**Deutscher Bundestag**
**9. Wahlperiode**

**Drucksache 9/1243**

30. 12. 81

Sachgebiet 204

# Unterrichtung

## durch den Bundesbeauftragten für den Datenschutz

## Vierter Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz gemäß § 19 Abs. 2 Satz 2 des Bundesdatenschutzgesetzes (BDSG)

Gliederung

| | | Seite |
|---|---|---|
| 1 | **Überblick** | 4 |
| 1.1 | Prüfung und Beratung | 4 |
| 1.2 | Mitwirkung an der Umsetzung der Datenschutzgesetze in Verwaltungsmaßnahmen und Beteiligung an Gesetzgebungsverfahren | 4 |
| 1.3 | Öffentlichkeitsarbeit | 4 |
| 1.4 | Dateienregister | 5 |
| 1.5 | Kooperation mit anderen Datenschutzinstanzen | 5 |
| 2 | **Feststellungen aus der Kontroll- und Beratungstätigkeit in den verschiedenen Bereichen der Bundesverwaltung** | 6 |
| 2.1 | Bundesamt für den Zivildienst | 6 |
| 2.1.1 | Umfang und Dauer der Datenspeicherung | 6 |
| 2.1.2 | Datenschutz im Anerkennungsverfahren für Kriegsdienstverweigerer | 7 |
| 2.2 | Bundeszentralregister | 7 |
| 2.2.1 | Datensicherheit | 7 |
| 2.2.2 | Auskunftspraxis, Direktabfrage | 7 |
| 2.3 | Deutsches Patentamt | 8 |
| 2.4 | Deutsche Bundespost | 8 |
| 2.4.1 | Allgemeines | 8 |
| 2.4.2 | Aufzeichnungen über Telefongespräche | 8 |
| 2.4.3 | Eintragung im amtlichen Fernsprechbuch | 9 |
| 2.4.4 | Bildschirmtext | 9 |
| 2.4.5 | Gehaltskontoverfahren | 10 |
| 2.5 | Rundfunkanstalten des Bundes | 10 |
| 2.6 | Personalverwaltungen | 10 |
| 2.6.1 | Bundesamt für Finanzen — Bundesbesoldungsstelle — | 10 |
| 2.6.2 | Personalinformationssystem PERFIS des Bundesministers der Verteidigung | 10 |
| 2.6.3 | Tests bei Offiziersbewerberprüfungen | 11 |
| 2.6.4 | Schwarze Personalakten bei einer Bundesbehörde | 12 |
| 2.6.5 | Auskunft über die gespeicherten Daten von Mitarbeitern | 13 |
| 2.7 | Sozialversicherung und Arbeitsverwaltung | 13 |
| 2.7.1 | Datenverarbeitung und Datenschutz bei der Bundesversicherungsanstalt für Angestellte | 13 |
| 2.7.2 | Sozialbericht bei Abhängigkeitskranken | 14 |
| 2.7.3 | Erhebungsbogen der Krankenkassen bei Krankenhauspflege | 15 |
| 2.7.4 | Nachweis der Qualifikation des Personals in Sozialeinrichtungen | 15 |
| 2.7.5 | Arztbericht im Vertrauensärztlichen Dienst | 16 |
| 2.7.6 | Prüfung der Bau-Berufsgenossenschaft Hamburg | 16 |

*Gemäß § 19 Abs. 2 Satz des Bundesdatenschutzgesetzes zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 192 111/6 — vom 30. Dezember 1981*

| | | Seite |
|---|---|---|
| 2.7.7 | Einzelfallprüfung bei einer Berufsgenossenschaft | 17 |
| 2.7.8 | Erhebung des Kindschaftsverhältnisses auf Formularen der Bundespost | 17 |
| 2.7.9 | Arbeitsverwaltung | 18 |
| 2.8 | Bundesgesundheitsamt | 19 |
| 2.9 | Deutsche Bundesbank | 19 |
| 2.10 | Kraftfahrt-Bundesamt | 20 |
| 2.10.1 | Zentrales Verkehrs-Informationssystem (ZEVIS) | 20 |
| 2.10.2 | Datensicherung beim Kraftfahrt-Bundesamt | 21 |
| 2.10.3 | Verarbeitung der Berufs- und Gewerbeangabe | 21 |
| 2.11 | Allgemeine Erkenntnisse bei den Sicherheitsbehörden | 21 |
| 2.11.1 | Prüfungsumfang | 21 |
| 2.11.2 | Gesamtergebnis | 21 |
| 2.11.3 | Zu den Ursachen festgestellter Mängel | 22 |
| 2.11.4 | Das Amtshilfeproblem | 22 |
| 2.12 | Bundeskriminalamt | 22 |
| 2.12.1 | Datei PIOS-Terrorismus | 22 |
| 2.12.2 | Abteilung Staatsschutz | 23 |
| 2.12.3 | Vorgangsnachweis Personalien (VNP) | 24 |
| 2.12.4 | Häftlingsüberwachung | 24 |
| 2.12.5 | Fahndungsmäßige Überprüfung von Personen | 25 |
| 2.12.6 | Zusammenarbeit der Polizeien (Meldedienste, Kriminalaktennachweis) | 25 |
| 2.12.7 | Interpol und Datenschutz | 26 |
| 2.13 | Bundesamt für Verfassungsschutz | 27 |
| 2.13.1 | Bereinigung der „Altbestände" | 27 |
| 2.13.2 | Meinungsunterschiede bei den Neueinspeicherungen | 28 |
| 2.13.3 | Weitere Grundsatzfragen | 28 |
| 2.13.4 | Prüfung einer Sonderdatei | 28 |
| 2.13.5 | Dateianfrage | 29 |
| 2.14 | Zusammenarbeit Verfassungsschutz/Polizei | 29 |
| 2.15 | Bundesgrenzschutz | 30 |
| 2.15.1 | Allgemeines | 30 |
| 2.15.2 | Zugriff anderer Polizeibehörden auf den geschützten Grenzfahndungsbestand | 31 |
| 2.15.3 | Grenzschutz und Zusammenarbeit mit Nachrichtendiensten | 31 |
| 2.15.4 | Personenkarteien bei Grenzschutzstellen | 31 |
| 2.16 | Bundesnachrichtendienst | 32 |
| 2.16.1 | Allgemeines | 32 |
| 2.16.2 | Amtshilfe-Richtlinien | 32 |
| 2.16.3 | Zusammenarbeits-Richtlinien | 32 |
| 2.16.4 | Löschungs-Richtlinien | 32 |
| 2.17 | Militärischer Abschirmdienst (MAD) | 32 |
| 2.18 | Zollkriminalinstitut | 33 |
| 2.18.1 | Zentrale Vorgangskartei | 33 |
| 2.18.2 | Zugriff des Zollkriminalinstituts auf den Zentralen Personenindex (ZPI) des Bundeskriminalamts | 33 |
| 2.18.3 | Ausschreibung von Personen zur zollrechtlichen Überwachung | 33 |
| 2.19 | Verbindungen der Sicherheitsbehörden zum Ausländerzentralregister (AZR) | 34 |
| 2.20 | Wehrermittlungsliste des Bundesverwaltungsamtes | 34 |
| 2.21 | Übermittlung von Gesundheitsdaten durch Bundeswehrdienststellen | 35 |
| 3 | **Übergreifende Feststellungen aus verschiedenen Verwaltungsbereichen** | 35 |
| 3.1 | Allgemeine Erfahrungen aus Prüfungen | 35 |
| 3.1.1 | Unzulässige Datenverarbeitung | 35 |
| 3.1.2 | Übersicht über die gespeicherten Daten | 35 |
| 3.1.3 | Maßnahmen zur Verbesserung der Datensicherung | 36 |
| 3.1.4 | Beauftragung von Dienstleistungsunternehmen | 36 |
| 3.1.5 | Konsequenzen für die Kontrolltätigkeit | 36 |
| 3.2 | Personalwesen | 37 |
| 3.2.1 | Beschaffung von Anschriften für Selbsthilfeeinrichtungen und Berufsverbände des öffentlichen Dienstes | 37 |
| 3.2.2 | Angaben in Hausmitteilungen | 37 |
| 3.2.3 | Benennung der in Kommunalvertretungskörperschaften tätigen Angehörigen einer Verwaltungseinheit | 38 |
| 3.2.4 | Beihilfewesen | 38 |
| 3.3 | Telefondaten | 39 |
| 3.4 | Bankauskünfte | 40 |
| 3.5 | Haushaltskontrolle von Zuwendungen | 40 |
| 3.6 | Verteiler für Informationsmaterial | 41 |
| 4 | **Umsetzung des Datenschutzes in bereichsspezifische Regelungen und Weiterentwicklung des Datenschutzrechts** | 41 |
| 4.1 | Rechtswesen | 41 |
| 4.1.1 | Mitteilungen in Strafsachen | 41 |

| | | Seite |
|---|---|---|
| 4.1.2 | Entwurf eines Gesetzes über die internationale Rechtshilfe in Strafsachen | 41 |
| 4.1.3 | Novellierung des Bundeszentralregistergesetzes (BZRG) | 42 |
| 4.1.4 | Anordnung über Mitteilungen in Zivilsachen | 43 |
| 4.1.5 | Personenstandswesen | 44 |
| 4.1.6 | Entwurf eines Mietspiegelgesetzes | 44 |
| 4.1.7 | Prozeßkostenhilfe | 44 |
| 4.1.8 | Schuldnerverzeichnis | 44 |
| 4.1.9 | Daten über Mietinteressenten | 45 |
| 4.2 | Sozialverwaltung und Gesundheitswesen | 45 |
| 4.2.1 | Sozialgesetzbuch, Zehntes Buch | 45 |
| 4.2.2 | Modellprogramm Psychiatrie | 45 |
| 4.2.3 | Heimgesetz | 46 |
| 4.3 | Forschung und Statistik | 46 |
| 4.3.1 | Auswirkungen des Datenschutzes auf die wissenschaftliche Forschung | 46 |
| 4.3.2 | Erfahrungen mit § 75 SGB X | 47 |
| 4.3.3 | Krebsregister | 48 |
| 4.3.4 | Entwicklungen im Bereich der Statistik | 49 |
| 4.4 | Anforderungen an ein Bundesarchivgesetz | 50 |
| 4.5 | Sicherheitsbereich | 51 |
| 4.5.1 | Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen (KpS), Dateien-Richtlinien für das BKA und bundeseinheitliche Richtlinien über erkennungsdienstliche Behandlung | 51 |
| 4.5.2 | Bereichsspezifische Gesetzgebungsvorhaben | 53 |
| 4.6 | Finanzverwaltung | 53 |
| 4.7 | Novellierung des BDSG | 53 |
| **5** | **Datenschutz im Ausland, internationale Zusammenarbeit** | 58 |
| 5.1 | Entwicklungstendenzen in Staaten mit Datenschutzgesetzen | 58 |
| 5.2 | Vorbereitung von Datenschutzgesetzen in weiteren Staaten | 59 |
| 5.3 | Neue Datenschutzgesetze | 60 |
| 5.4 | Internationale Übereinkommen | 61 |
| 5.4.1 | Datenschutz-Konvention des Europarats | 61 |
| 5.4.2 | OECD-Leitlinien | 62 |
| 5.4.3 | Europäische Gemeinschaft | 62 |
| 5.5 | Internationale Zusammenarbeit in Fragen des Datenschutzes | 62 |
| 5.5.1 | Allgemeines | 62 |
| 5.5.2 | Dritte Konferenz der nationalen Datenschutzkontrollinstitutionen | 62 |

# 1. Überblick

## 1.1 Prüfung und Beratung

Im Berichtsjahr wurden Datenschutzprüfungen und Beratungsbesuche bei folgenden öffentlichen Stellen des Bundes durchgeführt:

a) im Bereich der inneren Verwaltung, des Rechtswesens, der Finanzverwaltung:
   — Bundesamt für den Zivildienst;
   — Bundeszentralregister, Deutsches Patentamt;
   — Bundesamt für Finanzen, Zollkriminalinstitut;

b) im Bereich der Deutschen Bundespost:
   — Bildschirmtext-Zentrale Berlin;
   — ein Postscheckamt, eine Rentenrechnungsstelle;

c) im Bereich der sozialen Sicherung und des Gesundheitswesens:
   — Bundesversicherungsanstalt für Angestellte; mehrere Arbeitsämter, mehrere Berufsgenossenschaften; Arbeitsgemeinschaft der Bau-Berufsgenossenschaften, Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung (Essen);
   — Bundesgesundheitsamt;

d) im Bereich Wirtschafts- und Verkehrsverwaltung;
   — Bundesministerium für Wirtschaft;
   — Deutsche Bundesbank;
   — Kraftfahrt-Bundesamt;
   — Filmförderungsanstalt;
   — Deutsche Siedlungs- und Landesrentenbank;

e) im Bereich Wissenschaft und Forschung, Statistik, Medien:
   — Bundesministerium für Bildung und Wissenschaft, Bundesministerium für Forschung und Technologie;
   — Statistisches Bundesamt / Zweigstelle Berlin;
   — Deutschlandfunk, Deutsche Welle;

f) im Bereich öffentliche Sicherheit, Verteidigung:
   — Bundeskriminalamt, Bundesamt für Verfassungsschutz, Grenzschutzdirektion, mehrere Grenzschutzstellen, eine Dienststelle des MAD;

g) ferner: Bundeszentrale für politische Bildung und Bundesinstitut für ostwissenschaftliche und internationale Studien.

Die Prüfungen hatten unterschiedlichen Charakter; einige — vor allem die bei den angeführten Ministerien — zielten nur auf einen ersten Einstieg ab oder dienten der Vertiefung schon bestehender Kontakte, andere waren auf intensive und umfassende Aufarbeitung der jeweiligen Datenverarbeitung angelegt (so die Prüfungen bei der Bundesversicherungsanstalt für Angestellte, bei den Berufsgenossenschaften und beim Bundesgesundheitsamt) oder beschränkten sich auf Teile des DV-Systems (so beim Bundeskriminalamt und beim Bundesamt für Verfassungsschutz und — wegen des „Medienprivilegs" gemäß § 1 Abs. 3 BDSG — bei den beiden Rundfunkanstalten des Bundes).

Die Ergebnisse der Prüfungen werden in den Abschnitten 2 und 3 dieses Tätigkeitsberichts unter den Aspekten der jeweiligen Sachmaterie dargestellt. Soweit eine geprüfte Stelle nicht besonders erwähnt wird, wurden keine oder keine gewichtigen Datenschutzmängel festgestellt. Mängel in der Datensicherung, die mehrfach vorkamen, sind im Abschnitt 3.1 zusammengefaßt.

## 1.2 Mitwirkung an der Umsetzung der Datenschutzgesetze in Verwaltungsmaßnahmen und Beteiligung an Gesetzgebungsverfahren

Zur Verwirklichung der Gebote, die das gesetzliche Datenschutzrecht aufstellt, bedarf es vielfacher Maßnahmen der Verwaltung, die über den Einzelfall hinausreichen; es sind Rechtsverordnungen und Verwaltungsvorschriften (Richtlinien) zu erlassen sowie zahlreiche Vordrucke (neu) zu entwerfen. Hieran habe ich vielfach beratend mitgewirkt.

Ich habe im Laufe des Jahres auch zu mehreren Gesetzentwürfen — in den Ausschüssen des Deutschen Bundestages und in anderen Gremien — aus datenschutzrechtlicher Sicht Stellung genommen und mich darum bemüht, daß die schutzwürdigen Belange der Betroffenen in angemessener Form berücksichtigt wurden. Ich nenne den Entwurf des Mietspiegelgesetzes, des Sozialgesetzbuches (SGB) — Zusammenarbeit der Leistungsträger und ihre Beziehungen zu Dritten — (§§ 86 ff. SGB X), den Entwurf eines Gesetzes zur Bekämpfung der illegalen Beschäftigung, den Musterentwurf eines Gesetzes über ein Krebsregister und die geplante Novelle zum Bundeszentralregistergesetz. An Überlegungen zu gesetzlichen Regelungen des Archivwesens habe ich mich gemeinsam mit den Landesbeauftragten für den Datenschutz beteiligt.

Über diese Aktivitäten wird in Abschnitt 4 dieses Tätigkeitsberichts referiert.

## 1.3 Öffentlichkeitsarbeit

Das Interesse des Bürgers an datenschutzrechtlichen Fragen und sein Bedürfnis nach Informationen

über Gesetz und Anwendung sind unverändert groß. Täglich erreichen mich Briefe und Telefonanrufe, in denen um Rat und Auskunft zu allgemeinen Datenschutzproblemen, aber auch um Hilfe in konkreten Einzelfällen gebeten wird. Ich messe der telefonischen Beratung des Bürgers große Bedeutung bei, denn der Griff zum Telefonhörer fällt vielen Hilfesuchenden leichter als das Aufsetzen eines Schreibens an „die Behörde". Große Nachfrage herrscht weiterhin nach den von mir kostenlos abgegebenen Broschüren über das Bundesdatenschutzgesetz und die Rechte, die sich für den Bürger daraus ergeben. So wurden bislang von der Broschüre „Was bringt das Datenschutzgesetz?" und der unter dem Titel „Bürgerfibel Datenschutz" herausgebrachten Neuauflage dieser Schrift bereits über 100 000 Exemplare abgegeben. Nachfragende sind nicht nur interessierte Privatpersonen, sondern auch Institutionen jeglicher Art, die in Ausbildung und Lehre tätig sind. Auch Personal- und Betriebsräte haben um Übersendung der Broschüre gebeten. Die Druckschrift „Der Bürger und seine Daten", die gemeinsam mit den Datenschutzbeauftragten und Aufsichtsbehörden der Länder erarbeitet wurde und verteilt wird, ist weiterhin stark gefragt. Von meiner Dienststelle wurden bisher ca. 65 000 Exemplare auf entsprechende Anfragen hin versandt. Wegen des großen Interesses vor allem aus Kreisen interessierter Journalisten und öffentlicher Stellen an meinem 3. Tätigkeitsbericht habe ich insgesamt 4 000 Exemplare eines Sonderdruckes der Bundestagsdrucksache verschickt. An Fachwissenschaftler sowie in der Datenschutz-Praxis und -Gesetzgebung Tätige wendet sich die Schrift „Ziele und Mittel des Datenschutzes" mit Forderungen zur Novellierung des BDSG, die ich im September veröffentlicht habe. Auf große Resonanz in der Öffentlichkeit stieß die Herausgabe des „Datenscheckheftes" des Berliner Datenschutzbeauftragten. Da auch mich zahlreiche Nachfragen erreichten, versandte meine Dienststelle mehrere hundert Exemplare dieser Schrift, die mir vom Berliner Datenschutzbeauftragten überlassen wurden.

Wie auch im vergangenen Berichtszeitraum versuchte ich in zahlreichen Kontakten zu den Medien, Notwendigkeit und Wirkungsweise des Datenschutzes weiterhin deutlich zu machen. In diesem Sinne wirkten meine Mitarbeiter und ich auch an einer größeren Anzahl von Tagungen und Seminaren mit, bei denen datenschutzrechtliche Fragen teils im Mittelpunkt standen, teils in eine andere Problematik eingebettet waren.

### 1.4 Dateienregister

Die Anzahl der automatisiert betriebenen Dateien, die mir zum Register nach § 19 (4) BDSG gemeldet wurden, ist nur noch geringfügig gestiegen und liegt bei etwas über 1 000. Auch in diesem Berichtszeitraum haben nur wenige Bürger von ihrem Recht Gebrauch gemacht, Einsicht in das Register zu nehmen. Hieran wird sich auch kaum etwas ändern, denn kaum ein Bürger wird die Anreise nach Bonn in Kauf nehmen, nur um Einblick in das Dateienregister zu nehmen. Auch für seinen zweiten Verwendungszweck, nämlich dem Bundesbeauftragten für örtliche Kontrollen einen ersten Überblick über die Art der gespeicherten personenbezogenen Daten zu geben, ist das Register nur begrenzt aussagefähig. So sind jedenfalls hierfür weitere, detailliertere Angaben zu den einzelnen Dateien erforderlich (siehe hierzu auch unter Nr. 4.7).

### 1.5 Kooperation mit anderen Datenschutzinstanzen

Bei der Bewältigung von Auslegungsproblemen und bei der Weiterentwicklung und Anpassung des Datenschutzrechts an neue Fragestellungen ist die Kooperation mit den anderen Datenschutzinstanzen eine wesentliche Hilfe.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder trat im Berichtsjahr zu drei Sitzungen zusammen, auf denen eine Vielzahl gemeinsam interessierender Themen beraten wurde; in diesem Bericht wird darauf im jeweiligen Sachzusammenhang eingegangen.

An der Diskussion spezieller Probleme von übergreifendem Interesse in mehreren Arbeitsgruppen der Konferenz waren die Mitarbeiter meiner Dienststelle beteiligt:

— Eine Arbeitsgruppe hat für die Konferenz eine Entschließung zu der Frage vorbereitet, unter welchen Voraussetzungen die *Staatsanwaltschaften* Daten in zentralen Hinweiskarteien führen und nutzen sollten. Diese Entschließung wurde von der Konferenz verabschiedet; da sie sich im wesentlichen an die Länder richtet, gehe ich darauf nicht weiter ein.

— Ein anderer Arbeitskreis hat sich mit der Problematik der geplanten *Krebsregistergesetze* beschäftigt (siehe dazu unten Nr. 4.3.3).

  In einem Arbeitskreis „Archivwesen" wurden insbesondere die Anforderungen diskutiert, die an ein *Archivgesetz* zu stellen sind. Das Ergebnis wird zu einem entsprechenden Beschluß der Konferenz führen (dazu unten Nr. 4.4).

— Der Arbeitskreis *„Statistik"* hat vor allem einzelne Statistiken darauf überprüft, ob dem Bürger ohne gesetzliche Grundlage Auskünfte abverlangt wurden. Außerdem wurden Empfehlungen für Repräsentativstatistiken erarbeitet (dazu unten Nr. 4.3.4).

— Der Arbeitskreis *„Sicherheit"* erarbeitete Vorschläge für bereichsspezifische Datenschutzregelungen für die Sicherheitsbehörden und beteiligte sich insbesondere an der Diskussion der Richtlinien über Kriminalpolizeiliche personenbezogene Sammlungen (KpS) und über erkennungsdienstliche Unterlagen (dazu unten Nr. 4.5.1).

— Die erste Sitzung des neu eingerichteten Arbeitskreises *„Technische und organisatorische Datenschutzfragen"* diente der gegenseitigen Information über die Durchführung von Kontrollen. Ferner wurde vereinbart, sich gegenseitig ausführlich über erkannte Schwachstellen in Datenverarbeitungssystemen und -verfahren zu unterrichten.

— Arbeitskreise der Konferenz bemühen sich auch um eine einheitliche Behandlung der Datenschutzfragen in der *Sozial-* und *Finanzverwaltung.*

— Eine Arbeitsgruppe *„Datensatz für das Meldewesen"* überprüfte den im Auftrag der Innenministerien erstellten Entwurf des Datensatzes für das Meldewesen, der die Grundlage für die Datenübermittlung im öffentlichen Bereich sein soll. Dabei wurden die einzelnen Felder des Datensatzes kritisch an den Anforderungen des Datenschutzes, insbesondere an den Vorgaben des Melderechtsrahmengesetzes gemessen. Das Ergebnis war die Basis für eine gemeinsame Stellungnahme der Datenschutzbeauftragten und der Datenschutzkommission. Gemeinsam mit dem Bayerischen Landesbeauftragten für den Datenschutz habe ich mich in dem zuständigen Unterausschuß des Arbeitskreises II der Innenministerkonferenz darum bemüht, daß der Datenschutz bei der Anpassung des Landesmelderechts an das Melderechtsrahmengesetz des Bundes angemessen berücksichtigt wird.

Neben der Mitarbeit in der Konferenz der Datenschutzbeauftragten und in der internationalen Konferenz der Datenschutz-Kontrollinstanzen (siehe unten Nr. 5.5) wirkte ich in verschiedenen nationalen Gremien mit, die besondere Aspekte des Datenschutzes behandelten:

— Im „Düsseldorfer Kreis" wurde die bewährte Koordinierung unter den Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich fortgesetzt. Die Abstimmung war wie bisher in allen wesentlichen Punkten erfolgreich. Neben bereichsspezifischen Fragen z. B. aus den Bereichen Werbewirtschaft sowie Kredit- und Handelsauskunfteien wurde auch diskutiert, welche Novellierungsvorschläge sich aus den Erfahrungen in den einzelnen Bereichen ergeben.

Eine ad hoc-Arbeitsgruppe „schutzwürdige Belange" hat Grundsätze für die Auslegung dieses Begriffes erarbeitet; das Ergebnis wird zur Zeit vom Düsseldorfer Kreis beraten.

— An den Sitzungen des Gutachterausschusses „Datenschutz in der kommunalen Verwaltung" der Kommunalen Gemeinschaftsstelle für Verwaltungsvereinfachung (KGSt) und der Arbeitsgruppe „Datenschutz" der Bundesvereinigung der Kommunalen Spitzenverbände, die sich mit der Ausführung der Datenschutzgesetze in den Kommunalverwaltungen beschäftigen, nimmt regelmäßig ein Vertreter meiner Dienststelle als Gast teil.

— Der Bundesverband der Ärzte des Öffentlichen Gesundheitsdienstes e. V. plant für das Frühjahr 1982 einen Kongreß „Datenschutz im Öffentlichen Gesundheitsdienst". An den vorbereitenden Sitzungen nahm ein Vertreter meiner Dienststelle beratend teil.

— Für die zunehmende Datenfernübertragung auf Leitungen und Richtfunkstrecken kann die Verschlüsselung ein sinnvolles Mittel zur Sicherung sein. Die breite Anwendung der entsprechenden Verfahren setzt aber voraus, daß die Methoden genormt sind und das Schlüsselmanagement für den Anwender einfach ist. Um dieses Ziel zu erreichen, wirkt ein Vertreter meiner Dienststelle im Unterausschuß 2.1 „Datenverschlüsselung" des Normenausschusses Informationsverarbeitung des Deutschen Instituts für Normung (DIN) mit.

— Im Ausschuß für wirtschaftliche Verwaltung in Wirtschaft und öffentlicher Hand e. V. (AWV) beschäftigt sich der Fachausschuß „Datenschutz und Datensicherung", dem verschiedene Projektgruppen zugeordnet sind, mit den Auswirkungen und der Fortentwicklung des BDSG. An der Fachausschußleitung und in den Projektgruppen beteiligten sich Vertreter meiner Dienststelle.

## 2. Feststellungen aus der Kontroll- und Beratungstätigkeit in den verschiedenen Bereichen der Bundesverwaltung

Aus der Fülle der Ergebnisse sind im folgenden Abschnitt einige Feststellungen herausgehoben, weil sie bedeutsam, verallgemeinerungsfähig — oder auch weil sie erörterungsbedürftig sind.

### 2.1 Bundesamt für den Zivildienst

#### 2.1.1 Umfang und Dauer der Datenspeicherung

Das Bundesamt für den Zivildienst hat von seiner Aufgabenstellung her in großem Umfange personenbezogene Daten zu verarbeiten. Ich habe es daher einer eingehenden Überprüfung unterzogen. Insgesamt habe ich dabei einen positiven Eindruck gewonnen. Meine Anregungen zu Einzelpunkten wurden bereitwillig aufgegriffen und eine Beratung auch in anderen Fällen gesucht.

Die Überprüfung der Zentral-Datei aller Zivildienstleistenden ist noch nicht abgeschlossen. Dies ist erst dann möglich, wenn ihre Zweckbestimmung präzise definiert ist. Daran fehlt es bisher. Zwar unterliegen die anerkannten Kriegsdienstverweigerer der Zivildienstüberwachung nach § 23 des Zivildienstgesetzes bis zur Vollendung des 32. Lebensjahres. Die Daten bleiben aber länger gespeichert. Ob und wie lange dies notwendig ist, hängt davon ab, ob und wie die Kriegsdienstverweigerer im Verteidigungsfall eingesetzt werden sollen. Darüber gibt es bisher — soweit ersichtlich — keine konkreten Vorstellungen. Solange dies nicht geklärt ist, muß ich in der Spei-

cherung eine datenschutzrechtlich bedenkliche Vorratsspeicherung sehen. Offen ist auch noch, ob und in welchem Umfange das Bundesamt Daten über die Religionszugehörigkeit der Zivildienstleistenden speichern darf.

#### 2.1.2 Datenschutz im Anerkennungsverfahren für Kriegsdienstverweigerer

Ich hatte schon bei meiner ersten Kontaktaufnahme mit dem Bundesbeauftragten für den Zivildienst gefragt, ob es notwendig ist, die Unterlagen über das Verfahren der Anerkennung als Kriegsdienstverweigerer mit an das Bundesamt für den Zivildienst zu übermitteln (vgl. 3. TB. Nr. 3.1.5, S. 18). Diese Frage ist in der Zwischenzeit geprüft worden. Danach sind die in diesem Teil der Akten enthaltenen Angaben zwar in Einzelfällen nützlich, im Regelfall aber entbehrlich. Auf die Unterlagen, die im Verfahren vor dem Anerkennungsausschuß und gegebenenfalls den Gerichten bis zur Entscheidung über den Antrag entstehen, kann nach Ansicht des Bundesamtes und des Bundesbeauftragten für den Zivildienst verzichtet werden. Die sonstigen Unterlagen, beginnend mit der Wehrerfassung und der Musterung, würden hingegen benötigt.

Bei der datenschutzrechtlichen Bewertung dieses Sachverhalts ist zunächst festzustellen, daß das Bundesdatenschutzgesetz unmittelbar nicht anwendbar ist, weil es hier ausschließlich um Akten geht, für die dieses Gesetz nicht gilt (§ 1 Abs. 2 i. V. m. § 2 Abs. 3 BDSG). Wäre es anwendbar, wäre die Übermittlung nach § 10 BDSG unzulässig, weil sie weder zur Aufgabenerfüllung des jeweiligen Kreiswehrersatzamtes noch des Bundesamtes für den Zivildienst erforderlich ist. Die Nichtanwendbarkeit des BDSG bedeutet indessen nicht, daß der Datenschutz bei der Verarbeitung personenbezogener Daten in Akten gänzlich außer Acht gelassen werden könnte. Die Grundsätze des Datenschutzes sind auch hier anzuwenden. Das datenschutzrechtliche Problem, das in diesem Zusammenhang besteht, läßt sich wie folgt spezifizieren: Der Kriegsdienstverweigerer offenbart in dem nicht-öffentlichen Anerkennungsverfahren die Gründe, die ihn zur Ablehnung des Kriegsdienstes mit der Waffe geführt haben. Er macht dabei unter Umständen Angaben, die den Kernbereich seiner Persönlichkeit betreffen. Der Anerkennungsausschuß seinerseits ist verpflichtet, sich ein Bild von der Persönlichkeit des Kriegsdienstverweigerers zu verschaffen. Er muß dessen Angaben überprüfen und dazu möglicherweise auch dritte Personen befragen. Alle diese Erhebungen dienen ausschließlich dem Zweck, die Entscheidung über die Anerkennung als Kriegsdienstverweigerer vorzubereiten. Ich brauche nicht zu betonen, daß es sich hier um Daten von hohem Sensibilitätsgrad handelt. Mit der Entscheidung über den Antrag ist der Zweck, zu dem die Daten erhoben worden sind, erreicht. Tatsächlich bleiben die Daten aber — weil sie mit an das Bundesamt für den Zivildienst übermittelt werden — weiterhin für gänzlich andere Zwecke verfügbar. Sie bilden einen Teil der Personalakte und sind für jedermann zugänglich, der diese Akte einsehen kann. Damit wird nicht nur gegen einen wichtigen Datenschutzgrundsatz, den Grundsatz der Zweckbindung verstoßen; es werden schutzwürdige Belange des jeweils betroffenen Kriegsdienstverweigerers beeinträchtigt. Dieser äußert sich nämlich deswegen so offen in dem Anerkennungsverfahren, weil er davon ausgeht, daß es nicht öffentlich ist, und weil er darauf vertraut, daß seine Angaben auch entsprechend vertraulich behandelt werden. Diese Gewißheit kann er nicht haben, wenn er davon ausgehen muß, daß seine Angaben später Teil seiner Personalakte und somit eine zusätzliche Grundlage für spätere — völlig andersartige — Personalentscheidungen werden können. Auch das Bundesamt für den Zivildienst hat die darin liegende Problematik erkannt. Es ist der Auffassung, daß sein Verhältnis zu den Zivildienstleistenden sehr viel unbefangener sein könnte, wenn es nicht mit den Informationen aus dem Anerkennungsverfahren belastet wäre.

Aus diesen Erwägungen habe ich den Bundesminister der Verteidigung gebeten, das bisherige Verfahren der Übersendung sämtlicher Akten an das Bundesamt für den Zivildienst dahin gehend zu überprüfen, daß die Akten aus dem Anerkennungsverfahren bei den Kreiswehrersatzämtern verbleiben und dort nach Ablauf der Wehrüberwachung vernichtet werden. Der dafür erforderliche organisatorische Aufwand ist nach meiner Einschätzung gering, der datenschutzrechtliche Nutzen jedoch erheblich. Der Bundesminister der Verteidigung hat sich in einer ersten Stellungnahme ablehnend geäußert. Ich rechne aber dennoch damit, daß es zu einer besseren Lösung als der gegenwärtigen Praxis kommt. (Vgl. zu diesem Komplex auch unten Nr. 2.13.3, S. 28.)

### 2.2 Bundeszentralregister

#### 2.2.1 Datensicherheit

Im Rahmen einer erneuten Überprüfung des Bundeszentralregisters Berlin habe ich die Probleme angesprochen, die bei meiner Prüfung im vergangenen Jahr noch offen geblieben waren.

Ich konnte mich davon überzeugen, daß das Bundeszentralregister meine seinerzeitigen Anregungen einer eingehenden Prüfung unterzogen hat. Dies hatte zur Folge, daß spürbare Verbesserungen der Datensicherung in fast allen angesprochenen Punkten erreicht werden konnten.

#### 2.2.2 Auskunftspraxis, Direktabfrage

Das Bundeszentralregister erteilt z. Z. mehr als 5 Millionen Auskünfte jährlich. Bei einem solchen „Massengeschäft" ist es unvermeidlich, das Verfahren stark zu formalisieren. Der Auskunftsbetrieb wird weitestgehend formularmäßig abgewickelt. Mit der Bundeswehr wird ein Datenträgeraustauschverfahren praktiziert. Es liegt auf der Hand, daß bei dieser Sachlage Überlegungen angestellt werden, wie das Auskunftsverfahren weiter vereinfacht und beschleunigt werden kann. Entsprechende Forderungen kamen von den Stellen, die zahlreiche Auskunftsersuchen stellen müssen und die an raschen Antworten interessiert sind. Dies sind in erster Linie Strafverfolgungsbehörden, Sicherheitsbehörden und Gerichte. Das Bundeszentralregister hat daraufhin einen Organisationsvorschlag für die Er-

teilung von unbeschränkten Auskünften aus dem Zentralregister und von Auskünften aus dem Erziehungsregister durch unmittelbare Fernabfrage entwickelt.

Zu diesem Projekt habe ich mich kritisch geäußert. Die Intention des Bundeszentralregistergesetzes ist eindeutig auf eine weitgehende Abschottung der Vorstrafendaten gerichtet. Der ins Auge gefaßte Online-Verbund wäre insoweit ein Schritt zurück zum früheren Zustand der vollständigen Verfügbarkeit der Daten. Nach § 2 Abs. 2 Nr. 2 BDSG gilt mit dem Bereithalten zum Abruf der Gesamtbestand der Datei als übermittelt, und tatsächlich muß bei Eröffnung der unmittelbaren Fernabfrage damit gerechnet werden, daß davon in stärkerem Maße als bisher Gebrauch gemacht wird. Wegen dieser nicht von der Hand zu weisenden Mißbrauchsmöglichkeiten sollte die Entscheidung für oder gegen den Online-Anschluß durch den Gesetzgeber getroffen werden. Dabei müßte sehr sorgfältig geprüft werden, welche Stellen einen Online-Anschluß tatsächlich benötigen. Eine erste überschlägige Umfrage durch den Bundesminister der Justiz hat ergeben, daß ein akuter Bedarf nicht besteht. Sollte sich dieser Befund bei einer genaueren Analyse bestätigen, wird das Bundeszentralregister die Planung „Online-Anschluß" wohl vorerst zurückstellen und Alternativlösungen ins Auge fassen. Zum Bundeszentralregistergesetz siehe 4.1.3, S. 42, zur Auskunft an ausländische Stellen 4.1.2, S. 41, zur Direktabfrage allgemein 4.7 f., S. 55 f.

### 2.3 Deutsches Patentamt

Das Deutsche Patentamt speichert und verarbeitet zwar eine große Menge personenbezogener Daten; die damit verbundenen datenschutzrechtlichen Probleme sind aber vergleichsweise minimal, weil die Daten nahezu ausnahmslos veröffentlicht werden. Das Verfahren der Verarbeitung dieser Daten ist im einzelnen im Patentgesetz und in den dazu erlassenen Rechtsverordnungen geregelt. Die eindrucksvollen Sicherheitsvorkehrungen dienen weniger dem Datenschutz als der Sicherung der in den Patentunterlagen verkörperten wirtschaftlichen Werte und Interessen.

### 2.4 Deutsche Bundespost

#### 2.4.1 Allgemeines

Für die Post sind die meisten personenbezogenen Daten, die sie zu verarbeiten hat, nicht Grundlage eigener Entscheidungen, sondern Beförderungsgegenstand — sei es materiell im eigentlichen Postdienst, sei es immateriell im Fernmeldedienst mit seinen zahlreichen Leistungsangeboten. Einige personenbezogene Angaben sind unverzichtbar, um die Beförderungsleistung zu erbringen — in der Regel kaum mehr als Namen und Anschriften der Kommunikationspartner —; außerdem werden Bearbeitungsvermerke angebracht und eventuell registriert, und einige Daten entstehen bei der Abrechnung der Leistungen. Das Formularwesen der Post ist seit langem einheitlich durchstrukturiert; um der Rationalisierung willen werden regelmäßig nur die wirklich erforderlichen Mindestangaben erhoben und verarbeitet. Auskunft an Dritte über einzelne Leistungen z. B. über die Inhalte, Wege und Modalitäten von Postsendungen und Fernmeldeverbindungen darf die Post nur in wenigen, gesetzlich bestimmten Fällen erteilen; das Post- und Fernmeldegeheimnis ist im Grundgesetz (Artikel 10 GG) gewährleistet.

Diese sehr guten Voraussetzungen für eine datenschutzgerechte Verwaltungspraxis (auf die ich bereits früher hingewiesen habe, vgl. 3. TB zu 3.7, S. 30), rechtfertigen aber noch nicht den Schluß, daß die Forderungen des Datenschutzes bei der Post vollkommen realisiert seien. Das Post- und Fernmeldegeheimnis ist zwar insofern strenger als das Datenschutzrecht, als die Voraussetzungen seiner Durchbrechung sehr restriktiv bestimmt sind; es richtet sich aber nur gegen Dritte, läßt also die Speicherung der Daten sowie ihre Auswertung und Nutzung für eigene Zwecke der Post unberührt.

Der berechtigte Hinweis der Post auf die erfreulich strenge Gewährleistung des Fernmeldegeheimnisses darf also nicht zu der Erwartung verleiten, allein mit diesem Instrument auch die Datenschutzanforderungen bewältigen zu können, die sich aus der Einführung der Neuen Medien ergeben (dazu Weiteres unter 2.4.4). Dort geht es um eine neue Dimension von Datensammlung und -auswertung, und die enorme Vielfalt der möglichen Kommunikationen wird die Kontrolle erschweren. Überdies ist in den letzten Jahren deutlich geworden, daß der Fernmeldeverkehr mit verhältnismäßig geringem Aufwand abgeleitet und abgehört werden kann (vgl. den Bericht des Untersuchungsausschusses in Sachen Strauß/Scharnagl, BT-Drucksache 8/3835). Durch diese neuen Entwicklungen und Einsichten ist auch die Deutsche Bundespost zu neuen Anstrengungen im Interesse verbesserten Datenschutzes herausgefordert.

#### 2.4.2 Aufzeichnungen über Telefongespräche

Im meinem 3. Tätigkeitsbericht bin ich bereits ausführlich auf die Problematik der Aufzeichnung über Telefongespräche im elektronischen Wählsystems (EWS) eingegangen, mit dem einige Fernmeldeämter der Deutschen Bundespost ausgestattet sind (vgl. dort Nr. 3.7.1, S. 31).

Nach einer sehr lebhaften Reaktion in den Medien hatte die Deutsche Bundespost den Betriebsversuch beendet und erklärt, die weiteren Schritte mit mir und dem Bundesminister des Innern abzustimmen. Inzwischen hat sich auch der Postausschuß des Deutschen Bundestages der Angelegenheit angenommen. In seinem Beschluß fordert er die Deutsche Bundespost auf, mit der Einführung des elektronischen Wählsystems dem Kunden auf Antrag die Möglichkeit einzuräumen, einen Einzelgesprächsnachweis zu erhalten. Dabei sind die Interessen der regelmäßigen Mitbenutzer des Fernsprechanschlusses zu berücksichtigen. Aus Gründen eines möglichst weitgehenden Datenschutzes soll die detaillierte Fernmelderechnung nur Datum, Anfangszeit und Ende des Gesprächs und gegebenenfalls die Vorwahlnummer des Angerufenen enthalten. Die

Nummer des Angerufenen wird ohne Zugriffsmöglichkeit für Dritte aufgezeichnet und bis zum Ablauf der Widerspruchsfrist verwahrt. Dieses Beweismaterial wird nur auf richterliche Anordnung herausgegeben.

Der Ausschuß geht ferner davon aus, daß die Deutsche Bundespost die Entwicklung preisgünstiger Zähleinrichtungen fachlich unterstützt, die beim Kunden selbst auf Antrag installiert werden können und gegen Manipulation und unbeabsichtigte Störungen hinreichend gesichert sind.

Damit ist meinen Forderungen im 3. Tätigkeitsbericht entsprochen worden. Ich hoffe, daß die Bundesregierung diesen Beschluß voll verwirklicht.

#### 2.4.3 Eintragung im amtlichen Fernsprechbuch

Auf die datenschutzrechtliche Problematik bei der Eintragung im Fernsprechbuch habe ich schon im 3. TB hingewiesen (Nr. 3.7.2, S. 31). Auch im letzten Jahr haben sich wieder Bürger an mich gewandt, weil sie sich durch häufige und unerwünschte Telefonanrufe belästigt fühlten. Der Ausschuß für das Post- und Fernmeldewesen des Deutschen Bundestages hat meine Anregungen anläßlich der Beratung des 3. TB aufgegriffen und den Bundesminister für das Post- und Fernmeldewesen aufgefordert, die Fernmeldeordnung entsprechend zu ändern. Dies ist inzwischen geschehen. § 39 Abs. 2 Satz 6 der Fernmeldeordnung lautet nunmehr: „Ein Eintrag kann auf Antrag für eine angemessene Frist unterbleiben, wenn der Teilnehmer glaubhaft macht, daß für ihn oder eine andere Person im Falle der Eintragung eine Gefährdung oder erhebliche Belästigung eintreten kann." Ich halte die Änderung für einen begrüßenswerten Schritt zur Verbesserung des Datenschutzes in diesem Bereich. Dabei gehe ich davon aus, daß die Post ihren Ermessensspielraum voll ausschöpfen und bei der Entscheidung über Anträge auf Nichteintragung großzügiger als bisher verfahren wird.

#### 2.4.4 Bildschirmtext

Bildschirmtextversuche werden z. Z. in Nordrhein-Westfalen (Raum Düsseldorf) und in Berlin durchgeführt. Die für beide Versuchsgebiete vorgesehene Teilnehmerzahl von jeweils 3 000 wurde bislang nicht erreicht. Zur Zeit sind etwa 5 000 Teilnehmer insgesamt an den Dienst angeschlossen, in den rd. 750 Anbieter ihre Informationen eingeben. Besondere Bedeutung kommt hierbei denjenigen Anbietern zu, die ihre Dienstleistungen unter Zuhilfenahme einer eigenen ADV-Anlage im sog. Rechnerverbund anbieten. Zur Zeit sind 18 Anbieter auf diese Weise mit den Bildschirmtext-Zentralen verbunden.

Ein Nutzungsschwerpunkt zeichnet sich im Bereich der Warenversandhäuser und des Bankwesens ab.

Die wesentlichen datenschutzrechtlichen Probleme sind in den von den Datenschutzbeauftragten des Bundes und der Länder beschlossenen „Grundsätzen für den Datenschutz bei den Neuen Medien" vom 11. Dezember 1980 (s. Anhang zu meinem 3. TB, S. 66 ff.) dargelegt. Darüber hinaus sehe ich Gefährdungen des Datenschutzes insbesondere darin, daß die Anbieter aus kommerziellen Gründen daran interessiert sind, die über Bildschirmtext erlangten Daten der Teilnehmer möglichst lange festzuhalten und möglichst vielfältig auszuwerten und zu nutzen, was durch die hohe Leistungsfähigkeit der ADV-Anlagen möglich wird. So lassen sich beispielsweise aus der Art und Weise, wie der Bildschirmtextteilnehmer in dem „elektronischen Katalog" eines Warenhauses blättert, wie er Angebote und Preise vergleicht, zu seiner Kaufentscheidung und schließlich zur Wahl der Finanzierungsform gelangt, für das Versandhaus wichtige Rückschlüsse auf das Konsumverhalten und das *Persönlichkeitsbild* des Kunden gewinnen. Für das Handelsunternehmen wäre es z. B. möglich, künftig diesem Kunden — automatisch über Bildschirmtext — speziell auf ihn und seine Interessen zugeschnittene Angebote zukommen zu lassen und so eine normalerweise vorhandene Hemmschwelle gegenüber einem Kauf zu überwinden, ohne daß der Kunde dies bemerkt. Das Persönlichkeitsbild des Kunden könnte aber auch für Dritte von großem Interesse sein. Das Abbild des Betroffenen würde auf diese Weise in noch nicht voll voraussehbarer Weise verfügbar; der Mensch, um den es geht, würde in höherem Maße manipulierbar. Ich halte es schon auf der Grundlage des gegenwärtigen Datenschutzrechts für höchst bedenklich, daß Anbieter die ihnen vom Kunden zu bestimmten Zwecken (Lieferung von Waren, Dienstleistungen) überlassenen Informationen so aufbereiten und auswerten, daß sie auch für andere darüber hinausgehende Zwecke genutzt werden können. Zumindest ist zu fordern, daß die Bildschirmtext-Teilnehmer über die Folgen der Dateneingabe umfassend und genau informiert werden.

Bildschirmtext im endgültigen Ausbauzustand wird ein ADV-gestütztes Kommunikationssystem darstellen, bei dem sich schon aus der extrem hohen Teilnehmerzahl sowie der großen räumlichen Ausdehnung besondere Anforderungen an die Datensicherung ergeben. In diesem Zusammenhang muß die Frage erörtert werden, ob die Verarbeitung personenbezogener Daten von besonderer Vertraulichkeit und Bedeutung für den Betroffenen überhaupt in offenen Kommunikationsnetzen wie dem Bildschirmtext-Dienst zugelassen werden kann.

Nach dem Informationsbesuch bei der Bildschirmtext-Zentrale Düsseldorf (s. 3. TB, Nr. 3.8.3, S. 34) haben meine Mitarbeiter bei der Bildschirmtext-Zentrale in Berlin eine datenschutzrechtliche Prüfung durchgeführt. Wie in Düsseldorf wurde auch in Berlin meiner Kontrollbefugnis das Postgeheimnis entgegengehalten.

Ich habe den Bundesminister für das Post- und Fernmeldewesen davon unterrichtet und um Stellungnahme gebeten. In seiner Antwort hat er ein Prüfverfahren vorgeschlagen, von dessen Praktikabilität ich mich bei nächster Gelegenheit überzeugen werde. Über das Ergebnis werde ich berichten.

Die Ausführungen in meinem 3. Tätigkeitsbericht über die wissenschaftlichen Begleituntersuchungen zu den gegenwärtig laufenden Feldversuchen sind insofern zu ergänzen, als inzwischen nicht nur jede

hundertste, sondern schon jede zwanzigste Anschaltung in ihrem Ablauf vollständig gespeichert und für die wissenschaftliche Auswertung bereitgehalten wird. Nach wie vor halte ich auch außerhalb der wissenschaftlichen Begleituntersuchungen zu den beiden Bildschirmtextversuchen die Erforschung der rechtlichen und soziologischen Probleme des Bildschirmtextes für außerordentlich wichtig (vgl. hierzu 3. TB, Nr. 3.8.2, S. 34). Mit großem Bedauern mußte ich zur Kenntnis nehmen, daß nach Abschluß der Vorstudie das Forschungsprojekt DARUTS des Berliner Instituts für Zukunftsforschung von seiten des Bundesministers für Forschung und Technologie vorläufig nicht weiter gefördert wird.

Nach dem Beschluß des Deutschen Bundestages vom 9. April 1981 über die Einsetzung der Enquete-Kommission „Neue Informations- und Kommunikationstechniken" hat die Kommission auch die Aufgabe, die datenschutzrechtlichen Aspekte darzustellen und Empfehlungen für entsprechende Entscheidungen zu erarbeiten. Zur Unterstützung der Kommission bereite ich zur Zeit auf deren Wunsch eine entsprechende Stellungnahme vor.

#### 2.4.5 Gehaltskontoverfahren

Das von mir beanstandete Gehaltskontoverfahren der Deutschen Bundespost (siehe 3. TB Nr. 3.7.5, S. 32 f.) soll nach dem Willen des Bundesministers für das Post- und Fernmeldewesen im Einvernehmen mit dem Hauptpersonalrat unverändert fortgeführt werden. Der Kern meiner Bedenken lag darin, daß die Personalstelle die Angaben in der Kartei für andersartige Personalentscheidungen nutzen könnte. Dem will der Bundesminister für das Post- und Fernmeldewesen dadurch begegnen, daß er anordnet, diese Angaben nur zur Beantwortung von Dekkungsanfragen zu nutzen und nicht für andere Zwecke. Überdies soll der Bedienstete, der einen Antrag auf Teilnahme am Gehaltskontoverfahren stellt, deutlicher darauf hingewiesen werden, daß Auszahlungssperren aus dem genannten Grund dem Beschäftigungsamt mitgeteilt werden.

Ich halte die von der Post geplanten Änderungen noch nicht für ausreichend. Die von mir aufgezeigten Risiken sind nicht gewürdigt, die Vorschläge für Alternativlösungen sind nicht in Erwägung gezogen worden. Die von der Post vertretene Ansicht, daß der Bedienstete mit dem Antrag auf Teilnahme am Gehaltskontoverfahren gleichzeitig in die vorgesehene Speicherung und Übermittlung seiner Daten einwillige, kann ich nicht teilen. Ich hoffe, daß der Bundesminister für das Post- und Fernmeldewesen sich doch noch einer betroffenenfreundlicheren Auslegung des Bundesdatenschutzgesetzes anschließen wird.

### 2.5 Rundfunkanstalten des Bundes

Bei der Deutschen Welle und beim Deutschlandfunk wurden Prüfungen durchgeführt.

Der Intendant des Deutschlandfunks hat während der Prüfung und im Anschluß daran Zweifel an meiner Prüfungskompetenz geäußert. Ich halte diese für unbegründet. Deutschlandfunk und Deutsche Welle sind öffentliche Stellen des Bundes nach § 7 BDSG. Die von ihnen verarbeiteten Daten werden nach § 1 Abs. 2 BDSG grundsätzlich durch das BDSG geschützt. § 1 Abs. 3 BDSG nimmt nur solche Daten aus, die durch Unternehmen des Rundfunks ausschließlich zu eigenen publizistischen Zwecken verarbeitet werden. Daraus folgt zwingend, daß die Rundfunkanstalten im übrigen voll dem BDSG und damit auch der Prüfung des Bundesbeauftragten unterliegen.

Die verfassungsrechtlich garantierte Rundfunkfreiheit wird dadurch nicht beeinträchtigt. Auch wenn man davon ausgeht, daß Datenschutzmaßnahmen auch Rückwirkungen auf die redaktionelle Arbeit haben können, ist eine Beeinträchtigung der Rundfunkfreiheit ausgeschlossen. Die Maßnahmen der Datenschutzkontrolle haben keine rechtlich bindende Wirkung und schränken die Entscheidungsfreiheit der Rundfunkanstalten nicht ein.

Die Prüfungen haben nicht ergeben, daß schutzwürdige Belange Betroffener durch die Datenverarbeitung aktuell beeinträchtigt werden. Beide Rundfunkanstalten hatten auch interne Datenschutzbeauftragte bestellt. Ich mußte jedoch Verstöße gegen Vorschriften des BDSG feststellen, die jederzeit zur Beeinträchtigung von schutzwürdigen Belangen der Betroffenen hätten führen können: Beide Rundfunkanstalten führten keine vollständige Übersicht nach § 15 Nr. 1 BDSG, die für die Planung und Durchführung von Sicherungsmaßnahmen nach § 6 BDSG notwendig ist, und besaßen keine ausreichende Dokumentation, um die ordnungsgemäße Anwendung der DV-Programme zu sichern. Beim Deutschlandfunk habe ich außerdem festgestellt, daß die organisatorischen Maßnahmen zum Schutz personenbezogener Daten nach § 6 BDSG unzulänglich waren. Die Mängel sind teilweise bereits behoben, im übrigen ist ihre Beseitigung in Angriff genommen. Dem Wunsch, mich daran beratend zu beteiligen, komme ich gern nach.

### 2.6 Personalverwaltungen

#### 2.6.1 Bundesamt für Finanzen — Bundesbesoldungsstelle —

Die Beamten und Angestellten des Bundes, mit Ausnahme des Verteidigungsbereichs und der Sonderverwaltungen, erhalten ihre Besoldung bzw. Vergütung durch die Bundesbesoldungsstelle ausgezahlt. Die Zahlbarmachung der Löhne der Arbeiter des Bundes über die Bundesbesoldungsstelle ist in einigen Bereichen aufgenommen worden. Ich habe die Bundesbesoldungsstelle, die eine Abteilung des Bundesamtes für Finanzen ist, prüfen lassen. Datenschutzrechtliche Verstöße wurden dabei nicht festgestellt; meine Anregungen, die Datenverarbeitung noch sicherer zu gestalten, wurden in vollem Umfang übernommen.

#### 2.6.2 Personalinformationssystem PERFIS des Bundesministers der Verteidigung

a) Ich habe in meinem 3. Tätigkeitsbericht (vgl. dort Nr. 3.5.5.1, S. 28) bereits auf die Prüfung des „Per-

sonalführungs- und -informationssystems Soldaten" (PERFIS) hingewiesen. Hieran haben sich im abgelaufenen Berichtszeitraum Schriftverkehr sowie Beratungen mit dem Bundesministerium der Verteidigung angeschlossen.

Das System PERFIS hat die Aufgabe, die personalführenden Stellen der Bundeswehr in ihrer Arbeit zu unterstützen und sie sowie andere definierte Bedarfsträger mit Informationen über das Personal-Ist an aktiven Soldaten (Grundwehrdienstleistende, Soldaten auf Zeit und Berufssoldaten) zu versorgen. In seiner Funktionsweise kann das System PERFIS jedoch nicht für sich betrachtet werden, sondern ist in das „Informationskonzept Personalwesen" einzuordnen. Hierbei ist die Funktion von PERFIS nicht nur in Friedenszeiten, sondern auch im Spannungs- und Verteidigungsfall zu beurteilen. Für letzteren ist entscheidend, daß das System PERFIS innerhalb des bestehenden Informationskonzepts auf Datenbestände anderer Systeme zurückgreift und die Steuerung und den Einsatz des gesamten Personals, also nicht nur der aktiven Soldaten, übernimmt.

Vor diesem komplexen Hintergrund fanden im vergangenen Jahr die Gespräche und der Schriftverkehr über die Erforderlichkeit der Erhebung und Speicherung der Daten, über Nutzungsregelungen und Übermittlungsermächtigungen sowie über die Einbettung der Wehrpsychologie in die Organisation der Personalabteilung statt. Die Untersuchungen werden im nächsten Jahr fortgesetzt.

b) Ein so großer und differenzierter Datenbestand, wie ihn das System PERFIS verwaltet, eignet sich naturgemäß auch für andere Zwecke als die Aufgabe Personalverwaltung. Wegen der unvergleichlichen Vielfalt der Personalaufgaben in den Streitkräften ist jedoch die Abgrenzung zwischen Personalaufgaben und sonstigen Aufgaben häufig nur schwer zu vollziehen. Ich wollte mir ein Bild davon machen, wie diese notwendige Abschottung in der Praxis realisiert ist, und habe deshalb exemplarisch die Beziehungen zwischen der speichernden Stelle des Systems PERFIS und dem für Wehrpsychologie zuständigen Referat in der Personalabteilung überprüfen lassen.

Bei der Überprüfung von drei wehrpsychologischen Forschungsprojekten haben sich datenschutzrechtliche Probleme ganz anderer Art herausgestellt. Sie ergeben sich aus der Tatsache, daß eine Armee nach dem Prinzip von Befehl und Gehorsam organisiert sein muß und ein noch so guter, datenschutzfreundlicher Forschungsplan in der Praxis durch dieses Prinzip außer Kraft gesetzt werden kann.

Bei einem sozialpsychologischen Forschungsprojekt über Suizidversuche in der Bundeswehr war ein Verfahren gewählt worden, das zwar auf Freiwilligkeit beruhen sollte, das aber tatsächlich die Entscheidungsfreiheit der Betroffenen nicht gewährleistete. Es war auch Anonymität versprochen, gleichwohl war eine Verknüpfung der Testdaten mit anderen Angaben möglich. Da dieses Projekt im wesentlichen vor Erlaß des BDSG entworfen und zu einer Zeit durchgeführt wurde, wo noch keine einschlägigen Erfahrungen bestanden, habe ich mich darauf beschränkt, den Bundesminister der Verteidigung eindringlich zu bitten, die Beachtung der Persönlichkeitsrechte auch in diesem Zusammenhang noch schärfer zu kontrollieren. Es sind vor allem besondere Anforderungen an die Freiwilligkeit von Einwilligungserklärungen zu stellen. Die zuständige Stelle hat mir zugesagt, diese Anregung aufzugreifen.

#### 2.6.3 Tests bei Offiziersbewerberprüfungen

Aufgrund einer Eingabe habe ich mich mit der Frage befaßt, inwieweit Bewerber für die Offizierslaufbahn Auskunft über oder Einsicht in die Prüfungs-/Test-Unterlagen bei der Offiziersbewerber-Prüfzentrale der Bundeswehr in Köln (OPZ) erhalten.

Für Bewerber, die bereits in einem Soldatenverhältnis stehen oder in ein solches übernommen werden, richtet sich das Einsichtsrecht in die Personalunterlagen nach § 29 Abs. 3 Soldatengesetz. Danach hat der Soldat ein Recht auf Einsicht in seine vollständigen Personalakten. Dazu gehören alle ihn betreffenden Vorgänge; das sind regelmäßig auch Qualifikationstests, wie sie von der OPZ vorgenommen werden.

Für Bewerber, die nicht in einem Soldatenverhältnis stehen, sind für das Einsichtsrecht die Vorschriften des § 2 Abs. 3 Ziff. 2 i. V. m. § 29 Abs. 1 Verwaltungsverfahrensgesetz maßgeblich. Danach hat die Behörde den Beteiligten Einsicht in die das Verfahren betreffenden Akten zu gestatten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung ihrer rechtlichen Interessen erforderlich ist. Ausschließungsgründe gemäß § 29 Abs. 2 Verwaltungsverfahrensgesetz waren im konkreten Fall nicht ersichtlich.

Der Bundesminister der Verteidigung hat das Auskunftsverfahren unterschiedlich geregelt, je nachdem, ob der Bewerber durch die OPZ angenommen oder abgelehnt wurde.

Über die in Dateien der OPZ gespeicherten Daten angenommener Bewerber erhält der Betroffene keine Auskunft. Der Bundesminister der Verteidigung begründet seine Entscheidung damit, daß die Offenlegung dem Betroffenen Rückschlüsse auf Prüfverfahren, Prüfmethoden, Auswahlkriterien und Verwendungsgrundsätze der Bundeswehr in einem solchen Umfang ermöglichen würde, daß die sachgerechte Auswahl von geeigneten Offizieren beeinträchtigt würde. Die Bewerber hätten jedoch die Möglichkeit, die wesentlichen Ergebnisse der durchgeführten Prüfungen und Tests, die in einem Prüfbericht zusammengefaßt seien, einzusehen. Dieser Prüfbericht gehe in die Personalakten des Betroffenen. Ich habe dem entgegengehalten, daß sich auskunftsausschließende Gründe allein aus § 26 Abs. 4 BDSG ergeben könnten und nicht erkennbar sei, auf welche dieser Ausschließungsgründe der BMVg seine Entscheidung stütze. Der BMVg hat entschie-

den, daß in Zukunft Auskunft aus dieser Datei erteilt werde.

Bisher wurden die Daten der abgelehnten Bewerber nach Abschluß des Prüfverfahrens in einer separaten Suchdatei geführt. Die Suchdatei enthielt Name, Vorname, Anschrift, Personenkennziffer (PK), Bewerbungs- und Prüfungsdatum des Bewerbers und einen Hinweis auf den Verbleib der Bewerberakte. Auf Anfrage erhielt der abgelehnte Bewerber über diese Daten Auskunft. Nachdem ich den Datenumfang der Suchdatei in Frage gestellt habe, weil Daten wie Anschrift, Bewerbungsdatum usw. für eine Suchdatei, die lediglich zum Wiederauffinden der Prüfungsakte dient, nicht erforderlich sind, hat der Bundesminister der Verteidigung den Datenumfang der Suchdatei auf die PK und das gewünschte Eintrittsdatum des Bewerbers beschränkt; letzteres ist für die Aufbewahrungsdauer der Bewerbungsakte erforderlich. Außerdem werden abgelehnte Bewerber nach Geburtsjahrgängen für statistische Auswertungen zusammengefaßt.

#### 2.6.4 Schwarze Personalakten bei einer Bundesbehörde

Der Personalrat einer Bundesbehörde hatte mich in mehreren Eingaben um die Klärung datenschutzrechtlicher Probleme gebeten. Bei einer Prüfung vor Ort stellten sich folgende Sachverhalte heraus:

a) Im ersten Fall hatte die Verwaltung beim Personalrat beantragt, der Entlassung eines Angestellten während der Probezeit zuzustimmen. Dem Antrag war ein Vermerk beigefügt, der Tatsachen und Werturteile über die dienstliche Befähigung des Angestellten enthielt (z. B. „ist überheblich", „schmalspurig", „nicht geeignet"). Auf schriftliche Fragen des Personalrats bestätigte die Verwaltung, daß sich dieser Vermerk nicht bei den Personalakten befinde, für den Angestellten ungünstige Unterlagen würden vielmehr in einer *gesonderten* Akte aufbewahrt.

   Die entsprechenden Schriftstücke waren beim Personalrat zu Unterlagen zusammengefaßt, die die gesetzlichen Merkmale des Dateibegriffs i. S. des § 2 Abs. 3 Nr. 3 BDSG erfüllen. Die schriftlichen Behauptungen bestätigten sich bei der Einsichtnahme in die über den Angestellten geführten Akten, und zwar

   — seine Personalakte,

   — eine Akte mit der Aufschrift „Beschwerden oder ähnliches über Angehörige des ... (Name der Dienststelle)".

   Beide Akten hatten ein unterschiedliches Aktenzeichen. In der zweiten Akte werden neben dem genannten Vermerk der Schriftwechsel mit dem Personalrat und negative Äußerungen über den Angestellten seitens der Mitarbeiter aufbewahrt. Dieser Tatbestand verstößt gegen das Gebot, keine vor dem Angestellten geheimen Personal-(neben-)Akten zu führen, und vereitelt gegebenenfalls seinen Anspruch auf Einsicht in die *vollständigen* Personalakten, der sich aus § 13 Abs. 1 BAT ergibt. Die Personalakten sollen ein vollständiges und lückenloses Bild über die Laufbahn und das dienstlich bedeutsame Verhalten des Angestellten bieten. Danach gehören alle über die persönlichen und dienstlichen Verhältnisse des Angestellten vorhandenen Urkunden und aktenmäßig festgehaltenen Vermerke zu den Personalakten. Dieser Grundsatz wurde von der Behörde verletzt, weil die der Kündigung zugrundeliegenden Tatsachenbehauptungen nicht in der Personalakte selbst, sondern getrennt davon in der zweiten Akte aufbewahrt werden, so daß sich der Grund der Kündigung nicht aus der Personalakte selbst ergibt.

   In seiner Antwort auf meine Beanstandung, die ich gem. § 20 Abs. 1 BDSG gegenüber dem Bundesminister des Innern ausgesprochen habe, bestreitet dieser zwar nicht den festgestellten Sachverhalt, wohl aber meine Zuständigkeit, die sich angeblich nicht auf die Überprüfung von Akten beziehe. Gerade der vorliegende Fall zeigt, wie anfechtbar diese von mir schon in vergangenen Tätigkeitsberichten abgelehnte Rechtsauffassung sein kann. Der datenschutzrechtlich relevante Sachverhalt hat sich hier übrigens bereits aus der Prüfung einer Datei ergeben. Falls der Gesetzgeber wünscht, daß ich derartigen Rechtsverstößen in Zukunft nicht mehr nachgehe, sollte das entsprechend klargestellt werden.

b) Auch im zweiten Fall hat der BMI meine Zuständigkeit bestritten. Nach Einsicht in die Personalakten ergab sich folgender Sachverhalt:

   Eine Außenstelle der betreffenden Behörde teilte der Hauptstelle in einem kurzen Schreiben mit, daß ein Angestellter nicht die Voraussetzungen für den Bewährungsaufstieg erfülle, er habe sich vielmehr überhaupt nicht bewährt. Dem Schreiben waren zwei sog. „Beurteilungsbeiträge" der Vorgesetzten beigefügt. Das Anschreiben befand sich in der Personalakte, nicht jedoch die Beiträge. Wenig später erhielt der Angestellte eine sog. „Abmahnung".

   Er forderte daraufhin schriftlich die Einsichtnahme in seine Personalakte, die ihm auch gewährt wurde. Zu diesem Zeitpunkt enthielt die Personalakte weder das Anschreiben noch die sogenannten „Beurteilungsbeiträge". Diese Unterlagen befanden sich vielmehr in einem Wiedervorlagevorgang in der Registratur. Später hat die Dienststelle eine Gesamtbeurteilung erstellt. Über den Verbleib der sog. „Beurteilungsbeiträge" ist nichts Näheres bekannt geworden.

   Aus meiner Sicht verletzt dieses Verfahren den Anspruch des Angestellten auf Einsicht in seine vollständigen Personalakten (§ 13 Abs. 1 BAT). Dieses sein Recht wurde ihm teilweise vereitelt, weil ihm anläßlich der Einsichtnahme weder das Anschreiben noch die beiden beigefügten „Beurteilungsbeiträge" vorgelegt wurden. Der Angestellte hatte somit keine Möglichkeit, zu Beschwerden und Behauptungen tatsächlicher Art, die für ihn ungünstig sind oder ihm nachteilig werden können, Stellung zu nehmen. Da die „Abmahnung" nicht ohne jeden konkreten Anhaltspunkt erfolgt sein dürfte — dann wäre sie willkürlich gewesen —, müssen die ihr zugrundeliegenden Tatsachenbehauptungen und die daraus

abgeleiteten Werturteile aus den Personalakten erkennbar sein. Die Kennzeichnung der beigefügten „Beurteilungsbeiträge" als solche sagt nichts darüber aus, ob es sich lediglich um Beiträge zu einer noch abzufassenden Beurteilung oder aber um Unterlagen handelt, denen materiell der Charakter einer Beurteilung zukommt. Für letzteres spricht, daß die „Abmahnung" ohne eine „Beurteilung im formellen Sinne" auf der Grundlage der sogenannten „Beurteilungsbeiträge" erfolgte.

Wegen der Besonderheiten dieses Falles habe ich von einer Beanstandung abgesehen.

Ungeachtet der unterschiedlichen Rechtsauffassungen zu meiner Zuständigkeit hat der BMI in beiden Fällen, wie er schreibt, „sichergestellt, daß die entsprechenden dienstrechtlichen Vorschriften in Zukunft beachtet werden".

#### 2.6.5 Auskunft über die gespeicherten Daten von Mitarbeitern

Die Deutsche Bundesbahn (DB) speichert wie jede Personalverwaltung eine Reihe personenbezogener Daten über ihre Mitarbeiter (z. B. zur Berechnung der Bezüge, Erstellung von Lohnsteuerbescheinigungen).

Ich habe feststellen müssen, daß bei der DB bis heute kein Verfahren besteht, das eine zügige Auskunftserteilung gem. § 26 BDSG für die Mitarbeiter der Bundesbahn ermöglicht. Zwar wurden im Jahre 1981 die Datenarten der Mitarbeiterdateien in einem Amtsblatt der DB bekanntgemacht; ein Eisenbahner, der im Mai 1979 ein Auskunftsersuchen stellte, um die über ihn gespeicherten Dateninhalte zu erfahren, erhielt diese Auskunft jedoch erst im März 1981 und erst mit meiner Hilfe. Zu diesem Fall führte die DB aus, es sei der Eindruck entstanden, der Mitarbeiter habe sein Auskunftsersuchen zurückgezogen, was aber nicht belegt wurde und nach Aussage des Betroffenen auch nicht der Fall war. Was das Auskunftsverfahren allgemein betrifft, ist die Bundesbahn der Ansicht, dabei handele es sich „... (um) kostspielige, vom BDSG nicht vorgesehene Vorsorgemaßnahmen für hypothetische Fälle ...". Dies kann ich nicht akzeptieren. Es gibt sowohl in der öffentlichen Verwaltung als auch in der Privatwirtschaft hinreichend Vorbilder, wie das Auskunftsrecht des Betroffenen mit vertretbarem Aufwand realisiert werden kann. Ich gehe davon aus, daß es auch der DB möglich ist, einen gangbaren Weg zu finden, der es ihr ermöglicht, Auskunftsersuchen ihrer Mitarbeiter in angemessener Zeit zu beantworten.

### 2.7 Sozialversicherung und Arbeitsverwaltung

#### 2.7.1 Datenverarbeitung und Datenschutz bei der Bundesversicherungsanstalt für Angestellte

In der ersten Hälfte des Berichtszeitraumes haben meine Mitarbeiter eine zweiwöchige Kontrolle gemäß § 19 Abs. 1 BDSG bei der Bundesversicherungsanstalt für Angestellte (BfA) durchgeführt.

Die BfA ist einer der großen Anwender in meinem Zuständigkeitsbereich. Zur Betreuung der Versicherten ist eine moderne Datenverarbeitungsanlage eingesetzt. Zur Zeit steht ein Sachbearbeiterdialog kurz vor dem Einsatz, der die Effizienz der Anlage noch erhöhen wird. Technisch und organisatorisch ist ein hoher Stand erreicht. Auch die Sicherungsmaßnahmen für das Rechenzentrum halte ich für vorbildlich.

Von der Umsetzung des Datenschutzes in die Praxis habe ich insgesamt einen positiven Eindruck gewonnen. Dies gilt trotz der nachstehend geschilderten Probleme und obwohl ich einige Teilbereiche, z. B. den Personalbereich, nicht untersucht habe.

Folgende Mängel wurden festgestellt:

— Interne Übersicht gemäß § 15 Abs. 2 BDSG
  Die Übersicht der BfA enthält alle notwendigen Informationen. Lesbarkeit und Transparenz sind jedoch noch verbesserungsfähig.

— Einbettung des Datenschutzes in die Gesamtorganisation der BfA
  Ich habe trotz meiner bisher sehr guten Erfahrungen aus der Zusammenarbeit mit dem Datenschutzbeauftragten der BfA darauf hingewiesen, daß Ergänzungen und Erweiterungen möglich und erforderlich sind. Insbesondere halte ich die Schaffung einer EDV-Revision für unerläßlich.

— Technische und organisatorische Mängel
  Während die Sicherung der untersuchten automatisiert geführten Dateien einen hohen Stand erreicht hat, gibt es in konventionellen Verfahren erhebliche Probleme. Besucher könnten sich im Hause der BfA Zugang zu Versicherten-Unterlagen verschaffen. Ich bin überzeugt, daß eine technisch-organisatorische Absicherung der Stellen, an denen solche Unterlagen vorhanden sind, möglich ist, ohne Bürgernähe und Qualität der Beratungstätigkeit der BfA zu beeinträchtigen.

Arbeitsschwerpunkt der Prüfung war das sog. *Rehabilitations-Gesamtsystem.*

Hier handelt es sich in der jetzt realisierten Ausbaustufe um ein automatisches Verfahren, das die Sachbearbeitung und die ärztliche Begutachtung von Rehabilitationsleistungen unterstützen und steuern soll. Kern des Verfahrens ist das Rehabilitationskonto (Reha-Konto), in dem die Daten gespeichert werden, die bei der Verarbeitung der ärztlichen Gutachten bei allgemeinen Erkrankungen sowie der ärztlichen Entlassungsberichte nach Klinikaufenthalten entstehen. Eine Vorstellung von der Größe des Systems vermittelt die Zahl der stationären Heilbehandlungen wegen allgemeiner Erkrankungen mit dazugehörenden Gutachten; es sind ca. 300 000 pro Jahr. Ich habe bei meinem Besuch feststellen können, daß die BfA nicht der Versuchung erlegen ist, jedes nur denkbare Datum in diesen ohnehin schon hochsensiblen Datenbestand zu übernehmen. Sie hat vielmehr aus grundsätzlichen medizinisch-fachlichen und datenschutzrechtlichen Erwägungen auf die Speicherung einer Reihe von Merkmalen verzichtet. Es sind dies insbesondere:

— psychosoziale Belastung

— Aussagen zu Trink- und Rauchgewohnheiten

— Familienanamnese.

Im Zusammenhang mit der organisatorischen Einbettung des Reha-Gesamtsystems sehe ich noch einige klärungsbedürftige Probleme:

— Gegenwärtig erhalten die Sachbearbeiter der Rehabilitationsabteilung Kenntnis von Verwaltungsdaten und medizinischen Daten, ärztliche Diagnosen und Befunde eingeschlossen. Ich habe angeregt zu prüfen, ob ärztliche Daten und Verwaltungsdaten voneinander getrennt werden können.

— Während der ärztliche Entlassungsbericht an eine Mehrzahl von Stellen geht, ist ein Durchdruck für den Betroffenen nicht vorgesehen. Es soll ihm vielmehr überlassen bleiben, ob er sich zwecks Unterrichtung an den behandelnden Hausarzt wendet. Ich halte es für wünschenswert, den Betroffenen grundsätzlich über seinen Gesundheitszustand in geeigneter Form zu unterrichten.

— Akten über „Gesundheitsmaßnahmen wegen allgemeiner Erkrankungen" werden vier Jahre aufbewahrt, dagegen z. B. Unterlagen über Maßnahmen wegen Übergewichts und psychischer Erkrankungen zehn Jahre. In Gesprächen mit Medizinern der BfA sind diese sehr langen Aufbewahrungsfristen aus medizinischer Sicht ausführlich begründet worden. Ich habe angeregt zu prüfen, ob bei einer Abwägung der medizinischen Belange mit dem Interesse des Betroffenen an einer zeitnahen Behandlung seines Einzelfalles nicht kürzere Aufbewahrungsfristen für die genannten Ausnahmefälle möglich sind.

— Außerdem habe ich noch weitere Einzelpunkte angesprochen, z. B.

  — Kryptographische Verschlüsselung des gesamten Datenverkehrs der BfA mit Stellen in der Bundesrepublik

  — Zugangskontrollsystem

  — Registrierung von Ferngesprächen.

  Die BfA hat in einer ausführlichen ersten Stellungnahme aufgezeigt, daß manche der von mir aufgeworfenen Fragen längerfristiger Erörterungen bedürfen, so daß eine abschließende Stellungnahme noch nicht möglich sei. Insbesondere die Trennung von medizinischen und Verwaltungsdaten erfordere gegebenenfalls umfangreiche organisatorische Änderungen.

  Es wird in der Stellungnahme deutlich, daß sich die BfA derzeit intensiv um eine Lösung der aufgezeigten Probleme bemüht. Weitere Gespräche innerhalb der BfA sowie zwischen der BfA und Mitarbeitern meines Hauses werden im nächsten Berichtsjahr sicherlich zu konkreten Ergebnissen führen.

#### 2.7.2 Sozialbericht bei Abhängigkeitskranken

In meinem 3. Tätigkeitsbericht habe ich über den Sozialbericht bei Abhängigkeitskranken informiert (siehe dort Nr. 3.10.2.1, S. 39). Seitdem hat die dort genannte Arbeitsgruppe ihre Erörterungen beendet. Danach sind die Ergebnisse der Beratungen durch die in der Arbeitsgruppe vertretenen Datenschutzbeauftragten zusammengefaßt und der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorgelegt worden. Diese hat in ihrer Sitzung am 28./29. September 1981 einen Beschluß gefaßt, dessen wesentliche Teile wie folgt lauten:

„Für die nach § 1236 RVO und den sonstigen einschlägigen Bestimmungen (z. B. des Angestellten- und Knappen-Versicherungsrechts) von den Leistungsträgern zu treffenden Entscheidungen wird ein Formular ‚Sozialbericht' verwendet, dessen bisherige Fassung nicht den datenschutzrechtlichen Anforderungen entspricht. Das Formular sollte klarer als bisher erkennbar machen, daß die Mitwirkung des Betroffenen durch § 60 SGB I begrenzt wird. Erheblichkeit und Erforderlichkeit sind danach im Einzelfall zu prüfen, insbesondere im Hinblick auf

— Zuständigkeit für die Leistungsgewährung,

— Erfolgsaussichten der Suchtbehandlung,

— Zeitpunkt des Therapiebeginns,

— Auswahl der Behandlungsstätte und

— Auswahl der Leistungen zur Rehabilitation in dem in den §§ 1237 bis 1237b RVO bestimmten Umfang.

Daraus folgt, daß das Formular nicht in allen Fällen vollständig auszufüllen ist (‚Rahmenformular'). Dies sollte durch einen Hinweis in der ‚Ergänzenden Information' zum Sozialbericht klargestellt werden.

Es wird vorgeschlagen, das Formular wie folgt neu zu strukturieren:

1. Das Formular wird in einen datenerhebenden und einen bewertenden Teil gegliedert. Der erhebende Teil hat sich auf Tatsachenfeststellungen beim Betroffenen zu beschränken. Der bewertende Teil enthält die Begutachtung des Sozialarbeiters und etwaige von diesem erhobene anderweitige Tatsachen. Für den erhebenden Teil kommen etwa die Fragen 1 bis 3 und 5, für den bewertenden Teil die Fragen 4 und 6 bis 10 des bisherigen Formulars in Betracht. Die zuständigen Leistungsträger werden gebeten, auf dieser Grundlage das Formblatt neu zu entwerfen und die Konferenz über das Ergebnis ihrer Beratungen zu informieren.

2. In der ‚Ergänzenden Information' zum Sozialbericht sollte auf folgende Punkte hingewiesen werden:

   a) Angaben zur Dosis des Rauschmittels werden nur bei Alkohol und ‚legalen' Medikamenten erhoben.

   b) Auf die Tatsache, daß strafrechtlich relevante Hinweise nicht gegeben zu werden brauchen, sollte wegen der besonderen Bedeutung gerade bei den nach Ziffer 4 zu erhebenden Daten dort nochmals hingewiesen werden.

   c) Daten über laufende Strafverfahren und verbüßte Haftstrafen sind nur zu erheben, soweit

diese in den Zeitraum der Rehabilitationsmaßnahme fallen können.

d) Daten, die nur für die Behandlung des Betroffenen relevant sind, dürfen nicht erhoben werden, da § 1236 RVO insoweit keine Rechtsgrundlage bietet. Sie können jedoch mit Einwilligung des Betroffenen erhoben und den Behandlungseinrichtungen direkt zugeleitet werden."

Ferner wurden in dem Beschluß detaillierte Vorschläge zu einer Neufassung der „Erklärung des Betreuten" gemacht, die Teil des Sozialberichtsformulars ist.

Der Beschluß liegt nunmehr den an der Arbeitsgruppe beteiligten Rentenversicherungsträgern und Freien Wohlfahrtsverbänden zur Beratung vor. Nach deren Abschluß wird die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erneut über den Sozialbericht in der dann überarbeiteten Fassung beschließen.

#### 2.7.3 Erhebungsbogen der Krankenkassen bei Krankenhauspflege

Nach § 184 Abs. 1 RVO wird Krankenhauspflege (zeitlich unbegrenzt) gewährt, wenn die Aufnahme in ein Krankenhaus erforderlich ist, um die Krankheit zu erkennen oder zu behandeln oder Krankheitsbeschwerden zu lindern. Danach kommt Krankenhauspflege nicht in Betracht, wenn ein Dauerzustand vorliegt, der nicht mehr einer Heilung, Besserung, Verhütung der Verschlimmerung oder der Linderung von Krankheitsbeschwerden zugänglich ist, wenn also die erforderlichen Pflegemaßnahmen lediglich dem Zweck dienen, einem Zustand der Hilflosigkeit zu begegnen (Pflegefälle).

Diese Unterscheidung ist für die Frage der Kostenträgerschaft von Bedeutung, weil nur die notwendige Krankenpflege (in einem Krankenhaus) Teil der gesetzlichen Krankenhilfe ist, die von den Krankenkassen zu gewähren ist, nicht aber die allgemeine Pflege bei Hilflosigkeit.

Zur Abgrenzung zwischen Behandlungs- und Pflegefällen im Rahmen stationärer Krankenversorgung haben die Spitzenverbände der Krankenkassen ein Formblatt entwickelt, das in einschlägigen Fällen von dem behandelnden Krankenhausarzt ausgefüllt und der Krankenkasse übermittelt werden soll; anhand eines umfangreichen Fragenkatalogs soll der Krankenkasse die Entscheidung ermöglicht werden, ob es sich im Einzelfall um einen Fall der Krankenpflege handelt, deren Kosten die Krankenkasse im Rahmen der gesetzlichen Krankenhilfe zu erstatten hat, oder ob ein allgemeiner Pflegefall wegen Hilflosigkeit vorliegt. Die Verwendung dieses Erhebungsbogens wurde allen Mitgliedskassen der Spitzenverbände empfohlen.

Der Erhebungsbogen enthält neben den Angaben zur Person des Patienten und den Aufnahmedaten Fragen zur Diagnose, zum Befund bis hin zu zum Teil sehr detaillierten Fragen zur Therapie und zum Therapiekonzept.

Gegen diesen Erhebungsbogen wurden von verschiedenen Seiten datenschutzrechtliche Bedenken geltend gemacht. So hat sich eine sozialpsychiatrische Klinik dagegen gewandt, daß auf der Grundlage dieses Fragebogens Informationen erhoben werden, die im Zusammenhang mit § 184 Abs. 1 RVO für die Beurteilung der Erforderlichkeit der Krankenhauspflege nicht benötigt werden; insbesondere werden die einzelnen Fragen zur Therapie beanstandet, die den Eindruck erweckten, als ob die Maßnahmen des Arztes überwacht würden (Häufigkeit der Visiten, Dosierung von Medikamenten). Aus dem Bereich eines Landes wurde bekannt, daß die Erhebungsbogen von den Kliniken dieses Landes für die gesetzlichen Krankenkassen nicht ausgefüllt werden. Die Hauptverwaltung der Bundespostbetriebskrankenkasse hat mir mitgeteilt, daß auf meine Anfrage hin die Bezirksverwaltungen angewiesen wurden, diesen oder ähnliche Fragebogen wegen datenschutzrechtlicher Bedenken nicht mehr zu verwenden; er sei ohnehin nur in wenigen Fällen benutzt worden, die notwendigen Fragen könnten — wie bisher schon — formlos über den Vertrauensärztlichen Dienst der Krankenkassen gestellt werden.

Ich teile die Bedenken gegen die Verwendung dieses Erhebungsbogens. Die damit zu erhebenden Angaben unterliegen dem Sozialgeheimnis (§ 35 SGB I) und überwiegend den durch § 203 StGB besonders geschützten Berufsgeheimnissen. Ihre Offenbarung unterliegt — auch für die Erfüllung der gesetzlichen Aufgaben der Krankenhilfe (§ 69 Abs. 1 Nr. 1 SGB X) — dem Grundsatz der Erforderlichkeit. Die dazu von den verschiedenen Bundesverbänden der Krankenkassen gemeinsam gegebene Begründung: „Die Feststellung von Leistungsansprüchen (in diesem Bereich) setzt ... differenzierte Feststellungen zum Behandlungsbedarf voraus, für die sich der angesprochene Erhebungsbogen als erforderlich erwiesen hat", überzeugt nicht. Dem widerspricht schon, daß manche Krankenkassen selbst die Verwendung dieses Erhebungsbogens nicht für notwendig halten, um ihre Entscheidung über die Leistungsgewährung treffen zu können, z. B. die Bundespostbetriebskrankenkasse.

Die hier aufgeworfenen Fragen betreffen alle Träger der gesetzlichen Krankenversicherung und gehen damit über meinen Zuständigkeitsbereich hinaus. Eine allgemeine und abschließende Stellungnahme ist daher nur im Zusammenwirken mit den Datenschutzbeauftragten der Länder möglich. Zu diesem Zweck haben erste Kontakte stattgefunden. Nach Abschluß der Beratungen werde ich weiter berichten.

#### 2.7.4 Nachweis der Qualifikation des Personals in Sozialeinrichtungen

Eine Eingabe betraf die Frage, ob und inwieweit die Bundesversicherungsanstalt für Angestellte für die Prüfung der Eignung einer Einrichtung zur Behandlung von Suchtkranken schriftliche Nachweise zur Qualifikation des in diesen Einrichtungen beschäftigten Personals verlangen darf. Nach Erörterung mit der BfA habe ich die Notwendigkeit einer derartigen Prüfung anerkannt.

Ihre Erforderlichkeit ergibt sich aus der Verpflichtung zur wirtschaftlichen und sparsamen Verwendung der Gelder der Versichertengemeinschaft (§ 69 SGB IV). Den größten Anteil an dem einer Einrichtung pro Tag und Patient zu zahlenden Pflegesatz nehmen die Personalkosten ein. Diese müssen für die BfA transparent sein. Sie muß überprüfen können, für welches Personal mit welcher Qualifikation welche Gehälter gezahlt werden. Dies ist nur aufgrund entsprechender Nachweise möglich. Darüber hinaus ist eine Einrichtung zur Behandlung Suchtkranker dann für diese Aufgabe geeignet, wenn sie über Personal verfügt, das nach Zahl und Qualifikation in der Lage ist, die spezifischen Probleme einer Rehabilitationsmaßnahme zu meistern.

#### 2.7.5 Arztbericht im Vertrauensärztlichen Dienst

Die Eingabe eines Bürgers befaßte sich mit der angeblich unzulässigen Speicherung und Weitergabe (Offenbarung) medizinischer personenbezogener Daten durch einen Vertrauensärztlichen Dienst (VÄD).

Der Betroffene wandte sich dagegen, daß bei der Dienststelle des VÄD Fotokopien des ihm vom Hausarzt mitgegebenen Arztberichtes zu den Akten genommen wurden, obwohl er eine körperliche Untersuchung verweigert hatte, daß ihm das Original des Arztberichtes nicht ausgehändigt, sondern dem Hausarzt zurückgeschickt wurde und daß die Akten des örtlichen VÄD schließlich an den zuständigen Landesvertrauensarzt weitergegeben wurden.

Da nach ersten Stellungnahmen des Landesvertrauensarztes nicht auszuschließen war, daß eine weitere Offenbarung medizinischer personenbezogener Daten erfolgte, und zwar an die Arbeitsgemeinschaft für Gemeinschaftsaufgaben der Krankenversicherung (AGK), an welche die Angelegenheit — wie behauptet wurde — „wegen der grundsätzlichen Fragen weitergeleitet" worden war, habe ich die Vorgänge durch meine Mitarbeiter an Ort und Stelle prüfen lassen. Die dabei festgestellten Tatsachen führten zu folgenden datenschutzrechtlichen Bewertungen:

— Nach § 368 Abs. 2 RVO umfaßt die kassenärztliche Versorgung auch die Erstellung von Berichten (durch den behandelnden Arzt), die der VÄD zur Durchführung seiner gesetzlichen Aufgaben benötigt. Nach § 21 Abs. 7 Bundesmantelvertrag — Ärzte — erteilt der Kassenarzt dem VÄD diejenigen Auskünfte, die dieser zur Durchführung seiner gesetzlichen Aufgaben benötigt. Diese beiden Vorschriften bilden die Grundlage für die Offenbarung personenbezogener medizinischer Daten durch den Hausarzt an den VÄD.

— Die Aufbewahrung des Arztberichtes im Original oder in Fotokopie in den Akten des VÄD ist datenschutzrechtlich nicht zu beanstanden. Diese Unterlagen gehören zu dem Vorgang, über den ein Vertrauensarzt nicht zuletzt aus Haftungsgründen noch nach Jahren Rechenschaft ablegen können muß.

— Der Arztbericht wird für die Durchführung der Aufgaben des VÄD erstellt. Wenn der Bericht dem Patienten für die vertrauensärztliche Untersuchung mitgegeben (statt dem VÄD übersandt) wird, erfüllt der Betroffene lediglich die Funktion eines Boten, ohne daß er eigene Rechte, etwa das Recht der freien Verfügung über den Bericht, erwirbt. Auch bei einer Verweigerung der vertrauensärztlichen Untersuchung hat der Patient keinen Anspruch auf Herausgabe des Berichts zur freien Verfügung. Der Betroffene könnte allenfalls — unter den Voraussetzungen und im Rahmen des § 25 SGB X — ein Einsichtsrecht geltend machen.

— Die Aktenvorlage durch den örtlichen VÄD an den Landesvertrauensarzt war durch eine Beschwerde des Betroffenen veranlaßt. Abgesehen von der möglicherweise bereits in der Beschwerde enthaltenen Einwilligung war die Aktenvorlage und die damit verbundene Offenbarung des Arztberichtes zulässig, denn Adressat des Arztberichts ist nicht der einzelne Vertrauensarzt, sondern der VÄD als Institution, dessen Leiter der Landesvertrauensarzt ist.

— Die Übersendung von Aktenauszügen an die AGK erfolgte in vollständig anonymisierter Form und ist daher datenschutzrechtlich nicht relevant.

Dem besorgten Petenten konnte demgemäß mitgeteilt werden, daß seine Befürchtungen, hier seien Datenschutzvorschriften verletzt worden, unbegründet waren.

#### 2.7.6 Prüfung der Bau-Berufsgenossenschaft Hamburg

Die Prüfung der meiner Aufsicht unterstehenden Träger der gesetzlichen Unfallversicherung habe ich im abgelaufenen Berichtszeitraum durch einen Besuch bei der Bau-Berufsgenossenschaft Hamburg fortgesetzt.

Die Kontrolle erstreckte sich im wesentlichen auf die Unfallabteilung, die allgemeine Abteilung, hier insbesondere auf das Rechenzentrum, und auf die Personalstelle; über die Aufgaben und Organisation des arbeitsmedizinischen Dienstes haben sich meine Mitarbeiter informiert. Bei diesem Informationsgespräch wurden auch die bereits in meinem 3. Tätigkeitsbericht unter Ziffer 3.10.4.2, S. 41 gegen Teile des Formblattes „Ärztliche Untersuchung" erhobenen Bedenken erörtert. Wie die Bau-Berufsgenossenschaft mir mitteilte, befaßt sich z. Z. der Arbeitskreis „Arbeitsmedizin" der Bau-Berufsgenossenschaften mit der Frage besserer Definitions- und Dokumentationsmöglichkeiten für den psychischen Befund. Ich werde diese Entwicklung weiterhin beobachten.

Vor Aufnahme der eigentlichen Prüfung wollten meine Mitarbeiter anhand der gemäß § 15 Abs. 1 BDSG zu führenden Übersicht Prüfungsschwerpunkte festlegen. Diese Übersicht existierte bei der Bau-Berufsgenossenschaft Hamburg noch nicht. Es gab allerdings verschiedene Unterlagen, die einen Überblick über die Art der gespeicherten Daten und über die Aufgaben, zu deren Erfüllung die Kenntnis dieser Daten erforderlich ist, sowie über deren regelmäßige Empfänger gewährten; ein systematischer

Zugang war dadurch aber nur bedingt ermöglicht. Das Fehlen einer vollständigen, zusammenhängenden Übersicht habe ich beanstandet.

Bei der Prüfung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden (§ 15 Satz 2 Nr. 2 BDSG), wurde festgestellt, daß der EDV-Abteilung zwar ein schriftlicher Arbeitsauftrag der Fachabteilung zur Erledigung der jeweiligen Arbeit vorgelegt wird, diese Arbeitsaufträge waren jedoch hinsichtlich der Aufgabenbeschreibung, des Verwendungszweckes und der Anzahl der Ausdrucke nicht hinreichend präzisiert. Die Bau-Berufsgenossenschaft hat meine Anregungen aufgegriffen und zugesagt, das Verfahren der Auftragsvergabe und die dabei verwendeten Auftragsvordrucke zu prüfen.

Zum Zeitpunkt der Prüfung hatte die Bau-Berufsgenossenschaft hinsichtlich der Offenbarung und Auskunftserteilung nach den Vorschriften des SGB X lediglich eine Arbeitsanweisung zum Umfang der Offenbarung nach § 69 Abs. 1 Nr. 1 SGB X erlassen. Inzwischen liegt mir eine Dienstverfügung zur Offenbarung nach §§ 68 ff. SGB X vor. Eine Dienstverfügung zur Regelung des Auskunftsverfahrens nach § 13 BDSG besteht z. Z. noch nicht, wird aber vorbereitet.

Mehrere Mängel stellten meine Mitarbeiter im Bereich der Datensicherung fest. Die Ursache liegt im wesentlichen in der mangelnden räumlichen Ausstattung und der Vorläufigkeit mancher Regelungen bis zum Bezug eines neuen Verwaltungsgebäudes, das sich z. Z. im Bau befindet. Hier bietet sich für die Bau-Berufsgenossenschaft die Chance, bewährte Verfahren unter den Gesichtspunkten von Datenschutz und Datensicherung neu zu überdenken und in ein umfassendes Datenschutzkonzept zu bringen. Dabei wird darauf zu achten sein, daß die unterschiedlichen Aufgabenbereiche weiterhin gegeneinander abgeschottet bleiben, ohne damit die einer kleinen Organisation eigene persönliche Arbeitsatmosphäre durch unnötige Formalismen zu beeinträchtigen. Die Bau-Berufsgenossenschaft hat meine Anregungen bereits teilweise in die Konzeption zur Neugestaltung des Dienstgebäudes aufgenommen. Von der Durchführung auch dieser Maßnahmen werde ich mich in einer Nachfolgeprüfung überzeugen.

#### 2.7.7 Einzelfallprüfung bei einer Berufsgenossenschaft

Die Eingabe eines Bürgers befaßte sich mit der vermutlich unbefugten Offenbarung seiner Arbeitsunfähigkeit aus einer Nebenbeschäftigung an seinen (Haupt)Arbeitgeber durch seine Berufsgenossenschaft. Ich habe diesen Fall zum Gegenstand einer datenschutzrechtlichen Kontrolle gemäß § 19 Abs. 1 BDSG gemacht und bei der Berufsgenossenschaft den Sachverhalt vor Ort erhoben. Danach ergab sich:

Der Petent hat in der von seinem Arbeitgeber genehmigten Nebentätigkeit als Sportlehrer wiederholt Unfälle erlitten. Diese haben zunächst nur zu einer Arbeitsunfähigkeit in der Nebentätigkeit, nicht aber in der Hauptbeschäftigung geführt. Aufgrund des letzten (schweren) Unfalles hat die Berufsgenossenschaft einen eventuellen Rentenanspruch zu prüfen. Bei der dazu erforderlichen Feststellung des Jahresarbeitsverdienstes gemäß § 571 Abs. 1 Satz 1 RVO hat sie die Einkünfte aus der Hauptbeschäftigung zu berücksichtigen. In der Anfrage an den Arbeitgeber des Petenten beschränkte sich die Berufsgenossenschaft nicht auf die Erfragung des Jahresarbeitsverdienstes, sondern teilte mit, der Petent habe in seiner Eigenschaft als Sportlehrer diverse Unfälle erlitten, aus dem letzten Unfall ergebe sich die Prüfung eines Rentenanspruches. Die Angaben dieses Schreibens gingen also über das hinaus, was der Arbeitgeber wissen mußte, um der Berufsgenossenschaft den Gesamtarbeitsverdienst zu melden. Das Schreiben hatte zur Folge, daß der Arbeitgeber den Vorgesetzten des Petenten umgehend zu einer Stellungnahme über die Vereinbarkeit von Nebentätigkeit und Hauptbeschäftigung aufforderte.

Die von der Berufsgenossenschaft offenbarten Daten unterlagen den Vorschriften zum Schutze des Sozialgeheimnisses. Da sich der Vorgang im Jahre 1979 abspielte, war hier noch eine Beurteilung nach altem Recht vorzunehmen. Danach war eine Offenbarung dann nicht unbefugt, wenn der Betroffene zugestimmt hatte oder eine gesetzliche Mitteilungspflicht bestand (§ 35 Abs. 1 Satz 2 SGB I a.F.). Eine gesetzliche Mitteilungspflicht gegenüber dem Arbeitgeber bestand nicht, eine Einwilligung des Betroffenen zu einer Offenbarung lag auch nicht vor; somit war eine Offenbarung dieses Umfanges unbefugt.

Ich habe die Berufsgenossenschaft auf die Mitwirkungspflichten des Leistungsberechtigten gemäß § 60 SGB I hingewiesen und gefragt, warum sie in diesem Falle nicht die Verdienstbescheinigung über den Petenten angefordert habe. Die Berufsgenossenschaft führte hierzu aus, daß sie auch in Kenntnis des § 60 SGB I den Verletzten von dieser oft mühseligen Arbeit habe entlasten wollen. Sie habe das Verfahren jetzt dahin gehend umgestellt, daß der Verletzte auf seine Mitwirkungspflicht gemäß § 60 SGB I hingewiesen werde, aber die Erlaubnis erteilen könne, die erforderlichen Auskünfte von den Arbeitgebern einzuholen. Diese Auskünfte würden mittels eines Vordruckes angefordert, der so abgefaßt sei, daß es nicht mehr zu einer zu weitgehenden und damit unzulässigen Offenbarung von Daten kommen könne.

#### 2.7.8 Erhebung des Kindschaftsverhältnisses auf Formularen der Bundespost

Die Eingabe eines Bürgers befaßte sich mit der Frage, mit welcher Berechtigung auf Personalbögen der Deutschen Bundespost sowie auf Formblättern der Bundespostbetriebskrankenkasse und der Postbeamtenkrankenkasse zur Prüfung der Anspruchsvoraussetzungen für Familienhilfe nach § 205 Abs. 1 RVO Angaben über die Art des Kindschaftsverhältnisses, insbesondere die Tatsache einer Adoption, erhoben werden.

Meine Nachfrage bei dem Bundesminister für das Post- und Fernmeldewesen ergab, daß das Datum

„Adoptivkind" zur Zeit noch im Personalbogen erfaßt werde; da die rechtliche Stellung dieser Kinder aber der ehelicher Kinder gleich sei, werde in Zukunft die Beantwortung dieser Frage nicht mehr für erforderlich gehalten.

Die Gestaltung der Formblätter der Krankenkassen hat von folgender Rechtslage auszugehen: § 205 Abs. 2 RVO bestimmt, welche Kinder als Kinder im Sinne des Absatzes 1 gelten. Für alle dort genannten Kinder ist der Leistungsanspruch in gleicher Weise gegeben, so daß eine Frage nach den unterschiedlichen Kindschaftsverhältnissen grundsätzlich nicht erforderlich ist. Lediglich bei Stiefkindern und Enkeln sowie bei Pflegekindern (sonstige Angehörige, § 205 Abs. 2 RVO) sind zusätzliche Anspruchsvoraussetzungen gegeben: Die Frage nach dem überwiegenden Unterhalt bei Stiefkindern und Enkeln und die zusätzliche Frage nach der „häuslichen Gemeinschaft des Pflegekindes und des Versicherten und nach dem ganz oder überwiegenden Unterhalt" erstreckt sich nur auf diese Kindschaftsverhältnisse.

Die Postbeamtenkrankenkasse hat auf meine Vorhaltungen ihre Formblätter umgestellt und auf eine besondere Differenzierung der Angabe zum Kindschaftsverhältnis bei ehelichen, für ehelich erklärten, an Kindes statt angenommenen und nichtehelichen Kindern verzichtet.

Auch die Bundespostbetriebskrankenkasse hat nach einigem Zögern den „Fragebogen zur Prüfung des Anspruchs auf Familienhilfe" neu gestaltet und fordert nur noch bei Stief- und Enkelkindern sowie bei Pflegekindern detaillierte Angaben zum Kindschaftsverhältnis. Der mir in diesem Zusammenhang vorgelegte Entwurf des Fragebogens entsprach jedoch nicht den gesetzlichen Anforderungen, weil der gemäß § 9 Abs. 2 BDSG vorgeschriebene Hinweis nicht ausreichte. Meiner Forderung, diesen Hinweis in einer für das Mitglied verständlichen Form zu fassen, konnte die Bundespostbetriebskrankenkasse nicht mehr folgen, weil zum Zeitpunkt des Eingangs meines Schreibens der Druckauftrag bereits erteilt worden war. Da die Verpflichtung nach § 9 Abs. 2 BDSG bereits seit dem 1. Januar 1978 besteht, habe ich dieses Verhalten gemäß § 20 Abs. 1 BDSG beanstandet. Nachdem die Formulierung der Klausel nach § 9 Abs. 2 BDSG zwischen der Hauptverwaltung und meiner Dienststelle geklärt werden konnte, hat der Vorstand der Kasse veranlaßt, daß ab sofort ein neues Formblatt im Bereich der Kasse eingesetzt wird. Auf meine Anfrage hin bestätigte mir die Kasse, daß sie sämtliche Antragsformulare entsprechend den gesetzlichen Anforderungen geändert habe.

#### 2.7.9 Arbeitsverwaltung

a) Bei insgesamt sechs unangemeldeten Besuchen in verschiedenen Arbeitsämtern haben meine Mitarbeiter feststellen können, daß die Realisierung des Datenschutzes in der Arbeitsverwaltung zügig vorangegangen ist. Gravierende Verstöße sind nicht zu verzeichnen, auch wenn einige wiederkehrende Probleme noch gelöst werden müssen.

— Nach wie vor existieren Vermittlungsunterlagen mit veralteten Vermerken und unsachlichen Wertungen.

— Die räumlichen Gegebenheiten in vielen Arbeitsämtern führen gegenwärtig häufig dazu, daß Beratungsgespräche in Gegenwart Dritter geführt werden müssen. Die Arbeitsverwaltung ist bemüht, die hierin liegende Gefahr einer Offenbarung von Sozialdaten im Rahmen ihrer Möglichkeiten abzustellen.

— Nach wie vor existiert in der Arbeitsverwaltung keine interne Übersicht gemäß § 15 Nr. 1 BDSG. Ich hatte hierüber in meinem 2. und 3. Tätigkeitsbericht (vgl. 2.TB, Nr. 2.6.5, S. 30; 3.TB, Nr. 3.10.5.2, S. 43) berichtet. Angesichts der besonderen finanziellen und personellen Belastung gerade dieser Verwaltung bin ich der Auffassung, daß es wichtiger ist, ein Instrument zu schaffen, das als unerläßliches Arbeitsmittel allgemein akzeptiert wird, als auf der zeitgerechten Erfüllung einer formalen Pflicht zu beharren. Ich habe deshalb mit der Hauptstelle vereinbart, den vorgelegten Entwurf der Übersicht zunächst in ausgesuchten Arbeitsämtern zu erproben und die aufgrund der gewonnenen Erfahrungen neu erstellte Übersicht erst im April 1982 in der gesamten Arbeitsverwaltung einzuführen.

b) In einem Einzelfall, der ein süddeutsches Arbeitsamt betraf, habe ich eine Beanstandung wegen eines Verstoßes gegen die Vorschriften über den Schutz des Sozialgeheimnisses ausgesprochen.

Ein seit langem arbeitsloser Ingenieur befand sich in erfolgversprechenden Vertragsverhandlungen mit einem neuen Arbeitgeber. Unter Hinweis auf einen Termin mit diesem Arbeitgeber mußte der Betroffene einen Besprechungstermin beim Arbeitsamt absagen. Daraufhin wurde die zuständige Arbeitsberaterin angewiesen, beim Arbeitgeber anzurufen, um nachzuprüfen, ob der Betroffene zum angegebenen Zeitpunkt tatsächlich einen Termin vereinbart hatte. Der Arbeitgeber, der auf diese Weise von der Arbeitslosigkeit und damit der weitgehenden Mittellosigkeit erfahren hatte, änderte daraufhin seine Verhandlungsweise gegenüber dem Betroffenen zu dessen Nachteil so, daß diesem die Anstellungsbedingungen unannehmbar erschienen.

Aufgrund nachlässiger Führung der Vermittlungsunterlagen, nicht genau geregelter Informationsbeziehungen zwischen Vermittlungs- und Leistungsabteilung und eines unklaren Posteingangsverfahrens waren dem Arbeitsamt entscheidende Schriftstücke, welche die Besonderheit der anstehenden Vertragsverhandlungen hätten belegen können, entgangen.

c) Immer wieder erreichen mich Eingaben von Familienangehörigen, die im Rahmen von Arbeitslosenhilfeanträgen zu umfassenden Auskünften über ihre finanziellen Verhältnisse aufgefordert werden. Die Rechtspflicht zur Auskunftserteilung ergibt sich aus § 134 in Verbindung mit § 138 des Arbeitsförderungsgesetzes und der Unterhaltspflicht des § 1601 BGB.

Auch wenn ich in all diesen Fällen nicht helfen kann, so wird sich die Arbeitsverwaltung auf meine Anregung doch bemühen, das in solchen Fällen entstehende Mißtrauen durch gezielte Beratung und noch klarere Formulare abzubauen.

d) In einer Reihe von Eingaben beschweren sich Bürger über die Tatsache, daß die Leistungsbelege, über welche die Bundesanstalt ihren Zahlungsverkehr abwickelt, die Tatsache der Arbeitslosigkeit z. B. den Banken offenbaren. Die Betroffenen empfinden das in ihrer ohnehin schon schwierigen Situation als unnötige Diskriminierung. Die Bundesanstalt hat in ihrer Stellungnahme einen Verstoß gegen die Vorschrift des § 35 SGB I verneint. Die Angabe des Zahlungsgrundes auf den Überweisungsbelegen sei erforderlich, um die verschiedenen Leistungsarten zu unterscheiden. Im übrigen liege eine „konkludente Einwilligung" der Betroffenen in die Bekanntgabe dieser Daten an die Kreditinstitute vor.

Hierzu vertrete ich folgende Auffassung: Die Regelungen des Sozialgesetzbuches lassen aus gutem Grund eine „konkludente Einwilligung" nicht genügen, erforderlich ist vielmehr prinzipiell eine schriftliche Einwilligung. Ich sehe keine Notwendigkeit, hiervon Ausnahmen zu machen, zumal es möglich wäre, das Zahlungsverfahren ohne Offenbarung von Sozialdaten umzustellen. Denkbar wäre etwa eine Kennzeichnung der Leistungen durch Aktenzeichen o. ä. Im übrigen erhalten die Leistungsempfänger regelmäßig Leistungsbescheide, aus denen sie die Höhe der Leistungen entnehmen können.

Ich habe die Bundesanstalt erneut zur Stellungnahme aufgefordert.

### 2.8 Bundesgesundheitsamt

Ich hatte dem Bundesgesundheitsamt (BGA) für den Berichtszeitraum 1980 „schwerwiegende Mängel bei der Umsetzung des Datenschutzes" bescheinigen müssen (vgl. 3.TB, Nr. 3.10.6.2, S. 45). Bei einer Prüfung im Frühsommer 1981 konnte ich mich davon überzeugen, daß meine Anregungen aufgegriffen und im Rahmen der — insbesondere finanziellen — Möglichkeiten des BGA beseitigt waren.

Das Rechenzentrum des BGA ist schon aus baulichen Gründen — es ist gegenwärtig in einer Baracke untergebracht — kaum ausreichend zu sichern. Das BGA wird daher im Jahr 1982 vorübergehend bis zur Fertigstellung eines Neubaus Räume beziehen, die ausreichend gesichert werden können.

Bei der Prüfung hat sich gezeigt, daß einige Datensicherungsmängel in Eigenschaften dieser Installation begründet sind. So wird insbesondere das Paßwort solange auf dem Bildschirm angezeigt, bis es bewußt gelöscht wird. Dieser Paßwortschutz entspricht nicht mehr dem Stand der Technik. Es erscheint dringlich, daß diese Probleme, die bei allen Anwendern entsprechender Rechner auftreten dürften, unverzüglich gelöst werden.

### 2.9 Deutsche Bundesbank

Eine mehrtägige Prüfung der Deutschen Bundesbank — Direktorium — in Frankfurt am Main ergab, daß die dort verarbeiteten personenbezogenen Daten hervorragend gesichert sind. Die Organisation des Datenschutzes bei der Bundesbank ist vorbildlich. Kritische Feststellungen, die zu Änderungen oder weiteren Untersuchungen Anlaß gaben, betrafen die folgenden Einzelpunkte:

a) Die Vorkehrungen zum Schutz der in der Datenbank „Bankenaufsicht" gespeicherten Daten gegen unbefugte Verarbeitung wurden verbessert; die Möglichkeit weiterer Sicherungen wird untersucht.

b) Die Bundesbank führt auf der Grundlage von § 26 Außenwirtschaftsgesetz (i. V. m. §§ 55 ff. Außenwirtschaftsverordnung) eine Reihe von Statistiken durch. In den Erhebungsformularen, die die Bürger bei bestimmten außenwirtschaftlichen Vorgängen ausfüllen müssen, wird teilweise lediglich durch die Überschrift „Meldung nach § ... Außenwirtschaftsverordnung" über die Rechtsgrundlage der Auskunftspflicht aufgeklärt. Ich habe moniert, daß in diesen Fällen die nach § 9 Abs. 2 BDSG vorgeschriebene Aufklärung über das Bestehen und den Umfang der Auskunftspflicht nicht mit der wünschenswerten Klarheit erfolgt, und angeregt, in allen Fällen ausdrücklich darauf hinzuweisen, daß die Daten ausschließlich zur statistischen Auswertung verwendet werden und durch das Statistikgeheimnis geschützt sind.

c) Die Meldungen nach § 59 Außenwirtschaftsverordnung erfolgen auf einem Verbundformular, dessen oberer Teil den Zahlungsauftrag an das Kreditinstitut (für Zahlungen ins Ausland) und im unteren Teil die in diesem Fall vorgeschriebene Meldung an die Bundesbank enthält. Durch die Verknüpfung erhält das Kreditinstitut Kenntnis vom Inhalt der Meldung, z. B. von dem sehr detailliert anzugebenden Zahlungszweck. Entsprechend erhält die Bundesbank Angaben aus dem Überweisungsauftrag, die ihr nicht zustehen.

Das Verbundformular, sein Inhalt und der Meldeweg über das beauftragte Kreditinstitut sind durch die Außenwirtschaftsverordnung vorgeschrieben. Ich habe deshalb den Wirtschafts- und den Finanzminister darauf hingewiesen, daß aus datenschutzrechtlichen Gründen eine Änderung geboten ist, die den Betroffenen nur im sachlich unerläßlichen Umfang verpflichtet, seine Verhältnisse den beteiligten Institutionen gegenüber offenzulegen, und die Kreditinstitute an das Statistikgeheimnis bindet, soweit bei ihnen statistische Angaben durchlaufen.

d) In dem vom Bundesaufsichtsamt für das Kreditwesen vorgeschriebenen Formular „Anzeige nach § 14 KWG", mit dem Kreditinstitute der Bundesbank und über diese dem Bundesamt Kreditnehmer anzuzeigen haben, deren Verschuldung eine Million Deutsche Mark erreicht hat, sieht eine Aufgliederung nach der Kredit-

laufzeit vor. Durch § 14 KWG ist dies jedoch nicht gedeckt. Die Erhebung ist auch nicht auf einer anderen Rechtsgrundlage wirksam angeordnet. Die Inanspruchnahme der Kreditinstitute und der betroffenen Kunden sowie die nachfolgende Datenverarbeitung sind daher rechtswidrig; zugleich liegt ein Verstoß gegen die Aufklärungspflicht nach § 9 Abs. 2 BDSG vor. Ich habe deshalb gegenüber dem Bundesminister der Finanzen und gegenüber der Bundesbank eine Beanstandung ausgesprochen. Sofern die Angaben über die Fristigkeit für bankenaufsichtliche Zwecke benötigt werden — woran ich nicht zweifle —, ist eine rechtswirksame Begründung der Auskunftspflicht erforderlich, um Verstöße gegen den Datenschutz wie auch gegen das Bankgeheimnis auszuschließen.

e) Die Bundesbank — Direktorium — führt für ihre Bediensteten Gehaltskonten. Überziehungen sind bei diesen Konten nicht gestattet. Ich habe festgestellt, daß die kontoführende Stelle Anweisung hatte, alle gleichwohl vorkommenden Überziehungen (etwa durch Scheckvorlage oder Ausübung von Einzugsermächtigungen) der Personalabteilung mitzuteilen, wenn sie den Betrag von 100 DM übersteigen. Dies geschah jährlich in rund 400 Fällen. Die Mitteilungen sollen die Personalabteilung in den Stand versetzen, Verstöße disziplinarisch zu würdigen und gegebenenfalls Maßnahmen im Interesse der Sicherheit der Bank wie auch im Interesse der Fürsorge für den Bankangehörigen zu ergreifen. Tatsächlich kam es jedoch nur in Einzelfällen zu Ermahnungen, zum Entzug der Eurocheck-Karte oder zur Kontoschließung.

Auf meinen Hinweis, daß das Kontoführungsverhältnis und das Beschäftigungsverhältnis grundsätzlich zu trennen sind und daher Informationen über Kontobewegungen nur unter besonderen Umständen der Personalverwaltung für ihre Zwecke mitgeteilt werden dürfen, hat die Bundesbank die Meldungen auf Fälle bewußter und schwerwiegender Verstöße gegen die geltenden Vorschriften reduziert (insbesondere bewußte Überziehungen im Betrag über 1 000 DM und Scheckreiterei). Diese Lösung erscheint mir vertretbar.

### 2.10 Kraftfahrt-Bundesamt

In meinen früheren Tätigkeitsberichten hatte ich auf verschiedene Mängel bei der Datenverarbeitung durch das Kraftfahrt-Bundesamt (KBA) hingewiesen. Probleme hatten sich sowohl bei der Datensicherung wie bei der Nutzung und Verwertung personenbezogener Daten gezeigt.

Auch in diesem Jahr wurden die zur Verbesserung des Datenschutzes und der Datensicherung ergriffenen Maßnahmen an Ort und Stelle kontrolliert. Einige Probleme konnten zwischenzeitlich zufriedenstellend gelöst werden, andere Entscheidungen, die auch mit dem Bundesminister für Verkehr (BMV) erörtert wurden, stehen noch aus.

#### 2.10.1 Zentrales Verkehrs-Informationssystem (ZEVIS)

Das zentrale Verkehrs-Informationssystem ZEVIS wurde im Berichtsjahr weiter ausgebaut. Der Datenbestand sowie die Anzahl der Anschlüsse mit Direktzugriff (Ende 1981 ca. 50) wurden erweitert. In der ZEVIS-Datenbank sind jetzt der Kfz-Bestand für die Kennzeichen FL, NF, SL, der Gesamtbestand des Landes Baden-Württemberg sowie — für das gesamte Bundesgebiet — Angaben über entzogene bzw. versagte Fahrerlaubnisse enthalten. Angaben über Fahrzeuge mit Versicherungskennzeichen sollen, soweit diese maschinenlesbar dem Amt gemeldet werden, 1982 aufgenommen werden. Darüber hinaus läßt die augenblickliche Hardware eine Erweiterung des Datenbestandes und der angeschlossenen Benutzer nicht zu. ZEVIS ist mit Ausnahme des Wochenendes (Samstag/Sonntag) im 24-Stundenbetrieb auskunftsbereit.

Während meines Kontrollbesuches beim KBA habe ich die technische Abwicklung des Datenverkehrs überprüft. Die Anfrageberechtigung wird mit Hilfe von Kennungen nachgewiesen. Schon während der derzeit laufenden Pilotanwendung werden — auf meine Anregung hin — teilweise personenbezogene Kennungen vergeben. Dienststellenbezogene Kennungen halte ich wegen der geringen Überprüfungsmöglichkeit der Systembenutzung datenschutzrechtlich für nicht angemessen.

Das KBA protokolliert den gesamten Datenverkehr — also einschließlich der Anfragen und Antworten — vollständig, so daß sich jede abgerufene ZEVIS-Auskunft nachvollziehen läßt.

Die Überprüfung berechtigter Anfragen durch das KBA kann sich jedoch nur auf die Identifizierung des Übertragungsweges sowie des verwendeten Kennwortes beziehen.

Ob einer Auskunft eine zulässige Anfrage zugrundelag, muß der Online-Benutzer nachweisen. Diese verteilte Dokumentations- und Nachweisregelung entspricht auch der bisherigen Verfahrensweise bei manueller Bearbeitung. Ich halte — mit der gleichen Begründung wie für die bisherige Praxis — die Übernahme dieser Regelung für den Online-Betrieb für zweckgerecht: Die Übermittlung der polizeilichen Anfragegründe an das KBA und ihre Speicherung dort würden die schutzwürdigen Belange der Betroffenen gefährden und damit datenschutzrechtliche Bedenken auslösen.

Das Zugriffsverfahren erleichtert die Aufgabenerfüllung des KBA und kann zu einer schnelleren und effektiveren Arbeit bei den angeschlossenen Stellen beitragen.

Die besonderen Risiken des Datenmißbrauchs, die mit Direktzugriffsverfahren verbunden sind, machen es jedoch auch bei den nicht überdurchschnittlich empfindlichen Fahrzeug- und Halterdaten erforderlich, Direktanschlüsse nur solchen Stellen einzuräumen, bei denen die erreichbaren Vorteile für die Aufgabenerfüllung dies rechtfertigen. Ich begrüße deshalb die Absicht des Bundesministers für Verkehr, im geplanten Fahrzeugregistergesetz neben der materiellen Zulässigkeit der Datenübermitt-

lung auch die Voraussetzungen für Direktzugriffsverfahren im einzelnen zu regeln. Eine Klarstellung durch den Gesetzgeber ist dringend geboten, um die auf diesem Gebiet verbreitete Rechtsunsicherheit zu beheben. Ich habe meine Beratung dazu angeboten. Meine Vorstellungen, unter welchen Bedingungen Direktzugriffsverfahren akzeptabel sind, habe ich im Zusammenhang mit der Novellierung des BDSG dargelegt (Abschnitt 4.7).

#### 2.10.2 Datensicherung beim Kraftfahrt-Bundesamt

Der Umbau des Rechenzentrums hat gegenüber den früheren Verhältnissen zu erheblichen Verbesserungen geführt. Zugangs- und Abgangskontrollen sind den Datenbeständen entsprechend angemessen realisiert. Auch der Arbeitsablauf im Rechenzentrum wurde organisatorisch verbessert und den Anforderungen der Anlage zu § 6 BDSG angepaßt. Meine Empfehlungen aus früheren Kontrollbesuchen haben Eingang in die Sicherungskonzeption gefunden.

Zum Nachweis der ordnungsmäßigen Verfahrensentwicklung und des rechtmäßigen Programmeinsatzes liegen jetzt Dokumentationsrichtlinien vor, die eine ausreichende Nachprüfung ermöglichen.

An Verbesserungen des Verfahrens zur Sicherung der fristgerechten Tilgung von Eintragungen im Verkehrszentralregister (VZR) wird gearbeitet.

Die Datensperre für Fälle, in denen keine Einwilligung für die Auswertung der Halterdaten für Werbemaßnahmen vorliegt, wird vom Amt sorgfältig durchgeführt.

Durch die noch unbefriedigende Gestaltung der Formulare für die Übermittlung durch die Zulassungsstellen an das KBA treten — wenn auch nur vereinzelt — Übertragungsfehler auf; der logische und formale Aufbau im Zulassungsantrag und in den Meldevordrucken stimmen nicht überein. Ich setze mich im Zusammenwirken mit den Landesbeauftragten für eine Vereinheitlichung der Formulare ein; es bedarf dazu einer Absprache mit den Ländern.

#### 2.10.3 Verarbeitung der Berufs- und Gewerbeangabe

Die Erhebung der Berufs- bzw. Gewerbeangabe im Antrag für die Kraftfahrzeugzulassung ist durch § 23 Abs. 1 Nr. 1 Straßenverkehrszulassungsordnung (StVZO) zugelassen. Die Angaben dienen zwar nicht unmittelbar der Kfz-Zulassung, sondern der Ausführung des Bundesleistungsgesetzes (BLG) sowie des Verkehrssicherstellungsgesetzes (VSG). Die Verordnungsermächtigung (§ 6 Abs. 1 Nr. 3 StVG) erstreckt sich aber ausdrücklich auch auf Regelungen für Zwecke der Verteidigung. Kritisch ist hingegen die weitere Bearbeitung dieser Angaben beim Kraftfahrt-Bundesamt zu beurteilen (vgl. 3. Tätigkeitsbericht Nr. 3.9.1.1, S. 35). Nach dem Bundesleistungsgesetz und dem Verkehrssicherstellungsgesetz können in bestimmten Gefahrensituationen Bürger und Unternehmen zu Sach- und Dienstleistungen herangezogen werden (§§ 2 BLG, 13ff. VSG). Von dieser Leistungspflicht gibt es bestimmte Ausnahmen (§§ 17, 36 VSG; §§ 4, 95 BLG). Nach der Erklärung des Bundesministers für Verkehr sollen die Berufs- bzw. Gewerbeangaben dazu dienen, eine nach dem Gleichbehandlungs- und Verhältnismäßigkeitsgrundsatz (§§ 3 BLG, 2 VSG) ausgewogene Inanspruchnahme zu gewährleisten und Rückschlüsse auf die für Dienstleistungen erforderliche Sachkunde des Halters oder seiner Mitarbeiter zu ermöglichen.

Nach meinen Feststellungen ist eine solche Nutzung jedoch nach der Verschlüsselung, wie sie vom KBA vorgenommen wird, gar nicht mehr möglich. Die Berufsangaben von Nichtselbständigen werden den Gruppen Beamte, Angestellte, Arbeiter, Nichterwerbspersonen/Unbekannt zugeordnet und verlieren damit den für die gesetzlichen Befreiungstatbestände erforderlichen Informationswert.

Das gleiche gilt im Grundsatz für die Aufteilung der Gewerbeangaben von Selbständigen. Das KBA verwendet als Schlüssel eine Systematik, die vom Statistischen Bundesamt übernommen wurde und die sich an volkswirtschaftlichen Gesichtspunkten orientiert. Allenfalls einzelne der insgesamt 55 Gruppen eignen sich für Zwecke des BLG und des VSG. Auf meine Beanstandung hat mir der Bundesminister für Verkehr zugesagt, daß die Verarbeitung der Angaben beim KBA überprüft wird. Ergebnisse liegen noch nicht vor.

### 2.11 Allgemeine Erkenntnisse bei den Sicherheitsbehörden

#### 2.11.1 Prüfungsumfang

Im Bereich der Sicherheitsbehörden sind im letzten Jahr verstärkt Prüfungen vor Ort durchgeführt worden. Im einzelnen handelte es sich um vier Prüfungen beim Bundesnachrichtendienst, je eine Prüfung bei einigen Gruppen des Militärischen Abschirmdienstes sowie zwei weitere Prüfbesuche beim Amt für Sicherheit der Bundeswehr. Mehrere Prüfungen wurden beim Zollkriminalinstitut, beim Bundesamt für Verfassungsschutz und bei der Abteilung Staatsschutz des Bundeskriminalamts durchgeführt. Prüfgespräche fanden auch mit der Grenzschutzdirektion statt. Zeitlich am aufwendigsten waren die Prüfungen „Verfahren Dateianfrage", die Prüfung einer Sonderdatei beim Bundesamt für Verfassungsschutz (vgl. unten S. 28) und der Datei „PIOS-Terrorismus" (vgl. unten S. 22 f.). Im Rahmen der Prüfung „Dateianfrage" wurde bei mehreren obersten Bundesbehörden sowie bei Behörden des nachgeordneten Bereiches innerhalb und außerhalb von Bonn, z. B. in Hamburg, Kiel und Berlin, geprüft. Die Prüfungen erstreckten sich über mehrere Wochen.

#### 2.11.2 Gesamtergebnis

Die bei diesen Prüfungen gemachten Feststellungen ergeben in ihrer Gesamtheit leider kein erfreuliches Bild. Zum Teil wurden schwerwiegende Verstöße gegen Datenschutzrecht festgestellt. Hierbei handelte es sich vor allem um folgende Problembereiche:

— Speicherung von personenbezogenen Daten außerhalb des eigenen Zuständigkeits- und Aufgabenbereiches, zum Teil als Folge fehlender oder unklarer gesetzlicher und/oder innerdienstlicher Aufgabenzuweisungen.

— Speicherung von Informationen, die nicht mehr gespeichert sein dürften, weil sie nicht mehr erforderlich sind. Nach meinem Eindruck „schleppen" eine Reihe von Sicherheitsbehörden eine Vielzahl von Daten und Informationen mit sich fort, die zum Teil schon seit längerem zur Löschung anstehen.

— Zu großzügige Übermittlung aus Unterlagen, die unvollständig oder nicht mehr aktuell oder aus anderen Gründen zu löschen sind; Übermittlungen auch außerhalb der einschlägigen Richtlinien und für andere Zwecke als die, zu denen die Daten gesammelt worden sind, ohne daß entsprechende gesetzliche Grundlagen hierfür bestehen.

— Verstöße gegen die Dateien-Richtlinien. Dies ist besonders bedauerlich, weil die Dateien-Richtlinien ohnehin nicht voll befriedigend sind, sondern einen Kompromiß zwischen den datenschutzrechtlichen Wünschen und den Anforderungen der Sicherheitsbehörden darstellen (s. u. 4.5.1, S. 51 ff.). Auch in anderen Fällen waren Verstöße gegen eigene Richtlinien feststellbar.

— Einrichtung von Online-Verbindungen, ohne daß die gesetzlichen Voraussetzungen hierfür vorliegen.

— Verwendung von Erkenntnissen und Informationen der Sicherheitsbehörden durch andere Verwaltungsbehörden ohne Wissen der Betroffenen. Hierdurch wurde diesen die Chance der Rechtfertigung und damit praktisch der Rechtsweg genommen. Da die Sicherheitsbehörden nicht selten auf sog. „unbewertete" oder nicht beweisbare Informationen angewiesen sind, kann dies für die Betroffenen von ganz besonderem Nachteil sein.

#### 2.11.3 Zu den Ursachen festgestellter Mängel

Die Gründe für die festgestellten Mängel sind verschiedener Natur. Abgestellt werden können sie nur, wenn den datenschutzrechtlichen Belangen der Betroffenen stärker Rechnung getragen wird. Dies kann und muß im Einzelfall auch bedeuten, daß die Belange des Einzelnen überwiegen und gegebenenfalls auf bestimmte Informationen und Informationsübermittlungen verzichtet wird. Notwendig erscheint es mir auch, daß bei den Sicherheitsbehörden ein annäherndes Gleichgewicht zwischen der Neueinspeicherung von Daten und der Löschung nicht mehr erforderlicher Daten hergestellt wird. Andernfalls wird die Zahl der „löschungsreifen" Daten weiterhin steigen. Das von den Sicherheitsbehörden immer wieder vorgebrachte Argument, man habe zu wenig Personal für Löschungen, trägt nur teilweise — auch die Arbeit mit großen, teilweise inaktuellen Datenbeständen ist zeitaufwendig.

#### 2.11.4 Das Amtshilfeproblem

Ungelöst sind nach wie vor viele Fragen im Zusammenhang mit der Amtshilfe (vgl. hierzu 1. TB, Nr. 3.4.3.3, S. 25, 2. TB, Nr. 2.8.1, S. 44, 3 TB, Nr. 3.11.1, S. 45). Gerade hier käme es aber auf klare und gegenüber der augenblicklichen Praxis restriktive Regelungen an. Es muß nochmals betont werden, daß die Amtshilfe fehlende Befugnisse nicht ersetzen kann, soweit keine speziellen Regelungen vorliegen. Wenn beispielsweise in der StPO und in den Polizeigesetzen genau festgelegt ist, unter welchen Voraussetzungen erkennungsdienstliches Material hergestellt oder Beweismaterial erlangt werden kann, so ist es nach meiner Auffassung nicht zulässig, daß die Polizei sich im Wege der Amtshilfe von anderen Behörden, etwa Paßbehörden, dort befindliche Fotos von Bürgern geben läßt, ohne daß die Voraussetzungen nach dem für die Polizei geltenden Recht vorliegen. Gleiches gilt für die Weitergabe von erkennungsdienstlichen Unterlagen durch die Polizei. Ist der Empfänger, etwa ein Nachrichtendienst, gar nicht befugt, selbst ed-Material herzustellen, so darf er es — unabhängig vom Trennungsgebot — auch nicht im Wege der Amtshilfe erhalten. Meine Prüfungen haben aber ergeben, daß dies nicht immer beachtet wird.

### 2.12 Bundeskriminalamt

#### 2.12.1 Datei PIOS-Terrorismus

In der Zeit vom 24. August bis 15. Oktober habe ich das System PIOS-Terrorismus beim BKA überprüfen lassen. Als Ergebnis dieser Prüfung habe ich gegenüber dem Bundesminister des Innern eine Reihe von Beanstandungen ausgesprochen. In seiner gegenwärtigen Form bietet PIOS-Terrorismus Anlaß zu vielfältiger datenschutzrechtlicher Kritik.

Dies gilt vor allem für den Umfang der dort gespeicherten Personendaten. PIOS enthält zum Teil sogenannte „unbewertete" Daten, d. h. Angaben über Personen, bei denen eine Verbindung zum Terrorismus zwar vermutet wird, aber (noch) kein konkreter Verdacht im Sinne der Strafprozeßordnung oder des Polizeirechts besteht. So kann sogar der Fall eintreten, daß jemand, der nur einen zufälligen, ihm selbst möglicherweise gar nicht bewußten Kontakt mit Angehörigen des terroristischen Umfeldes hat, oder jemand, der sich kritisch mit den Formen der staatlichen Terrorismusbekämpfung auseinandersetzt, registriert wird. Daß dies überaus bedenklich ist, wird wohl niemand bestreiten. Deshalb kommt der ständigen Überprüfung, ob die Daten überhaupt oder noch erforderlich sind, besondere Bedeutung zu.

Zwar ist nicht zu verkennen, daß das BKA selbst in den vergangenen Jahren wiederholt Löschungen größeren Umfangs durchgeführt hat und sich weiterhin bemüht, die Bestände zu bereinigen. Nach wie vor ist in PIOS aber eine beträchtliche Zahl von Personen gespeichert, die irgendwann einmal, oft vor vielen Jahren, in einen (nicht selten zufälligen) Kontakt mit dem Terrorismus gekommen sind, der bei heutiger Betrachtung zumeist als irrelevant eingestuft werden kann.

Dies gilt insbesondere für die Kontaktpersonen aus den sogenannten „besonderen Meldediensten". Bereits im ersten Dateienbericht des BMI werden (auf S. 8 b) Zweifel darüber geäußert, ob es berechtigt ist, in einem derartigen Umfang Angaben über Personen zu speichern, die Kontakte zu lediglich Verdächtigen unterhalten oder unterhalten haben, ohne daß

zusätzliche belastende Anhaltspunkte vorliegen. In den eineinhalb Jahren seit dem ersten Dateienbericht hat sich aber beispielsweise die Zahl der im Rahmen der polizeilichen Beobachtung gespeicherten Kontaktpersonen um mehr als 50% erhöht, obwohl mittlerweile seit Einführung der Polizeidienstvorschrift 384.2 der Umfang der polizeilichen Beobachtung begrenzt wurde.

Auch die Zahl der im Rahmen der Häftlingsüberwachung gespeicherten Kontaktpersonen hat sich seit dem ersten Dateienbericht des BMI in ähnlichem Maßstab erhöht. Ich bezweifle, ob mit einer derartigen quantitativen Ausweitung der Häftlingsüberwachung auch eine qualitative Verbesserung überhaupt möglich ist. (Einzelheiten zur Häftlingsüberwachung vgl. unten 2.12.4)

Die Prüfung von PIOS hat auch mehrere Verstöße gegen die Dateien-Richtlinien ergeben. So sind beispielsweise entgegen Ziffer 4.2.10 der Dateien-Richtlinien noch Anzeigenerstatter, Hinweisgeber und Zeugen in PIOS gespeichert. Bislang wurden in PIOS noch nicht allgemein Wiedervorlagefristen eingespeichert. Diese Unterlassung macht die Einhaltung bestimmter, in den Dateien-Richtlinien vorgesehener Fristen nahezu unmöglich. Beispielsweise müssen im Regelfall nach Ziffer 4.5 der Dateien-Richtlinien Personen, die aufgrund der Ziffer 4.2.11 in PIOS gespeichert sind, ein Jahr nach Aufnahme der Speicherung von dieser Tatsache informiert werden. Eine Ausnahme besteht nur, wenn im Einzelfall der Zweck der Speicherung durch die Unterrichtung gefährdet werden würde. Nach meiner Kenntnis hat das BKA bislang jedoch noch in keinem Fall eine derartige Unterrichtung durchgeführt, obwohl aufgrund der Ziffer 4.2.11 nicht wenige Personen in PIOS gespeichert sind und nach meiner Überzeugung die Voraussetzung für die Ausnahme von der Unterrichtung nicht bei allen Personen vorliegt. Soll die Frist in Zukunft eingehalten werden, so müßte bei der Einspeicherung bereits ein entsprechendes Wiedervorlagedatum eingegeben werden. Im übrigen bestehen gegen die Ziffer 4.2.11 ohnehin erhebliche rechtliche Bedenken, auf die ich den BMI im Verlauf der Erarbeitung der Dateien-Richtlinien und insbesondere auch in meiner abschließenden Stellungnahme hingewiesen habe. (Zu den Dateien-Richtlinien näher s. u. 4.5.1).

Es ist schon aus Gründen der Geheimhaltung nicht möglich, hier die von mir festgestellten datenschutzrechtlichen Mängel von PIOS erschöpfend darzustellen. In den Einzelheiten ist dies gegenüber dem BMI in einem umfangreichen Prüfvermerk geschehen.

Leider wird aber trotz der Mängel von PIOS solchen Behörden, die keinen unmittelbaren Zugriff auf PIOS haben, Auskunft aus diesem System erteilt. Hiergegen habe ich gegenüber dem BMI Bedenken geäußert. Nach meiner Auffassung steht das Zweckbindungsprinzip der Verwendung von Daten, die speziell zur Terrorismusbekämpfung gesammelt worden sind und deren Erhebung unter diesem speziellen rechtlichen Gesichtspunkt beurteilt worden ist, für andere Verwaltungszwecke entgegen. Es ist schon äußerst problematisch, wenn Menschen im Wege der Speicherung in PIOS in einen nicht bewiesenen Zusammenhang mit dem Terrorismus gebracht werden. Was aber unter Berücksichtigung der Methoden und der besonderen Gefährlichkeit des Terrorismus insoweit noch hingenommen werden könnte, bekommt eine andere Qualität, wenn diese Daten für andere Verwaltungszwecke verwandt werden. Von diesem Grundbedenken einmal abgesehen, hatte ich auch Veranlassung, einzelne Auskunftsfälle zu beanstanden, in denen schon aus der Anfrage ersichtlich war, daß kein berechtigter Grund zur Auskunft vorlag. In anderen Fällen wurde Auskunft aus Vorgängen und aufgrund von Speicherungen erteilt, die bereits hätten vernichtet bzw. gelöscht sein müssen. Durch diese Auskunftspraxis erhalten auch die Bedenken gegen die Speicherpraxis in PIOS zusätzliches Gewicht.

In meinem Prüfbericht an den BMI habe ich zum Ausdruck gebracht, daß mir der Aufwand bewußt ist, der zur Bereinigung von PIOS erforderlich ist. Ich weiß auch, daß die dafür verfügbaren Ressourcen (wie jüngst auch der Bundesrechnungshof festgestellt hat) begrenzt sind. Mir ist auch klar, daß die Verantwortung für PIOS nicht allein beim Bund, sondern auch bei den Ländern liegt. Ich gehe aber davon aus, daß, so wie Bund und Länder sich hinsichtlich des Aufbaus von PIOS geeinigt haben, auch ein gemeinsames Vorgehen bei der Bereinigung möglich ist.

Am 22. Dezember 1981 erreichte mich eine erste Stellungnahme des Bundesministers des Innern. Der Bundesminister teilt hierin mit, daß er aufgrund meiner Anregungen eine Reihe von Maßnahmen eingeleitet habe, die erste Verbesserungen bringen. Freilich beziehen sich diese im wesentlichen auf die ohnehin seit langem fällige Bereinigung bereits seit längerer Zeit vorhandener Bestände, die zudem ohne großen Arbeitsaufwand möglich ist. In mehreren grundsätzlichen Fragen wie z. B. der Speicherung sogenannter „anderer Personen" halte ich dagegen weitere Erörterungen für erforderlich.

#### 2.12.2 Abteilung Staatsschutz

Die von mir in früheren Jahren an der sogenannten „Organisationskartei" geübte Kritik hat dazu geführt, daß das BKA eine neue Dienstanweisung für diese Organisationskartei erarbeitet hat, in der auch den datenschutzrechtlichen Belangen Rechnung getragen wurde. Die Zahl der in der eigentlichen Organisationskartei gespeicherten Organisationen ist auch deutlich zurückgegangen. Bei einer Nachprüfung im Juni dieses Jahres mußte ich aber feststellen, daß ein Teil der Organisationen zwar aus der „Organisationskartei" entfernt wurde, statt dessen nun aber in einer anderen Kartei, die eine andere Bezeichnung trägt, geführt wird. Ich habe das BKA um Bereinigung auch dieser Bestände gebeten und darauf hingewiesen, daß allein mit der Neubenennung einer Datei die datenschutzrechtlichen Probleme noch nicht gelöst sind.

Diese und weitere Prüfungen bei der Abteilung Staatsschutz haben ergeben, daß dort Unterlagen vorhanden sind, die datenschutzrechtliche Bedenken hervorrufen. Dies gilt einmal für den Inhalt von

Informationen, die an das BKA gemeldet und dort verarbeitet werden. Teilweise sind darunter Sachverhalte, die noch nicht die Schwelle der „Polizeirelevanz" überschritten haben, also schwerpunktmäßig allenfalls in die Zuständigkeit des Verfassungsschutzes fallen. (Hierzu erklärt das BKA soeben, einige Vorgänge würden „nur für eine kurze Zeit abgelegt, um ihre weitere Polizeirelevanz zu prüfen"; diese Darstellung ist neu.) Teilweise handelt es sich um Informationen, die nach meiner Auffassung nur regionale Bedeutung haben. Die Staatsschutzrichtlinien zwingen im übrigen auch nicht dazu, Personen nur wegen „wilden Plakatierens" nach § 303 StGB (ohne aus der Meldung erkennbaren terroristischen oder extremistischen Hintergrund) an das BKA zu melden, wie es in mehreren Einzelfällen festgestellt wurde.

Auch der Inhalt der einmal beim BKA angelegten Vorgänge gibt zu Sorgen Anlaß. Nicht selten melden Landespolizeibehörden nur die Entstehung eines Verdachts oder die Einleitung eines Verfahrens gegen eine Person, während über den weiteren Fortgang des Verfahrens nichts bekannt wird. Hierdurch werden häufig Verdachtsmomente gestreut, ohne daß Entlastendes in gleicher Weise bekanntgegeben würde. Da die Abteilung Staatsschutz des BKA ihre Vorgänge nach wie vor in NADIS speichert, führt dies relativ häufig zu Nachfragen anderer NADIS-Teilnehmer oder auch von Polizeibehörden, die das BKA, nicht selten zum Nachteil des Betroffenen, nur bruchstückhaft beantworten kann.

Da ich eine systematische Prüfung der Datenbestände bei der Abteilung Staatsschutz bislang noch nicht durchführen konnte und da auch eine vollständige interne Bereinigung der Bestände in absehbarer Zeit noch nicht realisiert sein wird, habe ich das BKA aufgefordert, in Zukunft nur noch dann Auskunft zu erteilen, wenn wirklich gesicherte und vollständige Erkenntnisse vorliegen. In anderen Fällen sollten anfragende Stellen an diejenigen Behörden verwiesen werden, die selbst die Ermittlungen führen oder geführt haben.

#### 2.12.3 Vorgangsnachweis Personalien (VNP)

Im Zusammenhang mit meiner Stellungnahme zum ersten Dateienbericht des BMI hat das Bundeskriminalamt erklärt, es werde eine klare Trennung zwischen verwaltungsmäßig und kriminalpolizeilich relevanter Registrierung von Personalien vorgenommen. Nur verwaltungsmäßig relevante Vorgänge werden nach Auskunft des BKA im sogenannten „Vorgangsnachweis Personalien" erfaßt.

Anhand von Eingaben und nach eigenen Nachforschungen habe ich aber den Eindruck gewonnen, daß der VNP nicht nur der rein verwaltungsmäßigen Registratur dient. Wäre dies so, so wäre es nicht notwendig, daß alle BKA-Mitarbeiter, die Zugriff auf den zentralen Personenindex (ZPI) haben, auch Zugriff auf den VNP haben. Das BKA selbst hat mir gegenüber eingeräumt, daß in den VNP sogenannte „Altbestände" aufgenommen worden sind, die nicht nur verwaltungsinterne Bedeutung haben.

Es handelt sich dabei um Kriminalakten, die nach den Richtlinien über die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS) an sich zur Bereinigung anstehen, die aber wegen der besonderen Schwere der zugrundeliegenden Verdachtsmomente erst nach vollständiger Einführung des zentralen Kriminalaktennachweises bereinigt werden sollen.

Stichprobenartige Kontrollen haben außerdem ergeben, daß im VNP auch Fälle registriert sind, in denen die Schwelle zur Anlegung einer Kriminalakte und zur Speicherung im ZPI nicht überschritten war, denen aber doch eine gewisse polizeiliche, nicht nur verwaltungsmäßige Relevanz beigemessen wurde. Derartige Fälle sind im VNP ebenso registriert wie Fälle rein verwaltungsmäßiger Natur.

Nach meiner Auffassung kann mit dieser Praxis die angestrebte Trennung von verwaltungsmäßiger und kriminalpolizeilich relevanter Registrierung von Personalien nicht erreicht werden. Es besteht darüber hinaus die Gefahr, daß die Voraussetzungen für die Anlegung einer Kriminalakte, so wie sie in den KpS beschrieben sind, auf dem Umweg über den VNP eine gewisse Erweiterung erfahren.

Ich habe deswegen das BKA gebeten, aus dem VNP alle Vorgänge mit — wenn auch geringer — polizeilicher Relevanz herauszunehmen und den VNP nur denjenigen BKA-Mitarbeitern zugänglich zu machen, die mit Verwaltungsaufgaben befaßt sind.

Außerdem bin ich der Auffassung, daß normale Bürgeranfragen keinesfalls im VNP jetzigen Zuschnitts gespeichert werden sollten. Hier stellt sich wegen der relativ geringen Zahl solcher Eingaben überhaupt die Frage nach der Erforderlichkeit automatisierter Registrierung. Sie ist m. E. zu verneinen. Davon abgesehen halte ich es für unerträglich, wenn Bürger, die sich mit irgendeinem, z. B. datenschutzrechtlichen Anliegen an das BKA wenden, in einer Datei zusammen mit kriminalpolizeilich relevanten Namen gespeichert werden.

Wenige Tage vor Drucklegung dieses Berichts teilte mir das Bundeskriminalamt mit, daß die Personalien derer, die sich mit der Bitte um Prüfung an mich gewendet haben, dort nicht mehr dateimäßig erfaßt werden.

#### 2.12.4 Häftlingsüberwachung

Als Beispiel für äußerst fragwürdige Speicherungen von Daten im System PIOS (die zwar weitgehend durch die Länder erfolgen, die jedoch das BKA nicht von seiner Sorgfaltspflicht als speichernde Stelle befreien können), sei die Datei Häftlingsüberwachung genannt.

Sie enthält nach dem Dateien-Bericht des BMI vom 25. April 1979 (s. 8b und S. 17), der insoweit wörtlich in der Zeitung „Die Welt" vom 25. April 1979, S. 4 abgedruckt ist, personenbezogene Daten von Personen, die inhaftierte terroristische Gewalttäter besuchen oder mit ihnen in Briefkontakt stehen. Soweit diese Personen unter polizeilicher Beobachtung stehen, werden auch die Personen gespeichert, die in Begleitung dieser Besucher angetroffen werden.

Hierzu gehören auch Eltern, Ehegatten, Verwandte, Verlobte usw. Lediglich Kinder, Geistliche, Beamte, Sozialarbeiter und Gutachter, soweit sie beruflich mit den Häftlingen zu tun hatten, waren nach dem Bericht des BMI von Anfang an ausgenommen.

Ich habe in meiner Stellungnahme vom Mai 1979 auf die großen Bedenken hingewiesen, die gegenüber einer so pauschalen Speicherung bestehen. Ich habe betont, daß hierfür auch keine Rechtsgrundlage ersichtlich ist. In einer eingehenden Besprechung sicherte mir der damalige Präsident des BKA zu, bei der Arbeitsgemeinschaft der Kriminalpolizeien des Bundes und der Länder (AG Kripo) dafür einzutreten, daß zumindest alle Personen über 50 Jahre und die Eltern der Inhaftierten von der generellen Beobachtung und Registrierung als Kontaktpersonen ausgenommen sein sollten. Ich habe daraufhin zunächst meine Bedenken zurückgestellt.

Die im Herbst dieses Jahres durchgeführte Prüfung des Systems PIOS (hierzu s. 2.12.1) hat jedoch ergeben, daß die Speicherungspraxis unverändert beibehalten wurde und keine systematischen Bereinigungen durchgeführt worden sind. Selbst die im Dateien-Bericht des BMI genannten und mir bei den erwähnten Gesprächen im BKA erneut genannten Minimalkriterien für Nichtspeicherung sind nicht voll eingehalten worden.

Ich habe diesen gravierenden Sachverhalt gegenüber dem Bundesminister des Innern als zuständiger oberster Bundesbehörde für das BKA beanstandet. Die Einzelheiten kann ich hier nicht aufführen. Die Daten werden überwiegend von den Ländern angeliefert oder direkt in PIOS eingestellt. Ich habe aber der Tatsache Rechnung getragen, daß dem BKA bei der Häftlingsüberwachung eine gewisse Schlüsselposition zukommt. Diese dokumentiert sich auch darin, daß im BKA parallel zu PIOS eine manuelle Datei zur Häftlingsüberwachung geführt wird.

Der BMI hat mir im Jahre 1980 einen Entwurf für eine Neuregelung zugesandt, zu dem ich in vielen Punkten noch erhebliche Bedenken geltend gemacht habe. Bis zur Drucklegung dieses Berichts liegt mir aber weder eine endgültige Neufassung noch eine wenigstens einigermaßen vertretbare Übergangsregelung vor. Allerdings hat mir der Bundesminister des Innern soeben Schritte angekündigt, die — sofern sie bald realisiert werden — meinen Bedenken weitgehend Rechnung tragen.

#### 2.12.5 Fahndungsmäßige Überprüfung von Personen

Als ein weiteres Beispiel rechtlich bedenklicher und einer Verbesserung des Verhältnisses von Bürgern und Polizei nicht gerade förderlicher Maßnahmen sei ein Beschluß der Innenministerkonferenz der Länder vom September 1977 erwähnt. Nach diesem Beschluß, der inzwischen durch Presseveröffentlichungen bekannt geworden ist, sollen *alle* Personen, die der Polizei bei der Erfüllung ihrer Aufgaben bekannt werden, durch Abfrage in der INPOL-Datei Personenfahndung überprüft werden. Hierzu gehören insbesondere auch Zeugen und Geschädigte. Da den Polizeien des Bundes und der Länder nach längeren Erörterungen in diesem Jahr empfohlen wurde, den Beschluß in den wesentlichen Punkten unverändert auszuführen — die vorerwähnte Abfrage bleibt Grundsatz, nicht etwa Ausnahme! — sehe ich mich veranlaßt, nochmals meine rechtlichen Bedenken darzulegen:

Die fahndungsmäßigen Überprüfungen von Personen sind Maßnahmen mit Eingriffscharakter. Deshalb bedarf es hierzu einer Rechtsgrundlage. Eine generelle fahndungsmäßige oder sonstige Überprüfung ohne weitere Voraussetzungen ist z. B. rechtlich zulässig im Rahmen der Grenzübertrittskontrolle (§§ 10ff. BGSG) sowie an einer Kontrollstelle, die für Maßnahmen der Gefahrenabwehr oder der Strafverfolgung im Rahmen des geltenden Rechts eingerichtet ist (vgl. § 11 Abs. 1 Nr. 4 NW PolG, § 111 StPO). Die gesetzliche Regelung der vorgenannten Kontrollstellen zur Gefahrenabwehr oder Strafverfolgung, die erst in der Zeit nach dem IMK-Beschluß erfolgte, sollte gerade die Lücken schließen, die bisher für allgemeine Fahndungsmaßnahmen bestanden. Darüber hinaus kann eine fahndungsmäßige Überprüfung dann zulässig sein, wenn zumindest eine Anscheinsgefahr besteht und damit die Voraussetzung für erste Maßnahmen aufgrund der allgemeinen polizeilichen Generalklausel gegeben ist. Dies kann jedoch nicht generell und ohne jegliche sonstige Begrenzung für alle im Fahndungsbestand von INPOL ausgeschriebenen Personen gelten. Daher ist es auch nicht gerechtfertigt, grundsätzlich alle Personalien, die der Polizei bekannt werden, fahndungsmäßig zu überprüfen.

Ich habe diese Bedenken dem Bundesminister des Innern seit Herbst 1980 mehrfach erläutert, leider ohne Erfolg. Freilich ist einzuräumen, daß die Durchführung des Beschlusses schwerpunktmäßig bei den Ländern liegt. Die Landesdatenschutzbeauftragte von Baden-Württemberg hat sich in ihrem ersten Tätigkeitsbericht 1980 (S. 25f.) zu dieser Praxis in ihrem Kontrollbereich ebenfalls kritisch geäußert.

#### 2.12.6 Zusammenarbeit der Polizeien (Meldedienste, Kriminalaktennachweis)

Die Innenministerkonferenz hat am 12. Juni 1981 die Richtlinien über den Kriminalaktennachweis (KAN) beschlossen. Danach sollen die Hinweise auf Akten von kriminalpolizeilicher Relevanz über vermutete bevorstehende, zu verhütende, begangene und aufzuklärende Straftaten in einer zentralen Datei für alle Kriminalpolizeidienststellen automatisch verfügbar gemacht werden. Der KAN ist das Kernstück der INPOL-Neukonzeption; gleichzeitig wurden frühere, umfassendere Ausbaupläne modifiziert.

Die entscheidende und bis zur Verabschiedung im Juni 1981 heftig umstrittene Änderung gegenüber allen vorherigen Vorhaben ist der Verzicht auf die totale Zentralisierung eines automatisierten Fundstellensystems beim BKA: Hinweise auf Akten von lediglich regionaler oder generell untergeordneter Bedeutung sind ausgenommen. Damit ist eine datenschutzrechtliche Kernforderung erfüllt, die ich

gemeinsam mit den Datenschutzbeauftragten der Länder von Anfang an vertreten habe und die sowohl nach dem Wortlaut des BKAG als auch nach dem Verfassungsgrundsatz der Verhältnismäßigkeit geboten ist. Im einzelnen kann ich hierzu auf meine früheren Stellungnahmen verweisen (2. TB, Nr. 2.8.1, S. 47; 3. TB, Nr. 3.11.2.1, S. 48 f.).

Die Entscheidungskriterien für die in den überregionalen KAN aufzunehmenden und damit im BKA zu speichernden Daten sind überwiegend vertretbar. Freilich sind einige der vorgesehenen Fallgruppen zu umfassend und sollten präzisiert werden, worauf ich den Bundesminister des Innern aufmerksam gemacht habe. Praktikabilität und konkrete Auswirkungen der Abgrenzungskriterien müssen neu erprobt werden; eventuell sind weitere Änderungsvorschläge zu erarbeiten.

Die noch bestehenden Bedenken können aber nur zurückgestellt werden, wenn das Grundanliegen des KAN-Konzepts verwirklicht wird. Zum einen müssen die Abgrenzungskriterien beim KAN selbst strikt eingehalten werden, zum anderen aber auch bei den zum „INPOL-Ausbaukonzept" gehörenden ergänzenden Dateien.

Ausnahmefälle stellen die Fahndungs- und die Haftdatei dar, erstere, weil bei ihr stets überregionale Bedeutung angenommen werden kann, letztere wegen des klaren Wortlauts von § 4 BKAG.

Im übrigen aber, also gegenwärtig bei der Straftaten/Straftäter-Datei und der Datei über erkennungsdienstliche (ed) Unterlagen, ist rechtlich und faktisch die Begrenzung der Sammlung im BKA auf Fälle überregional bedeutsamer Art geboten. Sonst würden die Beschlüsse zum KAN praktisch unterlaufen.

Nach der bisherigen Fassung der *bundeseinheitlichen Richtlinien über ed-Behandlung* sind die ed-Unterlagen grundsätzlich und ohne Ausnahme in einer Ausfertigung an das BKA zu senden und werden dort registriert. Es ist für den Betroffenen dann völlig unerheblich, wenn das Aktenzeichen der Kriminalakte mangels überregionaler Relevanz nicht ebenfalls im KAN des BKA bundesweit abrufbar gespeichert ist. Tatsächlich hat es im vergangenen Jahr einige Fälle mehr oder weniger pauschaler ed-Behandlung anläßlich von Hausbesetzungen oder Demonstrationen gegeben.

Die gegenwärtig auch aus anderen Gründen in Überarbeitung befindlichen bundeseinheitlichen Richtlinien über ed-Behandlung (vgl. 3. TB, Nr. 3.11.2.1, S. 49 sowie hier S. 52) bedürfen daher vor allem auch unter diesem Aspekt dringend der Revision. Hierauf habe ich den Bundesminister des Innern mehrfach mit Nachdruck hingewiesen. Der BMI hält jedoch bisher an der Auffassung fest, daß die Abschichtungskriterien nach dem KAN-Konzept nicht für andere Dateien gelten sollen.

#### 2.12.7 Interpol und Datenschutz

a) Seit längerem wird von offizieller Seite eine Verbesserung der internationalen Zusammenarbeit bei der Bekämpfung von Straftaten gefordert. Dies soll vor allem durch eine Aktivierung von Interpol als internationalem Informationszentrum der Polizei geschehen, mit dem das BKA als Nationales Zentralbüro dieser Organisation gemäß § 1 Abs. 2 BKAG zusammenarbeitet.

Es ist ein legitimes Anliegen, eine Verbesserung der Zusammenarbeit herbeizuführen. Es kann nicht bestritten werden, daß Rechtsbrecher in vielen Fällen Straftaten im Ausland vorbereiten oder sich der Strafverfolgung durch Flucht ins Ausland entziehen. Andererseits bedeutet Verbesserung der internationalen Zusammenarbeit in erster Linie auch Verstärkung des grenzüberschreitenden Informationsflusses und vermehrte Informationssammlung durch Interpol. Dies verstärkt die datenschutzrechtlichen Bedenken, die bei aller Notwendigkeit einer Institution wie Interpol bestehen.

Der Rechtsstatus dieser Organisation, deren Mitglieder nicht souveräne Staaten, sondern nationale Polizeiorganisationen sind, ist höchst unklar. Interpol selbst ist bisher der Auffassung, daß allein die Organisationsstatuten (in Verbindung mit hierzu ergangenen Regelungen der Organe von Interpol) für die Tätigkeit von Interpol ausschlaggebend seien. Nationale datenschutzrechtliche Vorschriften zum Schutz personenbezogener Daten (wie z. B. die KpS- und Dateien-Richtlinien) sind also für die Interpol-Zentrale irrelevant.

Die Interpol-Statuten sind aber weder völkerrechtlich noch innerstaatlich verbindlich, da sie weder durch Transformationsgesetz in nationales Recht umgesetzt noch überhaupt durch zuständige Organe, die für die Bundesrepublik Deutschland völkerrechtlich verbindlich handeln können, erlassen wurden. Die Statuten enthalten auch keinerlei Vorschriften über die informationelle Tätigkeit von Interpol, die sich durch stetige Sammlung, Auswertung und Übermittlung vorwiegend personenbezogener Daten kennzeichnen läßt, Tätigkeiten also, die nach unserer Rechtsordnung als polizeiliche Maßnahmen mit Eingriffscharakter zu werten sind. Sie enthalten darüber hinaus keinerlei Hinweise auf eine unabhängige externe Kontrolle durch Datenschutzbeauftragte. Unklar ist auch, vor welchem Gericht z. B. die bei uns selbstverständlichen Rechte auf Auskunft, Berichtigung oder Löschung gegenüber Interpol geltend zu machen sind oder gar wie das weitere Schicksal der Daten zu beeinflussen ist, die von einem nationalen Zentralbüro — in der Bundesrepublik also vom BKA — an Interpol gegeben, dort ausgewertet und an Polizeien anderer Länder übermittelt werden. Von einer externen Kontrolle kann keine Rede sein. Dabei verfügt Interpol gegenwärtig über Karteien, die ca. 1,5 Mio. personenbezogene Datensätze enthalten, und es werden gegenwärtig pro Monat ca. 10 000 Meldungen ausgewertet. Es ist durchaus möglich, daß sich hierunter Daten befinden, die nach innerstaatlichem Recht nicht oder nicht (mehr) so verwertet werden dürfen.

Die hier bestehenden Mängel an Rechts- und Datenschutz werden auch nicht dadurch behoben,

daß das BKA bei der Übermittlung von Daten an Interpol an das innerstaatliche Recht gebunden ist.

Soweit es um aktuelle Strafverfolgung geht, liegen zwar weitgehend völkerrechtlich verbindliche Rechtshilfeabkommen zugrunde. Diese regeln jedoch nur die Pflicht oder Zulässigkeit der Übermittlung, die in der Praxis zum Teil recht großzügig gehandhabt wird, nicht aber die weitere Tätigkeit und das weitere Schicksal der Daten bei Interpol oder gar die Kontrolle von Interpol in diesem Zusammenhang.

b) All dies zeigt, daß eine gemeinsame Lösung dringend notwendig ist, um die Probleme in den Griff zu bekommen.

Die Internationale Konferenz der Datenschutzbeauftragten hat sich bereits auf ihrer 1. Zusammenkunft 1979 in meiner Dienststelle mit Lösungsmöglichkeiten für die vorgenannten Rechtsschutzprobleme befaßt, die sowohl für manuelle als auch für beabsichtigte künftige automatisierte Datenverarbeitung bestehen. Auf der 3. Konferenz der Datenschutzbeauftragten, die vom 7. bis 10. Oktober 1981 in Paris stattfand, wurde das Thema erneut erörtert. Die Konferenz hat beschlossen, eine Arbeitsgruppe einzusetzen, der Vertreter der Datenschutz-Kontrollinstanzen von Frankreich, Luxemburg, Norwegen, Österreich und meiner Dienststelle angehören. Diese Arbeitsgruppe soll Vorschläge für die nächste Konferenz im Herbst 1982 ausarbeiten. Ich habe bereits ein Thesenpapier vorgelegt, das Grundlage für die Erörterungen der Arbeitsgruppe sein soll. Als wichtigste Punkte, die gegebenenfalls in Form einer völkerrechtlichen Konvention realisiert werden müssen, seien genannt:

— die Notwendigkeit klarer rechtsverbindlicher Regeln für datenverarbeitende Tätigkeit von Interpol (Kriterien für Sammlung, Auswertung und Speicherung sowie für Übermittlung und Löschung von Daten) und das Verhältnis zu den nationalen Zentralbüros;

— Schaffung eines unabhängigen *externen* Kontrollorgans sowie der Möglichkeit eines internationalen Rechtswegs gegen Maßnahmen von Interpol.

c) Bis zu diesem Zeitpunkt können die bestehenden Rechtsschutzlücken teilweise durch Kontrollen der Datenschutzbeauftragten gemildert werden, die in gemeinsamen Erörterungen zwischen dem Generalsekretär von Interpol einerseits, der französischen Datenschutzkommission und mir andererseits vereinbart werden konnten und sich in folgendem Rahmen bewegen:

— Interpol akzeptiert trotz bisher gegenteiliger Rechtsauffassung die aus dem Sitzstaatabkommen abzuleitende Anwendbarkeit des französischen Datenschutzgesetzes und damit die Kontrolle durch die französische Datenschutzkommission entsprechend dem Umfang, den das dort geltende Datenschutzgesetz bestimmt;

— Interpol ist auch einverstanden mit einer Kontrolle durch die anderen nationalen Datenschutzbeauftragten, sofern diese sich auf die Überprüfung der Daten beschränkt, die vom jeweiligen Nationalen Zentralbüro, in meinem Falle also dem BKA, an Interpol übermittelt werden.

Wegen der hierzu von Interpol erbetenen ausdrücklichen Zustimmung des Nationalen Zentralbüros habe ich mich mit dem BMI in Verbindung gesetzt. Ich gehe davon aus, daß die Zustimmung demnächst erteilt wird.

Auch wenn dies die Problematik keineswegs umfassend zu lösen vermag, so ist damit doch ein wichtiger Zwischenschritt getan, der gleichzeitig das Verständnis von Interpol für eine sachgerechte Berücksichtigung der datenschutzrechtlichen Erfordernisse zeigt.

### 2.13 Bundesamt für Verfassungsschutz

Im Berichtszeitraum wurde eine Reihe von Prüfungen beim Bundesamt für Verfassungsschutz durchgeführt. Es handelte sich sowohl um die Nachprüfung von Einzelfällen als auch um Querschnittsprüfungen nach dem Zufallsprinzip. Aus einer im Bereich der Terrorismusbekämpfung geführten Sonderdatei wurden einzelne Fälle geprüft. Es versteht sich von selbst, daß aus Gründen der Geheimhaltung hier keine Einzelheiten genannt werden können. Bei fast allen Prüfungen stieß ich jedoch auf folgende grundsätzliche Problempunkte:

#### 2.13.1 Bereinigung der „Altbestände"

Beim Bundesamt für Verfassungsschutz bestehen viele Unterlagen und Speicherungen, die wegen Zeitablaufs zu vernichten oder zu löschen sind. Ich konnte bei meinen Prüfungen häufig „Altbestände" entdecken, über deren „Vernichtungsreife" es auch beim BfV keine Zweifel gab. Hierunter waren Fälle, bei denen nach den NADIS-Löschungsfristen die Löschung bereits hätte erfolgen müssen. Aber auch innerhalb dieser Fristen, die ja nur einen formalisierten äußeren Rahmen bieten, gibt es nach dem Eindruck, den ich gewonnen habe, eine Reihe von Fällen, die zur Löschung anstehen. Dies gilt insbesondere, aber keineswegs ausschließlich, für den Bereich der Terrorismusbekämpfung. Hier sind unter dem Eindruck terroristischer Gewalttaten teilweise Speicherungen vorgenommen worden, die zumindest heute nicht mehr aufrechterhalten werden können.

Ich stehe auf dem Standpunkt, daß, je vager der Anfangsverdacht ist, um so früher und sorgfältiger die Notwendigkeit einer weiteren Speicherung geprüft werden muß. Nach meinem Eindruck wird die Tatsache, daß in NADIS viele Personendaten gespeichert sind, die inzwischen wegen Zeitablaufs oder aus anderen Gründen zu löschen wären, auch im BfV gesehen. Es wurden und werden dort auch Bemühungen unternommen, die Bestände, auch im eigenen Interesse, zu bereinigen. Offenbar müssen diese Anstrengungen aber noch verstärkt werden. Es geht nicht an, den Datenschutz ans Ende der Prioritätenskala zu setzen und Bereinigungen nur dann vorzuneh-

men, wenn die Arbeitslage es gerade erlaubt. Aus der Sicht des BfV wie anderer Sicherheitsbehörden mögen inaktuelle „Altbestände" ein nachrangiges Problem sein. Aus der Sicht des Datenschutzes werden sie um so „aktueller", je älter sie werden.

#### 2.13.2 Meinungsunterschiede bei den Neueinspeicherungen

Im Verlaufe der von mir durchgeführten Prüfungen sind erhebliche Meinungsverschiedenheiten über die rechtlichen Voraussetzungen zur Speicherung von Personendaten in NADIS zutage getreten. Nach meiner Auffassung haben die Verfassungsschutzbehörden im Extremismusbereich nicht primär die Aufgabe, personenbezogene Sammlungen anzulegen und zu führen, sondern Bestrebungen des im Verfassungsschutzgesetz näher geschilderten Inhalts zu beobachten und hierüber der Regierung und soweit möglich der Öffentlichkeit Bericht zu erstatten (vgl. schon 1. TB, Nr. 3.4.3.1, S. 22). Die Speicherung personenbezogener Daten muß diesem Zweck untergeordnet sein. Sie kommt nach meiner Auffassung nur in Betracht, wenn sich eine Person als Träger, d. h. als Funktionär einer verfassungsfeindlichen Bestrebung betätigt. Hingegen ist die bloße Mitgliedschaft in oder die Teilnahme an Veranstaltungen von Organisationen, die derartige Bestrebungen verfolgen, meines Erachtens kein Grund zu einer Speicherung bei den Verfassungsschutzbehörden.

Die Praxis und die Auffassung der Verfassungsschutzbehörden sehen freilich anders aus. Dies hängt aber nicht zuletzt mit den Anforderungen und Erwartungen zusammen, die bisweilen im Zusammenhang mit Verfassungstreueprüfungen an den Verfassungsschutz herangetragen werden.

Ich habe im Laufe der durchgeführten Prüfungen eine Reihe von Fällen gesehen, bei denen nach meiner Auffassung die Voraussetzungen für eine Speicherung nicht vorlagen. In diesen Fällen habe ich jeweils Beanstandungen ausgesprochen oder mich um eine einvernehmliche Lösung bemüht. Da ich bei meinen Prüfungen aber immer nur Einzelfälle beurteilen kann, müssen die hiermit zusammenhängenden Fragen auch generell geklärt werden.

#### 2.13.3 Weitere Grundsatzfragen

Ähnlich verhält es sich mit der Frage, inwieweit die Art der Erhebung und Gewinnung einer Information Auswirkungen auf die Rechtmäßigkeit ihrer Speicherung hat. Wie an anderer Stelle bereits dargestellt, gehe ich davon aus, daß mit polizeilichen Befugnissen erlangte Informationen außerhalb des Rahmens von § 7 Abs. 3 G 10 nicht an den Verfassungsschutz übermittelt und dort verarbeitet werden dürfen. Bei meinen Kontrollen habe ich jedoch in einer Reihe von Fällen die Verarbeitung derartiger Informationen beim Verfassungsschutz festgestellt. Auch hier halte ich einen grundsätzlichen Klärungsprozeß für dringend erforderlich.

Der Bundesminister des Innern hat mir mitgeteilt, daß er diese Grenzziehung trotz des Trennungsgebotes und der gesetzlich festgelegten Versagung polizeilicher Befugnisse für den Verfassungsschutz für zu eng hält. Insbesondere genüge eine solche Grenzziehung nicht den Sicherheitserfordernissen. Dies scheint mir jedoch weniger ein rechtliches als vielmehr ein rechtspolitisches Argument zu sein. Angesichts der bestehenden Rechtslage hat hierüber das Parlament zu befinden.

Erfreulich ist in diesem Zusammenhang, daß der BMI auf meine Initiative hin das BfV angewiesen hat, daß die Akten von anerkannten und nichtanerkannten Kriegsdienstverweigerern künftig nur noch mit Zustimmung des Betroffenen, etwa im Rahmen einer Sicherheitsüberprüfung, ausgewertet werden dürfen. Eine andere Praxis würde nach meiner Auffassung gegen Artikel 4 GG verstoßen. Der Kriegsdienstverweigerer ist im Rahmen des Anerkennungsverfahrens nämlich gezwungen, seine innersten Gewissensgründe zu offenbaren. Er tut dies nur zum Zwecke des Anerkennungsverfahrens und braucht nicht damit zu rechnen, daß diese Informationen für andere Zwecke, etwa des Verfassungsschutzes, verwendet werden (s. a. oben 2.1.2). Hierfür hat der BMI mit seiner Weisung gesorgt.

#### 2.13.4 Prüfung einer Sonderdatei

In einer mehrwöchigen Prüfung habe ich einige Fälle aus einer Sonderdatei geprüft. Hierbei handelt es sich um einen Sonderbestand, der nach anderen Gesichtspunkten aufgebaut ist als NADIS selbst. Der Zugriff auf diesen Bestand steht nur einigen Mitarbeitern der Verfassungsschutzbehörden offen, die für die entsprechenden Sachaufgaben zuständig sind. Die Prüfung hat Zweifel an der Effektivität und damit Erforderlichkeit dieser Datei entstehen lassen. Bevor ich mir ein endgültiges Urteil bilden kann, möchte ich allerdings eine Gesamtprüfung der Datei durchführen.

Schon jetzt kann allerdings gesagt werden, daß die Datei datenschutzrechtlich nicht unproblematisch ist. Was unter 2.13.2 über die Frage, unter welchen Voraussetzungen Personen in NADIS gespeichert werden dürfen, ausgeführt wurde, gilt auch und in verstärktem Maße für diese Spezialdatei. Grundsätzlich halte ich es auch für bedenklich, wenn Strukturen, Inhalte, kurz: qualitative Gedankenarbeit in den Computer verlagert werden soll. Hier werden häufig die äußeren und immanenten Grenzen dieser Technologie übersehen. Die daraus resultierenden Gefahren verstärken sich noch, wenn Computerspeicherungen nicht für jeden, der sie abrufen kann, anhand der Akten nachvollziehbar sind, wie das bei dieser Datei der Fall ist.

Ein weiterer Schwachpunkt dieser Sonderdatei ist, daß die Verantwortlichkeiten zwischen Bund und Ländern nicht mit der wünschenswerten Deutlichkeit geklärt sind.

Ich muß es auch an dieser Stelle bei diesen Bemerkungen bewenden lassen. Um die aus datenschutzrechtlicher Sicht problematischen Fragen zu klären, habe ich mich schriftlich an den Bundesminister des Innern und das Bundesamt für Verfassungsschutz gewandt und meine Auffassungen im einzelnen unter Anführung der Prüfungsergebnisse dargelegt.

Mit Schreiben vom 17. Dezember 1981 teilte mir der Bundesminister des Innern mit, daß er die Sonder-

datei unter Fragen der Effizienz wie unter allen im Zusammenhang mit dem Verfahren relevanten Fragen und damit auch unter datenschutzrechtlichen Gesichtspunkten kritisch überprüfen werde.

#### 2.13.5 Dateianfrage

Die Sicherheitsüberprüfung der Bundesbediensteten ist in den Richtlinien vom 15. Februar 1971, die Verfassungstreueprüfung in den Richtlinien vom 8. November 1978 (Bulletin Nr. 131 vom 14. November 1978, S. 1221; s. a. BT-Drucksache 8/2482) geregelt. In den vergangenen Jahren hat sich die sog. „Dateianfrage" als vereinfachte oder auch vorgezogene Form der Sicherheitsüberprüfung herausgebildet. Sofern sie nur eine gewisse Vorabinformation im Rahmen und unter Einhaltung der Verfahrenskautelen der Sicherheitsüberprüfung darstellt, ist aus datenschutzrechtlicher Sicht dagegen nichts einzuwenden.

Im Rahmen einer mehrwöchigen Überprüfungsaktion bei mehreren obersten Bundesbehörden und bei Behörden des nachgeordneten Bereichs mußte ich aber feststellen, daß die Dateianfrage auch dazu benutzt wurde, *vor* Beginn der Sicherheitsüberprüfung und ohne Einhaltung der dafür vorgeschriebenen Modalitäten von den Sicherheitsbehörden Informationen zu erhalten, die bei Stellenbesetzungen verwertet wurden. In vielen Fällen geschah dies ohne Wissen des Betroffenen. Waren mehrere Bewerber vorhanden, so war es möglich, die Auswahl auch unter dem Gesichtspunkt zu treffen, ob gegen einen Bewerber „etwas vorlag" oder nicht. Da die Bewerber von der Überprüfung — auch wenn sie mit einer Überprüfung rechnen mußten — in diesem Stadium noch nichts wußten, wurden ihnen bei einer Absage auch nicht deren Gründe eröffnet. Waren dafür Sicherheitsbedenken maßgebend, so war dem Bewerber die Chance zur Rechtfertigung genommen.

Darüber hinaus gab es noch weitere Fälle, in denen entgegen den vorgenannten Richtlinien ohne Wissen der Betroffenen beim Verfassungsschutz angefragt und zweckfremde Folgerungen aus den Antworten gezogen wurden.

So war es möglich, daß im Zuge der Überprüfung des sog. Rahmenpersonals (z. B. Reinigungskräfte, Handwerker usw.) der Arbeitgeber, dem Sicherheitsbedenken gegen einzelne seiner Bediensteten mitgeteilt wurden, hieraus arbeitsrechtliche Konsequenzen zog. Wenn die Bediensteten nichts von der Überprüfung wußten, war es möglich, daß für die arbeitsrechtlichen Maßnahmen ausweichende Begründungen gegeben wurden und für die Bediensteten keine Chance einer sachgerechten Verteidigung bestand.

Mit Schreiben vom 14. April 1981 an alle Obersten Bundesbehörden habe ich auf diese Mißbrauchsmöglichkeiten hingewiesen und gefordert, Überprüfungen auch im Wege der Dateianfrage nur noch mit Wissen des Betroffenen vorzunehmen.

Der Bundesminister des Innern hat mir daraufhin mitgeteilt, er habe folgendes veranlaßt:

— Alle Personen, die einer Sicherheitsüberprüfung unterzogen werden, sind auf diese Tatsache hinzuweisen. Das gilt auch für die Sicherheitsüberprüfung durch Dateianfrage.

— Mitteilungen an den Arbeitgeber, daß ein bestimmter Arbeitnehmer im Sicherheitsbereich nicht eingesetzt werden kann, werden mit einem Hinweis versehen, daß damit kein negatives Werturteil verbunden ist und die Mitteilung nur für den sicherheitsempfindlichen Bereich Bedeutung hat.

— Die Behörden, die Sicherheitsüberprüfungen veranlassen, werden auf die strikte Trennung von Personalverwaltung und Geheimschutz und die grundsätzliche Unzulässigkeit der Weitergabe von im Rahmen der Sicherheitsüberprüfung gewonnenen Erkenntnissen an personalverwaltende Stellen nochmals hingewiesen.

— Den Bundesressorts wird empfohlen, in den Fällen, in denen der Arbeitgeber von dem die Sicherheitsüberprüfung auslösenden Verhalten des Arbeitnehmers nur mittelbar betroffen ist, nur den Betroffenen selbst über das Ergebnis des Antrags zu unterrichten (Beispiel: Anträge auf Benutzung von in Sicherheitsbereichen liegenden Kantinen werden vom Arbeitgeber gesammelt und weitergegeben).

Ich begrüße diesen Schritt des BMI und werde die Einhaltung der Regelung überprüfen.

### 2.14 Zusammenarbeit Verfassungsschutz/Polizei

Die in diesem Jahr beim BKA und beim BfV durchgeführten Aktenprüfungen haben in einer Reihe von Fällen ergeben, daß Informationen verarbeitet werden, die von der jeweils anderen Behörde übermittelt worden waren. Kann aber der Verfassungsschutz Daten und Informationen verarbeiten, die die Polizei unter Anwendung polizeilicher Befugnisse erlangt hat, während umgekehrt die Polizei Informationen erhält, die mit nachrichtendienstlichen Mitteln des Verfassungsschutzes gewonnen wurden, so droht das Gebot der Trennung von Polizei und Verfassungsschutz zu einem Prinzip möglichst effektiver Arbeitsteilung zu verkümmern. Aufgaben- und Zuständigkeitsverteilungen, die für das demokratische Gemeinwesen grundlegend sind, dürfen aber nicht im Wege der Amtshilfe ausgehöhlt werden.

Im einzelnen hatte ich zu beanstanden, daß vergleichsweise häufig Informationen an den Verfassungsschutz übermittelt wurden, die aus Hausdurchsuchungen stammten. Über das Trennungsgebot hinaus stehen der Übermittlung und Verarbeitung derartiger Informationen auch Wortlaut und Sinn der §§ 108, 110 StPO entgegen. Ähnliches gilt für Informationen, die aufgrund polizeilicher Telefonüberwachungsmaßnahmen gewonnen wurden. Die in § 100b StPO geregelten Verwertungsvorschriften lassen nach meiner Auffassung eine Übermittlung von auf diesem Wege gewonnenen Informationen an den Verfassungsschutz und die Verar-

beitung derartiger Informationen durch den Verfassungsschutz nicht zu. In Fällen, in denen auch der Verfassungsschutz nach G 10 selbst Abhörmaßnahmen durchführen könnte, würde bei einer Verwendung polizeilicher Abhörunterlagen die Kontrollkompetenz der G-10-Kommission unterlaufen.

Im Zuge der Prüfungen beim BfV und beim BKA habe ich auch Feststellungen zur Art und zum Ausmaß der Zusammenarbeit beider Behörden im Rahmen der Terrorismusbekämpfung getroffen. Insbesondere im Jahre 1977 hat die Konferenz der Innenminister eine Reihe von Beschlüssen gefaßt, die diese Zusammenarbeit bei der Abklärung des terroristischen Umfeldes regeln. Nach meiner Auffassung stehen diese Beschlüsse zum Teil nicht im Einklang mit dem verfassungskräftigen Gebot der Trennung zwischen Polizei und Verfassungsschutz. Durch diese Beschlüsse sind umfangreiche Datenübermittlungen vom BKA an das BfV und umgekehrt vereinbart worden. BKA und BfV erhielten gemeinsam Aufgaben, die in einer eigenartigen Zuständigkeits-„Gemengelage" von beiden wahrgenommen werden, ohne daß die bisherigen Zuständigkeitsabgrenzungen beachtet würden.

Meine Bedenken habe ich dem Bundesminister des Innern im einzelnen vorgetragen. Grundsätzlich bin ich der Auffassung, daß die zu Recht als wichtiger datenschutzrechtlicher Fortschritt gewürdigte teilweise Abkoppelung des BKA von NADIS und die vollständige Abkoppelung des BfV von PIOS deutlich an Wert verliert, wenn statt dessen auf konventionellem Wege die Informationen übermittelt werden.

Es mag widersprüchlich klingen, wenn hier und anderswo von datenschutzrechtlicher Seite ein Zuviel an Informationsaustausch zwischen BKA und BfV beklagt wird, während aus Kreisen der Sicherheitsbehörden oder in der Öffentlichkeit nicht selten betont wird, datenschutzrechtliche Hemmnisse hinderten eine effektive Zusammenarbeit.

Datenschutz bedeutet keineswegs, daß Polizei und Verfassungsschutz sich gegenseitig nicht informieren dürfen. Sofern keine personenbezogenen Daten übermittelt werden, stellen sich ohnehin keine datenschutzrechtlichen Fragen. Im übrigen aber hat der Gesetzgeber in § 7 Abs. 3 G 10 diejenigen Rechtsgüter beschrieben, deren Schutz wichtiger ist als das ansonsten gerade bei Telefon- und Postüberwachungsmaßnahmen bedeutsame Zweckbindungsprinzip. Eine Beschränkung der gegenseitigen Informationen auf Fälle analog § 7 Abs. 3 G 10, wie ich sie seit langem fordere (vgl. 1. TB, Nr. 3.4.3.2, S. 24, 3. TB, Nr. 3.11.1.1, S. 47), würde einerseits die Aufmerksamkeit auf die wesentlichen Gesichtspunkte lenken und andererseits die datenschutzrechtlich besonders bedenklichen „Massengeschäfte" vermeiden. Hierdurch könnte zugleich ein Mehr an Sicherheit und an Rechtsstaatlichkeit erreicht werden. Zur in den letzten Tagen u. a. hierzu eingegangenen Stellungnahme des Bundesministers des Innern s. o. Nr. 2.13.3.

Schwierigkeiten bei der Zusammenarbeit der Sicherheitsbehörden, wie sie in der Öffentlichkeit bei spektakulären Fällen erörtert zu werden pflegen, haben regelmäßig andere Ursachen als gerade datenschutzrechtliche Anforderungen.

## 2.15 Bundesgrenzschutz

### 2.15.1 Allgemeines

Gegenstand des Prüfungsbesuches bei der Grenzschutzdirektion war die Prüfung der Einstellungskriterien für die Speicherung von Informationen im Grenzfahndungsbestand und im geschützten Zentralen Personenindex (ZPI) der Grenzschutzdirektion innerhalb des INPOL-Systems. Darüber hinaus habe ich einige bisher noch offene Punkte aus der Prüfungstätigkeit in den vorherigen Berichtszeiträumen (z. B. Amtshilfe für die Nachrichtendienste; hierzu s. 3. TB, Nr. 3.11.3, S. 53) angesprochen.

a) In meinem 2. Tätigkeitsbericht (S. 48) habe ich dargestellt, daß die Grenzschutzdirektion mir zugesichert hatte, nur noch solche Daten in den Zentralen Personenindex des Bundeskriminalamts einzugeben, die für alle angeschlossenen Polizeibehörden erforderlich sind, insbesondere Daten für die *allgemeine* aktuelle Fahndung. Personengrunddaten und Aktenfundstellen aus Vorgängen, die allein oder überwiegend für die Grenzschutztätigkeit relevant sind, sollten dagegen in einen geschützten Teil des Zentralen Personenindex eingestellt werden, auf den nur die Grenzschutzdirektion Zugriff hat. Bei der Durchsicht einiger Unterlagen der Grenzschutzdirektion mußte ich nunmehr feststellen, daß die Personengrunddaten und Aktenfundstellen aus den betreffenden Vorgängen entgegen der Zusicherung in den allgemeinen Zentralen Personenindex des Bundeskriminalamtes eingespeichert worden waren, obwohl es sich um vorwiegend oder ausschließlich grenzpolizeilich relevante Vorgänge handelte. Erst im Juni 1981 hat die Grenzschutzdirektion die Anweisung erteilt, Hinweise auf Vorgänge der Grenzschutzdirektion, die nicht der allgemeinen Fahndung dienen, nur noch in den geschützten Teil des Zentralen Personenindex einzugeben. Seit diesem Zeitpunkt ist somit ein Zugriff der anderen INPOL-Teilnehmer nicht mehr möglich. Es kommt jetzt darauf an, den allgemeinen Zentralen Personenindex so schnell wie möglich zu bereinigen und die Hinweise auf Vorgänge der Grenzschutzdirektion herauszunehmen. Kurz vor Drucklegung hat mir die Grenzschutzdirektion fernschriftlich mitgeteilt, daß diese Bereinigung inzwischen eingeleitet ist.

b) Auch die bei meiner Prüfung festgestellte Praxis der Einstellung von Personengrunddaten und Fundstellen zu Vorgängen der Grenzschutzdirektion in den *geschützten Teil* des Zentralen Personenindex erscheint mir nicht unproblematisch. Die Fahndungsleitstelle der Grenzschutzdirektion sammelt eingehende Informationen (z. B. Fernschreiben von Polizeidienststellen) nach der Zeitfolge und vergibt Personennummern für die bekanntgewordenen Personalien. Die Entscheidung über die Einstellung dieser

Personendaten in den geschützten Zentralen Personenindex traf allein der polizeiliche Sachbearbeiter, ohne daß ihm bisher hierfür Entscheidungshilfen zur Verfügung standen. Dies führte dazu, daß auch die Personalien solcher Personen eingestellt wurden, die für die Arbeit des Bundesgrenzschutzes ohne jeden Belang waren. Einige Fernschreiben von Polizeibehörden aus dem Jahre 1981 trugen den Bearbeitungsvermerk „Es ist nichts zu veranlassen". Die Personengrunddaten der genannten Personen waren gleichwohl durch die Grenzschutzdirektion in den Personenindex eingestellt worden. Auf der Grundlage dieser Feststellungen habe ich beim BMI und der Grenzschutzdirektion angeregt, in den Beständen des geschützten Zentralen Personenindex solche Informationen zu löschen, die keinen grenzpolizeilichen Bezug haben. Außerdem habe ich dringend gefordert, umgehend verbindliche Regelungen für die Einstellung von Informationen in Dateien des Bundesgrenzschutzes sowie für das Anlegen von Personenakten zu schaffen, um zu verhindern, daß in kurzer Zeit wegen der Sammlung nicht relevanter Informationen wiederum umfangreiche Bereinigungen von Akten und Datenbeständen erforderlich werden. Dies wurde mir zugesagt. Die Grenzschutzdirektion hat mir nunmehr fernschriftlich mitgeteilt, daß sie dem Bundesminister des Innern eine vorläufige Dienstanweisung als ergänzende Regelung zu den KpS-Richtlinien zur Genehmigung vorgelegt hat, die umfassend das Anlegen von Akten, die Einstellung und Löschung von Datensätzen regelt. Diese Dienstanweisung ist seit dem 1. September 1981 für die Fahndungsleitstelle und auch für die Zentralstelle für die Bekämpfung der unerlaubten Einreise von Ausländern vorläufig in Kraft.

#### 2.15.2 Zugriff anderer Polizeibehörden auf den geschützten Grenzfahndungsbestand

Bei dem Prüfungsbesuch beim Bundeskriminalamt Anfang dieses Jahres habe ich festgestellt, daß nach den INPOL-Verbundkonventionen auch die Staatsschutzdienststellen des Bundeskriminalamtes und der Landeskriminalämter auf den geschützten Grenzfahndungsbestand zugreifen können. Bereits in meinem 2. Tätigkeitsbericht (Nr. 2.8.3, S. 48) habe ich ausgeführt, daß die Aufgaben des Grenzschutzes und der allgemeinen Polizei nur zu einem geringen Teil identisch sind. Ich habe deshalb gegenüber den Vertretern des Bundeskriminalamts und der Grenzschutzdirektion erklärt, daß ich den Zugriff anderer Polizeidienststellen als der Dienststellen des Bundesgrenzschutzes datenschutzrechtlich nicht für zulässig halte.

Der Bundesminister des Innern hat mir inzwischen mitgeteilt, daß die Zugriffsberechtigung für die Staatsschutzdienststellen des Bundeskriminalamtes und der Landeskriminalämter und für das Zollkriminalinstitut auf den geschützten Grenzfahndungsbestand aufgehoben wird. Das Bundeskriminalamt ist angewiesen, die geänderte Zugriffsregelung auch technisch sicherzustellen.

Da der Gesamtbestand des Grenzfahndungsbestandes auch im Grenzfahndungsbuch enthalten ist, wird künftig auch die Übersendung des Grenzfahndungsbuches an die vorgenannten Polizeidienststellen eingestellt. Das Grenzfahndungsbuch wird auch nicht mehr an die Verfassungsschutzbehörden, den Bundesnachrichtendienst und das Amt für Sicherheit der Bundeswehr, verteilt. Diese Stellen haben zwar keinen direkten Zugriff auf den geschützten Grenzfahndungsbestand, waren aber Bezieher des Grenzfahndungsbuches. In dieser regelmäßigen Übersendung lag auch ein Verstoß gegen das Gebot der Trennung von Polizei und Nachrichtendiensten.

#### 2.15.3 Grenzschutz und Zusammenarbeit mit Nachrichtendiensten

Am 1. Dezember 1981 ist eine neue Dienstanweisung des BMI an den BGS auf der Grundlage von Amtshilfeersuchen der Nachrichtendienste in Kraft getreten. Damit wurde die umstrittene sogenannte „Sonderanweisung grenzpolizeiliche Kontrolle" (SoGK) abgeschafft. Die Neuregelung ist in der Öffentlichkeit teilweise geradezu überschwenglich begrüßt worden. Ich kann diese Einschätzung im Augenblick noch nicht teilen. Bei aller Anerkennung der gegenüber der früheren Rechtslage intendierten Fortschritte sind doch einige wesentliche Probleme nicht gelöst worden. Insbesondere ist auch durch die Neuregelung die Inanspruchnahme der grenzpolizeilichen Befugnisse des BGS durch den Verfassungsschutz nicht ausgeschlossen, worauf es aber nach den Gutachten der Professoren zur Amtshilfeproblematik und auch nach meiner Auffassung besonders angekommen wäre. Auch eine Reihe weiterer Fragen ist aus datenschutzrechtlicher Sicht noch zu klären.

Zusammen mit dem Bundesminister des Innern bin ich jedoch der Auffassung, daß vor allem die praktische Auswirkung der Neuregelung abgewartet werden soll. Ich beabsichtige, mir im Laufe des Jahres 1982 durch Kontrollbesuche ein Bild darüber zu verschaffen, ob durch die Neuregelung tatsächlich datenschutzrechtliche Verbesserungen eingetreten sind.

Darüber hinaus ist für meine Beurteilung der Neuregelung ausschlaggebend, daß der Bundesminister des Innern mehrfach ausdrücklich versichert hat — so auch anläßlich der Unterrichtung des Innenausschusses des Deutschen Bundestages im November 1981 — daß nach der Erprobungsphase die unerläßlichen gesetzlichen Grundlagen für die Zusammenarbeit des BGS mit den Nachrichtendiensten erarbeitet werden sollen.

#### 2.15.4 Personenkarteien bei Grenzschutzstellen

Bei den in meinem 3. Tätigkeitsbericht (s. dort Nr. 3.11.3, S. 53) erwähnten Kontrollen von Grenzschutzstellen wurde festgestellt, daß bei einer Grenzschutzstelle eine manuelle Personenkartei geführt wurde, in der neben den grenzpolizeilich relevanten Vorgängen auch Informationen über Meldungen nach der „Sonderanweisung Grenzkontrolle" (So-GK) personenbezogen festgehalten worden

waren. Gegenüber der Grenzschutzdirektion habe ich datenschutzrechtliche Bedenken gegen diese Kartei geäußert, soweit dort auch solche „Amtshilfefälle" erfaßt sind. Die Grenzschutzdirektion hat meine Bedenken zum Anlaß genommen, generell zu überprüfen, inwieweit Personenkarteien bei den Grenzschutzstellen überhaupt erforderlich sind. Als Ergebnis dieser Überprüfung sind die Grenzschutzämter inzwischen angewiesen worden, die Fortführung dieser Karteien einzustellen und die bestehenden personenbezogenen Karteien umgehend zu vernichten.

Soweit Personenkarteien bei den Grenzschutzämtern geführt werden, ist sicherzustellen, daß keine Erkenntnisse aufgenommen werden, die aufgrund von Amtshilfeersuchen und somit ohne grenzpolizeilichen Anlaß gewonnen werden.

## 2.16 Bundesnachrichtendienst

### 2.16.1 Allgemeines

Im Berichtszeitraum fanden mehrere Arbeitsbesuche statt. Die Überprüfungen haben jeweils die Richtigkeit gegebener Auskünfte und die Ausführung zugesagter Verbesserungen bestätigt. Kleinere Mängel, die zum Teil auf Dokumentationsfehlern oder Unterlassungen beruhten, wurden abgestellt.

Bei der Prüfung einer Stelle des BND zeigte sich, daß die nach § 15 BDSG erforderliche Dateienübersicht hinsichtlich der dort geführten Dateien noch nicht angefertigt war. Dies wird nachgeholt.

In einem nicht unbedeutenden Komplex, der die Befragung von Personen durch den BND betrifft, konnte ein relatives Höchstmaß an Durchschaubarkeit für den Befragten erzielt werden. Insbesondere wurden Praktiken, die der Freiwilligkeit der betroffenen Personen teilweise etwas „nachhalfen", abgestellt.

Aus meiner Kontrolltätigkeit bei anderen Stellen hatten sich Anhaltspunkte dafür ergeben, daß der BND personenbezogene Daten sammle und auswerte, die seinen Aufgabenbereich überschritten hätten. Eine Prüfung führte zu dem Ergebnis, daß diese Sorge unbegründet war.

### 2.16.2 Amtshilfe-Richtlinien

Die neuen Richtlinien über die Amtshilfe des BGS für die Nachrichtendienste (s. o. S. 31) stellen einen weiteren Schritt auf dem Wege zu einer rechtsstaatlichen Regelung dieser Informationsbeziehungen und damit der Tätigkeit des BND dar. Ich werde im Jahre 1982 prüfen, ob die mit den Richtlinien beabsichtigten Verbesserungen des Datenschutzes realisiert sind.

Der Bundesminister des Innern hat darüber hinaus erneut zugesagt, in absehbarer Zeit den Entwurf eines entsprechenden Gesetzes vorzulegen. Hiervon ist dann auch das notwendige Ausmaß an Transparenz und gesetzlicher Fundierung der Tätigkeit des BND in diesem Bereich zu erwarten.

### 2.16.3 Zusammenarbeits-Richtlinien

Problematisch ist nach wie vor, daß die Richtlinien für die Zusammenarbeit der Verfassungsschutzbehörden, des BND, des MAD, der Polizei und der Strafverfolgungsbehörden in Staatsschutzangelegenheiten (Zusammenarbeitsrichtlinien in der Fassung vom 23. Juli 1973) die gegenseitige Unterrichtung der vorgenannten Behörden ohne klare Zweckbindung verlangen. Die Richtlinien müssen daher präzisiert werden. Außerdem habe ich beim BND angeregt, bestehende Dienstanweisungen über Voraussetzungen für das Speichern und Übermitteln personenbezogener Daten präziser zu fassen, um schon durch den Wortlaut der Dienstanweisung eine restriktive Praxis sicherzustellen.

### 2.16.4 Löschungs-Richtlinien

Im August 1980 wurden Löschungsrichtlinien für den BND in Kraft gesetzt. Ihre Anwendung führte bereits zu einer beträchtlichen Anzahl von Löschungen. Dies ist aber auch eine Folge der Tatsache, daß früher die weitere Erforderlichkeit der Akten und Daten zumindest nicht regelmäßig überprüft wurde. Unabhängig davon halte ich es nicht für richtig, daß der BND für alle in seinem Tätigkeitsbereich gespeicherten Daten stets dieselbe Überprüfungsfrist zugrunde legt, ohne danach zu unterscheiden, in welchem Zusammenhang die Daten angefallen sind und zu welchem Zweck sie aufbewahrt werden. Ich habe daher entsprechende Vorschläge unterbreitet, die den Erfordernissen des Datenschutzes besser gerecht werden, ohne legitime Sicherheitsinteressen des BND zu gefährden.

## 2.17 Militärischer Abschirmdienst (MAD)

Im vergangenen Jahr habe ich bei den MAD-Gruppen Kiel, Düsseldorf und München datenschutzrechtliche Prüfungen durchgeführt.

Sowohl in Kiel als auch in Düsseldorf mußte ich feststellen, daß personenbezogene Daten außerhalb des Zuständigkeitsbereiches des MAD verarbeitet waren. Teilweise waren die Grenzen zum Zuständigkeitsbereich des Verfassungsschutzes verwischt. In einem Fall wurde eine Datei geführt, in der Informationen über Personen enthalten waren, deren Speicherung nach meiner Auffassung selbst durch den Verfassungsschutz nicht zulässig gewesen wäre, weil es sich nicht um Träger verfassungsfeindlicher Bestrebungen handelte.

Ein anderer Kritikpunkt ergab sich daraus, daß die Dateien der geprüften Gruppen mit „Altfällen" belastet waren. Es handelte sich dabei um Daten über Personen, deren Aufnahme in die Datei berechtigt war, die aber längst wieder hätten gelöscht werden müssen.

Wenn ich gleichwohl hinsichtlich des MAD zu einer positiven Gesamtwertung komme, so deswegen, weil die hier geschilderten Probleme auch dort erkannt wurden und weil, was noch wichtiger ist, daraus

Konsequenzen gezogen wurden. Bei den MAD-Gruppen Kiel und Düsseldorf wurden umfangreiche Bereinigungen vorgenommen, in deren Verlauf Tausende von Personendaten gelöscht wurden. Ich erwähne dies deshalb besonders, weil ein derart gutes Verständnis und eine derartige Bereitschaft, aus festgestellten Mängeln umgehend die notwendigen Konsequenzen zu ziehen, nicht immer bei Sicherheitsbehörden anzutreffen sind. Mit dem Bundesminister der Verteidigung und dem Amt für Sicherheit der Bundeswehr befinde ich mich in laufenden Gesprächen über die Frage, wie die innerdienstlichen Weisungen noch enger und präziser gefaßt werden können, damit in Zukunft nach Möglichkeit keine unberechtigten Speicherungen mehr entstehen. Die Initiative für diese Neuregelungen kam erfreulicherweise aus dem Amt für Sicherheit der Bundeswehr selbst. Auch wenn durch solche Richtlinien die weitgehend fehlende Rechtsgrundlage für die MAD-Arbeit generell nicht ersetzt werden kann, so können sie doch geeignet sein, bei der praktischen Arbeit einen handhabbaren Maßstab zu bilden.

## 2.18 Zollkriminalinstitut

### 2.18.1 Zentrale Vorgangskartei

Die derzeit noch betriebene Zentrale Vorgangskartei (ZVK) beim Zollkriminalinstitut umfaßt mehr als 170 000 Personendatensätze. Die Aufgaben dieser Kartei sind inzwischen in vollem Umfang von dem Informationssystem für den Zollfahndungsdienst INZOLL (vgl. 3. TB, Nr. 3.3.2.2, S. 22) übernommen worden. Darüber hinaus sind in der ZVK auch noch Informationen vorhanden, die wegen Zeitablaufs erst gar nicht in INZOLL eingestellt worden sind. Die ZVK ist somit für ihren ursprünglichen Zweck nicht mehr erforderlich. Ich habe dies dem Bundesminister der Finanzen mitgeteilt und um Vernichtung der Kartei gebeten. Der Bundesminister der Finanzen hat mir inzwischen berichtet, daß diese Arbeiten aufgenommen und mittlerweile ca. 90 % der zu vernichtenden Karteikarten entfernt worden sind. In Zukunft sollen beim ZKI nur noch Hinweise auf eigene Verwaltungsvorgänge in einer manuellen Kartei geführt werden.

### 2.18.2 Zugriff des Zollkriminalinstituts auf den Zentralen Personenindex (ZPI) des Bundeskriminalamts

Bei einem Prüfungsbesuch beim Zollkriminalinstitut habe ich festgestellt, daß das ZKI zu den wenigen Sicherheitsbehörden gehört, die Zugriff auf den Zentralen Personenindex des Bundeskriminalamts haben. Hierbei handelt es sich um den Zentralen Nachweis der beim BKA geführten Kriminalakten. Darüber hinaus gibt der ZPI Auskünfte über aktuelle und inaktuelle Fahndungs- und Haftnotierungen sowie Hinweise auf die ed-Unterlagen, Alias-Namen und Vorgänge in der Straftaten/Straftäter-Datei. Ich halte den Direktzugriff des Zollkriminalinstituts auf allgemeine polizeiliche Erkenntnisse für nicht erforderlich und damit auch nicht für zulässig. Der Bundesminister der Finanzen hat mir mit Schreiben vom 21. Dezember 1981 mitgeteilt, daß das ZKI inzwischen nur noch auf die aktuellen Fahndungsnotierungen zugreifen kann. Die bisherigen Zugriffsmöglichkeiten auf andere Datengruppen, insbesondere auf den ZPI, bestehen nicht mehr.

### 2.18.3 Ausschreibung von Personen zur zollrechtlichen Überwachung

Das Zollkriminalinstitut speichert in der INPOL-Fahndungsdatei u. a. Personen, die an den Grenzen besonderen zollrechtlichen Maßnahmen unterzogen werden sollen, ohne daß dies den Personen selbst bekanntwerden darf (Ausschreibung zur polizeilichen Beobachtung, Bereich zollrechtliche Überwachung — PB 50). Bei Antreffen von so ausgeschriebenen Personen dürfen nach der Polizeidienstvorschrift 384.2 lediglich Maßnahmen nach zollrechtlichen Bestimmungen (z. B. Anhalten, Durchsuchungen, Überholungen) getroffen werden. Zweck der zollrechtlichen Überwachung ist es nämlich, Zoll- und sonstige Steuerdelikte bei der Einfuhr von Waren zu bekämpfen. Maßnahmen anderer INPOL-Benutzer (z. B. Polizeibehörden) sind ausdrücklich ausgeschlossen, es handelt sich um ein rein zollrechtliches Instrument.

Informationen, die in den Datenbestand „zollrechtliche Überwachung" eingestellt werden, unterliegen als steuerliche Erkenntnisse dem Steuergeheimnis, soweit sie in einem Steuerverfahren gewonnen worden sind.

Sie dürfen nur unter den eng begrenzten Voraussetzungen des § 30 AO offenbart werden (vgl. 3. TB, Nr. 3.3.2.4, S. 23). Da aber die zollrechtliche Überwachung Teil des INPOL-Personenfahndungsprogramms ist, haben hierauf neben dem Zollkriminalinstitut auch das Bundeskriminalamt, die Polizeidienststellen der Länder, der Bundesgrenzschutz, die Grenzschutzdirektion, die Dienststellen der Bahnpolizei und die Hausinspektion des Deutschen Bundestages Zugriff. Alle diese Behörden sind nicht befugt, zollrechtliche Maßnahmen zu ergreifen. Die Übermittlung der Daten an diese Behörden ist zur Erreichung dieses Zieles nicht erforderlich und daher mit § 30 AO nicht vereinbar. Ich habe meine Bedenken gegen die generelle Offenbarung dieser Erkenntnisse dem Bundesminister der Finanzen mitgeteilt. Seine daraufhin erfolgte Ankündigung, er werde Weisung erteilen, daß keine Datensätze zur zollrechtlichen Überwachung mehr ausgeschrieben werden dürfen, bis ein eigener Datenbestand für das Zollkriminalinstitut geschaffen worden ist, ist allerdings noch nicht in die Tat umgesetzt worden. Ich muß deshalb meine datenschutzrechtlichen Bedenken weiterhin aufrecht erhalten.

Diese Bedenken verstärken sich noch aufgrund folgenden Sachverhalts:

Ich habe bei einer Sicherheitsbehörde festgestellt, daß Polizeidienststellen des Bundes und der Länder bei Inkrafttreten der Polizeidienstvorschrift 384.2 ca. 900 Personendatensätze aus der polizeilichen Beobachtung „Rauschgift und Waffen" gelöscht haben. Dies dürfte damit zusammenhängen, daß in diesen Fällen die nunmehr strengeren Voraussetzungen der PDV 384.2 für eine Ausschreibung zur polizeili-

chen Beobachtung nicht mehr erfüllt waren. Diese Personendatensätze sind dann an das Zollkriminalinstitut zur Prüfung übermittelt worden, ob eine Einstellung der Personen mit dem Ausschreibungsanlaß „zollrechtliche Überwachung" in Betracht komme. Hierbei ist zu bemerken, daß nach der PDV 384.2 für die Einstellung in die zollrechtliche Überwachung die begründete Vermutung, daß Personen in den Deliktsbereichen Rauschgift- und Waffenschmuggel in Erscheinung treten könnten, ausreicht. Der nahezu gleichzeitig zu beobachtende Anstieg der Fälle der zollrechtlichen Überwachung um ca. 900 legt die Vermutung nahe, daß die Fälle, die die Voraussetzungen für die polizeiliche Beobachtung „Rauschgift und Waffen" nicht mehr erfüllt haben, in der zollrechtlichen Überwachung erfaßt worden sind. Die mit Erlaß des PDV 384.2 beabsichtigte Verschärfung der Voraussetzungen für die polizeiliche Beobachtung hätte sich damit für diese 900 Personen überhaupt nicht ausgewirkt. Diese 900 Personen wären nämlich nach wie vor in der INPOL-Fahndungsdatei gespeichert, nur wäre der Ausschreibungsanlaß nunmehr ein anderer. Die Speicherung nur noch im Rahmen der zollrechtlichen Überwachung kann offenbar nicht verhindern, daß sie gleichwohl aufgrund dieser Ausschreibung auch polizeilichen Maßnahmen unterzogen werden. So konnte ich in einem konkreten Fall feststellen, daß ein zur zollrechtlichen Überwachung ausgeschriebener Bürger (in einer Großstadt, keineswegs an der Grenze) einer strengen polizeilichen Kontrolle unterzogen wurde. Da von dieser Kontrolle auch die übliche Meldung auf dem polizeilichen Meldeweg erstattet wurde, hatte jedenfalls in diesem Falle die Ausschreibung zur zollrechtlichen Überwachung genau denselben Effekt, wie ihn die Ausschreibung zur polizeilichen Beobachtung gehabt hätte.

Leider war es mir nicht möglich, die genaueren Umstände und Einzelheiten dieses Vorganges zu überprüfen. Das Zollkriminalinstitut hat sich nämlich auf den Standpunkt gestellt, daß die von der Polizei übermittelten 900 Datensätze „Steuerdaten" geworden sind, nachdem sie an das Zollkriminalinstitut übermittelt wurden. Ich halte diese Rechtsauffassung für unzutreffend und bedauere es, daß sich das Zollkriminalinstitut für den Bereich der zollrechtlichen Überwachung unter Berufung auf das Steuergeheimnis meiner Kontrolle zu entziehen sucht, obwohl gerade in diesem Bereich das Steuergeheimnis durch das Zollkriminalinstitut selbst verletzt wird. Leider hat sich bislang auch der Bundesminister der Finanzen unter Berufung auf das Steuergeheimnis geweigert, Einzelheiten aus der zollrechtlichen Überwachung datenschutzrechtlich überprüfen zu lassen. In diesem Bereich ist also eine effektive datenschutzrechtliche Kontrolle derzeit nicht möglich. Dies sollte spätestens mit der Novellierung des BDSG geändert werden.

### 2.19 Verbindungen der Sicherheitsbehörden zum Ausländerzentralregister (AZR)

Im Herbst 1980 habe ich das beim Bundesverwaltungsamt in Köln geführte Ausländerzentralregister überprüft. Hierbei habe ich festgestellt, daß das AZR im Laufe der Jahre immer mehr zu einer von den Sicherheitsbehörden mitbenutzten Datei geworden ist. Dies gilt sowohl für den Inhalt der dort gespeicherten Daten als auch für die Möglichkeit des Fernabrufs dieser Daten. Die Entwicklung des AZR bis zu dem Zustand, zu dem ich es bei meiner Prüfung angetroffen habe, hat sich ohne entsprechende Rechtsgrundlagen, nur auf der Basis von § 6 des Gesetzes über die Errichtung des Bundesverwaltungsamtes vom 28. Dezember 1959 (BGBl. I S. 829), und ohne erkennbares Konzept vollzogen. Im Ergebnis hat dies dazu geführt, daß kaum ein Beteiligter mehr den vollständigen Überblick über die Einzelheiten des AZR hatte. Beispielsweise waren dort noch Personendaten mit Aktenzeichen von Akten gespeichert, die bei der betreffenden Sicherheitsbehörde bereits Jahre zuvor vernichtet worden waren.

Besonders bedenklich erscheint mir, daß inzwischen eine ganze Reihe von Sicherheitsbehörden einen Online-Anschluß an das AZR besitzt. Hierfür gibt es keine Rechtsgrundlagen. Es geht nicht an, daß für eine Reihe von Sicherheitsbehörden Schritt für Schritt Online-Anschlüsse an eine Datei in der Größe des AZR geschaltet werden, ohne daß der Gesetzgeber und die im Rahmen eines Gesetzgebungsverfahrens informierte Öffentlichkeit hiervon wissen. Davon abgesehen habe ich bei mehreren der bereits angeschlossenen Behörden Bedenken hinsichtlich der Erforderlichkeit eines Online-Anschlusses.

Die Einzelheiten meiner Feststellungen habe ich dem Bundesminister des Innern unter dem 7. November 1980 in einem längeren Prüfbericht mitgeteilt. Eine inhaltliche Stellungnahme hierzu ist mir bislang noch nicht zugegangen. Der BMI hat aber aufgrund meines Berichts eine Arbeitsgruppe gebildet, die ein Konzept für die Neuordnung des AZR unter Berücksichtigung meiner Anregungen erarbeiten soll.

Ich bin jedoch der Auffassung, daß man unabhängig davon sofort versuchen muß, die bestehenden Verbindungen auf das sachlich unerläßliche Mindestmaß zu reduzieren. In einem Bereich konnte ich dies im Einvernehmen mit der betreffenden Sicherheitsbehörde bereits durchsetzen. Die Arbeit an der Neukonzeption, die verständlicherweise nicht in kurzer Zeit abgeschlossen sein kann, darf nicht dazu führen, daß die Beendigung des gegenwärtigen, rechtlich äußerst bedenklichen Zustandes verzögert wird.

### 2.20 Wehrermittlungsliste des Bundesverwaltungsamtes

Das Bundesverwaltungsamt führt eine sogenannte Wehrermittlungsliste. Sie dient dem Zweck, den Aufenthalt von Wehrpflichtigen festzustellen. In der Liste werden ausgeschrieben:

— Auf Antrag der Erfassungsbehörden (Meldebehörden) Personen, die sich der Erfassung als Wehrpflichtige entziehen oder die die Meldepflicht nach der Erfassung nicht erfüllen,

— auf Antrag der Kreiswehrersatzämter Personen, die sich der Wehrüberwachung entziehen,

— auf Antrag des Bundesamtes für den Zivildienst Personen, die sich der Zivildienstüberwachung entziehen.

Die Listen werden u. a. den Grenzkontrollstellen zugeleitet. In einem mir bekanntgewordenen Fall ist ein Wehrpflichtiger beim Grenzübertritt einer intensiven Kontrolle unterworfen worden, nur weil sich sein Name auf der Liste befand. Die Ausschreibung führt mithin zu einer Art polizeilicher Beobachtung im Wehrersatzwesen. Diese Form der Wehrüberwachung ist datenschutzrechtlich im Prinzip nicht zu beanstanden; zu fordern ist aber, daß der Betroffene darüber informiert wird. Das geschieht jedoch nicht. Die Tatsache der Ausschreibung wird dem Gesuchten nicht bekanntgegeben, damit er den soeben festgestellten Aufenthaltsort nicht vorzeitig wieder wechselt. Ich halte dieses Vorgehen für bedenklich und habe angeregt, die Wehrpflichtigen auf die Ausschreibung in der Wehrermittlungsliste hinzuweisen, weil mir so am ehesten gewährleistet scheint, daß sie ihren Obliegenheiten nach dem Wehrpflichtgesetz nachkommen. Der Bundesminister des Innern hat sich dieser Anregung gegenüber aufgeschlossen gezeigt. Er wird den ebenfalls an dem Ermittlungsverfahren beteiligten Bundesressorts vorschlagen, auf die bisher geübte Geheimhaltung zu verzichten.

### 2.21 Übermittlung von Gesundheitsdaten durch Bundeswehrdienststellen

In mehreren Eingaben haben sich ehemalige Soldaten, denen die Sonderfahrerlaubnis durch die Bundeswehr entzogen worden war, darüber beschwert, daß der zivilen Straßenverkehrsbehörde, die von der Entziehung unterrichtet worden war, auf Anforderung die zugrundeliegenden medizinischen Gutachten oder Stellungnahmen vom Sanitäts- und Gesundheitsdienst der Bundeswehr übersandt worden waren. Die Straßenverkehrsbehörde kann aus dem Vordruck, mit dem die Entziehung der Fahrerlaubnis mitgeteilt wird, entnehmen, ob dafür z. B. körperliche Mängel maßgebend waren. Sie kann dies zum Anlaß nehmen zu prüfen, ob auch die zivile Fahrerlaubnis entzogen werden muß. Nach § 15b Abs. 2 der Straßenverkehrs-Zulassungs-Ordnung kann sie bei Zweifeln an der Eignung zum Führen eines Kraftfahrzeugs vom Betroffenen ein amts- oder fachärztliches Zeugnis oder ein Gutachten einer amtlich anerkannten medizinisch-psychologischen Untersuchungsstelle, eines amtlich anerkannten Sachverständigen oder eines Prüfers für den Kraftfahrzeugverkehr verlangen. Der Betroffene muß sich also Gutachten oder Zeugnisse beschaffen und sie der Straßenverkehrsbehörde vorlegen. Die Straßenverkehrsbehörde darf derartige Zeugnisse und Gutachten jedoch nicht anfordern, und die Stellen, die solche Unterlagen besitzen, dürfen diese nicht übermitteln, ohne daß der Betroffene zugestimmt und die Ärzte von der Schweigepflicht entbunden hat.

Aufgrund meiner Hinweise hat der Bundesminister der Verteidigung die für die Entziehung militärischer Fahrerlaubnisse zuständigen Dienststellen und den Sanitäts- und Gesundheitsdienst angewiesen, Gutachten oder gutachtliche Stellungnahmen — insbesondere medizinischen Charakters — nur noch mit Zustimmung des Betroffenen an Straßenverkehrsbehörden weiterzugeben.

## 3. Übergreifende Feststellungen aus verschiedenen Verwaltungsbereichen

Die folgenden Ausführungen können nicht einem bestimmten Verwaltungsbereich allein zugeordnet werden (auch wenn die zugrundeliegenden Erkenntnisse nur in einem Bereich gewonnen wurden). Es handelt sich um Querschnittsthemen, die sich auch in sonst nicht verwandten Ressorts ähnlich stellen.

### 3.1 Allgemeine Erfahrungen aus Prüfungen

#### 3.1.1 Unzulässige Datenverarbeitung

Bei den im Berichtsjahr durchgeführten Prüfungen wurde nicht festgestellt, daß vorsätzlich personenbezogene Daten unzulässig verarbeitet wurden. Es gab jedoch eine erhebliche Anzahl von Fällen, in denen Behörden unzulässige Verarbeitungen für zulässig hielten und durchführten. Darüber ist in dem jeweiligen Sachzusammenhang berichtet.

Abgesehen davon kam es gelegentlich vor, daß personenbezogene Daten länger als erforderlich gespeichert wurden. So bewahrte z. B. eine Stelle die Magnetbänder, mit denen neue Daten in eine Bestandsdatei eingespielt worden waren, vorsichtshalber noch auf, auch wenn die Daten aus dem Bestand schon längst wieder gelöscht waren.

Im Rahmen der von mir angeregten Neuregelung wurde entsprechend dem tatsächlichen Sicherungsbedarf eine Aufbewahrungszeit von drei Monaten als angemessen erkannt und damit der Archivbestand an Magnetbändern erheblich vermindert. In anderen Fällen gab es für Belegsammlungen mit personenbezogenen Daten lediglich Mindestaufbewahrungsfristen und es kam vor, daß je nach dem vorhandenen Lagerraum diese Fristen erheblich überschritten wurden.

#### 3.1.2 Übersicht über die gespeicherten Daten

Die Ergebnisse der durchgeführten Kontrollen lassen vermuten, daß es noch immer eine bedeutende Anzahl von Stellen der Bundesverwaltung gibt, in denen die für den Datenschutz Verantwortlichen keine Übersicht über die Datenverarbeitung in ihrem Verantwortungsbereich haben. Wenn die ge-

mäß § 15 BDSG zu führende Übersicht lediglich aus einer Sammlung der Meldungen zur Veröffentlichung gem. § 12 BDSG oder zum Register gem. § 19 Abs. 4 BDSG besteht, kann die Ausführung der Datenschutzbestimmungen schon deswegen nicht gewährleistet werden, weil den Verantwortlichen nicht bekannt ist,

— an welchen Arbeitsplätzen und in welcher Form personenbezogene Daten vorliegen,

— wie die entsprechenden Datenträger behandelt, insbesondere geschützt werden und

— wo sie schließlich verbleiben, wenn sie nicht mehr benötigt werden (z. B. wie wird archiviert oder gelöscht).

Die für eine umfassende Übersicht notwendigen Informationen lagen zwar häufig vor, sie waren jedoch manchmal nicht zusammengeführt und daraufhin überprüft worden, ob die datenschutzgerechte Behandlung aller personenbezogener Daten gewährleistet ist. In diesen Fällen zeigten sich dann auch regelmäßig Schwachstellen bei der Sicherung der Daten gegen unbefugtes Entfernen und oft Unvollständigkeiten bei den Regelungen über die Archivierung bzw. die Vernichtung von Unterlagen mit personenbezogenen Daten.

#### 3.1.3 Maßnahmen zur Verbesserung der Datensicherung

Die Diskussion der Prüfungsergebnisse mit den kontrollierten Stellen ergab häufig, daß Probleme, nachdem sie erkannt waren, ohne oder mit geringem Aufwand gelöst werden konnten. Dies gilt besonders für die vor und nach der automatisierten Verarbeitung liegenden Verfahrensteile und das dabei bearbeitete Material. Aber auch in den Bereichen Rechenzentrum und Datenträgerarchiv bestehen im Rahmen der ohnehin gelegentlich erforderlichen Umgestaltungen kostengünstige Möglichkeiten, die Datensicherung zu verbessern, wenn diese Aspekte rechtzeitig in die Planung eingebracht werden. Diese Erfahrung paßt zu der Erkenntnis einiger Stellen wie z. B. der Deutschen Bundesbank, die sich frühzeitig bemüht haben, den Datenschutz bei allen Arbeitsabläufen zu berücksichtigen: auf Kostenprobleme von Bedeutung sind sie dabei nicht gestoßen. Schwierigkeiten bei der Behebung von Sicherheitsmängeln gibt es dagegen regelmäßig dann, wenn die äußere Gebäudesicherung nur schwach ist oder wenn eine Abgrenzung von Sicherheitsbereichen im Inneren eines Gebäudes angemessen wäre, aber nur durch umfangreiche und damit teure Umbauten realisiert werden kann. Nur in einem Fall war jedoch die Gebäudesicherung im Verhältnis zur Schutzbedürftigkeit der Daten so mangelhaft, daß ich deswegen eine Beanstandung aussprechen mußte.

#### 3.1.4 Beauftragung von Dienstleistungsunternehmen

Gelegentlich werden einzelne Bearbeitungsschritte wie z. B. Datenerfassung, Micro-Verfilmung oder Vernichtung von Unterlagen nicht durch die Behörden selbst, sondern von entsprechend spezialisierten Unternehmen durchgeführt, manchmal wird auch fremde ADV-Kapazität genutzt. In diesen Fällen muß der Auftraggeber sich davon überzeugen, daß der Auftragnehmer angemessene Maßnahmen zur Gewährleistung des Datenschutzes auch in dieser Phase der Verfahren durchführt.

Ich habe darauf hingewiesen, daß die vertraglichen Vereinbarungen auch Regelungen zur Datensicherung enthalten müssen und daß es durchaus angemessen sein kann, daß die Behörde sich z. B. durch Stichproben von deren Einhaltung überzeugt.

Ein Fall mangelhafter Vernichtung von Unterlagen, in dem offenblieb, ob damit auch vom BDSG geschützte Belange von Betroffenen gefährdet wurden, machte deutlich, daß vertragliche Zusicherungen des Auftragnehmers auch ohne Täuschungsabsicht dem Auftraggeber einen völlig falschen Eindruck vermitteln und damit erhebliche Sicherheitsmängel verbergen können. Ich werde in Zukunft verstärkt darauf hinwirken, daß die Bundesbehörden sich von der ordnungsgemäßen Ausführung zugesicherter Maßnahmen überzeugen.

Wichtig scheint mir auch zu sein, daß schon der Auftrag selbst hinreichend eingegrenzt wird und Festlegungen darüber treffen sollte, was mit den dem Auftraggeber übergebenen Unterlagen zu geschehen hat. So wurden im Berichtszeitraum Anschriften aus einer Adressendatei eines Bundesministeriums durch eine Firma, die mit dem Versand einer Publikation des Ministerium beauftragt war, an eine andere Firma zu Werbezwecken weitergegeben. Für diese Datenübermittlung lag weder eine Zustimmung der Betroffenen noch eine Weisung des Auftraggebers vor. Das Ministerium hat daraufhin zu Recht die Geschäftsbeziehungen zu der beauftragten Firma abgebrochen. Außerdem habe ich die Aufsichtsbehörde, die die Einhaltung der Datenschutzbestimmungen durch die beauftragte Firma zu überwachen hat, von dem Vorfall unterrichtet. Da nach § 8 Abs. 1 BDSG bei jeder Datenverarbeitung der Auftragnehmer sorgfältig auszuwählen ist, sollte sich jeder, der eine andere Stelle mit Datenverarbeitungsmaßnahmen beauftragen will, bei den zuständigen Aufsichtsbehörden erkundigen, ob gegen die Beauftragung der jeweiligen Firma im Einzelfall Bedenken bestehen. Auf diese Weise können ungeeignete Firmen ferngehalten und die Auftragnehmer zu einem gesetzmäßigen Verhalten motiviert werden.

#### 3.1.5 Konsequenzen für die Kontrolltätigkeit

Die angemessene Sicherung der Daten ist im wesentlichen eine Organisationsaufgabe, die zwar von vielen Bundesbehörden im erforderlichen Umfang wahrgenommen wird, aber durchaus noch nicht von allen. Um trotz meiner beschränkten Mittel die Breitenwirkung in diesem Bereich zu erhöhen, habe ich damit begonnen, Kontroll- und Beratungsbesuche durchzuführen, die sich auf die technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes konzentrieren. Für diese Besuche wurden Behörden ausgewählt, in denen keine besonderen Rechtsprobleme erwartet wurden, in denen ich aber andererseits wegen der Größe der Behörde oder wegen des Umfangs der Datenverarbeitung einen Einblick in die Organisation des Daten-

schutzes gewinnen wollte, um festzustellen, ob die Dokumentation der Datenverarbeitung und die Regelungen für den Umgang mit personenbezogenen Daten darauf schließen lassen, daß die angemessenen Maßnahmen gegen unbefugte Datennutzung getroffen sind. Erste Erfahrungen mit diesem Vorgehen veranlassen mich, auf Datensicherung konzentrierte Teilprüfungen auch im kommenden Jahr durchzuführen.

### 3.2 Personalwesen

#### 3.2.1 Beschaffung von Anschriften für Selbsthilfeeinrichtungen und Berufsverbände des öffentlichen Dienstes

a) Wiederholt haben mich Eingaben von Bürgern erreicht, die sich mit der Frage der Übermittlung von Anschriften durch Behördenbedienstete (Vertrauensleute) an Selbsthilfeeinrichtungen der Beamten befassen.

Die gemäß § 66 Abs. 1 Ziff. 4 BBG genehmigungsfreie Nebentätigkeit von Beamten in Selbsthilfeeinrichtungen läßt die dienstliche Verantwortlichkeit unberührt (§ 66 Abs. 2, 1. Halbsatz BBG). Der Beamte, der diese genehmigungsfreie Nebentätigkeit ausüben will, hat somit zu prüfen, ob die Ausübung der Nebentätigkeit mit seinen Beamtenpflichten vereinbar ist. Diese Selbstprüfung durch den Beamten wird negativ ausfallen müssen, wenn die Nebentätigkeit aus der Übermittlung von personenbezogenen Daten an Selbsthilfeeinrichtungen besteht *und* der Beamte eine Funktion innehat, in der ihm diese Daten als besonderes Amtsgeheimnis anvertraut und zugänglich sind. Hier muß schon der Anschein mißbräuchlicher Verwendung von Personaldaten vermieden werden. Eine Übermittlung personenbezogener Daten wäre für den das Personalaktengeheimnis wahrenden Beamten nur mit ausdrücklicher Zustimmung des Betroffenen im Einzelfall zulässig.

Es ist Pflicht des Dienstvorgesetzten, Mißbräuchen entgegenzutreten (§ 66 Abs. 2, 2. Halbsatz BBG). Ein Mißbrauch ist anzunehmen, wenn der Beamte bei Ausübung einer genehmigungsfreien Nebentätigkeit seine dienstlichen Pflichten verletzt oder wenn deren Verletzung nach den Umständen des Falles in absehbarer Zeit in hohem Maße wahrscheinlich ist, z. B. weil bei Ausübung der Nebentätigkeit eine Verletzung dienstlicher Pflichten unvermeidbar ist (vgl. BVerwGE 40, 11, 16). Auch wenn der im Personalwesen tätige Beamte die zu übermittelnden Anschriften Quellen entnehmen sollte, die für jedermann öffentlich zugänglich sind, könnte eine Übermittlung unzulässig sein, weil die übermittelten Daten gleichzeitig einem von ihm zu wahrenden besonderen Amtsgeheimnis unterliegen.

Die mir vorliegenden Eingaben zeigen, daß häufig ein in Personalverwaltungen Beschäftigter Anschriften, insbesondere von neu Eingestellten, an Selbsthilfeeinrichtungen weitergibt. Ich habe darauf hingewiesen, daß dies im Gegensatz zu § 66 Abs. 2 BBG stehen kann, und gebeten, darauf hinzuwirken, daß die Behörden ihre Beschäftigten auf die mögliche Unvereinbarkeit zwischen Nebentätigkeit und amtlicher Funktion aufmerksam machen. Das gilt nicht nur für Beamte, sondern auch für Angestellte des öffentlichen Dienstes und — allerdings wohl in seltenen Fällen — auch für Arbeiter.

Ich habe die obersten Bundesbehörden in einem Rundschreiben auf die Probleme hingewiesen. Der Bundesminister der Finanzen hat bereits seinen nachgeordneten Bereich entsprechend unterrichtet.

b) Der Bundesminister des Innern ist mit der Frage an mich herangetreten, ob die Fachhochschule des Bundes dem Deutschen Beamtenbund oder einer anderen Gewerkschaft Namenslisten der jeweiligen Studienanfänger zur Intensivierung und Effektivierung von Werbe- und Betreuungsmaßnahmen geben darf.

Die Übermittlung von personenbezogenen Daten im Anwendungsbereich des BDSG ist zulässig, wenn sie mit Einwilligung des Betroffenen erfolgt (§ 3 Satz 1 Nr. 2 BDSG). Es wäre daher der einfachste Weg, wenn die Fachhochschule sich zur Übermittlung der Namen die Einwilligung der Studienanfänger einholte.

Ob auch eine Übermittlung auf der Grundlage des § 3 Abs. 1 Nr. 1 BDSG (normative Grundlage) zulässig ist, läßt sich schwer abstrakt beantworten. Gemäß § 24 Abs. 1 BDSG wären vorher das berechtigte Interesse der übermittelnden Stelle, also der Fachhochschule, oder eines Dritten, hier des Deutschen Beamtenbundes, sowie die Beeinträchtigung schutzwürdiger Belange des Betroffenen, des Studienanfängers, zu prüfen.

Das kann in der Regel am sichersten durch Befragung der Betroffenen geschehen; dann aber kann auch gleich eine Einwilligung eingeholt werden.

Falls die Fachhochschule gegenüber den Studienanfängern personalverwaltende Aufgaben wahrnimmt, unterlägen die diesbezüglichen personenbezogenen Daten möglicherweise den Regeln über die Wahrung des Personalaktengeheimnisses. Diese Regeln gehen gegebenenfalls gemäß § 45 BDSG — als bereichsspezifische Vorschriften — dem BDSG vor.

#### 3.2.2 Angaben in Hausmitteilungen

Aufgrund einer Eingabe aus dem Bereich einer Standortverwaltung der Bundeswehr habe ich mich mit der Bekanntgabe von Personaldaten in Verwaltungsanordnungen, Hausmitteilungen und auf Personalversammlungen befaßt. Verwaltungsanordnungen, Hausmitteilungen oder ähnliche Mitteilungen dienen der Bekanntgabe von organisatorischen und Personalveränderungen innerhalb einer Behörde/eines Organisationsbereiches. Sie werden regelmäßig auch nur innerhalb dieser Behörde/dieses Organisationsbereiches verteilt. Für die Bekanntgabe liegt sowohl ein dienstliches als auch ein Interesse der Beschäftigten vor. Das dienstliche Interesse be-

steht insbesondere darin, den Mitarbeitern personelle und organisatorische Veränderungen bekanntzugeben, die bei der laufenden Sachbearbeitung berücksichtigt werden müssen, z. B. Aufgabenverschiebungen zwischen einzelnen Organisationseinheiten. Das persönliche Interesse der Beschäftigten liegt u. a. in der Transparenz der Personalpolitik einer Behörde. Deshalb habe ich mich nicht grundsätzlich für die Abschaffung solcher Mitteilungen ausgesprochen. Ich habe aber erreicht, daß die Gründe für Umsetzungen, Versetzungen, vorzeitiges Ausscheiden aus dem Dienst sowie für Namensänderungen nicht mehr veröffentlicht werden. In keinem Falle dürfen schutzwürdige Belange der Beschäftigten beeinträchtigt werden. Dies gilt auch bei der Bekanntgabe von personenbezogenen Daten in Personalversammlungen.

#### 3.2.3 Benennung der in Kommunalvertretungskörperschaften tätigen Angehörigen einer Verwaltungseinheit

Der Landesbezirk einer Gewerkschaft teilte mir mit, daß eine Grenzschutzverwaltungsstelle unter Berufung auf einen Erlaß des Bundesministers des Innern von den Leitern der nachgeordneten Verwaltungsstellen die Benennung derjenigen Bundesgrenzschutz-Angehörigen fordert, die in kommunalen Vertretungskörperschaften tätig sind. Eine Rückfrage beim Bundesminister des Innern ergab, daß dieser für den Tätigkeitsbericht des Bundesgrenzschutzes lediglich die *Zahl* der in kommunalen Vertretungskörperschaften tätigen BGS-Angehörigen erbat. Um weitere Mißverständnisse auszuschließen, hat der Bundesminister des Innern seinen Erlaß dahin gehend geändert, daß auch Erhebungen über die Zahl der in kommunalen Vertretungskörperschaften tätigen BGS-Angehörigen künftig entfallen.

#### 3.2.4 Beihilfewesen

Im vergangenen Jahr habe ich mich in mehreren Fällen mit Fragen des Beihilfewesens des Bundes auseinandergesetzt. Erwähnen möchte ich hier lediglich zwei Probleme, nämlich

a) die Vorlage des ärztlichen Schlußberichts nach Sanatoriumsaufenthalt oder Heilkur bei der Beihilfestelle und

b) die Abschottung der Beihilfestelle von der übrigen Personalverwaltung.

Zu a):

Gemäß Nr. 6 Abs. 1 und Nr. 7 Abs. 4 Ziff. 1 Beihilfevorschriften des Bundes (BhV) sind die Kosten für einen ärztlichen Schlußbericht beihilfefähig. Die Vorlage des ärztlichen Schlußberichts wird nach Abschluß eines Sanatoriumsaufenthaltes oder einer Kur von der Beihilfestelle gefordert. Sie will an Hand dieser Unterlagen feststellen, ob der Beschäftigte die ärztlichen Verordnungen befolgt und seinen Teil dazu beigetragen hat, daß die seitens der Beihilfestelle bewilligte Maßnahme auch ordnungsgemäß durchgeführt worden ist. Inhaltlich fällt der ärztliche Schlußbericht in der Praxis sehr unterschiedlich aus. Er kann den vollständigen Behandlungsplan für einen Kurverlauf wiedergeben, d. h. alle während der Kur getroffenen Verordnungen und verabreichten Anwendungen, er kann darüber hinaus personenbezogene Daten enthalten, z. B. Diagnosedaten, die teilweise sehr sensibel sein können; er kann schließlich so inhaltsarm sein, daß er nicht einmal für den Zweck der Abrechnung der Beihilfe ausreicht, so daß Rückfragen erforderlich werden.

Ich erkenne an, daß die Beihilfestelle für die Kontrolle der Abrechnung Informationen benötigt, aus denen hervorgeht, ob die abgerechneten Leistungen mit den getroffenen Verordnungen (z. B. des Kurarztes) übereinstimmen. Soweit der ärztliche Schlußbericht darüber hinausgehende Informationen gibt, sind diese für die Beihilfestelle aber nicht erforderlich. Hält der Sanatoriums- oder Kurzarzt Hinweise für die weitere Behandlung für erforderlich, so sind diese dem behandelnden Arzt am Wohnort des Beschäftigten und eventuell mit dessen Zustimmung dem Personalarzt in einem „Arztbrief" mitzuteilen. Der ärztliche Schlußbericht im Sinne des Beihilfewesens muß also dahin gehend konkretisiert werden, daß er nur eine Zusammenstellung der ärztlichen Verordnungen und durchgeführten Anwendungen enthält und bescheinigt, daß z. B. die Kur entsprechend den Verordnungen des Kurarztes in der vorgesehenen Zeit abgewickelt wurde.

Der Bundesminister des Innern hat nach Beratung dieses Problems in der Bund-Länder-Kommission für das Beihilferecht vorgesehen, diese Einschränkung den Bundesverwaltungen bekanntzugeben.

Zu b):

Wiederholt haben mich Eingaben erreicht, in denen Beschäftigte des öffentlichen Dienstes ihre Sorge vortragen, daß die im Rahmen der Beihilfegewährung ihrem Dienstherrn offenbarten Gesundheitsdaten (z. B. Diagnosen, Zeitraum der Behandlung, Anwendungen) nicht nur der Abrechnung und Gewährung von Beihilfen zugrundegelegt werden, sondern auch Einfluß auf Personalentscheidungen haben. Diese Befürchtung tritt vor allem dort auf, wo die Beihilfeabrechnung und die sonstige Personalbearbeitung in einer Hand liegen.

Auszugehen ist von dem schon in meinem ersten Tätigkeitsbericht (unter 3.5.4.2, S. 36) festgestellten Grundsatz, daß jeder zum Arzt, ins Krankenhaus oder zu einer Sozialbehörde gehen können soll, ohne befürchten zu müssen, daß diese Tatsache Außenstehenden bekannt wird oder daß ihm daraus Nachteile entstehen. Diese für den Anwendungsbereich des Sozialgeheimnisses getroffene Aussage gilt auch in Bereichen wie dem Beihilfewesen, bei dem die Interessenlage gleich ist: Der Beihilfeberechtigte darf durch die Art der Organisation des Beihilfewesens weder davon abgehalten werden, zum Arzt zu gehen, noch davon, entstandene Rechnungen zur Beihilfegewährung einzureichen. Daraus folgt, daß gewährleistet werden muß, daß die Beihilfestelle von der Personalverwaltung im übrigen abgeschottet ist, wie das in einigen Verwaltungen schon gegenwärtig der Fall ist.

Diese Forderung wird durch die Hilfserwägung gestützt, daß die Funktion der Beihilfestelle derjenigen einer Betriebskrankenkasse vergleichbar ist.

Diese Krankenkasse unterliegt als Körperschaft des öffentlichen Rechts der Verpflichtung aus § 35 SGB I und darf unter das Sozialgeheimnis fallende Daten ihrer Versicherten nur gemäß § 35 Abs. 2 SGB I offenbaren; es ist kein Grund ersichtlich, weshalb der darin zum Ausdruck kommende Grundsatz, daß Daten, die im Zusammenhang mit der Gewährung von Sozialleistungen nach dem SGB (§ 21 SGB I) erhoben und verarbeitet werden, vor dem Arbeitgeber als Sozialgeheimnis zu wahren sind, nicht auf das Beihilfewesen übertragen werden kann. Denn auch bei Beihilfen handelt es sich im weiteren Sinne um eine „Sozialleistung" des Dienstherrn/Arbeitgebers für seine Beschäftigten.

§ 5 Abs. 1 BDSG, der wegen seiner Beschränkung auf die Datenverarbeitung in Dateien für das Beihilfewesen nicht in allen Fällen unmittelbar gilt, enthält den allgemeinen Grundsatz der Zweckbindung, dessen entsprechende Anwendung aus den genannten Gründen auf „Beihilfedaten" geboten sein dürfte.

Schließlich verlangt auch die beamten- und arbeitsrechtliche Fürsorgepflicht des Dienstherrn bzw. Arbeitgebers eine Organisation des Beihilfeabrechnungswesens, die den Beschäftigten nicht aus Angst davor, daß seine Beihilfedaten an dafür nicht zuständige Mitarbeiter des Dienstherrn/Arbeitgebers gelangen, daran hindert, von den ihm zustehenden Beihilfeleistungen Gebrauch zu machen. Gerade bei psychiatrischen Behandlungen ist dies ein in Eingaben immer wieder vorgebrachter Gesichtspunkt.

Auf der Grundlage dieser Erwägungen habe ich den Bundesminister des Innern um Stellungnahme gebeten und eine Änderung des Personalaktenführungserlasses vom 21. Juli 1966 — 22-001-002/1 — dahin gehend vorgeschlagen, daß die Beihilfeakte von den übrigen Personalakten getrennt aufzubewahren und vor dem Zugriff der Mitarbeiter außerhalb der Beihilfestelle zu schützen ist. Das Interesse des Dienstherrn/Arbeitgebers, von Umständen unterrichtet zu sein, die die Dienstfähigkeit des Beschäftigten betreffen, wird durch diesen Vorschlag nicht beeinträchtigt. Denn der Dienstherr/Arbeitgeber erfährt ja auch weiterhin durch die Arbeitsunfähigkeitsbescheinigung von der Tatsache längerer Erkrankungen und kann diese dann zum Gegenstand von Gesprächen mit dem betroffenen Beschäftigten machen.

### 3.3 Telefondaten

Die Diskussion über die Frage, inwieweit Angaben über Telefongespräche, vor allem die angerufene Nummer, aufgezeichnet werden dürfen (vgl. 3. TB zu 3.5.5.3, S. 28 f.), ist im Berichtsjahr weitergegangen. Bei verschiedenen Prüfungen in der Bundesverwaltung habe ich festgestellt, daß sowohl dienstliche wie private Ferngespräche mit den Zielnummern registriert werden. Die Abrechnung der privaten Telefongespräche ist vielfach so organisiert, daß der Beschäftigte eine detaillierte Rechnung erhält, während ein zweiter Beleg für die Dienststelle selbst nur in Form einer Summenliste (mit Anzahl der Gebühreneinheiten und Gesprächskosten) oder — wenn Einzelbelege bei der Zahlstelle verbleiben — ohne die Daten über Ort und Rufnummer des Gesprächspartners aufbewahrt wird. Die Aufzeichnung der Zielnummern bei dienstlicher Benutzung der Fernsprecheinrichtungen ist in Nr. 9 der Dienstanschlußvorschriften — DAV — des Bundesministers der Finanzen vom 1. Juni 1976 (Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung mit Ausnahme der Deutschen Bundespost, Ministerialblatt des Bundesministers der Finanzen und des Bundesministers für Wirtschaft 1976, S. 487) vorgeschrieben.

Ich habe gegenüber dem Bundesminister der Finanzen und den übrigen betroffenen Bundesbehörden Bedenken gegen die Aufzeichnung der Zielnummern geltend gemacht. Diese Angabe wird als erforderlich bezeichnet, um prüfen zu können, ob Dienstgespräche in dem durchgeführten Umfang notwendig waren und ob es sich tatsächlich um Dienstgespräche gehandelt hat. Demgegenüber habe ich die bereits im 3. Tätigkeitsbericht (a. a. O.) skizzierte Ansicht vertreten, daß es für die haushaltsmäßige Kontrolle der Fernsprechmittel ausreichen dürfte, Datum, Nebenstellen-Nummer, Ziel*ort* sowie die Gebühreneinheiten nachzuweisen. Das personenbezogene Datum „Fernsprechnummer des Gesprächsteilnehmers" sollte nur im Zusammenhang mit der üblicherweise für die Akten anzufertigenden Telefonnotiz aufgezeichnet werden. Über diese Frage der Erforderlichkeit wird noch weiter zu verhandeln sein. Dabei sollte nach meiner Ansicht auch berücksichtigt werden, in welcher Weise solche Aufzeichnungen tatsächlich ausgewertet werden. Es spricht viel dafür, die Kontrolle, soweit sie für unverzichtbar gehalten wird, auf kostenrelevante (d. h. längere) Gespräche zu beschränken und nur stichprobenweise durchzuführen.

Abgesehen davon sprechen nach wie vor weitere Gründe gegen eine Aufzeichnung der Zielnummer. Die Sorge, daß durch Auswertung der Telefonkontakte eine unverhältnismäßige Kontrolle über die Beschäftigten ausgeübt werden könnte, ist nicht von der Hand zu weisen. Dies gilt insbesondere für telefonische Verbindungen zu Personalräten, Beschwerde- und Aufsichtsinstanzen sowie Bürgerbeauftragten (einschließlich meiner Dienststelle). Darüber hinaus sind weitere Fälle vorstellbar, in denen eine Offenlegung von (erlaubten) Telefonkontakten schutzwürdige Belange der Telefonierenden, vor allem auch des Angerufenen, beeinträchtigen würde, so etwa wenn bestimmten Informanten einer Behörde Vertraulichkeit zugesichert wurde oder wenn diese im Rahmen sozialer Hilfe und Beratung erwartet werden darf; man denke etwa an Stellen, die Gesundheits- oder Eheberatung betreiben.

Erst recht bestehen Bedenken gegen die Aufzeichnung der Zielnummern bei *privaten* Telefongesprächen von Dienstapparaten aus. Diese Aufzeichnungen sind gewiß für die eindeutige Abrechnung der Gebühren nützlich, vor allem wenn ein Anschluß von mehreren Personen für private Gespräche benutzt wird. Es bestehen aber erhebliche Zweifel, ob diese Aufzeichnungen in jedem Falle erforderlich

und rechtlich zulässig sind. In der vergleichbaren Frage, ob Hotels bei Telefongesprächen ihrer Gäste die Zielnummern aufzeichnen dürfen, vertreten die Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich die Ansicht, daß dies nicht zulässig sei. Auch mehrere Landesbeauftragte für den Datenschutz teilen die Ansicht, daß die Aufzeichnung der angerufenen Nummern bei Privatgesprächen von Behördenapparaten aus nicht zulässig sei. In diesem Zusammenhang wird auch auf das Fernmeldegeheimnis (Art. 10 GG) Bezug genommen.

Ich werde mich weiterhin mit den mir zustehenden Mitteln dafür einsetzen, daß solche Aufzeichnungen unterbleiben, die unangemessene Nachteile für die Betroffenen nach sich ziehen können. Ich werde besonders darauf achten, daß durch solche Notierungen nicht das Recht beeinträchtigt wird, sich unbeobachtet an Personalräte und andere Institutionen wenden zu können, die zum Schutze von Beschäftigten eingerichtet sind. Die Zweckbindung der gleichwohl aufgezeichneten Daten muß streng beachtet werden; eine Verknüpfung mit anderen Daten hat zu unterbleiben.

Auch vor endgültiger Klärung der grundsätzlichen Rechtsprobleme sollten praktische Lösungswege bedacht werden. So würde es einen Fortschritt darstellen, wenn die benutzten Verfahren der Aufzeichnung und Auswertung allgemein den Betroffenen bekanntgemacht würden; hierzu gehört auch ein zutreffender Hinweis auf die Rechtsgrundlage (§ 9 Abs. 2 BDSG) bzw. auf die Tatsache der Registrierung (vgl. § 26 Abs. 1 BDSG). Ferner sollte dafür gesorgt werden, daß alle aufgezeichneten Daten auf allen Datenträgern nach Ausdruck der zulässigen Listen und Abrechnungen gelöscht werden.

Ich appelliere auch an die Hersteller von Telefonaufzeichnungsgeräten, technische Lösungen zu entwikkeln, die den unterschiedlichen Anforderungen der Anwender Rechnung tragen und — wenn dies angemessen erscheint — dem Betroffenen die Wahl zwischen verschiedenen Aufzeichnungsarten (und entsprechenden Folgen für die Beweislage) lassen. Meines Wissens bemühen sich mehrere Unternehmen um solche Lösungen.

### 3.4 Bankauskünfte

Anläßlich einer Prüfung im Bereich der öffentlich-rechtlichen Banken habe ich mich mit der Problematik der sog. Bankauskunft auseinandergesetzt.

Mit „Bankauskunft" wird der Informationsaustausch zwischen Kreditinstituten über die Kreditwürdigkeit eines Kunden bezeichnet. Bankauskünfte dienen dazu, wirtschaftliche Risiken bei der Kreditvergabe zu mindern. Die Angabe des Kreditsuchenden über seine anderweitigen Bankverbindungen dient als Grundlage für die Anfrage bei dem betroffenen Kreditinstitut. Es handelt sich dabei um ein in der Branche vereinbartes Verfahren, bei dem die um Auskunft ersuchte Bank ihre Einschätzung der wirtschaftlichen, finanziellen und persönlichen Verhältnisse meist formularmäßig — in erster Linie durch Ankreuzen vorgegebener Beurteilungskriterien — abgibt. Bankauskünfte dienen nicht ausschließlich der anfragenden Bank als Grundlage für eigene Kreditentscheidungen, sondern können auch in Auskünfte an Kunden eingehen.

Die Datenübermittlung in Form der „Bankauskunft" stößt auf erhebliche datenschutzrechtliche Bedenken. Für die Zulässigkeit der Übermittlung durch die auskunftgebende Stelle ist nach § 24 Abs. 1 BDSG Voraussetzung, daß die Weitergabe im Rahmen des mit dem Kunden bestehenden Vertragsverhältnisses liegt (erste Alternative). Diese Voraussetzung ist in aller Regel nicht gegeben. Nach der zweiten Alternative der Vorschrift dürfen schutzwürdige Belange des Betroffenen nicht beeinträchtigt sein; auch dies wird man grundsätzlich nicht feststellen können, es sei denn, daß ausschließlich positive Angaben weitergegeben werden. Bei der Interessenabwägung nach der zweiten Alternative spielt insbesondere das Vertrauen des Kunden auf die Einhaltung des Bankgeheimnisses eine Rolle. Die Erteilung von „Bankauskünften" setzt deshalb in der Regel voraus, daß der Betroffene seine Einwilligung nach § 3 Abs. 1 Nr. 2 BDSG erteilt hat. Das überprüfte Institut verstößt also insoweit gegen das Bundesdatenschutzgesetz. Übrigens verfährt — soweit ersichtlich — die gesamte Kreditwirtschaft so (vgl. 2. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz Nordrhein-Westfalen S. 94 ff.).

Bedenken habe ich darüber hinaus gegen einige im Vordruck vorgesehene Beurteilungen erhoben, insbesondere soweit sie Persönlichkeitsbewertungen betreffen, wie z. B.: „Über Ruf und Charakter ist Nachteiliges nicht bekannt geworden"; „Der Kunde gilt als fleißig und vertrauenswürdig"; „Er erfreut sich eines guten Rufs"; „In persönlicher Hinsicht vermögen wir ein Urteil nicht abzugeben". Bei anderen Formulierungen bleibt offen, ob es sich um eigene Feststellungen der Bank handelt oder um Auskünfte Dritter, für deren Richtigkeit keine Gewähr übernommen wird. Dies gilt beispielsweise für: „Es wurden Wechselproteste beobachtet".

Eine förmliche Beanstandung habe ich zunächst zurückgestellt und die Bank um eine ausführliche Stellungnahme gebeten. Ich habe mich zu dieser Vorgehensweise entschlossen, weil die Erteilung von „Bankauskünften" ein in der Branche übliches Verfahren ist und es aus der Sicht des Datenschutzes darauf ankommt, ein mit der Kreditwirtschaft und den Datenschutzkontrollinstitutionen der Länder abgestimmtes Verfahren zu entwickeln. Dabei wird darauf hingewirkt werden müssen, daß — entsprechend den Ergebnissen der Verhandlungen mit den Handels- und Wirtschaftsauskunfteien — das Verfahren der Bankauskunft für den Betroffenen transparent wird, daß sich die Bankauskunft auf kreditrelevante und nachweisbare Tatsachen beschränkt und daß Werturteile nur weitergegeben werden, wenn ihnen erkennbar nachprüfbare Tatsachen zugrunde liegen und die Berechnungs- und Beurteilungsgrundlagen für Außenstehende überprüfbar sind.

### 3.5 Haushaltskontrolle von Zuwendungen

Im Wirtschaftsplan 1981 der pädagogischen Arbeitsstelle (PAS) des Deutschen Volkshochschulverban-

des war erstmals unter dem Titel 531 01 — Kosten für Veröffentlichungen und Dokumentation folgender Vermerk aufgenommen worden: „Ausgaben für Honorare dürfen nur geleistet werden, wenn der Honorarempfänger Angaben über sein hauptberufliches Beschäftigungsverhältnis gemacht und sein Einverständnis mit der Weitergabe dieser Angaben an den Zuwendungsgeber erklärt hat."

Durch diesen Vermerk bestand die Gefahr einer Beeinträchtigung von schutzwürdigen Belangen der betroffenen Honorarempfänger. Diese mußten befürchten, daß ihr Dienstherr bzw. Arbeitgeber Kenntnis von einer Nebentätigkeit erhalten könnte, und zwar unabhängig davon, ob diese anzeigefrei, anzeigepflichtig oder genehmigungspflichtig ist.

Der Vermerk geht auf einen Beschluß des Haushaltsausschusses des Deutschen Bundestages vom 16. November 1978 zurück. Auf diese Weise sollte ein Überblick darüber geschaffen werden, welche Geldbeträge in Form von Honoraren und Kostenersatz für Angehörige des öffentlichen Dienstes, insbesondere für Hochschullehrer ausgegeben werden.

Meinem Wunsch entsprechend hat der Bundesminister der Finanzen jetzt sichergestellt, daß dem Zuwendungsgeber nur noch die Zahl der Honorarzahlungen an Angehörige des öffentlichen Dienstes mit Angabe der Höhe und nicht Name und Anschrift der Honorarempfänger mitzuteilen ist und daß die Honorarempfänger selbst auch nur noch angeben müssen, ob sie im öffentlichen Dienst beschäftigt sind. Die vom Haushaltsausschuß des Deutschen Bundestages gewünschte (statistische) Information wird dadurch nicht geschmälert, die Datenschutzbedenken sind aber ausgeräumt.

#### 3.6 Verteiler für Informationsmaterial

Viele Stellen der Bundesverwaltung verteilen an Interessenten auf Anfrage Informationsmaterial über Themen aller Art aus Politik, Wirtschaft, Kultur, Wissenschaft und Technik. Bezieher solcher Publikationen fragen gelegentlich, was mit ihren Anschriften geschieht. Nach meinen bisherigen Erfahrungen werden die Anschriften in aller Regel nur vorübergehend aufbewahrt und dann vernichtet.

Bei der datenschutzrechtlichen Prüfung einer Stelle, die in besonders großem Umfang politisches Informationsmaterial versendet, haben meine Mitarbeiter sich vorrangig über die Behandlung der Namen und Anschriften von Interessenten informiert. Es muß sichergestellt sein, daß aus den Angaben über die jeweiligen Interessengebiete keine Persönlichkeitsprofile angefertigt werden und daß diese Angaben nicht zum Zwecke politischer Manipulation oder zur Überwachung politisch Andersdenkender genutzt werden. Tatsächlich besteht diese Gefahr nicht. Meine Mitarbeiter konnten sich davon überzeugen, daß bei Einzelanfragen diese Daten nicht gespeichert werden. Im Rahmen der Anfragen entstehende Unterlagen werden nach einem halben Jahr vernichtet.

## 4 Umsetzung des Datenschutzes in bereichsspezifische Regelungen und Weiterentwicklung des Datenschutzrechts

Zur Verwirklichung und Weiterentwicklung des Datenschutzes sind zahlreiche Rechts- und Verwaltungsvorschriften nötig, die das BDSG konkretisieren und ergänzen, insbesondere bereichsspezifische Gesetzesnormen und Verwaltungsvorschriften (Richtlinien). Im folgenden Abschnitt sind diese Entwicklungen in verschiedenen Verwaltungsbereichen dargestellt, soweit sie nicht wegen des unmittelbaren Zusammenhangs mit Prüfungsfeststellungen bereits in Abschnitt 2 oder 3 erwähnt wurden.

### 4.1 Rechtswesen

#### 4.1.1 Mitteilungen in Strafsachen

Die Justizminister des Bundes und der Länder haben die Anregungen, die meine Kollegen und ich zur Verbesserung des Datenschutzes gemacht haben (vgl. dazu 2. TB, Nr. 2.2.2, S. 16, 3. TB, Nr. 3.2.2, S. 19) aufgegriffen. Grundsätzlich halten auch sie es für geboten, für diese Mitteilungspflichten eine Rechtsgrundlage zu schaffen. Erwogen wird, den Bundesminister der Justiz zum Erlaß einer Rechtsverordnung mit Zustimmung des Bundesrats zu ermächtigen. Darüber hinaus anerkennen die Justizminister, daß es angebracht sei, den Umfang der Mitteilungspflichten mit dem Ziel einer generellen Reduzierung zu überprüfen. Im Benehmen mit den jeweiligen Empfängerbehörden soll geklärt werden, inwieweit es aus heutiger Sicht vertretbar erscheint, die jeweils widerstreitenden Interessen der Allgemeinheit und des Betroffenen unabhängig vom konkreten Einzelfall anders als bisher zu bewerten, so daß bestimmte Mitteilungspflichten entfallen oder inhaltlich reduziert werden können. Ich begrüße dieses Zwischenergebnis ausdrücklich. Über den Fortgang und den Abschluß werde ich berichten.

#### 4.1.2 Entwurf eines Gesetzes über die internationale Rechtshilfe in Strafsachen

Dem Deutschen Bundestag liegt der Entwurf eines Gesetzes über die internationale Rechtshilfe in Strafsachen (IRG) vor. Der Rechtshilfeverkehr zwischen deutschen und ausländischen Stellen ist datenschutzrechtlich besonders relevant, wenn Auskünfte aus dem Bundeszentralregister erteilt werden sollen. Die Zentralregisterauskunft enthält personenbezogene Daten von hohem Sensibilitätsgrad. In zahlreichen Datenschutzgesetzen anderer Staaten zählen Angaben über Vorstrafen zu den beson-

ders geschützten Daten. Im Bundesdatenschutzgesetz waren spezielle Regelungen über den Schutz dieser Daten nicht erforderlich, weil mit dem Gesetz über das Bundeszentralregister ein bereichsspezifisches Datenschutzgesetz geschaffen wurde, das den schutzwürdigen Belangen des Betroffenen Rechnung trägt. Die im Bundeszentralregistergesetz vorgesehenen Tilgungsfristen und das Verwertungsverbot geben dem Verurteilten die Möglichkeit, sich von den Belastungen seiner Vergangenheit zu befreien und sich wieder in die Gesellschaft einzugliedern. Seine Schutzfunktion kann das Bundeszentralregistergesetz freilich nur in seinem Geltungsbereich entfalten. Erfährt eine ausländische Stelle von einer Verurteilung, kann sie diese dem Betroffenen praktisch Zeit seines Lebens vorhalten und zu seinem Nachteil verwenden. Diese Tatsachen müssen bei einer Regelung der sog. „kleinen Rechtshilfe" nach §§ 58 ff. des Entwurfs berücksichtigt werden.

Problematisch erscheint in diesem Zusammenhang § 58 Abs. 3 des Entwurfs, der die Rechtshilfe unter den gleichen Voraussetzungen ermöglicht, unter denen deutsche Gerichte oder Behörden einander in entsprechenden Fällen Rechtshilfe leisten könnten. Hier werden unterschiedliche Sachverhalte einer gleichartigen Regelung unterworfen. Die Übermittlung einer Strafregisterauskunft an eine Stelle im Ausland ist ein Vorgang, dem datenschutzrechtlich weitaus größeres Gewicht beizumessen ist als einer Auskunftserteilung innerhalb der Bundesrepublik Deutschland. Der Informationswert des Datums „Zentralregistereintragung" ist im Ausland anders und für den Betroffenen belastender, als dies im Geltungsbereich des Bundeszentralregistergesetzes, das Tilgungsfristen vorsieht, der Fall sein würde. Es sollte zumindest versucht werden, eine differenzierende Lösung zu finden.

Ich habe dem Bundesminister der Justiz ferner vorgeschlagen, § 73 des Entwurfs dahin gehend zu ergänzen, daß Auskünfte über Vorstrafen nur durch das Bundeszentralregister erteilt werden. Dieses hätte dann zu prüfen, ob und in welchem Umfange die Auskunft nach dem geltenden Rechtshilfeabkommen zu geben ist und ob in den Fällen, in denen ein Abkommen nicht besteht, schutzwürdige Belange der Auskunftserteilung entgegenstehen könnten oder anderweitig zu berücksichtigen wären. Es wäre z. B. auch denkbar, in Fällen, in denen eine Tilgung unmittelbar bevorsteht, die Zeit bis zur Tilgungsreife abzuwarten oder die Auskunft mit einem Hinweis auf die bevorstehende Tilgung zu versehen. Dies könnte nur das Bundeszentralregister leisten.

#### 4.1.3 Novellierung des Bundeszentralregistergesetzes (BZRG)

Das Bundeszentralregistergesetz hat seit seinem Inkrafttreten am 1. Januar 1972 zahlreiche kleinere Änderungen erfahren. Eine erneute Novellierung ist beabsichtigt.

Ich habe in meinem 2. Tätigkeitsbericht (vgl. dort Nr. 2.2.1, S. 15) das BZRG als das Musterbeispiel eines gelungenen bereichsspezifischen Datenschutzgesetzes bezeichnet. Diese Bewertung halte ich aufrecht. Damit ist aber nicht gesagt, daß datenschutzrechtlich keinerlei Wünsche mehr offen wären. Dies kann schon deshalb nicht sein, weil das Datenschutzbewußtsein sich weiterhin entwickelt und auf das Recht einwirkt. Regelungen, die beim Erlaß eines Gesetzes generell akzeptierbar waren, können im Verlaufe dieser Entwicklung überprüfungsbedürftig werden. Das Gesetz vom 18. März 1971 hat die Bezeichnung „Gesetz über das Zentralregister ..." erhalten. Die bisherige Bezeichnung „Strafregister" wurde bewußt vermieden, um den Resozialisierungszweck des Gesetzes zu verdeutlichen. Gleichzeitig wurde damit aber auch die Möglichkeit eröffnet, andere Tatsachen als nur strafrechtliche Verurteilungen in das Register aufzunehmen, soweit diese in bestimmten Fällen für eine Beurteilung der Persönlichkeit des Eingetragenen erforderlich erschienen. Die darin liegende Erweiterung der Zweckbestimmung des Registers mag beim Erlaß des Gesetzes als unproblematisch angesehen worden sein. Inzwischen stoßen jedoch Register dieser Art auf wachsende Skepsis. Sie werden nicht mehr nur als Instrument einer effektiven Verwaltung empfunden, sondern vielfach als Medien der Überwachung und Kontrolle. Die Folge ist eine weithin zu beobachtende Abwehrhaltung. Ich will nicht behaupten, daß dies auch im Hinblick auf das Bundeszentralregister gilt. Es unterscheidet sich von anderen großen Informationssystemen dadurch, daß die hier betriebene Datenverarbeitung durch klare gesetzliche Regelungen weitgehend transparent ist.

Ungeachtet dessen sollte jedoch der Gesetzgeber die Möglichkeit der heranstehenden Novellierung nutzen, um zu prüfen, ob die bisherigen Regelungen dem gegenwärtigen Stand der Datenschutzdiskussion im vollen Umfang entsprechen. Ich habe dazu dem Bundesminister der Justiz eine Reihe von Vorschlägen zugeleitet, von denen ich an dieser Stelle einige aufführen will, um die Zielrichtung zu verdeutlichen:

— Nach § 10 BZRG sind gerichtliche Entscheidungen einzutragen, durch die jemand entmündigt wird. Wird die Entmündigung wieder aufgehoben, ist auch diese Entscheidung einzutragen. Dies bedeutet: dem Betroffenen wird durch die Aufhebung der Entmündigung zwar bescheinigt, daß er wieder gesund ist, im Register bleibt er aber als ehemals Entmündigter stigmatisiert. Vorstrafen werden getilgt; eine überwundene Krankheit aber soll praktisch auf Lebenszeit im Register gespeichert bleiben. Die nachteiligen Folgen für den Betroffenen können schwerer wiegen als die Kenntnis von Vorstrafen. Hier sollte der Gesetzgeber erwägen, die Eintragung entweder von Amts wegen zu löschen oder doch zumindest die Möglichkeit einer Löschung auf Antrag vorzusehen.

— Nach § 12 BZRG sind u. a. gerichtliche Entscheidungen und Verfügungen einer Strafverfolgungsbehörde einzutragen, durch die eine Strafverfolgung wegen Schuldunfähigkeit abgeschlossen wird. Diese Eintragung wird — ebenso wie die zuvor erwähnte — ebenfalls nicht getilgt, sondern bleibt bis zum Tode, spätestens bis zum 90. Lebensjahr im Register erhalten. Der nachstehend aufgeführte Einzelfall hat mich veran-

läßt, auch eine Überprüfung dieser Vorschrift anzuregen:

Der Petent, nahezu 80 Jahre alt, hatte einen Waffenerwerbsschein beantragt und von der zuständigen Behörde erfahren, die Zentralregisterauskunft weise die Eintragung „nicht verurteilungsfähig" auf. Sie beruht auf einem Verfahren, das 1950 gegen ihn durchgeführt worden war. Er war auf einer Kirmes im angetrunkenen Zustand mit zwei Polizisten aneinandergeraten und wegen Widerstands gegen die Staatsgewalt angeklagt worden. Das Verfahren wurde wegen trunkenheitsbedingter Zurechnungsunfähigkeit eingestellt und die Entscheidung in das Strafregister eingetragen. Der Petent, der sonst nie mehr straffällig geworden ist, sieht in dieser Eintragung eine Erklärung dafür, daß mehr als 10 Jahre später ein Vorschlag, ihn zum Schöffen zu bestellen, nicht weiter verfolgt wurde. Ich halte es für unerträglich, daß ein Mensch aufgrund eines einmaligen, vergleichsweise harmlosen Vorganges praktisch Zeit seines Lebens als nicht zurechnungsfähig gekennzeichnet bleibt. Erschwerend kommt hinzu, daß er davon unter Umständen nichts erfährt und demgemäß nicht auf eine Löschung nach § 23 BZRG (durch besondere Anordnung des Generalbundesanwalts) hinwirken kann.

Ich nehme diese Gelegenheit wahr, um auf ein Vollzugsdefizit bei der Verwirklichung des rechtspolitischen Zieles des § 49 des Bundeszentralregistergesetzes hinzuweisen. Nach dieser Bestimmung dürfen Vorstrafen, die im Bundeszentralregister getilgt worden sind, u. a. nicht zum Nachteil des Betroffenen verwendet werden. Dies geschieht jedoch noch häufig. Ein Beispielsfall mag für ähnliche angeführt werden.

Eine der Staatsanwaltschaft zugeleitete polizeiliche Ermittlungsakte enthielt einen Vermerk, in dem angegeben war, der Betroffene sei in der Schuldnerkartei eingetragen gewesen und mehrfach bei der Kriminalpolizei in Erscheinung getreten. Dabei wurden Verurteilungen aus den Jahren 1951, 1940 und 1928 angeführt. Nachforschungen des Betroffenen ergaben, daß weder die aktuelle Schuldnerliste noch das Bundeszentralregister eine Eintragung enthielt. Zwar hatte es Eintragungen gegeben, die aber ausnahmslos getilgt worden waren. Die Angaben über die Vorstrafen befanden sich in den polizeiinternen Unterlagen, die Auskunft über frühere und längst getilgte Eintragungen in der Schuldnerliste war fernmündlich von einer Mitarbeiterin des Amtsgerichts gegeben worden. Der Petent hat Strafanzeige gegen den Polizeibeamten erstattet. Das Verfahren wurde — vom Petenten nicht anders erwartet — mit der Begründung eingestellt, die Angaben seien zutreffend und daran ändere sich nichts dadurch, daß die Eintragungen in der Schuldnerkartei und im Bundeszentralregister gelöscht worden seien. Der Betroffene führt eine Reihe anderer Rechtsstreitigkeiten, in denen es auch auf seine Glaubwürdigkeit ankommt. Durch die Aufdeckung seiner „dunklen Vergangenheit" wird er aber als kriminelles Element abgestempelt und in seinen schutzwürdigen Belangen nachhaltig beeinträchtigt.

Anzumerken ist hier allerdings über den konkreten Fall hinaus, daß die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (KpS-Richtlinien, vgl. hierzu allgemein auch 4.5.1) einer schrankenlosen Aufbewahrung von Unterlagen über frühere Verurteilungen in Polizeiakten entgegenstehen. Die in Nr. 5 und 6 dieser Richtlinien geregelte Aussonderung von Polizeiakten, die in der Regel nach 10 Jahren erfolgt, hat die Vernichtung der gesamten Akte einschließlich der Unterlagen über frühere Verurteilungen zur Folge.

#### 4.1.4 Anordnung über Mitteilungen in Zivilsachen

Die in der Anordnung über Mitteilungen in Zivilsachen (MiZi) enthaltenen Mitteilungspflichten haben fast ausnahmslos personenbezogene Daten zum Gegenstand. Sie beziehen sich auf Sachverhalte, die in Verfahren der streitigen Zivilgerichtsbarkeit bekannt werden und die die Gerichte anderen öffentlichen Stellen mitteilen müssen. Die Mitteilungspflichten decken praktisch das gesamte Spektrum der Zivilgerichtsbarkeit ab. Finanzbehörden, Sozialbehörden, Staatsanwaltschaften, Standesämter und andere öffentliche Register erhalten auf diesem Wege Informationen über gerichtliche Entscheidungen, die sie zur Erfüllung ihrer Aufgaben mehr oder weniger dringend benötigen. Bei der Mehrzahl der Mitteilungspflichten ist die Notwendigkeit offenkundig und im Regelfall auch durch eindeutige Rechtsvorschriften abgedeckt. Es gibt aber auch Fälle, die heute anders zu bewerten sind als bei ihrer Begründung.

So sind z. B. die Staatsanwaltschaften zu unterrichten, wenn Verfahren zur Entmündigung wegen Geisteskrankheit oder Geistesschwäche eingeleitet werden. Schutzwürdige Belange des Betroffenen können erheblich beeinträchtigt werden, wenn das Verfahren nicht zur Entmündigung führt, die Unterlagen aber bei der Staatsanwaltschaft bleiben, ohne daß der Betroffene davon weiß.

Bei Räumungsklagen wegen Zahlungsverzugs des Mieters ist der örtliche Träger der Sozialhilfe zu benachrichtigen. Dieser soll dadurch in die Lage versetzt werden, rasch im Interesse des Mieters tätig zu werden. Der Verzug des Mieters muß indes nicht an seiner Mittellosigkeit liegen. Er kann sogar ein erhebliches Interesse daran haben, nicht als potentieller Sozialhilfeempfänger geführt zu werden.

Bei Klagen auf Nichtigerklärung einer Ehe oder Feststellung des Bestehens oder Nichtbestehens einer Ehe ist die Staatsanwaltschaft zu benachrichtigen, um sich am Verfahren beteiligen zu können. Wenn es in Hamburg ausreicht, die Mitteilungen listenmäßig unter Angabe von Termin, Rubrum und Aktenzeichen zu machen, dann ist aus datenschutzrechtlicher Sicht zu fragen, ob es geboten ist, daß in den übrigen Bundesländern die Akten oder die Klageschrift mit den möglicherweise höchst sensiblen Daten weiterhin übermittelt werden müssen. Zu dieser Problematik werde ich gemeinsam mit den Da-

tenschutzbeauftragten der Länder Empfehlungen für Regelungen erarbeiten, die den Datenschutz stärker berücksichtigen.

#### 4.1.5 Personenstandswesen

Der Bereich des Personenstandswesens ist bis in letzte Einzelheiten durch Rechtsvorschriften und Verwaltungsanordnungen geregelt. Nichtsdestoweniger bedarf es auch hier einer kontinuierlichen kritischen Überprüfung. Es gibt hier noch Mitteilungspflichten, die auf Bewertungen beruhen, die heute nicht mehr geteilt werden. Nach der Dienstanweisung für den Standesbeamten, einer allgemeinen Verwaltungsvorschrift zum Personenstandsgesetz, sind Standesbeamte verpflichtet, bei Eintragungen über umherziehende Personen ohne festen Wohnsitz die Kriminalpolizei zu unterrichten. Diese pauschale Diskriminierung einer Personengruppe muß ausgeräumt werden. Gemeinsam mit den Landesbeauftragten für den Datenschutz werde ich Vorschläge für eine Verbesserung des Datenschutzes im Personenstandswesen entwickeln.

#### 4.1.6 Entwurf eines Mietspiegelgesetzes

Verlangt bei einem Mietverhältnis über nicht-preisgebundenen Wohnraum der Vermieter eine Mieterhöhung in Anpassung an die ortsübliche Miete, muß er dieses Mieterhöhungsverlangen begründen. Dabei haben sich Übersichten über die ortsüblichen Entgelte (Mietspiegel) als das am besten geeignete Mittel zum Nachweis der Vergleichsmiete erwiesen. Mit dem Entwurf eines Mietspiegelgesetzes (Drucks. 9/745) sollen nunmehr Gemeinden bestimmter Größenordnungen unter gewissen Voraussetzungen gesetzlich zur Erstellung von Mietspiegeln verpflichtet werden. Der Mietspiegel enthält Angaben über Art, Größe, Ausstattung, Beschaffenheit und Lage des Wohnraumes sowie über die gezahlten Entgelte. Er muß, um als Arbeitsmittel geeignet zu sein, in Form einer Datei geführt werden. Damit werden personenbezogene Daten von hohem Sensibilitätsgrad gespeichert. Die Angaben lassen Rückschlüsse auf Einkommen und Lebensstil der Beteiligten zu. Das Bundesverfassungsgericht hat daher entschieden, daß niemand zur Erteilung von Auskünften über den Zustand und den Mietpreis seiner Wohnung verpflichtet sei (BVerfGE 37, 14). Wenn der Gesetzgeber nunmehr die Betroffenen dennoch zwingt, diese Angaben aus dem privaten Lebensbereich preiszugeben, muß er gleichzeitig dafür sorgen, daß sie angemessen geschützt werden. Auf meine Anregung hat die Bundesregierung daher in ihrem Entwurf zusätzlich zu dem Grundsatz, daß schutzwürdige Belange nicht beeinträchtigt werden dürfen, den Zweckbindungsgrundsatz mit aufgenommen. Einzelangaben mit Namen und Anschrift dürfen nur zum Zweck der Erstellung und Fortschreibung des Mietspiegels verwendet werden. Sie stehen nicht einmal den Finanzbehörden zur Verfügung. Die strenge Zweckbindung der Daten ist hier eine geeignete und notwendige Datenschutzmaßnahme.

#### 4.1.7 Prozeßkostenhilfe

Auf die Problematik der Prozeßkostenhilfe habe ich in meinem 3. Tätigkeitsbericht hingewiesen (vgl. dort Nr. 3.2.4, S. 20). Nach dem Gesetz über die Prozeßkostenhilfe vom 30. Juni 1980 muß derjenige, der Prozeßkostenhilfe beantragt, seine persönlichen und wirtschaftlichen Verhältnisse offenlegen. Dies hat zur Folge, daß diese Angaben allen Personen und Stellen, die das Recht der Akteneinsicht haben, zugänglich sind. Dagegen habe ich aus Gründen des Datenschutzes Bedenken erhoben.

Inzwischen haben der Bundesminister der Justiz und die Landesjustizverwaltungen in Durchführungsbestimmungen zu diesem Gesetz festgelegt, daß ab 1. Januar 1981 der Vordruck der Erklärung über die persönlichen und wirtschaftlichen Verhältnisse sowie die bei der Prozeßkostenhilfe entstehenden Vorgänge in einem Beiheft zur Prozeßakte zu führen sind.

Ich begrüße die jetzige Lösung als einen Beitrag zur schrittweisen Verbesserung des Datenschutzes in diesem Bereich. Das datenschutzrechtliche Problem konnte mit dieser Regelung allerdings noch nicht gelöst werden, da das Beiheft als Teil der Prozeßakten grundsätzlich auch vom Prozeßgegner eingesehen werden kann. Inzwischen hat sich auch die einschlägige Literatur mit dieser Problematik befaßt. Dabei ist die Ansicht geäußert worden, das Einsichtsrecht des Prozeßgegners erstrecke sich — aus verfassungsrechtlichen Gründen — nicht auf die Unterlagen der Prozeßkostenhilfe.

Ich werde die Diskussion aufmerksam weiterverfolgen und alle Bemühungen unterstützen, die in diesem Bereich den Persönlichkeitsschutz verstärken.

#### 4.1.8 Schuldnerverzeichnis

In meinem letzten Tätigkeitsbericht habe ich mich zu den Aussichten, den Datenschutz bei der Übermittlung von Angaben aus dem Schuldnerverzeichnis zu verbessern, pessimistisch geäußert. Zu meiner Genugtuung hat jedoch der Bundesminister der Justiz im vergangenen Jahr den Entwurf einer Verordnung über Abschriften aus dem Schuldnerverzeichnis erstellt, der in den Grundzügen meinen Vorschlägen entspricht. Der Entwurf wird z. Z. mit den Beteiligten im Bund und in den Ländern erörtert. Ich hoffe sehr, daß es zu einer Regelung kommt, bei der das bisher geübte Verfahren dahingehend geändert wird, daß vollständige Abschriften aus den Schuldnerverzeichnissen nur noch wenigen Stellen verfügbar gemacht werden und diese daraus Einzelauskünfte erteilen.

Das vom Bundesminister der Justiz vorgesehene Verfahren entspricht meinen Vorstellungen allerdings noch nicht in allen Einzelheiten. So soll es öffentlich-rechtlichen Berufsvertretungen wie bisher gestattet sein, ihren Mitgliedern vollständige Abschriften des Verzeichnisses zuzuleiten. Damit gelangen sehr sensible Daten zu einem unübersehbaren Empfängerkreis. Eine wirksame Kontrolle ist dort nicht mehr möglich. Während § 915 Abs. 4 Satz 1 ZPO die Erteilung von Abschriften unter dem Vorbehalt gestattet, daß die Einhaltung der Löschungsfrist gewährleistet ist, enthält der Entwurf in § 1 Abs. 1

Satz 1 die generelle Verpflichtung zur Erteilung von Abschriften. Diese Vorschrift fällt auch hinter die Anforderungen des derzeit geltenden § 1 der „Allgemeinen Vorschriften" zurück, der hinsichtlich privater Unternehmen eine Ermessensentscheidung vorsieht, bei der die Vertrauenswürdigkeit zu prüfen ist. Eine solche Prüfung ist sinnvoll, um der Gefahr von Mißbräuchen durch unseriöse Unternehmen entgegenzuwirken.

Wie notwendig es ist, die geltenden Vorschriften einschließlich der zugrunde liegenden gesetzlichen Regelung des § 915 ZPO zu überarbeiten, mag folgender Einzelfall verdeutlichen. Der Gläubiger eines im Schuldnerverzeichnis Eingetragenen hatte dem Amtsgericht mitgeteilt, seine Forderung sei beglichen worden. Da der Schuldner auf Betreiben dieses Gläubigers in das Schuldnerverzeichnis eingetragen worden war, läge es nahe anzunehmen, daß auch die Löschung durch den Gläubiger veranlaßt werden könnte. Das ist jedoch nicht der Fall. § 915 Abs. 2 ZPO sieht eine Löschung nur auf Antrag des Schuldners vor. In dem mir vorliegenden Einzelfall hat das Amtsgericht von sich aus den Schuldner angeschrieben und ihm anheimgestellt, die Löschung zu beantragen. Ob dies stets geschieht, möchte ich bezweifeln. Die Eintragung erfolgt nicht selten, ohne daß der Schuldner davon weiß. Angesichts dessen ist meines Erachtens sowohl der Gläubiger als auch das Amtsgericht für verpflichtet zu halten, auf die Löschung der Eintragung hinzuwirken, wenn die tatsächlichen Voraussetzungen dafür entfallen sind. Ein Schuldner, der seine Forderungen beglichen hat und dennoch im Schuldnerverzeichnis eingetragen bleibt, wird in seinen schutzwürdigen Belangen erheblich beeinträchtigt. Hier ist der Gesetzgeber aufgerufen, Abhilfe zu schaffen.

#### 4.1.9 Daten über Mietinteressenten

Als besonders dringlich sehe ich datenschutzrechtliche Regelungen zum Schutz von Mietinteressenten an. Wie ich aus der wachsenden Zahl von Beschwerden Betroffener und Anfragen durch Journalisten entnehme, gehen Vermieter, beginnend mit größeren Wohnungsbaugesellschaften, zunehmend dazu über, von Mietinteressenten detaillierte Auskünfte über die persönlichen Verhältnisse sowie eine Einwilligungserklärung für die Einholung von Auskünften bei Auskunfteien, früheren Vermietern und Arbeitgebern zu verlangen. Die Fragen zur Person beziehen sich nicht nur auf Einkommens- und Vermögensverhältnisse (Arbeitseinkommen, sonstige regelmäßige Einkünfte, Grundbesitz usw.), sondern auch auf familiäre Verhältnisse (Vornamen, Alter und Geschlecht von Kindern sowie weiterer Haushaltsangehöriger) bis hin zur Frage nach einer etwaigen Schwangerschaft eines Familienmitgliedes.

Die Mietinteressenten sind einem derartigen Ansinnen praktisch hilflos ausgeliefert, da sie damit rechnen müssen, von vornherein aus der Liste der Bewerber gestrichen zu werden, wenn sie auch nur einzelne der geforderten Angaben schuldig bleiben. Während die Arbeitsgerichte anerkannt haben, daß Fragen, die mit dem in Aussicht genommenen Arbeitsverhältnis nichts zu tun haben, nicht beantwortet zu werden brauchen und Falschangaben für den eingestellten Arbeitnehmer keine nachteiligen Folgen haben dürfen, fehlt es auf dem Gebiet des Mietrechts an einer entsprechenden Klärung. Das Schutzbedürfnis der Betroffenen betrachte ich hier als in ähnlicher Weise gegeben.

Das Bundesdatenschutzgesetz kann den notwendigen Schutz nicht bieten, da die Angaben von den Bewerbern auf freiwilliger Basis erhoben werden; abgesehen davon werden die Angaben in der Regel wohl nur in Akten, nicht aber in einer Datei verarbeitet, so daß das Bundesdatenschutzgesetz unanwendbar bleibt. Das BDSG bietet auch keine Handhabe dafür, die Wirksamkeit einer Einwilligung zur Einholung von Auskünften bei Auskunfteien und anderen Stellen in Zweifel zu ziehen, da es nur auf das einwandfreie Zustandekommen der Einwilligung abstellt, aber nicht danach fragt, ob die Datenverarbeitung, in die eingewilligt worden ist, zu dem angestrebten wirtschaftlichen Zweck erforderlich oder auch nur geeignet und angemessen ist. Ich würde es deshalb begrüßen, wenn die Bundesregierung dieser Entwicklung mit gesetzlichen Maßnahmen entgegenträte; neben dem Datenschutz sollten dabei auch die wohnungs- und sozialpolitischen Gesichtspunkte berücksichtigt werden.

### 4.2 Sozialverwaltung und Gesundheitswesen

#### 4.2.1 Sozialgesetzbuch, Zehntes Buch

Am 1. Januar 1981 traten die beiden ersten Kapitel des SGB X — Verwaltungsverfahren, Schutz der Sozialdaten — in Kraft. Die Anwendung der neuen Vorschriften über den Sozialdatenschutz hat zu einer Reihe von Auslegungsschwierigkeiten geführt, wie das bei einem neuen Gesetz nicht anders zu erwarten war. Größere Schwierigkeiten haben sich jedoch bisher — also nach relativ kurzer Erprobung — noch nicht ergeben. Auf das Problem des § 75 SGB X wird gesondert eingegangen (s. u. 4.3.2).

Bei den Beratungen des Dritten Kapitels des SGB X — Zusammenarbeit der Leistungsträger und ihre Beziehungen zu Dritten — galt meine Sorge insbesondere der Frage, wie das — erstrebenswerte — Ziel der Vermeidung überflüssiger Doppeluntersuchungen erreicht werden kann, ohne den Aufbau einer für die Freiheit des Bürgers bedrohlichen medizinischen Zentraldatei zu ermöglichen. Nach dem gegenwärtigen Stand des Gesetzgebungsverfahrens besteht Grund zu der Annahme, daß ein ausdrückliches Verbot einer derartigen Datei in das Gesetz aufgenommen werden wird.

#### 4.2.2 Modellprogramm Psychiatrie

Im Berichtsjahr haben weitere Beratungen über die Durchführung des Modellprogramms Psychiatrie (vgl. 3. TB, Nr. 3.10.6.1, S. 45) stattgefunden. Dabei hat sich gezeigt, daß die bei der Durchführung auftretenden Fragen in erster Linie in die Zuständigkeit der Länder fallen. Ich habe aber im Rahmen meiner Beratungsfunktion dem Bundesministerium für Jugend, Familie und Gesundheit Hinweise gegeben, wie das Modellprogramm in datenschutzrechtlich einwandfreier Weise realisiert werden könnte.

#### 4.2.3 Heimgesetz

Die entsprechend dem Altersaufbau der Bevölkerung ständig zunehmende Zahl von Heimbewohnern macht es immer notwendiger, ihren Interessen und Bedürfnissen entsprechende Regelungen für Heimträger und Heimpersonal zu schaffen. So wird u. a. für notwendig gehalten, in der Regel mindestens folgende Dateien zu führen, um eine Kontrolle der Heime auf Einhaltung der gesetzlichen Bestimmungen, insbesondere des Heimgesetzes, durch die zuständigen Behörden realisieren zu können:

— eine Datei der Heimbewohner

— eine Datei des in einem Heim beschäftigten Personals mit Angaben zu dessen beruflicher Qualifikation.

Es werden also schutzwürdige Belange verschiedener Personenkreise berührt; dabei verlangt die Schutzbedürftigkeit der Heimbewohner eine besonders sorgfältige Abwägung. Der Entwurf einer Verordnung über die Buchführungs- und Meldepflichten der Träger von Altenheimen, Altenwohnheimen und Pflegeheimen für Volljährige — Stand: 1. Oktober 1981 — versucht, hier zu angemessenen Regelungen zu kommen. Ich habe den Bundesminister für Jugend, Familie und Gesundheit im Zuge seiner Vorbereitungen zum Erlaß der genannten Verordnung beraten und stehe für weitere Gespräche zur Verfügung.

### 4.3 Forschung und Statistik

#### 4.3.1 Auswirkungen des Datenschutzes auf die wissenschaftliche Forschung

Die öffentliche Diskussion über die Auswirkungen des Datenschutzes auf die wissenschaftliche Forschung, die im Berichtsjahr fortgeführt wurde, hat in einigen zentralen Fragen zu wichtigen Klärungen geführt. Von der Westdeutschen Rektorenkonferenz und vom Wissenschaftsrat durchgeführte Umfragen vermitteln erstmals ein qualitativ repräsentatives Bild der Auswirkungen des Datenschutzes auf die wissenschaftliche Praxis. Die aus meiner Sicht wichtigsten Ergebnisse sind folgende:

a) Die pauschale Behauptung, der Datenschutz behindere die wissenschaftliche Forschung, ist widerlegt. Von den Forschern, die personenbezogene Daten verarbeiten, berichtet ein großer Teil, daß Datenschutzprobleme nicht aufgetreten sind oder mit angemessenem Aufwand gelöst wurden.

b) Soweit über Behinderungen berichtet wird, beruhen diese nur in den seltensten Fällen auf (richtig ausgelegten und angewendeten) Rechtsvorschriften des Datenschutzes; im Vordergrund stehen vielmehr Erschwernisse in der Planung und im Ablauf von Forschungsprojekten. Sie beruhen insbesondere
   — auf Verzögerungen des Datenzugangs als Folge unzureichender datenschutzrechtlicher Kenntnisse der Beteiligten,
   — auf Verzögerungen, weil notwendige Abstimmungen oder technische und organisatorische Datenschutzmaßnahmen nicht eingeplant waren,
   — auf Nicht-Entscheidungen der datenverwaltenden Stellen aus Risikoscheu.

c) Nicht selten wird der Datenschutz als Vorwand mißbraucht, wenn eine Stelle aus ganz anderen Gründen einem Forschungsprojekt die Unterstützung verweigern möchte.

d) Mitunter werden auch Restriktionen als Ausdruck eines „überzogenen Datenschutzes" bekämpft, die sich tatsächlich aus besonderen Rechtsvorschriften ergeben, die schon lange vor dem Bundesdatenschutzgesetz bestanden haben und deren Berechtigung nicht in Zweifel gezogen wird, wie etwa aus der ärztlichen Verschwiegenheitspflicht, dem Statistikgeheimnis und den Benutzungsordnungen der staatlichen Archive.

e) Die Notwendigkeit, vor der Verarbeitung personenbezogener Daten die Einwilligung der Betroffenen einzuholen, wird von einigen Forschern aus grundsätzlichen, insbesondere wissenschaftsmethodischen Gesichtspunkten abgelehnt, andere betrachten den dafür notwendigen Aufwand als unangemessen und unzumutbar.

f) Gegenstand einzelner Beschwerden ist schließlich die angeblich zu strenge Beurteilung der Frage, ob Daten hinreichend anonymisiert sind, um als nicht-personenbezogen gelten zu können und damit nicht unter das Gesetz fallen (s. u. S. 50).

Insgesamt zeigt sich also durchaus kein einheitliches Bild; jedoch erweisen sich die Äußerungen mancher Wissenschaftler, die den Untergang ganzer Disziplinen und einen Rückfall der deutschen Wissenschaft im internationalen Vergleich beschwören und dafür den Datenschutz verantwortlich machen, als abwegig. Zwar ist es offensichtlich, daß Forschung und Datenschutz — ganz abstrakt gesehen — entgegengesetzte informationspolitische Ziele verfolgen. Praktische Kompromisse sind deshalb aber nicht ausgeschlossen. Von der Seite des Datenschutzes wird dem Zugang der Forschung zu personenbezogenen Daten nicht widersprochen, wenn schutzwürdige Belange der Betroffenen nicht berührt werden oder wenn der Gesetzgeber der Forschung den Vorrang eingeräumt hat. Ebenso wird von der Seite der Forschung grundsätzlich zugestanden, daß der Anspruch des einzelnen auf Datenschutz den Freiraum der Wissenschaft begrenzen kann.

Wenn es in der konkreten Konfrontation von Datenzugangswünschen und Datenschutzauflagen vermehrt zu Schwierigkeiten kommt, ist dies die nicht überraschende Folge eines geschärften Problembewußtseins. Konsequenz kann aber nicht sein, eine grundsätzliche Neubestimmung des Verhältnisses von Forschung und Datenschutz zu verlangen. Vielmehr geht es darum, die praktische Verständigung zu fördern.

Für die Wissenschaft ist das zugegebenermaßen nicht immer einfach. Während in der Vergangenheit wissenschaftliches Renommee und persönliche Vertrauenswürdigkeit im allgemeinen als Grundlage

für den Zugang zu personenbezogenen Unterlagen ausreichten, ist jetzt eine Auseinandersetzung mit datenschutzrechtlichen Bestimmungen, die oft schwer aufzufinden und noch schwerer anzuwenden sind, unumgänglich. Die Forschung wäre schlecht beraten, wenn sie Aufwendungen für den Datenschutz als verlorene Investition ansähe; die Auskunftsbereitschaft der Bürger hängt maßgeblich von dem Vertrauen auf einen wirksamen Datenschutz ab. Bis zu einem gewissen Grad muß die Forschung einen erhöhten Aufwand akzeptieren. Die Datenschutzbehörden in Bund und Ländern bieten hierzu ihre Beratungen an und werden sich um ausgewogene Lösungen bemühen. Sie betrachten es als schädlich, wenn die Geheimhaltung — bewußt oder unbewußt — übertrieben oder als Vorwand für andere Motive benutzt wird. Denn dann werden die Rechte oder Chancen derjenigen, die auf den Zugang zu personenbezogenen Daten angewiesen sind, verkürzt. Darüber zu wachen, daß dies nicht geschieht, ist den Datenschutzinstanzen zwar vom Gesetz nicht ausdrücklich als Aufgabe zugewiesen; gleichwohl liegt es nach meiner Überzeugung im wohlverstandenen Interesse des Datenschutzes, keine überzogenen Anforderungen zu stellen. Unabhängig von dieser Beratungsmöglichkeit dürfte es für wissenschaftliche Einrichtungen zweckmäßig sein, sich eine eigene Beratungskapazität — gegebenenfalls auch überregional — aufzubauen.

Die Kontroversen um den Grad einer notwendigen Anonymisierung können nur fallbezogen beigelegt werden. Da die rechtliche Bewertung u. a. von der Einschätzung des Mißbrauchsrisikos und damit von subjektiven Faktoren abhängt, ist die Verständigung nicht immer einfach (vgl. unten 4.3.4). Auf die Notwendigkeit, objektivierende Verfahren zu entwickeln, habe ich bereits früher hingewiesen. Entsprechende Forschungsarbeiten sind im Gange.

Die Schwierigkeiten bei der Anwendung des Bundesdatenschutzgesetzes im Falle der Übermittlung personenbezogener Daten für wissenschaftliche Zwecke ergeben sich u. a. daraus, daß das BDSG — im Gegensatz zu mehreren Landesdatenschutzgesetzen — hierfür keine Sonderregelung vorsieht. Wird eine Stelle des Bundes von einer Hochschule oder einer anderen öffentlichen Stelle um Überlassung von Daten für wissenschaftliche Zwecke gebeten, so müßte nach der hier einschlägigen Regelung des § 10 Abs. 1 BDSG geprüft werden, ob die Kenntnis der Angaben für den Empfänger zur rechtmäßigen Erfüllung seiner Aufgaben erforderlich ist. Dieses Kriterium, das im Falle der Amtshilfe, also der Unterstützung bei Verwaltungsaufgaben, paßt, ist im Falle der Übermittlung zu wissenschaftlichen Zwecken untauglich, da es, je nach Auslegung, der Wissenschaft entweder einen praktisch unbegrenzten Zugang eröffnet oder sie vollständig ausschließt. Zudem ist schwer begründbar, warum öffentlich-rechtlich organisierte Forschungseinrichtungen anders behandelt werden sollen als privatrechtliche, denen gemäß § 11 der Datenzugang aufgrund einer Abwägung des Forschungsinteresses mit den schutzwürdigen Belangen der Betroffenen gewährt werden kann. Im Zuge der Novellierung des BDSG sollte klargestellt werden, daß das Abwägungsprinzip auch im Falle öffentlich-rechtlicher Forschungsträger anzuwenden ist. Zugleich sollten ergänzende Regelungen zum Schutz der Daten beim Empfänger erlassen werden (vgl. unten 4.7 l), S. 57).

#### 4.3.2 Erfahrungen mit § 75 SGB X

Mit Schreiben vom 23. Dezember 1980 teilte der Bundesminister für Jugend, Familie und Gesundheit den „Öffentlich-rechtlichen Krankenkassen im Raum Bayern" mit, zwei Forschungsinstitute führten im Auftrag des Ministeriums eine „Untersuchung über die Erfahrungen und Auswirkungen des Mutterschaftsurlaubs durch". Die Krankenkassen wurden gebeten, die Adressen der bei ihnen versicherten Mütter, die sich derzeit im Mutterschaftsurlaub befänden, einem der beiden Forschungsinstitute bekanntzugeben. Durch den Datenschutzbeauftragten einer der Krankenkassen wurde ich im Januar 1981 auf dieses Schreiben aufmerksam gemacht, also zu einem Zeitpunkt, als § 75 SGB X (seit dem 1. 1. 1981) schon in Kraft war. Das Ministerium hatte diese Vorschrift offenbar übersehen. Mit Schreiben vom 26. Januar 1981 habe ich das Ministerium auf die einschlägigen Bestimmungen hingewiesen. Das Ministerium hat der Presse gegenüber erklärt, es werde in Zukunft auf die Pflichten nach dem SGB hinweisen. Die Untersuchung sei vorübergehend gestoppt worden, um sicherzustellen, daß die noch fehlenden Adressen nur mit Zustimmung der Betroffenen weitergegeben werden.

Um mir einen Überblick über die Genehmigungspraxis gemäß § 75 Abs. 2 SGB X seit Inkrafttreten des SGB X zu verschaffen, habe ich den Bundesminister für Arbeit und Sozialordnung, den Bundesminister für Jugend, Familie und Gesundheit und den Bundesminister für Forschung und Technologie um Auskunft gebeten, ob in der Zeit vom 1. Januar bis 31. Oktober 1981 Genehmigungen erteilt wurden und — bejahendenfalls — die Forschungs- oder Planungsvorhaben und die Kriterien, die der Genehmigung zugrunde gelegt wurden, zu beschreiben. Alle drei Ministerien haben Fehlanzeige erstattet, der Bundesminister für Forschung und Technologie mit dem Zusatz, Genehmigungen gemäß § 75 Abs. 2 SGB X fielen nicht in seine Zuständigkeit.

Dieses Ergebnis läßt zwei Schlüsse zu: entweder hat es im Anwendungsbereich des § 75 SGB X im genannten Zeitraum keine Forschungs- und Planungsvorhaben gegeben oder die Bestimmung wird (noch) nicht angewendet. Für die zweite Alternative sprechen — außer dem oben erwähnten Fall — gewisse Anzeichen:

— Im Bericht des Ausschusses für Arbeit und Sozialordnung des Deutschen Bundestages zum Entwurf eines Sozialgesetzbuches — Verwaltungsverfahren (BT-Drucksache 8/2034) wird betont, § 75 (im Entwurf § 72) „ist im Verhältnis zu § 67 (jetzt: § 69) als Sonderregelung anzusehen" (S. 86). Demgegenüber vertritt der Bundesminister für Arbeit und Sozialordnung mündlich und schriftlich die Auffassung, soweit eine in § 35 SGB I genannte Stelle für die Erfüllung einer gesetzlichen Aufgabe nach dem SGB forsche oder plane, sei § 69 SGB X anzuwenden. Dabei bleibt

regelmäßig offen, ob Forschung oder Planung eine *gesetzliche* Aufgabe nach dem SGB ist. Ausdrückliche gesetzliche Regelungen von Forschungs- oder Planungsaufgaben — wie z. B. § 6 AFG — sind aber eher die Ausnahme.

— Nach dem zitierten Ausschußbericht soll § 75 Abs. 2 sicherstellen, „daß die Offenbarung für die Forschung oder Planung ein Ausnahmetatbestand bleibt, dessen Voraussetzungen in jedem Einzelfall sorgfältig zu prüfen sind" (aaO S. 87). Meine Empfehlung, die Genehmigungsbehörden mögen für diese sorgfältige Einzelfallprüfung Kriterien entwickeln (s. schon 3. TB, Nr. 2.5, S. 15), ist bisher ohne Ergebnis geblieben.

Ferner heißt es im Ausschußbericht: „Ist der für die offenbarende Stelle fachlich zuständige Bundes- oder Landesminister nicht zugleich auch der für die Forschung oder Planung zuständige Minister, ist dieser gemäß den Geschäftsordnungen der Bundes- oder Landesregierungen zu beteiligen. Der Zusatz des Bundesministers für Forschung und Technologie (siehe oben) dürfte also so zu verstehen sein, daß auch eine Beteiligung an einem Genehmigungsverfahren eines anderen Ressorts bisher nicht erfolgt ist.

Sicherlich ist die seit Inkrafttreten des SGB X verstrichene Zeit zu kurz, um schon ein abschließendes Urteil zu ermöglichen. Die bisherige Praxis läßt allerdings vermuten, daß die zuständigen Ressorts die Bedeutung des § 75 SGB X nicht richtig einschätzen.

#### 4.3.3 Krebsregister

Auf der Grundlage eines Nationalen Krebsberichtes, den die Bundesregierung am 16. Januar 1980 (BT-Drucksache 8/3556) vorgelegt hat, soll ein „Gesamtprogramm zur Krebsbekämpfung" entwickelt und durchgeführt werden. Unter anderem wurde hierzu eine „Geschäftsstelle Gesamtprogramm zur Krebsbekämpfung" mit Sitz in Köln eingerichtet, die den zuständigen Bundesressorts (Bundesministerium für Jugend, Familie und Gesundheit, Bundesministerium für Arbeit und Sozialordnung, Bundesministerium für Forschung und Technologie, Bundesministerium des Innern [Abteilung Umweltangelegenheiten]) zuarbeiten soll.

Innerhalb der fachlichen Schwerpunkte des Gesamtprogramms wurde Anfang 1981 eine Arbeitsgruppe „Rechtsfragen der Krebsregistrierung" gegründet, in der ich zusammen mit Epidemiologen und Vertretern der Verwaltung und der Landesdatenschutzbeauftragten mitgearbeitet habe. Ziel der Arbeitsgruppe war es, einen Musterentwurf für ein Krebsregistergesetz zu erarbeiten, den die Länder übernehmen könnten. Die Beratungen verliefen teilweise kontrovers; sie sind noch nicht abgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dazu einen Beschluß gefaßt. Er hat folgenden Wortlaut:

„1. Die Datenschutzbeauftragten erkennen die gesundheitspolitische Bedeutung der medizinischen Forschung, insbesondere im Zusammenhang mit der Bekämpfung von Krebserkrankungen, an. Es entspricht ihrer gesetzlichen Aufgabe, auch in diesem Bereich für die Wahrung der schutzwürdigen Belange der Patienten einzutreten. Ihre Bedenken und Vorschläge zielen daher ausschließlich darauf ab, die Freiheit der Forschung in ein ausgewogenes und rechtlich abgesichertes Verhältnis zu den grundrechtlich geschützten Belangen der Betroffenen zu bringen. Sie gehen davon aus, daß es möglich ist, Regelungen zu finden, die den Erfordernissen der Forschung wie auch des Schutzes der Individualsphäre gerecht werden. Die gelegentlich geäußerte pauschale Behauptung, der Datenschutz behindere die Krebsforschung, weisen sie als unbegründet zurück.

2. Es ist nicht die Aufgabe der Datenschutzbeauftragten, Sinn und Nutzen von Krebsregistern zu beurteilen. Sie warnen aber nachdrücklich vor der Gefahr, daß die Gesetzgebung zum Krebsregister ein erster Schritt zur Errichtung einer Vielzahl anderer Epidemiologieregister werden könnte. In diesem Zusammenhang weisen sie darauf hin, daß auch aus Kreisen der Ärzteschaft erhebliche Zweifel am Nutzen medizinischer Register geäußert werden, woraus sich Zweifel an der Erforderlichkeit derartiger Register ableiten lassen. Sie appellieren an die medizinische Forschung, stärker als bisher den bereits vorhandenen Forschungsstand zur Anonymisierung personenbezogener Daten zu nutzen und sich vordringlich um die Weiterentwicklung von Anonymisierungs- und Aggregationsmethoden zu bemühen. Diese methodologischen Überlegungen können wesentlich dazu beitragen, Probleme, die sich durch die ärztliche Schweigepflicht und den Datenschutz ergeben, gar nicht erst aufkommen zu lassen.

3. Für den Fall der politischen Entscheidung in den Ländern zugunsten der Schaffung von Krebsregistern halten sie es für notwendig, daß die Errichtung, Ausgestaltung und Nutzung von Krebsregistern in einem speziellen Gesetz geregelt werden. Der mit der Einrichtung eines Krebsregisters verbundene Eingriff in Grundrechtspositionen der Betroffenen ist nur durch ein Gesetz zu legitimieren, das die nachfolgenden Grundsätze beachtet (vgl. unten 4). Dabei wird davon ausgegangen, daß es sich um ein Register zur Erfassung der *Anzahl* der Neuerkrankungen (Inzidenzregister) bzw. der *Anzahl* erkrankter Personen (Prävalenzregister) handeln wird.

Eine im Anwendungsbereich unbestimmte allgemeine Rahmenregelung für die medizinische Forschung in einem Landesdatenschutzgesetz, die derzeit im Vordergrund baden-württembergischer Überlegungen steht, lehnen die Datenschutzbeauftragten daher — auch aus verfassungsrechtlichen Bedenken — ab.

4. Nach Auffassung der Datenschutzbeauftragten muß ein Krebsregistergesetz zumindest die folgenden Prinzipien berücksichtigen:

4.1. Die Meldung von Patientendaten mit Personenbezug an das Krebsregister bedarf grundsätzlich der Einwilligung des Betroffenen (bzw. der Entbindung von der ärztlichen Schweigepflicht). Nur in wenigen Ausnahmefällen kann die Meldung auch ohne Einwilligung des Patienten erfolgen, und zwar wenn sie für die Zwecke des Krebsregisters nachweisbar notwendig ist und dem Patienten dadurch, daß ihm die Art seiner Erkrankung bekannt wird, gesundheitliche Nachteile entstehen können. Soweit weder ein solcher Ausnahmefall noch eine Einwilligung vorliegt, unterbleiben Meldungen an das Register. Der zulässige Umfang der Einwilligung ist im Gesetz festzulegen.

4.2. Der gleiche Grundsatz gilt für die weitere Übermittlung durch das Krebsregister an andere Forschungseinrichtungen; für sie ist eine besondere Einwilligung erforderlich, wenn die Daten nicht in aggregierter oder anonymisierter Form weitergegeben werden. Für diese Übermittlung ist entsprechend der Regelung über die Forschung mit Sozialdaten ein Genehmigungsverfahren vorzusehen. Eine nochmalige Übermittlung durch die Forschungseinrichtung an Dritte ist unzulässig.

4.3. Der Gesetzeszweck, die Aufgaben des Krebsregisters, seine Rechtsform und institutionelle Ausgestaltung sind im Gesetz festzulegen. Im Interesse einer wirksamen Aufsicht sollte das Krebsregister in öffentlich-rechtlicher Trägerschaft geführt werden.

4.4. Der Kreis derjenigen Institutionen, die zu Forschungszwecken personenbezogene Daten des Krebsregisters erhalten können, sollte in der Weise beschränkt werden, daß die ausschließliche Verwendung zu Forschungszwecken gewährleistet ist.

4.5. Der in den Statistikgesetzen verankerte Grundsatz der Zweckbindung muß auch für die im Krebsregister gespeicherten Daten gelten.

Im übrigen sollte geprüft werden, ob ein gesetzliches Verbot eingeführt werden sollte, vom Betroffenen eine Bescheinigung über den Inhalt der im Krebsregister gespeicherten Daten zu verlangen. Ein solches Verbot könnte verhindern, daß potentielle Arbeitgeber oder sonstige Vertragspartner vom Betroffenen die Vorlage einer Art Negativ-Attest des Krebsregisters fordern.

4.6. Eine Verknüpfung mit anderen Datenbanken ist unzulässig.

4.7. Die Aufbewahrung personenbezogener Daten beim Krebsregister ist zu befristen. Patientendaten sind außerdem zu löschen, wenn sie nicht mehr benötigt werden.

4.8. Jeder Betroffene hat Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten aus dem Krebsregister. Dies gilt auch für Patienten, die über die Meldung nicht informiert worden sind. Entsprechend der Regelung für Sozialdaten in § 25 SGB X kann bei Gefahr für die Gesundheit des Patienten die Auskunft — vermittelt durch einen Arzt — erteilt werden."

Ich hoffe sehr, daß die zuständigen Instanzen diesen Bedenken und Anregungen Rechnung tragen werden, und bin bereit, bei den weiteren Beratungen — wie schon in der Vergangenheit — daran mitzuwirken, daß konkrete Lösungen entwickelt werden.

#### 4.3.4 Entwicklungen im Bereich der Statistik

Die bei mir und den Landesbeauftragten eingegangenen Beschwerden, die den Bereich der Bundesstatistik betreffen, zeigen, daß der Widerstand gegen Erhebungen wächst, wenn Fragen aus der Privat- oder Intimsphäre der Bürger gestellt werden und wenn die sachliche Notwendigkeit von Fragen nicht evident ist. In diesen Fällen empfindet man das Auskunftsverlangen als Zumutung, bezweifelt seine Erforderlichkeit und Rechtmäßigkeit und befürchtet, daß die Angaben trotz des gesetzlichen Statistikgeheimnisses Dritten zur Kenntnis gelangen können. Auf Ablehnung stößt insbesondere das Ansinnen, Namen und Anschrift in den Fragebogen einzutragen.

Mit den Landesbeauftragten bin ich der Ansicht, daß der hier sichtbare Konflikt wesentlich dadurch hervorgerufen und verschärft wird, daß der Staat mit Zwang in das Privatleben der Bürger eindringt. Es ist dem Betroffenen nämlich in aller Regel nicht freigestellt, ob er die gestellten Fragen beantworten will. Die Auskunft wird ihm vielmehr unter Bußgeldandrohung zur Pflicht gemacht.

Der Gesetzgeber sollte den sich verschärfenden Konflikt zum Anlaß nehmen, bei jeder einzelnen Repräsentativstatistik zu prüfen, in welchem Umfang ein Eindringen in das Privatleben wirklich unumgänglich ist und ob es nicht wenigstens ohne Drohung mit Zwangsmaßnahmen erfolgen kann. Die Freiheit des Bürgers, über die Offenlegung seiner Privatsphäre selbst zu entscheiden, sollte auf keinen Fall mehr als nötig eingeschränkt werden. Die Qualität der Ergebnisse einer Statistik braucht nicht unbedingt zu leiden, wenn die Auskunft freigestellt wird. Im westlichen Ausland jedenfalls wird eine sanktionsbewährte Auskunftspflicht bei Repräsentativstatistiken überwiegend für entbehrlich gehalten. In der Tat spricht viel dafür, daß der Anteil richtiger Antworten steigt, wenn die Betroffenen ohne Zwang antworten und über die Bedeutung der einzelnen Statistik aufgeklärt wurden.

In Fällen, in denen die Antwort nicht freigestellt werden kann, sollte dem Betroffenen die Notwendigkeit der Auskunftspflicht plausibel gemacht werden. Schon die Begründung zum Entwurf des Gesetzes sollte deshalb erkennen lassen, daß diese Frage eingehend geprüft wurde. Bei der Erhebung sollten die wesentlichen Gründe genannt werden. Der schlichte Hinweis auf gesetzliche Bestimmungen, wie er der heutigen Praxis entspricht, wird vom Bürger nicht mehr als ausreichende Information angesehen.

In den wenigen Fällen, in denen das Gesetz die Antwort auf eine Frage freistellt, ist die tatsächliche Freiwilligkeit in der Praxis nach meinen Beobachtungen nicht immer gewährleistet, weil eine ausrei-

chende Unterrichtung des Betroffenen mitunter versäumt wird. Zusammen mit den Landesbeauftragten habe ich deshalb in dem gemeinsamen Arbeitskreis Statistik Verfahrensvorschläge erarbeitet, die die notwendige Information garantieren sollen.

Die z. B. im Mikrozensusgesetz vorgesehene Möglichkeit, Fragen nicht im Gespräch mit einem Interviewer, sondern schriftlich gegenüber dem Statistischen Landesamt zu beantworten, wird nicht immer ausreichend bekanntgemacht, obwohl gerade sie gut geeignet ist, einen Teil der Vorbehalte auszuräumen. Auch hier hat der Arbeitskreis Verbesserungsvorschläge entwickelt.

Auch im abgelaufenen Jahr haben die Landesbeauftragten und ich einige Statistiken daraufhin überprüft, ob alle geforderten Angaben durch eine gesetzliche Grundlage gedeckt sind und ob sie für die Durchführung der einzelnen Statistik tatsächlich benötigt werden. Offensichtliche Rechtsverstöße wurden dabei nicht festgestellt. In einigen Bundesländern, die bei der Hochschulstatistik bei Bildungseinrichtungen der Sekundarstufe II noch die Namen und die Anschriften der Betroffenen erheben, war jedoch, wie schon im Jahre 1980 im Falle der Sozialhilfestatistik (vgl. 3. TB, Nr. 3.4.2, S. 24), zu fordern, auf diese Angaben zu verzichten, weil sich nach eingehender Prüfung herausgestellt hat, daß sie für die Durchführung der Statistik nicht erforderlich sind.

Immer wieder bin ich mit der Frage konfrontiert gewesen, ob Daten im Einzelfall als hinreichend anonymisiert angesehen werden können, so daß die Übermittlung datenschutzrechtlich unproblematisch ist. Gerade bei Fragen, die die Intimsphäre des Bürgers betreffen, ist es wichtig, das Statistikgeheimnis nach strengen Grundsätzen zu handhaben und an Dritte nur solche Daten zu übermitteln, die tatsächlich keinen Personenbezug mehr besitzen. Dies zwingt jedoch nach meiner Überzeugung nicht dazu, eine Anonymisierung erst dann als hinreichend anzuerkennen, wenn die Herstellung des Personenbezugs unter allen nur denkbaren Bedingungen, also auch theoretisch ausgeschlossen ist. Vielmehr sind schon solche Daten als anonymisiert anzusehen, für die der Datenempfänger und Dritte den Personenbezug nur noch mit einem völlig unangemessenen und nicht mehr zu erwartenden Aufwand herstellen könnten. Maßgeblich für die Beurteilung sind deshalb die Sensitivität der Daten, das denkbare Interesse Dritter an den personenbezogenen Daten und der Aufwand, der betrieben werden müßte, um den Personenbezug wieder herzustellen, im Vergleich mit dem notwendigen Aufwand, um dieselbe Information auf andere Weise zu erlangen.

Im Einzelfall kann die Anwendung dieses Grundsatzes schwierig sein. Dem Verzicht auf die theoretische Lückenlosigkeit der Anonymisierung entspricht ein geringes, aber eben nicht zu leugnendes praktisches Risiko, einmal falsch zu entscheiden. Dennoch meine ich daran festhalten zu müssen, um den Datenschutz nicht durch überzogene Forderungen in Mißkredit zu bringen und damit langfristig die Befolgung von Datenschutzvorschriften zu gefährden. Ich habe deshalb die Landesbeauftragten gebeten, zu Entscheidungen der Statistischen Landesämter Stellung zu nehmen. Auf die Bitte des Bundesministers des Innern, Daten für das Informationssystem über Krebsmortalitätsdaten und Krebscharakteristika bereitzustellen, hatten einige Landesämter eine hinreichende Anonymisierung m. E. zu Unrecht verneint, wenn eine bestimmte Krebsart ausgewiesen ist, die während eines Jahres in einem Landkreis nur einmal aufgetreten war. Das sensitivste Datum, nämlich daß eine bestimmte Person in einem Landkreis an einer bestimmten Krebsart gestorben ist, muß dem Dritten in diesem Fall bereits bekannt sein, wenn er (weitere) personenbezogene Daten zur Kenntnis nehmen will. Wenn man keinen Bruch der ärztlichen Schweigepflicht unterstellen will, kann er diese Daten nur aus dem nächsten Umfeld des Betroffenen erfahren haben. Dann aber kann wohl davon ausgegangen werden, daß ihm auch die anderen Daten (Sterbealter nach Fünf-Jahres-Gruppen, Geschlecht, Sterbeort — nur ob innerhalb oder außerhalb eines Krankenhauses —, Staatsangehörigkeit — deutsch oder nichtdeutsch —) bekannt sind. Jedenfalls wäre m. E. die Annahme völlig unrealistisch, jemand, der sich für diese Angaben interessiert, könnte die Anstrengung unternehmen, sie durch De-Anonymisierung aus dem erwähnten Informationssystem zu erlangen. Ebenso irreal erscheint mir die Gefahr personenbezogener Zufallsfunde.

Eine Aufgabe der nächsten Zeit ist die Überwachung der praktischen Durchsetzung des neuen § 11 Abs. 7 Bundesstatistikgesetz, der die statistischen Ämter verpflichtet, unter bestimmten Voraussetzungen die Identifizierungsmerkmale der Auskunftspflichtigen zu löschen.

### 4.4 Anforderungen an ein Bundesarchivgesetz

Die Bemühungen um ein Bundesarchivgesetz, auf dessen Erforderlichkeit ich in meinem 2. Tätigkeitsbericht (Nr. 2.1.5, S. 14) hingewiesen hatte, sind fortgeschritten. Auch in den Ländern werden Archivgesetze angestrebt. Die Landesbeauftragten für den Datenschutz und ich haben sich deshalb in dem gemeinsamen Arbeitskreis Archivwesen mit der Formulierung von Anforderungen des Datenschutzes an ein Archivgesetz befaßt. Diese Arbeiten sind fast abgeschlossen.

Ein Archivgesetz muß den Datenschutz als Schutz des allgemeinen Persönlichkeitsrechts und der Menschenwürde in einer Weise sicherstellen, die die notwendige Arbeit der Archive möglichst wenig beeinträchtigt. Denn Archive sind einerseits, wie zu Recht gesagt wird, das „notwendige Gedächtnis einer Nation". Andererseits besteht die Gefahr, daß auch solche Angaben über den Bürger nicht in Vergessenheit geraten, die für ihn ungünstig sind oder zu seinem Nachteil verwendet werden können.

Folgende Grundsätze, die in weiteren Beratungen noch zu konkretisieren und zu ergänzen sind, sollten deshalb beim Erlaß eines Archivgesetzes berücksichtigt werden:

a) Aufgabe des Gesetzes ist es, die schutzwürdigen Belange aller Bürger zu wahren, über die die ar-

chivierten Vorgänge Informationen liefern. Geboten ist ein abgestufter Schutz:

Er muß z. B. für den von einer Entscheidung betroffenen Bürger umfassender sein als für den entscheidenden Beamten. Ein Archivgesetz muß die angesprochenen Probleme umfassend regeln, unabhängig von der Frage, ob die Daten, über deren Verwendung zu entscheiden ist, in Akten, in Dateien oder in anderen Datenträgern enthalten sind. Es soll der schnellen Entwicklung der Informationstechnik Rechnung tragen.

b) Das Gesetz soll die Rechte der Betroffenen, die Pflichten der Archive und die Modalitäten der Benutzung festlegen. Dabei ist nach den verschiedenen Arten von Unterlagen zu unterscheiden: Klassisches Archivgut (archivwürdige Vorgänge, die von der abgebenden öffentlichen Stelle nicht mehr benötigt werden), Zwischen-Archiv-Vorgänge (Vorgänge, die von der abgebenden öffentlichen Stelle nicht mehr regelmäßig benötigt werden), ausgelagerte Verwaltungsvorgänge (Vorgänge, die von der abgebenden öffentlichen Stelle noch benötigt werden), privates Archivgut.

c) Das Gesetz sollte die unbefristete Aufbewahrung von Unterlagen nur dann gestatten, wenn ihre Archivwürdigkeit ausdrücklich festgestellt wurde. Die Vorgänge von öffentlichen Stellen sollen grundsätzlich nur ausschnittweise archiviert werden, weil vollständige Bestände die Gefahr eines Mißbrauchs erhöhen. Für die Beurteilung der Archivwürdigkeit trägt das Archiv die Verantwortung. Die Archivierung ist unzulässig, wenn die Beeinträchtigung schutzwürdiger Belange von Betroffenen (z. B. Resozialisierungschancen von Straftätern) zu befürchten ist. Deshalb sind bereits für den Zeitpunkt der Archivierung Entscheidungen über besondere Nutzungsbeschränkungen und Schutzmaßnahmen vorzuschreiben.

Auch zur Archivierung im Auftrag dürfen Archive z. B. private Vorgänge nur unter Bedingungen übernehmen, die nicht offenkundig schutzwürdige Belange Betroffener beeinträchtigen.

Ein generelles Archivierungsverbot für unrichtige Daten empfehle ich nicht, weil die Tatsache einer unrichtigen Datenverarbeitung historisch bedeutsam und deshalb archivwürdig sein kann. Unrichtige Daten dürfen jedoch nur zusammen mit einem Berichtigungsvermerk archiviert werden.

d) Das Gesetz soll dem Betroffenen ein Einsichtsrecht, hilfsweise ein Auskunftsrecht, und ein Gegendarstellungsrecht einräumen.

e) Für die Benutzung des Archivgutes muß das Gesetz Voraussetzungen und Bedingungen aufstellen, die gewährleisten, daß schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden. So ist sicherzustellen, daß die Vorgänge nicht von abgebenden Stellen unter Umgehung der für sie geltenden Löschungs- und Sperrfristen benutzt werden können.

Für die unterschiedlichen Arten der Benutzung (z. B. wissenschaftliche Nutzung, journalistische Nutzung, Nutzung zu Verwaltungszwecken) sind differenzierende Regelungen notwendig.

Das Gesetz soll eine allgemeine Sperrfrist vorsehen. Die Archive sollen das Recht erhalten, die Frist zu verlängern. Für bestimmte Archivvorgänge oder Nutzungen (z. B. Nutzung für ein bestimmtes zeitgeschichtliches Forschungsvorhaben) könnte das Gesetz dem Archiv gestatten, die Nutzung schon vor Ablauf der gesetzlichen Sperrfrist zuzulassen, wenn durch Auflagen oder Bedingungen die Beeinträchtigung schutzwürdiger Belange von Betroffenen im Einzelfall ausgeschlossen werden kann.

f) Ein Archivgesetz muß ausreichende Vorschriften über technische und organisatorische Maßnahmen zum Schutz vor einem Mißbrauch des Archivgutes, vergleichbar dem § 6 Bundesdatenschutzgesetz, enthalten.

## 4.5 Sicherheitsbereich

### 4.5.1 Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen (KpS), Dateien-Richtlinien für das BKA und bundeseinheitliche Richtlinien über erkennungsdienstliche Behandlung

a) Zum 1. März 1981 wurden für das Bundeskriminalamt die Richtlinien über kriminalpolizeiliche personenbezogene Sammlungen und die Dateien-Richtlinien in Kraft gesetzt. Sie stellen unbestreitbar eine erhebliche Verbesserung gegenüber dem vorher bestehenden faktischen Zustand dar. Es kommt nun allerdings darauf an, die Richtlinien auch wirklich umzusetzen und konsequent durchzuführen. Dies ist leider keineswegs selbstverständlich. Das zeigte schon die von mir im Juni 1979 durchgeführte Prüfung im Bereich Daktyloskopie: Damals mußte ich feststellen, daß nicht nur die früher geltende 25jährige Löschungsfrist nicht eingehalten worden war, sondern daß man bei der Verformelung von Fingerabdrücken auch die KpS-Richtlinien in der Erstfassung von 1979 nicht berücksichtigt hatte (vgl. 2. TB, Nr. 2.8.1, S. 47). Inzwischen sind diese Versäumnisse allerdings weitgehend behoben.

Ich werde laufend durch stichprobenartige Kontrollen prüfen, ob die den KpS-Richtlinien nicht mehr entsprechenden Altbestände in allen Bereichen nunmehr zügig vernichtet bzw. gelöscht werden.

Besonderer Wert ist auch darauf zu legen, daß für die verschiedenen Dateien Errichtungs- bzw. Feststellungsanordnungen entsprechend Nr. 10 und 11 der Dateien-Richtlinien erlassen werden. Tatsächlich gibt es erst seit einigen Monaten Entwürfe für eine Anzahl solcher Anordnungen.

Das Material dafür hätte bei Beachtung von § 15 Satz 2 Nr. 1 BDSG (Pflicht zur Erstellung von Da-

teienübersichten) bereits seit langem vorliegen müssen.

Erfreulich ist dagegen die Tatsache, daß die gebotene Trennung der Speicherung von Unterlagen nach § 3 Ausländergesetz von solchen, die aus Gründen der Strafverfolgung oder Gefahrenabwehr angefertigt wurden, jetzt endlich durchgeführt wird (vgl. 3. TB, Nr. 3.12.2.1, S. 49). Die Pflicht hierzu folgt nunmehr auch aus Nr. 4.2.4 der Dateien-Richtlinien, die aufgrund meiner Anregungen entsprechend formuliert wurde.

b) Unabhängig von den vorstehenden Bemerkungen können die Richtlinien in der jetzigen Fassung nicht voll befriedigen. Die Datenschutzbeauftragten haben in einer gemeinsamen Stellungnahme vor der endgültigen Verabschiedung im Januar 1981 auf eine Reihe von verbesserungsbedürftigen Punkten hingewiesen. Sie betreffen vor allem

— die Zulässigkeit der Speicherung von Daten über Geschädigte und „andere Personen, wenn zureichende tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß dies zur Aufklärung oder vorbeugenden Bekämpfung schwerwiegender Straftaten, zur Ergreifung von zur Festnahme gesuchten Personen oder zur Abwehr einer im einzelnen Fall bestehenden erheblichen Gefahr erforderlich ist" (Nr. 4.2.11 der Dateien-Richtlinien);

— die Übermittlung an ausländische Stellen (zu den hier bestehenden Problemen im Zusammenhang mit Interpol s. oben 2.12.7, S. 26f.);

— den Abgleich von Dateien;

— die noch unbefriedigenden Löschungsfristen in verschiedenen Fällen.

Ich habe darüber hinaus in meinem Anschreiben an den Bundesminister des Innern anläßlich der Übermittlung der gemeinsamen Erklärung zusätzlich auf folgende Punkte hingewiesen, die m. E. dringend regelungs- oder verbesserungsbedürftig sind:

— die grundsätzliche Frage der Rechtsgrundlage für polizeiliche Beobachtung und Rasterfahndung sowohl im präventiven wie auch im Strafverfolgungsbereich (hierzu auch 3. TB, Nr. 3.11.2.4, S. 50f. und Nr. 3.11.2.5, S. 52);

— die jetzige Regelung nach den KpS- und/oder Dateien-Richtlinien zur Übermittlung polizeilicher Daten an Nachrichtendienste (Ziff. 3.5.4 und 5 der KpS- bzw. 5.5.4 und 5 der Dateien-Richtlinien), die m. E. mit dem geltenden Recht jedenfalls in dieser Pauschalität nicht vereinbar ist. Dieses Problem ist im Zusammenhang mit der Problematik der Amtshilfe bzw. informationellen Zusammenarbeit zwischen Polizeibehörden und Nachrichtendiensten zu sehen (vgl. 3. TB, Nr. 3.11.1.1, S. 45f. und oben 2.14 und 2.15.3).

Zur Rasterfahndung hatte ich bereits im Frühjahr 1980 die Anfrage an den Bundesminister des Innern gerichtet, welche Rechtsgrundlagen dafür in Anspruch genommen werden. Die Antwort — gemeinsam von Bundesinnenministerium und Bundesjustizministerium — ist mir Mitte Dezember 1981 zugegangen. Meine Rechtsbedenken werden in diesem Schreiben gar nicht erörtert; dem Hauptproblem, ob nämlich § 163 StPO als Rechtsgrundlage für die als Rasterfahndung bezeichneten Maßnahmen der Strafverfolgung ausreicht, wird mit folgenden Sätzen ausgewichen:

„Ermittlungen, die als ‚Rasterfahndung' bezeichnet werden, können sowohl hinsichtlich des Zwecks als auch nach Art und Umfang höchst verschieden und damit unterschiedlich zu werten sein. Soweit Maßnahmen auf die Aufklärung einer Straftat abzielen, richtet sich ihre Zulässigkeit nach den Vorschriften der Strafprozeßordnung. Eine generelle Aussage über Zulässigkeit einer sogenannten ‚Rasterfahndung' ist nicht möglich. Es muß vielmehr — wie auch sonst — in jedem Einzelfall geprüft werden, ob gerade die beabsichtigte Maßnahme nach dem Gesetz zulässig ist."

Das trifft zwar abstrakt zu. Welche Vorschriften dies nun aber sein sollen, wird nicht gesagt. Ich halte die Frage daher — in Übereinstimmung mit den Datenschutzbeauftragten der Länder — weiterhin für dringend klärungsbedürftig. § 163 StPO wird übrigens von den beiden Ministerien nach wie vor als hinreichende Ermächtigungsgrundlage für die polizeiliche Beobachtung zum Zwecke der Strafverfolgung angesehen.

Die Vorbehalte in der gemeinsamen Erklärung der Datenschutzbeauftragten und in meinem Anschreiben an den Bundesminister des Innern zeigen, daß die Richtlinien aus datenschutzrechtlicher Sicht noch verbesserungsbedürftig sind. Es ist daher zu hoffen, daß der Bundesminister des Innern sich an seine Absichtserklärung hält, weitere Verbesserungen nach ersten Erfahrungen — etwa nach Ablauf eines Jahres — vorzubereiten.

c) Bereits vor knapp zwei Jahren habe ich den BMI auf die Notwendigkeit der Überarbeitung der *bundeseinheitlichen Richtlinien über ed-Behandlung* aufmerksam gemacht (vgl. 3. TB, Nr. 3.11.2.1, S. 49). Ein mir vor kurzem zugeleiteter Entwurf der hiermit von der Innenministerkonferenz beauftragten Arbeitsgemeinschaft der Kriminalpolizeien des Bundes und der Länder zeigte auch gewisse Verbesserungen, die einen Teil meiner Anregungen berücksichtigen. Das gilt insbesondere für den — gesetzlich ohnehin gebotenen — Ausschluß der ed-Behandlung zur vorbeugenden Bekämpfung bloßer Ordnungswidrigkeiten sowie das Verbot einer zentralen Speicherung beim BKA von Unterlagen, die nur zur Aufklärung aktueller Ordnungswidrigkeiten oder zur aktuellen Identitätsfeststellung dienen (wenn keine Anhaltspunkte für Wiederholungsgefahr bestehen). Der erwähnte Entwurf enthält aber noch eine Reihe von Mängeln und Unklarheiten, die beseitigt werden müssen.

Völlig ungenügend ist der Entwurf noch in einem entscheidenden Punkt: wenn die Voraussetzun-

gen für weitere Aufbewahrung vorliegen, sollen die erkennungsdienstlichen Unterlagen ohne Unterscheidung nach überregionaler oder nur regionaler Bedeutung zentral gespeichert werden. Was für den Kriminalaktennachweis eingeräumt wurde, soll hier also nicht gelten. Ich halte dies aus den bereits genannten Gründen (s. o. 2.12.6) für nicht annehmbar. In meiner abschließenden Stellungnahme habe ich den Bundesminister des Innern erneut darauf aufmerksam gemacht und eine entsprechende Ergänzung der Richtlinien vorgeschlagen, die mit den Datenschutzbeauftragten der Länder abgestimmt ist.

#### 4.5.2 Bereichsspezifische Gesetzgebungsvorhaben

Ich habe bereits häufig darauf hingewiesen, daß die Rechtsgrundlagen der Datenverarbeitung im Sicherheitsbereich in verschiedener Hinsicht unklar, unsicher oder zu pauschal sind (vgl. insbesondere 3. TB, Nr. 3.11.1.1, S. 45 ff.). Rechtsstaaliche Grundsätze, insbesondere der verfassungsmäßige Vorbehalt des Gesetzes für Eingriffe in Rechte des Einzelnen und das Verhältnismäßigkeitsprinzip bedingen eine Reihe von Klarstellungen, Eingrenzungen oder Ergänzungen in Gesetzesform.

In manchen Bereichen kann die Voraussetzung rechtmäßiger Datenverarbeitung nach dem BDSG, daß die jeweilige Aktivität zur rechtmäßigen Aufgabenerfüllung erforderlich ist, gar nicht erfüllt werden, weil keine Rechtsgrundlage für die entsprechenden informationellen Eingriffe in die Rechtssphäre der Betroffenen vorhanden ist. Dazu zählen auch manche Maßnahmen der Strafverfolgung und der Gefahrenabwehr, die aus polizeilicher Sicht inzwischen als unverzichtbar gelten.

Die Praxis hilft sich mit umstrittenen Konstruktionen wie der sogenannten „Schwellentheorie", wonach alle die Maßnahmen der Strafverfolgung zulässig sein sollen, bei denen die Intensität des Eingriffs in Betroffenenrechte unterhalb der Schwelle der von der StPO ausdrücklich zugelassenen Maßnahmen liegt (so die Rechtsansicht der Bundesregierung zur polizeilichen Beobachtung, vgl. oben 4.5.1). Damit wird § 163 StPO entgegen der bisher fast allgemein vertretenen Auffassung doch zu einer strafprozessualen General-Befugnisklausel (vgl. dazu 3. TB, Nr. 3.11.2.5, S. 52, m.w.N.).

Für die Nachrichtendienste gibt es bisher überhaupt nur ganz wenige Rechtsnormen, und die vorhandenen Gesetzesbestimmungen etwa über die Verfassungsschutzämter enthalten zu einem erheblichen Teil nur unbestimmte Allgemeinklauseln.

Freilich setzt sich zunehmend die Einsicht durch, daß diese Probleme nicht auf Dauer ungelöst bleiben können und daß die bisher gewählten Hilfskonstruktionen keinen gleichwertigen Ersatz für klare Gesetzesnormen darstellen. So hat der Bundesminister des Innern angekündigt, Regelungen über die wesentlichen Probleme der Amtshilfe des BGS für die Nachrichtendienste, die jetzt in den neuen Richtlinien geregelt sind (vgl. oben 2.15.3), nach einer gewissen Erprobungszeit in die Form eines Gesetzentwurfes zu bringen. Auch Änderungen des Bundesgesetzes über den Verfassungsschutz und des BGS-Gesetzes werden erwogen. Der BMI erkennt damit — wenn auch zum Teil auf der Grundlage einer anderen Rechtsmeinung — die Notwendigkeit und Bedeutung einer gesetzlichen, d. h. parlamentarischen Regelung dieser für das Verhältnis von Staat und Bürger wesentlichen Fragen an.

Über das hinaus, was unter dem Stichwort „Amtshilfe" in der Öffentlichkeit diskutiert wird, bedarf noch eine Reihe weiterer Gegenstände zumindest der Klarstellung durch Gesetz. Einiges davon ist bei den Ausführungen zu den KpS- und Dateien-Richtlinien (vgl. oben 4.5.1) erwähnt worden. Es sollte überlegt werden, ob und in welchem Umfang Grundsätze der beiden Richtlinien in Gesetzesform zu verankern wären. Manche Streitpunkte sind übrigens bisher erst wenig erörtert worden, so die Schwierigkeiten, die sich aus der Zuständigkeitsaufteilung auf Polizei und Verfassungsschutz ergeben. Als inhaltliche Orientierung sollte der Alternativentwurf einheitlicher Polizeigesetze des Bundes und der Länder sorgfältig ausgewertet werden.

### 4.6 Finanzverwaltung

In der Finanzverwaltung war im Berichtsjahr relativ wenig Bereitschaft erkennbar, auf Überlegungen über verstärkten Datenschutz einzugehen. Über Schwierigkeiten, die datenschutzrechtliche Kontrolle beim Zollkriminalinstitut durchzusetzen, ist an anderer Stelle berichtet (oben 2.18.3). Darüber hinaus besteht eine Meinungsverschiedenheit mit dem Bundesminister der Finanzen darüber, inwieweit trotz der Ausnahmeklausel des § 13 Abs. 2 BDSG den Betroffenen Auskunft über ihre bei Steuerfahndungsbehörden gespeicherten Daten erteilt werden kann. Ich habe auf die KpS-Richtlinien (s. oben 4.5.1) hingewiesen, nach denen die Polizei zur Auskunftserteilung verpflichtet ist, wenn das Interesse des Betroffenen an Offenlegung das öffentliche Interesse an der Geheimhaltung überwiegt. Der Bundesminister der Finanzen verweist demgegenüber, ohne auf diesen Vergleich einzugehen, auf den Wortlaut des § 13 Abs. 2 BDSG und erklärt, durch Auskünfte an die Betroffenen über die zu ihrer Person gespeicherten Daten würde die öffentliche Sicherheit beeinträchtigt. Damit kann ich mich nicht zufrieden geben: bei aller Anerkennung eines berechtigten Geheimhaltungsinteresses der Finanzverwaltung ist die pauschale Berufung auf die öffentliche Sicherheit angesichts der Tatsache, daß Sicherheitsbehörden im eigentlichen Sinne (bis hin zu den Nachrichtendiensten) im Einzelfall oder, wie die Polizei, sogar in größerem Umfang Auskünfte an die Betroffenen erteilen, alles andere als überzeugend. Die Finanzverwaltung sollte zumindest nachträgliche Auskünfte an die Betroffenen (nach Wegfall der Zweckgefährdung) in Erwägung ziehen.

### 4.7 Novellierung des BDSG

Die Bundesregierung hat in der Regierungserklärung vom 24. November 1980 eine Novellierung des BDSG für die laufende Legislaturperiode angekün-

digt. Seitdem wird das Thema auf den verschiedensten Ebenen, auf Fachtagungen, in Kreisen der Gesetzesanwender, der Wissenschaft, der Politik und auch der Kontrollorgane diskutiert. Ein Regierungsentwurf liegt noch nicht vor, doch werde ich schon jetzt häufig nach meinen Erwartungen an eine BDSG-Novellierung gefragt. Ich rechne auch damit, im Gesetzgebungsverfahren entsprechend meinem Beratungsauftrag zu gesetzgeberischen Möglichkeiten der Verbesserung des Datenschutzes gehört zu werden. Um meine Vorstellungen schon frühzeitig in die Diskussion einzubringen und um den mit der Gesetzesvorbereitung befaßten Stellen Hilfen zu geben, habe ich die aus meiner Sicht zu stellenden Forderungen an eine BDSG-Novelle in einem umfangreichen Papier niedergelegt. Diese Ausarbeitung habe ich dem Bundesminister des Innern zugeleitet und später unter dem Titel „Ziele und Mittel des Datenschutzes — Forderungen zur Novellierung des Bundesdatenschutzgesetzes" als Fachveröffentlichung herausgegeben in der Absicht, meine Überlegungen nicht nur den an der Gesetzgebungsarbeit unmittelbar Beteiligten, sondern darüber hinaus auch einer interessierten Öffentlichkeit zugänglich zu machen.

Um Wiederholungen zu vermeiden, verzichte ich an dieser Stelle auf eine Inhaltsangabe dieser Schrift. Es kommt jetzt darauf an, die dort dargestellten Überlegungen in handhabbare Gesetzesformulierungen umzusetzen oder zumindest so weit zu konkretisieren, daß sie unschwer als Gesetzestexte ausformuliert werden können. Ich habe dies in einer weiteren Stellungnahme gegenüber dem Bundesminister des Innern im August 1981 versucht.

Die Überlegungen sind in der Folgezeit weiter gereift; unter Berücksichtigung der zwischenzeitlich hinzugewonnenen Erkenntnisse führe ich im folgenden die wichtigsten Punkte und Vorschläge auf, die nach meiner Ansicht bei einer BDSG-Novellierung geregelt werden sollten und könnten:

a) Datenschutzbegriff

Die in der Aufgabenbeschreibung des Datenschutzes (§ 1 Abs. 1 BDSG) verwendete Mißbrauchsformel ist insofern irreführend, als nach allgemeinem Sprachgebrauch darunter nur absichtliches Fehlverhalten zum Nachteil anderer oder zum eigenen Vorteil verstanden werden könnte. Betrachtet man indessen die Ausgestaltung des Datenschutzes in den weiteren Vorschriften des Gesetzes, wird sogleich deutlich, daß es beim Datenschutz um die Rechte des einzelnen und um die Wahrung seiner schutzwürdigen Belange bei der Verarbeitung personenbezogener Daten geht, um dementsprechend ausgestaltete Zulässigkeitsregelungen für die Datenverarbeitung und um die angemessene Verteilung der Informationen entsprechend der Zuständigkeitsordnung der Staatsorganisation.

Soll § 1 Abs. 1 BDSG als Auslegungshilfe dienen, muß in der Beschreibung der Aufgabe „Datenschutz" — ebenso wie in der Gesetzesüberschrift — die Mißbrauchsformel entfernt und deutlicher, auch sprachlich besser, zum Ausdruck gebracht werden, daß Rechte und schutzwürdige Belange des Bürgers zentraler Gegenstand des Datenschutzes sind und durch Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten nicht verletzt oder beeinträchtigt werden dürfen.

b) Dateibezug

Daß die Verarbeitung personenbezogener Daten vom BDSG — von wenigen Ausnahmebestimmungen abgesehen — nur geregelt wird, wenn sie in Dateien gespeichert bzw. aus Dateien übermittelt werden, ist bei den Betroffenen weitgehend auf Unverständnis gestoßen. Insbesondere wird nicht verstanden, warum die Übermittlung aus Akten und anderen Aufzeichnungen an Dritte nicht vom BDSG geregelt wird und der Betroffene insoweit keinen Auskunftsanspruch hat. Bei Kontrollen hat sich gelegentlich ein auffälliges Mißverhältnis zwischen den auf das BDSG gestützten Sicherungsmaßnahmen für oft „harmlose" Datei-Daten und mangelhafter Sicherung von Aktenbeständen mit zuweilen sehr weitgehenden Aussagen über den Betroffenen gezeigt.

Zwar ist ein zweckmäßiges Abgenzungskriterium bei einigen BDSG-Vorschriften (z. B. denen über die Auskunftserteilung), die überhaupt nur auf strukturierte Datensammlungen angewendet werden können, unverzichtbar. Ich meine allerdings, daß andere Vorschriften des BDSG ohne Einbuße an Praktikabilität auch für personenbezogene Daten gelten können, die in Akten geführt werden (z. B. diejenigen über die Zulässigkeit der Datenverarbeitung). Meinen ursprünglichen Gedanken, für jede Vorschrift oder für bestimmte Gruppen von Vorschriften jeweils besonders festzulegen, ob der Dateibezug gelten soll oder nicht, möchte ich jedoch zunächst nicht weiter verfolgen, weil die gesetzestechnische Lösung schwierig wäre und den Gesetzesanwendern möglicherweise zu kompliziert erschiene. Als Ersatzlösung erwarte ich allerdings, daß

— der Dateibegriff so umformuliert und erweitert wird, daß bisher strittige Grenzfälle eindeutig in den Anwendungsbereich des Gesetzes einbezogen werden,

— die sogenannten internen Dateien im öffentlichen Bereich voll den BDSG-Vorschriften unterworfen werden und im nicht-öffentlichen Bereich eine Reihe geeigneter Vorschriften (insbesondere diejenigen über das Datengeheimnis und die Aufsicht) auf interne Dateien für anwendbar erklärt werden und

— klargestellt wird, daß die Regelung der Datenerhebung und der Kontrollbefugnisse des Bundesbeauftragten und der Aufsichtsbehörden hinsichtlich der „anderen Vorschriften über den Datenschutz" nicht auf Dateien beschränkt ist.

c) Erhebung von Daten

Schon in meinem zweiten Tätigkeitsbericht (siehe dort unter 4.3.2, Seite 62) habe ich zu erwägen gegeben, eine Bestimmung in das BDSG aufzunehmen, wonach personenbezogene Daten grundsätzlich beim Betroffenen selbst erhoben werden sollten. An

diesem Grundsatz halte ich fest; Ausnahmen sollten nur dann gemacht werden, wenn die Nutzung vorhandener Informationen oder eine Befragung Dritter den Interessen des Betroffenen dient oder aus anderen überwiegenden Interessen erforderlich ist.

Durch die Art und Weise der Erhebung dürfen schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Hier denke ich insbesondere an mögliche unfaire Befragungsmethoden von Auskunfteien oder Detekteien, aber auch an Befragungen des Betroffenen selbst unter Vorspiegelung vermeintlicher Vorteile oder falscher Tatsachen. Die Erhebung von Daten beim Betroffenen sollte in Anlehnung an die Zulässigkeitsvoraussetzung für sonstige Phasen der Datenverarbeitung an die Bedingung geknüpft werden, daß eine Rechtsvorschrift sie erlaubt oder der Betroffene die Angaben freiwillig macht. Sofern eine Auskunftspflicht besteht, ist dem Betroffenen die zugrundeliegende Rechtsvorschrift zu nennen, im Falle freiwilliger Angaben muß er über deren Verwendungszweck und über mögliche Folgen einer Nichtbeantwortung in verständlicher Form aufgeklärt werden. Eine eigentlich selbstverständliche, aber gleichwohl möglichst im Gesetz zu verankernde Folge unzulässiger Datenerhebung sollte ein Verarbeitungs- und Nutzungsverbot sein sowie eine Löschungspflicht, wenn unzulässig erhobene Daten bereits gespeichert sind.

d) Einwilligung

Ähnliche Verfeinerungen der Aufklärungspflicht gegenüber dem Betroffenen wie bei der Datenerhebung sollten auch für die Einwilligung in sonstige Verarbeitungsformen vorgesehen werden. Wenn die Einwilligung das Selbstbestimmungsrecht des Betroffenen über seine Daten im gesetzesfreien Raum konkretisiert, so muß er Ausmaß, Bedeutung und Konsequenzen seiner Entscheidung klar erkennen können. Ich halte es deswegen für notwendig, die datenverarbeitenden Stellen gesetzlich zu verpflichten, den Betroffenen über Gegenstand, Inhalt und Umfang der beabsichtigten Verarbeitung, insbesondere die Art der Daten, im Falle von Datenübermittlungen die Empfänger, den Verwendungszweck, die Dauer der Aufbewahrung der Daten sowie mögliche Folgen einer Verweigerung der Einwilligung zu informieren.

Nicht selten ist die irrige Meinung anzutreffen, daß alle Vorschriften des Datenschutz- und Informationsrechts unbeachtet bleiben können, wenn die Einwilligung des Betroffenen vorliegt; sie zu erlangen, wird deshalb als der bequemere Weg angesehen, der es ermöglicht, lästigen gesetzlichen Auflagen zu entgehen und vorgeschriebene Abwägungen zu unterlassen. Ich meine, daß einem solchen Vorgehen schon allgemeine Grundsätze von Treu und Glauben entgegenstehen. Der Gesetzgeber sollte durch eine geeignete Formulierung im Gesetzestext — etwa in Anlehnung an das Gesetz über Allgemeine Geschäftsbedingungen — sicherstellen, daß die Einwilligung nicht alle denkbaren Verarbeitungen und Nutzungen personenbezogener Daten legitimiert und von den im BDSG festgelegten Grundsätzen des Datenschutzes nicht völlig dispensieren kann.

In diesen Zusammenhang gehört auch der Sachverhalt, daß zunächst die Einwilligung des Betroffenen verlangt wird und, obwohl sie verweigert wird, die Datenverarbeitung schließlich dennoch stattfindet, weil sie sich — vielleicht eingeschränkt oder unter einengenden Bedingungen — auf eine Erlaubnisvorschrift stützen läßt. Hier muß sichergestellt sein, daß der Betroffene, der sich möglicherweise auf die Wirkung seiner Verweigerung verläßt, über die Rechtsvorschrift aufgeklärt wird.

e) Zweckbindung der Daten

Das *Zweckbindungsprinzip* ist im geltenden BDSG nur unzureichend ausgestaltet. Seine stärkere Betonung ist im Interesse des Betroffenen zunächst für den Fall geboten, daß die Daten dem Betroffenen selbst auf freiwilliger Grundlage unter Hinweis auf einen bestimmten Zweck abverlangt wurden; der Betroffene muß sich hier regelmäßig darauf verlassen können, daß sie nur für den ihm bekannten Zweck verwendet werden. Ferner sollte die strenge Zweckbindung — entsprechend dem Vorschlag der CDU/CSU-Fraktion in der Drucksache 8/3608 — für nach § 11 und § 24 BDSG an nicht-öffentliche Stellen übermittelte Daten gelten. Darüber hinaus halte ich es für notwendig, die Zweckbindung als allgemeines Prinzip des Datenschutzrechts im Gesetz niederzulegen. Eine solche Vorschrift würde den Ausnahmecharakter der Übermittlungsvorschriften, deren Anwendung regelmäßig eine Zweckentfremdung der Daten bedeutet, hervorheben. Freilich verkenne ich nicht, daß Datenübermittlungen im Rahmen der Amtshilfe und aufgrund spezieller Bestimmungen notwendig, ja unverzichtbar sein können; sie können auch im Interesse des Betroffenen selbst liegen. Doch sollte — entsprechend Nr. 9 der Datenschutz-Leitlinien der OECD — zumindest eine Beschränkung von Mehrfachnutzungen auf solche Zwecke vorgesehen werden, die mit den ursprünglichen Zwecken „vereinbar" sind.

Mit einer gesetzlichen Ausformung des Zweckbindungsprinzips ließe sich ein Verbot der Herstellung von *Persönlichkeitsbildern* verbinden, genauer: der mit diesem Effekt in automatisierten Verfahren vorgenommenen Zusammenführung von Daten, die aus unterschiedlichen Lebensbereichen eines Betroffenen herrühren. Ähnlich riskante Verarbeitungen personenbezogener Daten, wie solcher über politische oder religiöse Anschauungen, sollten nur mit Einwilligung des Betroffenen oder aufgrund besonderer gesetzlicher Vorschriften (also außerhalb des BDSG) erlaubt werden. Datenverarbeitung im Rahmen von Mitgliedschaftsverhältnissen durch politische Vereinigungen oder Religionsgemeinschaften oder zu karitativen Zwecken muß allerdings erlaubt bleiben, ebenso Datenverarbeitung zu Zwecken der wissenschaftlichen Forschung.

f) Direktabfrage

Als besonders problematisch hat sich in der Kontrollpraxis die Beurteilung von Verfahren der Direktabfrage von Datenbeständen (On-line-Anschlüs-

sen) erwiesen. Gemäß § 2 Abs. 2 Nr. 2 BDSG (Übermittlungsbegriff) gilt eine Datensammlung bereits als übermittelt, wenn sie zur Einsichtnahme, namentlich zum Abruf bereitgehalten wird. Damit setzt z. B. die Einrichtung eines Abfrageterminals voraus, daß die Übermittlung der Gesamtheit der Daten, auf die damit zugegriffen werden kann, erforderlich und dadurch zulässig ist. Die Erforderlichkeit der Übermittlung dieser Gesamtheit dürfte indessen allenfalls in extremen Ausnahmefällen gegeben sein, im Regelfall decken die Erlaubnisvorschriften nur die tatsächlich erfolgenden einzelnen Abrufe oder Einsichtnahmen. Damit läuft die strenge Interpretation des Übermittlungsbegriffs des BDSG auf die grundsätzliche Unzulässigkeit von Direktabfrageverfahren hinaus. Dies dürfte vom Gesetzgeber nicht gewollt gewesen sein. Ich trete deshalb für eine klarstellende Neufassung des Übermittlungsbegriffs im Gesetz ein. Er muß so umformuliert werden, daß die in der Zulässigkeitsvorschrift für die Datenübermittlung verlangte Erforderlichkeit sich auf den einzelnen Abruf bezieht. Ergänzend dazu sind gesetzliche Rahmenbedingungen für die allgemein als riskanter als die einzelfallbezogene Datenübermittlung angesehene On-line-Verbindung zu schaffen.

Mein Vorschlag geht dahin, die Zulässigkeit eines automatisierten Abrufverfahrens davon abhängig zu machen, daß die zum Abruf bereitgehaltenen Daten ihrer Art nach für die Empfänger erforderlich sind und das Bereithalten zum jederzeitigen Abruf unter Berücksichtigung der schutzwürdigen Belange der Betroffenen und der Aufgaben der beteiligten Stellen angemessen ist. Damit wäre sichergestellt, daß eine Interessenabwägung schon vor Eröffnung der Direktabfragemöglichkeit stattfindet. Zu fordern sind ferner die beteiligten Stellen verpflichtende Festlegungen der jeweils obersten Dienstbehörden über die näheren Einzelheiten, insbesondere die verfügbaren Daten, die Zugriffsberechtigung, Verwendungszwecke, Maßnahmen zur Sicherheit und Kontrolle, letzteres auch in Bezug auf die Erforderlichkeit des einzelnen Abrufs. Angesichts des mit der Einrichtung von On-line-Anschlüssen verbundenen Gefährdungsrisikos halte ich eine obligatorische Unterrichtung des Bundesbeauftragten für den Datenschutz für notwendig. Dieser kann im Einzelfall dann, wenn ihm dies als geboten erscheint, auf strengere Sicherungen, z. B. auch auf den Erlaß von speziellen Rechtsvorschriften hinwirken.

In Bereichen, in denen die Datenverarbeitung Eingriffscharakter hat, insbesondere beim Datenaustausch zwischen Sicherheitsbehörden mit unterschiedlichen Aufgaben oder zwischen Sicherheitsbehörden und anderen Stellen, ist darüber hinaus stets eine ausdrückliche gesetzliche Zulassung der Direktabfrage zu fordern.

g) Dateistatuten

Die Generalklauseln des BDSG, die schon vor seinem Inkrafttreten als zu weitgehend kritisiert wurden, haben nicht zu der ursprünglich befürchteten Rechtsunsicherheit geführt und sich in der Praxis als flexible Auffangvorschriften für die Bereiche, in denen Spezialrecht fehlt, als brauchbar erwiesen. Die für jede DV-Anwendung notwendige Konkretisierung muß von den datenverarbeitenden Stellen selbst vorgenommen werden, und dafür sollten gesetzliche Vorgaben geschaffen werden. Ihre Beachtung und Ausfüllung würde mehr Transparenz schaffen und überdies die Arbeit der Kontrollorgane erleichtern. Nach meinem Vorschlag sind die datenverarbeitenden Stellen zu verpflichten, für jede automatisiert auswertbare Datei in selbstbindender Form (Dateistatut) Festlegungen über die wesentlichen Bedingungen und Formen der Datenverarbeitung und des Datenschutzes zu treffen. Die denkbaren Inhalte eines solchen Dateistatuts habe ich bereits in meinem zweiten Tätigkeitsbericht (siehe dort Nr. 4.3.3, S. 62) bezeichnet. Um auch hier den Grundsatz der Verhältnismäßigkeit zur Geltung zu bringen, sollte einschränkend bestimmt werden, daß der Aufwand für diese Festlegungen dem angestrebten Schutzzweck zu entsprechen hat.

h) Verpflichtung auf das Datengeheimnis

Ich habe die Vorschrift des § 5 BDSG, nach der jeder bei der Datenverarbeitung Beschäftigte auf das Datengeheimnis zu verpflichten ist, stets so verstanden, daß sie den Abschluß einer Belehrung über die Rechte und Pflichten nach dem Bundesdatenschutzgesetz bildet. Tatsächlich wird sie aber mehr oder weniger formal vollzogen. Es ist auch weitgehend ungeklärt geblieben, wie weit der Kreis der bei der Datenverarbeitung Beschäftigten zu ziehen ist. Nach der Devise „Im Zweifel lieber verpflichten" wurde manchmal das gesamte Personal formal verpflichtet. Der eigentliche Sinn der Verpflichtung ist damit verfehlt. Bei der bevorstehenden Novellierung des BDSG könnte diese Vorschrift gestrichen werden, insbesondere dann, wenn durch den Erlaß des Dateistatuts (s. o.) die bei der Verarbeitung dieser Daten Beschäftigten mit den Vorschriften vertraut gemacht werden.

i) Transparenz

Die Wirksamkeit des Datenschutzes ist ganz wesentlich davon abhängig, daß für die Betroffenen die Verarbeitung ihrer personenbezogenen Daten durchschaubar wird und Auskunftsrechte wahrgenommen werden können. Die dafür als Hilfsmittel gedachten Veröffentlichungen über die gespeicherten Daten (§ 12 BDSG) haben diesen Zweck nur unzureichend erfüllt. Nach den Erfahrungen sind die stark schematisierten, oft für den Bürger wenig verständlichen und überdies kostspieligen Veröffentlichungen kaum geeignet, dem Betroffenen diejenigen Stellen aufzuzeigen, die Daten zu seiner Person speichern. Ähnliches gilt auch für das vom Bundesbeauftragten für den Datenschutz geführte Dateienregister in seinem bisherigen Informationsgehalt. Vom Einsichtsrecht in das Register wird kaum Gebrauch gemacht; als Arbeitsmittel für den Bundesbeauftragten ist es nur bedingt brauchbar.

Ich habe Vorschläge gemacht, um welche Angaben das Register erweitert werden sollte. Insbesondere sollten auch die nicht-automatisierten Dateien einbezogen werden mit Ausnahme der internen Datei-

en. Die Veröffentlichungen könnten nach meiner Auffassung dagegen entfallen, wenn zugleich der Bundesbeauftragte verpflichtet würde, in geeigneter Form und in bestimmten Zeitabständen den Registerinhalt übersichtlich zu veröffentlichen. Daß dies der bessere Weg wäre, zeigt auch die anhaltend rege Nachfrage nach der Broschüre „Der Bürger und seine Daten", die eine Übersicht über die häufigsten Datenspeicherungen vermittelt. Eine zusätzliche Hilfe für die Betroffenen würde es bedeuten, wenn sie der Praxis entsprechend neben dem wenig beanspruchten Einsichtsrecht ein Recht auf kostenfreie Auskunft aus dem Register erhielten, mit dem zugleich gewährleistet wäre, daß der Betroffene in sachkundig aufbereiteter Form Antwort auf seine Fragen erhielte. (Zum Auskunftsrecht im übrigen s. u. zu n)

j) Stärkung der Kontrollinstanzen

Im Initiativentwurf der Fraktionen der SPD/FDP zur Änderung des BDSG (Drucksache 8/3703) war vorgesehen, die Position der Kontrollorgane zu verbessern; die Behörden und sonstigen öffentlichen Stellen des Bundes sollten verpflichtet werden, den Bundesbeauftragten für den Datenschutz über den geplanten Aufbau personenbezogener automatisierter Informationssysteme Nachricht zu geben. Ich greife diesen Vorschlag auf und möchte aus meiner Sicht noch folgende Ergänzungen empfehlen:

— Der dem Bundesbeauftragten obliegende Beratungsauftrag, der durch bessere Unterrichtung über DV-Planungen gestärkt werden soll, wäre dahingehend zu erweitern, daß der Bundesbeauftragte auch zu den Auswirkungen neuer Informationstechniken auf den Datenschutz Stellung nehmen kann (Technologiefolgenkontrolle).

— Um seine Unabhängigkeit stärker zu betonen, sollte dem Bundesbeauftragten und seinen Mitarbeitern ein Zeugnisverweigerungsrecht vor Gericht eingeräumt werden.

— Auf die Notwendigkeit der Klarstellung seiner Befugnis zur Kontrolle der Einhaltung anderer Vorschriften über den Datenschutz, auch wenn für diese kein Dateibezug besteht, wurde bereits oben (zu b)) hingewiesen.

— In diesem Zusammenhang sollte auch klargestellt werden, daß dem Bundesbeauftragten bei seiner Kontrolle gesetzliche Geheimhaltungsvorschriften (z. B. das Steuergeheimnis) nicht entgegengehalten werden können. Hinsichtlich des Postgeheimnisses bedarf die Grundrechtseinschränkung schon nach Art. 19 Abs. 1 Satz 2 GG gesetzlicher Regelung.

Die Befugnisse der Aufsichtsbehörden im nicht-öffentlichen Bereich sollten so geregelt werden, daß ein Tätigwerden nicht nur — wie bisher — im Falle einer Beschwerde möglich ist, sondern auch dann, wenn sonstige Anhaltspunkte für einen Gesetzesverstoß vorliegen.

k) Medienprivileg

Die Fassung des Medienprivilegs in § 1 Abs. 3 BDSG ging von der Erwartung aus, daß das seinerzeit gleichzeitig in Vorbereitung befindliche Presserechtsrahmengesetz ergänzende Datenschutzregelungen schaffen würde. Diese Erwartung ist nicht eingetroffen; daher bedarf es einer Ergänzung der BDSG-Vorschrift um Regelungen der Gegendarstellung, des Auskunfts- und Berichtigungsrechts. Aber schon die bisherige Regelung des Medienprivilegs ist unzulänglich. Sie entzieht die von den Medienunternehmen zu publizistischen Zwecken gespeicherten Daten dem Anwendungsbereich des BDSG; diese Daten wären auch dann ungeschützt, wenn sie beispielsweise in Pressearchiven enthalten sind, die von einigen Unternehmen auch kommerziell genutzt werden, also Dritten zugänglich sind. Es dürfen aber nur diejenigen Verarbeitungsformen priviligiert werden, die unmittelbar eigenen journalistisch-redaktionellen Zwecken dienen. Dies muß durch eine Änderung des geltenden Rechts sichergestellt werden.

l) Forschungsklausel

Die Anwendung der Übermittlungsvorschriften des BDSG auf die Übermittlung von Daten zu Zwecken der wissenschaftlichen Forschung hat sich als problematisch erwiesen (vgl. oben 4.3.1).

Die von mir für notwendig erachteten Datenschutzregelungen sollen die Wissenschaft nicht stärker einschränken als dies zum Schutz der Betroffenen geboten ist. Im einzelnen schlage ich vor:

— Die Übermittlung personenbezogener Daten ist jeweils nur für ein bestimmtes Forschungsvorhaben zulässig.

— Sie bedarf der Einwilligung der Betroffenen. Kann der Forschungszweck weder auf diese Weise noch mit anonymisierten Daten erreicht werden, so soll die Datenübermittlung nur zulässig sein, wenn kein Grund zur Annahme besteht, daß schutzwürdige Belange beeinträchtigt werden.

— Die übermittelten Daten müssen so bald wie möglich anonymisiert werden; Merkmale, mit denen der Personenbezug wiederhergestellt werden kann, sind gesondert zu speichern und so bald wie möglich zu löschen.

— Die Weitergabe oder anderweitige Nutzung der übermittelten Daten bedarf der Einwilligung der Betroffenen.

m) Arbeitnehmerdatenschutz

In vielen Eingaben von Betroffenen wird gerügt, daß personenbezogene Daten, die im Zusammenhang mit einer Bewerbung oder nach Abschluß eines Arbeitsvertrages vom Arbeitnehmer angegeben wurden, vom Arbeitgeber an Dritte übermittelt werden, ohne daß es dafür aus dem Vertragsverhältnis heraus eine Rechtfertigung gibt. Ich trete für eine stärkere Zweckbindung von Arbeitnehmerdaten ein, die in einer Spezialvorschrift im BDSG verankert werden sollte. Die zulässigen Verwendungszwecke sollen strikt auf die Erfordernisse der Eingehung, Durchführung, Beendigung und Abwicklung des Arbeitsverhältnisses beschränkt sein. Weitergehende Nutzungen sollten weder auf berechtigte Interessen

Dritter noch auf eine im Arbeitsverhältnis leicht erhältliche Einwilligung gestützt werden dürfen. Ferner empfehle ich ein Mitbestimmungsrecht des Betriebsrats bzw. Personalrats bei der Einrichtung von Dateien mit Arbeitnehmerdaten.

n) Rechte der Betroffenen

Die Kostenfreiheit des Auskunftsanspruchs des Betroffenen ist als eine der wichtigsten Forderungen an die BDSG-Novelle weitgehend unumstritten. Das gleiche gilt für die Einführung eines vom Verschuldensnachweis unabhängigen Schadensersatzanspruchs, der auch immaterielle Schäden einbeziehen sollte.

Das generelle Recht der Sicherheitsbehörden, die Auskunft an den Betroffenen zu verweigern (§ 13 Abs. 2 in Verbindung mit § 12 Abs. 2 Nr. 1 BDSG) sollte entfallen. Für die Polizei ist es bereits in den KpS-Richtlinien (dort Nr. 4.1) und in den Dateien-Richtlinien (dort Nr. 6.1) aufgelockert worden; die Auskunft wird nur dann nicht erteilt, wenn die Einzelfallprüfung ergibt, daß die Belange des Bürgers hinter dem öffentlichen Interesse an der Nichtherausgabe der jeweiligen Daten zurücktreten müssen. Das in beiden Richtlinien wiedergegebene Auskunftsverbot des § 13 Abs. 3 Nr. 2 und 3 BDSG reicht also für die Auskunftpraxis der Polizei aus, um eine Gefährdung der eigenen Aufgabenerfüllung zu vermeiden und eine im Einzelfall gebotene Auskunftverweigerung zu rechtfertigen. Es ist nicht einzusehen, weshalb die anderen in § 12 Abs. 2 Nr. 1 BDSG genannten Sicherheitsbehörden nicht ebenso verfahren können, d. h. aufgrund einer Interessenabwägung im Einzelfall über den Auskunftsanspruch des Betroffenen entscheiden.

Eine weitere Stärkung der Rechte der Betroffenen ließe sich dadurch erreichen, daß der Auskunftsanspruch allgemein auch auf die Herkunft der Daten und die Empfänger regelmäßiger Datenübermittlungen erstreckt würde, und zwar unabhängig davon, ob diese Informationen zur Person des Betroffenen gespeichert werden; es muß genügen, daß sie der speichernden Stelle in anderer Weise zur Verfügung stehen. Ein so erweiteter Auskunftsanspruch kann dem Betroffenen besser dazu verhelfen, Fehlerquellen nachzugehen, kann ihm Aufschluß geben über weitere Stellen, die seine Daten verarbeiten, und versetzte ihn in die Lage, eventuell auch dort fehlerhafte Angaben korrigieren zu lassen. Der Berichtigungsanspruch des Betroffenen umfaßt nach meiner Auffassung auch die Ergänzung von Datenbeständen, wenn der vorhandene Informationsgehalt so unvollständig ist, daß er trotz richtiger Daten ein falsches Bild vermittelt. Da dieser Standpunkt nicht unbestritten ist, sollte er im Gesetz festgelegt werden. Für eine wichtige Ergänzung halte ich auch die im Landesrecht schon teilweise vorhandene Verpflichtung der datenverarbeitenden Stellen, im Falle der Berichtigung von Daten die Stellen zu unterrichten, denen die unrichtigen Daten bereits übermittelt worden sind.

Im Bereich der Datenverarbeitung durch nicht-öffentliche Stellen des 4. Abschnitts des Gesetzes erwarte und unterstütze ich die Aufnahme einer Vorschrift, wie sie bereits im Initiativentwurf der CDU/CSU-Fraktion (Drucksache 8/3608) vorgesehen war, wonach im Falle einer Entscheidung zu Ungunsten des Betroffenen, etwa über einen Kreditantrag, die aufgrund einer Datenübermittlung (z. B. einer Kreditauskunft) getroffen wurde, dem Betroffenen die übermittelten Daten und die übermittelnde Stelle mitzuteilen sind.

Eine wesentliche Verbesserung der Transparenz der Datenverarbeitung würde schließlich dadurch erreicht, daß dem Betroffenen bei der Benachrichtigung über die erstmalige Speicherung seiner Daten (§ 26 Abs. 1 BDSG) auch mitgeteilt werden müßte, welcher Art die gespeicherten Daten sind und wem sie regelmäßig übermittelt werden. Eine solche Verpflichtung läge auch im Interesse der speichernden Stelle; denn so würden viele der sonst oft nachfolgenden Auskunftsersuchen unterbleiben, weil die Betroffenen bereits hinreichend informiert sind.

## 5 Datenschutz im Ausland, Internationale Zusammenarbeit

### 5.1 Entwicklungstendenzen in Staaten mit Datenschutzgesetzen

Ein Blick über die Grenzen zu unseren Nachbarn und Partnern im Ausland, die schon seit längerem Datenschutzgesetze erlassen haben, ergibt, daß dort die Entwicklung ähnlich wie bei uns verläuft. Sie läßt sich generell mit den Schlagworten Konsolidierung, Spezifizierung und Konzentration charakterisieren.

Die erste Orientierungsphase ist weithin abgeschlossen. Anfängliche Schwierigkeiten mit der Umsetzung der neuen Rechtsvorschriften in konkrete Maßnahmen sind behoben, und der Datenschutz ist zu einer normalen Rahmenbedingung der Informationsverarbeitung geworden. Die darin liegende Konsolidierung bedeutet jedoch nicht Stillstand und Routine. Die Bestimmungen der allgemeinen Datenschutzgesetze erfassen entweder bestimmte Bereiche der Informationsverarbeitung nicht, oder sie werden den dort anzutreffenden besonderen Gegebenheiten nicht hinlänglich gerecht. Ebenso wie bei uns ist daher auch im Ausland die Tendenz zu einer gewissen Spezifizierung des Datenschutzes erkennbar. Die Schwerpunkte liegen bei der Datenverarbeitung im Gesundheitswesen, der sozialen Sicherung, der Forschung und Statistik, der öffentlichen Sicherheit sowie der Presse, namentlich der Neuen

Medien. Auch der Europarat hat seine Aufmerksamkeit auf einige dieser Themen gerichtet.

Die vorangegangenen Ausführungen könnten den Eindruck vermitteln, als expandiere der Datenschutz fortwährend. Dies wäre ein unzutreffendes Bild. Er wird auch korrigiert, wo sich zeigt, daß Datenschutzmaßnahmen nicht oder nicht in diesem Umfange erforderlich sind. Die Anstöße dazu gehen von den Datenschutzkontrollinstitutionen selbst aus. Als Beispiel sei die im schwedischen Datenschutzgesetz vorgesehene Lizenzierungspflicht erwähnt. Sie bezog sich auf Datenbanken aller Art. Der damit verbundene Aufwand war erheblich, der Datenschutz-Ertrag jedoch vergleichsweise gering, weil zahlreiche Informationssysteme Daten enthielten, von denen offenbar keinerlei Gefährdungen für den einzelnen zu erwarten waren. Auf Vorschlag der Datenschutzinspektion ist die Lizenzierungspflicht in der Novelle zum schwedischen Datenschutzgesetz aus dem Jahre 1979 vereinfacht worden (siehe 2. Tätigkeitsbericht, Nr. 5.1.2, S. 73). Die Datenschutzinspektion hält weitere Erleichterungen für vertretbar. Das Thema wird z. Z. in einer Regierungskommission erörtert, in der die Diskussion noch nicht abgeschlossen ist. Auch in Norwegen und Österreich wird erwogen, das Verfahren der Registrierung von Datenbanken zu erleichtern und zu vereinfachen.

Die an diesen Beispielsfällen zu beobachtende Tendenz, den Datenschutz zu konzentrieren und ihn von unnötigen bürokratischen Elementen zu entlasten, ist zu begrüßen. Ich halte es für wichtig, dies zu berichten. Es würde dem Gedanken des Datenschutzes schaden, wenn er über das, was zum Schutze der Rechte und Interessen des Bürgers notwendig ist, hinausginge. Insbesondere wäre es falsch, das Datenschutzrecht zum Schutz der nationalen Wirtschaft einzusetzen.

Diese wenigen Bemerkungen mögen genügen, um den Stand des Datenschutzes in den Ländern mit einschlägiger Gesetzgebung zu kennzeichnen.

### 5.2 Vorbereitung von Datenschutzgesetzen in weiteren Staaten

Es wäre unrealistisch anzunehmen, daß sich die Entwicklung der nationalen Datenschutzgesetzgebung in dem bisherigen Tempo fortsetzt. Der gesetzgeberische Elan der späten 70er Jahre, der nach dem schwedischen (1974) und dem Bundesdatenschutzgesetz (1977) in rascher Folge zur Verabschiedung von sieben weiteren Gesetzen (Neuseeland [1976], Frankreich, Dänemark, Norwegen, Kanada [1978], Luxemburg, Österreich [1978]) führte, ist abgeschwächt. Zwar sind in zahlreichen Ländern die Vorarbeiten für eine Datenschutzgesetzgebung aufgenommen, teilweise auch weit fortgeschritten, die Umsetzung in gesetzgeberische Aktivitäten läßt aber auf sich warten, oder sie vollzieht sich — wo sie eingeleitet wurde — nur schleppend. Dies ist deswegen zu bedauern, weil es sich nachteilig für die internationale Kommunikation auswirken kann, soweit diese personenbezogene Daten zum Gegenstand hat. Es ist zu hoffen, daß die im vorigen Herbst verabschiedeten internationalen Datenschutzübereinkommen des Europarats und der OECD (siehe dazu 3. TB Nr. 5.2.1 und 5.2.2, S. 61) der nationalen Datenschutzgesetzgebung neue Impulse geben und zur weiteren Harmonisierung des Datenschutzrechts führen werden.

Zum aktuellen Stand der Diskussion in diesen Ländern die folgenden Hinweise:

*Belgien*

In Belgien hat dem Parlament bereits 1976 der Entwurf eines Datenschutzgesetzes vorgelegen (1. TB, Nr. 5.2.7.1, S. 60). Zur Verabschiedung kam es nicht, weil das Parlament aufgelöst wurde. In der Zwischenzeit wechselte die Regierung mehrmals. Nunmehr liegt ein Entwurf vor, der gegenüber dem aus dem Jahre 1976 einige Änderungen aufweist: Es werden nur noch natürliche Personen geschützt (bisher auch juristische Personen). Eine unabhängige Kontrollinstitution ist z. Z. nicht vorgesehen. Statt des bisher angestrebten Registrierungs-/Lizenzierungssystems nach dem Muster des schwedischen Datenschutzgesetzes gibt es nur noch die Verpflichtung zur Anmeldung von Dateien zu einem vom Justizminister zu führenden Register.

*Niederlande*

In den Niederlanden ist der Entwurf eines Datenschutzgesetzes von der Regierung fertiggestellt und dem Parlament am 1. Dezember 1981 zugeleitet worden. Er enthält Regelungen für den Datenschutz im öffentlichen und im privaten Bereich. Er folgt einem Datenschutzkonzept, das bereits 1975 für die Behörden der Zentralregierung eingeführt wurde: Jede Dienststelle ist verpflichtet, für die von ihr geführten Dateien ein Dateistatut zu erstellen, das den Datenschutz, bezogen auf die gespeicherten Daten, sicherstellt (1. TB, Nr. 5.2.7.3, S. 61). Es gibt bisher etwa einhundert solcher Statute. Der Gesetzentwurf wird für Informationssysteme mit besonders sensitiven Daten eine Lizenzierungspflicht vorsehen, andere bedürfen lediglich der Registrierung. Statt eines unabhängigen Kontrollorgans ist eine Registrierungskammer vorgesehen, die ein gewisses Maß an Unabhängigkeit haben wird. Die Rechte des Betroffenen entsprechen denen nach dem Bundesdatenschutzgesetz. Der Auskunftsanspruch erstreckt sich auch auf die Angabe der Herkunft der Daten. Der Betroffene hat ferner einen Schadensersatzanspruch, der auch den immateriellen Schaden umfaßt.

*Schweiz*

Zwei Expertenkommissionen haben 1979 den Auftrag erhalten, Vorschläge für eine schweizerische Datenschutzgesetzgebung zu erarbeiten. Der Entwurf für eine Regelung des Datenschutzes im Bereich der öffentlichen Verwaltung ist fertiggestellt. Er soll den gesetzgebenden Körperschaften noch in diesem Jahre zugeleitet werden. Die Vorarbeiten für eine gesetzliche Regelung des Datenschutzes im nicht-öffentlichen Bereich sind noch nicht abgeschlossen.

Ähnlich wie in den Niederlanden hat auch der schweizerische Bundesrat bereits einen ersten Schritt getan und am 16. März 1981 „Richtlinien für die Bearbeitung von Personendaten in der Bundesverwaltung" erlassen. Personendaten dürfen danach von der Bundesverwaltung nur auf der Basis einer Rechtsgrundlage und nur im erforderlichen Umfange für bestimmte Zwecke verarbeitet werden. Ähnliche Grundsätze gelten für die Übermittlung. Bedeutsam erscheint mir, daß Personendaten, die in ohne weiteres zugänglichen amtlichen Veröffentlichungen enthalten sind, bekanntgegeben werden dürfen, bis der Betroffene widerspricht. Die Gestaltung des Auskunfts-, Berichtigungs- und Löschungsrechts gleicht im wesentlichen den Bestimmungen des Bundesdatenschutzgesetzes. Personendaten, die für die Statistik, Planung und Forschung verarbeitet werden sollen, unterliegen einer strengen Zweckbindung. Im Bundesamt für Justiz ist ein Dienst für Datenschutz eingerichtet, der alle Organe des Bundes bei der Anwendung der Richtlinien und in anderen Fragen des Datenschutzes berät.

*Italien*

Der italienischen Regierung liegt ein Kommissionsbericht vor, der zum Erlaß eines umfassenden Datenschutzgesetzes rät. Die Regierung hat ihn bisher nicht veröffentlicht. Sie hat aber eine interministerielle Kommission gebildet, die einen ersten Gesetzentwurf erarbeitet hat. Die interne Diskussion darüber ist noch nicht abgeschlossen.

*Großbritannien*

In Großbritannien liegen der Regierung die Berichte der Younger-Kommission und der Lindop-Kommission vor. Beide enthalten detaillierte Vorschläge für eine Datenschutzgesetzgebung. Die Regierung hat die Europarats-Konvention am 14. Mai 1981 gezeichnet und erklärt, eine Datenschutzgesetzgebung vorbereiten zu wollen, die den Mindeststandards der Konvention entspricht. Sie hat aber auch zu erkennen gegeben, daß sie nicht beabsichtigt, eine unabhängige Datenschutzkontrollinstitution einzuführen, wie dies von der Lindop-Kommission vorgeschlagen worden war. Die Regierung erwägt zunächst nur eine Registrierungspflicht für bestimmte Informationssysteme. Gegen den Mißbrauch von personenbezogenen Daten sollen entsprechende Sanktionen vorgesehen werden. Die allgemeine Gesetzgebung soll sich auf die Festlegung von Datenschutzgrundsätzen beschränken.

*Finnland*

In Finnland macht sich das Fehlen einer eigenen Datenschutzgesetzgebung wegen der Zugehörigkeit zur Gemeinschaft der nordischen Staaten besonders bemerkbar. Inzwischen ist dort die 4. Kommission zur Prüfung und zur Erarbeitung von Vorschlägen eingesetzt worden. Sie kann die bisherigen Erfahrungen und neuen Entwicklungen berücksichtigen. Sie wird z. B. sicher nicht das generelle Lizenzierungssystem aus Schweden übernehmen, weil sich dieses dort als zu aufwendig und relativ ineffektiv aus der Sicht des Datenschutzes erwiesen hat. Statt dessen wird erwogen, den speichernden Stellen die Erstellung von Dateistatuten vorzuschreiben, die auch von den Betroffenen eingesehen werden können. Als Kontrollorgan ist z. Z. ein Ombudsman mit etwas erweiterten Befugnissen im Gespräch.

*Portugal*

Die portugiesische Verfassung aus dem Jahre 1976 enthält das Recht auf Auskunft über die eigenen Daten. Dem Parlament ist im April 1981 der Entwurf eines Datenschutzgesetzes zugeleitet worden, der inhaltlich dem französischen Datenschutzgesetz entspricht. Das Parlament hat in einem ersten Durchgang die Grundkonzeption des Entwurfs gebilligt. Die Beratung der Details soll bis Anfang 1982 abgeschlossen sein.

*Japan*

In Japan ist die Entwicklung des Datenschutzes in der Bundesrepublik Deutschland stets aufmerksam beobachtet worden. Das Bundesdatenschutzgesetz wurde ins Japanische übersetzt. Ich hatte mehrfach die Gelegenheit, Besucher aus Japan über den Stand des Datenschutzes in der Bundesrepublik Deutschland zu unterrichten. Nunmehr hat der Ministerpräsident eine Kommission von Sachverständigen aus Wirtschaft und Verwaltung gebildet, die bis Anfang 1982 einen Bericht mit Vorschlägen für eine japanische Datenschutzgesetzgebung vorlegen soll.

### 5.3 Neue Datenschutzgesetze

Neue Datenschutzgesetze sind im Berichtsjahr in Ungarn und Israel erlassen worden.

Das ungarische Datenschutzgesetz gilt seit dem 1. Juli 1981. Es liegt mir in einer Übersetzung noch nicht vor.

In Israel gilt seit dem 11. November 1981 ein Persönlichkeits- und Datenschutzgesetz (Protection of Privacy Law). Es enthält generelle Regelungen zum Schutz der Privatsphäre und spezielle Bestimmungen zum Schutz personenbezogener Daten, die in automatischen Datenverarbeitungsanlagen gespeichert werden. Das Gesetz verbietet, die Privatsphäre eines anderen ohne seine Zustimmung zu beeinträchtigen. Als Beeinträchtigung (Eingriff, englisch: infringement of privacy) gilt

— das Ausforschen oder Verfolgen in belästigender Weise,

— gesetzlich verbotenes Mithören,

— Fotografieren innerhalb des privaten Bereichs,

— die Veröffentlichung einer Fotografie in einer Weise, die geeignet ist, den Betroffenen zu demütigen oder verächtlich zu machen,

— die Auswertung von Briefen und anderen nicht zur Veröffentlichung bestimmten Schriftstücken (mit Ausnahmen, z. B. fünfzehn Jahre nach der Abfassung),

— die Benutzung des Namens, des Bildes oder der Stimme zu gewerblichen Zwecken,

— die Verletzung gesetzlich vorgeschriebener oder vereinbarter Geheimhaltungspflichten,

— ganz allgemein die zweckwidrige Nutzung von Informationen (using, or passing on to another, information on a person's private affairs otherwise than for the purpose for which it was given) und schließlich

— die Veröffentlichung von Informationen, die nach diesen Bestimmungen rechtswidrig erlangt waren, und sonstiger Angaben über die Intimsphäre (intimate life), der Gesundheitszustand oder das private Verhalten (conduct in the private domain).

Die Verletzung der Privatsphäre in einer dieser Regelungsformen kann eine Schadensersatzpflicht auslösen oder, wenn sie vorsätzlich erfolgt, strafbar sein. Das Gesetz sieht aber auch eine Reihe von Rechtfertigungsgründen (defences) vor, die u. a. die Pressefreiheit und die Staatssicherheit schützen sollen.

Die generellen Regelungen werden ergänzt durch spezielle Vorschriften über den Schutz von personenbezogenen Daten, die in automatischen Datenverarbeitungsanlagen verarbeitet werden. Geschützt sind Daten über persönliche Verhältnisse, Gesundheit, die wirtschaftliche Position, berufliche Qualifikation, Meinungen und Glaubensüberzeugungen. Datenverarbeitungsanlagen, in denen personenbezogene Daten dieser Art verarbeitet werden, sind zu registrieren. Die registerführende Stelle kann die Eintragung versagen, wenn Grund zu der Annahme besteht, daß die Datenbank für rechtswidrige Zwecke genutzt werden soll. Sie überprüft die weitere Nutzung der Datenbanken.

Werden Daten erhoben, die in einer dieser Datenbanken verarbeitet werden sollen, ist der Betroffene auf die Rechtsgrundlage oder auf die Freiwilligkeit seiner Angaben hinzuweisen. Ihm sind der Zweck, zu dem die Information genutzt werden soll, und die Empfänger der Daten anzugeben. Der Betroffene hat einen Auskunftsanspruch. Er kann verlangen, daß unrichtige, unvollständige oder veraltete Daten berichtigt oder gelöscht werden. Das Gesetz verbietet, die so verarbeiteten Daten zu anderen als den ursprünglich vorgesehenen Zwecken zu verarbeiten, es zählt gleichzeitig eine Reihe von Gründen auf, in denen eine anderweitige Nutzung dennoch zulässig oder zumindest entschuldbar ist.

Das Gesetz gilt für automatisiert geführte Datenbanken im öffentlichen und privaten Bereich. Die Übermittlung personenbezogener Daten zwischen öffentlichen Stellen ist erlaubt, soweit sie nicht gesetzlich oder durch andere Regelungen (auch: Normen einer Standesethik) verboten sind und soweit sie der Aufgabenerfüllung der empfangenden oder der speichernden Stelle dienlich sind.

Das israelische Gesetz verdient Aufmerksamkeit, weil hier erstmals versucht wird, Formen der Beeinträchtigung der „privacy" konkreter zu beschreiben und weil es die Zweckbindung stark betont. Inwieweit seine Bestimmungen für die Datenschutzdiskussion in anderen Ländern fruchtbar gemacht werden können, bedarf weiterer Prüfung.

### 5.4 Internationale Übereinkommen

#### 5.4.1 Datenschutz-Konvention des Europarats

Das Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten des Europarats ist inzwischen von den Regierungen der Länder Bundesrepublik Deutschland, Dänemark, Frankreich, Luxemburg, Norwegen, Österreich, Portugal, Schweden, Türkei und Großbritannien gezeichnet worden. Soweit diese Länder eigene Datenschutzgesetze haben, wird das Ratifizierungsverfahren voraussichtlich zügig ablaufen. In den Ländern ohne Datenschutzgesetzgebung wird erwogen, diese zunächst einzuführen und erst dann die Konvention zu ratifizieren.

In der Bundesrepublik Deutschland ist das Ratifizierungsverfahren eingeleitet worden. Offen ist noch, welche Stelle dem Europarat als hilfeleistende Stelle nach Artikel 13 des Übereinkommens benannt werden soll. Nach dieser Vorschrift verpflichten sich die Vertragsparteien, einander bei der Durchführung des Übereinkommens Hilfe zu leisten. Zu diesem Zweck bezeichnet jede Vertragspartei gegenüber dem Generalsekretär des Europarats eine oder mehrere Behörden. Die so bezeichnete Stelle erteilt Auskünfte über das Recht und die Verwaltungspraxis im Bereich des Datenschutzes und der automatisierten Datenverarbeitung. Sie unterstützt ferner im Ausland lebende Personen bei der Wahrnehmung ihrer Rechte nach dem jeweiligen innerstaatlichen Datenschutzgesetz. Beschwert sich ein im Ausland lebender Deutscher oder ein Ausländer, durch eine deutsche öffentliche oder private Stelle in seinen schutzwürdigen Belangen beeinträchtigt worden zu sein, soll die benannte Behörde ihn insoweit unterstützen. Dies erweist sich in der Bundesrepublik als schwierig, weil hier die Kontrollzuständigkeiten verteilt sind. Für einen Betroffenen im Ausland ist es praktisch unmöglich festzustellen, welche Stelle im Einzelfall für die Datenschutzkontrolle zuständig ist. Dies würde auch nicht dadurch erleichtert, daß sämtliche Kontrollinstitutionen im Bund und in den Ländern mit ihrem jeweiligen sachlichen und örtlichen Zuständigkeitsbereich dem Europarat gegenüber benannt würden. Es besteht Einvernehmen, daß möglichst nur eine, notfalls nur einige wenige Stellen benannt werden. Sie leiten Eingaben, für deren Erledigung sie selbst nicht zuständig sind, weiter.

Der Bundesminister des Innern vertritt bisher die Auffassung, daß er diese Aufgabe übernehmen sollte. Damit kann ich mich nicht einverstanden erklären, weil dies bedeuten würde, daß jede aus dem Ausland eingehende Beschwerde zunächst von einer Stelle in Empfang genommen und gesichtet würde, die selbst Adressat der Beschwerde sein könnte. Es ist nicht auszuschließen, daß eine als Beschwerde gedachte Eingabe als Auskunftsersuchen verstanden wird und nicht an mich oder an die sonst zuständige Aufsichtsbehörde weitergeleitet wird. Es ist auch nicht auszuschließen, daß Untersuchungen vorab eingeleitet werden, ehe die Beschwerde die zuständige Kontrollinstanz erreicht. Ich unterstelle nicht, daß bewußt so verfahren würde. Die bloße Möglichkeit muß ich aber als eine Einschränkung