehalten.

Ferner wurde für die entwickelten und für künftige Programm-Module ein Freigabeverfahren festgelegt, das im Rahmen der Möglichkeiten des Landesamtes eine ordnungsgemäße Verarbeitung der Antragsdaten sicherstellt.

Nicht zuletzt wurde ein umfangreiches Handbuch erstellt, in dem detaillierte Installationsabläufe für die Netzwerke und die notwendigen Anweisungen für das Tagesgeschäft in den Ämtern für Regionalentwicklung, Landschaftspflege und Landwirtschaft festgelegt wurden.

19.2.3
Abweichung vom Soll

So begrüßenswert das Konzept des Hessischen Landesamts für Regionalentwicklung und Landwirtschaft ist: Leider mußte ich bei einem Prüfbesuch in einem Amt für Regionalentwicklung, Landschaftspflege und Landwirtschaft feststellen, daß die im Installationshandbuch vorgegebenen Randbedingungen nicht vollständig eingehalten wurden. Diese Fehler bei der Umsetzung der Installationsvorgaben sind u.U. noch mit der kurzfristigen Einführung der Systeme erklärbar. Sie zeigen jedoch, daß eine DV-Revision ein unverzichtbarer Bestandteil einer ordnungsgemäßen und datenschutzgerechten Datenverarbeitung ist. Eine geregelte Kontrolle der durchgeführten Installationen hätte in jedem Fall die Unstimmigkeiten ausgeschlossen, die ich festgestellt habe.

20. Arbeitsgruppe Korruptionsbekämpfung

Die Landesregierung hat am 16. März 1993 die Einsetzung einer Arbeitsgruppe beschlossen, die unter Federführung des Hessischen Ministeriums des Innern und für Europaangelegenheiten ein ressortübergreifendes Konzept für die Bekämpfung der Korruption innerhalb der Landesverwaltung erarbeiten soll. An der aus Vertretern mehrerer Ressorts

bestehenden Arbeitsgruppe, deren erste Sitzung am 7. September stattfand und die seitdem mehrmals getagt hat, nehme ich als Berater teil. (Dies ist übrigens ein weiteres Beispiel dafür, daß der Datenschutz sich keineswegs auf die Bearbeitung von Beschwerden und die Kontrolle von Behörden beschränkt, sondern ein wesentlicher Teil meiner Tätigkeit aus der Beratung bei der Planung und Gestaltung von Datenverarbeitungsvorhaben besteht.)

Eine zentrale Rolle in dem Korruptionsbekämpfungskonzept werden Vergabesperren spielen. Bewerber bzw. Unternehmen, die bei öffentlichen Ausschreibungen von Verträgen über Lieferungen und Leistungen nachweislich eine schwere Verfehlung begangen haben, die ihre Zuverlässigkeit in Frage stellt, können von der Teilnahme am Wettbewerb ausgeschlossen werden (§ 7 Nr. 5 lit. c Verdingungsordnung für Leistungen – ausgenommen Bauleistungen, VOL; § 8 Nr. 5 lit. c Verdingungsordnung für Bauleistungen, VOB; jeweils i.V.m. § 55 Landeshaushaltsordnung). Da eine landesweite Sperre angestrebt wird, stellt sich zwangsläufig die Frage nach dem notwendigen Informationsaustausch.

Nach den gegenwärtigen Überlegungen der Arbeitsgruppe sollen in der Regel die jeweiligen Mittelbehörden oder die Dienststelle, in deren Zuständigkeitsbereich die Verfehlung festgestellt wurde, die Vergabesperre verhängen. Um eine landesweite Wirkung zu erzielen, muß daher ein Informationsaustausch organisiert werden. Zwei Modelle stehen zur Diskussion: Informeller Informationsaustausch zwischen den Landesressorts oder zentrales Melde- und Informationssystem.

Die Arbeitsgruppe hat sich auf folgenden Datensatz verständigt:

A) Identifikation des Bewerbers/Unternehmers: 1. Unternehmen, 2. Gewerbezweig, 3. Anschrift, 4. Handelsregister-Nr. – falls bekannt.

B) Angaben zur Auftragssperre: 1. aussprechende Behörde, 2. Datum, 3. Aktenzeichen, 4. Name eines Ansprechpartners, 5. Telefon-Nummer des Ansprechpartners.

Die nachfolgenden Überlegungen zur Frage der Zulässigkeit eines ressortübergreifenden Informationsaustausches gehen von diesem Datensatz aus.

Da es sich um personenbezogene Daten handelt und unter den von einer Vergabesperre betroffenen Unternehmen nicht nur juristische Personen, sondern auch Einzelkaufleute sein werden, richtet sich die Zulässigkeit der Verarbeitung mangels spezialgesetzlicher Regelungen nach den allgemeinen Vorschriften des Hessischen Datenschutzgesetzes (HDSG). Öffentliche Stellen dürfen danach personenbezogene Daten speichern und übermitteln, wenn dies zu ihrer Aufgabenerfüllung oder zur Erfüllung von Aufgaben des Empfängers erforderlich ist (§§ 11 und 14 HDSG).

Es kommen hier mehrere Übermittlungskonstellationen in Betracht:

a) Eine untere Behörde verhängt für ihren Bereich eine Vergabesperre. Sie unterrichtet darüber die Mittelbehörde, diese gibt die Information an die oberste Landesbehörde weiter.

b) Eine Mittelbehörde verhängt eine Vergabesperre und informiert die untere Behörde sowie die oberste Landesbehörde.

c) Die oberste Landesbehörde erläßt für ihren Geschäftsbereich eine Vergabesperre und teilt dies den nachgeordneten Behörden mit.

d) Eine oberste Landesbehörde benachrichtigt eine andere (oder sämtliche) oberste(-n) Landesbehörde(-n) über eine von ihr oder in ihrem Bereich ausgesprochene Vergabesperre.

e) Die Empfänger geben diese Nachricht an ihre nachgeordneten Behörden weiter.

Jeder dieser Übermittlungsschritte müßte die Voraussetzungen der §§ 11 oder 14 HDSG erfüllen. Wird die von nachgeordneten Behörden zu verhängende Vergabesperre an die Zustimmung der obersten Landesbehörde geknüpft, so ist die Datenübermittlung der nachgeordneten Behörden schon aus diesem Grunde erforderlich. Darüber hinaus haben sicherlich sämtliche Behörden der Landesverwaltung ein legitimes Interesse, nicht mit Unternehmen zu kontrahieren, die von anderen Behörden wegen schwerer Verfehlungen von der Teilnahme am Wettbewerb ausgeschlossen wurden. Neben diesem Interesse, nicht ebenfalls übervorteilt zu werden, läßt auch der Sanktionscharakter der Vergabesperre eine Datenübermittlung erforderlich erscheinen. Bliebe die Sperre den übrigen Behörden unbekannt, könnte das betroffene Unternehmen problemlos in andere Vergabebereiche ausweichen.

Daran wird allerdings auch deutlich, daß nicht jede Behörde über jede Vergabesperre informiert sein muß. Erforderlich ist die Information nur für die Behörde, die gleiche Aufträge vergibt. Wenn beispielsweise das Hessische Ministerium für Wissenschaft und Kunst gegen Wäschereien eine Vergabesperre verhängt hat, dürfte dies für ein Staatsbauamt, ein Wasserwirtschaftsamt oder ein Staatliches Schulamt uninteressant sein. Die Übermittlung wäre daher rechtswidrig. Eine Veröffentlichung im Staatsanzeiger, die datenschutzrechtlich eine Übermittlung an andere öffentliche Stellen aber auch an Private wäre, muß aus diesem Grunde gleichfalls ausscheiden.

Weil es für die Beurteilung der Zulässigkeit immer auf die einzelne Vergabesperre und den jeweiligen Empfänger der Übermittlung ankommt, dürfte ein die datenschutzrechtlichen Anforderungen erfüllender informeller Informationsaustausch, der die oben aufgezählten Übermittlungsvorgänge umfassen würde, nur schwer zu organisieren sein. Ein

praktikableres Modell wäre wahrscheinlich eine zentrale Datei, auf welche die Behörden in einem noch festzulegenden Verfahren bei Bedarf zugreifen könnten. Damit ließe sich auch das Problem der Aktualisierung besser lösen. In dem informellen Informationsaustauschverfahren wäre nämlich kaum zu garantieren, daß eine Aufhebung der Sperre auch alle vorherigen Empfänger erreicht.

Die gleichen datenschutzrechtlichen Bedingungen gelten übrigens auch für Übermittlungen an Gemeinden. Sie könnten unter Beachtung des Erforderlichkeitsgrundsatzes ebenfalls an dem Informationssystem teilnehmen.

Fazit: Beide Verfahren („Informeller Informationsaustausch" oder „zentrales Meldesystem") sind grundsätzlich datenschutzrechtlich möglich, die praktischen Schwierigkeiten dürften jedoch bei einer zentralen Datei wesentlich geringer sein. Bislang konnte sich die Arbeitsgruppe noch auf keines der beiden Verfahren verständigen.

21. Datensicherheit

21.1
Aspekte der Datensicherheit in Netzen

Die sich aus der zunehmenden Vernetzung von Rechnern ergebenden Risiken für den einzelnen und die Gesellschaft sind erheblich. Der Datenschutz umfaßt in diesem Fall viele Einzelfragen, auf die an dieser Stelle nicht näher eingegangen werden soll. Beispielhaft sollen lediglich einige Punkte genannt werden, die aus Sicht des Datenschutzes relevant sind, ohne daß die Aufstellung abschließend ist:

- Die Ansätze zur Vernetzung von Rechnern orientieren sich an den Möglichkeiten der Technik. Die Konsequenzen für den einzelnen und die Gesellschaft im Sinne einer Technikfolgenabschätzung werden selten in der Konzeption bedacht.

- Die Vernetzung von Rechnern macht Informationsflüsse möglich, die es bisher nur eingeschränkt gegeben hat. Daraus ergeben sich Konsequenzen für die Informationstrennung und die Zweckbindung von Informationen.

  Die aus dem Urteil des Bundesverfassungsgerichts zum Volkszählungsgesetz 1983 abgeleiteten Prinzipien der Informationstrennung und der Zweckbindung von Informationen sind mit den herkömmlichen Maßnahmen nicht mehr zu gewährleisten. Durch die prinzipiell mögliche Kommunikation von jedem mit jedem können die Informationen so betrachtet werden, als seien sie in einem großen Datenpool vorgehalten. Probleme ergeben sich z. B., wenn Personen, die berechtigterweise Zugriff auf Informationen haben, diese gesetzwidrig übermitteln. Technische Maßnahmen, die dies unmöglich machen, sind derzeit in der Regel nicht verfügbar.

  Eine Voraussetzung für die Vernetzung ist in der Praxis eine weitgehende Standardisierung der Technik; solange nur DV-Inseln existierten, waren die Gefahren geringer. Die Standardisierung bietet aber auch die Chance, daß bessere technische Datensicherungsmaßnahmen verfügbar werden.

- Es gibt kaum praktikable Kontrollmöglichkeiten.

- Soweit es das DV-Netz der hessischen Landesverwaltung und ähnlich gelagerte Fälle betrifft, kann noch auf die im 16. Tätigkeitsbericht (Ziff. 4.4) aufgestellten Forderungen und die sich daraus ergebenden Fragen verwiesen werden.

Die folgende Darstellung geht auf Probleme ein, denen die Datensicherheit in DV-Netzen ausgesetzt ist. Kaum berührt werden gesellschaftliche oder rechtliche Probleme, auch Fragen des Datenschutzes sind nur eingeschränkt berücksichtigt.

21.1.1
Ausgangslage

Stand der Technik in der Datenverarbeitung ist nicht mehr der einzelne Rechner, der isoliert betrieben wird, sondern die Tendenz geht dahin, Rechner zu vernetzen. Die Vernetzung kann lokal begrenzt sein, aber auch weiträumig oder weltweit erfolgen. Die Zwecke, zu denen die Vernetzung erfolgt, können vielgestaltig sein. Ein wesentlicher Aspekt ist die schnelle Kommunikation mit anderen Personen oder Institutionen. Damit die Kommunikation ihren Zweck erfüllen kann, werden implizit Anforderungen an die Qualität der Dienstleistung gestellt, die oft nicht bewußt gemacht werden.

In den Anfängen war das Hauptaugenmerk auf die Sicherung der Verfügbarkeit und Zuverlässigkeit des Netzes gelegt, d.h. die Informationen mußten den Adressaten erreichen. Nachdem diese Ziele weitgehend erreicht sind und durch die Tendenz, die übertragenen Informationen als authentisch anzusehen und zu verschiedensten Zwecken automatisiert weiterzuverarbeiten, entstehen neue Anforderungen. Die Vertraulichkeit, Integrität und Authentizität der Daten muß gewährleistet werden. Mit den damit verbundenen Problemen haben sich verschiedene Institutionen befaßt. Für den Bereich der offenen Systeme sollen einige Beispiele genannt werden:

- Sicherheitsarchitekturen
  ISO (International Standards Organisation) hat in einem Standard eine Sicherheitsarchitektur beschrieben. (ISO 7498-2)

– Sicherheitsprotokolle
IEEE (Institute of Electrical and Electronic Engineers) entwickelt einen Sicherheitsstandard für die Verbindungsschicht in einem LAN's (Local Area Network).
(IEEE 802.10)

– Sicherheitstechniken und -mechanismen
Der DES (Data Encryption Standard) wurde durch das NBS (National Bureau of Standards) standardisiert. Die ISO registriert mittlerweile nur noch Verschlüsselungsalgorithmen; es ist nicht beabsichtigt, diese zu standardisieren.
Als weitere Mechanismen, die standardisiert wurden, können bei der Authentifizierung die Empfehlungen von CCITT X.509, Hashfunktionen oder Unterschriftsmechanismen genannt werden.

– Anwendungen
Bei Anwendungen kann auf die Sicherheitsfunktionalität von CCITT X.400 verwiesen werden.

Es haben sich auch Interessengruppen gebildet, die in Teilbereichen tätig sind. TeleTrusT (Verein, der die Entwicklung einheitlicher technischer, organisatorischer und rechtlicher Maßnahmen anstrebt, mit dem Ziel, Telekooperation zwischen verschiedenen Partnern realisieren zu können) oder OSF (Open System Foundation) mit DCE (Distributed Computing Environment; geht auch auf die Sicherheit bei vernetzten UNIX-Rechern ein) können hier als Beispiele genannt werden. Für spezielle Probleme bieten alle großen und viele kleine Anbieter Lösungen an.

Fraglich ist, ob der Aufwand gerechtfertigt ist. In einer vom Bundesforschungsministerium in Auftrag gegeben Studie haben acht Institute unter Leitung des Fraunhoferinstituts für Systemtechnik und Innovationsforschung analysiert, welche Technologien zu Beginn des 21. Jahrhunderts entscheidend sein werden. Es wurden neun Gebiete mit 41 Themen genannt. Im Gebiet Software waren fünf Themen aufgeführt: Modellbildung und Simulation, Bioinformatik, nichtlineare Dynamik, unscharfe Logik (Fuzzy Logic) und Datensicherheit in Netzen.
Die Sicherheit in Kommunikationsnetzen zu erreichen, ist eine der wichtigsten Aufgaben für die Zukunft.

21.1.2
Betrachtungen zur Datensicherheit

Die Überlegungen zur Datensicherheit in Netzen lassen sich unter verschiedenen Gesichtspunkten anstellen. Die folgende Darstellung lehnt sich vorrangig an die Ansätze der ITSEC (Information Technology Security Evaluation Criteria) und der OSI-Sicherheitsarchitektur (ISO International Standard 7498-2: Open Systems Interconnection Reference Model – Part 2: Security Architecture; 1988) an.

21.1.2.1
Grundbedrohungen

Abhängig vom Zweck gibt es Bedrohungen, denen eine Kommunikation ausgesetzt ist:

– Verlust der Vertraulichkeit
Unter Vertraulichkeit von Informationen versteht man die Tatsache, daß die Informationen nur Befugten zugänglich sind und kein unbefugter Informationsgewinn stattfinden kann.

– Verlust der Integrität
Unter Integrität von Informationen versteht man die Tatsache, daß Informationen nur von Befugten in beabsichtigter Weise verändert und nicht unzulässig modifiziert werden können.

– Verlust der Verfügbarkeit
Mit Verfügbarkeit bezeichnet man den Tatbestand, daß Funktionen eines IT-Systems ständig innerhalb einer vorgegebenen Zeit, die von Funktion zu Funktion unterschiedlich sein kann, zur Verfügung stehen und die Funktionalität des IT-Systems nicht vorübergehend oder dauerhaft beeinträchtigt ist.

– Verlust der Verbindlichkeit
Verbindlichkeit bedeutet in diesem Zusammenhang, daß Informationen korrekt sind, die Nachweisbarkeit des Sendens und Empfangens gegeben ist, elektronische Unterschriften geleistet werden können und neutrale Gutachter existieren. Die Methoden und Verfahren müssen auch juristisch akzeptiert werden. Dies betrifft insbesondere vertragliche Transaktionen, die über Kommunikationssysteme zustande kommen.

– Verlust der Anonymität
Anonymität bedeutet die Möglichkeit, Transaktionen durchzuführen, ohne den anderen Institutionen die eigene Identität preisgeben zu müssen. Bei Streitigkeiten müssen die Transaktion und die beteiligten Partner rekonstruierbar sein. Die theoretische Möglichkeit, so zu verfahren, wurde nachgewiesen.

  Diese – aus Sicht des Datenschutzes wesentliche – Grundbedrohung wird oft nicht gesondert aufgeführt, sondern auch unter den „Verlust der Vertraulichkeit" gefaßt.

21.1.2.2
Angriffe auf Kommunikationsnetze

Die aufgeführten Bedrohungen beruhen auf Gefahren, denen ein Kommunikationsnetz ausgesetzt ist. Hier können höhere Gewalt, menschliches oder technisches Versagen genannt werden, wobei in den beiden letztgenannten Fällen zufällige oder bewußt herbeigeführte Gefahren auftreten können.

Durch die über Kommunikationsnetze übertragenen Daten werden ganz verschiedene Handlungen ausgelöst. So erfolgen bei Banküberweisungen aufgrund der Daten Geldzahlungen oder in Polizeinetzen werden sensible Daten von Personen übertragen. Es lassen sich viele weitere Beispiele aufführen, in denen Außenstehende Interesse daran haben können, auf die Kommunikation Einfluß zu nehmen. Man kann sich verschiedene Angriffe vorstellen, die zu diesem Zweck unternommen werden. Die Angriffe sollen am Beispiel dreier fiktiver Transaktionen in Kommunikationsnetzen dargestellt werden: einer Zahlungsanweisung in einem Bankennetz, einer Fahndungsmeldung in einem Polizeinetz und einer Bestellung bei einem Versandhaus. Allerdings darf daraus nicht geschlossen werden, daß tatsächlich existierende Netze dieser Institutionen die genannten Schwächen haben; es ist eher das Gegenteil der Fall.

- Abhören der Kommunikation; passiver Angriff

  Netzverwaltungsdaten werden abgehört, um später aktive Angriffe zu starten. Wenn Benutzerkennungen und nicht verschlüsselte Paßwörter erkannt werden, ist es später möglich, in die Identität der entsprechenden Person zu schlüpfen. Inhaltsdaten können zur Kenntnis genommen werden, etwa vertrauliche Schreiben.

- Wiederholen/Verzögern von Nachrichten

  Zahlungsanweisungen werden dupliziert.
  Die bewußte Verzögerung von Fahndungsmeldungen in polizeilichen Informationssystemen ist ebenfalls als Angriff gegen das Kommunikationsnetz zu betrachten.
  Eine Bestellung wird wiederholt, so daß mehr Waren als eigentlich bestellt geliefert werden.

- Einfügen/Löschen von Nachrichten

  Eine Zahlungsanweisung wird während der Übertragung eingefügt oder gelöscht.
  Ein Fahndungsersuchen wird gelöscht.
  Eine Bestellung wird gelöscht, d.h. es erfolgt keine Lieferung.

- Störung des Netzes

  Durch Überlastung des Netzes können keine Zahlungsanweisungen übertragen werden. Es wäre denkbar, mit einer an sich gesperrten Scheckkarte Geldbeträge abzuheben.
  Durch Störungen erreicht die Bestellung das Versandhaus zu spät. Die garantierte Lieferzeit kann nicht eingehalten werden.

- Modifikation der Daten

  In einer Zahlungsanweisung werden der Betrag oder der Empfänger geändert.
  Bei Fahndungsersuchen wird die Personenbeschreibung gefälscht.
  Eine Bestellung wird gefälscht.

- Vortäuschen einer Identität

  Ein Kommunikationsteilnehmer gibt sich als Bank A aus und veranlaßt Banküberweisungen.
  Ein Kommunikationsteilnehmer gibt sich als Polizeidienststelle aus und initiiert eine Fahndung.
  Bestellungen werden im Namen anderer Personen vorgenommen.

- Leugnen einer Kommunikationsbeziehung

  Eine angeschlossene Bank A behauptet, nie die Zahlungsanweisung von Bank B erhalten zu haben.
  Die Polizei gibt an, ein Fahndungsersuchen nicht erhalten zu haben.
  Das Versandhaus bestreitet, eine Bestellung erhalten zu haben.

- System-Anomalien

  Einschleusen von Programmviren o.ä., die zu Störungen des Netzes oder der angeschlossenen Rechner führen.

Auch wenn das folgende Beispiel, das Gegenstand einer Anfrage im Hessischen Landtag war, nicht ganz in den oben dargestellten Zusammenhang paßt, zeigt es doch Schwächen, die heute schon relevant werden können.

In der Presse hatte es Berichte gegeben, wie per Telefax Betrügereien vorgenommen wurden. Dazu wurden mit kopierten Briefköpfen per Telefax Bestellungen abgegeben. Da auf dem Telefax als Kopfzeile die Absenderangaben erschienen, wurden die Bestellungen als authentisch angesehen und die Lieferungen erbracht.

Die Kopfzeile kann in jedes Telefaxgerät eingegeben werden. Der Inhalt ist frei wählbar. Eine dort stehende Telefonnummer oder ein Absender müssen nicht authentisch sein. Die Betrüger hatten keine Mühe, eine andere Identität vorzutäuschen und darunter Lieferungen entgegen zu nehmen.

21.1.2.3
Sicherheitsdienste

Um diesen Angriffen zu begegnen, wurden fünf primäre Sicherheitsdienste bzw. Sicherheitsfunktionen in der ISO Sicherheitsarchitektur definiert. (In einer feineren Aufschlüsselung werden 14 Sicherheitsdienste beschrieben.)

- Authentisierung (auf Partnerebene)
  Garantie, daß während einer Datenübertragung auch tatsächlich die gewünschten Partner miteinander kommunizieren.

– Zugriffskontrolle
Ausschluß der unberechtigten Verwendung von Betriebsmitteln bei der Datenübertragung.

– Vertraulichkeit
Geheimhaltung der Daten während der Datenübertragung.

– Datenintegrität
An allen dazu erforderlichen Stellen bei der Übertragung müssen die relevanten Daten aus dem Datenstrom rekonstruierbar sein.

– Kommunikationsnachweis
Der Kommunikationsnachweis besteht aus zwei Teilen. Der Urheber eines Datenstroms muß identifiziert und authentisiert werden, der Nachweis über Ursprung und Empfang von Daten muß geführt werden. Die Problematik tritt insbesondere auf, wenn juristisch verbindliche Informationen ausgetauscht werden.

Als weiterer Sicherheitsdienst kann noch das Auditing (Protokollierung und Überwachung) genannt werden.

21.1.2.4
Sicherheitsmechanismen

Diese Sicherheitsfunktionen können durch technische und organisatorische Maßnahmen ausgeführt werden. Dabei werden bei der Implementierung der technischen Funktionen Sicherheitsmechanismen genutzt. Die Sicherheitsmechanismen werden in acht Klassen unterteilt, die den primären Sicherheitsdiensten wie folgt zugeordnet werden können:

	Authentisierung	Kommunikationsnachweis	Zugriffskontrolle	Vertraulichkeit	Datenintegrität
Verschlüsselung	×				×
elektronische Unterschrift	×	×			×
Zugriffskontrolle			×		
Datenintegrität		×			×
Authentisierungsmechanismen	×				
Fülldaten				×	
Routingkontrolle				×	
Notariatsmechanismen		×			

21.1.3
Anmerkungen zu einigen Klassen von Sicherheitsmechanismen

21.1.3.1
Verschlüsselung; technische Begriffe und Abläufe

Bis vor kurzem hatte die Kryptographie, also die Wissenschaft vom Verschlüsseln von Nachrichten, in der Öffentlichkeit den Ruf, nur vom Militär oder von Geheimdiensten eingesetzt zu werden. Diese Einschätzung muß revidiert werden. In den letzten Jahren haben die Fortschritte auf dem Gebiet der Kommunikationstechnologien die Kryptographie zu einer Schlüsselfunktion für einen sicheren Einsatz von Rechnern werden lassen. Ohne funktionierende Produkte für die Datensicherheit, die die Ergebnisse der Kryptographie nutzen, sind offene Rechnernetze in der Zukunft nicht denkbar. Diese Fortschritte führten auch für nicht vernetzte Rechner zu Produkten, welche die Datensicherheit verbessern. So können beispielsweise bei PC's und speziell bei Laptops alle auf der Festplatte gespeicherten Daten verschlüsselt werden, was die Risiken durch einen Diebstahl (u.a. Verlust der Vertraulichkeit) erheblich reduziert. Die Datenverschlüsselung ist Stand der Technik. Beim Erstellen von Sicherheitskonzepten sind deren Möglichkeiten in Betracht zu ziehen.

Ganz wesentlich haben zu dieser Entwicklung auch die Fortschritte der Rechnerleistung beigetragen. Es führte in der Vergangenheit beispielsweise bei PC's zu wesentlich schlechteren Anwortzeiten, wenn Daten in großem Umfang verschlüsselt wurden. Durch die jetzt vorhandenen Rechner mit Verarbeitungskapazitäten, die früher Großrechnern vorbehalten waren, ist der Performanceverlust bei gewissen Klassen von Verschlüsselungsalgorithmen tolerierbar.

Die bekannten technischen Lösungsansätze zur Verschlüsselung von Nachrichten beruhen auf der Kombination verschiedener Verschlüsselungsarten. Dabei werden sogenannte symmetrische und asymmetrische Verschlüsselungsalgorithmen kombiniert.

21.1.3.1.1
Symmetrischer (Verschlüsselungs-)Algorithmus

Ein symmetrischer Verschlüsselungsalgorithmus ist eine Vorschrift, nach der Daten ver- und entschlüsselt werden. Um die Operationen auszuführen, wird der Nachrichtentext sowohl bei der Ver- als auch bei der Entschlüsselung mit dem gleichen Schlüssel(wert) verarbeitet.

Symmetrische Algorithmen sind in der Regel schneller als asymmetrische Algorithmen. Wenn größere Datenmengen zu verschlüsseln sind, gelangen sie zum Einsatz. (Beispiel: DES; Data Encryption Standard.)

21.1.3.1.2
Asymmetrischer (Verschlüsselungs-)Algorithmus

Im Unterschied zum symmetrischen Algorithmus wird mit einem Schlüsselpaar statt eines einzigen Schlüssel(wertes) gearbeitet. Das Schlüsselpaar besteht aus einem allgemein zugänglichen öffentlichen Schlüssel (public-key) und einem, nur dem Eigentümer bekannten, geheimen Schlüssel (private-key). Wird eine Nachricht mit einem der beiden Schlüssel verschlüsselt, so kann die Nachricht nur mit dem passenden anderen Schlüssel entschlüsselt werden.

Asymmetrische Algorithmen sind rechenintensiv. Man bemüht sich, sie so einzusetzen, daß nur kleine Datenmengen verschlüsselt werden müssen. (Beispiel: RSA; nach den Forschern Rivest, Shamir, Adleman benannt.)

21.1.3.1.3
Verschlüsselte Kommunikation

Wenn eine Kommunikation verschlüsselt erfolgen soll, gibt es in Abhängigkeit vom eingesetzten Algorithmus unterschiedliche Abläufe.

Werden symmetrische Algorithmen eingesetzt, so muß zwischen den beiden Kommunikationsteilnehmern eine Absprache über den Algorithmus und den verwendeten Schlüssel erfolgen, bevor eine Nachricht ausgetauscht werden kann. Haben die Teilnehmer einen geheimen Schlüssel vereinbart, so verschlüsselt der Sender die Nachricht mit dem Schlüssel, und nur der Empfänger kann mit dem identischen Schlüssel die Ursprungsnachricht wiederherstellen.

Wird ein asymmetrischer Algorithmus verwendet, so ist es möglich, aus einem öffentlich zugänglichen Verzeichnis einen dem Empfänger zugeordneten Algorithmus mit dem öffentlichen Schlüssel zu entnehmen. Hierauf aufbauend wird die Kommunikation begonnen. Der Sender verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des Empfängers. Die Nachricht kann mit dem, nur dem Empfänger bekannten, geheimen Schlüssel des Empfängers entschlüsselt werden. Es ist nicht erforderlich, eine Absprache über die eingesetzten Schlüssel vor dem Austausch von Nachrichten zu treffen.

In beiden Fällen ist die Konsequenz, daß Nachrichten für Außenstehende nur mit erheblichem technischen Aufwand oder mit Kenntnis der benutzten Schlüssel eingesehen werden können.

Als Lösung für eine verschlüsselte Kommunikation in offenen Kommunikationsnetzen werden auch sog. Hybridverfahren angewandt. Der Kommunikationsaufbau erfolgt mittels asymmetrischer Verfahren. Dabei werden dann für jede Sitzung zufällig generierte Schlüssel für einen symmetrischen Algorithmus ausgetauscht. Es werden also die Vorteile beider Verfahren kombiniert.

21.1.3.1.4
Schlüsselmanagement

Unter Schlüsselmanagement ist die Generierung, Verteilung und Verwaltung von (Kommunikations-)Teilnehmerschlüsseln zu verstehen. Dies kann beispielsweise durch Ausgabe von Chipkarten und das Führen von Teilnehmerverzeichnissen geschehen.

– Probleme des Schlüsselmanagements bei offenen Netzen

Wollen mehrere Kommunikationsteilnehmer Nachrichten verschlüsselt übertragen, so muß vorher eine Absprache erfolgen, welcher Algorithmus und welcher Schlüssel benutzt werden sollen. Werden symmetrische Algorithmen verwendet, so ist je Teilnehmerpaar ein anderer Schlüssel erforderlich. Bei einer Anzahl von n Teilnehmern sind $((n \cdot n - n)/2)$ verschiedene Kommunikationsbeziehungen – und damit auch Schlüssel – möglich. Bei asymmetrischen Algorithmen wird dagegen je Teilnehmer ein Schlüsselpaar (geheimer und öffentlicher Schlüssel) benötigt. Wenn in einem Netz zwischen beliebigen Teilnehmern Daten ausgetauscht werden sollen, müssen beispielsweise für zehn, 1000 bzw. 100.000 Teilnehmer die folgende Anzahl von Schlüsseln vereinbart werden:

Algorithmus	Anzahl Schlüssel(paare) bei		
	10	1.000	100.000 Teilnehmern
symmetrisch	45	499.500	4.999.950.000
asymmetrisch	10	1.000	100.000

Es zeigt sich, daß in einem offenen Kommunikationsnetz nicht jede denkbare Kommunikationsbeziehung mit einem eigenen Schlüssel versehen werden kann. Daher wird die Aufnahme einer Kommunikationsbeziehung mittels asymmetrischer Algorithmen verschlüsselt. Anschließend ist es dann möglich, ganz gezielt weitere Schlüssel zu vereinbaren. Es sind dabei Voraussetzungen hinsichtlich der Verwaltung der öffentlichen Schlüssel zu erfüllen (vgl. unten: Zertifizierungsinstanz).

– Zertifizierungsinstanz

Um die asymmetrischen Verschlüsselungsverfahren in der Praxis einsetzen zu können, müssen einige Probleme gelöst werden. Problematisch sind beispielsweise die Erzeugung von Schlüsselpaaren und der Nachweis, daß ein öffentlicher Schlüssel authentisch ist.

Im ersten Fall bereitet es Schwierigkeiten, immer die nötige DV-Kapazität zur Verfügung zu halten, um Schlüsselpaare zu erzeugen. Im zweiten Fall muß sichergestellt werden, daß nicht ein Teilnehmer A seinen Schlüssel als den Schlüssel von B ausweisen kann, um dann die an B gerichteten verschlüsselten Nachrichten zu entschlüsseln.

Als Lösung werden derzeit Zertifizierungsinstanzen in Erwägung gezogen. Aufgaben dieser Instanzen wären insbesondere:

– Auf Antrag wird ein Schlüsselpaar erzeugt.
– Dem Antragsteller wird der geheime Schlüssel mitgeteilt oder auf einem anderen Weg zur Verfügung gestellt (z. B. über eine Chipkarte, die genutzt werden kann, ohne den Schlüssel selbst zu kennen).
– Der öffentliche Schlüssel wird allgemein zugänglich gemacht.
  Die Echtheit wird durch die Zertifizierungsinstanz mit einer Art elektronischen Unterschrift bestätigt.
  Damit ein Kommunikationsteilnehmer diese Unterschrift prüfen kann, muß der öffentliche Schlüssel der Zertifizierungsinstanz bekannt sein. Dieser muß in geeigneter Weise bekanntgegeben werden.

Es gibt Überlegungen, der Zertifizierungsinstanz noch weitere Aufgaben zuzuordnen, die sie zu einem „vertrauenswürdigen Dritten" machen würden. Hier sind zu nennen:

– Notariat, d.h. Nachweis, daß eine Nachricht gesendet und empfangen wurde.
– Anonymität bei Geschäftsvorfällen.
– Archivfunktionen.

21.1.3.1.5
Voraussetzungen für eine sicher verschlüsselte Kommunikation

Damit die genannten Abläufe tatsächlich die gewünschte Sicherheit erreichen, müssen bestimmte Voraussetzungen erfüllt werden. Hierzu gehören u.a.:

a) Die Algorithmen müssen praktisch sicher sein, d.h. es muß die Möglichkeiten eines „Angreifers" übersteigen, die Nachrichteninhalte zu entschlüsseln, bzw. die Kosten eines „Angreifers" müssen den zu erwartenden Gewinn übertreffen.

b) Die geheimen Schlüssel dürfen nur berechtigten Personen oder Institutionen bekannt sein bzw. zur Verfügung stehen.
  Im Fall der symmetrischen Algorithmen betrifft dies alle Schlüssel, im asymmetrischen Fall die geheimen Schlüssel.

zu a)
Es gibt Algorithmen, die z.Zt. nach dieser Definition als sicher betrachtet werden können. Der Begriff der Sicherheit ist aber relativ. Er hängt von der Situation ab, in der die Verschlüsselung eingesetzt wird, und neue technische oder mathematische Entwicklungen können die Kosten einer Entschlüsselung so verringern, daß sie wieder vertretbar werden.

zu b)
Bei den symmetrischen Algorithmen muß durch Vereinbarungen auf bilateraler Ebene erreicht werden, daß die Schlüssel geheim bleiben.
Bei asymmetrischen Verfahren gibt es neben dem Eigentümer eines Schlüssels die Zertifizierungsinstanz, die zumindest zum Zeitpunkt der Generierung dessen geheimen Schlüssel kannte. Die Zertifizierungsinstanz ist insoweit noch wichtiger, als sie im Prinzip von allen Eigentümern, deren geheime Schlüssel sie generiert hat, die Schlüssel kannte. Es muß sichergestellt sein, daß die Zertifizierungsinstanz nach der Schlüsselverteilung die geheimen Schlüssel nicht mehr kennt und mit ihrem Wissen allein nicht mehr rekonstruieren kann.

21.1.3.2
Elektronische Unterschrift

Die derzeitig diskutierten Abläufe zur Nutzung elektronischer Unterschriften benötigen eine Hashfunktion (Algorithmus zur Erzeugung von Zahlen, die ein Dokument charakterisieren), einen asymmetrischen Verschlüsselungsalgorithmus und ein zugehöriges Schlüsselpaar.

Um eine elektronische Unterschrift zu einem Dokument zu erzeugen, wird für das Dokument mit der Hashfunktion die charakteristische Zahl errechnet. Mit dem geheimen Schlüssel des Unterzeichners wird dieser Wert verschlüsselt und dann dem Dokument hinzugefügt.

Um die Echtheit eines Dokuments zu prüfen, wird die charakteristische Zahl des Dokuments errechnet und mit dem Wert der, mit dem öffentlichen Schlüssel, entschlüsselten Unterschrift verglichen. Bei Gleichheit wird die Unterschrift als authentisch betrachtet und das Dokument als echt anerkannt.

Eine elektronische Unterschrift unterscheidet sich in vielerlei Hinsicht von einer eigenhändigen Unterschrift. An dieser Stelle soll das Für und Wider nicht näher untersucht werden. Es bleibt aber festzustellen, daß der Gesetzgeber noch tätig werden und festlegen muß, in welcher Weise und in welchem Umfang der Entwicklung des elektronischen Rechtsverkehrs Rechnung getragen wird:

- Soll die elektronische Unterschrift generell neben und gleichwertig mit der eigenhändigen Unterschrift stehen?
- Soll die elektronische Unterschrift nur für rechtliche Teilgebiete bzw. neue Rechtsinstitute zugelassen werden?
- Ist ein Abgehen von der Rechtsdogmatik zur eigenhändigen Unterschrift und zur Urkunde möglich und sinnvoll?

21.1.3.3
Routingkontrolle

Um die Vertraulichkeit von Informationen zu verbessern, kann man die Übertragungswege so wählen, daß unbefugte Personen möglichst keinen Zugriff auf das Übertragungsmedium erhalten.

Bei LAN's sind derzeit broadcastorientierte Produkte wie Ethernet oder Token-Ring stark verbreitet. Dabei werden alle Informationen an sämtliche am Netz angeschlossen Endgeräte übertragen. Das jeweilige Endgerät entscheidet, ob eine Information an es gerichtet ist. Die oben geschilderten Angriffe werden dadurch sehr erleichtert.

Dem kann dadurch begegnet werden, daß durch Kopplungselemente wie Bridges oder Router Teilnetze gebildet werden, die auch unter dem Gesichtspunkt der Lastentkopplung wünschenswert sind. In den Teilnetzen werden Informationen weiterhin broadcastorientiert übertragen. Nach außen bzw. nach innen gelangen nur noch Informationen, die außerhalb bzw. innerhalb des Teilnetzes benötigt werden. Im Extremfall kann bei einer sternförmigen Verkabelung jedes Kabel – und damit Endgerät – über ein Kopplungselement ein Teilnetz bilden. Ein Abhörer kann dann nur noch Daten empfangen, die an sein Kabel/Endgerät gerichtet sind. Liegt ein Teilnetz in einem gesicherten räumlichen Umfeld, kann dadurch ein hoher Schutz erreicht werden. (Die räumliche Sicherung der Netzwerkkomponenten wie Verteilerschränke, Bridges, Router u.ä. ist besonders wichtig.)

Im Fall von Weitverkehrsnetzen spielt es ebenfalls eine Rolle, ob ein Angreifer überhaupt die gewünschten Informationen erhält. Wenn die Übertragungswege schnell wechseln und immer nur Bruchteile einer Information verfügbar sind, ist ein Angriff erschwert. Auch hier gilt es, die Stellen besonders zu schützen, an denen Informationen zusammenfließen oder ausgefiltert werden.

Es ist einsichtig, daß auch das Übertragungsmedium eine Rolle spielt, wenn die Vertraulichkeit von Daten erreicht werden soll. Es hängt beispielsweise vom Kabeltyp ab, welcher Aufwand erforderlich ist, um abzuhören. Als besonders unsicher muß hier die Funkübertragung gelten (vgl. 21. Tätigkeitsbericht, Ziff. 16.3.3.3), weil ein Abhörer sich nicht einmal mehr die Mühe machen muß, das richtige Kabel zu finden und anzuzapfen. Hier kann nur eine Verschlüsselung von Daten den benötigten Schutz erreichen.

21.1.3.4
Authentisierungsmechanismen

Üblich ist derzeit die Authentisierung, d.h. der Identitätsnachweis des Benutzers, gegenüber einem Rechner; diese kann durch die Eingabe eines Paßwortes/einer PIN geschehen, durch den Besitz einer Chipkarte oder durch die Prüfung biometrischer Merkmale wie den Fingerabdruck. Bei Geldausgabeautomaten muß beispielsweise eine Karte vorhanden sein und eine PIN eingegeben werden. Noch nicht üblich ist, daß sich der Rechner gegenüber dem Benutzer ausweist; ist es tatsächlich ein korrekt arbeitender Geldausgabeautomat?

In Kommunikationsnetzen, in denen gleichberechtigte Partner beteiligt sind, müssen sich alle Benutzer untereinander ausweisen können. Die Abläufe sind sehr viel komplizierter als bei der Arbeit mit einem einzigen Rechner. Auf eine Verschlüsselung kann nicht verzichtet werden, da die Informationen, mit denen sich ein Benutzer ausweist, höchst sensibel sind. Gelangen unbefugte Personen in den Besitz, so können sie sich als berechtigte Personen ausgeben. Ihre Aktionen würden dann der berechtigten Person zugerechnet.

Wenn es gelingt, eine Authentisierung zu überwinden und in eine fremde Identität zu schlüpfen, ist weder die Vertraulichkeit noch die Integrität oder die Verbindlichkeit gewährleistet.

21.1.3.5
Fülldaten

Aus Sicht des Datenschutzes ist es nicht nur wichtig, Kommunikationsinhalte gegen unberechtigte Zugriffe zu schützen. Ebenso wichtig ist es, die Kenntnis von Kommunikationsbeziehungen vor Unbefugten zu schützen. Um das zu erreichen, können mit Fülldaten zufällige Nachrichten übertragen werden. Aus einer Verkehrsflußanalyse

könnten dann keine Informationen gezogen werden. Aber auch hier kann das Ziel nur erreicht werden, wenn die Fülldaten verschlüsselt sind und daher nicht als solche erkannt werden.

21.1.3.6
Datenintegrität

Durch geeignete Mechanismen sollen unbemerkte Veränderungen der geschützten Daten verhindert werden. In der Regel ist es nicht möglich, eine Änderung zu verhindern, sondern es kann nur nachträglich festgestellt werden, daß eine Veränderung stattgefunden hat. Wird nur eine Veränderung festgestellt, so spricht man von verbindungsloser Integrität. Ist es auch möglich festzustellen, ob die Reihenfolge von Datenpaketen geändert wurde und Datenpakete hinzugefügt oder entfernt wurden, spricht man von verbindungsorientierter Integrität.

Um Veränderungen festzustellen, wird mit Prüfsummen gearbeitet, die kryptografisch geschützt werden müssen. Der Ablauf kann dabei dem einer elektronischen Unterschrift ähnlich sein. Soll die Integrität verbindungsorientiert erreicht werden, werden weitere Sicherheitsmechanismen genutzt. Ein Richtungsindikator zeigt an, ob ein Datenpaket gespiegelt und dem Absender zurückgesandt wurde. Eine Sequenznummer läßt erkennen, ob Datenpakete entfernt oder hinzugefügt wurden. Da dabei noch bekannt sein muß, welche Sequenznummern zur Anwendung gelangen, werden abschließende Sequenznummern ausgetauscht.

21.1.4
Beispiele für heute verfügbare Lösungen zu speziellen Problemen

Es ist noch ein weiter Weg, bis zur Lösung der Probleme entsprechende Produkte vorhanden sind. In einer Reihe von Fällen wurden mittlerweile Lösungen gefunden, auch wenn sie nicht unbedingt in allen Punkten vorhandenen Standards entsprechen.

Im Bankenbereich werden bei Geldautomaten oder im elektronischen Zahlungsverkehr Maßnahmen getroffen, welche die Integrität der Daten gewährleisten und Kommunikationsnachweise beinhalten.

Eine Datenverschlüsselung auf privaten Rechnernetzen wird teilweise bereits vorgenommen. Für X-25 Netze, aber auch in herstellerspezifischen Netzen, gibt es entsprechende Produkte, die dazu geeignet sind. Im Landesverwaltungsnetz Baden-Württemberg wurde ein Pilotversuch gestartet, inwieweit die Datensicherheit damit verbessert werden kann. Auch die DATEV (Dienstanbieter für Steuerberater) bietet ihren Kunden diese Dienstleistung an. Eine Konsequenz könnte sein, daß die sich aus der Nutzung von SK12-Knoten durch die Telekom ergebende Problematik, wie ich sie in meinem 14. Tätigkeitsbericht (Ziff. 8.3) beschrieben habe, entfiele.

Für LAN's, die Protokolle nach IEEE 802.3 nutzen, gibt es Kryptoboxen, die zwischen einem PC und dem Netzanschluß eingebaut werden können. Zwischen Kryptoboxen können die Daten verschlüsselt übertragen werden, ein Abhörer hätte keine Chance. Andere Produkte ver- und entschlüsseln auf den PC's die Daten, so daß die übertragenen Nutzdaten nicht zur Kenntnis genommen werden können.

In der baden-württembergischen Justizverwaltung, mit der DV-Abteilung des Oberlandesgerichts als koordinierender Stelle, wird getestet, ob Mahnanträge mit elektronischer Unterschrift versehen per Datenübertragung übermittelt werden können und dabei die gesetzlichen Vorgaben eingehalten werden. Dazu wird ein Produkt benutzt, welches Dateien mit einer elektronischen Unterschrift versehen und verschlüsseln kann. (Die Daten werden im File-Transfer-Modus der PC-Fax-Karte übertragen; das Fax-Protokoll ist lediglich der Transportmechanismus.) Dadurch wäre sichergestellt, daß der Inhalt des Antrags auf dem Übertragungsweg nicht geändert wurde und der Absender feststellbar ist.

Das Produkt erlaubt es auch, ein Telefax verschlüsselt an eine Person (Institution) zu schicken. Andere Personen können die Daten nicht entschlüsseln. Die in meinem 18. Tätigkeitsbericht (Ziff. 16.1) und 20. Tätigkeitsbericht (Ziff. 9.1.3) beschriebenen Probleme bei Telefax können dadurch weitgehend behoben werden. Voraussetzung ist, daß die Teilnehmer in einem öffentlichen Teilnehmerverzeichnis eingetragen sind und die Telefaxe mit entsprechend ausgerüsteten PC's übertragen und empfangen werden.

Das provet-Institut hat kürzlich ein Umfeld simuliert, in dem Rechtsanwälte durch elektronisch unterschriebene Dokumente kommunizieren. Dabei wurde getestet, inwieweit es möglich ist, elektronische Unterschriften zu manipulieren. Es gab eine Reihe von Angriffspunkten. Neben anderen Ansätzen wurden beispielsweise die Anwendungsprogramme so geändert, daß sie nicht den gesamten Text eines Dokumentes anzeigten. Der Unterzeichner versah dann auch ihm nicht angezeigte Teile des Dokumentes mit seiner elektronischen Unterschrift. Mit dieser und anderen Manipulationen konnten Sicherheitsvorkehrungen unterlaufen werden. In welchen Anwendungen die gefundenen Schwachstellen relevant sind und durch welche Maßnahmen die erkannten Lücken geschlossen werden können, sei dahingestellt.

Wenn die aufgezeigten Schwachstellen beseitigt sind, kann die elektronische Unterschrift in vielen Fällen sinnvoll genutzt werden. Aber auch jetzt bedeutet sie oft einen Gewinn an Datensicherheit, wie das Beispiel mit dem Telefax zeigt. Das Dokument ist bei der Übertragung geschützt, es kann nur vom vorgesehenen Empfänger zur Kenntnis genommen werden und der Absender ist identifizierbar. Ob der Absender das Originaldokument überträgt, muß

auch im jetzt üblichen Umfeld sichergestellt sein. Es ist kein Problem, welches erstmalig mit der elektronischen Unterschrift auftritt.

Aber der Einsatz der elektronischen Unterschrift ist in jedem Fall mit dem Restrisiko möglicher Manipulationen behaftet.

Beim Datenträgeraustausch ist es derzeit schon problemlos möglich, die Daten zu verschlüsseln. So arbeiten die Ämter für Regionalentwicklung, Landschaftspflege und Landwirtschaft mit einem entsprechenden Verfahren (vgl. Ziff. 19.2.2). Auf fast allen Rechnern gibt es Produkte, die den DES nutzen. Einige Anbieter haben bereits Hybrid-Verfahren entwickelt, die in spezielleren Konstellationen eingesetzt werden können. In jedem Fall müßten adäquate organisatorische Maßnahmen gewährleisten, daß das Sicherheitsmanagement, und dabei insbesondere das Schlüsselmanagement, funktioniert.

Fazit:
Auf dem Gebiet der Kommunikationssicherheit sind in der Praxis noch zahlreiche Probleme zu lösen. Die vorhandenen Produkte sind nicht in der Lage, allen Anforderungen gerecht zu werden, insbesondere beim Sicherheitsmanagement treten Schwierigkeiten auf. Der Stand der Technik ist aber so weit fortgeschritten, daß getroffene Sicherheitsmaßnahmen vor dem Hintergrund verfügbarer Lösungen nunmehr angepaßt werden müssen.

21.2
Prüfungen von Novell-Netzwerken

In meinem letzten Tätigkeitsbericht habe ich einen Teil der Möglichkeiten des Netzwerkbetriebssystems Novell Netware dargestellt, datenschutzgerechte Lösungen in den Bereichen der Nutzerverwaltung und der Zugriffsabgrenzungen zu realisieren (21. Tätigkeitsbericht, Ziff. 16.4).

Dem Grad der Einsatzhäufigkeit entsprechend lag auch in diesem Jahr ein Schwerpunkt meiner Prüfungstätigkeit bei derartigen Netzwerken. Die Ergebnisse der Prüfungen lassen vermuten, daß die Verwaltungen vor der Einführung von Netzwerken nicht die notwendigen Vorüberlegungen anstellen, die in ein entsprechendes Einführungskonzept einfließen müssen (vgl. 21. Tätigkeitsbericht, Ziff. 16.4.2).

Leider besteht hier immer noch nicht das notwendige Bewußtsein, daß zwischen dem Einsatz von mehreren Stand-alone-PCs und einem PC-Netzwerk ein wesentlicher qualitativer Unterschied, insbesondere unter Aspekten des Datenschutzes besteht. Hier kommt der Beratung im Vorfeld einer Netzwerkinstallation durch die beauftragten DV-Unternehmen eine wichtige Bedeutung zu. Diese Unternehmen sind in aller Regel durch ihre vielfältigen Erfahrungen in der Lage, ihren Kunden die notwendigen vorbereitenden Hinweise zu geben, welche grundsätzlichen organisatorischen Maßnahmen und datenschutzrelevanten Vorüberlegungen unumgänglich sind, um einen in jeglicher Hinsicht „einwandfreien" Betrieb eines PC-Netzwerkes über einen längeren Zeitraum hinweg zu gewährleisten.

In den mit den Prüfungen einhergehenden Beratungsgesprächen stellte ich fest, daß in den betreffenden Verwaltungen meist nur unzureichende Vorstellungen über die technischen und organisatorischen Rahmenbedingungen existieren, die vor der Einführung von Netzwerken abgeklärt werden müssen. Die Notwendigkeit für ein umfassendes Einführungskonzept wird somit oft gar nicht oder nicht im notwendigen Umfang erkannt.

Diese Notwendigkeit ist den Verwaltungen unter Umständen zunächst auch nicht sofort einsichtig, denn bei kleineren Netzwerken lassen sich viele, nicht nur datenschutzrelevante, Probleme noch ohne großen Aufwand sofort beheben, so daß das Fehlen einer Konzeption noch nicht bemerkt wird.

Aber DV-Netze haben die Eigenschaft zu wachsen. Und irgendwann, spätestens bei einem Wechsel des Systembeauftragten, wird dann deutlich, daß Systemeinstellungen nicht dokumentiert wurden oder z. B. die Vergabe von Zugriffsrechten nicht mehr nachvollziehbar ist. Derartige Probleme haben sich auch bei den einzelnen Prüfungen gezeigt.

21.2.1
Prüfungsfeststellungen

Insgesamt habe ich bei allen Prüfungen von Netzwerken Mängel bei der Benutzerverwaltung gefunden. Dazu zählen:

- fehlender Paßwortzwang;
- zu kurze Paßwörter;
- fehlender Paßwortwechsel;
- Paßwortverwaltung und -wechsel nur durch den Supervisor;
- fehlende Notfallkennung (einschließlich organisatorischer Regelungen);
- Vermischung unterschiedlicher Aufgaben in einer Kennung (z. B. Anwendungs- und Supervisor-Tätigkeit).

Ein weiterer Bereich, in dem ich fast immer mehr oder weniger gravierende Mängel vorfand, waren die Zugriffsabgrenzungen zu den Datenbeständen. Der freie Zugriff von der DOS (Betriebssystem)-Ebene auf die Textverarbeitung

einer Personalstelle war ein besonders unrühmlicher Höhepunkt in diesem Teilbereich. Generell ist hier zu bemerken, daß in den meisten Fällen die Vorgaben für den Ablauf und die Dokumentation bei der Zuweisung von Zugriffsrechten fehlen oder unzureichend sind. Darüber hinaus fehlten oft organisatorische Regelungen zur Datensicherung, zum Umgang mit anfallenden Protokollen oder zu Fragen der räumlichen Zugangssicherung.

Häufig werden diese Fragen erst dann behandelt, wenn der Personalrat einige Zeit nach der Erstinstallation auf den Abschluß einer Dienstvereinbarung zur Einführung des Netzwerkes drängt und bei dieser Gelegenheit über eine entsprechende Dienstanweisung nachgedacht werden muß.

21.2.2
Gespräche mit dem Kommunalen Gebietsrechenzentrum (KGRZ) Kassel

Da ein Teil der geprüften Verwaltungen vom KGRZ Kassel betreut wird, habe ich mit diesem stellvertretend für alle anderen betreuenden Unternehmen Gespräche geführt, um festzustellen, wo sich aus Sicht des KGRZ Probleme bei der Einführung und Pflege von Netzwerken ergeben, die als Ursachen für die von mir festgestellten Mängel anzusehen sind.

Dabei ergab sich, daß das KGRZ zu dieser Zeit mit einer Partnerfirma, die im Auftrag des KGRZ bei den Verwaltungen tätig ist, einen internen Leitfaden über die Vorgehensweise bei Netzwerkinstallationen diskutierte. Das KGRZ stimmte mir aus eigener Erfahrung zu, daß dem vorbereitenden Aspekt bei der Einführung von Netzwerken eine größere Bedeutung zuzumessen ist. Aus der Sicht des dienstleistenden Unternehmens ist dies schon allein deshalb sinnvoll, um umfangreiche Nachbesserungen zu vermeiden.

Das KGRZ Kassel hat meine Anregungen aufgegriffen und will den oben angesprochenen Leitfaden in einer unter Datenschutzaspekten abgestimmten Version zur Grundlage zukünftiger Netzwerkinstallationen machen. Dabei soll insbesondere im Vorfeld der Installation anhand eines Maßnahmenkatalogs der auftraggebenden Verwaltung ein Überblick über die notwendigen organisatorischen Regelungen und die anstehenden Vorbereitungen zur technischen Administration eines Netzwerkes gegeben werden.

Ein solcher Maßnahmenkatalog ist natürlich auch für alle anderen Diensteanbieter in gleicher Weise von Interesse. Ich beabsichtige daher, diesen Katalog bei geeigneter Gelegenheit mit den anderen Rechenzentren zu erörtern, um eine im Hinblick auf den Datenschutz weitgehend gleiche Einführung von Netzwerken zu erreichen.

21.3
Heimarbeit im Bereich der Produktionssteuerung von Rechenzentren

Der Datenschutzbeauftragte eines Rechenzentrums hat sich mit einer Anfrage zur Heimarbeit von Mitarbeitern der Produktionssteuerung an mich gewandt. Es war geplant, daß einige Mitarbeiter mittels eines PC's oder Terminals vom häuslichen Arbeitsplatz aus auf die in ihrem Verantwortungsbereich liegenden Abrechnungsläufe zugreifen können.

Das Rechenzentrum sah sich durch betriebliche Abläufe zu dieser Maßnahme gezwungen. An den Rechner waren ca. 1.200 Terminals angeschlossen. In der Zeit von 7.00 Uhr bis 19.00 Uhr stand der Rechner den Anwendern Online zur Verfügung. Aus Performancegründen, und weil verschiedene Abläufe einander ausschließen, gab es noch eine Reihe von Programmen, die nach Ende der Online-Zeiten abliefen. Diese Programme (Datensicherung, Änderungsläufe, Drucken usw.) mußten in der Zeit von 19.00 Uhr bis 6.00 Uhr beendet sein, damit den Anwendern die Verfahren mit aktuellen Daten wieder zur Verfügung standen. Hierzu wurde im Operating (Rechnerbedienung) mit drei Schichten gearbeitet.

Die Laufzeit einiger Verfahren war im Nachtbetrieb so lang, daß bei kleinen Abweichungen, beispielsweise durch Jobfehler verursacht, die garantierten Zeiten für den Online-Betrieb teilweise nicht eingehalten werden konnten. Zu diesen Verfahren gehörten das Finanzwesen und das Personalwesen. Die verantwortlichen Mitarbeiter der Produktionssteuerung, die zur Fehlerbehebung anreisen mußten, brauchten 30 Minuten und mehr, um im Rechenzentrum zu sein. Dies war aus Sicht des Betreibers nicht akzeptabel.

Im Spannungsfeld zwischen garantierten Online-Zeiten und dem Ziel, Personal im Bereich der Produktionssteuerung einzusparen, wurde ein Teleservice geplant. Danach könnten die Mitarbeiter im Fehlerfall vom häuslichen Arbeitsplatz aus tätig werden. In vielen Fällen würde dies bedeuten, daß wegen der weggefallenen Fahrzeiten die Abläufe noch korrekt beendet würden. Es blieben allerdings immer noch Konstellationen, in denen die Fahrt ins Rechenzentrum nötig wäre oder die Abläufe am nächsten Tag wiederholt werden müßten.

Die Produktionssteuerung hatte die Forderung erhoben, im Rahmen des Teleservice die gewohnten Zugriffsrechte zu bekommen. Folglich könnten alle Verarbeitungsergebnisse angesehen, alle Jobs geändert, die Jobs gestartet werden, und es wäre der Zugriff auf Produktionsdateien möglich.

Aus Sicht des Datenschutzes sind solche Planungen bedenklich. Die Probleme konzentrieren sich dabei auf die Umsetzung angemessener Datensicherungsmaßnahmen nach § 10 HDSG. Zur rechtlichen Einordnung ist anzumerken, daß keine Datenverarbeitung im Auftrag und keine Datenübermittlung vorliegt. Der Heimarbeitsplatz ist ein

Arbeitsplatz der datenverarbeitenden Stelle. Die geplante Konstellation ähnelt in den Abläufen und bei der Betrachtung von Risiken für die Datensicherheit weitgehend einer Fernwartung. Was Maßnahmen gegen Eingriffe unberechtigter Personen auf den Rechner oder auf das Kommunikationsnetz betrifft, so sind diese vergleichbar.

Schwierigkeiten ergeben sich im Rahmen einer Heimarbeit beim häuslichen Arbeitsplatz. In den Rechenzentren wird durch eine ausgefeilte Zugangskontrolle nicht-berechtigten Personen der Zutritt zu sensiblen Bereichen wie der Produktionssteuerung verwehrt. Bei der Heimarbeit hingegen kann die datenverarbeitende Stelle keinen direkten Einfluß darauf nehmen, welche Personen sich am Arbeitsplatz aufhalten. Der Mitarbeiter bestimmt, wer sich in seiner Wohnung aufhält. Konsequenzen können sich für die Speicherkontrolle, die Benutzerkontrolle und den Zugang zu dem vor Ort installierten Rechner ergeben.

Es ist im Prinzip nicht auszuschließen, daß unbefugte Personen das Endgerät benutzen oder dem Mitarbeiter bei der Arbeit zusehen. Die Kenntnisnahme sensibler personenbezogener Daten kann durch von der datenverarbeitenden Stelle getroffene bauliche, technische und organisatorische Maßnahmen daher nicht in jedem Fall unterbunden werden. Der Mitarbeiter muß die zwischen ihm und seinem Arbeitgeber festzulegenden Vorkehrungen umsetzen.

Ein weiteres Manko betrifft die Kontrollmöglichkeiten der datenverarbeitenden Stelle und durch den Hessischen Datenschutzbeauftragten. Wenn Datensicherungsmaßnahmen ergriffen werden, müssen diese kontrolliert werden können und kontrolliert werden. In der vorliegenden Konstellation ergeben sich Probleme, wenn in der Wohnung des Mitarbeiters die dort getroffenen Maßnahmen geprüft werden sollen. Der Zutritt zur Wohnung ist nur mit der Zustimmung der Bewohner möglich. Dies gilt auch, wenn wegen eines Verdachts eine unangemeldete Prüfung erfolgen soll. Ob unter diesen Voraussetzungen eine ausreichende Kontrolle gegeben ist, bedarf noch einer weitergehenden Prüfung.

Die Frage, ob eine Heimarbeit zulässig ist, muß auch unter Berücksichtigung der Sensibilität der Daten beantwortet werden. Handelt es sich um Daten, die besonderen Berufs- und Amtsgeheimnissen unterliegen, so muß ein anderer Maßstab angelegt werden als bei weniger sensiblen Daten. Es wäre kaum nachvollziehbar, wenn es Mitarbeitern der Verwaltung untersagt ist, Akten mit nach Hause zu nehmen, der Mitarbeiter der Produktionssteuerung aber auf erheblich mehr Daten vom heimischen Arbeitsplatz aus ohne weiteres zugreifen kann.

Ohne eine endgültige Aussage treffen zu können, unter welchen Voraussetzungen eine Heimarbeit zulässig ist, gibt es doch Anforderungen, die in jedem Fall erfüllt sein müssen:

- Es muß erforderlich sein, die Tätigkeit als Heimarbeit durchzuführen.
- Unter Berücksichtigung der mit einer Heimarbeit verbundenen Risiken muß der Verzicht auf die Heimarbeit zu nicht tragbaren Konsequenzen führen.
- Die Verantwortung für die Einhaltung der Sicherungsmaßnahmen trägt die datenverarbeitende Stelle.
- Es muß festgelegt werden, welche Sicherungsmaßnahmen zu ergreifen sind. Dies gilt insbesondere für den heimischen Arbeitsplatz.
- Wird für andere Stellen eine Datenverarbeitung im Auftrag vorgenommen, so sind die Auftraggeber zu informieren, daß und in welchem Umfang Heimarbeit stattfindet. Die getroffenen Sicherungsmaßnahmen sollten geschildert werden.
- Die räumlichen Gegebenheiten in der Wohnung müssen es prinzipiell erlauben, den Zugang unbefugter Personen zum PC bzw. zum Terminal zu verhindern.
- Die Zugriffsmöglichkeiten sind auf das unbedingt erforderliche Maß zu reduzieren. Ein Zugriff auf personenbezogene oder andere sensible Daten ist so weit wie möglich auszuschließen.
- Als Endgerät sollte nur ein Terminal genutzt werden. Wird ausnahmsweise ein PC eingesetzt, so muß dieser so gesichert sein, daß er nur für die Heimarbeit genutzt werden kann.
- Es muß protokolliert werden, wann auf welche Daten zugegriffen wurde.
- Die übertragenen Daten sind zu protokollieren.
- Die Abläufe der Heimarbeit müssen im Rahmen einer Revision geprüft werden.
- Es muß festgestellt werden, ob die tatsächlich vorgenommenen Tätigkeiten, und damit die Zugriffe auf personenbezogene Daten, im Einzelfall erforderlich waren.
- Es sind Maßnahmen gegen Eingriffe unbefugter Personen auf den Rechner oder die Kommunikationsverbindung zu treffen (vgl. 20. Tätigkeitsbericht, Ziff. 15.1).

Fazit:
Die datenverarbeitenden Stellen sehen sich verschiedenen Anforderungen gegenüber:

- Die Zeiten, zu denen das Hilfsmittel EDV zur Verfügung stehen muß, werden länger.
- Die Leistungen sollen wirtschaftlicher erbracht werden. Es soll folglich kein zusätzliches Personal eingestellt werden.

– Es wird versucht, dem Personal flexiblere und humanere Arbeitsmöglichkeiten zu bieten.

Eine Lösung, die in einigen Konstellationen sinnvoll eingesetzt werden kann, ist die Heimarbeit. Sie dürfte von den Betroffenen in vielen Fällen als wünschenswert angesehen werden, darf aber nicht dazu führen, daß den Erfordernissen des Datenschutzes nicht mehr genügt werden kann.

21.4
Einsatz von Software zur Fernsteuerung in PC-Netzen

Vor einiger Zeit fragte ein Datenschutzbeauftragter an, welche Anforderungen an den Einsatz von Software zur Fernsteuerung von Rechnern gestellt werden. In seiner Institution war ein PC-Netz mit mehr als 100 PC's auf einem weitläufigen Gelände installiert. Mit der Betreuung der etwa 200 Benutzer waren ein Netzwerkadministrator und dessen Vertreter betraut. Diese mußten im Fehlerfall, oder wenn die Benutzer in der Handhabung von Geräten und Programmen nicht sicher waren, den Benutzern helfen. Obwohl es sich um einheitlich ausgestattete Arbeitsplätze handelte, gab es häufig Probleme, die nicht am Telefon geklärt werden konnten. Die Betreuer mußten zur Unterstützung die Arbeitsplätze der Benutzer aufsuchen. Es geschah oft, daß sie, wenn um eine Unterstützung gebeten wurde, unterwegs waren. Auch kamen sie nicht im gewünschten Umfang zu ihrer eigentlichen Tätigkeit, der Netzwerkadministration.

Um den Aufgaben wieder besser nachkommen zu können, wurde überlegt, ein Programm zur Fernsteuerung von PC's, oft „Remote-Control-Software" genannt, einzusetzen. Dieser Begriff kann irreführend sein, wenn ein Programm nur lesende Zugriffe erlaubt, aber keine steuernden Eingriffe. Im weiteren wird trotzdem von Fernsteuerung die Rede sein, da im Regelfall die Programme auch Eingriffsmöglichkeiten bieten. Eine derartige Software erlaubt es prinzipiell, vom Arbeitsplatz eines Betreuers aus fremde Rechner in einem Netz zu steuern. Je nachdem, welche Funktionalität die Software bietet, kann dies beispielsweise bedeuten, daß der Betreuer von dem gesteuerten Rechner

– eine Übersicht der Hardkomponenten und der gerade aktiven Software erhält,
– den Bildschirm angezeigt bekommt,
– die Tastatur blockieren kann,
– die Bedienung übernehmen kann,
– auf Dateien zugreifen oder
– den gesteuerten Rechner booten (neu starten) kann.

Hieraus ergibt sich eine Reihe von Mißbrauchsmöglichkeiten:

– Es wäre dem Betreuer möglich, die Tätigkeit von Mitarbeitern zu verfolgen, d.h. ein Mißbrauch im Sinne einer unzulässigen Leistungskontrolle ist denkbar.
– Der Betreuer könnte unzulässigerweise auf Daten zugreifen.
– Schutzmaßnahmen könnten umgangen werden.
  Wird beispielsweise eine Verschlüsselung von Benutzerdaten vorgenommen, so könnte der Betreuer die unverschlüsselten Daten am Bildschirm sehen oder evtl. die Eingabe der Schlüsselwerte verfolgen.

Die Mißbrauchsmöglichkeiten sind den Softwareentwicklern bewußt, so daß praktisch alle angebotenen Produkte Schutzfunktionen beinhalten. Je nach Produkt sind die Schutzfunktionen aber unterschiedlich und können in vielen Fällen bei der Installation teilweise ausgeschaltet werden.

Eine allgemeine Aussage, ob der Einsatz einer Fernsteuerungssoftware datenschutzrechtlich zulässig ist, kann ich nicht treffen. Hierzu ist die Erforderlichkeit im Einzelfall zu prüfen, und es sind eine Reihe von Forderungen an die Software und das organisatorische Umfeld zu erfüllen. Da die Ausgangslage einer Fernwartung ähnelt, treffen auch hier die grundsätzlichen Überlegungen zu, die ich im 20. Tätigkeitsbericht (Ziff. 15.1) dargelegt habe.

Damit der Einsatz einer derartigen Software zulässig sein kann, ist folgendes zu gewährleisten:

– Der Einsatz muß angemessen sein.

  Auf den Einsatz kann verzichtet werden, wenn ein Betreuer innerhalb kurzer Zeit die Arbeitsplätze der Benutzer erreichen kann. Eine Hilfe vor Ort ist in der Regel besser und wirkungsvoller.

– Zu klären ist, welche Funktionen die Software haben muß und welche sie nicht haben darf.

  Bietet eine Software Funktionen, die nicht vorhanden sein dürfen, und sind diese nicht auszuschalten, ist vom Einsatz abzusehen.

– Zu gewährleisten ist, daß die Fernsteuerung nur mit Wissen und Wollen des Benutzers begonnen werden kann.

  Im allgemeinen gibt es jeweils ein Programm für den steuernden Rechner und eines für den gesteuerten lokalen Rechner. Damit die Fernsteuerung beginnen kann, müssen beide Programme aktiv sein. Der Benutzer kann die

Fernsteuerung dann kontrolliert anfordern, wenn er zuerst das Programm auf dem lokalen Rechner aufrufen muß.

Nicht akzeptabel ist, wenn das Programm auf dem zu steuernden Rechner ohne Einfluß durch den Benutzer, z. B. beim Rechnerstart, aktiviert wird.

– Es muß klar erkennbar angezeigt werden, wenn eine Fernsteuerung stattfindet.

In der Regel wird im Fall einer Fernsteuerung eine Meldung oder ein Symbol auf dem Bildschirm angezeigt. Diese Anzeige muß während der gesamten Dauer der Tätigkeit sichtbar sein. Der Benutzer ist darauf hinzuweisen, welche Bedeutung die Anzeige hat.

Kann die Anzeige wahlweise unterdrückt werden, muß bei der Installation und durch Kontrollen im Rahmen der Revision sichergestellt werden, daß die Anzeige immer erfolgt.

– Nach einer Fernsteuerung sollte es möglich sein, das Steuerprogramm auf dem lokalen Rechner wieder zu deaktivieren.

Kann das Steuerprogramm im laufenden Betrieb nicht deaktiviert werden, so muß ein Neustart des Rechners die Fernsteuerung beenden können.

– Der Zugriff auf Dateien und Verzeichnisse sollte unterbunden werden können.

Größte Vorsicht ist geboten, wenn mit dem Fernsteuerungsprogramm ein Zugriff auf Dateien des lokalen Rechners möglich ist. In diesem Fall sollte die Software die Möglichkeit bieten, den Zugriff einzuschränken.

– Nur berechtigten Personen darf es möglich sein, die Software zu benutzen.

Die Programme müssen in Bereichen gespeichert sein, auf die nur die berechtigten Personen zugreifen können. Außerdem sollten diese Programme Benutzerkennungen und Paßwörter abfragen, bevor sie arbeiten.

– Es müssen Protokolle erstellt werden, wann wer welche Funktionen auf welchem Rechner ausgeführt hat.

Am günstigsten wäre, wenn diese Protokolle automatisiert erzeugt würden. Anderenfalls sind die Protokolle manuell zu führen. Die Protokolle müssen dahingehend ausgewertet werden, ob die Software nur bestimmungsgemäß eingesetzt wurde. Eine weitergehende Auswertung ist nach § 13 Abs. 5 Hessisches Datenschutzgesetz unzulässig.

– Schließlich müssen organisatorische Regelungen getroffen werden, um den zulässigen Einsatz der Software zu gewährleisten.

Kontrolliert werden muß insbesondere, ob die Software richtig implementiert ist, d.h. ob nur die vorgesehenen Funktionen ausführbar und die Sicherheitsmechanismen eingeschaltet sind.

Durch die weiter fortschreitende Ausstattung von Arbeitsplätzen mit Rechnern wird der Bedarf an fachkundiger Unterstützung steigen. Wegen der finanziellen Engpässe in allen Bereichen der öffentlichen Verwaltung ist zu befürchten, daß für die Benutzerunterstützung kein weiteres Personal eingestellt wird. Es dürfte daher verstärkt über die Nutzung von Hilfsmitteln nachgedacht werden, welche die Effizienz steigern. Hierzu gehört die Fernsteuerungssoftware. Das Problem des datenschutzgerechten Einsatzes derartiger Hilfsmittel wird sich in steigendem Maße stellen.

22. Bilanz

22.1
Anträge der Polizei an Gesundheitsaufsicht und Gesundheitsamt mit dem Ziel „lästige Anzeigeerstatter" zu überprüfen (21. Tätigkeitsbericht, Ziff. 4.2)

Der Fall von Frau D. aus Frankfurt – über sie hatte die Polizei Daten über eine vermeintliche psychische Erkrankung ohne Rechtsgrundlage an das Sozialamt – Sozialpsychiatrischer Dienst – sowie an das Gesundheitsamt – Abteilung Psychiatrie – und gemäß § 22 Abs. 1 Hessisches Gesetz über die öffentliche Sicherheit und Ordnung an die für Maßnahmen nach dem Hessischen Freiheitsentziehungsgesetz zuständige Ordnungsbehörde übermittelt – hat sich wie folgt entwickelt:

Das Sozialamt habe ich darauf hingewiesen, daß die Mitteilung der Polizei über Frau D. und damit auch jegliche Weiterverarbeitung dieser Daten durch das Sozialamt unzulässig waren. § 19 Abs. 4 Hessisches Datenschutzgesetz (HDSG) regelt, daß solche Daten zu löschen sind. Das Sozialamt teilte mir mit, daß es die Unterlagen über Frau D. vernichtet hat.

Das Gesundheitsamt konnte einen Vorgang über Frau D. nicht auffinden. Jedenfalls teilte es mir mit, es existiere weder eine Akte noch eine Karteikarte über Frau D.

Dem Ordnungsamt habe ich mitgeteilt, daß das Hessischen Freiheitsentziehungsgesetz keine ausreichende Rechtsgrundlage dafür bietet, Personen nach dem Geisteszustand ihrer Nachbarn zu befragen. Nur wenn im Einzelfall der Schutz von Leben und Gesundheit dies gebietet (§ 12 Abs. 3 HDSG) ist dieses Vorgehen gerechtfertigt. Weiterhin hielt ich die vorgesehene Aufbewahrungsdauer der Akte und der dazugehörigen Karteikartei von zehn Jahren für zu lange. Es antwortete mir, künftig, von Ausnahmefällen abgesehen, auf Nachbarschaftsbefragungen zu verzichten. Die vorgesehene Aufbewahrungsdauer wurde auf fünf Jahre verkürzt. Es stützte sich dabei auf die „Aufbewahrungsbestimmungen für Akten und sonstiges Schriftgut der Dienststellen des Landes Hessen" (StAnz. 1986 S. 2107 ff., Ziff. 6.1). Auf meine Entgegnung, daß bei Anwendung dieses Erlasses eine Aufbewahrungsdauer von einem Jahr (Ziff. 8.1 a.a.O) naheliegt, hat das Ordnungsamt der Stadt Frankfurt noch nicht geantwortet.

22.2
Justizprüfungsamt (21. Tätigkeitsbericht, Ziff. 5.4)

Im Rahmen eines Gesprächs mit dem Justizprüfungsamt wurden einvernehmlich bestimmte Grundsätze für die Ausgabe von Prüfungsakten entwickelt.

Danach müssen Akten, die ohne Schwierigkeiten anonymisierbar sind, auch anonymisiert ausgegeben werden. In den übrigen Fällen sollen die Verfahrensbeteiligten davon unterrichtet werden, daß die Ausgabe als Prüfungsakte beabsichtigt ist. Werden Einwendungen dagegen erhoben, wird geprüft, ob überwiegende Interessen des Betroffen der Ausgabe entgegenstehen.

Die Ausgabe der Akten erfolgt an einem anderen Ort, als sich der Fall abgespielt hat. Dies gilt insbesondere dann, wenn Personen, die im öffentlichen Leben stehen und deshalb erkannt werden könnten, beteiligt sind.

Aktenteile, deren Kenntnis für die Lösung des Falles nicht erforderlich sind, wie Spurenakten usw., werden nicht ausgegeben. Akten, die beispielsweise Straftaten gegen die sexuelle Selbstbestimmung betreffen, werden wegen der besonderen Schutzwürdigkeit der in dieser Akte verarbeiteten Daten nach Möglichkeit nicht ausgegeben. In Fällen, die der Sozial- oder Finanzgerichtsbarkeit unterliegen, wird vor Ausgabe der Akten immer das Einverständnis der Betroffenen eingeholt.

22.3
Verordnung über den automatisierten Abruf von Daten aus dem Liegenschaftskataster (21. Tätigkeitsbericht, Ziff. 14.2).

Im letzten Tätigkeitsbericht hatte ich über den Verordnungsentwurf der Landesregierung zum automatisierten Abruf von Daten aus dem Liegenschaftskataster berichtet.

Dieser Entwurf ist mit kleinen Änderungen am 1. August 1993 in Kraft getreten (GVBl. I S. 280). So wurde auf meine Anregung hin noch der Katalog der abrufbaren Daten um das Merkmal „Beruf" reduziert. Allerdings bleibt es dabei, daß bei den zum Abruf bereitgehaltenen Daten nur eine Trennung zwischen Eigentümerdaten einerseits und Flurstückdaten andererseits möglich gemacht wird. Die von mir geforderte Datentrennung auch innerhalb dieser beiden Datengruppen auf den jeweils erforderlichen Umfang ist nicht realisiert worden. Begründet wurde dies erneut damit, daß eine solche Trennung mit den zur Verfügung stehenden Programmen nicht möglich sei. Eine Änderung sei erst mit Nachfolgeprogrammen realisierbar, die allerdings erst in fünf bis zehn Jahren zur Verfügung stünden.

22.4
BOS-Funk, schnurlose Telefone (21. Tätigkeitsbericht, Ziff. 16.3)

22.4.1
BOS-Funk

In meinem 21. Tätigkeitsbericht hatte ich von den Folgen berichtet, die sich aus dem Abhören von Funkgesprächen ergeben können. Besonders hingewiesen hatte ich auf den Bereich des BOS-Funks (BOS: „Behörden und Organisationen mit Sicherheitsaufgaben"; z. B. Polizei oder Rettungsdienste). Das gleiche Problem stellt sich auch für Privatpersonen, die schnurlose Telefone oder Funktelefone des B- und C-Netzes benutzen. Obwohl die Möglichkeit zum Abhören schon immer bestand, hatte sich die Lage Mitte 1992 durch die Umsetzung einer EG-Richtlinie verschärft, welche die Liberalisierung des Marktes für Rundfunkgeräte brachte.

Nunmehr können legal sog. Scanner erworben werden. Scanner sind (Rund-) Funkempfänger für einen weiten Frequenzbereich, in dem z. B. der BOS-Funk oder schnurlose Telefone senden. Das Abhören des Polizeifunks, von Rettungsdiensten oder eben auch normalen Telefonaten war damit möglich.

Die sich ergebenden Probleme wurden nicht nur von Datenschutzbeauftragten erkannt. Auch die Innenminister des Bundes und der Länder haben sich damit befaßt. Die Folgen für die Arbeit der Polizei wurden als so gravierend erachtet, daß ein Ad-hoc-Ausschuß der technischen Kommission gebildet wurde. Der Ausschuß beschäftigt sich mit der Frage, wie der Funkverkehr gesichert werden kann. Unabhängig von den Ergebnissen der Arbeitsgruppe sind bereits einige Länder tätig geworden, um Lösungen zu suchen.

In einem Bundesland wurde mittlerweile damit begonnen, die Funkgeräte der Polizei mit einem Modul auszustatten, das einen gewissen Schutz gegen Mithörer bietet. Es gibt jedoch bereits Scanner, die im Standard so ausgestattet sind,

daß diese Maßnahme aufgehoben wird. Diese Lösung ist daher kaum geeignet, die Vertraulichkeit im erforderlichen Maß zu gewährleisten; vielmehr müssen andere technische Lösungen gesucht werden, die für die Polizei tauglich sind. Derzeit wird in Hessen in einem Pilotversuch bei der Polizeidirektion Limburg ein Produkt auf seine Praxistauglichkeit untersucht, das einen wesentlich besseren Schutz ergeben soll. In einem weiteren Bundesland läuft ein ähnlicher Versuch mit einem anderen Produkt. Ausgehend von den gewonnenen Ergebnissen soll dann entschieden werden, welche Lösung für die hessische Polizei eingeführt wird.

So wichtig es ist, die Polizei mit den erforderlichen Geräten auszustatten: Auch der Bereich der anderen Organisationen, die den BOS-Funk nutzen, wie Rettungsdienste, muß abgedeckt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat deshalb in ihrer 46. Sitzung eine „Entschließung zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten" gefaßt, auf die ich verweisen möchte (vgl. 23.6).

22.4.2
Funktelefone und schnurlose Telefone

Für Funktelefone des B-, C- und D-Netzes hat sich die Lage zwischenzeitlich nicht geändert. Das D-Netz ist weitestgehend abhörsicher, das C-Netz nur sehr eingeschränkt, und das B-Netz ist nicht abhörsicher.

Für Käufer von schnurlosen Telefonen hat sich die Situation etwas gebessert. Die Masse der angebotenen schnurlosen Telefone kann weiterhin problemlos abgehört werden. Es gibt aber mittlerweile analoge Telefone, die mit einer Sprachinvertierung arbeiten. Daraus ergibt sich ein Schutz ähnlich dem eines C-Netz-Telefons. Zum Abhören wird ein Scanner mit eingebautem Sprachinverter benötigt, der im Handel verfügbar ist. Insbesondere gegen ältere Scanner ist aber durchaus ein Schutz gegeben.

Ein anderer Weg wird mit Geräten beschritten, die die Sprache digital übertragen. Als Standards kann hier auf CT2 („Cordless Telephone 2") oder DECT („Digital European Cordless Telephone") verwiesen werden. Ein Abhören ist mit den derzeit im Handel verfügbaren Scannern nicht möglich. Diese Standards beinhalten keine Verschlüsselung der Datenübertragung. Wenn in absehbarer Zeit die Chips, mit denen die Sprache digitalisiert wird, allgemein verfügbar sind, dürften sie in Scanner eingebaut werden. Ab diesem Zeitpunkt könnten dann auch digitale schnurlose Telefone abgehört werden. Der Aufwand ist aber höher, insbesondere wenn alte Scanner nachgerüstet werden sollten. Insofern ist z.Zt. der Abhörschutz bei schnurlosen Telefonen mit digitaler Sprachübertragung erheblich besser als bei analoger Sprachübertragung.

Wiesbaden, den 11. Februar 1994

gez. Professor Dr. Hassemer

23. Materialien

23.1.
Entschließung der 45. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar 1993 in Berlin zur Richtlinie des Rates vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (30/313/EWG)

Im Interesse eines wirksamen Umweltschutzes hat der Ministerrat der Europäischen Gemeinschaft die Umweltinformationsrichtlinie erlassen, die jedem Bürger ein Recht auf Zugang zu den bei Behörden vorhandenen Informationen über die Umwelt gewährt. Da es nicht gelungen ist, die Richtlinie innerhalb der vorgegebenen Frist bis Ende 1992 in deutsches Recht umzusetzen, herrscht gegenwärtig Rechtsunsicherheit bei Bürgern und Behörden über den Zugang zu Umweltinformationen.

Die Konferenz der Datenschutzbeauftragten sieht in der Gewährleistung eines freien Zugangs zu Umweltinformationen einen wesentlichen Beitrag zu größerer Transparenz des Verwaltungshandelns. Informationsfreiheit und Datenschutz bilden dabei keinen unlösbaren Gegensatz. Die Konferenz hält es für geboten, die Arbeit am Entwurf des Umweltinformationsgesetzes (UIG) zügig zum Abschluß zu bringen. Sie begrüßt entsprechende Initiativen auf Landesebene.

In den Gesetzen sind folgende datenschutzrechtliche Grundsätze zu berücksichtigen:

Soweit Umweltinformationen auf Personen beziehbar sind, ist das Grundrecht auf informationelle Selbstbestimmung zu beachten. Deshalb sind Informationen grundsätzlich in anonymisierter oder aggregierter Form zu geben. Wenn damit das Informationsinteresse nicht erfüllt werden kann, sind Eingriffe in das Persönlichkeitsrecht nur unter klaren gesetzlichen Voraussetzungen zulässig, welche die Rechte, insbesondere die Verfahrensrechte, der Betroffenen wahren.

23.2
Entschließung der 45. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar 1993 in Berlin zum geänderten Vorschlag der EG-Kommission für eine Datenschutzrichtlinie (KOM 92/422 endg.)

Die Konferenz der Datenschutzbeauftragten tritt auf der EG-Datenschutzkonferenz, gegenüber der EG-Kommission sowie den in Deutschland mit der Richtlinie befaßten Ministerien und Gremien (z. B. dem „Düsseldorfer Kreis") u. a. für folgende Positionen ein:

1. Ein über den durch die Richtlinie harmonisierten Standard hinausgehender Datenschutz im einzelstaatlichen Recht für Datenverarbeitung ohne grenzüberschreitenden Bezug muß zulässig bleiben.

2. Die Meldepflicht zum Dateienregister sollte selektiv ausgestaltet werden. Dem nationalen Gesetzgeber ist dabei mehr Spielraum für die Regelung von Ausnahmefällen einzuräumen.

3. Die Zulässigkeit der Speicherung/Nutzung einerseits und der Übermittlung andererseits ist differenziert zu regeln.

4. Die in der Richtlinie statuierte Unabhängigkeit der nationalen (Datenschutz-) Kontrollbehörden von Regierung und Exekutive muß unangetastet bleiben.

5. In der Richtlinie sollte dem einzelstaatlichen Gesetzgeber ausdrücklich die Option eröffnet werden, eine Kontrollinstitution innerhalb datenverarbeitender Stellen (betrieblicher bzw. behördlicher Beauftragter für den Datenschutz) vorzusehen.

23.3
Entschließung der 45. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16./17. Februar 1993 in Berlin zum Grundrecht auf Datenschutz

Die Konferenz hat zur Kenntnis genommen, daß sich in der Gemeinsamen Verfassungskommission von Bundesrat und Deutschem Bundestag nicht die erforderliche Mehrheit für die ausdrückliche Aufnahme eines Grundrechts auf Datenschutz in das Grundgesetz gefunden hat. Die Konferenz bekräftigt ihre Forderung, diese in einer modernen Informationsgesellschaft unabdingbare Verfassungsergänzung vorzunehmen, und verweist auf ihre Entschließung vom 28. April 1992.

23.4
Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin zum Datenschutz bei der Privatisierung der Deutschen Bundespost Telekom und bei der europaweiten Liberalisierung des Telefonnetzes und anderer Telekommunikationsdienste

Im Zuge der sog. Postreform soll die Deutsche Bundespost Telekom – nach der dafür notwendigen Änderung des Grundgesetzes – in Form einer Aktiengesellschaft privatisiert werden. Zugleich hat der Ministerrat der Europäischen Gemeinschaften in seiner Entschließung vom 22. Juli 1993 (Amtsblatt der EG Nr. C 213 vom 6. August 1993) seine Entschlossenheit bekräftigt, die Monopole im öffentlichen Sprachtelefondienst (Festnetz) der Mitgliedstaaten bis zum 1. Januar 1998 zu beseitigen.

In absehbarer Zeit werden daher in Deutschland neben der „Telekom AG" auch im Telefondienst andere private Unternehmen Telekommunikationsdienstleistungen anbieten. Diese Privatisierung hat Konsequenzen für den Datenschutz, der bisher für die Deutsche Bundespost Telekom auf einem vergleichsweise hohen Niveau geregelt ist. Insbesondere das grundgesetzlich garantierte Fernmeldegeheimnis würde für private Netzbetreiber und Dienstean-bieter jedenfalls nicht mehr unmittelbar gelten.

Die Datenschutzbeauftragten des Bundes und der Länder halten es für unabdingbar, daß durch die Privatisierung und Liberalisierung der Schutz der Bürger insbesondere in solchen Bereichen nicht verringert wird, die – wie der Telefondienst – der Daseinsvorsorge zuzurechnen sind. So wie bisher die konkurrierenden privaten Betreiber der Mobilfunknetze einen gleichmäßig hohen Datenschutzstandard gewährleisten müssen, hat dies auch zu gelten, wenn in Zukunft private Unternehmen im Wettbewerb miteinander stationäre Telefonnetze betreiben und entsprechende Dienste anbieten. Die Einhaltung von datenschutzrechtlichen Bestimmungen bei Telekommunikationsnetzen und -diensten muß zukünftig von einer unabhängigen Stelle nach bundesweit einheitlichen Kriterien und von Amts wegen kontrolliert werden können.

Da der Wettbewerb zwischen privaten Netzbetreibern und Diensteanbietern nicht nur national begrenzt, sondern im europäischen Binnenmarkt stattfinden wird, sind auch Rechtsvorschriften der Europäischen Gemeinschaften erforderlich, die einen möglichst hohen, einheitlichen Datenschutzstandard in der Telekommunikation gewährleisten.

23.5
Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin zur Gewährleistung des Datenschutzes bei der Mobilkommunikation

Die Verbreitung mobiler Sprach- und Datenübertragungsdienste hat in jüngster Vergangenheit stark zugenommen. So gibt es bereits in Deutschland mehr als eine Million Teilnehmer der Funktelefonnetze C und D; mit der Aufnahme

des Regelbetriebs von MODACOM ist seit Juni dieses Jahres auch ein öffentlicher mobiler Datenübertragungsdienst in Deutschland verfügbar. Es ist zu erwarten, daß sich die Teilnehmerzahl mobiler Kommunikationsdienste in Zukunft weiter vergrößern wird.

Die mit der Nutzung von Mobilfunkdiensten verbundenen Vorteile gehen mit Gefährdungen für den Datenschutz einher. Neben den auch bei anderen Telekommunikationsdiensten gespeicherten Angaben, wer wann mit wem in Verbindung war, wird bei der Mobilkommunikation auch erhoben, wo sich der mobile Teilnehmer jeweils aufhält. Die Speicherung dieser Daten ermöglicht die Bildung von problematischen Bewegungsprofilen.

Darüber hinaus ist vielfach auch die Vertraulichkeit der Kommunikationsinhalte gefährdet, insbesondere dann, wenn Daten unverschlüsselt per Funk übertragen werden. Dies gilt sowohl für die analogen Funktelefon-Netze B und C als auch für den von der Deutschen Bundespost Telekom betriebenen mobilen Datenübertragungsdienst MODACOM. Bei satellitengestützten Diensten ist es sogar möglich, die übertragenen Daten im gesamten, teilweise viele tausend Quadratkilometer umfassenden Abstrahlbereich des Satelliten unbemerkt abzuhören und aufzuzeichnen.

Von den Herstellern und Betreibern mobiler Kommunikationsdienste ist zu fordern, daß sie diesen Gefahren für das Fernmeldegeheimnis und für den Datenschutz durch eine entsprechende Gestaltung entgegenwirken und technische Vorkehrungen für eine sichere Kommunikation treffen.

Die Teilnehmer mobiler Kommunikationsdienste müssen von den Anbietern, Herstellern und Betreibern über die mit der Nutzung verbundenen Risiken und das erreichte Sicherheitsniveau aufgeklärt werden. Sofern bei bestimmten Diensten Sicherheitsmerkmale realisiert sind – wie z. B. in den digitalen D-Netzen –, muß die Sicherheit für die Aufsichts- und Kontrollorgane auch nachprüfbar sein. Falls durch den Dienstbetreiber nicht die erforderliche Sicherheit gewährleistet werden kann, ist eine Übertragung personenbezogener oder sonstiger sensibler Daten mit dem jeweiligen Dienst nur dann vertretbar, wenn der Benutzer zusätzliche Sicherheitsvorkehrungen trifft, also z. B. die übertragenen Daten anwendungsseitig verschlüsselt.

Zusätzlich kompliziert wird die Datenschutzproblematik bei der Mobilkommunikation dadurch, daß unter Umständen bei verschiedenen Dienst- und Netzbetreibern, aber auch bei anderen Unternehmen – den sog. Service-Providern, die lediglich Dienste vermarkten –, personenbezogene Daten gespeichert werden.

Hier muß im Zuge der anstehenden Überarbeitung des Telekommunikationsrechts dafür Sorge getragen werden, daß sich die Verarbeitung der Kommunikationsdaten auf das wirklich erforderliche Maß beschränkt und daß die Nutzer darüber aufgeklärt werden, bei welcher Stelle welche personenbezogenen Daten gespeichert oder sonst verarbeitet werden.

Besonders problematisch ist es, wenn bei der internationalen Mobilkommunikation auch in solchen Staaten personenbezogene Daten gespeichert werden, in denen kein ausreichendes Datenschutzniveau gewährleistet ist oder in denen das Fernmeldegeheimnis nicht sichergestellt wird. Deshalb ist es erforderlich, auf internationaler Ebene Regelungen zu treffen, die den Datenschutz bei mobilen Kommunikationsdiensten gewährleisten.

Die Konferenz unterstreicht aus diesem Grunde ihre Forderung, die Arbeiten an der EG-Richtlinie über Datenschutz im ISDN und in öffentlichen digitalen Mobilfunknetzen zu einem datenschutzrechtlich befriedigenden Abschluß zu bringen. Auch für den noch gänzlich datenschutzrechtlich ungeregelten Bereich der Satellitenkommunikation müssen endlich völkerrechtlich verbindliche Regelungen getroffen werden.

23.6
Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin zur Gefährdung der Vertraulichkeit der Funkkommunikation von Sicherheitsbehörden und Rettungsdiensten

Durch die Aufhebung der bisher gültigen Beschränkungen der zulässigen Empfangsbereiche für Rundfunkempfänger zum 30. Juni 1992 werden zunehmend Empfangsgeräte betrieben, die das Abhören des Funkverkehrs ermöglichen. Dies stellt eine erhebliche Bedrohung des Fernmeldegeheimnisses dar.

Die Datenschutzbeauftragten des Bundes und der Länder beobachten die damit verbundene Gefährdung der Vertraulichkeit der Funkkommunikation von Behörden und Organisationen mit Sicherheitsaufgaben (BOS) mit Sorge. Sie erkennen die Bemühungen der Polizeiverwaltungen der Länder an, durch zusätzliche technische Maßnahmen die Sicherheit des Sprechfunkverkehrs zu erhöhen. Sie stellen jedoch fest, daß die erforderliche Vertraulichkeit bisher nicht gewährleistet werden konnte. Auch Sprachverschleierungssysteme erreichen diese nicht hinreichend.

Daher begrüßt die Konferenz die im Rahmen des Schengener Abkommens getroffene grundsätzliche Entscheidung, im BOS-Bereich eine europäische Normierung zu erarbeiten, die die Digitalisierung und eine Verschlüsselung des BOS-Funkverkehrs vorsieht.

Die Konferenz hält es für erforderlich, daß das Normierungsverfahren so zügig wie möglich durchgeführt wird und auch schon vor der Umsetzung dieser Norm alle Möglichkeiten für einen effektiven Schutz der Vertraulichkeit des BOS-Funkverkehrs entsprechend dem jeweiligen Stand der Technik genutzt werden.

Die Konferenz weist weiter darauf hin, daß nicht nur bei den Behörden der Polizei, sondern auch in anderen BOS-Bereichen, wie z. B. dem Rettungswesen, eine Vertraulichkeit des Funkverkehrs zu gewährleisten ist. Daher sind auch in den übrigen BOS-Bereichen frühestmöglich entsprechende Absicherungen zur Vertraulichkeit des Funkverkehrs gefordert.

23.7
Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin zu kartengestützten Zahlungssystemen im öffentlichen Nahverkehr

Mit der Weiterentwicklung von Chipkarten werden kartengestützte Zahlungssysteme zunehmend auch im Verkehrsbereich eingesetzt. Damit besteht die Gefahr, daß sehr detaillierte Bewegungsprofile entstehen, die den persönlichen Bereich jedes Einzelnen einschränken und z. B. auch für Strafverfolgungsbehörden, Finanzämter und für die Werbewirtschaft von Interesse sein könnten. Da sämtliche Fahrten für einen gewissen Zeitraum aufgelistet werden können, hat jeder Kontoinhaber die Möglichkeit, Fahrten sämtlicher Familienmitglieder jederzeit nachzuvollziehen.

So sind im öffentlichen Nahverkehr zahlreiche sog. Postpaid-Verfahren in Erprobung, bei denen dem Fahrgast am Monatsende die aufsummierten Fahrpreise vom Konto abgebucht werden. Diese Zahlungsweise erfordert die Speicherung umfangreicher personenbezogener Daten: Neben der Konto-Nr. und Bankleitzahl des Fahrgastes werden sowohl Datum und Uhrzeit des Fahrscheinkaufs bzw. des Fahrtantritts als auch Automatennummer und Preisstufe der jeweiligen Fahrt erhoben.

Eine solche Vorgehensweise ist um so problematischer, als technische Alternativen existieren, die weitaus datenschutzfreundlicher sind. Im öffentlichen Nahverkehr können – wie skandinavische und auch deutsche Projekte aufzeigen – Wertkartensysteme eingesetzt werden, bei denen im voraus bezahlt wird und die daher gänzlich ohne personenbezogene Daten auskommen.

Die Datenschutzbeauftragten halten es daher für dringend erforderlich, daß mehr als bisher bei der Einführung kartengestützter Zahlungssysteme darauf geachtet wird, die „datenfreie Fahrt" zu ermöglichen. Im öffentlichen Nahverkehr sollte weiterhin auch die datenschutzfreundlichste Lösung angeboten werden: Der Kauf einer Fahrkarte am Automaten mit Bargeld.

Die Konferenz fordert weiter, daß noch vor der Pilotierung der dargestellten Technikvorhaben im Verkehrsbereich eine Untersuchung möglicher Alternativen, eine Analyse der von ihnen ausgehenden Gefahren für das informationelle Selbstbestimmungsrecht und eine Darstellung der technischen und organisatorischen Möglichkeiten zur Gewährleistung des Persönlichkeitsschutzes zu erstellen ist (Technikfolgen-Abschätzung). Nur Verfahren mit dem geringsten Eingriff in das allgemeine Persönlichkeitsrecht sollten eine Chance zur Erprobung erhalten.

23.8
Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin zum Integrierten Verwaltungs- und Kontrollsystem (InVeKoS) (Verordnungen der EWG Nrn. 3508/92 und 3887/92)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedstaaten dabei zur Einführung eines „Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem „Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein Überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem Übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige Überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;
- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;
- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;
- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z. B. zu Kontrollzwecken bei anderen landwirtschaftlichen Fördermaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z. B. zur Besteuerung).

23.9
Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 in Berlin zu regelmäßigen Datenübermittlungen an die öffentlich-rechtlichen Rundfunkanstalten und die Gebühreneinzugszentrale (GEZ)

(gegen die Stimme Bayerns und bei Stimmenthaltung Sachsens)

Die öffentlich-rechtlichen Rundfunkanstalten drängen seit langem auf die Schaffung einer Rechtsgrundlage für die regelmäßige Übermittlung von Meldedaten aller Einwohner an die gemeinsame Gebühreneinzugszentrale (GEZ). Sie verweisen dazu auf bereits bestehende Regelungen in den Ländern Hessen und Nordrhein-Westfalen. Auf Bitten der Konferenz der Regierungschefs der Länder hat deshalb nunmehr der zuständige Arbeitskreis der Innenministerkonferenz einen Musterentwurf für eine bundesweite Lösung im Melderecht erarbeitet. Der Entwurf sieht vor, daß künftig alle Meldebehörden in der Bundesrepublik im Fall der Anmeldung, Abmeldung oder des Todes eines volljährigen Einwohners bis zu acht Kerndaten an die GEZ übermitteln dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen eine derartige Regelung aus folgenden Gründen ab:

Die Regelung könnte im Ergebnis zu einem bundesweiten Melderegister bei Volljährigen führen. Sie könnte außerdem gegen das verfassungsrechtlich garantierte Verhältnismäßigkeitsprinzip verstoßen. Den Rundfunkanstalten stünde möglicherweise der unkontrollierte Zugriff auf Millionen personenbezogener Daten volljähriger Einwohner der Bundesrepublik zu, obwohl es für die Rundfunkanstalten nur von Interesse ist, welcher Einwohner bei ihnen gebührenpflichtig ist und bislang seine Gebührenpflicht nicht angemeldet hat. Das vorgesehene generelle Übermittlungsverfahren kennt keine Unterscheidung zwischen erforderlichen und nicht erforderlichen Daten, sondern überläßt diese Unterscheidung der GEZ. Über die Frage, ob ein Volljähriger überhaupt gebührenpflichtig ist, geben die Meldedaten keine Auskunft. Das muß nach wie vor im herkömmlichen Verfahren durch Befragung ermittelt werden.

Die Datenschutzbeauftragten des Bundes und der Länder sind bereit, an geeigneten und verfassungskonformen Lösungen der Landesregierungen zur Sicherung des Gebührenaufkommens der Rundfunkanstalten mitzuwirken.

Anlagen

Orthopädische Klinik Kassel

Aufnahmebeleg

Bitte in **Druckbuchstaben** schreiben. Stark umrandete Felder **nicht** ausfüllen. Die Angaben zu den schraffierten Feldern sind freiwillig. Bitte lesen Sie hierzu die **Anmerkungen auf der Rückseite.**

Aufnahme-Nr.	Aufnahme-Tag	Uhrzeit	Station

Patient/in: Zu- und Vorname

Straße und Hausnummer | PLZ und Wohnort

Geburts-Datum | Geburts-Name | Geburts-Ort

weiblich männlich bitte ankreuzen | Konfession | Familienstand | Nationalität

Hauptversicherte/ter: Zu- und Vorname Wenn identisch mit Patientendaten, hier nur **ja** ankreuzen

Geburts-Datum | Straße und Hausnummer | PLZ und Wohnort

Beruf und Arbeitgeber (bei Arbeitsunfall unbedingt abgeben!)

Hausarzt

Einweisender Arzt

Dringende Nachricht an: (z.B. Name, Adresse, Telefon)

Krankenkasse oder Zahlungspflichtiger (Bitte genaue Anschrift angeben. Evtl. auch Versicherungs-Nr. etc.)

Müssen Sie in diesem Jahr noch Ihrer Zuzahlungspflicht nachkommen ? **ja** ☐ **nein** ☐

Hinweis: Die noch zu leistenden Zuzahlungen wollen Sie bitte in jedem Fall vor Verlassen des Krankenhauses in unsere Aufnahme einzahlen.

bitte ankreuzen

Ich bin damit einverstanden, daß meine Personalien (Familienname, Vorname, Wohnanschrift, Aufnahmetag, Station, und Zimmer-Nr.) an die Informationszentrale der Orthopädischen Klinik übermittelt werden, um Besuchern auf Nachfrage Auskunft erteilen zu können. **Das Informationsblatt - Hinweis auf die Datenverarbeitung im Krankenhaus - habe ich erhalten.**

☐ Ich bin einverstanden ☐ Ich bin nicht einverstanden

Kassel, den _____

_____

Unterschrift der Patientin / des Patienten
oder der gesetzlichen Vertreterin / des Vertreters

Anmerkungen

Konfession

Wenn Sie hier einen Eintrag vornehmen, wird Ihre Relegionsgemeinschaft über Ihren Aufenthalt in unserer Klinik informiert. Übermittelt werden Name, Anschrift, Geburtsdatum, Aufnahmetag und Zimmernummer.

Beruf, Arbeitgeber

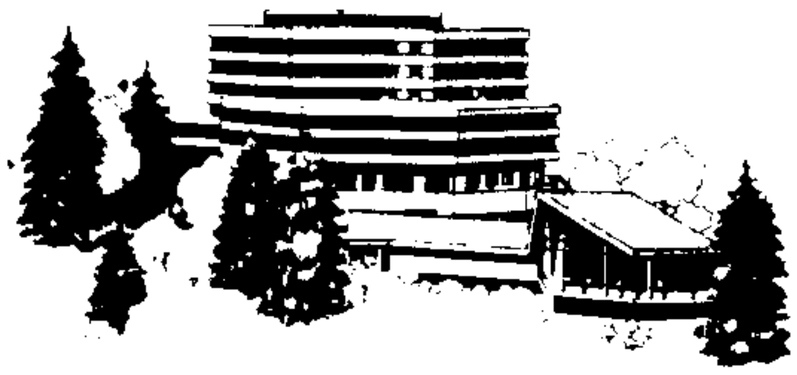
Sie erleichtern Ihrer Krankenkasse die Arbeit, wenn Sie trotz Freiwilligkeit Angaben machen. Sollten Sie aufgrund **eines Arbeitsunfalles** bei uns sein, so **müssen** Sie Angaben machen.

Hausarzt

Ihr behandelnder Krankenhausarzt möchte evtl. Rücksprache mit Ihrem Hausarzt nehmen. Sie erleichtern ihm die Arbeit, wenn Sie Ihren Hausarzt benennen.

Dringende Nachrichten, Telefon-Nr.

Wenn Sie wollen, können Sie hier Angaben über einen nächsten Angehörigen oder eine andere Vertrauensperson machen, die notfalls informiert werden soll.



ZENTRUM FÜR RHEUMATOLOGIE
MEDIZINISCHE KLINIK I UND II

DES HESSISCHEN STAATSBADES SCHLANGENBAD
VERWALTUNG

Hinweis auf die
Datenverarbeitung im Krankenhaus und Benachrichtigung

Sehr geehrte Patienten,

im Krankenhaus werden Ihre personenbezogenen Daten verarbeitet, soweit dies für die Durchführung Ihrer Behandlung erforderlich ist, insbesondere auch für die Abrechnung mit den Kostenträgern. Rechtsgrundlage für die Verarbeitung Ihrer Daten ist § 12 des Hessischen Krankenhausgesetzes in Verbindung mit den Vorschriften des Hessischen Datenschutzgesetzes. Darüber hinaus schreibt § 28 Abs. 3 des Hessischen Meldegesetzes jedem Krankenhaus vor, bestimmte Daten von Ihnen zu erheben.

Im Verwaltungsbereich der Klinik werden Ihre bei der Aufnahme erhobenen Daten automatisiert in einer Patientenstammdatei verarbeitet. Die Sperrung der Daten erfolgt innerhalb von 2 Jahren nach dem Aufnahmedatum; die Löschung erfolgt nach 4 Jahren.

Im medizinischen Bereich werden Ihre Daten in einer Krankenakte geführt. Diese wird 30 Jahre im Krankenhaus aufbewahrt.

Darüber hinaus werden medizinische Daten in einer oder mehreren automatisierten oder manuellen Dateien gespeichert. Um welche Dateien es sich im einzelnen handelt, hängt von dem Verlauf Ihrer Behandlung ab und kann zum Zeitpunkt der Krankenhausaufnahme noch nicht konkret benannt werden. Wir machen Sie aber darauf aufmerksam, daß Sie einen Anspruch auf Auskunft über die zu Ihrer Person in einer Datei gespeicherten Daten haben. Die Daten werden nach 2 Jahren gelöscht.

Sollten Sie nähere Informationen wünschen, können Sie sich an die Klinikverwaltung wenden.

Ihre
Klinikverwaltung