121 Seiten

Deutscher Bundestag
12. Wahlperiode

Drucksache 12/553

16. 05. 91

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

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

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz — I — 111/15 — vom 16. Mai 1991 gemäß § 19 Abs. 2 des Bundesdatenschutzgesetzes.

1 Überblick über das Berichtsjahr

1.1 1990, ein bedeutsames Jahr für den Datenschutz

Das Berichtsjahr war in dreifacher Hinsicht für den Datenschutz von zentraler Bedeutung, nämlich wegen

- der Herstellung der deutschen Einheit
- der Verabschiedung des neuen Bundesdatenschutzgesetzes im Rahmen des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes vom 20. Dezember 1990 und
- der Vorlage eines „Vorschlages für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" durch die Kommission der Europäischen Gemeinschaften am 13. September 1990.

Diese drei Ereignisse zeigen, wie der Datenschutz einerseits in die politische Entwicklung Deutschlands und Europas eingebunden ist, und andererseits seinen Beitrag dazu leistet, daß in Deutschland und Europa mit den Grundrechten auch das Persönlichkeitsrecht der Bürger und der Schutz ihrer Privatsphäre in die Praxis umgesetzt werden.

1.1.1 Kurzfristige Verschiebung des Berichts

Die vorgenannten Ereignisse, vor allem die deutsche Einheit, sind der entscheidende Grund dafür, daß dieser Tätigkeitsbericht nicht — wie gewohnt — im Februar, sondern wenige Monate später dem Deutschen Bundestag und der Öffentlichkeit vorgelegt wird.

Am 3. Oktober ist das Bundesdatenschutzgesetz auch in der früheren DDR in Kraft getreten. Der Bundesbeauftragte für den Datenschutz wurde nicht nur für die im Beitrittsgebiet neu errichteten Bundesbehörden zuständig; seine Kompetenz wurde bis zur Schaffung einer Datenschutzkontrolle in den neuen Ländern, längstens bis zum 31. Dezember 1991, auch auf die Behörden der Länder und Gemeinden ausgedehnt, soweit diese Bundesrecht ausführen. Bundestag und Öffentlichkeit erwarten daher sicher mit Recht von diesem Bericht eine erste Darstellung der datenschutzrechtlichen Probleme in den neuen Ländern. Meine Mitarbeiter und ich haben deshalb seit dem 3. Oktober 1990 in erster Linie eine Bestandsaufnahme der datenschutzrechtlichen Situation in der DDR gemacht.

Die zeitliche Verschiebung der Vorlage des Berichts hat auch Auswirkungen auf dessen Inhalt. Zwar wird grundsätzlich nur über Ereignisse des Jahres 1990 berichtet; soweit sich datenschutzrechtliche Sachverhalte des Berichtsjahres oder früherer Jahre aber in den ersten Monaten des Jahres 1991 fortentwickelt haben, wurde dies im Interesse der Aktualität des Berichts noch bei der Darstellung berücksichtigt.

1.1.2 Die deutsche Einheit

In meinem 12. Tätigkeitsbericht hatte ich darauf hingewiesen, daß das Streben der Bevölkerung in der früheren DDR und in Osteuropa nach Freiheit auch auf den Schutz des Persönlichkeitsrechts einschließlich der Sicherstellung der Privatsphäre gerichtet ist. Dies haben die in der Zwischenzeit gewonnenen Erfahrungen bestätigt. Insbesondere das Ausmaß der bekanntgewordenen Bespitzelungen der Bürger durch das ehemalige Ministerium für Staatssicherheit hat deutlich gemacht, was Grundrechtsschutz im allgemeinen und Datenschutz im besonderen für die Bürger bedeuten.

Nach der kommunistischen Staatsdoktrin durfte es keine Klassengegensätze geben. Allein deshalb hielt man einen Schutz personenbezogener Daten nicht für erforderlich. Datenschutz im Sinne von Persönlichkeitsschutz war deshalb in der früheren DDR kein Thema. Als man dort nicht mehr umhin konnte, sich mit „Datenschutz" zu befassen, hat man diesen so definiert, daß er lediglich die Datensicherung umfaßte und sich damit als Instrument gegen die Einsichtnahme des Bürgers in seine eigenen Daten verwenden ließ. So hat das Wörterbuch der politisch-operativen Arbeit der Hochschule des Ministeriums für Staatssicherheit den Begriff „Datenschutz" wie folgt umschrieben:

> „Datenschutz,
> der durch ein System abgestimmter rechtlicher, organisatorischer, personeller, technischer und politisch-operativer Maßnahmen gewährleistete zuverlässige Schutz von Informationen, die auf einem materiellen Datenträger gespeichert und im Interesse der Staats- und Gesellschaftsordnung geheimzuhalten sind. Ziel des Datenschutzes ist es, die Informationen allseitig und nach einheitlichen Gesichtspunkten abzusichern und dazu die notwendigen Voraussetzungen zu schaffen."

Es verwundert nicht, daß die Umstellung eines Verwaltungssystems mit diesem Grundverständnis von Datenschutz auf das einer rechtsstaatlichen Verwaltung, die Grundrechte und Datenschutz als integralen Bestandteil ihrer Tätigkeit anerkennt, auf erhebliche Schwierigkeiten stoßen muß. Es ist ja nicht damit getan, Datensammlungen, die nach dem Recht der Bundesrepublik Deutschland nicht hätten erhoben werden dürfen, einfach zu vernichten. Dem stehen nicht nur schutzwürdige Belange Betroffener entgegen. Vielfach wird ein Teil der erhobenen Daten auch von einer rechtstaatlichen Verwaltung benötigt, wie etwa die Aufzeichnungen über bestimmte Straftaten im Bundeszentralregister oder bei der Polizei zur Gefahrenabwehr. Andere Datensammlungen, die in der früheren DDR zentral angelegt waren, sind nach den Rechtsvorstellungen des föderalistischen Staates aus guten Gründen nur dezentral vorgesehen, wie z. B. die Register der Meldebehörden. Schließlich gab es in der DDR Register, für die es in der Bundesrepublik Deutschland nichts oder nur partiell Vergleichbares gibt, wie etwa das Nationale Krebsregister der ehemaligen DDR.

Die Beispiele zeigen, daß bei der Umstellung der Datensammlungen der früheren DDR auf die neue

Verwaltung jeweils sorgfältig vorgegangen werden muß, um einerseits im Widerspruch zu rechtsstaatlichen Vorstellungen angelegte Datensammlungen so schnell wie möglich zu beseitigen, andererseits schutzwürdige Belange Betroffener und berechtigte Interessen einer rechtsstaatlichen Verwaltung zu wahren. Dabei müssen klare grundsätzliche Positionen eingenommen, aber auch Flexibilität und Phantasie gezeigt werden, um beide Ziele möglichst schnell und umfassend zu erreichen.

Der Abschnitt 2 dieses Berichts gibt einen vorläufigen Überblick über die wichtigsten datenschutzrechtlichen Fragen, die bisher im Beitrittsgebiet erkennbar geworden sind. Ich bin sicher, daß die Liste der Probleme damit noch nicht vollständig ist.

1.1.3 Das neue Bundesdatenschutzgesetz

Es ist erfreulich, daß das neue Bundesdatenschutzgesetz im Berichtsjahr noch verabschiedet und verkündet worden ist. Ich habe mich an der Diskussion um dieses Gesetz — zuletzt mit einer schriftlichen Stellungnahme an den Innenausschuß des Deutschen Bundestages — intensiv beteiligt. Obwohl nicht alle meine Vorstellungen verwirklicht worden sind, erkenne ich an, daß das Gesetz für den öffentlichen Bereich einen deutlichen datenschutzrechtlichen Fortschritt bringt, über den ich im einzelnen unter 26 berichte.

Wenn es auch mühsam war, dieses Ergebnis — zuletzt über eine Entscheidung des Vermittlungsausschusses von Bundestag und Bundesrat — zu erreichen, so möchte ich doch allen, die daran beteiligt waren, aufrichtig danken. Es kommt jetzt darauf an, das Gesetz datenschutzfreundlich auszulegen und anzuwenden. Die Zurückhaltung des neuen Bundesdatenschutzgesetzes bei der Fortentwicklung des Datenschutzes im nicht-öffentlichen Bereich macht es erforderlich, in besonders sensiblen Bereichen wie z. B. bei Arbeitnehmern, in der Versicherungs- und Kreditwirtschaft sowie für Auskunfteien bereichsspezifische Regelungen zu schaffen. Ich habe mich bereits an den Bundesminister für Arbeit mit der Bitte gewandt, doch möglichst bald ein Arbeitnehmerdatenschutzgesetz vorzulegen.

1.1.4 Datenschutz in der Europäischen Gemeinschaft

Die Kommission der Europäischen Gemeinschaft ist jetzt nach langem Zögern in Sachen Datenschutz endlich aktiv geworden. Die von ihr unterbreiteten Vorschläge sind durchaus erfreulich (s. 28.). Obwohl aus meiner Sicht noch einiges verbessert werden sollte, können die Vorschläge der EG eine qualitativ neue Phase für den Datenschutz in Europa eröffnen. Wichtig ist vor allem, daß die Richtlinie keine Zwangsjacke gegen noch bessere Datenschutzregelungen darstellt. Es muß deshalb klargestellt werden, daß sie nur einen datenschutzrechtlichen Mindeststandard vorschreibt und nationalen Regelungen, die einen noch besseren Datenschutz gewährleisten, nicht im Wege steht.

Das Bemühen um den Datenschutz in Europa macht auch unabhängig von der EG-Richtlinie Fortschritte; dabei wird auch gern auf die Erfahrungen deutscher Datenschutzbehörden zurückgegriffen. So habe ich auf einer Veranstaltung der Autonomen Provinz Bozen (Südtirol) zur Vorbereitung eines Datenschutzgesetzes für diese Provinz das einleitende Grundsatzreferat gehalten. Die für die Beratung des neuen schweizerischen Datenschutzgesetzes zuständige Kommission des Schweizer Nationalrats hat mich neben einem Vertreter der französichen Datenschutzkommission als Sachverständigen gehört.

1.1.5 Wissenschaftliche und technische Entwicklungen

Wissenschaftliche und technische Entwicklungen und die praktische Anwendung der neuesten Erkenntnisse sind auch im Berichtsjahr weitergegangen, ohne daß immer die erforderlichen datenschutzrechtlichen Vorkehrungen getroffen waren.

Für die Praxis besonders bedeutsam ist die Entwicklung der Telekommunikation, die vom Bundesminister für Post und Telekommunikation mit Recht als ein Schlüsselsektor der Volkswirtschaft angesehen wird. Besondere Bedeutung kommt dabei der auch internationalen Einführung von ISDN in Europa zu. Nach der Einrichtung der ersten internationalen ISDN-Verbindung zwischen der Bundesrepublik Deutschland und den Niederlanden im Oktober 1989 wurde ein Jahr später die Verbindung zum französischen Netz und im Dezember 1990 mit der britischen Fernmeldeverwaltung hergestellt. Der Bundesminister für Post und Telekommunikation bewertete dies mit Recht als Einrichtung von Autobahnen für die Telekommunikation. Telekommunikationsautobahnen benötigen aber besondere Verkehrsregelungen. Diese fehlen immer noch. Weil die Entwicklung auch im Mobilfunk weitergeht (s. unten 8.1.3 und 8.7), ist es höchste Zeit, daß die erforderlichen Rechtsvorschriften jetzt schnell geschaffen werden (s. unten 8.1).

Die Genomanalyse ist inzwischen durch die Rechtssprechung anerkannte Praxis im gerichtlichen Verfahren, ohne daß der Gesetzgeber die erforderlichen gesetzlichen Vorkehrungen gegen einen Mißbrauch der durch Genomanalyse gewonnenen besonders schützenswerten Daten geschaffen hat (vgl. unter 4.2)

Die Erfahrung, daß die erforderliche Rechtsetzung der wissenschaftlichen und technischen Entwicklung hinterherhinkt, könnte noch durch weitere Beispiele verdeutlicht werden. Es besteht Anlaß, erneut an Bundesregierung und EG zu appellieren, bei der Planung neuer technischer Einrichtungen, die für das Persönlichkeitsrecht der Bürger von Bedeutung sind, rechtzeitig die erforderlichen konzeptionellen Vorgaben zu machen und dabei nicht nur technischen Fortschritt und wirtschaftlichen Erfolg, sondern ganz selbstverständlich auch den Schutz des Persönlichkeitsrechts der Bürger anzustreben. Eine rechtzeitige Beteiligung der Datenschutzkontrollinstanzen wäre der Erreichung dieses Zieles sicher förderlich (s. unten 8.7).

1.1.6 Beratung durch den Bundesbeauftragten für den Datenschutz

Das Ende der abgelaufenen Legislaturperiode und die vom Gesetzgeber im Zusammenhang mit der deutschen Einheit zu lösenden Probleme haben dazu geführt, daß im Berichtszeitraum meine Beratung im Bereich der Gesetzgebung besonders in Anspruch genommen worden ist.

Im Zusammenhang mit der deutschen Einheit hat die Bundesregierung mich insbesondere bei der Beratung der Vorschriften über die künftige Geltung des Bundesdatenschutzgesetzes in den neuen Ländern und über die vorläufige Regelung für die Unterlagen des früheren Ministeriums für Staatssicherheit intensiv beteiligt. Auch bei der Ausarbeitung der Benutzerordnung des Sonderbeauftragten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes konnte ich von Anfang an mitwirken.

Aus dem Bereich der Bundesgesetzgebung erwähne ich besonders das Gesetz zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, mit dem auch ein neues Verfassungsschutzgesetz sowie Gesetze über den Militärischen Abschirmdienst und den Bundesnachrichtendienst geschaffen worden sind. Bei den Beratungen konnte ich manche datenschutzrechtlichen Verbesserungen erzielen.

Als erstes größeres Gesetzgebungsvorhaben aus den neuen Ländern hat mir das sächsische Innenministerium den Entwurf eines neuen Polizeigesetzes zugeleitet, zu dem ich auch bereits Stellung genommen habe.

In recht großem Umfang haben nicht nur Behörden aus den „alten" Bundesländern, sondern auch nachgeordnete Behörden aus dem Beitrittsgebiet um Beratung zu den verschiedensten datenschutzrechtlich bedeutsamen Fragen gebeten, von der Frage nach der sachgerechten Behandlung von Personalakten über die Behandlung von Gesundheitsdaten bis zum Umgang mit Sozialdaten. Wegen der nur zögernden Bildung der Landesregierungen in den neuen Ländern ist die Beratungstätigkeit diesen gegenüber nur schleppend in Gang gekommen. Ich werde noch vermehrt eigene Initiativen ergreifen, um meine Beratungsaufgabe gerade im Beitrittgebiet zu erfüllen.

1.1.7 Eingaben von Bürgern

Im Berichtsjahr haben wiederum eine große Zahl von Bürgern von ihrem Recht Gebrauch gemacht, sich mit Eingaben an mich zu wenden. Die Eingaben haben wieder fast den gesamten Bereich der Bundesverwaltung betroffen. Einige Beispiele mögen dies verdeutlichen:

1. Ein Bürger aus Nordrhein-Westfalen beklagte sich darüber, daß eine Grundstücksverwaltungsgesellschaft offenbar von seinem bei einer thüringischen Stadt gestellten Rückerstattungsantrag für ein Grundstück erfahren hatte. Meine Ermittlungen ergaben den dringenden Verdacht, daß diese Information tatsächlich pflichtwidrig weitergegeben worden war. Die betroffene Stadt hat Strafanzeige bei der Staatsanwaltschaft erstattet.

2. Ein ehemaliger Bausoldat der Nationalen Volksarmee der früheren DDR erkundigte sich bei mir danach, welche Unterlagen über ihn noch jetzt bei Behörden der (neuen) Bundeswehr vorhanden seien. Im Rahmen eines Kontrollbesuchs beim zuständigen Kreiswehrersatzamt in Sachsen konnte ich feststellen, welche Unterlagen noch über den Petenten vorhanden sind und ihm anschließend mitteilen, daß er jederzeit Einsicht in diese nehmen kann.

3. Ein Bürger kaufte sich in einem Reisebüro ein Supersparpreis-Ticket der Deutschen Bundesbahn, das nur an bestimmten Tagen benutzt werden darf. Die Ausschlußtage waren im Fahrscheinheft angegeben und die Gültigkeit für die späteste Hinfahrt und früheste Rückfahrt auf dem Umschlag des Fahrscheinheftes handschriftlich notiert. Bei der Rückreise teilte ein Zugbegleiter dem Fahrgast mit, sein Fahrschein habe für den von ihm gewählten Rückreisetag keine Gültigkeit, obwohl dieser Tag als frühester Rückreisetag auf dem Umschlag des Fahrscheinheftes eingetragen war. Auch eine Durchsicht des Verzeichnisses der Ausschlußtage im Fahrscheinheft brachte dem Fahrgast keinen Hinweis darauf, daß die Auffassung des Zugbegleiters richtig war. Er weigerte sich daher, das von dem Zugbegleiter verlangte erhöhte Beförderungsentgelt zu zahlen. Nachdem der Fahrgast auch der Aufforderung des Zugbegleiters nicht nachkam, sich auszuweisen, wurde er am nächsten Haltebahnhof von zwei Bahnpolizisten aufgefordert, den Zug zu verlassen. Trotz des Hinweises des Fahrgastes, daß er einen wichtigen Termin wahrzunehmen habe und er nach Verlassen des IC seinen Anschlußzug nicht mehr erreiche, versuchten Bahnpolizisten, ihn unter Anwendung unmittelbaren Zwangs aus dem Zug zu holen. Erst nachdem er seine Personalien angegeben und sich ausgewiesen hatte, konnte er die Fahrt fortsetzen.

   Meine auf die Eingabe des Bürgers durchgeführte Rückfrage bei der Deutschen Bundesbahn ergab, daß durch eine gesonderte Veröffentlichung die Ausschlußtage für das Angebot „Supersparpreis" erweitert und alle Verkaufsstellen gebeten worden waren, diese Tage handschriftlich in die Heftumschläge einzutragen. Durch ein Versehen des Reisebüros war dieser handschriftliche Zusatz in dem Fahrscheinheft des Fahrgastes unterblieben. Dieser konnte — weil der fragliche Tag ausdrücklich als erster Rückreisetag eingetragen war — erst recht davon ausgehen, daß er berechtigt war, die Fahrkarte an diesem Tag zu benutzen. Die Deutsche Bundesbahn akzeptierte diese Erklärung und versicherte, daß die in diesem Zusammenhang erhobenen personenbezogenen Daten gelöscht worden seien.

4. Einem Petenten, der Arbeitslosenhilfe beantragt hatte, war vom zuständigen Arbeitsamt zur Überprüfung seiner Bedürftigkeit ein Fragebogen vorgelegt worden, der u. a. Angaben über die Namen von Mietern in einem Haus des Petenten vorsah.

Die Bundesanstalt für Arbeit hat auf meine Nachfrage eingeräumt, daß die namentliche Bezeichnung der Mieter für ihre Aufgabenerfüllung nicht erforderlich ist. Sie hat das betreffende Arbeitsamt angewiesen, auf die Frage nach den Namen der Mieter künftig zu verzichten und im Falle des Petenten die Namen der Mieter in der Leistungsakte zu schwärzen.

5. Ein Petent beschwerte sich darüber, daß das Arbeitsamt seiner mehrfachen Bitte, Bewerbungsunterlagen erst nach seiner vorherigen Information und Zustimmung an Dritte weiterzugeben, nicht entsprochen hatte.

   Die Bundesanstalt für Arbeit hat eingeräumt, daß die mehrfachen Anträge des Petenten keinen entsprechenden Hinweis in seinen Vermittlungsunterlagen bewirkt hatten. Sie nahm die Eingabe zum Anlaß, im Rahmen einer Rundverfügung auf die bestehende Weisungslage hinzuweisen, die eine Weitergabe von Bewerbungsunterlagen nur mit Zustimmung des Bewerbers zuläßt, wenn dieser einen entsprechenden Wunsch geäußert hat.

6. Ein Bürger hat sich an mich gewandt, weil das Bundeskriminalamt ihm eine Auskunft über gespeicherte Daten verweigert hatte. Er hatte bereits das Verwaltungsgericht angerufen mit dem Antrag, ihm Einsicht in Unterlagen des BKA zu gewähren. Ich konnte feststellen, daß die Mehrzahl der beim Bundeskriminalamt gespeicherten Vorgänge dem Betreffenden ohnehin bekannt waren, z. B. erkennungsdienstliche Behandlungen und strafgerichtliche Verfahren. Ich habe dem BKA daher dargelegt, daß es verpflichtet ist, zumindest eine Teilauskunft über die in Dateien gespeicherten Daten zu geben und gebeten, soweit es die Auskunft ablehnen möchte, mir gegenüber zu begründen, inwiefern durch eine Auskunft die Aufgabenerfüllung der Krimninalpolizei gefährdet würde. Das BKA hat das abgelehnt und auch die Zustimmung dazu verweigert, daß ich dem Betroffenen etwas über die beim BKA vorhandenen Daten mitteile. Das BKA meint, auch durch eine solche Teilauskunft werde seine Position im anhängigen Verwaltungsgerichtsverfahren verschlechtert.

   Ich habe die vollständige Auskunftsverweigerung durch das BKA beanstandet. Weder die Verpflichtung der Behörden, den Betroffenen Auskunft zu erteilen, noch das Recht der Betroffenen, sich beim Bundesbeauftragten über eine Verletzung ihrer Datenschutzrechte zu beschweren, entfällt deshalb, weil ein gerichtliches Verfahren mit einem weitergehenden Streitgegenstand anhängig ist.

7. Als ich die Eingabe eines ausländischen Mitbürgers bearbeitete, stellte ich fest, daß das Bundesamt für Verfassungsschutz die Akten des Asylbewerbers komplett kopiert, zu seinen Akten genommen und auch dann noch weiter aufbewahrt hatte, als der Asylantrag positiv beschieden worden war. Aufgrund meiner Intervention wurde das Verfahren umgestellt: In Zukunft nimmt der Verfassungsschutz nur noch solche Erkenntnisse zu seinen Akten, die verfassungsschutzrelevante Informationen enthalten.

8. Ein Petent hat sich dagegen gewandt, daß er Mitteilungen des Kreiswehrersatzamtes mit personenbezogenen Daten auf offenen Postkarten erhielt. Aufgrund meiner Intervention hat der Bundesminister der Verteidigung die Weisung gegeben, solche Mitteilungen in Zukunft nur noch in verschlossenem Umschlag zu versenden.

9. Ein Wehrpflichtiger hat mit Recht beanstandet, daß der vom Bundesminister der Verteidigung verwandte Fragebogen zur Wehrüberwachung Fragen enthielt, die für die Aufgabe der Wehrüberwachung überhaupt nicht erforderlich waren, wie z. B. nach dem Geschlecht eines Kindes, dem Arbeitgeber und der Schulbildung der Ehefrau. Der Bundesminister der Verteidigung hat daraufhin angeordnet, daß der entsprechende Fragebogen des Kreiswehrersatzamtes nicht mehr verwendet wird.

1.1.8 Datenschutzrechtliche Kontrollen

Die Erkenntnisse, die aus Kontroll- und Informationsbesuchen gewonnen werden, sind, das hat sich gerade im Berichtsjahr gezeigt, für einen wirksamen Datenschutz unverzichtbar. Es kommt immer wieder vor, daß das daraus gewonnene Wissen bei Verhandlungen mit Ausschüssen des Deutschen Bundestages und mit obersten Bundesbehörden entscheidend ist, weil diese sich über die Verhältnisse vor Ort oft nicht so intensiv unterrichten können, wie das im Rahmen einer Datenschutzkontrolle möglich ist. Die Kontrollen reichten im Berichtszeitraum von Bundesministerien bis zu den untersten nachgeordneten Behörden, etwa Arbeitsämtern, Bahnhöfen, Fernmeldeämtern.

Seit dem 3. Oktober 1990 haben meine Mitarbeiter auch Behörden der (neuen) Bundesverwaltung in den neuen Ländern sowie dort als gemeinsame Ländereinrichtungen fortbestehende Dienststellen besucht. Die dabei ausgeübte Tätigkeit war in der Sache sicher „Kontrolle", die meine Mitarbeiter aber ganz bewußt im Sinne von Beratung und eigener Information ausgeübt haben. Die Schwerpunkte lagen bei den Archiven und Lagern für die Unterbringung der Stasi-Unterlagen und bei den großen Datensammlungen der DDR, wie dem Zentralen Einwohnerregister, der Datei „Dora" des Zentralen Kriminalamts und dem Strafregister des früheren Generalstaatsanwalts der DDR. Die Dienststellen haben die gegebenen Vorschläge und Anregungen in aller Regel akzeptiert und soweit irgend möglich umgesetzt.

1.1.9 Zur Lage des Datenschutzes

Der Datenschutz ist bei den meisten Bundesbehörden anerkannt. Gleichwohl fallen immer wieder Mängel auf, die zeigen, wie notwendig eine laufende datenschutzrechtliche Kontrolle ist. Die Verwirklichung des Datenschutzes in der Praxis ist sehr oft ein mühsames Ringen, das einen langen Atem und Durchsetzungsbereitschaft erfordert. Bei meinen Bemühungen um stärkeren Schutz des Persönlichkeitsrechts der Bürger sind Fehlschläge nicht ausgeblieben. Gleichwohl: die

Erfolge können sich sehen lassen, wie auch dieser Bericht zeigt.

In den neuen Ländern zeigt sich viel guter Wille, Forderungen des Datenschutzes gerecht zu werden. Andererseits wird aber gelegentlich auch das Mißverständnis sichtbar, der Datenschutz stehe etwa Auskünften aus Stasi-Unterlagen oder der Einsicht in solche Unterlagen prinzipiell entgegen. Das trifft schon deshalb nicht zu, weil die Transparenz der Datenverarbeitung, also das Recht, Auskunft über gespeicherte Daten, wenn möglich auch Einsicht in solche, zu erhalten, zu den Grundforderungen des Datenschutzes gehört. Einschränkungen können sich nur aus den Rechten Dritter ergeben.

Im Berichtszeitraum mußte sich der Datenschutz auch gegen unberechtigte Angriffe verteidigen (s. 4.1).

Nach jedem neuen Terroranschlag gehört es inzwischen zu einem mit einiger Sicherheit zu erwartenden Ritual, daß gefordert wird, jetzt müßten endlich Persönlichkeitsrecht und Datenschutz zurücktreten. Dabei gehört es auch zu der Erfahrung, daß im Zusammenhang mit solchen Forderungen keinerlei konkrete Hinweise gegeben werden, welche datenschutzrechtliche Regelung welchen polizeilichen Maßnahmen zur Verhinderung des jeweils letzten Terroranschlags im Wege gestanden hat. Tatsache ist, daß ich in meiner nun fast dreijährigen Amtszeit niemals einen Vorschlag des Bundeskriminalamts zur Verbesserung der Terrorismusbekämpfung aus Datenschutzgründen abgelehnt habe. Ich habe in diesem Bereich keine Maßnahme des BKA oder BfV gerügt, geschweige denn förmlich beanstandet, obwohl der Gesetzgeber im Bereich des Polizei- und Strafprozeßrechts die erforderlichen Rechtsvorschriften bis heute nicht erlassen hat. Ich habe gerade wegen der möglichen Auswirkungen auf die Arbeit der Polizei und der Staatsanwaltschaft nie einen Termin genannt, an dem der Übergangsbonus für Eingriffe in das Recht auf informationelle Selbstbestimmung ohne ausdrückliche Rechtsgrundlage abgelaufen ist oder ablaufen wird. Ich fordere daher alle Beteiligten zu einer fairen Diskussion auf. Für mich ist bedeutsam, was ein anerkannter polizeilicher Fachmann im Heft 3 des Datenschutzberaters 1991 unter der Überschrift „Sicherheitsbehördliche Ermittlungen blockiert durch den Datenschutz?" als Fazit seiner Untersuchung feststellte:

> „Vorfeldermittlungen der Polizei, insbesondere im Rahmen der vorbeugenden Verbrechensbekämpfung, scheitern nicht an dem vielgeschmähten und als ‚Tatenschutz' diskriminierten Datenschutz"

Ich brauche nicht zu betonen, daß ich jederzeit zu Gesprächen und auch zu Mitverantwortung bereit bin, wenn es darum gehen sollte, echte oder vermeintliche datenschutzrechtliche Schranken für ein Tätigwerden der Strafverfolgungsorgane bei der Terrorismusbekämpfung zu erörtern und — wenn möglich — zu beheben. Es ist aber einfach zu billig, den Datenschutz als Sündenbock für mangelnde Erfolge bei der Terrorismusbekämpfung, die ich niemandem anlaste, vorzuführen.

1.2 Kontrollen und Beratungen

Bei folgenden Behörden haben Mitarbeiter meiner Dienststelle im Berichtszeitraum Kontrollen, Beratungen und Informationsbesuche durchgeführt:

- Bundeskanzleramt
- Auswärtiges Amt
- Bundesminister des Innern
- Bundesminister der Justiz
- Bundesminister der Finanzen
- Bundesminister für Wirtschaft
- Bundesminister für Ernährung, Landwirtschaft und Forsten
- Bundesminister für Arbeit und Sozialordnung
- Bundesminister der Verteidigung
- Bundesminister für Jugend, Familie, Frauen und Gesundheit
- Bundesminister für Verkehr
- Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit
- Bundesminister für Post und Telekommunikation
- Bundesminister für Raumordnung, Bauwesen und Städtebau
- Bundesrechnungshof
- Bundesnachrichtendienst
- eine Botschaft
- Bundesverwaltungsamt
- Statistisches Bundesamt
- Bundesarchiv
- Bundesamt für Verfassungsschutz
- Bundeskriminalamt
- Dienststelle des Sonderbeauftragten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes einschl. einiger Archive
- Grenzschutzdirektion
- Generalbundesanwalt beim Bundesgerichtshof (Abteilung IV Bundeszentralregister)
- Bundesaufsichtsamt für das Kreditwesen
- Zollkriminalinstitut
- Deutsche Genossenschaftsbank
- Physikalisch-Technische Bundesanstalt
- Bundesforschungsanstalt für Viruskrankheiten der Tiere
- Bundesanstalt für Arbeit
- Militärischer Abschirmdienst
- Bundesgesundheitsamt
- Kraftfahrt-Bundesamt
- Bundesanstalt für Flugsicherung
- Deutsche Bundesbahn
- Deutsche Bundespost TELEKOM
- Deutsche Bundespost POSTDIENST
- Bundesversicherungsanstalt für Angestellte
- Versorgungsanstalt der Deutschen Bundespost
- Bundesverband der Betriebskrankenkassen

- Verband der Angestellten-Ersatzkassen
- eine Geschäftsstelle der Barmer Ersatzkasse
- Betriebskrankenkasse Salzgitter
- Kaufmännische Krankenkasse Hannover
- Maschinenbau-Berufsgenossenschaft, Düsseldorf
- Bau-Berufsgenossenschaft, Wuppertal
- Chemie-Berufsgenossenschaft, Heidelberg
- eine berufsgenossenschaftliche Unfallklinik
- Zentrales Einwohnerregister für das Beitrittsgebiet
- Gemeinsames Landeskriminalamt für das Beitrittsgebiet
- die Treuhandanstalt
- ein Kreiswehrersatzamt in den neuen Bundesländern
- ein Bahnhof der Deutschen Bundesbahn
- eine Heimatschutzbrigade der Bundeswehr
- ein Arbeitsamt

Nachfolgend sind wichtige aktuelle Themen und die Art ihrer Bearbeitung aufgeführt:

Thema	**Art der Erledigung**
Einigungsvertrag	Beteiligung an den Vertragsverhandlungen im Rahmen der bundesdeutschen Verhandlungsdelegation sowie Stellungnahmen gegenüber mehreren Bundesministerien
Inverwahrnahme, Sicherung und Verwendung der Unterlagen des Staatssicherheitsdienstes der früheren DDR (Stasi-Unterlagen)	Beratung des Sonderbeauftragten der Bundesregierung und des BMI durch schriftliche Empfehlungen, insbesondere bei der Vorbereitung der Benutzerordnung
Übernahme des Strafregisters beim Generalstaatsanwalt der DDR	Beratung des BMJ bei Vorbereitung der Regelungen im Einigungsvertrag sowie des Generalbundesanwalts beim Bundesgerichtshof (Abteilung IV-Bundeszentralregister) für die Durchführung der Übernahme
Ausländergesetz und Verordnungen hierzu	Beratung des Innenausschusses des Deutschen Bundestages und schriftliche Stellungnahmen gegenüber dem BMI
Regierungsentwurf eines Gesetzes über das Ausländerzentralregister	Beratung und schriftliche Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages und dem BMI
Datenverarbeitungstechnische Neukonzeption des Ausländerzentralregisters	Beratung und schriftliche Empfehlungen gegenüber dem BMI
Gesetz zur Regelung des Aufnahmeverfahrens für Aussiedler	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Durchführung des Aussiedleraufnahmeverfahrens	Beratung des BMI und des Bundesverwaltungsamtes
Behandlung von Unterstützungsunterschriften im Zusammenhang mit Wahlen	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Bundesratsentwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität	Schriftliche Empfehlungen gegenüber dem BMJ, Mitberatung in der Datenschutzkonferenz
Diskussionsentwurf einer gesetzlichen Regelung zum genetischen Fingerabdruck (Genomanalyse im Strafverfahren)	Beratung und schriftliche Stellungnahme gegenüber dem BMJ

Thema	Art der Erledigung
Arbeitsentwurf eines Dritten Gesetzes zur Änderung des Bundeszentralregistergesetzes	Beratung des BMJ
Zivilprozeßordnung	Schriftliche Empfehlungen zu verschiedenen Problemen gegenüber dem BMJ
Entwurf eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis	Schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Gesetzes über Mitteilungen der Justiz von Amts wegen in Zivil- oder Strafsachen	Schriftliche Stellungnahme gegenüber dem BMJ
Entwurf einer Steuerdaten-Abrufverordnung	Beratung des BMF
Fünftes Gesetz zur Ändeung des Steuerberatungsgesetzes	Schriftliche Stellungnahme gegenüber dem BMF
Entwurf eines Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften	Beratung und schriftliche Stellungnahme gegenüber dem BMI, dem BMVg, dem Innenausschuß und dem Verteidigungsausschuß des Deutschen Bundestages
Kinder- und Jugendhilfegesetz	Beratung des BMJFFG und des zuständigen Ausschusses des Bundestages
Bundeserziehungsgeldgesetz	Schriftliche Stellungnahme gegenüber dem BMJFFG
Gesetz zur Änderung des Kraftfahrzeugsteuergesetzes und des Straßenverkehrsgesetzes	Stellungnahme gegenüber dem BMV sowie dem Verkehrs- und dem Finanzausschuß des Deutschen Bundestages
Zehntes Gesetz zur Änderung des Luftverkehrsgesetzes	Stellungnahme gegenüber dem BMV sowie dem Innen- und dem Verkehrsausschuß des Deutschen Bundestages
Gesetz über Gebühren für die Benutzung von Bundesfernstraßen mit schweren Lastfahrzeugen	Stellungnahme gegenüber dem BMV sowie dem Verkehrsausschuß des Deutschen Bundestages
Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen	Schriftliche Änderungsanregung gegenüber dem BMBau
Entwurf eines Strafverfolgungsstatistikgesetzes	Beratung und schriftliche Stellungnahme gegenüber dem BMJ
Gesetz zur Änderung des Mikrozensusgesetzes	Beratung des BMI und des Innenausschusses des Deutschen Bundestages sowie schriftliche Stellungnahme gegenüber dem BMI
Justizinformationssystem (JUSTIS)	Beratung und schriftliche Stellungnahme gegenüber dem BMJ
Entwurf eines Gesetzes zur Änderung datenschutzrechtlich relevanter Vorschriften im Gewerberecht	Schriftliche Stellungnahme gegenüber dem BMWi
Gesetz über Wasser- und Bodenverbände	Schriftliche Stellungnahme gegenüber dem BML

Thema	Art der Erledigung
Ernährungsvorsorgegesetz und Ernährungssicherstellungsgesetz	Schriftliche Stellungnahme gegenüber dem BML und dem BMI
Verordnung über die Anforderungen in der Meisterprüfung im Weinbau und Verordnung über die Anforderungen in der Meisterprüfung für den Beruf Landwirt/Landwirtin	Schriftliche Stellungnahme gegenüber dem BML
Richtlinie des Rates der Europäischen Gemeinschaften vom 7. Juni 1990 zu Informationen über die Umwelt	Beratung und schriftliche Stellungnahme gegenüber dem BMU
EG-Statistikverordnung vom 11. Juni 1990	Beratung und schriftliche Stellungnahme gegenüber dem BMI
Verordnung des Rates der Europäischen Gemeinschaften vom 7. Mai 1990 zur Errichtung einer Europäischen Umweltagentur und eines Europäischen Umweltinformations- und Umweltbeobachtungsnetzes	Schriftliche Stellungnahme gegenüber dem BMU
Vorschlag einer Verordnung des Rates der Europäischen Gemeinschaften zur Änderung der Verordung Nr. 283/72 betreffend die Unregelmäßigkeiten und die Wiedereinziehung zu Unrecht gezahlter Beiträge im Rahmen der Finanzierung der Gemeinsamen Agrarpolitik sowie die Einrichtung eines einschlägigen Informationssystems	Schriftliche Stellungnahme gegenüber dem BMF und dem BML
Entwurf einer EG-Datenschutzrichtlinie	Schriftliche Stellungnahme gegenüber den zuständigen Ressorts, Beratung mit in- und ausländischen Datenschutzbeauftragten
EG-Asylzuständigkeitsabkommen	Schriftliche Stellungnahme gegenüber dem BMI
Errichtungsanordnungen für Dateien des BfV	Schriftliche Stellungnahmen gegenüber dem BMI und dem BfV
Verkartungspläne für eine Abteilung des BfV	Schriftliche Stellungnahme gegenüber dem BMI und dem BfV
Organisatorische und technische Fragen der Datensicherheit beim BND	Beratung des BND
Fahndungsunion mit der ehemaligen DDR und Vorbereitung der Überführung von Dateien von Polizeidienststellen der ehemaligen DDR in Inpol	Beratungen mit dem BMI, dem BMF, dem Innenminister der früheren DDR, dem BKA und dem Zentralen Kriminalamt der ehemaligen DDR
Vorschriften für den personellen Geheimschutz	Beratungen und schriftliche Stellungnahme gegenüber dem BMVg und dem BMWi
Gesundheitsreformgesetz (datenschutzrechtliche Fortentwicklung)	Schriftliche Stellungnahme und Beratung gegenüber dem BMA und den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung

Thema	Art der Erledigung
Gesundheitsreformgesetz (Gestaltung der Krankenversichertenkarte)	Schriftliche Stellungnahme und Beratung gegenüber dem Verband der Angestellen-Krankenkassen
Ausweis für Arbeit und Sozialversicherung im Bereich der ehemaligen DDR	Schriftliche Stellungnahme und Beratung gegenüber dem BMA
Organisationsdienst für nachgehende Untersuchungen (ODIN)	Beratung und schriftliche Stellungnahme gegenüber dem BMA und der Chemie-BG
Automatisierte Personaldatenverarbeitung einschließlich APC-Einsatz, Beihilfe-, Telefondaten- und Textverarbeitung sowie entsprechende Dienstvereinbarungen	Beratungen und schriftliche Stellungnahmen gegenüber mehreren Behörden und Personalvertretungen
Verordnung zur Bestimmung des Musters und des Inhalts des Sozialversicherungsausweises, seiner Ausstattung mit einem Lichtbild und der Form der Eintragungen (Sozialversicherungsausweis-Verordnung)	Beratung und schriftliche Stellungnahme gegenüber dem BMA
Entwürfe von Datenschutzverordnungen für die Unternehmen der Deutschen Bundespost (Telekom, Postdienst und Postbank)	Beratung des BMPT und des Ausschusses für Post und Telekommunikation des Deutschen Bundestages sowie schriftliche Stellungnahme gegenüber dem BMPT
Sicherheit bei Telefax	Übersendung von Hinweisen sowie eines Merkblattes an die obersten Bundesbehörden
Beschaffung und Betrieb von Telekommunikationsanlagen	Rundschreiben mit Hinweisen an die obersten Bundesbehörden
Verbindungsdatenspeicherung bei Funktelefondiensten	Besprechunggen und Beratungen mit dem BMPT und zukünftigen Netzbetreibern
Regelungen für den datenschutzgerechten Einsatz von Arbeitsplatzcomputern	Mitwirken bei der Erstellung von Regelungen und Dienstanweisungen, insbesondere bei der DBP POSTDIENST und der DBP TELEKOM
Verbrauchsdatenerfassung mit TEMEX	Beratung des Bundesministers für Wirtschaft beim Entwurf von Datenschutzregelungen in den entsprechenden Verordnungen über allgemeine Bedingungen für die Versorgung
Einführung einer Kundennummer durch die DBP TELEKOM	Beratung und schriftliche Stellungnahme gegenüber der Generaldirektion
Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik	Beratungen des BMI, des Interministeriellen Koordinierungsausschusses für die Sicherheit in der Informationstechnik und des Innenausschusses des Deutschen Bundestages sowie schriftliche Stellungnahme gegenüber dem BMI
Datenverarbeitung durch Unternehmen mit Treuhandbeteiligung	Beratung der Treuhandanstalt

1.3 Besondere Erfolge und erfreuliche Feststellungen

Der Bundesbeauftragte für den Datenschutz ist nach § 19 BDSG Kontrollorgan. Seine Tätigkeit ist damit auf kritische Prüfung angelegt. Er ist, wie unter 1.4 noch ausgeführt wird, auch zu förmlichen Beanstandungen verpflichtet. Es ist ihm aber nicht untersagt, auch Lob auszusprechen. Solches ist insbesondere veranlaßt, wenn eine gesetzliche Regelung deutlich über das aus verfassungsrechtlichen Gründen gebotene Mindestmaß hinausgeht oder wenn Verwaltungsbehörden beim Vollzug von Rechts- und Verwaltungsvorschriften zum Schutz des Persönlichkeitsrechts der Bürger mehr tun, als die ihnen vorgegebenen Regelungen eigentlich fordern.

Dieser Bericht enthält verstreut in den einzelnen Kapiteln und Abschnitten derartige Feststellungen. Sie mögen für sich allein gesehen nichts besonders Großartiges darstellen. Sie zeigen aber jeweils eine besondere Sensibilität der Beteiligten für die Wahrung des Datenschutzes und verdienen es deshalb, besonders genannt zu werden. Da sie bei einer Gesamtlektüre des Berichts leicht untergehen, möchte ich erstmals einige aus meiner Sicht besonders datenschutzfreundliche Ereignisse des Berichtsjahres in einem eigenen Berichtsteil zusammenfassen und dabei auch die dafür verantwortlichen Behörden ausdrücklich hervorheben.

1. Unter den Gesetzen, die im Berichtszeitraum verabschiedet wurden, steht das *Gesetz zur Neuordnung des Kinderund Jugendhilferechts* auf einem hohen datenschutzrechtlichen Niveau. In enger und vertrauensvoller Zusammenarbeit mit dem *Bundesministerium für Jugend, Familie, Frauen und Gesundheit* und dem *Bundesministerium für Arbeit und Sozialordnung* ist noch während der Beratung des Gesetzentwurfs im Deutschen Bundestag ein besonderes Kapitel bereichsspezifischer Datenschutzregelungen erarbeitet und dem federführenden *Ausschuß für Jugend, Familie, Frauen und Gesundheit* als Formulierungshilfe vorgeschlagen worden. Dieser hat den Vorschlag in das Gesetz aufgenommen (s. 12.1).

2. Der *Bundesminister für Verkehr* hat die Erfassung und Verarbeitung von Telefongesprächsdaten in seinem neuen Dienstgebäude unter meiner Beteiligung so geregelt, daß alle meine datenschutzrechtlichen Vorschläge voll verwirklicht wurden (s. 7.2).

3. Die *Grenzschutzdirektion Koblenz* dokumentiert bei Abrufen aus dem Zentralen Verkehrsinformationssystem ZEVIS über die gesetzlich vorgeschriebenen Auswahlprotokollierungen hinaus jeden in diesem Zusammenhang erforderlichen Abruf auch in den Ermittlungsakten. Das läßt die Verantwortlichkeit für solche Abrufe eindeutig feststellen und beugt Mißbräuchen vor (s. 9.1.2).

4. Das *Zollkriminalinstitut* führt bei ZEVIS-Abrufen eine vollständige Zusatzprotokollierung durch. Dies führt im wesentlichen zu einem ähnlichen datenschutzfreundlichen Ergebnis wie das Verfahren der Grenzschutzdirektion (s. 9.1.2).

5. Das *Statistische Bundesamt* sieht davon ab, Einzelangaben nach § 14 Abs. 1 des Volkszählungsgesetzes 1987 zu veröffentlichen, wenn diese weniger als 50 Einzelfälle betreffen. Es gewährleistet damit einen hohen Grad an Anonymität des Bürgers und schützt damit das Persönlichkeitsrecht (s. 10.3).

1.4 Beanstandungen

Rechtsverstöße gegen Bestimmungen des Bundesdatenschutzgesetzes oder auch gegen datenschutzrechtliche Bestimmungen anderer Gesetze habe ich nach § 20 des Bundesdatenschutzgesetzes zu beanstanden. Die Anzahl der im Berichtsjahr ausgesprochenen Beanstandungen entspricht der des vergangenen Jahres. In diesem Zusammenhang muß aber erwähnt werden, daß meine Kontroll- und Beratungstätigkeit sich seit dem 3. Oktober 1990 stark auf die Behörden und öffentlichen Stellen in den neuen Ländern konzentriert hat. Dort habe ich von förmlichen Beanstandungen bewußt abgesehen, weil der Gedanke des Datenschutzes erst Fuß fassen mußte. Ich habe mich insoweit bei meiner Kontrolle ganz bewußt auf eine Beratung konzentriert.

Die gleichbleibend hohe Zahl von Beanstandungen gegenüber dem Bundesminister für Post und Telekommunikation ist ebenso augenscheinlich wie dessen Weigerung, rechtswidrige Datenverarbeitungen, die in den Vorjahren beanstandet worden waren, zu beheben. Der Umgang mit den Daten der Postkunden ließ in manchen Fällen nicht den notwendigen Respekt vor deren Persönlichkeitsrecht erkennen. Manche Beanstandung ließe sich vermeiden, wenn mich der Bundesminister für Post und Telekommunikation jeweils so rechtzeitig in seine Planungen einbeziehen würde, daß die datenschutzrechtlichen Fragen und Problemstellungen von Anfang an berücksichtigt werden können.

Von erheblicher Bedeutung ist auch die gegenüber dem Bundesminister des Innern ausgesprochene Beanstandung wegen der Gewährung unmittelbaren Zugriffs von Polizeidienststellen der Länder auf den Aktennachweis des BKA (BKA-AN). Dieser seit langem von mir kritisierte Zustand ist erst auf meine förmliche Beanstandung hin beseitigt worden.

Hervorzuheben sind auch die Beanstandungen beim Bundesnachrichtendienst, zu denen das Bundeskanzleramt und der Bundesnachrichtendienst aber erfreulicherweise schnelle Abhilfe zugesagt haben.

Aus dem Rahmen fällt schließlich die Beanstandung bei einem als bundesunmittelbare Anstalt des öffentlichen Rechts geführten Versicherungsunternehmen, das den Inhalt von Kundenanrufen aufgezeichnet und anschließend für Schulungszwecke verwendet hat. Diese Praxis ist nach meiner Beanstandung eingestellt worden.

Es fällt auf, daß mehrere Beanstandungen wegen mangelnder Unterstützung meiner Dienststelle ausgesprochen werden mußten. Zwar verläuft die Zusammenarbeit mit den allermeisten Behörden vertrauensvoll und reibungslos. Gleichwohl gibt es im-

mer wieder Fälle, in denen das Verhalten von Behörden und Dienststellen die Erfüllung meiner Aufgaben beeinträchtigt. Wenn z. B. eine für die weitere Durchführung einer datenschutzrechtlichen Kontrolle getroffene Absprache trotz Fristsetzung nicht eingehalten und erst nach förmlicher Beanstandung umgesetzt wird, wie im Bundesministerium der Verteidigung, oder erbetene Auskünfte ohne jede Reaktion und trotz Fristsetzung nicht erteilt werden — so bei der Bundesanstalt für Flugsicherung —, so zeugt dies für wenig Verständnis für die Aufgaben meiner Dienststelle.

Die Beanstandungen im einzelnen:

Staatssekretär beim Bundeskanzler	Verstoß gegen § 9 Abs. 1, § 19 Abs. 3 BDSG und gegen andere Vorschriften des Datenschutzes durch den Bundesnachrichtendienst (siehe 20.)
Bundesminister des Innern	— Verstoß des Bundeskriminalamtes gegen das Bundesdatenschutzgesetz durch weitere Gewährung des unmittelbaren Zugriffs von Polizeidienststellen der Länder auf den BKA-AN; Verstoß gegen § 10 BDSG (s. 17.3) — Verstoß des Bundesamtes für Verfassungsschutz gegen das Bundesdatenschutzgesetz in einem Einzelfall im Zusammenhang mit der Durchführung der Sicherheitsüberprüfung bei einer obersten Bundesbehörde; Verstoß gegen § 10 BDSG (siehe 19.3)
Bundesminister der Verteidigung	Nichteinhaltung einer Absprache über notwendige Vorbereitungen zur Durchführung einer Datenschutzkontrolle; Verstoß gegen § 19 Abs. 3 BDSG (siehe 7.3)
Bundesminister für Verkehr	Verweigerung erbetener Auskünfte durch die Bundesanstalt für Flugsicherung; Verstoß gegen § 19 Abs. 3 BDSG (siehe 7.2)
Bundesminister für Post und Telekommunikation	— Rechtswidrige Übermittlung von Daten über Kontosperren aufgrund einer Verfügung des Bundesministers für Post und Telekommunikation; Verstoß gegen § 10 BDSG (siehe 8.3) — Unzulässige Übermittlung der Daten von Mobilfunkkunden an ein Marktforschungsinstitut durch die Deutsche Bundespost TELEKOM; Verstoß gegen § 11 BDSG (siehe 8.6) — Entgegen § 454 Abs. 1 TKO durchgeführte und deshalb unzulässige Nutzung der Daten von BTX-Mitbenutzern für Werbezwecke (siehe 8.6)
Bundesminister für Raumordnung, Bauwesen und Städtebau	— Mangelnde organisatorische Sicherstellung des Datenschutzes, insbesondere beim Umgang mit Personaldaten; Verstoß gegen § 15 BDSG (siehe 5.1) — Nichtaufnahme von Dateien in die Dateiübersicht und Nichtmeldung zum bei mir geführten Register; Verstoß gegen § 15 und § 19 Abs. 4 BDSG (siehe 5.1)
Bundesanstalt für Arbeit	Verstoß gegen das in § 1758 BGB verankerte Ausforschungsverbot durch Verwendung unzulässiger Vordrucke (siehe 13.)
Eine Berufsgenossenschaft	Verletzung des Personalaktengeheimnisses (siehe 7.3)
Ein Versicherungsunternehmen (bundesunmittelbare Anstalt des öffentlichen Rechts)	Unzulässige Tonbandaufzeichnung von Kundenanrufen und Verwertung dieser Aufzeichnungen; Verstoß gegen § 201 Nr. 1 und 2 1. Alternative StGB (siehe 6)

1.5 Zusammenarbeit mit den Landesbeauftragten für den Datenschutz und mit anderen Stellen

Im Berichtszeitraum hat die Konferenz der Datenschutzbeauftragten von Bund und Ländern Entschließungen zu folgenden Themen gefaßt:

- Bundesdatenschutzgesetz und Bundesverfassungsschutzgesetz (Entschließung vom 22./23. März 1990, Anlage 3)
- Datenschutz im deutsch-deutschen Verhältnis (Entschließung vom 22./23. März 1990, Anlage 4)
- Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (Entschließung vom 27. Juni 1990, Anlage 5)
- Neuregelung des Melderechtsrahmengesetzes (Entschließung vom 4./5. Oktober 1990, Anlage 6)
- Erarbeitung von Krebsregister-Gesetzen in Bund oder Ländern (Entschließung vom 4./5. Oktober 1990, Anlage 7)
- Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nicht öffentlich gesprochenen Wortes (Entschließung vom 4./5. Oktober 1990, Anlage 8)
- Vorschlag der EG-Kommission für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten (Entschließung vom 29. Januar 1991, Anlage 9).
- Telekommunikation und Datenschutz (Entschließung vom 8. März 1991, Anlage 10).

Die Arbeitskreise der Konferenz bereiteten im Berichtszeitraum nicht nur vorstehend genannte Entschließungen vor, sie bearbeiteten auch Probleme, die für den Datenschutz in Bund und Ländern bedeutsam waren. So hat sich z. B. der Arbeitskreis Personalwesen eingehend mit dem Entwurf eines Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften befaßt und zahlreiche Einzelfragen, u. a. das Fragerecht des Arbeitgebers, erörtert.

Unverändert gut ist die Zusammenarbeit mit europäischen Institutionen des Datenschutzes geblieben (s. hierzu insbesondere Abschnitt 28 dieses Berichts).

Nach wie vor zeigte sich als wichtig, daß ich an Sitzungen des Düsseldorfer Kreises teilnehme, in dem die Aufsichtsbehörden der Länder ihre gemeinsamen Probleme beraten, in deren Arbeitsgremien mitarbeite und mich damit über aktuelle Fragen des Datenschutzes im nicht-öffentlichen Bereich informieren kann (s. unten 27).

Im Berichtszeitraum habe ich viele Gespräche mit Vertretern von Firmen geführt, die DV-Anlagen und Software-Produkte herstellen oder vertreiben, und dabei für die Belange des Datenschutzes geworben.

Unverändert sind die Teilnahme von Vertretern meiner Dienststelle an Sitzungen der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV), von Gremien des deutschen Instituts für Normung e. V. (DIN) und die gute Zusammenarbeit mit dem jetzigen Bundesamt für Sicherheit in der Informationstechnik, früher Zentralstelle für Sicherheit in der Informationstechnik.

1.6 Die Dienststelle

Die Arbeit meiner Dienststelle ist durch die Vorbereitung des Einigungsvertrags und durch Hilfestellung zum Aufbau der Verwaltung in den neuen Ländern beeinflußt worden. Trotz der damit verbundenen Auswirkungen auf meine kleine Dienststelle war es selbstverständlich, daß ich umgehend einen Referenten für Arbeiten des Bundesministers des Innern im Zusammenhang mit dem Einigungsvertrag freigestellt und einen Referatsleiter vier Monate lang für den Aufbaustab einer Landesregierung zur Verfügung gestellt habe. Die mit der deutschen Vereinigung auch für mich eingetretene Aufgabenzunahme konnte natürlich nicht ohne Einfluß auf die personelle Ausstattung meiner Dienststelle bleiben. Der Einigungsvertrag hat mir unter anderem im Zusammenhang mit der Sicherung und Nutzung der MfS-Unterlagen zusätzliche und weitreichende Kontrollaufgaben eingeräumt. Aus diesem Grunde habe ich ein neues Referat „Aufarbeitung der MfS-Unterlagen, Allgemeine Innere Verwaltung, Strafrecht" gebildet. Die Vermehrung der Aufgaben zeigt sich auch auf allen anderen Gebieten. Die Zahl der zu kontrollierenden Behörden hat sich durch die Errichtung einer großen Zahl von Bundesbehörden im Beitrittsgebiet erhöht. Die Überleitung der früheren DDR-Verwaltung und -Gesetzgebung auf die Bundesverwaltung und Bundesgesetzgebung wirft völlig neue datenschutzrechtliche Fragen auf. Bürger der DDR machen in großer Zahl von ihrem Recht, Eingaben an mich zu richten, Gebrauch. Ich habe deshalb bei den Haushaltsverhandlungen darauf gedrungen, meiner Dienststelle in ausreichendem Maße Personal zur Verfügung zu stellen, um von Anfang an die Beratungs- und Kontrollaufgaben in einem den Bürgern der ehemaligen DDR sichtbaren und damit Vertrauen schaffenden Umfang einleiten und durchführen zu können.

Meinen in diesem Zusammenhang erhobenen Personalforderungen wurde im wesentlichen entsprochen, wofür ich allen Beteiligten dankbar bin. Leider wurde die Stelle für den Leiter des genannten neuen Referates, die im Haushaltsentwurf auf Regierungsebene bereits zugestanden war, im weiteren Verlauf der Verhandlungen gestrichen. Auch die seit Jahren fehlende Stelle für den Leiter des Referats Informationstechnik ist noch nicht bewilligt worden. Ich halte es für unerläßlich, daß die noch offenen Stellenforderungen in den Haushalten 1991 und 1992 noch berücksichtigt werden.

2 Datenschutz im Beitrittsgebiet

2.1 Überblick

Schon zu Beginn des Berichtsjahres wurde erkennbar, daß die auf eine Vereinigung hinsteuernde, von Woche zu Woche enger werdende Zusammenarbeit beider Staaten angesichts des vollständigen Fehlens vergleichbarer Datenschutzbestimmungen in der DDR eine Fülle von Fragen zum Datenschutz und zum Umgang mit personenbezogenen Daten allgemein aufwarf. In enger Zusammenarbeit mit dem Bundesministerium des Innern habe ich damals Grundsätze für den Austausch personenbezogener Daten zwischen den beiden deutschen Staaten erarbeitet. Die Konferenz der Datenschutzbeauftragten von Bund und Ländern hat sich am 22./23. März 1990 mit diesem Thema befaßt. Die damals gefaßte Entschließung (Anlage 4) hat weitgehend die zwischen dem Bundesminister des Innern und mir erarbeiteten Grundsätze übernommen.

Als der Entschluß gefaßt war, im Zusammenhang mit der für den 1. Juli 1990 vorgesehenen Wirtschafts-, Währungs- und Sozialunion die Grenzkontrolle zwischen beiden deutschen Staaten abzuschaffen, war es unvermeidbar, unverzüglich Fragen des Datenaustausches und der informationellen Zusammenarbeit zwischen den Sicherheitsbehörden der Bundesrepublik Deutschland und der DDR zu klären. Deshalb habe ich noch vor Herstellung der in diesem Zusammenhang vereinbarten Fahndungsunion (s. unten 2.3) dem Innenminister der DDR Inhalt und Funktion des Datenschutzes und der Datenschutzkontrolle im Zusammenhang mit der Arbeit der Polizei in einem persönlichen Gespräch erläutert. Schon bei dieser Begegnung wurde deutlich, welche ungeheuere Last die Dateien und Unterlagen des ehemaligen Staatssicherheitsdienstes darstellten (s. 2.5). Nach der Vereinbarung der Fahndungsunion hat der Ministerrat der DDR — einem Wunsch des Deutschen Bundestages folgend — mich mit der datenschutzrechtlichen Kontrolle des Umgangs der DDR-Behörden mit den durch das Bundeskriminalamt an Stellen der DDR übermittelten Fahndungsdaten beauftragt. Entsprechend diesem Auftrag habe ich schon vor dem 3. Oktober 1990 die Verarbeitung dieser Daten durch Stellen der DDR kontrolliert und diese Stellen in Datenschutzfragen beraten.

Noch zur Jahresmitte 1990 war die DDR bestrebt, die Voraussetzungen für die Vereinigung durch eine möglichst weitgehende Rechtsangleichung herzustellen. Die DDR hatte eine interministerielle Kommission zur Ausarbeitung eines Datenschutzgesetzes berufen, die von Experten aus „alten" Bundesländern und aus meiner Dienststelle beraten wurde. Die Arbeit dieser Kommission wurde jedoch mit dem Beginn der Verhandlungen über den Einigungsvertrag obsolet.

Die Bundesregierung hat mich an den Arbeiten zum Einigungsvertrag in vorbildlicher Weise beteiligt. Dadurch war es möglich,die Belange des Datenschutzes innerhalb des Vertragswerks von Anfang an hinreichend zur Geltung zu bringen (s. unten 2.2).

Mit der Herstellung der Einheit Deutschlands am 3. Oktober 1990 sind Qualität und Umfang der Fragen, die sich auf dem Gebiet des Datenschutzes stellen, erst voll deutlich geworden. Datenschutzrechtliche Probleme ergaben sich in fast allen Lebensbereichen, und zwar sowohl bei der öffentlichen Verwaltung als auch im nicht-öffentlichen Bereich. Besonders deutlich wurden sie bei den großen zentralen Datensammlungen der ehemaligen DDR wie z. B. dem Zentralen Einwohnerregister (s. 2.8) einschließlich des sogenannten Fahrerlaubnisregisters (s. 2.10), dem Datenspeicher „Gesellschaftliches Arbeitsvermögen" (s. unten 2.14), dem Zentralen Strafregister des früheren Generalstaatsanwalts der DDR (s. 2.9), dem dialogorientierten Auswertungs- und Recherchesystem DORA des Zentralen Kriminalamts der früheren DDR (s. 2.4) und dem Nationalen Krebsregister (s. 2.12). Das rechtlich und menschlich schwierigste datenschutzrechtliche Problem stellen jedoch die Dateien und Unterlagen des ehemaligen Ministeriums für Staatssicherheit dar (s. unten 2.5).

Andere völlig neue datenschutzrechtliche Fragen ergaben sich aus der Existenz von Einrichtungen, die der Effizienz der Verwaltung im kommunistischen Staat hatten dienen sollen, wie etwa der einheitlichen Personenkennzahl (s. unten 2.8.5) oder dem „Ausweis für Arbeit und Sozialversicherung" der DDR, der eine Fülle besonders schützenswerter Sozial- und Gesundheitsdaten enthält (s. unten 2.11.1).

Es war von vornherein klar, daß diese Instrumente nicht von der Bundesrepublik Deutschland übernommen werden konnten.Sie konnten aber nicht sofort ersatzlos abgeschafft werden, ohne zugleich die Erfüllung wichtiger im Interesse der Bürger liegender Aufgaben zu gefährden. Weitere Probleme ergaben sich aus der Privatisierung ehemals öffentlicher Einrichtungen in den neuen Ländern, darunter auch Rechenzentren, die personenbezogene Daten für die öffentliche Verwaltung verarbeiteten.

Immer mehr trat im Laufe der letzten Monate die Frage in den Vordergrund, wie Personalfragebogen in den neuen Ländern, aber auch in der Bundesverwaltung, aussehen sollten und durften, die Bewerber für den öffentlichen Dienst auszufüllen hatten. Die zahlreichen Petitionen hierzu kreisten stets um das Thema, welche Fragen den Bewerbern in Bezug auf ihre Tätigkeit und ihr Leben vor der Wende gestellt werden dürfen (s. unten 2.7).

Viele Bürger aus den neuen Bundesländern haben bereits Anfragen und Eingaben an mich gerichtet. Die Aufgabe, dort bis zur Einsetzung von Landesbeauftragten für den Datenschutz die Einhaltung des Datenschutzes auch im Bereich der Landes- und Kommunalverwaltung zu kontrollieren, verstehe ich in erster Linie als Auftrag, die Behörden mit den Erfordernissen des Datenschutzes vertraut zu machen und Hilfe beim Aufbau einer eigenen Datenschutzkontrolle zu leisten. Mit dieser Zielrichtung habe ich alle Minister der neuen Bundesländer durch eine Grundinformation zum Datenschutz auf die wichtigsten Regelungen des Bundesdatenschutzesgesetzes hingewiesen und ihnen meine Beratungen in allen Fragen des Datenschutzes angeboten. Auf meine Initiative

hin hat die Bundesakademie für öffentliche Verwaltung den Datenschutz in ihr Schulungs- und Ausbildungsprogramm für die neuen Bundesländer aufgenommen.

2.2 Einigungsvertrag

Kernstück der datenschutzrechtlichen Regelungen des Einigungsvertrages ist die Überleitung des Bundesdatenschutzgesetzes (Anlg. I, Kap. II, Sachgebiet C, Abschnitt III, 3.), das allerdings im Hinblick auf die Gegebenheiten in der früheren DDR für eine Übergangszeit durch einige Maßgaben modifiziert wurde.

Vordringlich war vor allem, eine allgemeine Regelung für den Umgang mit solchen Datenbeständen zu finden, die nach dem Beitritt infolge des Wegfalls von Aufgaben und Behörden nicht mehr gebraucht werden oder deren Speicherung nach Bundesrecht von vornherein unzulässig gewesen wäre. § 14 Abs. 3 des noch geltenden BDSG, der die Löschung im ersten Fall in das Ermessen der Behörde stellt, wurde mit Blick auf die ab 1. Juni 1991 geltende Fassung des Gesetzes, die in solchen Fällen eine Löschung vorschreibt, auch für die Zeit vorher als unzureichend angesehen. Deshalb ist bestimmt worden, daß Daten grundsätzlich stets unverzüglich zu löschen sind, wenn ihre Kenntnis nicht mehr erforderlich ist oder sie nach Bundesrecht nicht hätten gespeichert werden dürfen. Diese Löschungsverpflichtung steht unter dem Vorbehalt, daß damit nicht schutzwürdige Belange der Betroffenen beeinträchtigt werden. Es soll damit sichergestellt werden, daß die Aufarbeitung der Vergangenheit nicht auf dem Rücken der Betroffenen und ausschließlich mit dem Reißwolf erfolgt. Ob dies gelingt, wird freilich davon abhängen, daß die Verantwortlichen ein ausreichendes Gespür für die Belange der Bürger entwickeln, und daß die Bereitschaft besteht, den Betroffenen in Zweifelsfällen vor einer Löschung Gelegenheit zur Geltendmachung ihrer Belange zu geben.

Einer weiteren Maßgabe zufolge habe ich in dem durch § 7 Abs. 2 BDSG vorgegebenen Rahmen bis zur Einsetzung von Landesbeauftragten für den Datenschutz, längstens jedoch bis zum Ende des Jahres 1991, die Datenschutzkontrolle auch gegenüber Behörden der Länder als Organ der Länder auszuüben. Angesichts der bestehenden Verhältnisse in den neuen Bundesländern kann dies indessen nicht die sofortige Übertragung der in den „alten" Ländern gewohnten Kontrollpraxis bedeuten. Ich sehe meine Aufgabe vielmehr in erster Linie darin, die Verwaltungen der Gemeinden und der Länder sowie die neuen Stellen der Bundesverwaltung mit den Bestimmungen des bereichsspezifischen und des allgemeinen Datenschutzrechts und den bewährten Grundsätzen für ihre Umsetzung vertraut zu machen. Der Akzent bei der Wahrnehmung meiner Aufgaben im Beitrittsgebiet wird deshalb in besonderem Maße auf der Beratung in allen Fragen des Datenschutzes liegen.

Das Schicksal der in der früheren DDR verwendeten einheitlichen, d. h. in allen Verwaltungszweigen identischen Personenkennzahl (s. 2.8.5) ist in einer Anmerkung zur Überleitungsbestimmung geregelt worden. Danach sind alle Dateien in den neuen Bundesländern — also auch solche aus dem Bereich der Privatwirtschaft —, die nach diesem einheitlichen Personenkennzeichen geordnet sind, unverzüglich nach anderen Merkmalen umzuordnen. Das Personenkennzeichen ist in allen Dateien zum frühestmöglichen Zeitpunkt zu löschen. Wie bereits in den Verwaltungen der Bundesrepublik Deutschland wird damit die Möglichkeit, über ein einheitliches Zugriffskriterium alle im staatlichen Bereich vorhandenen Daten über eine Person zusammenzuführen, ausgeschlossen.

Der Einigungsvertrag enthält auch eine vorläufige Regelung des Umgangs mit den Akten des Staatssicherheitsdienstes (s. unten 2.5), die solange gelten soll, bis der gesamtdeutsche Gesetzgeber eine endgültige Regelung verabschiedet hat (Anlg. I Kap. II, Sachgebiet B, Abschnitt II; s. unten 2.5.3). Die Unterlagen des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit der früheren DDR sind von einem Sonderbeauftragten der Bundesregierung in sichere Verwahrung zu nehmen. Kernstück der materiellrechtlichen Regelung ist die Sperrung der betreffenden Dateien und Unterlagen. Die Übermittlung und Nutzung von Daten aus diesen ist ausgeschlossen. Von diesem strengen Verbot gibt es allerdings eng umgrenzte Ausnahmen. Sie stehen unter dem Vorbehalt, daß die Übermittlung und Nutzung unerläßlich und nicht bis zu einer abschließenden gesetzlichen Regelung aufschiebbar ist.

In den Einigungsvertrag sind schließlich einige datenschutzrechtlich bedeutsame Bestimmungen zum Melderecht aufgenommen worden, die insbesondere die Abwicklung des Zentralen Einwohnerregisters der DDR betreffen (s. unten 2.8). Insbesondere ist vorgesehen, das Melderecht in den neuen Bundesländern innerhalb eines Jahres nach Wirksamwerden des Beitritts nach den Vorschriften des Melderechtsrahmengesetzes zu gestalten und die örtlichen Melderegister unverzüglich in der Weise umzustellen, daß die Inanspruchnahme des Zentralen Einwohnerregisters entbehrlich wird.

Von erheblicher Bedeutung ist auch, daß der Einigungsvertrag die Rechtsgrundlage, auf der das Nationale Krebregister der früheren DDR betrieben wurde, nicht aufrechterhalten hat. Daraus ergeben sich eine Reihe von Problemen, die in einem besonderen Abschnitt dargestellt werden (s. unten 2.12).

2.3 Fahndungsunion

Im Zusammenhang mit der Einführung der Wirtschafts-, Währungs- und Sozialunion haben die Regierungen der Bundesrepublik Deutschland und der ehemaligen DDR beschlossen, die grenzpolizeilichen Personenkontrollen an der deutsch-deutschen Grenze zum 1. Juli 1990 abzubauen. Es wurde deshalb zur gemeinsamen Bekämpfung der Kriminalität und zur Durchführung von Maßnahmen der Strafverfolgung von den Innenministerien beider Länder unter meiner Mitwirkung eine Fahndungsunion zwischen den Poli-

zeidienststellen vereinbart. Diese Fahndungsunion wurde auch im Staatsvertrag über die Wirtschafts- und Währungsunion verankert; der dabei zulässige Datenaustausch wurde genau umschrieben, nachdem ich darauf hingewiesen hatte, daß dafür eine einwandfreie Rechtsgrundlage erforderlich sei. Die Fahndungsunion wurde bis zum 3. Oktober 1990 wie folgt durchgeführt:

Nach Artikel 15 der Vereinbarung über die Aufhebung der Personenkontrollen an den innerdeutschen Grenzen übermittelten die Polizeidienststellen beider Länder aus den Fahndungsbeständen die Ausschreibungen zur Festnahme wegen einer Straftat oder zur Strafvollstreckung aufgrund einer bestehenden oder beantragten richterlichen Entscheidung, die Ausschreibungen zur Festnahme von Ausländern aufgrund rechtskräftiger ausländerrechtlicher Entscheidungen, außerdem Ausschreibungen von minderjährigen Vermißten oder von sonstigen Personen, die im Interesse des eigenen Schutzes in Gewahrsam genommen werden sollten. Daneben wurden der Grenzfahndungsbestand, beschränkt auf Ausschreibungen zur Zurückweisung, zur ausschließlichen Verwendung durch die mit grenzpolizeilichen Aufgaben betrauten Stellen, und der Bestand „Zollrechtliche Überwachung" zur ausschließlichen Verwendung durch die Grenzzollstellen zu Zwecken der Rauschgiftbekämpfung übermittelt.

Die Übermittlung der genannten Fahndungsbestände der Bundesrepublik Deutschland erfolgte durch das Bundeskriminalamt mittels Magnetbändern an das Zentrale Kriminalamt der ehemaligen DDR. Hier hatten zwei Terminals Online-Zugriff auf das Inpol-Fahndungssystem, allerdings beschränkt auf die vorerwähnten Ausschreibungen ohne die Bestände Grenzfahndung und Zollrechtliche Überwachung. Bei der Grenzschutzhauptdirektion der ehemaligen DDR hatte ein weiteres Terminal diesen Online-Zugriff, jedoch erweitert um den Bestand Grenzfahndung. Beim Zentralen Zollfahndungsamt der ehemaligen DDR hatte ein Terminal lediglich Zugriff auf den Bestand Zollrechtliche Überwachung. Unter meiner Mitwirkung wurden zusätzliche Regelungen, wie z. B. die Zweckbindung der übermittelten Daten, erarbeitet. Die Beachtung dieser Regelungen habe ich bei zwei Kontrollen noch vor der Verwirklichung der deutschen Einheit überprüft. Dabei ergaben sich keine Anhaltspunkte, daß unzulässige Abfragen im Inpol-Personenfahndungsbestand vorgenommen worden sind. Die Vereinbarung hatte vorgesehen, daß das Zentrale Kriminalamt die Datenbestände mittels Diskette an die 150 auf dem Gebiet der DDR bei Bezirks- und Kreiskriminalämtern installierten Personalcomputer verteilt. Hierzu ist es aber wegen der am 3. Oktober vollzogenen Vereinigung Deutschlands nicht mehr gekommen.

Zur Erhöhung der Sicherheit der PC-Anwendungen habe ich dem Zentralen Kriminalamt, das jetzt als gemeinsame Behörde der neuen Länder geführt wird, vorgeschlagen, eine vom Bundesamt für Sicherheit in der Informationstechnik empfohlene Sicherheitssoftware einzusetzen. Dieser Vorschlag wird derzeit geprüft.

Seit dem 3. Oktober 1990 haben die Polizeidienststellen der neuen Bundesländer Zugriff auf den gesamten Inpol-Personenfahndungsbestand erhalten. Er wird — wie für die Fahndungsunion geplant — mittels Terminals beim Gemeinsamen Landeskriminalamt der fünf neuen Bundesländer, beim Zentralen Zollfahndungsamt, bei der Grenzschutzdirektion, Außenstelle Berlin, und — in der Fläche — über 150 Personalcomputer bei Bezirks- und Kreiskriminalämtern durchgeführt. Die Bestände „zollrechtliche Überwachung" und „Grenzfahndung" sind auch in den neuen Ländern für die Dienststellen der allgemeinen Polizei nicht zugänglich. Es ist geplant, die Polizeidienststellen der neuen Länder auch auf andere polizeiliche Datenbestände, wie PIOS- und SPUDOK-Anwendungen, zugreifen zu lassen.

2.4 Datei DORA der Kriminalpolizei der ehemaligen DDR

Die Kriminalpolizeidienststellen in der früheren DDR verfügten seit 1988 über ein dialogorientiertes Auswertungs- und Recherchesystem (DORA), das beim Zentralen Kriminalamt betrieben wurde. Es wurde auch von 15 Bezirkskriminalämtern sowie 104 Kreiskriminalämtern genutzt.

Der Umfang des in DORA gespeicherten Personendatensatzes war unterschiedlich. Bei geringfügigen Straftaten, Straftaten ohne überregionale Bedeutung und Straftaten, die keine Rückfalltaten waren, konnten die meldepolizeilichen Daten, der Urteilsspruch, Haftinformationen, der Hinweis auf erkennungsdienstliche Unterlagen und das Delikt, wegen dessen ermittelt wurde, gespeichert werden. Bei Straftaten von erheblicher Bedeutung konnte der Datensatz darüber hinaus auch Daten zur Beschreibung der Person, zum Tathergang und zur polizeilichen Beobachtung enthalten. In der Datei wurden auch Daten über Personen gespeichert, bei denen der Verdacht oder auch nur die Vermutung bestand, daß sie als Republikflüchtlinge in Betracht kommen könnten. Schließlich enthielt die Datei auch Daten über Fahrerlaubnisse und andere Erlaubnisse (z. B. Jagdschein) und Informationen über Arbeitsstellen. Andere Untersuchungsorgane (z. B. Dienststellen der Staatssicherheit) konnten Informationen an DORA weitergeben.

Durch Abgleich der DORA-Daten mit den entsprechenden Dateien des Zentralen Melderegisters (Zentrale Personendatei), der Haftdatei und der Kriminalstatistik Teil II, die beim Generalstaatsanwalt der früheren DDR geführt wurde und Informationen über Gerichtsurteile enthielt, wurden die in DORA gespeicherten Informationen ständig aktualisiert.

Nach der Vereinigung der beiden deutschen Staaten wurde das Zentrale Kriminalamt der früheren DDR als Gemeinsames Landeskriminalamt der neuen Bundesländer (GLKA) weitergeführt. Es ist damit auch speichernde Stelle für die Datei DORA.

Strafrechtsänderungsgesetze der ehemaligen DDR nach der „Wende" und die neue Rechtslage aufgrund

der Vereinigung Deutschlands haben zu umfassenden Bereinigungsaktionen des Datenbestandes der Datei geführt. Jetzt werden in DORA nur noch Daten von Personen erfaßt, die Straftaten begangen haben. Dadurch ist auch die Speicherung der Personen, die als Republikflüchtlinge in Betracht kommen konnten, entfallen; allein diese Maßnahme hat zu einem Wegfall von 65 000 Datensätzen geführt. Nach 750 000 Datensätzen im Jahre 1988 waren im Berichtsjahr in der Datei DORA nur noch ca. 450 000 Personendatensätze gespeichert. Darunter können immer noch Daten sein, die auf rechtsstaatlich nicht zulässige Art erhoben worden sind. Deshalb muß der DORA-Bestand noch weiter überprüft und bereinigt werden. Eine Arbeitsgruppe, die ich berate, entwickelt derzeit die Kriterien für eine Übernahme der DORA-Daten in das INPOL-System. Wenn, wie beabsichtigt, das überarbeitete DORA-Verfahren beim GLKA und den Polizeidienststellen im Beitrittsgebiet weiterbetrieben wird, muß sichergestellt sein, daß nur solche Daten in das INPOL-System übernommen werden, die die Kriterien für die Aufnahme in den Kriminalaktennachweis erfüllen.

Um die Meldedaten in der Datei DORA auf dem neuesten Stand zu halten, findet ein Datenabgleich mit dem Zentralen Einwohnerregister statt. Allerdings ist der bisher im Zentralen Einwohnerregister gespeicherte Hinweis auf kriminalpolizeiliche Vorgänge zur Person (sog. K-Vermerk) mittlerweile gelöscht worden.

Im Unterschied zu den Verbund-Dateien der Kriminalpolizei des Bundes und der „alten" Bundesländer steht den Kriminalpolizeidienststellen im Beitrittsgebiet der Gesamtdatenbestand von DORA nicht in direktem Zugriff zur Verfügung. Diesen hat lediglich das GLKA. Die Stand-alone-Personalcomputer in den Bezirkskriminalämtern haben Zugriff auf die für den Bezirk relevanten Daten; dies gilt für die Kreiskriminalämter entsprechend.

Das GLKA ist jetzt auch für die Beantwortung von Auskunftsersuchen der Kriminalpolizeidienststellen des Bundes und der alten Bundesländer zuständig. Wegen der erheblichen Schwierigkeiten bei der Kommunikation, aber auch aus personellen Gründen, ist es jedoch nicht in der Lage, die anfallenden ca. 8 000 Auskunftsersuchen der Kriminalpolizeidienststellen pro Monat zu beantworten. Deshalb ist beabsichtigt, solche Auskunftsersuchen durch das Bundeskriminalamt anstelle des GLKA bearbeiten zu lassen. Das Bundeskriminalamt soll hierzu mittels dreier Personalcomputer auf eine sog. FINDEX-Datei zugreifen, die komprimierte Datensätze aus DORA enthält. Der FINDEX-Datensatz soll aus den Personengrunddaten, aus dem Aktenzeichen sowie der Anschrift der aktenführenden Kriminalpolizeidienststelle bestehen. Weitere Hinweise soll sie nicht liefern. Da, wie bereits erwähnt, DORA bis zur endgültigen Bereinigung auch noch Daten enthält, die auf unzulässige Weise erhoben sein können, ist aus datenschutzrechtlicher Sicht eine Auskunftserteilung des Bundeskriminalamtes an die anfragende Polizeidienststelle nur hinzunehmen, wenn u. a. folgende Kriterien eingehalten werden:

- Das Bundeskriminalamt weist die anfragende Dienststelle bei einem Treffer in der DORA-FINDEX-Datei lediglich auf das Vorhandensein von Informationen bei der aktenführenden Polizeidienststelle und außerdem darauf hin, daß es sich hierbei um ungeprüfte Informationen handelt.
- Die anfragende Polizeidienststelle ergreift aufgrund dieser Auskunft grundsätzlich keine strafprozessualen Maßnahmen gegen den Betroffenen und erteilt über diese Speicherung keine Auskunft.
- Die aktenführende Polizeidienststelle nimmt das Auskunftsersuchen zum Anlaß für eine umfassende Prüfung der Zulässigkeit der Speicherung und der weiteren Aufbewahrung der Akte; der interne Datenschutzbeauftragte ist daran zu beteiligen.
- Soweit die Speicherung nicht mehr zulässig ist, werden die Akte aus der aktuellen Kriminalaktenhaltung entfernt und der Personendatensatz dem Zugriff in der aktuellen DORA-Datei entzogen. Diese eigentlich auszusondernde Kriminalakte und der Personendatensatz dürfen dann nur noch für Zwecke der Rehabilitierung des Betroffenen genutzt werden.
- Danach wird Auskunft in rechtmäßigem Umfang erteilt.
- Ergibt die Prüfung die Zulässigkeit der weiteren Speicherung, so ist das BKA über das GLKA zu unterrichten. Der Datensatz in der FINDEX-Datei wird dann mit dem Hinweis auf die erfolgte Prüfung versehen.

Inzwischen wurde mir bekannt, daß die Innenminister der neuen Bundesländer beabsichtigen, das Gemeinsame Landeskriminalamt zum 31. Dezember 1991 aufzulösen und neue Landeskriminalämter zu errichten. Die Art der Weiterführung von DORA, der Umfang des Zugriffs des BKA mittels der FINDEX-Datei und die Auskunftserteilung an die Polizeidienststellen der alten Bundesländer müssen daher durch die Innenminister der neuen Bundesländer neu geregelt werden. Die vorstehenden Grundsätze sollten dabei beachtet werden.

2.5 Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

2.5.1 Regelungen des Einigungsvertrages

Die Mißachtung von Grundrechten — namentlich auch des Rechts auf informationelle Selbstbestimmung — durch die frühere DDR als Überwachungsstaat verkörpert sich besonders eindringlich in den Stasi-Akten. Von den Aufgaben, die die Deutsche Einheit mit sich gebracht hat, werden Fragen des Umgangs mit den Akten der ehemaligen Staatssicherheit am heftigsten diskutiert, verbinden sich doch mit ihnen neben den juristischen auch schwierige menschliche Probleme.

Wie Unterlagen des ehemaligen Ministeriums für Staatssicherheit (und dessen kurzlebigen Nachfolgers, des Amtes für nationale Sicherheit) der DDR im geeinten Deutschland zu behandeln sind, wurde im

Zusammenhang mit dem Einigungsvertrag intensiv und teilweise leidenschaftlich erörtert. Der Einigungsvertrag ist Vorstellungen vor allem aus dem Bereich der früheren DDR nicht gefolgt, die Regelung dieser Frage noch der DDR mit Wirkung für Gesamtdeutschland zu überlassen. Er hat vielmehr selbst eine bewußt vorläufige Regelung getroffen, die in der neuen Legislaturperiode durch ein endgültiges Gesetz abgelöst werden soll.

Wesentlicher Kern der für die Übergangszeit getroffenen Regelung ist, daß die genannten Unterlagen durch einen Sonderbeauftragten der Bundesregierung in sichere Verwahrung zu nehmen und gegen unbefugten Zugriff zu sichern sind (§ 1 der Regelung im Einigungsvertrag, siehe Anlage 1). Die damit getroffene organisationsrechtliche Entscheidung, die Unterlagen in die Obhut einer Institution des Bundes zu nehmen, habe ich unter dem Gesichtspunkt der dringend erforderlichen einheitlichen Behandlung unterstützt. Soweit länderspezifische Besonderheiten bei Verwaltung, Archivierung und Nutzung der Unterlagen zu berücksichtigen sind, kann der Sonderbeauftragte auf Rat und Unterstützung von Beauftragten der neuen Bundesländer zurückgreifen (vgl. die sog. Ergänzungsvereinbarung — siehe Anlage 2 — Artikel 1 Nr. 4, 5 und 7). Nach § 1 Abs. 4 der Regelung im Einigungsvertrag habe auch ich den Sonderbeauftragten zu unterstützen. Er hat mich in wichtigen Angelegenheiten zu beteiligen und unterliegt nach § 4 meiner datenschutzrechtlichen Kontrolle.

Maßgebend für das Grundkonzept der Übergangsregelung war die Erwägung, daß der politischen Entscheidung des gesamtdeutschen Parlaments nicht vorgegriffen werden sollte. In diesem Sinne bestimmt der Einigungsvertrag, daß die Unterlagen des ehemaligen MfS zu erhalten sind (§ 2 Abs. 1 Satz 2: „Ihre Löschung ist unzulässig") und ihre Verwendung grundsätzlich gesperrt ist (§ 2 Abs. 1 Satz 1). Damit aber bis zu einer Entscheidung durch den gesamtdeutschen Gesetzgeber nicht irreversible Schäden eintreten, wurde eine Verwendung für einige besonders wichtige Zwecke insoweit zugelassen, als dies unerläßlich und unaufschiebbar ist (§§ 2 und 3):

Betroffenen ist hiernach ein Auskunftsanspruch zum Zweck der Wiedergutmachung und der Rehabilitierung sowie zur Abwehr einer gegenwärtigen oder drohenden Verletzung ihres Persönlichkeitsrechts eingeräumt. Sie können sich mit einem formlosen schriftlichen Auskunftsantrag an den Sonderbeauftragten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes, Behrenstraße 14—16, O-1086 Berlin, wenden. In dem Antrag hat der Betroffene die Zwecke zu benennen, für die er Auskunft begehrt, und den zugrundeliegenden Sachverhalt sowie Unerläßlichkeit und Unaufschiebbarkeit glaubhaft zu machen. Ich empfehle Antragstellern, im Interesse eines erleichterten und beschleunigten Bearbeitungsablaufs darzulegen, welche Schäden unter Nutzung der Kenntnisse aus den Unterlagen ausgeglichen oder wiedergutgemacht oder welche Persönlichkeitsrechtsverletzungen mit diesen Kenntnissen behoben oder abgewehrt werden können. Ich rate außerdem, in dem Antrag auch darauf einzugehen, welche erheblichen Nachteile dem Betroffenen bei einem weiteren Zuwarten entstehen können oder aus welchen anderen Umständen ihm ein längeres Zuwarten nicht zugemutet werden kann.

Auch die Nutzung der in den Stasi-Unterlagen enthaltenen personenbezogenen Daten durch *Dritte* ist in der Übergangsregelung nur für eng umgrenzte Zwecke zugelassen, nämlich

- für die Wiedergutmachung und Rehabilitierung von Betroffenen,
- zur Feststellung einer offiziellen oder inoffiziellen Tätigkeit für das ehemalige Ministerium für Staatssicherheit in bestimmten Fällen und zwar
  a) für die Überprüfung von Abgeordneten und Kandidaten für parlamentarische Mandate mit Zustimmung der Betroffenen,
  b) für die Weiterverwendung von Personen im öffentlichen Dienst nach Maßgabe des Einigungsvertrages mit deren Kenntnis und
  c) für die Einstellung von Personen in den öffentlichen Dienst und für Sicherheitsüberprüfungen mit Zustimmung der Betroffenen,
- zur Verfolgung von Straftaten, die im Zusammenhang mit der Tätigkeit der ehemaligen Staatssicherheit stehen und
- zur Aufklärung und Verfolgung der schweren Straftaten, wegen der nach dem Gesetz zu Artikel 10 des Grundgesetzes auch das Brief- und Fernmeldegeheimnis durchbrochen werden dürfte.

2.5.2 Durchführung der Regelungen des Einigungsvertrages

Ich habe versucht, mich an Ort und Stelle darüber zu unterrichten, inwieweit der Sonderbeauftragte der Bundesregierung die ihm obliegende Aufgabe, die Unterlagen des ehemaligen MfS in sichere Verwahrung zu nehmen und gegen unbefugten Zugriff zu sichern, tatsächlich bereits erfüllt. Zu diesem Zweck haben Mitarbeiter meiner Dienststelle einige der in insgesamt 15 Städten vorhandenen Archive des Sonderbeauftragten aufgesucht.

Dabei zeigte sich, daß als Folge der Arbeit der Bürgerkomitees zur Auflösung des Staatssicherheitsdienstes dessen Unterlagen in recht unterschiedlichen Formen aufbewahrt worden sind. Große Teile der Unterlagen, zu denen außer personenbezogenen Unterlagen auch Dienstvorschriften, Formulare jeglicher Art, Unterrichtsmaterialien, Stadtpläne, Telefonbücher und Mikrofilme gehören, sind — z. T. unter fachlicher Anleitung von Mitarbeitern des Staatsarchivs Potsdam — geordnet in Regalen untergebracht worden. Unterlagen aus weniger geregelten Inverwahrungsnahmen (z. B. aus einigen offenbar überstürzt geräumten Kreisverwaltungen des MfS) befanden sich dagegen nur mäßig sortiert in Kartons, Kisten oder auch Säkken; einiges war auch lose aufgeschüttet. Das ist verständlich, weil es seinerzeit das vordringliche Ziel war, die Unterlagen der befürchteten Vernichtung oder Weiterverwendung zu entziehen. Unter diesen

Umständen konnten Bestandslisten, mit denen man die Vollzähligkeit der Unterlagen überwachen könnte, nicht immer angelegt werden; deshalb fehlen solche z. T. heute noch. Auch ist zu berücksichtigen, daß das gesamte in allen Archiven vorhandene Material hintereinandergelegt über eine Strecke von mehr als 200 km reicht. Davon waren im Zeitpunkt meiner Besuche lediglich etwa 10 % einigermaßen erschlossen. Diese 10 % dürften aber die wichtigsten Materialien enthalten.

Die Aufbewahrungsräume für die Unterlagen befinden sich überwiegend auf dem Gelände ehemaliger Bezirksverwaltungen des Staatssicherheitsdienstes. Teils handelt es sich um Kellerräume oder Lagerhallen, die gut gesichert und für die Zukunft auch deswegen geeignet sind, weil zumutbare Arbeitsbedingungen zumindest in unmittelbarer Nähe geschaffen werden können, teils aber auch um Bunker, deren Eingänge zunächst einfach zugemauert wurden und die jetzt besonders bewacht werden, in denen zu arbeiten aber niemandem zugemutet werden kann, und wo auch sichere und akzeptable Arbeitsmöglichkeiten in der Nähe kaum geschaffen werden können. In einigen Fällen gehören zu der Dienststelle, die Unterlagen einer ehemaligen Bezirksverwaltung des MfS verwaltet, auch mehrere kilometerweit voneinander entfernt liegende Lagerstellen.

Angesichts dieser schwierigen Ausgangslage hat der Sonderbeauftragte als eine seiner ersten Aktivitäten eine Analyse der physischen Sicherung aller Lagerstellen von Unterlagen durchgeführt. Er wurde dabei von einem Sicherheitsexperten des Bundeskriminalamtes fachlich unterstützt. Im Rahmen meiner Kontrollen konnte ich mich davon überzeugen, daß die sofort ergriffenen Maßnahmen das unter den gegebenen Umständen Mögliche veranlaßt haben und die längerfristigen Planungen den erforderlichen hohen Anforderungen Rechnung tragen. Die Anforderungen an die Sicherheit der Archive sind deswegen hoch, weil man mit Gefährdungen aus recht unterschiedlichen Gründen rechnen muß. So könnte z. B. versucht werden,

- Anschläge zu verüben, um gezielt Teile der Unterlagen zu vernichten oder um für Unruhe zu sorgen,
- Unterlagen zu stehlen oder zu rauben, um bestimmte Personen zu schützen oder um bestimmten Personen zu schaden, oder
- Material für Sammlerzwecke oder publizistische Auswertungen zu erlangen.

Deshalb ist es nicht überzogen, wenn die Türen der Lagerräume z. B. durch Kontaktschalter kontrolliert und die Eingänge ständig durch Kameras überwacht werden. Es ist erforderlich, die als notwendig erkannten Verbesserungen so bald wie möglich durchzuführen, damit die noch bestehenden Schwachstellen nicht ausgekundschaftet und dann ausgenutzt werden können. Weil die Unterlagen nicht nur sicher verwahrt, sondern auch erschlossen und nutzbar gemacht werden müssen, sind schließlich Investitionen für Maßnahmen notwendig, die ein Arbeiten mit den Materialien unter sicheren und kontrollierbaren Bedingungen ermöglichen.

Die sinnvollen Maßnahmen zur Sicherung der Bestände müssen möglichst bald um durchgreifende Verbesserungen der Arbeitssituation für die Bediensteten ergänzt werden. Die Art, in der die Unterlagen gelagert sind, führt dazu, daß Arbeiten, wie z. B. die gezielte Suche nach Material für Auskunftszwecke, sehr viel Zeit beanspruchen, und oft unter nahezu unzumutbaren Bedingungen durchgeführt werden müssen. Viele dieser Mängel können bisher nur durch außergewöhnlich hohe Einsatzbereitschaft der Mitarbeiterinnen und der Mitarbeiter der Dienststelle des Sonderbeauftragten ausgeglichen werden.

In Ergänzung des Einigungsvertrags hat der Sonderbeauftragte die bereits in der sog. Ergänzungsvereinbarung zum Einigungsvertrag (Artikel 1 Nr. 7 — Anlage 2 —) erwähnte *Vorläufige Benutzerordnung* erlassen. Ich habe den Sonderbeauftragten bei der Abfassung dieser Benutzerordnung zusammen mit Vertretern der beteiligten Bundesressorts beraten.

Von zentraler Bedeutung ist die Aussage in der Benutzerordnung, daß alle Informationsträger mit personenbezogenen Daten, die beim ehemaligen Ministerium für Staatssicherheit oder auf dessen Veranlassung entstanden, in seinen Besitz gelangt oder ihm zur Nutzung überlassen worden sind, Unterlagen des MfS im Sinne des Einigungsvertrages sind. Zu diesen Unterlagen gehört deshalb auch einschlägiges Material, das zwar vom Staatssicherheitsdienst stammt, aber im Zeitpunkt der Auflösung dieses Dienstes nicht mehr in seinem Gewahrsam war. Von solchen Unterlagen gehen, wie der Bundesminister der Justiz mit Recht festgestellt hat (Grußwort an die Teilnehmer der 14. Datenschutzfachtagung am 15./16. November 1990 in Köln), „besondere Gefährdungen aus, weil sie sich in der Verfügungsgewalt von vielen Personen und Stellen befinden, die die vielfache Verletzung der Persönlichkeitsrechte der Betroffenen durch weitere Benutzung fortsetzen und damit neue Persönlichkeitsrechtsverletzungen begehen können". Vor diesem Hintergrund trete ich dafür ein, daß die Herausgabe solcher Unterlagen des MfS sowohl von öffentlichen Stellen und Einrichtungen als auch von Privatpersonen verlangt und durchgesetzt wird, soweit nicht ein besonderes Recht entgegensteht.

In der Vorläufigen Benutzerordnung ist der Sonderbeauftragte auch meiner Anregung gefolgt, deutlich zum Ausdruck zu bringen, daß seine Auskunft auch die Mitteilung von Tatsachen umfaßt, die es dem Betroffenen und der anfragenden zuständigen Stelle ermöglichen, die Zuverlässigkeit der übermittelten Informationen aus den MfS-Unterlagen zu bewerten. Gegebenenfalls wird die Auskunft vom Sonderbeauftragten auch erläutert. Diese Anforderung an die Auskunft des Sonderbeauftragten ist notwendig, weil personenbezogene Daten in den Unterlagen des MfS nach den vorliegenden Erkenntnissen häufig unzuverlässig sind und zu ihrem Verständnis nicht selten ergänzende Angaben benötigt werden.

Ein weiterer wichtiger Punkt meiner Beratung war die Bestimmung der „zuständigen Stellen" (§ 2 Abs. 2 Satz 1 — siehe Anlage 1 —), die zu den im Einigungsvertrag genannten Zwecken jeweils Empfänger von Übermittlungen des Sonderbeauftragten sein können. Ich habe Wert darauf gelegt, daß — wie von der Eini-

gungsvertragsregelung vorgesehen — die Informationen aus den Stasi-Unterlagen nicht weiter verbreitet werden, als dies für die jeweiligen Zwecke — wie es in der Regelung ausdrücklich heißt — „unerläßlich" ist. In einem Verwaltungsverfahren ist die Kenntnis einer Information „unerläßlich" allenfalls für die Stelle, die die abschließende Entscheidung zu treffen hat. Eine Übermittlung an — sachverständig — im Verfahren lediglich mitwirkende Stellen (beispielsweise das Bundesamt für Verfassungsschutz in Verfahren der Sicherheitsüberprüfung) ist deshalb nur dann „unerläßlich", wenn im Einzelfalle eine angemessene Bewertung ohne Hinzuziehung des spezifischen Sachverstandes dieser Stelle nicht vorgenommen werden kann. Letzteres darf nur die verfahrensleitende Stelle selbst beurteilen. Eine direkte Übermittlung von personenbezogenen Daten durch den Sonderbeauftragten darf deshalb nur an die verfahrensleitende Stelle erfolgen; eine Mitteilung entsprechender Informationen an lediglich mitwirkende Stellen ist demzufolge unzulässig.

Eine Weitergabe von personenbezogenen Informationen aus Unterlagen des MfS durch den Erstempfänger an sachverständige Dritte ist nur für denselben Zweck und auch nur im Rahmen einer pflichtgemäßen Beurteilung der Unerläßlichkeit unter Berücksichtigung der Erfordernisse des konkreten Einzelfalles zulässig. Auch ist zu prüfen, ob es nicht ausreicht, statt der Übermittlung personenbezogener Informationen sachverständigen Dritten lediglich nicht personenbezogene Fragen zu stellen.

Der Sonderbeauftragte hat diese Empfehlungen in seiner Vorläufigen Benutzerordnung berücksichtigt: Eine Übermittlung zur Feststellung einer offiziellen oder inoffiziellen Stasi-Tätigkeit ist im Rahmen einer Sicherheitsüberprüfung im öffentlichen Dienst danach nur zulässig, an „die zuständigen obersten Bundes- oder Landesbehörden, im übrigen die Geheimschutzbeauftragten".

Will ein Empfänger personenbezogener Daten aus MfS-Unterlagen diese weiter übermitteln, ist er an den ursprünglichen Übermittlungszweck gebunden (§ 2 Abs. 2 Satz 3). In diesem Zusammenhang muß ich allerdings auch deutlich darauf hinweisen, daß die in der öffentlichen Diskussion gelegentlich vertretene Auffassung, nach dem Einigungsvertrag dürften die Auskunftsempfänger „nicht mit dem Betroffenen darüber sprechen", eine Fehlinterpretation ist. Wann und inwieweit mit dem Betroffenen ein Dialog zu führen ist, bestimmt sich vielmehr nach den bestehenden allgemeinen, für die jeweilige Entscheidung des Auskunftsempfängers geltenden Regelungen. Dabei fordert es der Rechtsstaat zwingend, daß aus personenbezogenen Informationen für den Bürger belastende Konsequenzen nur gezogen werden dürfen, wenn er Gelegenheit hatte, sich dazu zu äußern. Diesem Grundsatz kommt erhöhte Bedeutung zu, wenn aus den Unterlagen des MfS belastende Folgerungen gezogen werden sollen, weil die so gewonnenen Erkenntnisse mit einem hohen Unsicherheitsfaktor belastet sind.

Die in der Vorläufigen Benutzerordnung enthaltene Regelung über Auskünfte an den Betroffenen ist nur für eine Übergangszeit akzeptabel. Für eine solche Zeit ist hinnehmbar, das Auskunftsrecht von Bürgern einzuschränken, weil zunächst Auskünfte zu Zwekken der Rehabilitierung und Wiedergutmachung sowie zur Vermeidung von Verletzungen des Persönlichkeitsrechts vordringlich sind. Gleichwohl halte ich auch in der Übergangszeit die in § 16 Abs. 1 Satz 2 der Vorläufigen Benutzerordnung getroffene Regelung für problematisch. Sie sieht vor, Auskünfte an Betroffene zum Zwecke der Wiedergutmachung nur im Hinblick auf solche Schäden zu erteilen, „bei denen Anhaltspunkte für eine Beteiligung des MfS bestehen". Ich habe den Sonderbeauftragten darauf hingewiesen, daß diese Beschränkung des Auskunftsanspruchs Betroffener keine Grundlage in der Einigungsvertragsregelung findet. Gesetzliches Erfordernis ist, daß die Kenntnis der Informationen aus den Unterlagen des MfS zur Schadensbeseitigung erforderlich ist; Voraussetzungen im Hinblick auf den Schadensverursacher werden nicht aufgestellt. Ich hoffe sehr, daß sich aus dieser Regelung keine negativen Folgen für Geschädigte ergeben. Auszuschließen ist das nicht, weil Fälle denkbar sind, in denen aus MfS-Unterlagen bestätigt wird, daß eine andere Stelle einen Betroffenen in politischer Verfolgungsmotivation geschädigt hat.

2.5.3 Ausblick

In der sog. Ergänzungsvereinbarung zum Einigungsvertrag haben die Vertragsparteien ihre Erwartung bekräftigt, daß die Gesetzgebungsarbeit zur endgültigen Regelung der Materie unverzüglich nach dem 3. Oktober 1990 aufgenommen wird. Im anstehenden Verfahren zur Erarbeitung eines Entwurfs für ein Gesetz über die Sicherung und Nutzung der personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes, das auch aus meiner Sicht zu den vordringlichsten Gesetzgebungsvorhaben der laufenden Legislaturperiode zählt, werde ich selbstverständlich meine Beratungsaufgabe gegenüber der Bundesregierung und dem Deutschen Bundestag wahrnehmen. Mein Ziel wird es dabei insbesondere sein, das Auskunftsrecht des Betroffenen — unter Wahrung schutzwürdiger Interessen Dritter — soweit irgend möglich auszuweiten. Der Auskunftsanspruch des Bürgers sollte nicht von qualifizierenden Voraussetzungen abhängig sein. Insbesondere sollten einschränkende Regelungen, wie sie in dem von der Volkskammer am 24. August 1990 verabschiedeten Gesetz vorgesehen waren, nicht übernommen werden. Dieses Gesetz enthielt gerade in bezug auf die Auskunft an Betroffene gravierende Datenschutzdefizite. So sollte z. B. eine Auskunft unterbleiben, „wenn Interessen anderer Staaten dieser entgegenstehen" (§ 11 Abs. 2 Nr. 2 des Volkskammergesetzes). Außerdem war vorgesehen (§ 11 Abs. 1 Satz 3), Betroffenen, die keine Persönlichkeitsverletzung darlegen konnten, grundsätzlich erst nach Abschluß der archivarischen Aufbereitung der Unterlagen Auskunft zu erteilen. Angesichts der kaum vorstellbaren Fülle vorhandenen Materials könnte eine solche Regelung einen Aufschub des Auskunftsanspruch für lange Zeit bedeuten. Solche Einschränkungen des Auskunftsanspruchs sind mit dem Gebot der Transparenz der Datenverarbeitung nicht vereinbar.

Bei der Neuregelung wird zu prüfen sein, ob für die Behandlung unterschiedlicher Unterlagen des MfS auch differenzierte Verwaltungs-, Auskunfts- und Nutzungsregelungen getroffen werden können. So müssen z. B. Personalunterlagen des MfS nicht nach den gleichen Grundsätzen behandelt werden, wie Akten über die Bespitzelung von Bürgern. Ein weiteres Problemfeld ergibt sich daraus, daß in den MfS-Unterlagen Informationen enthalten sein können, die unter Bruch besonderer Geheimnisse, wie z. B. des Post- und Fernmeldegeheimnisses oder des Arztgeheimnisses, gewonnen worden sind. Es könnte sich etwa das Abhörprotokoll eines Telefongesprächs eines Pfarrers finden, in dem ein Vater dem Geistlichen anvertraut hat, sein Sohn habe sich ihm gegenüber als Zuträger der Stasi zu erkennen gegeben. Soll auf ein entsprechendes Ersuchen diese Information im Rahmen der Prüfung einer Bewerbung des Sohnes für den öffentlichen Dienst zur Verfügung gestellt werden? Ich trete dafür ein, daß sich der Gesetzgeber dabei an den in einschlägigen Datenschutzbestimmungen — wie z. B. dem Gesetz zu Artikel 10 des Grundgesetzes — enthaltenen Wertentscheidungen orientiert. Für den obigen Beispielsfall ergäbe sich daraus, daß eine Verwendung für die Einstellungsentscheidung ausscheidet, da unsere Rechtsordnung eine Verwendung von selbst durch legale Maßnahmen zur Durchbrechung des Fernmeldegeheimnisses gewonnenen Informationen zu diesem Zweck nicht zuläßt.

Auch hinsichtlich der Dauer zulässiger Nutzung personenbezogener Informationen aus der Hinterlassenschaft der Stasi bedarf es — hinsichtlich der jeweiligen Auskunftszwecke möglicherweise differenzierter — präziser Regelungen. Dabei muß der Gesetzgeber auch eine Löschung von Informationen und eine Vernichtung von Unterlagen zulassen. Das gilt insbesondere dann, wenn der Betroffene dies wünscht. Selbstverständlich muß auch eine wissenschaftliche Aufarbeitung der MfS-Unterlagen möglich sein. Für diesen Zweck ist es aber nicht erforderlich, den gesamten Aktenbestand aufzubewahren. Vielmehr ist es ausreichend, auf Dauer nur solche Unterlagen aufzubewahren, die nach den Grundsätzen des Archivrechts als archivwürdig zu bewerten sind.

2.6 Abhöreinrichtungen des Staatssicherheitsdienstes

In Presseberichten und Eingaben wurde die Besorgnis artikuliert, auch nach der Herstellung der deutschen Einheit seien die Einrichtungen des ehemaligen Ministeriums für Staatssicherheit weiter illegal zum Abhören von Telefongesprächen genutzt worden. Auf meine Nachfrage hin hat mich die Generaldirektion der Deutschen Bundespost TELEKOM in einem ersten Bericht über technische Einrichtungen der ehemaligen Post der DDR informiert, die eine „systematisch und mit unerwartet hohem Aufwand" betriebene Abhörpraxis des ehemaligen Staatssicherheitsdienstes der DDR belegen. Die TELEKOM hat mir mitgeteilt, daß schon vor der Vereinigung umfangreiche Maßnahmen mit dem Ziel durchgeführt worden waren, die Stasi-Abhörzentralen vom Netz der Deutschen Post abzutrennen und die Abhöreinrichtungen abzubauen. Schwieriger als bei den genannten größeren Abhörzentralen ist das Aufdecken von Manipulationen und Abhörschaltungen in den Fernmeldenetzen der ehemaligen DDR, die verdeckt angelegt sind. Wegen der Größe der zu untersuchenden Netze, aber auch wegen fehlender Dokumentationen, gestalten sich die Aufklärungsarbeiten sehr zeit- und personalintensiv.

Ich habe die Deutschen Bundespost TELEKOM darauf hingewiesen, daß die Benutzung der genannten Einrichtungen ohne das Vorliegen der gesetzlichen Voraussetzungen und ohne angemessene Sicherungen des Verfahrens für die betroffenen Bürger zu schwerwiegenden Grundrechtsverletzungen führen kann. Ich habe sie daher aufgefordert, ihre Bemühungen zur Aufdeckung und Unschädlichmachung der genannten Einrichtungen fortzusetzen und mich sehr bald über die bestehende Lage zu informieren.

2.7 Bewerber für den öffentlichen Dienst aus dem Beitrittsgebiet

Das Verfahren der Übernahme oder Neueinstellung von Bewerbern aus dem Beitrittsgebiet in den öffentlichen Dienst war im Berichtsjahr Anlaß für zahlreiche Eingaben. In nahezu allen Fällen wurde der Inhalt von Personalfragebögen angesprochen, die Bewerber für den öffentlichen Dienst aus dem Beitrittsgebiet ausfüllen sollten. Eine nähere Prüfung ergab, daß der Inhalt der Personalbögen von den Ressorts jeweils in eigener Zuständigkeit festgelegt worden war; dabei kam es zu sehr unterschiedlichen und teilweise datenschutzrechtlich problematischen Lösungen. Einige Beispiele können dies verdeutlichen:

2.7.1 Fragen zum früheren Beschäftigungsverhältnis des Bewerbers und zur Überprüfung der Verfassungstreue

In Fragebögen wurde u. a. die Frage gestellt, ob der Bewerber in seinem früheren Tätigkeitsbereich an der rechtswidrigen Anwendung von Gewalt oder unerlaubten Vernehmungsmethoden beteiligt war. Mit dieser Frage wird eine Selbstbezichtigung verlangt, was nach der Rechtsprechung des Bundesverfassungsgerichts unzulässig ist.

Zur Verfassungstreue wurden u. a. folgende Fragen gestellt:

„Waren Sie Mitarbeiter des Ministeriums für Staatssicherheit oder beim Amt für Nationale Sicherheit? Wenn ja, welcher Art war diese Tätigkeit (auch nebenamtlich) und von welcher Dauer war sie?"

„Haben Sie vor dem 9. November 1989 eine Funktion in der SED, in Massenorganisationen/gesellschaftlichen Organisationen oder eine sonstige herausgehobene Funktion im System der DDR innegehabt? Wenn ja, welcher Art war diese Funktion und von welcher Dauer?"

„Waren oder sind Sie Mitglied einer kommunistischen, rechtsradikalen oder inzwischen für verfassungswidrig erklärten Partei oder Organisation?"

„Hatten oder haben Sie sonstige Verbindungen z. B. beruflicher oder geschäftlicher Art zu einer der vorgenannten Parteien oder Organisationen?"

„Haben Sie in der Fremdenlegion oder in sonstigen fremden Streitkräften einschließlich der Nationalen Volksarmee, der Volkspolizei, der Grenzpolizei und der Kampfgruppen Dienst geleistet?"

„Hatten oder haben Sie oder die mit Ihnen in einem Haushalt lebenden nahen Angehörigen sonstige Beziehungen (verwandtschaftliche, geschäftliche, gesellschaftliche, kulturelle, sportliche, wissenschaftliche, technische usw.) in den kommunistischen Machtbereich?"

Für den Bereich der Bundesverwaltung hat der Bundesminister des Innern in einem Rundschreiben vom 11. September 1990 (BMI D I 3—216 100/40) darauf hingewiesen, daß in diesem Zusammenhang auch die Regelungen des Einigungsvertrages für den Personenkreis der in der öffentlichen Verwaltung der DDR beschäftigten Arbeitnehmer zu berücksichtigen sind. Danach gilt folgendes: „Ein wichtiger Grund für eine außerordentliche Kündigung ist insbesondere dann gegeben, wenn der Arbeitnehmer

1. gegen die Grundsätze der Menschlichkeit oder Rechtsstaatlichkeit verstoßen hat, . . . oder
2. für das frühere Ministerium für Staatssicherheit/Amt für Nationale Sicherheit tätig war

und deshalb ein Festhalten am Arbeitsverhältnis unzumutbar erscheint."

Nach dem BMI-Rundschreiben scheidet — sofern diese Kündigungsgründe vorliegen — die Einstellung in ein Beamtenverhältnis in der Regel aus.

Darüber hinaus bestehen nach dem Inhalt des Rundschreibens Zweifel an der Verfassungstreue bei Bewerbern, die sich im politischen System der DDR exponiert haben, indem sie vor dem 9. November 1989 Funktionen in den Bereichen SED sowie Massenorganisationen/Gesellschaftlichen Organisationen innehatten. Bei diesen Personengruppen könne nicht generell von einer fehlenden Verfassungstreue ausgegangen werden, sondern es müsse eine Einzelfallprüfung unter besonderer Berücksichtigung der früheren Verhältnisse in der DDR (u. a. Höhe der Funktion, Zahl der Funktionen, Abstufung nach haupt- oder nebenamtlicher Funktion) erfolgen.

Die Ausführungen des Bundesministers des Innern erscheinen mir plausibel. Deshalb bestehen auch gegen die beiden oben erstgenannten Fragen zur Verfassungstreue keine Bedenken. Soweit ich sehe, beschränken sich die Behörden der Bundesverwaltung, die ursprünglich teilweise weitergegangen waren, inzwischen in aller Regel auf diese Fragen.

Anders ist die Lage nach dem Eindruck, den ich aus zahlreichen Eingaben gewonnen habe, bei den Verwaltungen der neuen Länder, die in ihren Fragen teilweise erheblich weitergehen und auch keine einheitliche Praxis verfolgen. Welche Fragen darüber hinaus zulässig sind, ist letztlich davon abhängig, welche Sachverhalte für die Begründung eines Dienst- oder Arbeitsverhältnisses von Bedeutung sind. Hierzu fehlt es — soweit ich sehe — an klaren rechtlichen Vorgaben oder verbindlichen Richtlinien. Ich habe deshalb vorgeschlagen, das Problem in der Innenministerkonferenz zu erörtern, materielle Regelungen für die an Bewerber für den öffentlichen Dienst zu stellenden Anforderungen möglichst konkret festzulegen und auf eine möglichst einheitliche, die Grenzen des Fragerechts des Dienstherrn/Arbeitgebers berücksichtigende Regelung für die Gestaltung der Personalfragebogen hinzuwirken.

2.7.2 Verfahren der Überprüfung der Verfassungstreue

Die Fragen zur Verfassungstreue waren bei einigen Ressorts in einem Zusatzbogen zum Personalfragebogen, bei anderen im Fragebogen selbst enthalten. In beiden Fällen war vorgesehen, die Fragebogen und Zusatzbögen in der Personalabteilung aufzubewahren. Die Personalvertretung war in einzelnen Fällen an der Erstellung der Fragebogen nicht beteiligt worden.

Ich habe vorgeschlagen, für die — zulässigen — Fragen zur Verfassungstreue einen eigenen Vordruck vorzusehen und diesen auch gesondert zu führen. Die Überprüfung der Verfassungstreue erfordert vielfach Auskünfte dritter Stellen, etwa des Sonderbeauftragten der Bundesregierung für die personenbezogenen Unterlagen des ehemaligen Staatssicherheitsdienstes, die gerade nicht auf Dauer in der allgemeinen Personalakte enthalten sein dürfen. Nach dem Einigungsvertrag dürfen Auskünfte des Sonderbeauftragten, die zum Zwecke einer Entscheidung über die Weiterverwendung oder die Einstellung in den öffentlichen Dienst übermittelt worden sind, nicht für andere Zwecke verwendet werden; sie dürfen also im Rahmen nachfolgender Personalentscheidungen keine Berücksichtigung mehr finden (s. oben 2.5.1). Zur organisatorischen Sicherung dieser Nutzungsbeschränkung sind jedenfalls diese Unterlagen gesondert zu verwahren.

Soweit Personalvertretungen bei der Gestaltung der Fragebogen nicht beteiligt worden waren, habe ich unter Hinweis auf die Bestimmungen des § 75 Abs. 3 Nr. 8 und des § 76 Abs. 2 Nr. 2 BPersVG, die eine Mitbestimmung bei der Regelung des Inhalts von Personalfragebögen vorsehen, angeregt, die Beteiligung der Personalvertretungen nachzuholen.

Einige Ressorts haben meine Empfehlungen bereits aufgegriffen und ihr Verfahren entsprechend geändert. So wurden der datenschutzrechtlich bedenkliche Inhalt einiger Fragen — soweit noch keine Personalgespräche geführt worden waren — unkenntlich gemacht und neue Fragebogen entwickelt. Die beschriebene Überprüfung der Verfassungstreue und die Aufbewahrung der dabei angefallenen Unterlagen wurden in einem Ressort dem Geheimschutzbeauftragten übertragen.

Der Bundesminister des Innern hat mir mitgeteilt, er halte seine derzeitige Praxis, Fragen zur Verfassungstreue in den Personalbogen und damit in die Personalakte mitaufzunehmen, für rechtens. Gleiches gelte auch für Auskünfte, die in diesem Zusammenhang

von dritten Stellen, z. B. dem Sonderbeauftragten, eingeholt worden seien.

Ich habe gebeten, diese Entscheidung noch einmal zu überprüfen und in die vorgeschlagene Erörterung des Gesamtproblems in der Innenministerkonferenz einzubeziehen.

Ich hoffe, daß es schnell gelingt, Inhalt und Verfahren der Überprüfung der Verfassungstreue von Bewerbern aus dem Beitrittsgebiet möglichst einheitlich für Bund und Länder zu regeln. Dabei sollten der Umfang der Datenerhebung auf das erforderliche Maß beschränkt und den Beteiligten die aus zahlreichen Eingaben ersichtliche erhebliche Rechtsunsicherheit genommen werden.

2.8 Zentrales Einwohnerregister (ZER)

2.8.1 Organisation und Aufgaben des ZER

Als Folge eines Beschlusses des Ministerrates der ehemaligen DDR wurde 1973 das „Büro für Personendaten" als selbständige Dienststelle der Hauptabteilung Paß- und Meldewesen des Ministerium des Innern gegründet. Sein Auftrag lautete, einen „Personenspeicher" zu organisieren. In den Jahren 1977 bis 1982 wurden dann die Daten der Einwohner für ein automatisiertes zentrales Register erfaßt; diese Personendatenbank — später ZER — wurde am 1. Januar 1984 offiziell in Betrieb genommen.

Die Personendatenbank sollte das Zentrum des Meldewesens bilden und in die sonstige Verwaltung integriert sein. Der Minister des Innern oder sein Stellvertreter hat mit den sog. Integrationspartnern — also Empfängern von Datenübermittlungen aus dem ZER — Verträge geschlossen, in denen festgelegt wurde, welche Daten das ZER wie zu liefern hatte. Grundlage für die Arbeit des ZER war die „Ordnung der Personendatenbank" (Verwaltungsvorschrift). Sie enthielt u. a. Regelungen über

- die Zulässigkeit der Datenverarbeitung
- den Umfang des Datensatzes,
- die Zweckbindungen,
- das Verfahren der Aktualisierung,
- die Anforderungen zum Datenschutz (dies waren in Wirklichkeit Vorschriften zur Datensicherung) und
- das Verfahren zur Auskunftserteilung (dies entsprach einer Datenübermittlung im Sinne des Bundesdatenschutzgesetzes).

Die Kreise erhielten eine eigene derartige Ordnung, die einen Auszug aus der vorgenannten Ordnung darstellte.

Das ZER war eine den Bürgern der früheren DDR kaum bekannte Dienststelle. Die Bürger hatten Kontakte zu den Meldestellen oder zu den Polizeikreisämtern. Die Meldestellen führten Meldekarten und meldeten Veränderung auf Datenerfassungsbelegen an die Polizeikreisämter. Die Polizeikreisämter sammelten alle Belege und gaben diese täglich mit Hilfe eines besonderen Kurierdienstes an das ZER weiter. Das ZER verarbeitete die Datenerfassungsbelege und erstellte die erforderlichen neuen Karteikarten für die Meldestellen und für die Polizeikreisämter sowie sonstige Datenträger (z. B. Magnetbänder) für Empfänger regelmäßiger Datenübermittlungen, wie z. B. das Rechenzentrum Statistik oder die Staatliche Versicherung der früheren DDR.

Auf der Ebene der Bezirke der früheren DDR wurden die sog. Einwohnerdatenspeicher (EDS) gebildet. Deren Projektträger war das Statistische Amt. Der EDS war keine Meldekartei; er war vielmehr Hilfsmittel für den Rat des Bezirkes und enthielt auch Daten, die nicht im ZER enthalten waren. Der EDS war sowohl Planungshilfe als auch Mittel zur besseren Betreuung von Bürgern, z. B. in sozialen Angelegenheiten.

Innerhalb der Bezirke gab es Kreise. Zuständig für die Aufgaben des Meldewesens im Kreis war das „Paß- und Meldewesen des Volkspolizeikreisamtes", dem eine oder mehrere Meldestellen zugeordnet waren, wobei eine Meldestelle für mehrere Gemeinden zuständig sein konnte. Es gab rund 200 Kreise und ca. 700 Meldestellen.

2.8.2 Daten des ZER

Das ZER verfügte bis Oktober 1989 über einen Datenbestand, der weit über den hinausging, den in der „alten" Bundesrepublik Deutschland Meldebehörden speichern dürfen. So hatte es zum Beispiel folgende Daten gespeichert:

- Reisen nach dem Ausland
- Einreisen
- Anträge auf ständige Ausreise
- Reisesperren
- Arbeitsstelle (Hinweise auf Arbeit/Tätigkeit)
- überwiegend ausgeübte Tätigkeit außerhalb der DDR
- Besonderheiten zur Person
- Grund der Wohnsitznahme bei Rückkehrern/Zuziehenden
- Vermerke und Kontrollmaßnahmen für Rückkehrer/Zuziehende
- Spezial- und Sprachkenntnisse.

Diese Daten wurden bereits im Oktober 1989 gesperrt und im Frühjahr 1990 aus dem aktuellen Bestand des Registers gelöscht. Bis zum Inkrafttreten des Einigungsvertragsgesetzes hatte das ZER weitere Daten gelöscht und bereits einen Teil seiner Integrationsbeziehungen/regelmäßigen Datenweitergaben eingestellt.

2.8.3 Stand der Datenverarbeitung nach dem Einigungsvertrag

Der Einigungsvertrag enthält besondere Vorschriften zum Zentralen Einwohnerregister. Nach der Anlage I, Kapitel II Sachgebiet C Abschnitt III Nr. 4. ist das Mel-

derecht im Beitrittsgebiet innerhalb eines Jahres nach den Vorschriften des Melderechtsrahmengesetzes zu gestalten. Ferner ist vorgesehen, daß vom Melderechtsrahmengesetz abweichende Daten, insbesondere Ordnungsnummern, nur weiter verarbeitet werden dürfen, soweit und solange sie für die Weiterführung der Melderegister erforderlich sind. Die Verarbeitung neu anfallender Daten ist zulässig. Die Verwendung solcher Daten ist unverzüglich durch Verfahren abzulösen, die ihre Verwendung entbehrlich machen. Nach dieser Ablösung, spätestens jedoch bis zum 31. Dezember 1992, sind die nach dem Melderechtsrahmengesetz nicht zulässigen Daten zu löschen. Das Zentrale Einwohnerregister darf weitergeführt werden, soweit es Aufgaben des Meldewesens wahrnimmt und solange die örtlichen Melderegister ihre Aufgaben nicht ohne das zentrale Register erfüllen können; es ist jedoch spätestens am 31. Dezember 1992 aufzulösen. Soweit im ZER andere als Meldedaten gespeichert sind, sind sie zu löschen, soweit sie nicht für die Aufgabenerfüllung anderer Fachbereichsverwaltungen erforderlich sind. Auch diese Daten sollen spätestens zum 31. Dezember 1992 gelöscht werden. Die örtlichen Melderegister sind unverzüglich in der Weise umzustellen, daß die Inanspruchnahme des ZER entbehrlich wird.

Das ZER hat bereits einen erheblichen Teil der Auflagen nach dem Einigungsvertrag erfüllt. Bis zum Aufbau funktionierender örtlicher Fahrerlaubnisbehörden wird das ZER noch Daten zum Führerscheinbesitz verwalten; die Daten zum Führerscheinentzug wurden inzwischen nach deren Übermittlung an das Kraftfahrt-Bundesamt gelöscht (s. unten 2.10). Nach den mir vorliegenden Datensatzbeschreibungen entsprechen die vom ZER jetzt verwalteten Daten weitgehend dem Melderechtsrahmengesetz.

Für die inhaltliche Ausformung der Daten nach dem Melderechtsrahmengesetz ist üblicherweise der bundeseinheitliche Datensatz für das Meldewesen zugrunde zu legen. Hieran gemessen gibt es im automatisierten ZER noch Schlüsselungen, die unüblich sind. Ich habe jedoch gegenüber dem ZER und dem Bundesminister des Innern akzeptiert, daß aufgrund der schwierigen Personalsituation beim ZER und der Probleme bei der Feststellung, wer die Kosten des ZER zu tragen hat, eine schnellere Anpassung der Daten nicht durchgeführt werden kann. Ich gehe davon aus, daß das ZER weiterhin bemüht ist, alle erforderlichen Änderungen vorzunehmen.

2.8.4 Empfänger von Datenübermittlungen

Das ZER war, wie vorstehend erwähnt, in zahlreiche regelmäßige Datenübermittlungen eingebunden. Diese sind mittlerweile soweit reduziert worden, daß die Datenübermittlungen, die das ZER jetzt noch regelmäßig oder auch auf Antrag (z. B. von Meldebehörden) durchführt, rechtens sind. Die regelmäßigen Übermittlungen an die Deutsche Versicherungs AG sind leider erst zum 31. Dezember 1990 eingestellt worden. Weil die Deutsche Versicherungs AG die Staatliche Versicherung der früheren DDR übernommen hat, gingen auf sie als Rechtsnachfolger zunächst auch die Verträge mit dem ZER über. Das ZER fühlte sich insofern an seinen Vertrag mit der staatlichen Versicherung der früheren DDR gebunden. Ich hatte erhebliche Zweifel, daß die weitere regelmäßige Übermittlung von Datensätzen an die Deutsche Versicherungs AG rechtlich vertretbar war. Dem wurde u. a. entgegengehalten, daß die Deutsche Versicherungs AG noch so lange regelmäßig informiert werden müßte, bis auch die Übernahme von ca. 600 000 Datensätzen, die sich auf Rentner beziehen und die die Deutsche Versicherungs AG an die Rentenversicherung weitergegeben hat, abgewickelt war. Wenig empfindsam hat die Deutsche Versicherungs AG die Personenkennzahl als Versicherungsnummer verwendet, was zu Beschwerden führte, da die früheren DDR-Bürger die PKZ, die für sie Symbol des früheren Staates ist, nicht mehr verwenden möchten. Die Deutsche Versicherungs AG, die nicht meiner Kontrolle unterliegt, hat den Vertrag mit dem ZER, den sie als noch gültig und nicht durch den Einigungsvertrag aufgehoben ansah, zum 31. Dezember 1990 gekündigt.

Wichtig ist mir auch, daß das ZER seit 1. Januar 1991 keine Daten mehr für die Fortführung der Einwohnerdatenspeicher zur Verfügung stellt. Es werden noch regelmäßig Daten zur Sicherung von Rentenansprüchen weitergegeben; die Anpassung dieser Datenübermittlungen an die Vorschriften der Zweiten Meldedatenübermittlungsverordnung des Bundes wird noch einige Zeit in Anspruch nehmen.

Das Landeseinwohneramt von Berlin hat mittels mehrerer Terminals einen lesenden Zugriff auf alle Daten von Personen, die das Merkmal „Haupt- oder Nebenwohnung in Berlin" enthalten. Es hat dem ZER zugesagt, bis Mitte 1991 die technischen Voraussetzungen zu schaffen, um die „Berliner Datensätze" zu übernehmen.

Insbesondere letzteres zeigt, daß die im Einigungsvertrag vorgesehene Auflösung des ZER selbst für eine hochtechnisierte Verwaltung nicht einfach zu bewältigen ist. Insofern ist verständlich, daß den Verwaltungen der neuen Länder nicht einfach die Datensätze ihrer Einwohner zur Verfügung gestellt werden können. Vielmehr bedarf es dort zunächst funktionierender Verwaltungen, die wissen, welche Aufgaben sie aufgrund des Melderechts mit welchen Daten zu erfüllen haben. Hierbei ist zu berücksichtigen, daß das Meldewesen auch in den alten Ländern in viele Verwaltungsbeziehungen integriert ist und daß ohne ein funktionierendes Meldewesen insbesondere kommunale Aufgaben, zu denen auch die Anmeldung von Ansprüchen zum Finanzausgleich gehört, nicht durchgeführt werden können. Es widerspricht nicht dem Datenschutzrecht und auch nicht dem Einigungsvertrag, wenn das ZER vorläufig weiterhin dafür sorgt, daß die Aufgaben des Meldewesens in den neuen Ländern und in Teilen Berlins ordnungsgemäß vollzogen werden. Die Wahrung schutzwürdiger Belange der Bürger verlangt allerdings, daß der Umgang mit ihren Daten rechtlich nachvollziehbar und auch kontrollierbar ist. Dies ist jetzt beim ZER gewährleistet. Ich habe jedoch Sorge, daß die Länder nicht in der Lage sein werden, in der vom Einigungsvertrag gesetzten Frist, die am 2. Oktober dieses Jahres endet, Landesmeldegesetze nach dem Vorbild des Melde-

rechtsrahmengesetzes zu schaffen und Meldebehörden aufzubauen, die den rechtlichen Anforderungen entsprechen. Das ZER in seiner jetzigen Form ist laut Einigungsvertrag bis 31. Dezember 1992 aufzulösen; dieses kann nur geschehen, wenn die Einwohnerdaten an funktionierende Verwaltungen abgegeben werden können. Wie zeitaufwendig das ist, zeigt das Beispiel Berlins sehr deutlich. Die Abgabe aller Daten „auf einen Schlag" ist eine Utopie. Insofern bleiben die Verantwortlichen in Gesetzgebung und Verwaltung der neuen Länder aufgefordert, schnell das Erforderliche zu tun. Sonst kann der Einigungsvertrag in diesem Punkt nicht fristgerecht vollzogen werden.

2.8.5 Personenkennzahl

Im Einigungsvertrag ist vorgesehen, daß sämtliche Dateien im Beitrittsgebiet, die nach Personenkennzahlen geordnet sind, unverzüglich nach anderen Merkmalen umzuordnen sind. Die Personenkennzahlen müssen in allen Dateien zum frühestmöglichen Zeitpunkt gelöscht werden. Die Personenkennzahl der früheren DDR war zwölfstellig: 6 Ziffern = Geburtsdatum, 1 Ziffer = Geschlecht, 4 Ziffern = Unterscheidungszahl und 1 Ziffer = Prüfziffer. Die Personenkennzahl (PKZ) wurde in der DDR als allgemeines Ordnungsmerkmal verwendet, das in zahlreichen Dateien gespeichert wurde und so ermöglichte, Datensätze leichter miteinander zu verbinden.

Die Personenkennzahl wird im ZER und im Austausch mit den Meldebehörden noch als Ordnungsmerkmal verwendet. An Stellen außerhalb des Meldewesens, insbesondere im Zusammenhang mit Datenübermittlungen nach der Zweiten Meldedatenübermittlungsverordnung, soll die PKZ voraussichtlich ab Sommer 1991 nicht mehr verwendet werden.

Nach dem Einigungsvertrag soll die PKZ als Ordnungsmerkmal zum frühestmöglichen Zeitpunkt gelöscht werden. Das bedeutet, daß sowohl das ZER als auch die Meldebehörden in den Ländern in einer angemessenen Frist das PKZ durch ein anderes Ordnungsmerkmal ersetzen müssen. Hierauf habe ich das ZER und den Bundesminister des Innern, der das ZER ebenfalls berät, hingewiesen.

2.9 Strafregister des ehemaligen Generalstaatsanwalts der DDR

Nach dem Einigungsvertrag ist mit dem Wirksamwerden des Beitritts auch das Bundeszentralregistergesetz in den neuen Ländern in Kraft getreten, „soweit durch diesen Vertrag nichts anderes bestimmt" ist. Dabei mußte dem Strafregister beim Generalstaatsanwalt der DDR die besondere Aufmerksamkeit des Datenschutzes gelten. Schon im Sommer 1990 habe ich in Gesprächen mit dem Bundesminister der Justiz und mit dem Generalbundesanwalt (Abteilung IV — Dienststelle Bundeszentralregister) das Vorhaben unterstützt, für die Übernahme dieses Registers ergänzende Vorschriften im Bundeszentralregistergesetz zu schaffen. Das Kernproblem war hierbei die notwendige Differenzierung zwischen solchen Eintragungen über strafrechtliche Entscheidungen, die rechtsstaatlichen Maßstäben entsprachen und somit konsequenterweise in das Bundeszentralregister zu übernehmen waren, und Eintragungen über solche strafrechtliche Maßnahmen, die unseren rechtsstaatlichen Grundsätzen widersprachen und deshalb nicht in das Bundeszentralregister übernommen werden durften. Die durch den Einigungsvertrag in das Bundeszentralregistergesetz neu eingefügten §§ 64 a und 64 b sehen vor, daß über die Übernahme in jedem Einzelfalle eine besondere Entscheidung zu treffen ist. Sie entsprechen meinen Vorstellungen. Wichtig sind auch die getroffenen Übergangsregelungen, nach denen die Eintragungen im bisher beim DDR-Generalstaatsanwalt geführten Register bis zur Entscheidung über die Übernahme in das Bundeszentralregister außerhalb desselben zu speichern und — ebenso wie auch Eintragungen, deren Übernahme abgelehnt worden ist — für Auskünfte nach dem Bundeszentralregistergesetz zu sperren sind. Die Eintragungen im ehemaligen DDR-Strafregister sind nach Ablauf von drei Jahren zu vernichten. Dies gilt — darauf habe ich von Anfang an hingewiesen — auch dann, wenn bis dahin nicht in allen Fällen die Übernahmeentscheidungen getroffen sein sollten. Bis zur Löschung ist die Nutzung der Eintragungen im ehemaligen DDR-Strafregister beschränkt: Außer für eine etwaige Nachprüfung der Übernahme und der Schlüssigkeit der Eintragung dürfen die Informationen nur für die Übermittlung an für die Rehabilitierung zuständige Stellen für Zwecke der Rehabilitierung verwandt werden. Eine Verwendung für andere Zwecke ist nur mit Einwilligung des Betroffenen zulässig.

Allein mit dieser gesetzlichen Regelung war es freilich nicht getan: Das ehemalige DDR-Strafregister existierte als Handregister in einer Größenordnung von etwa 200 000 Karteikarten. Um zu vermeiden, daß auf ein Auskunftsersuchen an das BZR in jedem Falle neben dem Einblick in den BZR-Bestand die Handkartei daraufhin durchgesehen werden muß, ob sich darin Eintragungen über den Betroffenen befinden, die in das BZR zu übernehmen und über die dann Auskunft zu erteilen ist — was auch unter Gesichtspunkten des Datenschutzes zu unvertretbaren Verzögerungen geführt hätte —, habe ich von Anfang an das Vorhaben des Generalbundesanwaltes unterstützt, zur Erschließung der manuell geführten Datei neben dem Bundeszentralregister eine automatisiert geführte Personendatei zu erstellen. Für deren Erstellung wurde das Zentrale Einwohnerregister (ZER) der DDR genutzt: Veranlaßt noch durch den damaligen Generalstaatsanwalt der DDR übergab das ZER dem Generalbundesanwalt in maschinenlesbarer Form (Magnetband) Datensätze zu allen Personen, die im ZER gespeichert und mit einem Vermerk des Inhalts gekennzeichnet waren, daß im Strafregister beim Generalstaatsanwalt der DDR über sie eine Eintragung vorliegt. Ein Abgleich zwischen den vom ZER übergebenen Personendatensätzen und dem manuell geführten DDR-Strafregister ergab eine Differenz von etwa 10 000 Datensätzen zu Personen, die nicht im ZER, wohl aber im ehemaligen Strafregister erfaßt sind. Sie betreffen Ausländer im Sinne der früheren DDR, d. h. zu einem wesentlichen Teil Personen, die im Zusammenhang mit Strafverfahren im DDR-Straf-

register gespeichert worden waren, zum Zeitpunkt des Beitritts der DDR ihren Wohnsitz aber nicht mehr in den alten Ländern hatten und deshalb nicht mehr im ZER gespeichert waren. Diese etwa 10 000 Datensätze wurden von Mitarbeitern des Generalbundesanwalts manuell aus der Handkartei erfaßt und in die automatisiert geführte Personendatei eingespeichert.

Die Einhaltung der oben genannten Gesetzesvorschriften über die Übernahme des Strafregisters beim ehemaligen DDR-Generalstaatsanwalt, namentlich auch bei der Nutzung dieser automatisiert geführten Personendatei, war Gegenstand eines von mir im November 1990 durchgeführten Beratungs- und Kontrollbesuchs bei der Abteilung IV des Generalbundesanwalts in Berlin.

Stichproben in der erwähnten Personendatei haben im Einklang mit von mir schon im August gegebenen Empfehlungen gezeigt, daß in dieser Datei keine anderen Personendaten übernommen und enthalten sind als die, die zulässigerweise im BZR als Identifizierungsdaten verwandt werden. Die automatisiert geführte Personendatei ist eine vom Bundeszentralregister logisch getrennte Datei, auch wenn sie durch dasselbe Datenbankbetriebssystem verwaltet wird, mit dessen Hilfe das Bundeszentralregister aufgebaut ist. Die Trennung entspricht dem von mir bereits im August 1990 empfohlenen Konzept: Ist eine Person, über die eine BZR-Auskunft begehrt wird, in dieser Personendatei nicht genannt, so bedeutet dies, daß über sie eine Eintragung in der Handkartei, über deren Übernahme noch zu entscheiden ist, nicht vorliegt — sei es, daß es eine solche Eintragung dort nie gegeben hat, sei es, daß bereits über ihre Übernahme ins BZR — positiv oder negativ — entschieden ist. Ist eine Person in dieser Datei genannt, so bedeutet dies, daß über sie eine möglicherweise eintragungsfähige Entscheidung in der Handkartei vorliegt.

Ich habe mich bei meinem Besuch durch Prüfung einer größeren Zahl von Einzelfällen davon überzeugt, daß entsprechend diesem Konzept verfahren wird, und daß die Datensätze der automatisiert geführten Personendatei im Einklang mit den gesetzlichen Vorschriften gesperrt sind. Ein Hemmnisvermerk schließt BZR-Auskünfte aus der Personendatei aus.

Meine Kontrolle einzelner Übernahmeentscheidungen sowie die Prüfung der festgelegten Entscheidungsabläufe und der vorgelegten Arbeitsanweisungen hat datenschutzrechtliche Bedenken nicht erkennen lassen. Auf die sich aus der gesetzlichen Regelung ergebende Frage, welches die Verurteilungen und Erkenntnisse sind, die mit rechtstaatlichen Maßstäben nicht vereinbar sind oder bei denen der zugrunde liegende Sachverhalt nicht mehr mit Strafe bedroht ist, ist mit dem vom Generalbundesanwalt — Dienststelle Bundeszentralregister — erstellten Katalog der sogenannten indizierten Normen des DDR-Strafgesetzbuchs eine auch aus meiner Sicht plausible Antwort gegeben.

Schwierig ist die Übernahmeentscheidung in den Fällen der sogenannten *Mischverurteilungen*, d. h. in Fällen, bei denen die Verurteilung sich auf einen oder mehrere indizierte *und* nicht indizierte Tatbestände stützt. Positiv bewerte ich hierbei die Praxis, daß in Fällen, in denen die indizierte Straftat — z. B. ungesetzlicher Grenzübertritt — mit einer weniger bedeutsamen nicht-indizierten Straftat — z. B. Sachbeschädigung — zusammentrifft, auch bezüglich der letzteren auf Nichtübernahme entschieden wird. Ich habe keine Bedenken dagegen erhoben, daß das Bundeszentralregister z. B. beim Zusammentreffen einer Verurteilung wegen des aus Gründen mangelnder Normenklarheit indizierten Tatbestandes des Rowdytums (§ 215 DDR StG) mit einer Verurteilung wegen Körperverletzung für die letztere eine positive Übernahmeentscheidung getroffen hat.

Wird bei einer Mischverurteilung auf eine teilweise Übernahme entschieden, so wird der Zusatz: „Der *Strafausspruch* erstreckt sich auf einen weiteren nicht eintragungsfähigen Teil des *Schuldspruchs*" in die BZR-Eintragung aufgenommen.

Ich habe Zweifel, ob dies den Vorstellungen der Einigungsvertragspartner entsprach, weil dieser Eintrag dazu führt, daß die nicht rechtsstaatliche Verurteilung doch eine Spur hinterläßt. Auch eine eingehende Erörterung der Problematik mit dem Generalbundesanwalt hat aber keine Lösungsmöglichkeit erkennen lassen, die den berechtigten Belangen des Betroffenen besser entspräche. Ein Verzicht auf die Eintragung des *Strafausspruchs* im BZR würde zu Unklarheiten führen und ebenso auf eine frühere nicht rechtsstaatliche Verurteilung hinweisen wie der Zusatz. Ein Verzicht auf den genannten Zusatz käme den Belangen des Betroffenen noch weniger entgegen. Im Ergebnis bleibt bei dieser Problematik meine Empfehlung, bei Mischverurteilungen im Rahmen des Vertretbaren möglichst großzügig auf Nichtübernahme zu entscheiden.

Eine vergleichbare Problematik stellt sich, wenn über die Übernahme einer Entscheidung befunden werden muß, die eine frühere nicht zu übernehmende Entscheidung in eine zu übernehmende Verurteilung einbezogen hat. In diesen Fällen vermerkt das BZR: „Der Strafausspruch der einbezogenen nicht eintragungsfähigen Entscheidung lautet auf . . . (z. B. zwei Jahre sechs Monate Freiheitsstrafe)". In diesen Fällen einen nach einer Subtraktionsrechnung geänderten Strafausspruch einzutragen, dürfte — darin teile ich die Auffassung des BZR — dessen Kompetenzen überschreiten. Bei der Berechnung der Frist für die Tilgung aus dem BZR halte ich diese Subtraktionsrechnung im Strafausspruch aber nicht nur für zulässig, sondern für geboten.

Eine andere Problematik bilden solche Verurteilungen, die — wie z. B. Steuerhinterziehung — durchaus eintragungsfähig sind, bei denen die Höhe des Strafausspruchs aber auf nichtrechtsstaatlichen Erwägungen beruht (Beispiel: Dem Strafausspruch lag das Ziel zugrunde, den Betroffenen zur Aufgabe von Antiquitäten zu zwingen). Meine Vermutung, Fälle dieser Art könnten sich aus den Eintragungen im ehemaligen DDR-Strafregister erkennen lassen, hat sich bei meiner Kontrolle nicht bestätigt. Die jeweils eingetragene Strafhöhe läßt zuverlässige Rückschlüsse dieser Art

nicht zu. Ich teile daher die Auffassung des Generalbundesanwalts, daß in diesen Fällen dem Betroffenen in erster Linie die Möglichkeit zur Verfügung steht, die Aufhebung des Strafurteils oder die Beseitigung seiner Wirkungen außerhalb der Zuständigkeit der Abteilung IV des Generalbundesanwalts durch ein Verfahren der Kassation oder Rehabilitierung zu erreichen. Allerdings sollte — so habe ich angeregt — der Generalbundesanwalt die Vorschriften der §§ 49 Abs. 1 und 39 Abs. 1 BZRG großzügig handhaben, wonach unter bestimmten Voraussetzungen im Einzelfalle die Eintragung vorzeitig getilgt oder auf ihre Aufnahme in ein Führungszeugnis verzichtet werden kann, wenn im Rahmen eines entsprechenden Antrags des Betroffenen Anhaltspunkte dafür erkennbar werden, daß der Strafausspruch durch nicht rechtsstaatliche Erwägungen beeinflußt ist.

Der Bundesminister der Justiz hat in einem Merkblatt vom 25. Oktober 1990 für Betroffene Hinweise „zu den Möglichkeiten, die Aufhebung rechtskräftiger Strafurteile der DDR oder die Beseitigung ihrer Wirkungen zu erreichen, insbesondere durch Kassation und Rehabilitierung" gegeben; jeder Bürger kann das Merkblatt dort anfordern. Die genannten Verfahren stehen dem Betroffenen auch bei den zuvor genannten Mischverurteilungen offen, namentlich auch dann, wenn der Betroffene die Löschung einer teilweisen Übernahme in das BZR anstrebt.

Meine besondere Aufmerksamkeit galt auch der Verwendung von Informationen im ehemaligen DDR-Strafregister für die Rehabilitierung von Betroffenen. Im Einklang mit dem genannten Merkblatt des Bundesjustizministeriums und mit Überlegungen des Generalbundesanwalts habe ich befürwortet, den in der gesetzlichen Regelung (§ 64 b Satz 3 BZRG) verwandten Begriff „Rehabilitierung" zugunsten der Betroffenen weit auszulegen. Es darauf ankommen zu lassen, ob ein Verfahren der Rehabilitierung im engeren Sinne oder ob ein Kassationsverfahren eingeleitet wurde, wäre nicht sachgerecht. Das Verfahren des Generalbundesanwalts, die Übermittlung von Informationen für Zwecke der Rehabilitierung durch Ablichtung aus der Handkartei abzuwickeln, wird von mir — auch unter Gesichtspunkten der Klarheit und Praktikabilität der Arbeitsabläufe — gutgeheißen.

Im engen Zusammenhang mit den vorgenannten Schwerpunkten meiner Kontrolle beim Generalbundesanwalt bin ich auch der Frage der Auskunftsersuchen an das Bundeszentralregister aus den neuen Bundesländern nachgegangen. Anträge auf Erstellung eines Führungszeugnisses werden durch die Bürger der neuen Bundesländer an die für sie jeweils zuständige Meldestelle gerichtet (dies sind die Meldestellen bei den Kreisverwaltungsbehörden, die früher in den Volkspolizeikreisämtern eingerichtet waren), welche diese Anträge an das Zentrale Einwohnerregister weiterleiten. Beim ZER werden die Personendaten der Antragsteller so aufbereitet, wie das Bundeszentralregister sie zur weiteren Bearbeitung benötigt und diesem auf Magnetband zur Verfügung gestellt. Die weitere Bearbeitung erfolgt, wie ich festgestellt habe, in der bisher im BZR üblichen Weise. Diese Verfahrensweise ist für die Zeit bis zum Aufbau funktionsfähiger Meldebehörden in den neuen Bundesländern und der damit verbundenen Auflösung des ZER nicht zu vermeiden. Abweichend von dem oben Gesagten stellen die Ostberliner und Potsdamer Meldestellen die Anträge auf Erteilung eines Führungszeugnisses nicht über das ZER, sondern bereits jetzt direkt an das Bundeszentralregister.

2.10 Zentrales Fahrerlaubnisregister

In dem Zentralen Einwohnerregister der ehemaligen DDR waren den Personendatensätzen u. a. auch Daten über den Führerscheinbesitz (Positivdaten) und über den Führerscheinentzug (Negativdaten) zugeordnet; diese Datensammlung wird im Einigungsvertrag als Zentrales Fahrerlaubnisregister bezeichnet. Die erwähnten Negativdaten sind gemäß Anlage I, Kapitel XI, Sachgebiet B, Abschnitt III Nr. 1 f) des Einigungsvertrages inzwischen vom Kraftfahrt-Bundesamt (KBA) übernommen worden und werden dort als besonderer und getrennter Teil des Verkehrszentralregisters geführt.

Bis zu einer in der zitierten Stelle des Einigungsvertrages angekündigten gesetzlichen Regelung über die endgültige Übernahme der Negativdaten in das Verkehrszentralregister ist die Erteilung von Auskünften aus dieser Datei durch das KBA nicht unproblematisch, weil die gespeicherten Informationen über den Entzug einer Fahrerlaubnis in der früheren DDR keine Aussage über die Gründe für diese Maßnahme liefern. So könnten in der ehemaligen DDR sachfremde Gründe, die keinen Bezug zum Straßenverkehr aufwiesen, zu einem Entzug der Fahrerlaubnis geführt haben. Das Kraftfahrt-Bundesamt weist daher bei Auskunftserteilung aus dem besonderen Teil des Verkehrszentralregisters mit Recht darauf hin, daß die betreffende Fahrerlaubnis nach den Bestimmungen der ehemaligen DDR entzogen wurde. Ob dieser Hinweis den Fahrerlaubnisbehörden Anlaß geben wird, zunächst die Hintergründe für derartige Fahrerlaubnisentzüge zu erforschen und erst danach fahrerlaubnisrechtliche Entscheidungen zu treffen, werde ich durch Kontrollbesuche bei den örtlichen Fahrerlaubnisbehörden in der ehemaligen DDR feststellen und gegebenenfalls Vorschläge für ein datenschutzrechtlich einwandfreies Vorgehen machen. Wegen der genannten Unsicherheiten bleibt der Bundesminister für Verkehr aufgerufen, die vorgesehene gesetzliche Regelung möglichst bald einzuleiten.

Eine Übernahme der Daten über den Besitz eines Führerscheins (Positivdaten) durch das Kraftfahrt-Bundesamt ist bisher nur insoweit durchgeführt worden, als zu dieser Person auch Negativdaten vorhanden sind. Eine weitergehende Übernahme ist nach meiner Ansicht auch nicht zulässig. Für die Behandlung verwaltungsfremder Daten aus dem Zentralen Einwohnerregister trifft die Anlage I, Kapitel II, Sachgebiet C, Abschnitt III Nr. 4 Buchstabe c, bb) zum Einigungsvertrag eine abschließende Regelung. Diese ist auf die hier in Rede stehenden Daten anzuwenden, da eine zentrale Sammlung aller erteilten Fahrerlaubnisse von der gegenwärtigen Rechtsordnung nicht gedeckt ist. Die Überführungsregelung in Kapitel XI des Einigungsvertrages kann sich daher nur auf die Negativ-

daten beziehen. Die Positivdaten sind zum frühestmöglichen Zeitpunkt im Zentralen Einwohnerregister zu löschen.

2.11 Sozialdatenschutz im Beitrittsgebiet

Auch im Bereich des Sozialdatenschutzes haben sich durch den Beitritt der früheren DDR neue Probleme ergeben. Vor allem galt es den Aufbau eines gegliederten Sozialversicherungssystems entsprechend den Übergangsregelungen des Einigungsvertrages unter datenschutzrechtlichen Gesichtspunkten zu begleiten. Die nachfolgenden Beiträge stellen einige Schwerpunkte meiner Arbeit auf diesem Gebiet dar.

2.11.1 Ausweis für Arbeit und Sozialversicherung

Ein besonderes Problem des Sozialdatenschutzes stellt die Weiterverwendung des „Ausweises für Arbeit und Sozialversicherung" dar.

Dieser Ausweis, den jeder Arbeitnehmer und Sozialversicherte im Gebiet der früheren DDR besitzt, enthält neben Daten der Schul- und Berufsausbildung sowie der bisherigen Beschäftigungsverhältnisse einschließlich der Arbeitsentgelte u. a. besonders schützenswerte Angaben über Arbeitsunfähigkeitszeiten, die entsprechenden ärztlichen Untersuchungen und Behandlungsdaten, einschließlich Diagnosen, sowie verordneter Heil- und Hilfsmittel.

Die Eintragungen in den Ausweis, insbesondere über Beschäftigungszeiten und Arbeitsentgelte, wurden in der ehemaligen DDR auch als Grundlage für Rentenberechnungen genutzt. Der Ausweis mußte dem Arbeitgeber zur Eintragung der dafür notwendigen Daten vorgelegt werden. Damit war es ihm möglich, von allen darin enthaltenen Angaben Kenntnis zu nehmen.

Aufgrund der übergeleiteten Vorschriften des § 80 des Gesetzes über die Sozialversicherung der DDR vom 28. Juni 1990 ist das Arbeitsentgelt bis Ende 1991 weiterhin vom Arbeitgeber in den Ausweis einzutragen. Erst ab 1. Januar 1992 soll das entsprechende in den alten Bundesländern bestehende DEVO/DÜVO-Verfahren auch im Beitrittsgebiet uneingeschränkt praktiziert werden.

Die sich hieraus für sämtliche Arbeitnehmer der neuen Bundesländer ergebende Notwendigkeit, ihre Ausweise bis Ende 1991 den Arbeitgebern vorzulegen, kann unter datenschutzrechtlichen Gesichtspunkten nicht einfach hingenommen werden. Ich habe deshalb den Bundesminister für Arbeit und Sozialordnung dringend um eine Übergangsregelung gebeten, die meine datenschutzrechtlichen Bedenken berücksichtigt. Da der Ersatz des Ausweises durch eine besondere Bescheinigung aus praktischen Gründen nicht realisierbar erschien, habe ich empfohlen, ein Verfahren zu wählen, bei dem die notwendigen Eintragungen in den Ausweis entweder nur in Anwesenheit der betroffenen Arbeitnehmer oder einer von dem Arbeitnehmer hierzu beauftragten Vertrauensperson (z. B. einem Mitglied der Personalvertretung) erfolgen. Eine Vorlage des Ausweises aus anderen Gründen soll nicht gefordert werden dürfen. Der Bundesminister für Arbeit und Sozialordnung hat daraufhin ein Merkblatt verfaßt, das u. a. Hinweise auf ein möglichst datenschutzgerechtes Verfahren im Umgang mit dem Ausweis für Arbeit und Sozialversicherung enthält. Es soll über Arbeitnehmerorganisationen und öffentliche Einrichtungen, die im Gebiet der ehemaligen DDR in engem Kontakt mit den Arbeitnehmern stehen, verbreitet werden. Dieses Verfahren entspricht unter den gegebenen Bedingungen im wesentlichen meinen Vorstellungen. Ich habe diese Übergangsregelung deshalb unter Zurückstellung von Bedenken hingenommen.

Ein vergleichbares Problem ergibt sich aus der bis Ende 1990 bestehenden Praxis, nach der ein dem Arbeitgeber vorzulegender Arbeitsunfähigkeitsnachweis ebenfalls die Diagnose enthält. Diese beim Arbeitgeber vorhandenen Diagnosedaten müssen noch so lange vorgehalten werden, bis feststeht, ob eine Übernahme der Daten in das Versicherungskonto des Arbeitnehmers beim Rentenversicherungsträger erforderlich ist, oder eine abschließende Prüfung durch den zuständigen Sozialversicherungsträger über Beitragszahlung und gegebenenfalls auftragsweise Leistungserbringung durch den Arbeitgeber stattgefunden hat. Der Bundesminister für Arbeit und Sozialordnung wird auf meine Veranlassung auf eine konsequente Abschottung der Diagnoseangaben gegenüber den Personalstellen des jeweiligen Arbeitgebers hinwirken.

2.11.2 Sozialdatenschutz in der Arbeitsverwaltung

Mit dem Wirksamwerden des Einigungsvertrages am 3. Oktober 1990 gingen die Dienststellen der Arbeitsverwaltung der bisherigen DDR in den Verantwortungsbereich der Bundesanstalt für Arbeit über. Diese bemüht sich, ihre gesetzlichen Aufgaben mit sächlicher und personeller Hilfe aus den alten Bundesländern zügig und datenschutzgerecht zu erbringen. Die Bundesanstalt hat in den neuen Bundesländern Organisations- und Verfahrensregelungen sowie Weisungen zur Rechtsanwendung — unter Anpassung an die dortigen besonderen Verhältnisse — in Kraft gesetzt und den Mitarbeitern durch Einweisungen, Besprechungen und Schulungsveranstaltungen erläutert.

Nach den Regelungen des Einigungsvertrages sind neben dem Bundesdatenschutzgesetz die Datenschutzvorschriften des SGB I und des SGB X für den Bereich der Bundesanstalt für Arbeit ab 3. Oktober 1990 in vollem Umfang anzuwenden. In einer für die Dienststellen der neuen Bundesländer herausgegebenen Verwaltungsvorschrift vom 7. Dezember 1990 hat die Bundesanstalt auf die besonderen Voraussetzungen, unter denen personenbezogene Daten an Dritte offenbart werden dürfen, und die Rechte der Bürger nach dem BDSG hingewiesen.

Ein Schwerpunkt der Verwaltungsvorschrift gilt mit Recht dem Auskunftsverfahren. Auskunftsersuchen von Betroffenen ist im Interesse größtmöglicher Transparenz des Verwaltungshandelns weitestgehend zu entsprechen. Auskünfte aus Dateien sollen

grundsätzlich unentgeltlich erfolgen, nur in Sonderfällen eines unverhältnismäßig hohen Verwaltungsaufwandes kann eine Gebühr erhoben werden, eine Regelung, die auch nur noch bis zum Inkrafttreten des neuen Bundesdatenschutzgesetzes zulässig ist. Auf Verlangen schließt die Auskunft auch die kostenlose Fertigung von Fotokopien ein; ausgenommen hiervon sind lediglich ärztliche und psychologische Gutachten.

Die Bundesanstalt hat mir mitgeteilt, die Datenverarbeitung im Beitrittsgebiet erfolge vielfach noch manuell. Da die Aufgabenerledigung sich zudem unter erschwerten räumlichen Bedingungen vollziehe, könnten die Ansprüche an Datenschutz und Datensicherheit im bisherigen Bundesgebiet nicht immer sofort durchgesetzt werden. Ich habe hierfür Verständnis und beabsichtige, im Jahre 1991 gemeinsam mit Vertretern der Bundesanstalt Informationsbesuche bei Arbeitsämtern im Beitrittsgebiet durchzuführen, um die Bundesanstalt dann noch besser beraten zu können.

2.11.3 Sozialdatenschutz in der Rentenversicherung

Datenschutzfragen der Rentenversicherung in den neuen Bundesländern waren u. a. Gegenstand von Erörterungen mit der Bundesversicherungsanstalt für Angestellte. Dabei war von den besonderen Regelungen des Einigungsvertrags über die Rentenversicherung auszugehen, die folgendes vorsehen:

Das zum Zeitpunkt des Beitritts bestehende Rentenversicherungsrecht der ehemaligen DDR gilt im Grundsatz bis zum 31. Dezember 1991 weiter. Ausnahmen von dieser Regel bestehen insbesondere für die bereichsübergreifenden Vorschriften des Sozialgesetzbuches sowie für die von der Rentenversicherung durchzuführende Rehabilitation. So sind das Sozialgesetzbuch — Allgemeiner Teil (SGB I) — und das Sozialgesetzbuch — Verwaltungsverfahren (SGB X) — für den Bereich der Rentenversicherung ab 1. Januar 1991 im Beitrittsgebiet anzuwenden. Auch das Sozialgesetzbuch — Gemeinsame Vorschriften für die Sozialversicherung (SGB IV) — gilt seit diesem Zeitpunkt, allerdings mit einer Reihe von Maßgaben.

Seit 1. Januar 1991 erstreckt sich die Zuständigkeit der bundesweiten Träger der Rentenversicherung (Bundesversicherungsanstalt für Angestellte, Bundesknappschaft, Seekasse, Bundesbahnversicherungsanstalt) auch auf das Beitrittsgebiet. Im Interesse einer geordneten Überleitung der Aufgaben wurde der bisherige Träger der Sozialversicherung der DDR nicht zum 31. Dezember 1990 aufgelöst, sondern in eine „Überleitungsanstalt Sozialversicherung" als rechtsfähige Anstalt des öffentlichen Rechts umgewandelt. Diese hat längstens bis zum 31. Dezember 1991 im Namen und im Auftrag der zuständigen Träger der Rentenversicherung deren Aufgaben zu erfüllen. Die Aufsicht über die Überleitungsanstalt führt das Bundesversicherungsamt.

Die Datenschutzvorschriften des SGB I und SGB X sowie des BDSG gelten ab 1. Januar 1991 auch für die Überleitungsanstalt. Sie hat daher das Sozialgeheimnis zu wahren.

2.12 Nationales Krebsregister der ehemaligen DDR

Das Nationale Krebsregister der ehemaligen DDR wird gegenwärtig vom Zentralinstitut für Krebsforschung in Berlin geführt. Das Zentralinstitut besteht gemäß Artikel 38 Abs. 2 Satz 3 des Einigungsvertrages zunächst bis zum 31. Dezember 1991 als Einrichtung der Länder im Beitrittsgebiet fort. Die Übergangsfinanzierung des Instituts ist bis zu diesem Zeitpunkt dadurch sichergestellt, daß vom Bund und den neuen Bundesländern die erforderlichen Mittel zur Verfügung gestellt werden.

Bei den im Bestand des Krebsregisters erfaßten Daten handelt es sich um Gesundheitsdaten von Patienten, die mit deren Namen an das Register gemeldet wurden. Die Daten sind personenbezogen gespeichert. Zu dem Krebsregister wurde auch noch nach dem Beitritt ohne Einwilligung der Patienten unter Hinweis auf eine bestehende Meldepflicht von Ärzten und Kliniken gemeldet.

Mit dem Gesetz über die amtliche Statistik der DDR vom 17. August 1990 hatte der Gesetzgeber in der ehemaligen DDR in § 6 Abs. 1 bestimmt, daß die republikweiten amtlichen Statistiken durch Gesetz anzuordnen sind. In Absatz 2 des § 6 in Verbindung mit einer Anlage zu diesem Gesetz war das Nationale Krebsregister als amtliche Statistik angeordnet worden.

Das Nationale Krebsregister besitzt nur dann auch heute noch eine ausreichende gesetzliche Grundlage, wenn die in § 6 des Gesetzes über die amtliche Statistik der DDR zum Krebsregister getroffene Regelung fortgilt. Diese Voraussetzung ist nach Anlage II, Kap. XVIII, Abschn. III des Einigungsvertrages jedoch nicht gegeben. Auch als Landesrecht gilt die betroffene Regelung nicht fort, weil die Voraussetzungen des Artikel 9 Abs. 1 des Einigungsvertrags nicht gegeben sind.

Bei dieser Sachlage halte ich in Übereinstimmung mit dem Bundesminister der Justiz, dem Bundesminister des Innern und dem Bundesminister für Gesundheit die Erhaltung des Datenbestandes im Nationalen Krebsregister der ehemaligen DDR während einer Übergangszeit nur dann für möglich, wenn

1. deutlich erkennbar gemacht wird, daß das Krebsregister in absehbarer Zeit auf eine gesetzliche Grundlage gestellt wird,
2. die personenbezogenen Daten und Unterlagen im Krebsregister sofort gesperrt und anonymisiert werden und
3. die erforderlichen Sicherungsmaßnahmen getroffen werden.

Nach meiner Auffassung, die mit der Ansicht der oben genannten Bundesressorts übereinstimmt, darf bis zu dem Zeitpunkt, zu dem der Gesetzgeber seine Entscheidung über das Krebsregister getroffen hat, nur

noch auf der Grundlage einer Meldeberechtigung — also keiner Meldeverpflichtung — der Ärzte oder Kliniken und mit Einwilligung des Patienten unmittelbar an das Krebsregister gemeldet werden. Auch für die Verarbeitung neuer Meldungen im Krebsregister gelten die vorstehend genannten drei Bedingungen.

Um dem Gesetzgeber die erforderliche Gelegenheit und Zeit zur Meinungsbildung zu geben, habe ich in Abstimmung mit dem Berliner Landesdatenschutzbeauftragten, der in Teilbereichen für das Zentralinstitut für Krebsforschung in Berlin zuständig ist, vom Institut gefordert, daß zunächst im Sinne der o. g. Bedingungen verfahren wird. Ich habe die Innenminister der neuen Bundesländer, für die ich nach Maßgabe der Regelung des Einigungsvertrages in Anlage I Kapitel II Sachgebiet C Abschnitt III Nr. 3 noch zuständig bin, gebeten, das Meldeverfahren entsprechend zu gestalten und den Meldebogen auf die Angabe der rechtmäßigen Daten zu begrenzen.

Die notwendigen schnellen Entscheidungen in bezug auf das Nationale Krebsregister der früheren DDR werden sicher auch die allgemeine Diskussion über die Einrichtung von Krebsregistern in der Bundesrepublik Deutschland wieder beleben. Zu den Fragen, die bei der Schaffung solcher Register unter Datenschutzaspekten zu lösen sind, hat die Datenschutzkonferenz von Bund und Ländern in ihrem Beschluß vom 4./5. Oktober 1990 (Anlage 7) Stellung genommen.

2.13 Aufbau des Wehrersatzwesens im Beitrittsgebiet

Der Bundesminister der Verteidigung hat im Oktober 1990 die Einrichtung von insgesamt 26 Kreiswehrersatzämtern in den neuen Bundesländern angeordnet. Bei der Kontrolle eines der neuen Kreiswehrersatzämter ergaben sich eine Reihe datenschutzrechtlich relevanter Fragen, die ich auch mit dem Bundesminister der Verteidigung erörtert habe.

2.13.1 Übernahme von Personalunterlagen

Das Kreiswehrersatzamt hat für die Aufgaben des Wehrersatzwesens Daten von ungedienten Wehrpflichtigen aus dem Beitrittsgebiet und von ehemaligen Angehörigen der NVA zu übernehmen, die in

- einer Suchkartei
- einer Wehrkartei und
- in Unterlagen zur Person

enthalten sind.

Die manuell geführte *Suchkartei* dient dazu, die in der Wehrkartei enthaltenen Wehrstammkarten der einzelnen Wehrpflichtigen aufzufinden und auf vorhandene Unterlagen zur Person hinzuweisen. Die Suchkartei ist nach Personenkennzahlen (PKZ) geordnet; sie enthält jeweils neben Namen und Anschrift die Nummer der sogenannten Nachweisgruppe, in die die Wehrstammkarte in der ebenfalls manuell geführten *Wehrkartei* alphabetisch eingeordnet ist. In der Wehrstammkarte sind die personenbezogenen Daten des Wehrpflichtigen eingetragen. *Unterlagen zur Person* sind sonstige Unterlagen wie etwa Gesundheitsunterlagen.

Die im Beitrittsgebiet zu übernehmenden Personalunterlagen betreffen etwa 4—5 Mio. Personen. Zur Unterstützung der Übernahme in das Wehrersatzwesen-Informationssystem (WEWIS) der Bundeswehr hat das Zentrale Einwohnerregister dem BMVg auf dessen Ersuchen einmalig Daten aller männlichen Deutschen des Beitrittsgebiets vom 18. bis zum 60. Lebensjahr *auf automatisierten Datenträgern* zur Verfügung gestellt. Diese Unterstützungsmaßnahme ist den monatlichen Übermittlungen der Meldebehörden nach § 2 Abs. 2 der Zweiten Meldedaten-Übermittlungsverordnung des Bundes (2. BMeldDÜV) über alle männlichen Deutschen vom 18. bis zum 32. Lebensjahr für Zwecke der Wehrüberwachung an die Kreiswehrersatzämter vergleichbar, die Familienname, Vorname, Anschrift, Geburtsort und Familienstand umfassen. Das Zentrale Einwohnerregister hat dem BMVg darüber hinaus noch die Gesamtzahl der Kinder der Wehrpflichtigen mitgeteilt. Alle übermittelten Daten sind den neuen Wehrersatzbehörden bereits aufgrund der Wehrstammkarten bekannt.

Mit Hilfe der übermittelten Daten werden für alle Wehrpflichtigen des Beitrittsgebietes zwischen 18 und 60 Jahren nach Einspeicherung in WEWIS maschinell Personenkennziffern (PK) der Bundeswehr vergeben. Außerdem werden für die 18- bis 32jährigen ungedienten und gedienten Wehrpflichtigen die in WEWIS zu speichernden Daten anhand der Wehrstammkarten ergänzt und Personalstammblätter ausgedruckt, die dann wie üblich in die manuelle *Gesamtkartei* (Sammlung der sogenannten Klarsichthüllen/Personalunterlagen) des jeweiligen Kreiswehrersatzamtes eingestellt werden. Die Wehrstammkarten selbst werden dort als Anlage beigefügt. Das Verfahren soll bis Mitte 1991 abgeschlossen sein. Die Wehrstammkarten der 32- bis 60jährigen Wehrpflichtigen werden anhand der PK in der manuellen *Ablagekartei* der Kreiswehrersatzämter abgelegt. Vorhandene Unterlagen zur Person werden den Personalstammblättern oder den in die Ablagekartei eingeordneten Wehrstammkarten beigefügt. Die Suchkarten werden laufend vernichtet, wenn die Wehrstammkarten der Gesamt- oder Ablagekartei zugeführt sind. Außerdem werden die Wehrstammkarten der ungedienten Wehrpflichtigen über 32 Jahre vernichtet, da diese Daten für das Wehrersatzwesen nicht mehr benötigt werden.

2.13.2 Datenübermittlung vom Zentralen Einwohnerregister an den BMVg

Obwohl für die dargestellte umfangreiche Datenübermittlung vom Zentralen Einwohnerregister an den BMVg keine ausdrückliche Rechtsgrundlage vorhanden ist, kann sie datenschutzrechtlich hingenommen werden.

In der Sache handelt es sich weitgehend um eine Datenübermittlung entsprechend § 2 Abs. 2 der Zweiten Meldedaten-Übermittlungsverordnung des Bundes. Die Meldebehörden konnten die Daten nicht in geeigneter Form übermitteln, weil sie diese nicht auf automatisierten Datenträgern besaßen. Andererseits hatte der BMVg nach dem Beitritt der neuen Länder die Aufgabe, sich möglichst schnell eine vollständige und verläßliche Übersicht über die Wehrpflichtigen des Beitrittsgebiets zu verschaffen und die vorhandenen Personalunterlagen im Rahmen des Erforderlichen zu übernehmen.

Auf meine Bitte hin hat der BMVg *alle* übermittelten Daten auf den vom Zentralen Einwohnerregister übergebenen Datenträgern gelöscht. Damit ist gewährleistet, daß BMVg und Wehrersatzbehörden nach Übernahme der Daten in WEWIS nur über die Informationen verfügen, die sie benötigen.

2.13.3 Löschung von Daten auf den Wehrstammkarten

Während beabsichtigt ist, die *Suchkarten* aller Wehrpflichtigen zu vernichten, sollen die *Wehrstammkarten* weitgehend aufbewahrt werden. Diese enthalten jedoch zum Teil Daten, die für Zwecke des Wehrersatzwesens nicht benötigt werden oder deren Speicherung nach Bundesrecht unzulässig gewesen wäre (z. B. „Aufenthalt in der Bundesrepublik Deutschland und anderen nichtsozialistischen Staaten sowie Berlin (W)", „Soziale Herkunft", „Partei seit ..."). Der Einigungsvertrag bestimmt, daß abweichend von § 14 Abs. 3 Satz 1 und 2, Halbsatz 1 BDSG die personenbezogenen Daten, deren Kenntnis nach Bundesrecht für die speichernde Stelle zur rechtmäßigen Erfüllung der in ihrer Zuständigkeit liegenden Aufgaben nicht mehr erforderlich ist oder deren Speicherung nach Bundesrecht unzulässig gewesen wäre, unverzüglich zu löschen sind, soweit nicht schutzwürdige Belange des Betroffenen entgegenstehen (Anlage I Kapitel II Sachgebiet C Abschnitt III Nr. 3 Buchstabe c).

Der BMVg wendet sich generell gegen eine Löschung von Daten auf den Wehrstammkarten. Er macht geltend,

- jedenfalls zum gegenwärtigen Zeitpunkt sei nicht abzusehen, ob einer Löschung von Daten schutzwürdige Belange entgegenstehen,
- die Löschung eines Teils der Daten auf den 4 bis 5 Mio. Wehrstammkarten bedeute einen unvertretbaren Aufwand.

Das erste Argument ist bisher nicht näher begründet worden.

Ein hoher Aufwand kann auch nicht davon entbinden, eine klare gesetzliche Regelung, die für den Grundrechtsschutz von erheblicher Bedeutung ist, zu vollziehen.

2.13.4 Bausoldaten

Wehrpflichtige der ehemaligen DDR, die „aus religiösen Anschauungen ... oder ähnlichen Gründen" (Anordnung des Nationalen Verteidigungsrats der DDR vom 16. September 1964, GBl. DDR 1964 S. 129) den Wehrdienst mit der Waffe ablehnten, hatten als sogenannte Bausoldaten in Baueinheiten der NVA Dienst ohne Waffe zu leisten. Die Erklärung, als Bausoldat dienen zu wollen, bedurfte der Schriftform. Nach Auskunft von Mitarbeitern des besuchten Kreiswehrersatzamtes haben sich diese Erklärungen in der Regel auf die Aussage beschränkt, aus den in der maßgeblichen Anordnung des Nationalen Verteidigungsrates der DDR festgelegten Gründen als Bausoldat dienen zu wollen. Gelegentlich seien auch eingehende schriftliche Begründungen gegeben worden. Beispiele für Erklärungen, als Bausoldat Dienst leisten zu wollen, konnten meinen Mitarbeitern allerdings nicht vorgelegt werden. Das Kreiswehrersatzamt begründete dies damit, daß die vorhandenen Unterlagen noch nicht vollständig gesichtet seien. Es sei aber nicht damit zu rechnen, daß sich derartige Unterlagen beim Kreiswehrersatzamt befänden. Die Erklärungen *gedienter* Wehrpflichtiger seien nämlich bei Dienstantritt an die Truppe abgegeben worden.

Ich habe den BMVg gebeten, dem Verbleib der Erklärungen nachzugehen und für diese einen gleichwertigen Schutz sicherzustellen wie für die Akten aus den Anerkennungsverfahren der Kriegsdienstverweigerer (vgl. § 2 Abs. 6 Kriegsdienstverweigerungsgesetz).

Wie mir mitgeteilt wurde, sollten die Erklärungen *ungedienter* Wehrpflichtiger bei Einführung des Zivildienstes in der DDR im Februar 1990 nach Befragung der Betroffenen, ob sie Wehrdienst oder Zivildienst leisten wollten, entsprechend der damaligen Rechtslage an den Direktor des Amtes für Arbeit des zuständigen Rates des Kreises abgegeben werden. Einem Entwurf eines Erlasses des BMVg habe ich jedoch entnommen, daß in den Wehrersatzbehörden des Wehrbereichs VII noch etwa 9 000 Erklärungen *ungedienter* Wehrpflichtiger vorliegen, in denen diese erklären, als Bausoldat dienen zu wollen oder auch den Wehrdienst mit der Waffe *und* den Dienst als Bausoldat ablehnen. Der BMVg hat inzwischen Weisung erteilt, die betroffenen Wehrpflichtigen durch die Kreiswehrersatzämter über die seit dem 3. Oktober 1990 bestehende neue Rechtslage zu unterrichten und darauf hinzuweisen, daß sie einen schriftlichen Antrag auf Anerkennung als Kriegsdienstverweigerer beim Kreiswehrersatzamt stellen können, wenn sie aus Gewissensgründen die Beteiligung an jeder Gewalt zwischen Staaten ablehnen. Wenn bis zu einem bestimmten Termin keine gegenteilige Äußerung erfolge, gehe das jeweilige Kreiswehrersatzamt davon aus, daß der Betroffene für einen Wehrdienst nach dem Wehrpflichtgesetz zur Verfügung stehe.

Eine solche Befragung ist ein erster Schritt, *die dringend erforderliche Klarheit über den weiteren Verbleib* der erwähnten Erklärungen zu erhalten, zumal ich davon ausgehen muß, daß in diesen zumindest zum Teil auch eingehender dargelegt ist, warum die Leistung des Wehrdienstes mit der Waffe abgelehnt wird.

2.14 Datenspeicher „Gesellschaftliches Arbeitsvermögen"

Während eines Informationsbesuches in Sachsen wurde mir vom sogenannten Datenspeicher „Gesellschaftliches Arbeitsvermögen" berichtet. Dabei handelt es sich um eine für statistische Zwecke der ehemaligen DDR angelegte und für Zwecke des Staatssicherheitsdienstes der ehemaligen DDR mitbenutzte Sammlung personenbezogener Daten von über 8 Mio. Arbeitnehmern der früheren DDR. Sie enthielt u. a. Daten wie Personenkennzahl, Grad des Körperschadens, Rentenart, Datum und Grund des Abbruches eines Lehrverhältnisses sowie Datum, Grund und Form des Abgangs aus dem Betrieb. Die Stammdaten waren nach Wirtschaftsorganisationen und Territorien der ehemaligen DDR gegliedert und in zwei Rechenzentren gespeichert. Die Lohndaten wurden in einem weiteren Rechenzentrum zentral gespeichert.

Die Führung des Datenspeichers wurde im Jahre 1990 eingestellt. Zur Zeit wird geprüft, ob eine Kopie der Datensammlung dem Bundesarchiv überlassen werden kann. Die Bundesanstalt für Arbeit, Institut für Arbeitsmarkt- und Berufsforschung, besitzt eine anonymisierte Kopie der Datei, die sie für künftige wissenschaftliche Auswertungen nutzen will. Die damit zusammenhängenden Fragen werden noch zwischen dem Bundesminister für Arbeit und Sozialordnung und mir erörtert.

2.15 Treuhandanstalt

Seit dem 3. Oktober 1990 untersteht die Treuhandanstalt meiner datenschutzrechtlichen Kontrolle.

Die THA wurde durch Gesetz zur Privatisierung und Reorganisation volkseigenen Vermögens (Treuhandgesetz) vom 17. Juni 1990 durch die Volkskammer der ehemaligen DDR errichtet. Nach Artikel 25 des Einigungsvertrages gilt das Gesetz mit bestimmten Maßgaben fort. Seit dem Beitritt der neuen Länder ist die THA eine rechtsfähige bundesunmittelbare Anstalt des öffentlichen Rechts.

Vorrangig galt es mit der THA Lösungen für das Problem des Verbleibs personenbezogener Dateien oder Akten ehemals staatlicher Einrichtungen zu finden, die nicht unternehmerischen Zwecken dienten.

Die Verantwortlichen in der THA sind aufgeschlossen für Fragen des Datenschutzes und der Datensicherung. Innerhalb der THA selbst sind die nach dem BDSG notwendigen Maßnahmen eingeleitet worden. Eine wichtige Arbeitsgrundlage für die Tätigkeit der THA ist die Unternehmensdatenbank, in der die wesentlichen Angaben über die rund 9 000 Firmen mit Treuhandbeteiligung gespeichert sind. Die Unternehmensdatenbank enthält einige wenige personenbezogene Daten, im übrigen aber Angaben über Unternehmen, die nicht unter den Schutz des BDSG fallen. Die Belange der Datensicherheit werden gesehen und beachtet.

Nach meinem Eindruck wird über den internen Treuhandbetrieb hinaus die politische Verantwortung für den Verbleib unternehmensfremder personenbezogener Daten in den Betrieben erkannt. In Absprache mit mir hat die THA aus diesem Grunde sämtliche Treuhandbetriebe angeschrieben, auf die wesentlichen Bestimmungen des Bundesdatenschutzgesetzes hingewiesen und die Betriebe, in denen die Voraussetzungen hierfür vorliegen, aufgefordert, Datenschutzbeauftragte zu benennen. Ferner wurden die Betriebe darauf aufmerksam gemacht, daß Dateien und Unterlagen, die nicht rein betriebliche Aufgaben erfüllen, umgehend für jede Nutzung zu sperren sind. Jeder Treuhandbetrieb hat einen Text des neu gefaßten Datenschutzgesetzes erhalten.

Ich habe nachdrücklich angeregt, daß ein gleichlautendes Schreiben der THA den rund 100 Rechenzentren in den neuen Ländern, die früher im staatlichen Auftrag tätig waren und jetzt weitgehend privatisiert werden sollen, zugeleitet wird.

Das Ergebnis der gesamten Aktion stand bei Redaktionsschluß noch nicht fest. Ich beabsichtige, nach Auswertung des Ergebnisses gemeinsam mit der THA ein Konzept zu entwickeln, das den Mißbrauch personenbezogener Daten, die früher staatlichen Zwecken dienten, soweit irgend möglich verhindern soll. Insbesondere muß gewährleistet werden, daß durch Behörden gespeicherte personenbezogene Daten von den privatisierten Rechenzentren an die zuständigen Behörden herausgegeben werden oder aber ein klares Rechtsverhältnis zur Datenverarbeitung im Auftrag zwischen Behörde und Rechenzentrum begründet wird.

2.16 Nicht-öffentlicher Bereich

Seit Inkrafttreten des Einigungsvertrages haben die Unternehmen und Betriebe in den neuen Bundesländern die für den nicht-öffentlichen Bereich geltenden Bestimmungen des Bundesdatenschutzgesetzes zu beachten. Dies bedeutet in der Regel völliges Neuland, da es in der Wirtschaft der früheren DDR ein vergleichbares Datenschutzverständnis nicht gegeben hat.

Wie ich Eingaben entnommen habe, haben früher unbekannte Werbemethoden der Wirtschaft teilweise Verwunderung und Ärger erregt. Mir wurde die Frage gestellt, wie die werbenden Unternehmen denn an die Adressen der Bürger gelangt seien. Ich konnte nur darauf verweisen, daß die geschilderten Werbemaßnahmen nach geltendem Datenschutzrecht grundsätzlich zulässig sind, das künftige Datenschutzrecht dem Betroffenen aber die Möglichkeit bietet, der Verwendung seiner Daten für Zwecke der Werbung zu widersprechen.

Die Unternehmen sind — soweit ich das bisher beurteilen kann — bemüht, die Vorschriften des BDSG zu beachten. Sie werden dabei durch Organisationen aus den „alten" Ländern unterstützt, die schon vor der Vereinigung verschiedene Initiativen zur Verbreitung des Gedankens des Datenschutzes ergriffen haben. So sind nach dem Vorbild der Erfahrungsaustauschkreise der Gesellschaft für Datenschutz und Datensi-

cherung (GDD) auch in den neuen Bundesländern entsprechende Gremien konstituiert worden. Ich selbst und auch meine Mitarbeiter haben auf derartigen Veranstaltungen erste Informationen zum Datenschutz auch im privatrechtlichen Bereich gegeben. Mein Angebot, auch im nicht-öffentlichen Bereich zur Verbesserung des Datenschutzes im Beitrittsgebiet beizutragen, wird weiter angenommen.

Ich habe mich in diesem Aufgabenbereich als Berater und Informationsgeber engagiert, obwohl ich für die Kontrolle des nicht-öffentlichen Bereichs nicht zuständig bin, weil die Datenschutzaufsichtsbehörden in den neuen Ländern erst allmählich aufgebaut werden konnten und bis vor kurzem noch nicht einsatzfähig waren.

3 Innere Verwaltung und Auswärtiger Dienst

3.1 Neuregelung des Ausländerrechts

In meinem Zwölften Tätigkeitsbericht (S. 22f.) habe ich auf bereits bei der Vorbereitung des Regierungsentwurfs für ein Gesetz zur Neuregelung des Ausländerrechts erreichte datenschutzrechtliche Verbesserungen des Regierungsentwurfs hingewiesen. An der weiteren Vorbereitung des Gesetzes in den parlamentarischen Beratungen war ich ebenfalls intensiv beteiligt. Es ist inzwischen am 1. Januar 1991 in Kraft getreten.

Die Durchführung des Ausländerrechts obliegt im wesentlichen den Ländern. Für die notwendige Abstimmung mit den Landesbeauftragten für den Datenschutz ließen — wie schon bei der Vorbereitung des Regierungsentwurfs — die engen Fristen der Gesetzesvorbereitung nur unzureichenden Raum. Dennoch sehe ich in den schließlich erreichten datenschutzrechtlichen Bestimmungen, die ja vom materiellen Inhalt des Ausländergesetzes ausgehen müssen, insgesamt eine angemessene und ausgewogene Regelung. Die Praxis wird freilich erweisen müssen, ob und inwieweit dieses Urteil zutrifft.

Kernstück des Gesetzes zur Neuregelung des Ausländerrechts ist das neue Ausländergesetz. Es geht ausdrücklich von dem allgemeinen datenschutzrechtlichen Grundsatz aus, daß die mit der Ausführung dieses Gesetzes betrauten Behörden die zu ihrer Aufgabenerfüllung erforderlichen Daten beim Ausländer selbst zu erheben haben. Das Ausländergesetz legt im einzelnen fest, wann ausnahmsweise eine Erhebung von Daten bei anderen öffentlichen Stellen zulässig ist, so z. B. dann, wenn die Mitwirkung des Ausländers nicht ausreicht oder einen unverhältnismäßigen Aufwand erfordern würde. In solchen Fällen dürfen aber keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Ausländers durch die Beteiligung einer anderen öffentlichen Stelle beeinträchtigt werden.

Für die Übermittlung von Daten eines Ausländers durch eine andere öffentliche Stelle an die Ausländerbehörde unterscheidet das Gesetz zwischen

- Mitteilungen *auf Ersuchen* der Ausländerbehörde, die ihrerseits zuvor stets im Einzelfall die Erforderlichkeit der Mitteilung zur Erfüllung ihrer Aufgaben zu prüfen hat, und

- Mitteilungen *ohne Ersuchen* der Ausländerbehörde in Fällen, in denen der Gesetzgeber selbst ein überwiegendes Allgemeininteresse an der Unterrichtung der Ausländerbehörde bejaht hat. Dies gilt zunächst, wenn eine öffentliche Stelle von Ausweisungsgründen Kenntnis erlangt, d. h. von Tatsachen, die ergeben, daß der Aufenthalt des Ausländers die öffentliche Sicherheit und Ordnung oder sonstige *erhebliche* Interessen der Bundesrepublik Deutschland beeinträchtigt (§ 76 Abs. 2 Ausländergesetz). Mitteilungen ohne Ersuchen sind auch in den Fällen zu machen, die der Bundesminister des Innern in der Ausländerdatenübermittlungsverordnung, die ebenfalls am 1. Januar 1991 in Kraft getreten ist, festgelegt hat.

Ein wichtiges Anliegen war es mir, bei der Übermittlung von Daten an die Ausländerbehörden die Beachtung vorhandener gesetzlicher Verwendungsregelungen — wie z. B. des Arztgeheimnisses, des Steuergeheimnisses und namentlich auch des Sozialgeheimnisses — sicherzustellen. Ich habe mich besonders dafür eingesetzt, daß Datenübermittlungen unterbleiben müssen, wenn solche Verwendungsregelungen entgegenstehen, und daß Fälle, in denen der Gesetzgeber eine Durchbrechung dieses Grundsatzes für unabweislich hält, normenklar beschrieben wurden. Das Ausländergesetz bestimmt dementsprechend z. B., daß das Arztgeheimnis nur durchbrochen werden darf, wenn der Ausländer die öffentliche Gesundheit gefährdet und besondere Schutzmaßnahmen zum Ausschluß der Gefährdung nicht möglich sind oder von dem Ausländer nicht eingehalten werden, oder soweit die Daten für die Feststellung erforderlich sind, ob der Ausländer Heroin, Kokain oder ein vergleichbar gefährliches Betäubungsmittel verbraucht und nicht zu einer erforderlichen, seiner Rehabilitation dienenden Behandlung bereit ist oder sich ihr entzieht.

Unter den gleichen Gesichtspunkten wurden in Artikel 8 des Neuregelungsgesetzes durch Änderung des Sozialgesetzbuchs einschränkende und präzise Regelungen darüber geschaffen, wann unter Durchbrechung des Sozialdatenschutzes ausnahmsweise eine Offenbarung personenbezogener Daten eines Ausländers zulässig ist. Für Mitteilungen auf Ersuchen sind hier jeweils sowohl der Zweck, für den die Daten benötigt werden (z. B. „für die Entscheidung der Ausländerbehörde über den Aufenthalt oder über die ausländerrechtliche Zulassung oder Beschränkung einer Erwerbstätigkeit"), als auch die Art der zu offenbarenden Daten (z. B. „über die Arbeitserlaubnis oder eine sonstige Berufsausübungserlaubnis") festgelegt.

Das Gesetz schafft Rechtsgrundlagen für die Einrichtung der zur Durchführung des Ausländergesetzes erforderlichen Dateien, indem es den Bundesminister des Innern zum Erlaß hierfür erforderlicher Rechtsverordnungen ermächtigt. Die entsprechende Ausländerdateienverordnung, die die Führung von Ausländ-

derdateien durch die Ausländerbehörden und die Führung von Visadateien durch die Auslandsvertretungen betrifft, ist inzwischen am 1. Januar 1991 in Kraft getreten. Am selben Tage ist die Verordnung zur Durchführung des Ausländergesetzes in Kraft getreten, die für bestimmte Ausländergruppen aufenthalts- und paßrechtliche Erleichterungen vorsieht und die Rechtsgrundlage für die Führung von Dateien über Reisedokumente, Grenzgängerkarten und Reiseausweise als Paßersatz enthält. Diese beiden Verordnungen berücksichtigen — ebenso wie die schon genannte Ausländerdatenübermittlungsverordnung — von mir gegebene Anregungen.

Zur Zeit arbeitet eine Bund-Länder-Arbeitsgruppe an Allgemeinen Verwaltungsvorschriften zur Durchführung des Ausländergesetzes. Hierbei trete ich besonders dafür ein, daß für die Durchführung der oben erwähnten Regelung über die unverzügliche Unterrichtung der zuständigen Ausländerbehörde bei Kenntnis von Ausweisungsgründen (§ 76 Abs. 2 AuslG) auf der Grundlage des Verhältnismäßigkeitsgrundsatzes möglichst konkret festgelegt wird, worüber der Ausländerbehörde wegen „Beeinträchtigung erheblicher Interessen der Bundesrepublik Deutschland" (§ 45 Abs. 1 AuslG) Mitteilung zu machen ist. Die Notwendigkeit, hierzu mehr Klarheit zu schaffen, ist auch von Landesbeauftragten für den Datenschutz unterstrichen worden.

3.2 Gesundheitsdaten von Asylbewerbern

Im 12. TB (S. 23) habe ich über einen Bericht des von der Arbeitsgemeinschaft der Leitenden Medizinalbeamten (eingerichtet durch die Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder) eingesetzten Ausschusses für Seuchenhygiene berichtet, der sich mit der Frage einer ausreichenden Rechtsgrundlage für routinemäßige ärztliche Untersuchungen von Asylbewerbern befaßt hat. Die Konferenz der für das Gesundheitswesen zuständigen Minister und Senatoren der Länder hat diesen Bericht inzwischen zustimmend zur Kenntnis genommen und dazu einen Beschluß gefaßt. Danach wird es für erforderlich gehalten, daß der öffentliche Gesundheitsdienst ein angemessenes Untersuchungsprogramm für Asylbewerber bereitstellt. Solche Untersuchungen seien aus seuchenhygienischen und fürsorgerischen Gründen auf freiwilliger Basis sinnvoll und geboten. Den datenschutzrechtlichen Anforderungen müsse dabei Rechnung getragen werden. In diesem Beschluß ist festgehalten, daß „eine Rechtsgrundlage, die jeden einzelnen Asylbewerber unmittelbar verpflichtet, an ärztlichen Untersuchungen teilzunehmen" nicht besteht. Eine Verpflichtung bestehe nur im Einzelfall, „wenn die Gesundheitsbehörde auf der Grundlage der Bestimmungen des Bundes-Seuchengesetzes oder die Ausländerbehörde auf der Grundlage des Asylverfahrensgesetzes Untersuchungen anordnet".

Das Prinzip der Freiwilligkeit der Untersuchungen habe ich bereits in meinem 12. TB als erfreulichen Ansatz gekennzeichnet. Soweit jedoch der Beschluß als Grundlage für die ausnahmsweise Anordnung von zwangsweisen Untersuchungen das Asylverfahrensgesetz nennt, habe ich schon in meinem 10. TB (S. 15) auf den Mangel an Normenklarheit des als Rechtsgrundlage angeführten § 20 Abs.2 Satz 1 Asylverfahrensgesetz hingewiesen. Nach wie vor gilt meine Empfehlung, präzise Gesetzesvorschriften zu schaffen, wenn die zwangsweise Erhebung medizinischer Daten von Asylbewerbern tatsächlich erforderlich sein sollte.

3.3 Aussiedleraufnahmegesetz

Die veränderten tatsächlichen Verhältnisse in den Aussiedlungsgebieten sowie verbesserte Reisemöglichkeiten haben für Aussiedler und das bei ihrer Aufnahme zweckmäßige Verfahren eine neue Ausgangslage geschaffen. Das im Juli 1990 in Kraft getretene Gesetz zur Regelung des Aufnahmeverfahrens für Aussiedler (Aussiedleraufnahmegesetz) sollte dem Rechnung tragen. Es galt, auf gesetzlicher Grundlage das Aufnahmeverfahren so auszugestalten, daß die Prüfung der Voraussetzungen für eine Aufnahme in einem vom Bundesverwaltungsamt zu führenden Verfahren bereits vor Verlassen des Herkunftsgebietes abgeschlossen werden konnte. Damit sollte sichergestellt werden, daß nur solche Personen als Aussiedler einreisen, die zum schutzwürdigen Personenkreis im Sinne des Gesetzes gehören. Dieses auch aus meiner Sicht nicht zuletzt im Interesse der Betroffenen selbst zu befürwortende Konzept mindert freilich nicht die auch im bisherigen Verfahren schon bestehenden Schwierigkeiten, in jedem Einzelfall die maßgebenden gesetzlichen Voraussetzungen festzustellen. So ist z. B. zu einem Antragsteller oder zu maßgebenden Bezugspersonen (Eltern, Großeltern) zu ermitteln, ob bei Beginn von gegen Deutsche gerichteten Verfolgungs- und Vertreibungsmaßnahmen die deutsche Staatsangehörigkeit oder die deutsche Volkszugehörigkeit vorgelegen hat.

Meine bei der Vorbereitung des Regierungsentwurfs wegen dessen Eilbedürftigkeit nur unzureichende Beteiligung konnte durch einen intensiven Dialog mit dem BMI im Zuge der parlamentarischen Beratungen des Gesetzes ausgeglichen werden. Dieser hat zu einem gemeinsamen Vorschlag für eine besondere Vorschrift über den Datenschutz und zu einer entsprechenden gesetzlichen Regelung (§ 29 des Bundesvertriebenengesetzes) geführt. Da die Antragsteller selbst meist nicht über ausreichende Unterlagen verfügen, kam es darauf an, in Betracht kommende Unterlagen, die bei einer Vielzahl von Stellen vorhanden sein können, für die Entscheidung nutzbar zu machen, zugleich aber diese Nutzung möglichst präzise zu begrenzen. Die erreichte Regelung läßt in dem Verfahren eine Nutzung bei anderen Stellen vorhandener Unterlagen nur insoweit zu, als sie „über die Vertriebeneneigenschaft Aufschluß geben", und dies auch nur, soweit es zur Feststellung der Voraussetzungen für die Erteilung des Aufnahmebescheides erforderlich ist. Zudem ist festgelegt, daß Daten, die beim Bundesverwaltungsamt und den im Aufnahme-

verfahren mitwirkenden Behörden vorhanden sind, mit Vorrang vor Daten bei anderen öffentlichen und nicht öffentlichen Stellen heranzuziehen sind. Wichtig ist besonders die Klarstellung, daß die Nutzung in jedem Fall unterbleibt, „wenn besondere gesetzliche Verwendungsregelungen oder überwiegende schutzwürdige Interessen des Betroffenen oder Dritter entgegenstehen". Besonders habe ich mich auch für eine präzise Zweckbindung der im Aufnahmeverfahren gesammelten Daten eingesetzt. Nach der nunmehr geschaffenen Regelung dürfen sie, soweit gesetzlich nichts anderes bestimmt ist, nur für Zwecke dieses Verfahrens und in der vorliegenden Regelung näher bestimmte hiermit im Zusammenhang stehende Verfahren, z. B. für den Lastenausgleich, genutzt und übermittelt werden.

Mit der neu geschaffenen gesetzlichen Regelung allein ist es freilich nicht getan. In engem Kontakt mit dem Bundesminister des Innern und mit dem Bundesverwaltungsamt bin ich bemüht, auch zu einer datenschutzgerechten Durchführung des Verfahrens in der Praxis beizutragen.

3.4 Gesetz über den Auswärtigen Dienst

Das am 1. Januar 1991 in Kraft getretene Gesetz über den Auswärtigen Dienst geht in seinem § 2 davon aus, daß das Auswärtige Amt (Zentrale) und die Auslandsvertretungen „zusammen eine einheitliche Bundesbehörde unter Leitung des Bundesministers des Auswärtigen bilden". Wenn ich bei der Vorbereitung des Gesetzentwurfs auch erst spät beteiligt wurde, so habe ich im Auswärtigen Amt doch Verständnis dafür erreichen können, daß die Einführung des unter haushaltsrechtlichen und personalrechtlichen Gesichtspunkten verfolgten Prinzips der „ministeriellen Einheit" von Auslandsvertretungen und Zentrale nicht zu einer Minderung des Datenschutzes führen darf. Eine unmodifizierte Einführung des Grundsatzes der organisatorischen Einheit von Auslandsvertretungen und Zentrale hätte bedeutet, daß die Weitergabe personenbezogener Informationen zwischen der Zentrale und den Auslandsvertretungen sowie zwischen den letzteren nicht als Datenübermittlung im Sinne des Bundesdatenschutzgesetzes zu beurteilen gewesen wäre. Die Folge wäre gewesen, daß das datenschutzrechtliche Gebot der Erforderlichkeit als Voraussetzung für die Übermittlung personenbezogener Informationen zwischen den genannten Stellen nicht gegolten hätte.

Mit Unterstützung des Auswärtigen Amtes habe ich in den parlamentarischen Beratungen die Einfügung eines besonderen Paragraphen über den Datenschutz (§ 34) erreichen können, der festlegt, daß bei Anwendung datenschutzrechtlicher Vorschriften „das Auswärtige Amt (Zentrale) und die einzelnen Auslandsvertretungen als selbständige öffentliche Stellen im Sinne des Bundesdatenschutzgesetzes" gelten. Damit ist sichergestellt, daß die organisatorische Neuregelung des Auswärtigen Dienstes den Datenschutz in diesem Bereich nicht beeinträchtigt.

4 Rechtswesen

4.1 Bundesratsentwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität

Zu den Rechtsetzungsvorhaben, die im zurückliegenden Jahr — mit Recht — in der Öffentlichkeit ein hohes Maß an Aufmerksamkeit gefunden haben, zählt der vom Bundesrat beschlossene Entwurf eines Gesetzes zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG — BR-Drucksache 74/90 Beschluß, BT-Drucksache 11/7663 —).

Ohne Frage machen die zunehmenden Herausforderungen, denen die Bürger unseres Staates durch die organisierte Kriminalität, insbesondere durch die Drogenkriminalität, ausgesetzt sind, besondere Maßnahmen — und dies bedeutet unter Gesichtspunkten der Erforderlichkeit im überwiegenden Allgemeininteresse auch besondere Eingriffe in die Freiheitsrechte der Bürger — notwendig. Der Datenschutz stellt sich also nicht etwa Bemühungen entgegen, die notwendigen Vorschriften zur Bekämpfung des illegalen Rauschgifthandels und der Organisierten Kriminalität zu schaffen. Mir liegt sehr daran, dies im Hinblick auf gerade in jüngster Zeit gegen Datenschutzbeauftragte erhobene unberechtigte Vorwürfe klarzustellen (vgl. auch 1.1.9). Der Gesetzentwurf hat sich aber besonders bei den vorgesehenen Änderungen der Strafprozeßordnung und des Fernmeldeanlagengesetzes nicht auf Maßnahmen zur Bekämpfung bestimmter Typen von Straftaten beschränkt. Während die Überschrift des Gesetzentwurfes nahelegte, daß es dabei um besondere Eingriffsbefugnisse zur Bekämpfung von Rauschgift- und sonstiger organisierter Kriminalität ging, fehlte es bei Vorschriften, die Eingriffsbefugnisse mit besonderer Eingriffstiefe gewähren sollten, an entsprechenden Begrenzungen.

Als Anknüpfungspunkt für besondere Eingriffsmaßnahmen, die — vor allem wegen der damit notwendig verbundenen Einbeziehung Nicht-Verdächtiger — als Einsatzmittel nur in dem zwingend erforderlichen Umfang akzeptiert werden können, bediente sich der BR-Entwurf durchweg des Begriffs der „Straftat von erheblicher Bedeutung". Damit wurden — nach der Begründung des Gesetzentwurfs — nicht nur Straftaten der schweren, sondern auch der mittleren Kriminalität einbezogen. Die Anwendung der besonderen Befugnisse wäre mit einiger Sicherheit allenfalls bei Bagatell- und Kleinkriminalität nicht in Betracht gekommen.

Wogegen ich mich zusammen mit Kollegen in den Ländern (vgl. die als Anlage 5 abgedruckte Entschließung) wende, ist, daß unter dem Deckmantel der Bekämpfung der Rauschgiftkriminalität und der organisierten Kriminalität in das Strafverfahrensrecht weit über die Bekämpfung solcher Straftaten hinaus neue Ermittlungsmethoden eingeführt werden, die tief in die Privatsphäre auch unverdächtiger und unbeteiligter Bürger eingreifen, ohne daß dabei die sich aus der gebotenen Abwägung zwischen den Belangen der Allgemeinheit und den Grundrechten der Bürger er-

gebenden notwendigen Differenzierungen vorgenommen werden. Einige Beispiele können dies verdeutlichen:

- Während — wenn auch über Rauschgiftdelikte und Delikte der Organisierten Kriminalität weit hinausgehend — der vom Bundesminister der Justiz vorbereitete Entwurf des Strafverfahrensänderungsgesetzes 1989 bei der Rasterfahndung (§ 98a StPO) eine Begrenzung durch einen Straftatenkatalog vorsah, wurde der Versuch einer Begrenzung auf bestimmte Deliktsarten oder -formen im Bundesrats-Entwurf völlig aufgegeben.
- Noch weiter ging (in dem vorgesehenen § 100c StPO) der Gesetzentwurf hinsichtlich der Herstellung von Lichtbildern und Bildaufzeichnungen sowie des Einsatzes besonderer Sichthilfen: Wegen jeder — auch der kleinsten — Straftat, die nicht das Mindeste mit der Rauschgiftkriminalität oder mit Organisierter Kriminalität zu tun zu haben brauchte, wäre es nach dem Entwurf zulässig gewesen, unter Zuhilfenahme von Infrarotgeräten selbst in der Nachtzeit die Bürger bis hinein in ihre Wohnungen zu beobachten.
- Auch in bezug auf die Gefahrenabwehr schoß der Gesetzentwurf des Bundesrates über das gesteckte Ziel deutlich hinaus, indem er durch Änderung des Fernmeldeanlagengesetzes (Einfügung eines neuen § 12a) eine Überwachung und Aufzeichnung des Fernmeldeverkehrs selbst dann zuließ, wenn dies zur Abwehr einer gegenwärtigen Gefahr „für Leben, Leib oder Freiheit einer Person erforderlich ist". Damit hätte — um es an einem Beispiel anschaulich zu machen — das Fernmeldegeheimnis schon dann durchbrochen werden können, wenn es darum gegangen wäre, auch nur eine leichte — selbst fahrlässige — Körperverletzung zu verhindern.

In der am 27. Juni 1990 gefaßten Entschließung (vgl. Anlage 5) hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder gegen die Stimme des Datenschutzbeauftragten Bayerns und bei Abwesenheit der Datenschutzkommission Rheinland-Pfalz insgesamt zu dem Entwurf Stellung genommen und dabei schwerwiegende datenschutzrechtliche Bedenken gegen die vorgesehene globale Ausweitung der polizeilichen Ermittlungsbefugnisse in der Strafprozeßordnung erhoben. Der damalige Vorsitzende der Innenministerkonferenz ließ — wahrscheinlich ohne den Wortlaut der Entschließung vom gleichen Tage überhaupt zu kennen — aus diesem Anlaß eine Pressemitteilung verteilen, in der u. a. erklärt wurde: „Wie viele Kinder und Jugendliche müssen noch den Drogentod sterben, bis die ‚hohen Datenschützer' das Elend der Drogensucht und das mörderische Tun der Drogendealer wahrnehmen?" Dabei ist in dem Beschluß kein Wort enthalten, das sich gegen eine Verbesserung der Bekämpfung der Rauschgiftkriminalität richtet. Ich habe die Vorwürfe nachdrücklich zurückgewiesen und meiner Hoffnung Ausdruck verliehen, daß es über die wichtigen Fragen, die der Gesetzentwurf aufwirft, zu einer sachlichen und fairen Diskussion kommen wird.

Die Bundesregierung hat in ihrer Gegenäußerung zum Gesetzentwurf des Bundesrates darauf hingewiesen, „daß einzelne Vorschläge unter verfassungsrechtlichen und datenschutzrechtlichen Gesichtspunkten nicht unproblematisch erscheinen und näherer Prüfung bedürfen". Dies gelte namentlich für die vorgesehenen Regelungen der Rasterfahndung und des Einsatzes Verdeckter Ermittler. Prüfungsbedarf bestehe insbesondere, soweit die Rasterfahndung und die polizeiliche Beobachtung keiner oder nur einer eingeschränkten richterlichen Kontrolle oder richterlichen Anordnungskompetenz unterstellt sind. Darüber hinaus fehlten — so hat die Bundesregierung bemängelt — „bei einzelnen Vorschriften Übermittlungs- und Verwendungsbegrenzungen sowie Subsidiaritätsregelungen". Die Bundesregierung hat ihre Stellungnahme mit den Worten zusammengefaßt, sie halte „eine ins einzelne gehende Prüfung im weiteren Gesetzgebungsverfahren für notwendig".

Die Bundesregierung hat schließlich darauf hingewiesen, daß auch für die Bereiche der Fahndung nach Beschuldigten und Zeugen, die längerfristige Observation, die Akteneinsicht sowie die Verarbeitung personenbezogener Daten in Dateien und deren Nutzung, die in dem Gesetzentwurf des Bundesrates nicht geregelt waren, Regelungsbedarf besteht.

Ich sehe hierin eine weitgehende Übereinstimmung mit meinen Empfehlungen, die Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, zu beschleunigen. Hierzu habe ich — wie auch meine Kollegen in den Ländern — wiederholt konkrete Vorschläge vorgelegt (vgl. 11. TB S. 20, 12. TB S. 25 nebst Anlage 3 S. 102f.). Auf die Dringlichkeit, für die Bürger wie auch für die Strafverfolgungsbehörden möglichst bald Klarheit über die bei der Strafverfolgung zulässigen Verfahren und Methoden zu schaffen, weise ich erneut hin.

4.2 Genomanalyse im Strafverfahren

Schon in meinem 11. und 12. Tätigkeitsbericht habe ich auf die Dringlichkeit hingewiesen, für die Anwendung der Genomanalyse im gerichtlichen Verfahren alsbald Rechtsnormen zu schaffen, die die Praxis steuern, damit die Praxis nicht gezwungen ist, sich selbst zu helfen, und den Gesetzgeber vor vollendete Tatsachen stellt. Meine Befürchtungen haben sich leider bestätigt. Die Rechtsprechung hat inzwischen die Verwendung der Genomanalyse im Strafverfahren und im Abstammungsverfahren nicht nur zugelassen, sondern hält deren Anwendung u. U. sogar für geboten. So hat der Bundesgerichtshof z. B. ein Urteil aufgehoben, weil ein Gericht den von der Verteidigung gestellten Antrag auf Vornahme einer Genomanalyse abgelehnt hatte. Damit ist genau das eingetreten, was Anlaß zu meiner Sorge und meiner Mahnung an den Gesetzgeber war: Die Genomanalyse ist Praxis, die erforderlichen gesetzlichen Regelungen zur Verhinderung der sich daraus für die Bürger ergebenden Risiken aber fehlen. Deshalb weise ich noch einmal darauf hin, daß Regelungen über die Anwendung der Genomanalyse im Strafverfahren vordringlich sind. Ich akzeptiere grundsätzlich die Anwendung der Genomanalyse im Strafverfahren, weil sie geeignet ist,

zur Wahrheitsfindung und damit zu mehr Gerechtigkeit beizutragen. Es kommt entscheidend darauf an, die mit Hilfe der Genomanalyse mögliche Eingriffstiefe in das informationelle Selbstbestimmungsrecht der Bürger auf das erforderliche Maß zu beschränken, eine strenge Zweckbindung der so erhobenen Daten zu gewährleisten und Sicherungen zur Vermeidung von Fehlern und zur Verhinderung von Mißbrauch in diesem empfindlichen Bereich vorzuschreiben.

Der vom Bundesminister der Justiz Anfang 1990 vorgelegte erste Diskussionsentwurf einer gesetzlichen Regelung der Genomanalyse im Strafverfahren weist in diese Richtung. Im Mittelpunkt des Entwurfs steht die sogenannte *Identitätsfeststellung*: Der Entwurf sieht die gentechnische Untersuchung von Spurenmaterial und Körperzellen des Beschuldigten vor, um festzustellen, „ob aufgefundenes Spurenmaterial von dem Beschuldigten stammt". Bei dieser Analyse geht es also um die Vergleichsuntersuchung zweier Zellproben zur Feststellung ihrer Identität oder Nichtidentität. Andere Feststellungen über die Person des Beschuldigten dürfen nicht getroffen werden. Um dies sicherzustellen, sagt der Entwurf: „Die Untersuchung darf sich nicht auf die Bereiche des menschlichen Genoms erstrecken, die Aufschluß über Erbanlagen, Krankheiten, Krankheitsanlagen oder sonstige persönliche Merkmale des Beschuldigten geben können".

Der Entwurf läßt zu, andere Personen, die nicht Beschuldigte sind, zu einer solchen Identitätsfeststellung heranzuziehen, „wenn dies zur Erforschung der Wahrheit unerläßlich ist". In der Tat kann es zur Wahrheitsfindung im Einzelfalle von Bedeutung sein, ob eine Blutspur nicht vom Beschuldigten, sondern z. B. vom Opfer der Straftat stammt. Gleichwohl eröffnet eine solche Regelung auch Problemfelder. Soll es zum Beispiel möglich sein, die Genomanalyse an einer gesamten Bevölkerungsgruppe — bei einem Sexualdelikt etwa an allen Männern eines bestimmten Alters in einer bestimmten Gegend — vorzunehmen, um den dort vermuteten Straftäter zu ermitteln, wie dies in Großbritannien in einem Strafverfahren geschehen sein soll?

Ein interessanter und problematischer Punkt des Diskussionsentwurfs ist, daß er auch eine gentechnische Untersuchung in Bezug auf *„äußerlich sichtbare Körpermerkmale"* zuläßt. Der Bundesminister der Justiz hat diese Regelung im Hinblick auf erwartete künftige Entwicklungen der Genomanalyse vorgesehen, obwohl es nach meinen Informationen bisher keine zuverlässige Untersuchungsmethode zur zweifelsfreien Feststellung solcher Merkmale gibt. Zweck einer solchen Untersuchung soll sein, äußerlich sichtbare Körpermerkmale, wie z. B. Hautfarbe, Augenfarbe und Größe der Person, von der die Spur stammt, festzustellen, um den Kreis der als Täter in Betracht kommenden Personen einzugrenzen und — z. B. in Kombination mit Aussagen von Zeugen — auf der Basis der genomanalytischen Erkenntnisse eine Fahndung einzuleiten. Die gentechnische Erhebung solcher Merkmale für Fahndungszwecke wirft besondere und grundsätzliche Probleme auf:

— Wenn es zuverlässige Untersuchungsmethoden zur Erreichung dieses Zieles nicht gibt, ist es unmöglich, solche zur Vermeidung von Fehlern vorzuschreiben und die jeweils notwendigen Sicherungsmaßnahmen vorzusehen.

— Wenn — wie vorstehend dargestellt — gewährleistet sein soll, daß eine Gewinnung von Erkenntnissen über *Krankheiten* oder sonstige persönliche Merkmale ausgeschlossen werden soll, so fragt sich, wo die *Grenzlinie* zu den „äußerlich sichtbaren Körpermerkmalen" liegt. Gibt es nicht viele Krankheiten, die sich in äußerlich sichtbaren Körpermerkmalen manifestieren? Zählen zu den „äußerlich sichtbaren Körpermerkmalen" auch äußerlich sichtbare körperliche Funktionsstörungen oder Verhaltensweisen? Dieses Problem ließe sich allerdings dadurch lösen, daß man die mit Hilfe der Genomanalyse zu ermittelnden äußerlichen Merkmale ausdrücklich und abschließend im Gesetz nennt.

— Ein gewichtiges Problem liegt außerdem darin, daß nach den mir bislang vorliegenden Erkenntnissen das Untersuchungsinstrumentarium, das für eine Feststellung von äußerlich sichtbaren Körpermerkmalen in Betracht kommt, ein erheblich höheres Risiko in sich birgt, zugleich Informationen über Krankheiten, Erbanlagen und andere Eigenschaften der untersuchten Personen zu liefern, als dies bisher bei der Identitätsfeststellung der Fall ist. Der Schritt vom Unbedenklichen zum Bedenklichen wäre hier wahrscheinlich sehr klein und mit den in Betracht kommenden Untersuchungsmethoden leicht zu tun.

Weiterer Diskussion bedürfen auch die Sicherungen, die unter Gesichtspunkten des Datenschutzes bei Anordnung und Durchführung der Genomanalyse im Strafverfahren vorzusehen sind. Ich habe u. a. empfohlen, den Entwurf durch eine Ermächtigung zu ergänzen, mit der der Bundesregierung oder dem Bundesminister der Justiz auferlegt wird, die als zulässig anerkannten *gentechnischen Methoden* zu benennen, aus denen die anordnende Stelle im Rahmen der Anordnung auszuwählen hat. Daß dies eine Frage von durchaus praktischer Bedeutung ist, zeigen Presseberichte aus den Vereinigten Staaten, wonach bei Genomanalysen eindeutige Fehldiagnosen festgestellt worden sind.

Eine andere wichtige Frage ist, *wer* Genomanalysen durchführen soll. Mit der Feststellung, daß mit gentechnischen Untersuchungen nur „Amtsträger oder öffentlich bestellte Sachverständige" beauftragt werden dürfen, sucht der Entwurf dem datenschutzrechtlichen Anliegen entgegenzukommen, nur *Institute* zu betrauen, die unter Kriterien der *Zuverlässigkeit* zugelassen sind. Dies wird teilweise nicht als ausreichend angesehen und eine funktionelle Trennung von Strafverfolgung und Genomanalyse gefordert. Ein Kompromiß in dieser Frage könnte darin bestehen, daß Amtsträger oder Sachverständige der mit den Ermittlungen beauftragten Behörde nicht mit der Untersuchung beauftragt werden dürfen. Dies ließe es zu, die Genomanalyse durch ein Labor einer anderen Strafverfolgungsbehörde durchführen zu lassen.

Es ist notwendig, die erforderlichen *„technischen und organisatorischen Einrichtungen und Maßnahmen"*

möglichst durch Rechtsvorschrift zu regeln und nicht — wie dies der Entwurf vorsieht — allein den untersuchenden Amtsträgern und Sachverständigen zu überlassen. Ich habe empfohlen, durch eine entsprechende Ermächtigung vorzusehen, daß die Bundesregierung oder der Bundesminister der Justiz durch Rechtsverordnung einen Mindeststandard solcher Einrichtungen und Maßnahmen bestimmt. Hierzu sollte auch eine normative Festlegung zählen, daß die Untersuchungsstellen Zellproben nur unter einer *Code-Nummer* erhalten, also ohne den Namen des Betroffenen, das Aktenzeichen des Strafverfahrens oder den Tatvorwurf zu erfahren.

Der Diskussionsentwurf sieht vor, daß die Anordnung einer Genomanalyse grundsätzlich nur durch einen Richter erfolgen darf. Auch hier sind aber noch Detailfragen offen, nämlich in welchem Umfang als Ausnahme hiervon in dringenden Fällen eine Anordnung der Staatsanwaltschaft zugelassen werden soll und wie das Verfahren in solchen Fällen zu regeln ist.

Weiterer Diskussionsbedarf besteht auch in den Fragen zulässiger Verwendung der durch Genomanalyse gewonnenen Daten und deren Aufbewahrung und Vernichtung. Grundsätzlich muß die Nutzung der im Rahmen eines Strafverfahrens erhobenen genomanalytischen Daten auf dieses Verfahren beschränkt werden. In diesem Zusammenhang entsteht die Frage, ob, unter welchen Voraussetzungen und für welche Zeit es zulässig sein soll, genomanalytische Daten in einer Datenbank zu speichern, und damit für andere strafrechtliche Ermittlungsfälle bereitzuhalten. Eine solche Speicherung ist nach Presseberichten im amerikanischen Bundesstaat Kalifornien für Straftaten der Schwerkriminalität vorgesehen.

Ich empfehle dringend, daß der Gesetzgeber in der laufenden Legislaturperiode die unter Gesichtspunkten des Datenschutzes unerläßlichen Regelungen über den Einsatz der Genomanalyse im Strafverfahren schafft.

5 Bauwesen

5.1 Bundesministerium für Raumordnung, Bauwesen und Städtebau

Gegenstand einer datenschutzrechtlichen Kontrolle im Bundesministerium für Raumordnung, Bauwesen und Städtebau war der Umgang mit personenbezogenen Daten in diesem Hause sowie die dort stattfindende automatisierte Datenverarbeitung. Dabei habe ich Mängel feststellen müssen.

In der Personalabteilung des Ministeriums war der Umgang mit Personalakten und sonstigen personenbezogenen Unterlagen nicht zufriedenstellend; deren Verwahrung war nicht immer so sorgfältig, daß ein Zugang Dritter ausgeschlossen war. Ferner fehlte eine klare Organisation des Datenschutzes, insbesondere eine ausreichende Regelung über die Nutzung der Datenverarbeitungssysteme. Beide Mängel habe ich gemäß § 20 BDSG beanstandet.

Weiterhin habe ich festgestellt, daß einige der im Ministerium geführten Dateien mit personenbezogenen Daten überhaupt nicht oder erst vor kurzem zur internen Übersicht des Hauses gemäß § 15 Satz 2 Nr. 1 BDSG und verschiedene automatisierte Dateien nicht zu dem von mir nach § 19 Abs. 4 BDSG geführten Register gemeldet worden waren. Dies habe ich ebenfalls nach § 20 BDSG beanstandet.

Für sehr bedenklich habe ich gehalten, daß der interne Datenschutzbeauftragte in Personalunion die Funktion als Geheimschutzbeauftragter wahrnimmt und zugleich für die Bearbeitung von Beihilfe-Angelegenheiten zuständig ist. § 5 Abs. 4 der Sicherheitsrichtlinien vom 11. November 1987 (GMBl. 1988 S. 70) fordert eine strikte Trennung von Personalverwaltung und personellem Geheimschutz. Da die Bearbeitung von Beihilfeanträgen zur Personalverwaltung gehört, war die Wahrnehmung dieser Aufgabe durch den Geheimschutzbeauftragten nicht zulässig. Eine organisatorische Trennung der Funktionen des Datenschutzbeauftragten und des Geheimschutzbeauftragten wird bisher nicht ausdrücklich in Rechts- oder Verwaltungsvorschriften gefordert. Die gleichzeitige Wahrnehmung der Funktionen als Datenschutz- und Geheimschutzbeauftragter kann aber Anlaß zu Mißdeutungen geben, wie in den vom BMI herausgegebenen Erläuterungen zu § 5 Abs. 1 der Sicherheitsrichtlinien mit Recht betont wird. Sie sollte deshalb vermieden werden. Daher habe ich empfohlen, die Funktion des Geheimschutzbeauftragten und des Datenschutzbeauftragten verschiedenen Organisationseinheiten zu übertragen.

Aufgrund einer Petition galt mein besonderes Interesse der Führung der Adreßdatei des Ministeriums. Ich konnte feststellen, daß aus dem Ministerium in einem Fall Adressen in datenschutzrechtlich unzulässiger Weise an die Landesgeschäftsstelle einer Partei übermittelt worden waren. Ich habe von einer förmlichen Beanstandung nur deshalb abgesehen, weil das Ministerium den Verstoß eingeräumt und zugesagt hat, den Umgang mit der Adreßdatei in einer Dienstanweisung so zu regeln, daß die Wiederholung eines solchen Falles ausgeschlossen ist.

Im Zusammenhang mit der Kontrolle habe ich auch die Datenverarbeitung beim Betrieb der Telefonanlage des Ministeriums überprüft. Dabei habe ich festgestellt, daß die entsprechenden Regelungen in der Geschäftsordnung des Ministeriums lückenhaft sind. Die automatisch in einen APC übertragenen Daten der Telefongespräche werden mittels eines besonderen Programmpaketes ausgewertet. Dieses ermöglicht dem Systemverwalter — möglicherweise auch dem Wartungstechniker —, die gespeicherten Daten, wie z. B. die Nummern der Kurzwahlziele für jeden Anschluß, zu lesen. Darüber hinaus können aus den Verbindungsdaten Aussagen über das Telefonierverhalten gewonnen werden. Die vorgelegte Dokumentation über die Auswertungsmöglichkeiten, die das Programm zuläßt, war veraltet und unvollständig.

In seiner Stellungnahme hat das Ministerium die von mir kritisierten Mängel weitgehend eingeräumt. Es hat mitgeteilt, die datenschutzrechtlichen Defizite seien zum Teil bereits behoben, eine umfassende Dienstanweisung zum Datenschutz und zur Datensicherheit werde vorbereitet.

5.2 Abbau von Fehlsubventionierung im Wohnungswesen

Nach dem Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen (AFWoG) haben Inhaber öffentlich geförderter Mietwohnungen eine Ausgleichszahlung zu leisten, wenn das Einkommen eine bestimmte Grenze übersteigt (und zusätzliche Voraussetzungen hinzutreten). Maßgebend ist dabei — mit gewissen Ausnahmen — das Gesamteinkommen aller Personen, die die Wohnung nicht nur vorübergehend benutzen. Bestimmungen darüber, wie die zuständige Behörde sich die Information über dieses maßgebende Einkommen verschaffen kann, enthält § 5 des Gesetzes. Die Vorschrift ist unter einigen Gesichtspunkten problematisch.

Zum einen sieht sie vor, daß die Verwaltung die Information auch über die mitzurechnenden Einkommen der Hausgenossen durch den Wohnungsinhaber bezieht, dem hierzu seinerseits ein Auskunftsanspruch gegenüber seinen Mitbewohnern eingeräumt ist. Für die Zwecke des Gesetzes ist es jedoch keineswegs erforderlich, daß der Wohnungsinhaber Kenntnis über das Einkommen seiner Mitbewohner erhält. Die Gesetzesbegründung geht davon aus, daß die Verpflichtung zum Nachweis des Einkommens der im Haushalt lebenden Personen auch dadurch erfüllt werden kann, daß der Wohnungsinhaber von den Mitbewohnern einen verschlossenen Umschlag mit den erforderlichen Angaben zur Weitergabe an die zuständige Behörde erhält. Eine solche Verfahrensmöglichkeit ist datenschutzrechtlich geboten. Sie sollte auch im Gesetz selbst zum Ausdruck gelangen.

Zum anderen ist für die datenschutzrechtliche Ausgestaltung des Verfahrens bedeutsam, daß die Abschöpfung von Fehlsubventionierungen beim Mieter der Sache nach die Rückerstattung einer fehlgeleiteten staatlichen Transferleistung bezweckt. Die staatliche Förderung des sozialen Wohnungsbaus ermöglicht die gesetzliche Beschränkung des Mietzinses auf die Kostenmiete, so daß die aufgewendeten Mittel letztlich dem Mieter zugute kommen. Ist der begünstigte Mieter im konkreten Fall nicht bedürftig, so wird die — fehlgeleitete — Subvention von ihm durch die Fehlbelegungsabgabe zurückverlangt. Dieser Sachverhalt ist sehr ähnlich dem, daß unberechtigt erlangtes Wohngeld zurückzuerstatten ist, denn derselbe Lebensbereich der Betroffenen wird in sehr ähnlicher Weise berührt. Die rechtstechnisch unterschiedliche Ausgestaltung des Weges der Zuwendung ist dabei kein sachlicher Grund, das Verfahren einer etwaigen oder auch tatsächlichen Rückabbwicklung datenschutzrechtlich unterschiedlich zu gestalten. Da im Wohngeldrückerstattungsverfahren, das nach den Bestimmungen des Sozialgesetzbuches erfolgt, der hohe Datenschutzstandard des Sozialgeheimnisses gilt, liegt es nahe, die Geltung des Sozialgeheimnisses auch für das Verfahren nach dem AFWoG vorzusehen. Die Nähe zum Wohngeldverfahren wird insbesondere in den Fällen deutlich, in denen als Ergebnis des Verfahrens festzustellen ist, daß keine Fehlbelegungsabgabe zu zahlen ist.

Beim Bundesverwaltungsgericht ist derzeit ein Revisionsverfahren anhängig, das auch Fragen des Datenschutzes im Zusammenhang mit dem AFWoG berührt. Die von mir angesprochenen Datenschutzfragen könnten aber unabhängig davon geregelt werden. Es ist daher — entgegen der Ansicht des BMBau — nicht erforderlich, zu deren sachgerechter Regelung das Urteil des Bundesverwaltungsgerichts abzuwarten.

6 Öffentlich-rechtliche Unternehmen

— *Tonbandaufzeichnung aller Kundenanrufe durch ein Versicherungsunternehmen* —

Ein meiner Kontrolle unterliegendes öffentlich-rechtliches Versicherungsunternehmen hat einen telefonischen Kundendienst eingerichtet, dessen Mitarbeiter die eingehenden Telefongespräche weitgehend ohne Wartezeiten für die Kunden selbst abwickeln können. Dies wird dadurch erreicht, daß dieser Kundendienst mit Fachkräften (Versicherungskaufleuten, Versicherungsfachwirten) besetzt ist, die die Fragen der Kunden in großem Umfang selbst beantworten können, ohne daß es der Weiterleitung zu anderen Sachbearbeitern bedarf. Um die Möglichkeit zu schaffen, das eigene Gespräch zu kontrollieren und die Gesprächsführung ständig zu verbessern, wurden alle Kundenanrufe auf Tonband aufgezeichnet.

Das Versicherungsunternehmen bewertete die Aufzeichnung der Telefongespräche angesichts der schnellen Entwicklung im technischen Bereich als im Wirtschafts- und Geschäftsverkehr üblich. Darüber hinaus will es von einer mutmaßlichen Einwilligung der Kunden ausgegangen sein, weil die Tonbandaufzeichnungen nahezu ausschließlich im Interesse einer Verbesserung des Kundendienstes und damit auch im Interesse der Kunden gelegen hätten.

Ich habe das Aufzeichnen der Kundenanrufe sowie die Verwertung der Tonbandaufzeichnungen zur eigenen Gesprächskontrolle der Mitarbeiter des telefonischen Kundendienstes sowie zur Verbesserung ihres Telefonierens gemäß § 20 BDSG förmlich beanstandet.

Für mündliche Äußerungen, insbesondere auch in einem Telefongespräch, ist charakteristisch, daß sie im Bewußtsein der Flüchtigkeit des gesprochenen Wortes und seiner jederzeitigen Korrigierbarkeit gemacht werden. Das gilt nicht nur für private telefonische Besprechungen, sondern auch für Telefonate über geschäftliche Angelegenheiten. Die Fixierung und Konservierung auch eines sich nur mit geschäftlichen Dingen befassenden Telefongesprächs in einer Tonbandaufnahme greift angesichts der damit bewirkten Verfestigung der aus der Spontaneität heraus formulierten Gedanken mit der Möglichkeit ihrer jederzeitigen Abrufbarkeit und Wiederholbarkeit intensiv in das Recht auf Selbstbestimmung des Betroffenen über sein nichtöffentlich gesprochenes Wort ein. Diese grundsätzliche Bewertung wird durch die Strafvorschrift des § 201 Abs. 1 Nr. 1 und Nr. 2 StGB bestätigt.

Eine Befugnis für die Tonbandaufzeichnungen und deren anschließende Verwertung war nicht gegeben. Sie ergab sich insbesondere nicht daraus, daß es sich

bei den aufgezeichneten Gesprächen um solche im Geschäftsverkehr gehandelt hat. Bei den Telefongesprächen zwischen den Kunden und den Mitarbeitern des telefonischen Kundendienstes eines Versicherungsunternehmens handelt es sich keineswegs nur um einfache Durchsagen oder eine Übermittlung von Daten, die von der persönlichen Sphäre des Versicherungskunden völlig losgelöst sind. In diesen Gesprächen werden vielmehr jeweils vom Kunden individuell auch persönliche Dinge dargelegt, wobei er damit in der Regel zugleich einen Teil seiner Persönlichkeit — z. B. seine eigene Geschicklichkeit beim Telefonieren oder auch seine Unbeholfenheit — preisgibt.

Ebensowenig kann in solchen Fällen von einer Befugnis zur Aufzeichnung und Verwertung der Kundenanrufe für Zwecke der Selbstkontrolle der Mitarbeiter der Versicherung aufgrund mutmaßlicher Einwilligung der Betroffenen ausgegangen werden. Die gute Qualität des telefonischen Kundendienstes des Versicherungsunternehmens liegt zwar durchaus auch im Interesse der Kunden. Man kann deshalb jedoch nicht unterstellen, daß die Kunden auch bereit sind, der Tonbandaufzeichnung ihrer Anrufe zuzustimmen.

Das Versicherungsunternehmen hat die beanstandeten Tonbandaufzeichnungen eingestellt.

Die dargelegte Unzulässigkeit der Aufzeichnung aller Kundenanrufe auf Tonband schließt nicht aus — und darauf möchte ich zur Klarstellung hinweisen —, daß im Einzelfall unter dem Aspekt der Notwehr z. B. bei erpresserischen Bombendrohungen die Befugnis zur Aufzeichnung telefonischer Anrufe durchaus gegeben sein kann. Dies rechtfertigt aber nicht, unterschiedslos und ohne entsprechenden konkreten Anlaß Gespräche aufzuzeichnen, die mit einem telefonischen Kundendienst geführt werden.

7 Personalwesen

7.1 Entwurf eines Gesetzes zur Neuordnung des Personalaktenrechts

In meinem 11. Tätigkeitsbericht hatte ich den Stand der Vorarbeiten für die Gesetzgebung zum Personalaktenrecht der Beamten und Soldaten dargestellt (vgl. S. 25). Im Berichtszeitraum hat die Bundesregierung den Entwurf eines Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften in die parlamentarische Beratung eingeführt. Obwohl der Gesetzentwurf der Bundesregierung eine Reihe erfreulicher Regelungen enthielt, habe ich mich nach intensiver Beratung mit meinen Kollegen in den Ländern veranlaßt gesehen, den Vorsitzenden des Innen- und des Verteidigungsausschusses des Deutschen Bundestages weitere Verbesserungsvorschläge zu unterbreiten. Hervorheben möchte ich in diesem Zusammenhang folgende Punkte: Um eine datenschutzrechtliche Schlechterstellung der Bundesbediensteten gegenüber zahlreichen Landesbeamten, für die es keinen sachlichen Grund gibt, zu beseitigen, habe ich vorgeschlagen, die Regelung des § 12 Abs. 4 BDSG n. F., die der des § 7 Abs. 3 des bisherigen BDSG entspricht, aufzuheben, wonach für die Datenverarbeitung im Zusammenhang mit Dienst- und Arbeitsverhältnissen an die Stelle der für den öffentlichen Bereich sonst geltenden Vorschriften die für den nicht-öffentlichen Bereich konzipierten Vorschriften des Bundesdatenschutzgesetzes gelten sollen. Meinen Vorschlag gründete ich zusätzlich auch auf die Unsicherheit in der Rechtsanwendung, die dadurch entsteht, daß die genannten Regelungen des Bundesdatenschutzgesetzes weitgehend, aber nicht vollständig, durch die beamtenrechtlichen Spezialvorschriften verdrängt werden und diese nur solche Personalaktendaten erfassen, die mit dem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen, während nach den Vorschriften des BDSG darüber hinausgehend alle Daten erfaßt werden, die für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse verarbeitet oder genutzt werden.

Im Hinblick darauf, daß § 13 BDSG n. F. den besonderen Bedürfnissen bei der Datenerhebung im Beamten- und Soldatenverhältnis nicht gerecht wird, habe ich vorgeschlagen, eine besondere Erhebungsvorschrift in das Beamtenrechtsrahmengesetz, das Bundesbeamtengesetz und das Soldatengesetz aufzunehmen, dabei den Erhebungszweck auf die Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses zu begrenzen und eine heimliche Datenerhebung mit technischen Mitteln zu verbieten. Darüber hinaus habe ich mich insbesondere für eine noch stärkere Abschottung der Beihilfebearbeitung, ein Einsichtsrecht in sog. Sachakten, die personenbezogene Personalaktendaten enthalten, sowie für die Einführung einer Pflicht zur unverzüglichen Rückgabe von Beihilfeunterlagen mit Erkrankungsdaten nach Entscheidung über den Beihilfeantrag eingesetzt.

Der Innenausschuß hat daraufhin gegenüber dem Bundesministerium des Innern angeregt, über meine Vorschläge mit dem Ziel eines Einvernehmens erneut zu verhandeln. In diesen Verhandlungen ist mir der Bundesminister des Innern gerade in den für mich sehr bedeutsamen Punkten der Einführung einer Datenerhebungsvorschrift und der Einführung eines Rechts auf Einsicht auch in Akten, die formell keine Personalakten sind (Sachakten), aber personenbezogene Daten über den Betroffenen enthalten, entgegengekommen.

Obwohl in der Absprache einige für mich wichtige Punkte nicht durchgesetzt werden konnten, habe ich es sehr bedauert, daß das Gesetz in der vergangenen Legislaturperiode nicht mehr verabschiedet worden ist. Inzwischen hat die Bundesregierung das Gesetz in der gleichen Fassung wie in der vergangenen Legislaturperiode — also ohne die im Gesetzgebungsverfahren abgesprochenen Verbesserungen — wieder eingebracht. Ich gehe davon aus, daß dies nur aus formalen Gründen geschehen ist und in der Sache weiterhin Einvernehmen über die abgesprochenen Änderungen der Regierungsvorlage besteht.

Die inzwischen weitergeführten Überlegungen haben zu der Erkenntnis geführt, daß in das Gesetz auch noch entsprechende Regelungen für Zivildienstleistende aufgenommen werden müssen.

7.2 Telefondatenverarbeitung

Einen Schwerpunkt im Bereich der automatisierten Personaldatenverarbeitung stellte auch im zurückliegenden Jahr die Speicherung und Verwendung von Daten dienstlicher und privater Telefongespräche in der Bundesverwaltung dar (vgl. hierzu u. a. 7. TB S. 19f., 10. TB S. 30f., 11. TB S. 26f., 12. TB S. 32).

Leider sind auch im Jahre 1990 die neuen *„Allgemeinen Verwaltungsvorschriften über die Einrichtung und Benutzung dienstlicher Fernmeldeanlagen für die Bundesverwaltung mit Ausnahme der Deutschen Bundespost (Dienstanschlußvorschriften — DAV —)"*, in deren Entwurf ich meine datenschutzrechtlichen Empfehlungen weitgehend einbringen konnte, nicht verabschiedet worden. Laut Auskunft des Bundesministers der Finanzen ist ein Termin dafür aus Gründen, die nicht mit dem Datenschutz in Zusammenhang stehen, auch jetzt noch nicht absehbar. Ich kann dies nur bedauern, weil die Telefondatenerfassung in der Praxis eine bedeutsame Rolle spielt und empfindliche Daten betrifft.

Der Bundesminister für Verkehr hat die Gesprächsdatenerfassung und -verarbeitung in seinem neuen Dienstgebäude neu geregelt und mich dabei beteiligt. Meinen Anregungen für eine datenschutzgerechte Telefondatenverarbeitung wurde in vollem Umfang Rechnung getragen.

Beim Bundesaufsichtsamt für das Kreditwesen hatte sich die mir zugesagte Anpassung der Fernsprechdatei an den Entwurf der neugefaßten Dienstanschlußvorschriften zunächst verzögert. Inzwischen hat mir das Bundesaufsichtsamt für das Kreditwesen jedoch zugesagt, meine Forderungen für eine datenschutzgerechte Telefondatenverarbeitung im Rahmen der Systemerweiterung ihrer Telefonanlage durch eine neue Software-Version zu erfüllen. Die mit nicht unerheblichen Kosten verbundene Softwareänderung — in der ich eine angemessene und erforderliche Maßnahme zur Gewährleistung des Datenschutzes sehe — begrüße ich ausdrücklich. Derartige Kosten lassen sich vermeiden, wenn bei Einrichtung von Telefonanlagen die Belange des Datenschutzes von vorneherein berücksichtigt werden. Ein schnelles Inkraftsetzen der neugefaßten Dienstanschlußvorschriften würde dazu entscheidend beitragen.

Die Bundesanstalt für Flugsicherung hat auf meine datenschutzrechtlichen Empfehlungen zur *Telefondatenverarbeitung* (12. TB, S. 32) auch nach erneuter Aufforderung nicht reagiert. Diese unzureichende Unterstützung bei der Erfüllung meiner Aufgaben habe ich als Verstoß gegen § 19 Abs. 3 BDSG beanstandet. Die Bundesanstalt für Flugsicherung hat mir daraufhin zugesichert, daß die Telefondatenverarbeitung künftig über eine neue Nebenstellenanlage nach den Bestimmungen des Entwurfs der Dienstanschlußvorschriften (DAV) abgewickelt wird. Die neue Telefonanlage wurde zwischenzeitlich installiert und wird z. Z. auch hinsichtlich der datenschutzrechtlichen Anforderungen programmiert. Über das weitere Verfahren werde ich mich unterrichten lassen.

7.3 Einzelfälle

— *Kontrolle beim Bundesminister der Verteidigung*

Aus Anlaß einer Eingabe habe ich im Berichtsjahr eine datenschutzrechtliche Kontrolle beim Bundesminister der Verteidigung durchgeführt, die den Umgang mit Patientenakten von Bediensteten zum Gegenstand hatte.

Die Prüfung führte unter anderem zu folgenden Feststellungen:

Schriftliche Regelungen des BMVg für den Umgang mit Patientenakten unter Berücksichtigung des Patientengeheimnisses und des Personalaktengeheimnisses, insbesondere für den Zugriff der Mitarbeiter auf diese, existieren nicht. Aus der Kartei, die in alphabetischer Reihenfolge Name, Vorname, Geburtsdatum der untersuchten Personen sowie das Jahr der letzten Bearbeitung enthält, ergab sich lediglich, daß die in der Petition angesprochene Patientenakte zuletzt im Jahre 1987 aus dem Aktenschrank genommen worden war. Weitergehende Hinweise auf den Anlaß einer späteren Entnahme, den Bearbeiter sowie den Verbleib der Akte konnten auch von den Angehörigen der zuständigen Arbeitseinheit nicht gegeben werden. Nach den getroffenen Feststellungen ist nicht auszuschließen, daß nicht nur diese, sondern auch alle anderen Patientenakten ohne weiteres von Angehörigen dieser Arbeitseinheit zur Kenntnis genommen und an einem nicht nachprüfbaren Ort aufbewahrt werden konnten.

Ich habe dringend empfohlen, schriftliche Regelungen für den referatsinternen Umgang mit Patientenakten zu schaffen. Diese sollten insbesondere die Zugriffsrechte der Angehörigen der Arbeitseinheit aufgabenbezogen regeln sowie eine Dokumentation der Einzelzugriffe dergestalt vorsehen, daß insbesondere Zeitpunkt, Bearbeiter und Anlaß der Bearbeitung nachvollziehbar und gegegebenfalls nachprüfbar sind. Personenbezogene Daten dürfen auch innerhalb einer Behörde und einer Arbeitseinheit nur den jeweils für die Bearbeitung zuständigen Mitarbeitern in dem erforderlichen (Mindest-)Umfang bekannt werden. Ich habe darauf hingewiesen, daß das nach § 203 StGB geschützte Patientengeheimnis grundsätzlich auch zwischen Ärzten gilt und Durchbrechungen nur nach Maßgabe dieser Vorschrift zulässig sind. Ein ohne jeden dienstlichen Anlaß allein aus der Vorgesetztenfunktion hergeleitetes Zugriffsrecht auf Patientenunterlagen, die von unter die ärztliche Schweigepflicht fallenden Mitarbeitern verwaltet werden, wäre damit nicht vereinbar.

Der Bundesminister der Verteidigung hat zwar bereits während der Kontrolle zugesagt, meine Empfehlung aufzugreifen, konkrete Ergebnisse lagen aber auch nach sechs Monaten noch nicht vor.

Im Verlauf der Kontrolle ergaben sich für mich darüber hinaus konkrete Anhaltspunkte für datenschutzrechtliche Mängel bei der Zusammenarbeit der geprüften Arbeitseinheit mit der Personalverwaltung. Die deswegen von meinen Mitarbeitern erbetene Einsicht in nach einem Zufallsprinzip auszuwählende Patientenakten wurde vom BMVg verweigert, worauf-

hin ich die Kontrolle zunächst unterbrochen habe. Auch die daraufhin getroffene Vereinbarung, nach der der BMVg sich um eine Einwilligung von mir bestimmter Beschäftigter in die Einsichtnahme ihrer Gesundheit- und Personalakten durch meine Mitarbeiter bemühen wollte, kam dieser trotz mehrfacher Erinnerungen weder innerhalb der vereinbarten Frist noch nach deren Ablauf nach.

Ich habe dieses Verhalten des BMVg als Verstoß gegen die Bestimmung des § 19 Abs. 3 Satz 1 BDSG, der die in Absatz 1 Satz 1 genannten Behörden und sonstigen Stellen verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben u. a. durch Auskünfte und Akteneinsicht zu unterstützen, gemäß § 20 BDSG beanstandet.

Der BMVg hat mir daraufhin zugesagt, das abgesprochene Verfahren durchzuführen, was nach einer inzwischen eingegangenen Mitteilung auch geschehen ist.

— *Auskunftsanspruch des Personalrats über die Ergebnisse von Beurteilungsrunden*

Eine oberste Bundesbehörde bat mich um datenschutzrechtliche Stellungnahme zu der Frage, ob und gegebenenfalls in welcher Form nach Abschluß einer Beurteilungsrunde (Durchführung sämtlicher Regelbeurteilungen) ein Notenspiegel erstellt und dem Personalrat sowie allen Beurteilten zur Kenntnis gegeben werden kann.

Während es dem Personalrat der obersten Bundesbehörden auf einen nach Abteilungen und Laufbahngruppen gegliederten Notenspiegel ankam, um gegebenenfalls auf eine unterschiedliche Beurteilungspraxis hinweisen zu können, vertrat die Dienststelle die Auffassung, die Wahrung der datenschutzrechtlichen Belange der Mitarbeiter lasse eine Bekanntgabe der Ergebnisse nur in allgemeiner Form zu; insbesondere müsse angesichts der in vielen Bereichen geringen Zahl der zu beurteilenden Mitarbeiter verhindert werden, daß Beurteilungsnoten einzelner Bediensteter durch interessierte Kollegen ermittelt werden könnten.

Beurteilungsnoten unterstehen als typischer Inhalt von Personalakten dem Grundsatz des besonderen Vertrauensschutzes der Bediensteten (Personalaktengeheimnis). Bei der Bewertung der Zulässigkeit der Bekanntgabe von Beurteilungsnoten habe ich zwischen dem Personenkreis der Mitglieder des Personalrats sowie allen übrigen Bediensteten der Dienststelle unterschieden:

Die Personalvertretung hat gemäß § 68 Abs. 1 Ziff. 2 BPersVG u. a. darüber zu wachen, daß die zugunsten der Beschäftigten geltenden Verwaltungsanordnungen durchgeführt werden. Gemäß § 68 Abs. 2 BPersVG ist sie zur Durchführung ihrer Aufgaben rechtzeitig und umfassend zu unterrichten. Ihr sind die hierfür erforderlichen Unterlagen vorzulegen.

Die dem Beurteilungsverfahren zugrundeliegenden Beurteilungsrichtlinien stellen eine Verwaltungsanordnung im Sinne des § 68 Abs. 1 Ziff. 2 BPersVG dar. Eine Aufgliederung des Notenspiegels nach Abteilungen und Laufbahngruppen stellt für den Personalrat ein wesentliches Hilfsmittel zur Bewertung der Beurteilungspraxis in einer größeren Behörde unter dem Gesichtspunkt der Gleichbehandlung aller Angehörigen der Dienststelle dar. Erfahrungsgemäß bestehen teilweise Unterschiede bei den von Vorgesetzten angelegten Beurteilungsmaßstäben, die sich auf das Ergebnis der Beurteilungen der Mitarbeiter auswirken. Die Kenntnis derartiger Unterschiede kann für die Willensbildung der Personalvertretung von Bedeutung sein. Die Aufgliederung des Notenspiegels nach Abteilungen ist danach für die Aufgabenerledigung des Personalrats erforderlich. Gemäß § 10 Abs. 1 BPersVG sind die Angehörigen der Personalvertretung verpflichtet, über die ihnen bei Wahrnehmung ihrer Aufgaben nach dem BPersVG bekannt gewordenen Angelegenheiten und Tatsachen Stillschweigen zu bewahren.

Dagegen waren mir Gründe für eine nach Abteilungen aufgeschlüsselte Bekanntgabe der Ergebnisse der Beurteilungsrunde an das gesamte Personal der Dienststelle, die schwerer wiegen als die aus einer solchen Maßnahme folgenden Risiken für die beurteilten Bediensteten nicht erkennbar. Ich habe daher empfohlen, eine allgemeine Form der Bekanntgabe (z. B. Angabe der prozentualen Verteilung der einzelnen Noten in der Dienststelle insgesamt, Notenverteilung laufbahnbezogen) zu wählen.

Die oberste Bundesbehörde hat mir mitgeteilt, sie werde meinen Empfehlungen entsprechen. Darüber hinaus beabsichtigte sie, in dem nach Abteilungen und Laufbahngruppen aufgegliederten Notenspiegel an den Personalrat einzelne Bereiche zusammenzufassen, so weit die darin enthaltenen Angaben weniger als fünf Personen betreffen.

— *Auskunftsanspruch des Personalrats gegenüber dem Dienstherrn hinsichtlich der Ableistung von Mehrarbeits- und Überstunden*

Der Personalrat einer obersten Bundesbehörde beabsichtigte, sich des Problems der Anordnung von Mehrarbeit und Überstunden in bestimmten Arbeitseinheiten seiner Dienststelle besonders anzunehmen. Unter Hinweis auf seine Aufgaben, insbesondere gemäß § 67 Abs. 1, § 68 Bundespersonalvertretungsgesetz (BPersVG), verlangte er von dem Dienstherrn eine Namensliste mit dem jeweiligen Stand des Mehrarbeits-/Überstundenkontos der Mitarbeiter. Soweit dies nicht möglich sein sollte, erklärte er sich auch mit einer anonymisierten Liste der Mehrarbeits-/Überstundenkonten — unterteilt nach einzelnen Arbeitsbereichen und innerhalb der Arbeitsbereiche nach Hierarchieebenen — einverstanden.

Der Dienstherr begründete seine datenschutzrechtlichen Bedenken gegen dieses Auskunftsersuchen insbesondere mit der Bestimmung des § 68 Abs. 2 Satz 3 BPersVG, nach der Personalakten nur mit Zustimmung des Beschäftigten und nur von den von ihnen bestimmten Mitgliedern der Personalvertretung eingesehen werden dürfen. Er schlug dem Personalrat vor, das Einverständnis der Beschäftigten mit der Ein-

sicht in ihre jeweiligen Mehrarbeitsübersichten einzuholen.

In meiner Stellungnahme habe ich zum Ausdruck gebracht, daß unter Datenschutzaspekten eine Lösung, die einen möglichst hohen Anonymisierungsgrad gewährleistet, vorzuziehen ist. Um feststellen zu können, ob alle Bediensteten bei der Belastung mit Überstunden „nach Recht und Billigkeit behandelt werden" (vgl. § 67 Abs. 1 Satz 1 BPersVG) benötigt der Personalrat nach meinen Feststellungen die Kenntnis der Arbeitseinheiten und eine Aufteilung nach Hierarchieebenen, bei denen Überstunden angefallen sind. In welchem Umfang eine datenschutzfreundliche und deshalb anzustrebende Zusammenfassung von Arbeitseinheiten möglich ist, ohne die Aufgabe des Personalrats zu gefährden, muß anhand der konkreten Situation entschieden werden. Dabei ist auch ein zweistufiges Verfahren denkbar, nämlich in einer ersten Übersicht eine stärkere Zusammenfassung von Arbeitseinheiten vorzunehmen und erst dann, wenn sich daraus keine hinreichende Beurteilungsmöglichkeit für die vom Personalrat wahrzunehmende Aufgabe ergibt, bei einzelnen — zweifelhaften — Bereichen eine feinere Aufgliederung vorzunehmen. § 68 Abs. 2 Satz 3 BPersVG würde einem solchen Verfahren nicht entgegenstehen. Die Verhandlungen zwischen Personalrat und Dienstherrn dauerten bei Redaktionsschluß noch an.

— *Meldeverfahren der Bundesanstalt für Arbeit für die Krankenversicherung der Versorgungsempfänger*

Aufgrund der Eingabe eines früher bei der Bundesanstalt für Arbeit beschäftigten Petenten habe ich festgestellt, daß das für die Zahlung von Versorgungsbezügen zuständige Zentralamt der Bundesanstalt für Arbeit im Rahmen des Meldeverfahrens gemäß § 202 SGB V der Krankenkasse des Petenten nicht nur die Höhe seiner Bruttoversorgungsbezüge, sondern darüber hinaus auch deren Berechnungsgrundlage im einzelnen mitgeteilt hatte. Auf dem verwendeten Vordruck waren u. a. Angaben über die Höhe der ruhegehaltsfähigen Dienstbezüge, die Besoldungsgruppe sowie den Familienstand des Petenten vorgesehen. Diese waren für die Aufgabenerledigung der Krankenkasse nicht erforderlich. Ich habe die Übermittlung dieser Daten durch das Zentralamt als Verstoß gegen die Grundsätze des Personalaktengeheimnisses bewertet.

Die Bundesanstalt für Arbeit hat ihr Meldeverfahren für die Krankenversicherung zwischenzeitlich modifiziert. Gegen den Inhalt des neu entwickelten Vordrucks habe ich keine datenschutzrechtlichen Bedenken.

— *Einsichtnahme in ärztliche Gutachten durch Dienst- und Fachvorgesetzte*

Ein Petent beschwerte sich darüber, daß seine Dienst- und Fachvorgesetzten, u. a. der Hauptgeschäftsführer der Berufsgenossenschaft, dessen Stellvertreter, der Personalreferent sowie sein Fachvorgesetzter, Einsicht in ein dienstlich veranlaßtes nervenfachärztliches Gutachten genommen hatten. Die BG begründete die Einsicht in das komplette Gutachten mit der Notwendigkeit einer Entscheidung über die weitere berufliche Verwendung des Petenten.

Nachdem die Berufsgenossenschaft trotz von mir erhobener Bedenken ihre Verfahrensweise verteidigt hatte, habe ich die Gewährung der Einsicht in das komplette Gutachten hinsichtlich des Fachvorgesetzten als Verstoß gegen die Grundsätze des Personalaktengeheimnisses beanstandet. Der Grundsatz des Personalaktengeheimnisses gebietet dem Dienstherrn, den Kreis der mit Personalakten befaßten Beschäftigten möglichst eng begrenzt zu halten und auch Teilakten, Auszüge oder einzelne Angaben nicht ohne dienstlichen Grund anderen Beschäftigten zur Kenntnis zu geben (BVerwG in NJW 1987, S. 1214 ff.). Dabei sind sensible Daten, zu denen insbesondere solche über den Gesundheitszustand gehören, als besonders schutzbedürftig mit besonderer Vertraulichkeit zu behandeln und nur dem insoweit zuständigen Personenkreis zugänglich zu machen (BAG in RDV 1988, S. 27).

Der Fachvorgesetzte des Petenten besaß keine Personalentscheidungskompetenz. Für eine Abstimmung über den künftigen Tätigkeitsbereich des Petenten zwischen Dienst- und Fachvorgesetzten hätte eine Mitteilung der für die Verwendung des Beamten relevanten Ergebnisse des ärztlichen Gutachtens ausgereicht.

Darüber hinaus habe ich auch die Einsicht des Hauptgeschäftsführers, dessen Stellvertreters sowie des Personalreferenten in das komplette Gutachten als datenschutzrechtlich bedenklich angesehen. Unter Berücksichtigung der besonderen Sensibilität der in dem Eingabefall angesprochenen Arztgutachten wäre eine Information über die Ergebnisse der Gutachten — etwa durch den Personal- oder Vertrauensarzt — angemessener gewesen.

Die Berufsgenossenschaft hat mir inzwischen mitgeteilt, der Inhalt ärztlicher Gutachten werde künftig nach tatsächlichen Behauptungen und medizinischen Einzelbefunden getrennt. Fachvorgesetzten würden nur noch umstrittene Tatsachen (keinesfalls medizinische Einzelfeststellungen) mitgeteilt, soweit dies aus Gründen der dienstlichen Fürsorgepflicht erforderlich sei.

8 Post und Telekommunikation

Nach der Poststrukturreform obliegt die Wahrnehmung unternehmerischer und betrieblicher Aufgaben allein den drei Unternehmen (Postdienst/Postbank/Telekom) der Deutschen Bundespost. Der Bundesminister für Post und Telekommunikation (BMPT) hat nur noch politische und hoheitliche Aufgaben wahrzunehmen; er führt die Rechtsaufsicht über die Unternehmen. Diese Aufgabendifferenzierung sollte dazu führen, daß der Bundesminister gegenüber den Unternehmen eine sachlich objektive, von unternehmerischen Erwägungen unabhängige Position einnimmt.

Eine solche Haltung habe ich im Hinblick auf den Datenschutz bisher leider noch nicht durchgängig erkennen können.

8.1 Datenschutzverordnungen

Die Bundesregierung hat mittlerweile Entwürfe von Rechtsverordnungen für die Unternehmen der Deutschen Bundespost zum Schutz personenbezogener Daten der am Post- und Fernmeldeverkehr Beteiligten vorgelegt, die aufgrund der Poststrukturreform erforderlich sind (12. TB S. 36f.). Diese Datenschutzverordnungen, die zum 1. Juli 1991 in Kraft treten sollen, habe ich intensiv mit dem Bundesminister für Post und Telekommunikation, mit dem Innenauschuß und dem Ausschuß für Post und Telekommunikation des Deutschen Bundestages sowie dem Infrastrukturrat der Bundespost erörtert.

8.1.1 Deutsche Bundespost Postdienst

Bereits in meinem Elften Tätigkeitsbericht (11. TB S. 30) habe ich auf die Gefahr hingewiesen, mit dem Argument der „Gleichbehandlung" könnte der Datenschutz unter Hinweis auf die Wettbewerbssituation bei der Post auf das geringere Niveau des nicht-öffentlichen Bereichs abgebaut werden. In der Tat hat der Entwurf der vom BMPT vorgelegten Rechtsverordnung über den Datenschutz bei der Deutschen Bundespost Postdienst zunächst vorgesehen, daß in Zukunft in den Geschäftsbereichen, bei denen die Deutsche Bundespost Postdienst im Wettbewerb mit anderen Anbietern steht, nicht die Vorschriften des Zweiten Abschnitts des Bundesdatenschutzgesetzes, sondern die des Dritten Abschnitts, der den Datenschutz im nicht-öffentlichen Bereich regelt, gelten sollen.

In den Verhandlungen über den Entwurf habe ich die Auffassung vertreten, die Tätigkeit der Deutschen Bundespost Postdienst berühre die sensible Privatsphäre kommunikativer Beziehungen so eng, daß eine Absenkung des Standards des Datenschutzes, die damit verbunden wäre, abzulehnen sei. Sofern aus Wettbewerbsgründen eine einheitliche Behandlung von Konkurrenten unerläßlich sein sollte, wäre die Gleichbehandlung auf dem Niveau des im Bereich öffentlicher Stellen angemessenen Schutzes herzustellen. Im übrigen ließe sich durchaus die Frage stellen, ob ein guter Datenschutz nicht ein günstiger Wettbewerbsfaktor für die Deutsche Bundespost Postdienst wäre. Die vorgesehene Regelung hätte auch innerhalb der Deutschen Bundespost Postdienst zu unterschiedlichen Datenschutzvorschriften geführt, was zumindest in Grenzbereichen erhebliche Praktikabilitätsprobleme mit sich gebracht hätte. Unterschiedliche Regelungen über die Erhebung und Verwendung von Daten innerhalb des Unternehmens wären ein Risiko für den gesamten Datenschutz im Bereich der Deutschen Bundespost Postdienst gewesen.

Nach intensiven Beratungen hat sich der BMPT meiner Auffassung angeschlossen. Der letzte Entwurfsstand der Postdienst-Datenschutzverordnung sieht vor, daß für den Gesamtbereich der Deutschen Bundespost Postdienst auch in Zukunft die für den öffentlichen Bereich geltenden Vorschriften des Bundesdatenschutzgesetzes anzuwenden sind, soweit die Verordnung keine bereichsspezifischen Regelungen enthält. Im Interesse der Normenklarheit sind dabei die anzuwendenden Vorschriften des Bundesdatenschutzgesetzes im einzelnen aufgeführt.

Im übrigen habe ich darauf hingewiesen, daß es meine Unterstützung fände, auch bei Konkurrenten der Deutschen Bundespost Postdienst im Gesetzeswege diese Bedingungen gleichermaßen einzuführen. Das Postgesetz könnte hierzu — orientiert am Telekom-Bereich — um eine § 14a Abs. 2 des Gesetzes über Fernmeldeanlagen entsprechende Verordnungsermächtigung ergänzt werden, nach der die Bundesregierung insbesondere für Leistungen des Paketdienstes durch Private Vorschriften zum Schutz personenbezogener Daten der Beteiligten zu erlassen hätte.

Die Datenschutzverordnung wird voraussichtlich auch weitere Verbesserungen „im Anschriftenprüfungsverfahren" (12. TB, S. 45) bewirken. Künftig wird danach unterschieden, ob die bloße Mitteilung erfolgen soll, daß eine vom anfragenden Dritten angegebene — diesem also bereits bekannte — Anschrift richtig oder falsch ist, oder ob darüber hinaus die richtige Anschrift des Betroffenen mitgeteilt werden soll. Die bloße Mitteilung „richtig"/„falsch" ist immer bereits dann zulässig, wenn es Zwecken des Postverkehrs dient. Eine richtige Anschrift darf hingegen nur in zwei Fällen mitgeteilt werden:

- wenn eine Postsendung nicht unter der angegebenen Anschrift ausgeliefert werden konnte, sofern der Empfänger bei Stellung eines Nachsendungsantrages nach Hinweis auf sein Widerspruchsrechts nicht schriftlich widersprochen hat oder
- wenn der Betroffene zuvor befragt worden ist und der Mitteilung nicht widersprochen hat.

In beiden Fällen muß die Mitteilung der Anschrift wiederum Zwecken des Postverkehrs dienen.

Zur Auskunft über Postfachinhaber will der BMPT nunmehr meinen Anregungen (12. TB, S. 47) folgen. Die Anschrift des Postfachinhabers soll künftig nur dann mitgeteilt werden, wenn der Dritte ein berechtigtes Interesse an der Kenntnis im Einzelfall glaubhaft macht, das im Zusammenhang mit dem postalischen Dienstleistungsangebot steht. In jedem Falle ist jedoch ein Widerspruch des Postfachinhabers zu beachten. Auf ihr Widerspruchsrecht werden Postfachinhaber künftig ausdrücklich hingewiesen. Wichtig war mir auch sicherzustellen, daß die Ausübung des Widerspruchsrechts mit keinen belastenden Folgen verknüpft werden darf. Ursprünglich hatte der BMPT in der Verordnungsbegründung die Auffassung vertreten, aus Anlaß des Widerspruchs könnte dem Postfachinhaber gekündigt werden. Auf meinen dringenden Rat hin hat der BMPT seine Meinung geändert.

Die Erhebung von Ausweisdaten im Schalterdienst war in der Vergangenheit mehrfach Gegenstand von Bürgeranfragen an mich. Das kommende Recht wird

hierzu eine klare Regelung bringen, die die Erhebung und Speicherung auf das erforderliche Maß begrenzt, die Nutzung nur für die Beweisführung über die ordnungsgemäße Ausführung einer Dienstleistung zuläßt und anordnet, daß die Daten mit Ablauf des auf die Erhebung folgenden Kalenderjahres zu löschen sind.

8.1.2 Deutsche Bundespost Postbank

Auch für die Deutsche Bundespost Postbank stand die Frage im Raum, ob künftig die Vorschriften des Zweiten oder des Dritten Abschnitts des Bundesdatenschutzgesetzes gelten sollen (vgl. oben 8.1.1). Anders als im Postdienst-Bereich spielt das Post- und Briefgeheimnis bei der Postbank keine Rolle. Auch dem oben erwähnten Problem unterschiedlicher Datenschutzregelungen kommt bei der Deutschen Bundespost Postbank geringere Bedeutung zu als bei der Deutschen Bundespost Postdienst. Ich bin mir im klaren, daß im Bereich der Postbank der Wettbewerbsgerechtigkeit besonderes Gewicht zukommt. Auch hier sollte allerdings nicht verkannt werden, daß guter Datenschutz ein Wettbewerbsvorteil sein kann.

Unter den einzelnen bereichsspezifischen Bestimmungen der Postbank-Datenschutzverordnung ist die vorgesehene Neuregelung zu Auskünften über Kontonummer und Kontobezeichnung hervorzuheben. Künftig werden solche Auskünfte nur noch anderen in die Abwicklung eines Auftrags eingeschalteten Institutionen (wie insbesondere Geld- und Kreditinstituten) erteilt, und auch dies nur, soweit es für die Abwicklung dieses Zahlungsverkehrsauftrages erforderlich ist.

Großes Interesse hat bei mir die Initiative der SPD-Fraktion zum besseren Schutz des Privatgirokontos (Bundestagsdrucksache 11/8333) gefunden. Mit ihr wurde ein besserer Datenschutz beim Privatgirokonto, insbesondere eine Nutzungsbegrenzung der Informationen, die einer Bank aus dem Girobereich — vor allem aus dem Zahlungsverkehr zu Dritten — zugänglich sind, in die politische Diskussion gebracht. Es bleibt abzuwarten, ob in dieser Legislaturperiode eine entsprechende Initiative — gegebenenfalls unter Ausdehnung auf Konten bei anderen Geldinstituten — ergriffen wird.

8.1.3 Datenschutzverordnungen für die Telekommunikation

In meinem 12. Tätigkeitsbericht (12. TB S. 37 ff.) habe ich von den technologischen Fortschritten in der Telekommunikation berichtet, die dem Anwender größeren Nutzen und mehr Komfort, aber auch neue und verstärkte Datenschutzprobleme bringen. Die Ursache dafür liegt darin, daß — angeblich unvermeidbar — Fortschritte in der Technik der Telekommunikation stets die Speicherung von immer mehr, auch personenbezogenen, Daten und ihre immer noch längere Aufbewahrung verlangen. Gerade bei meinen Datenschutzkontrollen ist mir jedoch immer wieder deutlich geworden, daß viele personenbezogene Daten für die betreffende Aufgabe überhaupt nicht erforderlich waren und daß die getroffenen Sicherheitsvorkehrungen mit dem Sicherheitsbedarf der enorm angewachsenen Datenbestände nicht Schritt gehalten hatten.

Angesichts dieser Probleme einerseits und des ständig steigenden Bedarfs an Diensten und Einrichtungen andererseits kommt es — auch für die Sicherstellung des „Grundrechtes auf unbeobachtete Kommunikation" der Bürger — entscheidend darauf an, *jetzt* die Weichen richtig zu stellen, damit auch in der Zukunft Partner, die miteinander telefonieren, sicher sein können, daß weder der Inhalt der Verbindung noch deren nähere Umstände gegen ihren Willen bekannt werden. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen „Gesetz zur Neustrukturierung des Post- und Fernmeldewesens und der Deutschen Bundespost" (Poststrukturgesetz) die Voraussetzungen für eine sach- und grundgesetzgemäße Regelung geschaffen, indem er die Bundesregierung zum Erlaß von Rechtsverordnungen „zum Schutz personenbezogener Daten der am Post- und Fernmeldeverkehr Beteiligten" verpflichtete, und zwar sowohl für die Deutsche Bundespost TELEKOM als auch für private Anbieter von Telekommunikationsdienstleistungen. Ich habe frühzeitig und wiederholt dem Bundesminister für Post und Telekommunikation (BMPT) meine Beratung für den Entwurf der Verordnungen angeboten und konnte dabei auch auf Erfahrungen verweisen, die ich durch die Mitarbeit in verschiedenen Expertengremien aus Verwaltung, Wirtschaft und Wissenschaft gewonnen habe, so zum Beispiel in der Arbeitsgemeinschaft für wirtschaftliche Verwaltung (AWV) sowie in der Informationstechnischen Gesellschaft (ITG). Bei der Arbeit in diesen Gremien, aber auch durch zahlreiche Eingaben sowohl von Bürgern als auch von kirchlichen Einrichtungen und Verbraucherorganisationen, war deutlich geworden, welche Bedeutung die Sicherstellung einer unbeobachteten Telekommunikation besitzt und welche weit verbreiteten Befürchtungen bestehen, diese könne in Zukunft nicht mehr gewährleistet sein. Dabei wurden zwei Schwerpunkte erkennbar, die sich zunächst zwar nur auf die sogenannten ISDN-Anschlüsse beziehen (vgl. 12. TB S. 39 f.), die aber nach Meinung von Experten in Zukunft für die gesamte Telekommunikation gelten, weil erwartet werden kann, daß das „gute alte Telefon" mittel- bis langfristig vom ISDN-Anschluß völlig verdrängt und schon lange vorher die Datenverarbeitung insgesamt auf dem ISDN-Niveau angeglichen wird. Problemschwerpunkte sind:

1. Anzeige der Rufnummer des Anrufers beim Angerufenen

In künftiger Telefontechnik soll am Anzeigedisplay des angerufenen Telefons, über das schon heute viele Apparate verfügen, die Rufnummer des Anrufers angezeigt werden. Diese Funktion ist zwar im allgemeinen nützlich und willkommen, sie kann aber auch im Einzelfall unerwünscht und lästig sein. Es ist daher auch im Sinne des Rechtes auf informationelle Selbstbestimmung der Telefonkunden geboten, daß dieser *selbst* entscheiden kann, ob er im *Einzelfall* seine Rufnummer beim Angerufenen anzeigen lassen möchte oder nicht. Besonders die Telefonseelsorge sowie

kirchliche und andere Beratungsstellen, wie z. B. die AIDS-Hilfe, haben mir sehr eindringlich dargelegt, wie wichtig es ist, daß Hilfesuchende sich ihnen auch anonym anvertrauen können. Wenn jedoch die Rufnummer des Anrufers zwangsweise angezeigt wird, so fürchten die Beratungsstellen mit der Aufhebung der Anonymität des Anrufers auch den Wegfall einer wichtigen Grundlage für ihre Tätigkeit. Aus Sicht des Datenschutzes muß daher gefordert werden, daß die Rufnummernanzeige sowohl generell als auch im Einzelfall unterdrückt werden kann; entsprechend müssen die Kommunikationsnetze gestaltet werden. Nach klärenden Gesprächen mit dem BMPT war ich zunächst davon überzeugt, daß diese sinnvolle Lösung realisiert würde. Das wurde auch seitens der Bundesregierung in der Antwort auf eine parlamentarische Anfrage im Mai des vergangenen Jahres (s. Drucksache 11/7317, Antwort zu Frage 74) ausdrücklich bestätigt:

„In einer weiteren Ausbaustufe wird die Deutsche Bundespost TELEKOM als weiteres Leistungsmerkmal für den Anrufer die Möglichkeit bereitstellen, die Anzeige seiner Rufnummer fallweise zu unterdrükken."

Die in den Verordnungsentwürfen vorgesehene Lösung ist jedoch starr, bürokratisch und kompliziert:

Neben den bisherigen, analogen Anschlüssen sollen Anschlüsse angeboten werden, deren Rufnummer *immer* beim Angerufenen angezeigt wird, wenn das dort möglich ist. Außerdem sollen Anschlüsse angeboten werden, deren Rufnummern *nie* beim Angerufenen angezeigt werden.

Weil der Anrufer die Nummernanzeige im Einzelfall nicht beeinflussen kann, sollen zum Schutz der Vertraulichkeit von Anrufen bei Beratungsstellen auch Anschlüsse angeboten werden, bei denen die Rufnummer eines Anrufers nie angezeigt wird, unabhängig davon, von welcher Art Anschluß der Anruf kommt.

Abgesehen von den offensichtlichen Schwächen dieser Lösung ergeben sich auch Komplikationen mit den EG-Partnern, die entsprechend den Verabredungen für den europäischen ISDN-Verbund die Wahlmöglichkeit im Einzelfall eröffnen: Das deutsche Netz muß nach diesen den Anschluß von Endgeräten mit Wahlmöglichkeit auf technisch einfache Weise erlauben, weil sonst ein Handelshemmnis bestünde. Die vom Anrufer getroffene Entscheidung muß aber nach den Verordnungen ignoriert werden, weil sonst die Teilnehmer ungleich behandelt würden. Technisch mag dies im fest geschalteten Netz mit etwas Aufwand lösbar sein. Beim Mobilfunk, bei dem ein einreisender EG-Bürger aber sein Gerät und seine Teilnahmeberechtigung mitbringt, kann man jedoch aus praktischen Gründen nicht bei der Einreise die grundsätzliche Entscheidung „immer oder nie die Nummer anzeigen" verlangen; andererseits darf man aber auch seiner aktuellen Entscheidung nicht folgen.

Ich hoffe, daß im Verlauf der weiteren Diskussion eine einfachere, flexiblere und dem Selbstbestimmungsrecht besser Rechnung tragende Lösung gefunden wird.

2. Registrierung der Verbindungsdaten

Die im Dezember 1990 vorgelegten Entwürfe der Rechtsverordnung sehen eine vollständige Registrierung und Speicherung der Daten aller Telekommunikationsverbindungen, einschließlich des genauen Zeitpunktes und der vollständigen Rufnummer des Angerufene auch für alle Orts- und Nahbereichsgespräche vor.

Insbesondere gegen diese „Vollspeicherung" sind in weiten Kreisen massive Widerstände laut geworden, die sich nicht nur in Presseveröffentlichungen, sondern auch in Schreiben an führende Politiker und den BMPT geäußert haben. Ich habe Verständnis dafür, wenn in diesem Zusammenhang teilweise von einer „Aufhebung des Fernmeldegeheimnisses mit anderen Mitteln" und von der „Abschaffung des Grundrechtes auf unbeobachtete Kommunikation" gesprochen worden ist. Es kann und darf nicht dahin kommen, daß dem Bürger die spontane Unbefangenheit genommen wird, zu telefonieren, wann immer es ihm einfällt und mit wem immer er möchte. Dies ist aber zu befürchten, wenn er stets damit rechnen muß, daß ihm die automatisiert gespeicherten, verarbeiteten und — nach den Vorstellungen der Deutschen Bundespost TELEKOM — monatelang gespeicherten Verbindungsdaten vorgehalten werden können. Mit Nachdruck habe ich daher die Deutsche Bundespost TELEKOM und den Bundesminister für Post und Telekommunikation aufgefordert, nur solche Daten überhaupt zu speichern, die erforderlich, d. h. unerläßlich sind, und sie auch nur solange aufzubewahren, wie es für Zwecke der Telekommunikation geboten ist. Dies gilt nicht nur für den drahtgebundenen Fernmeldeverkehr, sondern ebenso für die Mobilkommunikation, insbesondere das Autotelefon, für deren Verbreitung in den kommenden Jahren außerordentlich hohe Zuwachsraten erwartet werden.

Die Entwürfe der vom Postminister vorgelegten Datenschutzverordnungen für die Telekommunikation — „TELEKOM-Datenschutzverordnung" für die Deutsche Bundespost TELEKOM und „Teledienstunternehmen-Datenschutzverordnung" für private Anbieter — enthalten in Einzelpunkten durchaus positive Vorschläge: So soll den Telefonkunden die von mir seit Jahren geforderte Möglichkeit eingeräumt werden, einer Eintragung im Telefonbuch widersprechen zu können. Die erläuterten zentralen Forderungen werden demgegenüber nicht berücksichtigt. Die Diskussion im Rahmen einer Anhörung des Ausschusses für Post und Telekommunikation des Deutschen Bundestages am 5. März dieses Jahres zu den Datenschutzverordnungen hat in die von mir vertretene Richtung gewiesen.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in einer Entschließung zu „Telekommunikation und Datenschutz" vom 8. März meine Forderungen unterstützt (s. Anlage 10).

Wegen der ganz besonderen Bedeutung, die ich jetzt und für die Zukunft der Sicherstellung einer unbeobachteten Telekommunikation beimesse, nehme ich alle Möglichkeiten wahr, sowohl die Öffentlichkeit als auch die Entscheidungsträger in der Politik und in den gesellschaftlichen Gruppierungen auf die Bedeutung

dieser Frage hinzuweisen und sie um Unterstützung zu bitten. Ein gewisser Erfolg meiner Bemühungen und des Engagements vieler Anderer, insbesondere auch der Kirchen, zeichnet sich jetzt ab: Zum Redaktionsschluß hat der Infrastrukturrat beim Bundesminister für Post und Telekommunikation eine Lösung vorgeschlagen, nach der in der Regel die Rufnummer des Angerufenen nur um drei Ziffern verkürzt gespeichert werden wird. Eine Vollspeicherung der Rufnummer des Kommunikationspartners soll nur erfolgen, wenn der entgeltpflichtige Teilnehmer dies wünscht und bereits den Antrag auf Erteilung eines (entgeltpflichtigen) Einzelgebührennachweises gestellt hat. Diese Regelung stellt einen tragbaren Kompromiß dar und erkennt insbesondere die von mir stets vertretene Grundauffassung an, daß die Vollspeicherung für die Erfüllung der Aufgaben der Deutschen Bundespost TELEKOM nicht erforderlich ist.

8.2 Ermittlungen durch Postzusteller

Bereits mehrfach habe ich in meinen Tätigkeitsberichten über unzulässige Ermittlungen durch Postzusteller berichtet (8. TB S. 23, 9. TB S. 34f., 12. TB S. 45). Wie ich im Berichtszeitraum festgestellt habe, sind Zusteller der Deutschen Bundespost Postdienst weiterhin angehalten, Anschriften von Konfirmanden, Erstkommunikanten und Abiturienten zu ermitteln, um sie der Deutschen Bundespost Postbank für deren Werbezwecke zur Verfügung zu stellen (dazu bereits 9. TB S. 34f.). Dabei werden die Zusteller z. B. aufgefordert, mit ihren guten Kontakten zu den Pfarrämtern solche Anschriften nicht nur aus den Gemeindeblättern oder öffentlichen Aushängen, sondern auch „auf andere geeignete Weise" zu beschaffen.

Veranlaßt durch Eingaben hierzu habe ich die Frage der Ermittlungstätigkeit durch Postzusteller nach der Poststrukturreform erstmalig auch mit der Deutschen Bundespost Postdienst erörtert. Ich habe insbesondere darauf hingewiesen, daß die Deutsche Bundespost Postdienst zum Umgang mit personenbezogenen Daten nur soweit befugt ist, wie ihre gesetzlichen Aufgaben reichen. Für das Unternehmen Postdienst besteht keine allgemeine Aufgabe, Werbeinteressen des anderen Unternehmens Postbank zu fördern. Für die Erfüllung eigener Postdienst-Aufgaben ist die Erhebung von Konfirmanden- und Erstkommunikanten-Anschriften nicht erforderlich. Eine aufgabenfremde Ermittlungstätigkeit durch Postzusteller ist deshalb besonders bedauerlich, weil der Zusteller wohl derjenige Behördenvertreter ist, der dem Bürger am häufigsten begegnet. Es ist dabei nahezu zwangsläufig, daß der Zusteller gelegentlich seiner Tätigkeit einen weitreichenden Überblick über persönliche Lebensverhältnisse der Bewohner in seinem Zustellungsgebiet gewinnt. Das Vertrauen der Bürger, daß ihnen mit dem Postzusteller in ihrer unmittelbaren Lebensumwelt nicht zugleich gewissermaßen ein verdeckter Ermittler begegnet, sollte gerade im wohlverstandenen Unternehmensinteresse der Deutschen Bundespost Postdienst keinen unnötigen Irritationen ausgesetzt werden.

Die Erörterung dieser Frage hat bislang leider noch kein abschließendes Ergebnis gezeitigt, vielmehr erklärte die Generaldirektion der Deutschen Bundespost Postdienst trotz der von mir vorgetragenen Bedenken, daß sich die Unternehmen der Deutschen Bundespost „im Marketingbereich alle Optionen für die Zukunft offenhalten müssen".

8.3 Gehaltskontoverfahren

Bereits in meinem 3. und 4. Tätigkeitsbericht (3. TB S. 32f. 4. TB S. 10) hatte ich Anlaß, mich mit dem Gehaltskontoverfahren der Deutschen Bundespost zu befassen. Die meiner bereits 1979 ausgesprochenen ersten Beanstandung zugrundeliegenden tatsächlichen und rechtlichen Verhältnisse haben sich bis heute nicht entscheidend verändert. Ich mußte deshalb erneut beanstanden, daß die Deutsche Bundespost Postbank die Sperre des Gehaltskontos von Postbediensteten deren Personalstelle mitgeteilt hat.

Dabei handelte es sich nicht um einen Einzelfall. Die Postgiroämter teilen vielmehr generell eine infolge unzulässiger Überziehung verfügte Sperre des Kontos eines bei der Post Beschäftigten, der am Gehaltskontoverfahren teilnimmt, dessen Personalstelle mit. Diese Mitteilung ist nach wie vor unzulässig, weil keine Rechtsvorschrift diese Übermittlung erlaubt und auch eine wirksame Einwilligung der Betroffenen nicht eingeholt wird.

Die in meinem 4. Tätigkeitsbericht (4. TB S. 10) angekündigte Verfügung des Bundesministers für Post und Telekommunikation ist im Jahre 1982 ergangen. Mit ihr ist im Wege einer Dienstanweisung für die Beschäftigungsstelle eine Zweckbindung der Aufzeichnung über die Sperre insofern eingeführt worden, als sie ausschließlich der Bearbeitung von Deckungsanfragen dienen darf. Die Teilnehmer am Gehaltskontoverfahren werden auf die mögliche Sperrmitteilung in einem gesonderten Merkblatt hingewiesen, auf welches im Antrag auf Teilnahme am Gehaltskontoverfahren Bezug genommen wird.

Diese Antragstellung enthält keine wirksame Einwilligungserklärung des Betroffenen. Die formellen Voraussetzungen nach § 3 Satz 2 des Bundesdatenschutzgesetzes für eine solche sind nicht gewahrt. Dem Antragsteller wird mit dem bloßen Hinweis auf ein gesondertes Merkblatt in dem Antragsformular nicht klar, in was er einwilligt. Die Post muß dieses eindeutig erklären.

Ohne wirksame Einwilligungserklärung ist die Sperrmitteilung unzulässig, weil trotz der durch Dienstanweisung angeordneten Zweckbindung weiterhin schutzwürdige Belange des Betroffenen beeinträchtigt werden. Auch ist nicht gewährleistet, daß die Zweckbindung wirklich effektiv ist. Aus Eingaben sind mir konkrete Fälle bekannt, in denen die Zweckbindung mißachtet wurde (vgl. 9. TB S. 25), bis hin zur Androhung disziplinarischer Konsequenzen. Das ist nicht verwunderlich, weil es eine Verfügung des Bundesministers für Post und Telekommunikation aus dem Jahre 1983 gibt, nach der unzulässige Überziehungen von Postgirokonten durch Beamte der Deutschen Bundespost unter bestimmten Voraussetzungen disziplinarisch geahndet werden können. Eine

solche Ahndung setzt die Kenntnis dieser Umstände voraus, die am einfachsten durch eine Übermittlung des Postgiroamtes erlangt werden kann.

Eine Stellungnahme des Bundesministers für Post und Telekommunikation zu meiner neuerlichen Beanstandung lag bei Redaktionsschluß noch nicht vor.

8.4 Eurocheque-Vordrucke

Bislang stellte die Deutsche Bundespost Postbank ihren Kunden lediglich Eurocheque-Vordrucke zur Verfügung, auf denen — neben den üblichen Angaben — auch Name und Wohnort des Kontoinhabers ausgedruckt wurden. Nach überraschend langwierigen Erörterungen dieser Praxis hat die Deutsche Bundespost Postbank mir nunmehr angekündigt, meinen Anregungen zu folgen und ihren Kunden die Wahlmöglichkeit einzuräumen, ob auf ihren Vordrucken Name und Ort angegeben sein sollen. Ab 1991 werden geänderte Eurocheque-Bestellzettel verwendet, auf denen der Kunde seinen entsprechenden Wunsch äußern kann.

8.5 Schalterbildschirme im Postgirodienst

In Eingaben haben mir Bürger Einzelfälle dargelegt, in denen Schalterbildschirme im Postgirodienst so aufgestellt waren, daß Dritten die Einsicht auf über den Bildschirm abgerufene personenbezogene Kundendaten möglich war, zum Teil über entsprechende Spiegelungen in der Rundumverglasung der Schalterarbeitsplätze.

Neben einer Behebung der Mängel in den jeweiligen Einzelfällen habe ich eine generelle Verfügung der für den Postgiro-Schalterdienst zuständigen Deutschen Bundespost Postdienst erwirkt, die nachdrücklich dazu verpflichtet, die Bildschirmgeräte so auszurichten und zu handhaben, daß von Kundenseite kein Einblick auf die Bildschirmanzeige möglich ist. Zur organisatorischen Sicherung einer solchen Aufstellung ist nunmehr angeordnet, die Schalterkräfte regelmäßig auf diese Verfügung hinzuweisen, ferner deren Einhaltung zu kontrollieren („der Beachtung ist besonderes Augenmerk zu widmen").

8.6 Zweckfremde Verwendung von Kundendaten

Im Rahmen der Neustrukturierung der Deutschen Bundespost wurde der Fernmeldebereich, die sog. „Graue Post", in das Unternehmen Deutsche Bundespost TELEKOM übergeführt. Die stärkere Betonung des unternehmerischen Prinzips zeigt sich am deutlichsten in wesentlich intensivierten Marktforschungs- und Werbeaktivitäten. Diese sind als legitime Mittel eines Unternehmens zur Gewinnung neuer Kunden und zur Steigerung des Umsatzes grundsätzlich nicht zu kritisieren. Zu berücksichtigen ist jedoch hierbei, daß die von der Deutschen Bundespost TELEKOM angebotenen „Telekommunikationsdienstleistungen und -endgeräte" nur sehr bedingt mit anderen Gegenständen unternehmerischer Tätigkeiten zu vergleichen sind. So habe ich zum Beispiel wiederholt auf die ganz besondere Bedeutung des Telefons in der heutigen Gesellschaft hingewiesen; auch im Privathaushalt ist es heute unverzichtbar geworden. Nach wie vor ist jedoch die Deutsche Bundespost TELEKOM aufgrund des gesetzlichen Telefondienstmonopols einziger Anbieter: Der Telefonkunde kann daher nicht zu einem anderen Anbieter gehen, wenn ihm etwa die Konditionen der TELEKOM nicht zusagen.

Diese Abhängigkeit des Telefonkunden verlangt von der Deutschen Bundespost TELEKOM eine besondere Sensibilität und besondere Sorgfalt im Umgang mit den ihr von ihren Kunden anvertrauten personenbezogenen Daten. Entsprechend bestimmt § 454 Abs. 1 der Telekommunikationsordnung: „Die vom Teilnehmer erhobenen personenbezogenen Daten werden von der Deutschen Bundespost nicht zu anderen als Telekommunikationszwecken verwendet." Sowohl der Wortlaut dieser Vorschrift als auch deren sich aus dem Kontext ergebende Zielrichtung lassen es nicht zu, Daten von Telefonkunden ohne deren Einwilligung für Marktforschungs- und Werbezwecke zu verwenden. Da aber Marktforschung und Werbung für ein Unternehmen nötig sind, war insoweit ein Regelungsdefizit zu beheben. Ich habe daher angeregt, in die neuen Datenschutzverordnungen des Bundesministers für Post und Telekommunikation (s. 8.1.3) eine Regelung aufzunehmen, nach der die TELEKOM Kundendaten verarbeiten und nutzen darf, soweit dies für Zwecke der Beratung ihrer Kunden, der Werbung, der Marktforschung und zur bedarfsgerechten Gestaltung seiner Telekommunikationsdienstleistungen erforderlich ist und der Kunde nicht widersprochen hat.

Im Berichtszeitraum verdeutlichten zwei Fälle die Bedeutung des Problems. Im ersten Fall hatte die Deutsche Bundespost TELEKOM die Daten von über 200 000 Kunden — u. a. die Anschriften aller Funktelefonteilnehmer — einem Marktforschungsunternehmen übermittelt. Dieses wählte auftragsgemäß lediglich 1 400 Kunden aus, um an sie heranzutreten und ihnen Fragen zur Akzeptanz und Anwendung des von ihnen verwendeten Mobilfunkgerätes zu stellen. Aus Sicht des Datenschutzes war nicht nur zu kritisieren, daß die Übermittlung — wie dargelegt — nach der zur Zeit geltenden Fassung der Telekommunikationsordnung nicht zulässig war, sondern auch das eklatante Mißverhältnis zwischen den zur Marktforschung benötigten und den wirklich übermittelten Daten.

Ein zweiter Fall wurde aus dem Kreis der Mitbenutzer im Bildschirmtext an mich herangetragen. Hierbei handelt es sich um Personen, denen ein Bildschirmtext-Kunde der Deutschen Bundespost ein Mitbenutzungsrecht für einen Anschluß eingeräumt hat. Dies tut der Kunde dadurch, daß er in sein Bildschirmtextgerät den Namen des Mitbenutzers eingibt und diesem eine sogenannte Mitbenutzernummer zuweist. Das geschieht ohne Mitwirkung der Deutschen Bundespost, die dadurch auch nicht in eine vertragliche Rechtsbeziehung mit dem Mitbenutzer eintritt; der Mitbenutzer ist gewissermaßen „Untermieter" des Bildschirmtextkunden und kann in dieser Eigenschaft auch direkt — unter seiner Mitbenutzernummer — elektronische Post empfangen. Die Daten der Mitbe-

nutzer werden — ebenso wie die der Kunden — in einem zentralen Rechner der Deutschen Bundespost TELEKOM gespeichert. In einer groß angelegten Werbeaktion hatte die Deutsche Bundespost ohne Wissen und Einwilligung der Kunden die Daten von deren Mitbenutzern aus dem Rechner ausgelesen und sich direkt mit einem Werbeschreiben an sie gewandt. In diesem wurden sie aufgefordert, ihrerseits im Bekanntenkreis Käufer für Zusatzgeräte zu werben, mit deren Hilfe Fernsehgeräte zu Btx-Geräten aufgerüstet werden können. Diese zweckfremde Nutzung von Kunden- und Mitbenutzerdaten ohne deren Wissen widerspricht den Vorschriften der Telekommunikationsordnung und dem allgemeinen Zweckbindungsgrundsatz des Datenschutzes.

Beide Fälle habe ich gemäß § 20 des Bundesdatenschutzgesetzes förmlich beanstandet. Während die Deutsche Bundespost TELEKOM im Falle der Marktforschungsbefragung zugesagt hat, künftig datenschutzgerechtere Verfahren anzuwenden, hat der Bundesminister für Post- und Telekommunikation meine Beanstandung der zweckfremden Verwendung der Daten der Bildschirmtext-Mitbenutzer zurückgewiesen, da er „eine Beeinträchtigung schutzwürdiger Belange der betroffenen Mitbenutzer nicht erkennen kann". Diese Argumentation verkennt nicht nur, daß es bei einer verbotswidrigen Zweckentfremdung der Daten hierauf nicht ankommt; sie nimmt auch keine Rücksicht auf bestehende schutzwürdige Belange der Kunden. Diese räumen nämlich das Mitbenutzungsverhältnis z. T. gegen Entgelt ein und haben die Werbeaktionen auch als „Abwerbung" ihrer Kunden bewertet.

Es ist leider zu befürchten, daß die Deutsche Bundespost TELEKOM auch in Zukunft solche oder ähnliche Auswertungen und Aktionen durchführen wird. Belegt wird dies durch einen dritten Fall aus dem Ende des Berichtszeitraumes: Ein Fernmeldeamt hatte einer Gemeinde Computerlisten derjenigen Kunden zugeschickt, die einen Fernseh-Kabelanschluß beantragt hatten. Die Gemeinde richtete daraufhin an alle anderen Bürger ein höchst eindringliches Werbeschreiben, in dem versucht wurde, sie doch noch zur Beantragung eines Kabelanschlusses zu bewegen.

Auch in diesem Fall wurde gegen das eindeutige Übermittlungsverbot des § 454 Abs. 2 TKO und das Zweckbindungsgebot des § 454 Abs. 1 TKO verstoßen — ein Rechtsverstoß, der auch durch kommerzielle Interessen nicht gerechtfertigt werden kann.

8.7 Funktelefondienst

Von den atemberaubenden Fortschritten in der Chiptechnologie, insbesondere der Miniaturisierung der elektronischen Bauelemente, haben nicht nur die „drahtgebundenen" Telefone profitiert; auch die Angebote der Funkdienste wurden grundlegend verbessert. Eine Vielzahl neuer Dienste ermöglicht es, an nahezu jedem Ort Nachrichten entgegenzunehmen oder Nachrichten abzusenden, ohne daß dabei ein Anschlußkabel benötigt wird. Von besonderer Bedeutung in der Mobilkommunikation ist dabei der Funktelefondienst, denn er ermöglicht das hochkomfortable Telefonieren von nahezu jedem Ort der Bundesrepublik Deutschland aus und bereits jetzt grenzüberschreitend in den Niederlanden, in Luxemburg und in Österreich. Neben den im Fahrzeug eingebauten Geräten, über die auch Telefaxsendungen zu empfangen sind, werden kleine Taschengeräte angeboten, die nur unwesentlich größer als der Hörer eines „normalen" Telefones sind. Im sogenannten C-Netz der Deutschen Bundespost TELEKOM sind derzeit nahezu 300 000 Funktelefone in Betrieb; der Endausbau — 600 000 Teilnehmer — wird in wenigen Jahren erreicht sein.

Mitte des Jahres 1991 wird ein neues paneuropäisches digitales zellulares Funktelefonnetz seinen Betrieb aufnehmen, das in der Bundesrepublik Deutschland D-Netz heißt. Vor allem ein Grund ist es, der alle Experten zu z. T. euphorischen Prognosen für dieses Netz veranlaßt: Im Rahmen der Neustrukturierung der Deutschen Bundespost durch das Poststrukturgesetz 1989 (s. 12. TB, S. 36f.) wurde der Telekommunikationsmarkt grundsätzlich dem Wettbewerb geöffnet; hierzu gehört erklärtermaßen gerade auch der Mobilfunkbereich. Deshalb wird zu dem geplanten Termin, nämlich am 1. Juli 1991, nicht nur die Deutsche Bundespost TELEKOM ihr D 1-Netz, sondern auch das privatwirtschaftliche Unternehmen Mannesmann Mobilfunk sein D 2-Netz in Betrieb nehmen. Die Absicht nahezu aller europäischen Staaten, dieses Netz unter Zugrundelegung derselben technischen Bedingungen auch in ihren Ländern zu errichten, die große Systemkapazität — 10 bis 15 Mio. Teilnehmer — und vor allem der Wettbewerb lassen bisher nicht gekannte Zuwachsraten erwarten. Als eine Folge wird erwartet, daß der Gerätepreis in wenigen Jahren auf etwa 1 000 DM sinken wird.

Die Gestaltung moderner Kommunikationsnetze ist nicht möglich ohne die Verarbeitung personenbezogener Daten, insbesondere der dem Fernmeldegeheimnis unterliegenden Daten über die Kommunikationsverbindungen. Ich habe deshalb wiederholt auch gegenüber der Deutschen Bundespost TELEKOM die Notwendigkeit betont, bereits in einem sehr frühen Projektstadium Datenschutzgesichtspunkte bei der Systemgestaltung zu berücksichtigen. Gleichwohl hat die Deutsche Bundespost TELEKOM weder mich noch andere Datenschutzinstanzen entsprechend früh hinzugezogen, sondern vielmehr bereits im Jahre 1987 in einem sogenannten „Memorandum of Understanding (MoU)" gemeinsam mit den anderen europäischen Interessenten wesentliche Festlegungen getroffen. Damit wurde in Kauf genommen, daß von den Fernmeldeverwaltungen getroffene Vereinbarungen im Widerspruch zu geltenden oder bis zur Anwendung geschaffenen Rechtsvorschriften stehen, was weder der technischen Entwicklung noch der Akzeptanz der Systeme dient. Auf meine dringenden Bitten hin erläuterte mir die Deutsche Bundespost TELEKOM im August 1990 die grundsätzliche Netzarchitektur sowie die aus Datenschutzsicht wichtigsten vorgesehenen Verarbeitungen und Übermittlungen personenbezogener Daten.

Zu begrüßen ist, daß die deutlich erhöhte Systemsicherheit einen Mißbrauch — etwa durch Manipulation an den Funkgeräten — wesentlich erschwert, da

die Inbetriebnahme nur mit Hilfe einer besonderen Zugangskarte, dem Subscriber Identity Module (SIM), möglich ist, die ihrerseits — ähnlich wie bei der Euroscheckkarte — nur mittels einer nur dem Eigentümer bekannten „Geheimnummer", der PIN (Personal Identifikation Number) benutzt werden kann. Weiterhin wird die Funkübertragungsstrecke kryptographisch verschlüsselt, so daß auch auf diesem Weg der Angriff für Mißbrauchsversuche nahezu unmöglich wird. Aufgrund dieser erhöhten Sicherheit entfällt auch die Notwendigkeit für eine „Vorratsspeicherung" aller Verbindungsdaten, wie sie noch im C-Netz zur Mißbrauchsbekämpfung als erforderlich angesehen wird.

Bedenklich erscheint jedoch, daß die derzeitige Konzeption der Gebührenabrechnung vorsieht, generell die vollständigen Verbindungsdaten aller Telefonate zu speichern und sie für sechs Monate aufzubewahren. Diese Festlegung ist besonders erstaunlich, weil eine solche Speicherung durch die schon damals geltende Telekommunikationsordnung nicht gedeckt war. Vielmehr stieß schon die Speicherung der Verbindungsdaten für 80 Tage nach Absendung der Rechnung in den Funktelefondiensten auf Kritik und wurde nur wegen der Unsicherheit dieser Netze für tragbar gehalten. Um so verwunderlicher ist es, daß nach dem Wegfallen der Sicherheitsargumente die Verbindungsdatenspeicherung nicht nur nicht vermindert, sondern sogar noch deutlich erweitert wurde. Derartige Ergebnisse sind nur möglich, weil diese und andere technische Festlegungen („Spezifikationen") ohne Kontrolle der nationalen Regierungen, etwa des Bundesministers für Post und Telekommunikation, im European Telecommunikations Standards Institute (ETSI) in Südfrankreich erfolgen, dem außer nationalen Betreibergesellschaften in erster Linie Großunternehmen der Telekommunikationsindustrie angehören.

Ich habe in den Gesprächen mit der Deutschen Bundespost TELEKOM, aber auch gegenüber dem Bundesminister für Post und Telekommunikation im Zusammenhang mit der Beratung von Entwürfen von Datenschutzverordnungen gemäß § 30 Abs. 2 des Postverfassungsgesetzes und § 14a Abs. 2 des Fernmeldeanlagengesetzes (s. 8.1.3) betont, daß auch die technische Gestaltung moderner Nachrichtensysteme den Vorgaben des Gesetzgebers für eine datenschutzgerechte Gestaltung der Telekommunikation folgen muß; ein rechtliches Nachvollziehen und damit Legalisieren von ohne Rücksicht auf geltendes Recht bereits getroffenen technischen Festlegungen wäre ein verhängnisvoller Weg. Gerade wenn sich die optimistischen Zuwachsprognosen der Deutschen Bundespost TELEKOM und der Lieferindustrie bewahrheiten sollten, wird die datenschutzgerechte Gestaltung des Funktelefondienstes sehr schnell hohe Bedeutung gewinnen.

8.8 Mithören von Telefongesprächen durch Programmfehler in digitalen Vermittlungsstellen

Die entscheidenden Punkte im gesamten Telekommunikationsnetz der Deutschen Bundespost TELEKOM sind die sogenannten Vermittlungsstellen: Da für keine Telefonverbindung eine durchgehende Leitung zur Verfügung steht, muß jede Verbindung — entsprechend der vom Benutzer gewählten Telefonnummer des gewünschten Anschlusses — aus einzelnen Leitungsstücken zusammengeschaltet werden. Dies geschieht in den Vermittlungsstellen, die bis in die sechziger Jahre lediglich aus einer Ansammlung elektromechanischer Schalter bestanden. Inzwischen hat die Deutsche Bundespost begonnen, mit großem Nachdruck und hohem Aufwand den Ersatz dieser konventionellen „EMD-Technik" zu betreiben: Anstelle der elektromechanischen Schalter finden sich jetzt leistungsfähige Computer in den Vermittlungsstellen, die damit zwar deren hohe Leistungsfähigkeit, aber auch die typischen Probleme programmgesteuerter Rechenanlagen aufweisen (s. auch 10. TB, S. 34f.).

Im Berichtszeitraum haben zwei Vorkommnisse gezeigt, daß die Deutsche Bundespost TELEKOM ihre Anstrengungen noch verstärken muß, um diese Probleme zu beherrschen und damit Beeinträchtigungen schutzwürdiger Belange der Telefonkunden noch besser entgegenzuwirken.

Vom ersten Fall erfuhr ich im Mai 1990. Damals wurde meine Dienststelle von einer besorgten und zu Recht auch etwas empörten Anruferin darüber unterrichtet, daß man von Bonn aus durch die Wahl einer bestimmten Telefonnummer in Berlin geführte Telefonate mithören könne.

Nachdem ich mich von der Richtigkeit der zunächst kaum glaubhaften Behauptung überzeugt hatte, informierte ich einen Mitarbeiter des Datenschutzbeauftragten des BMPT, der noch am selben Tag diesen Sachverhalt bei der Landespostdirektion Berlin vortrug und auch die Zusage erreichte, daß man sich so schnell wie möglich um die Angelegenheit kümmern werde. Trotzdem dauerte es fünf Tage, bis der Fehler behoben war.

Meine Versuche, den Fehler so zu erkennen und zu beschreiben, daß man die Ursache gezielt suchen konnte, und die detaillierte Prüfung durch eine Expertengruppe ergaben das Folgende:

Wenn man eine Telefonnummer wählte, die im Nummernbereich einer großen Nebenstelle lag, zu der dort aber kein Apparat gehörte, dann signalisierte die Nebenstelle an den Computer in der (Post-)Vermittlungsstelle, daß eine Verbindung nicht möglich sei, denn zu *dieser* Nummer gab es kein Telefon. Statt nun an den Anrufer zu signalisieren „kein Anschluß unter dieser Nummer" und die Verbindung abzubauen, ließ der Vermittlungscomputer — und da lag der Fehler! — die Verbindungsstrecke vom Anrufer bis in seinen Speicher bestehen und gab trotzdem (das war zwar im Prinzip richtig, verschlimmerte aber die Wirkung des Fehlers) diesen Speicherbereich für neue Verbindungen frei. Wurde nun über diesen Speicherbereich eine Verbindung hergestellt, so wurde der zunächst erfolglose Anruf in die neue Verbindung so einbezogen, daß er alles mithören, sich den anderen Beteiligten aber nicht bemerkbar machen konnte. Auch die übrige Verarbeitung war korrekt, was zur Folge hatte, daß die Versuche gebührenfrei waren und als „erfolglose Versuche im Fernverkehr" planmäßig nach insgesamt zwei Minuten vom Netz her abgebrochen wurden.

Weil alles genau so funktionierte, wie es (falsch) programmiert war, konnte der Fehler natürlich durch fernmeldetechnische Messungen nicht gefunden werden. Erschwerend war auch, daß der Fehler nur dann auftrat, wenn der Versuch nicht aus Berlin, sondern aus bestimmten anderen Ortsnetzen gestartet wurde. Dies erklärt auch, warum eine schon mehrere Wochen vorher eingegangene Fehlermeldung in derselben Sache nicht zu den in diesem Fall gebotenen Maßnahmen führte. In der Zwischenzeit hatte sich diese Möglichkeit des kostenlosen Zeitvertreibs wohl als besonders interessant herumgesprochen, zumal häufig Gespräche einer großen Polizeidienststelle mitzuhören waren, die über diese Vermittlungsstelle mit dem Postnetz verbunden war. Weil die bekannte Nummer im Nummernkreis der Nebenstelle dieser Behörde lag, war auch zunächst hier der Fehler gesucht worden. Das fehlerhafte Programm wurde übrigens nicht nur in dieser Vermittlungsstelle eingesetzt, sondern noch in einer anderen. Dort war der Fehler jedoch (noch) nicht bekannt geworden.

Von dem zweiten Fall erfuhr ich durch einen Journalisten im Herbst 1990. Dabei lagen die Verhältnisse ähnlich, auch hier war der Fehler schon gemeldet worden, ohne daß man mit den zunächst eingeleiteten Prüfungen die Ursache gefunden hatte. Zwar konnte dieser Fehler von mir nicht experimentell nachvollzogen werden, aber nach den Erfahrungen aus dem ersten Fall und den mir mitgeteilten Einzelheiten sprach sehr viel für einen Programmfehler im Computer der Vermittlungsstelle. Nachdem ich die DBP TELEKOM darüber informiert hatte, wurde dieser bald gefunden und beseitigt.

Beide Fälle zeigen, daß die bisher angewandte Sorgfalt beim Erstellen und Testen von Programmen für Vermittlungsstellen offenbar nicht ausreicht, um zu gewährleisten, daß die Programme in den Vermittlungsstellen die erwarteten Ergebnisse liefern und kein ungewolltes und das Fernmeldegeheimnis verletzendes Mithören von Telefongesprächen bewirken.

An die Fehlerfreiheit der Software für Vermittlungsstellen sind aber allerhöchste Ansprüche zu stellen, denn Fehler der beschriebenen Art führen zu schwerwiegenden Verletzungen des Fernmeldegeheimnisses; andere Fehler könnten zu Ausfällen mit erheblichen wirtschaftlichen Folgen führen. Dies ist auch deshalb von besonderer, zukünftig noch steigender Bedeutung, weil mit dem zunehmenden Einsatz von Computern in Vermittlungsstellen solche Fehler nicht lediglich einen oder nur wenige Knotenpunkte betreffen, sondern vielleicht Hunderte von baugleichen und mit derselben Software ausgestattete Vermittlungsstellen beeinträchtigen und sogar stillegen könnten. Für vorbeugende Tests der dort einzusetzenden Software, die alle denkbaren Betriebsbedingungen berücksichtigen und die unterschiedlichsten Situationen durchspielen, ist auch ein außergewöhnlich hoher Aufwand gerechtfertigt.

Alle Bemühungen um Fehlerfreiheit von Software können jedoch nach dem heutigen Stand der Programmierkunst für Systeme dieser Größe Fehler zwar unwahrscheinlicher machen, aber doch nicht mit absoluter Sicherheit ausschließen. Zu viele Bedingungen sind in den Programmen zu berücksichtigen, und wenn Tausende von Einzelanweisungen sich ergänzen und dabei z. T. in komplizierten wechselseitigen Abhängigkeiten stehen, genügt — wie die Beispiele gezeigt haben — eine Kleinigkeit, um unter bestimmten Bedingungen eine fatale Wirkung zu erzielen. Deshalb muß als ständige Vorsorge gegen vielleicht doch nicht vermiedene Fehler oder unvermeidbare Störungen die notwendige Organisation zur richtigen Behandlung von ungewöhnlichen Situationen vorgehalten werden.

Beide Fälle belegen, daß bei der Deutschen Bundespost TELEKOM ein erheblicher Organisationsmangel bestand, der auch schon bei der Klärung von Problemfällen im Bildschirmtextdienst (s. 10. TB, S. 40f.) hinderlich war: Es fehlte eine Organisationseinheit, die bekannt, jederzeit erreichbar und in der Lage war, Fehlfunktionen der automatisierten Datenverarbeitung für Kommunikationszwecke zu lokalisieren, ihre Wirkungen zunächst zu beschränken und eine sachgerechte Korrektur einzuleiten. Und es fehlte bei den Stellen, denen die Fehler gemeldet wurden, die Sensibilität dafür, daß es sich zumindest dann, wenn man den gemeldeten Fehler mit den traditionellen Verfahren des fernmeldetechnischen Messens und Prüfens nicht finden kann, um einen Fehler neuer Art mit neuen, unvorhersehbaren Wirkungen handeln könnte, gegen den möglichst schnell entsprechende Maßnahmen eingeleitet werden müssen. Zu solchen Maßnahmen können auch Warnungen an diejenigen Stellen und Personen gehören, die — vielleicht ohne es zu wissen — durch die festgestellten Fehlfunktionen in ihren Rechten verletzt werden können. Immerhin konnten durch den Fehler in der Berliner Vermittlungsstelle nicht nur viele Privatpersonen abgehört werden, sondern unter anderem auch Gespräche der Polizei, einer Bezirksverwaltung, von Rechtsanwaltskanzleien und der früheren Ständigen Vertretung der Bundesrepublik Deutschland in Ost-Berlin. Zwar konnte man sich das jeweilige „Opfer" nicht gezielt aussuchen, aber es gibt keine Garantie, daß dies bei zukünftigen Fehlern nicht doch möglich ist.

8.9 ISDN-Richtlinie der EG-Kommission

Die Anschlußzahlen im ISDN-Netz steigen in der Bundesrepublik Deutschland nur äußerst schleppend: Anfang 1991 war noch nicht einmal ein Tausendstel der Telefonanschlüsse in der Form eines sogenannten Universalanschlusses an das ISDN-Netz angeschlossen. Die Europäische Gemeinschaft fördert und unterstützt die Einführung eines europaweiten ISDN-Netzes („Euro-ISDN"); dies kommt in der „Empfehlung des Rates vom 22. Dezember 1986 über die koordinierte Einführung des diensteintegrierenden digitalen Fernmeldenetzes (ISDN) in der Europäischen Gemeinschaft (86/659/EWG)" deutlich zum Ausdruck. Nach dieser Empfehlung sollen bis 1993 etwa 5 Mio. ISDN-Anschlüsse in der EG installiert werden, so daß aufgrund des geographischen Deckungsgrades etwa 80 % der Teilnehmer die Möglichkeit hätten, einen ISDN-Anschluß zu wählen. Bereits im Oktober 1989 konnte die erste Internationale ISDN-Verbindung — zwischen der Bundesrepublik und den Niederlan-

den — aufgebaut werden. Im Oktober 1990 wurde die Verbindung zum französischen Netz, im Dezember mit dem der britischen Fernmeldeverwaltung hergestellt. Im Frühjahr 1991 ist der Verbund mit den Telekommunikationsnetzen der japanischen Gesellschaften NTT und KDD sowie mit dem Netz der amerikanischen Gesellschaft AT & T vorgesehen.

Sowohl der Rat der Europäischen Gemeinschaft als auch das Europäische Parlament haben wiederholt die Bedeutung geeigneter Maßnahmen für die Sicherstellung des Schutzes der Daten und der Privatsphäre im Hinblick auf die neuen Entwicklungen der Telekommunikation und insbesondere des ISDN hervorgehoben. Die EG-Kommission legte daher gleichzeitig mit dem Vorschlag für eine allgemeine Datenschutzrichtlinie (siehe unten Nr. 28) einen „Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen" (SYN 288), vor. Die Initiative der EG-Kommission ist zu begrüßen, zumal der Entwurf ein durchaus erfreuliches Datenschutzniveau aufweist. In einigen Punkten scheint jedoch eine Nachbesserung dringend geboten:

Der demnächst auch in der Bundesrepublik Deutschland gültige Grundsatz, daß kein Teilnehmer gegen seinen Willen in öffentliche Verzeichnisse eingetragen werden darf, sollte Eingang in die Richtlinie finden.

Ähnliches gilt für das Recht auf Auskunft des Betroffenen; die Richtlinie sollte klarstellen, daß — wie im neugefaßten BDSG — die Auskunft grundsätzlich kostenlos erfolgt.

Unzureichend sind die Vorschriften des Artikel 7 des Entwurfes, der lediglich verlangt, die Kommunikationsdaten „vertraulich zu behandeln". Hier erscheint eine Formulierung geboten, die — etwa in Anlehnung an die des deutschen Fernmeldeanlagengesetzes — die Einhaltung eines definierten Fernmeldegeheimnisses verlangt und auch eine Strafbewehrung fordert.

In dem zentralen Punkt der Verbindungs- und Gebührendatenverarbeitung stellt der Entwurf (Artikel 9 und 10) die Speicherung und Verarbeitung der vollständigen Rufnummer des Angerufenen lediglich unter den allgemeinen Vorbehalt der Erforderlichkeit. Dies widerspricht dem Gebot, in wichtigen Fragen klare Vorgaben zu machen, und — wenn es als Erlaubnis mißverstanden wird — in mehrfacher Hinsicht Grundsätzen des Datenschutzes (siehe oben Nr. 8.1.3). Der Entwurf sollte dahingehend geändert werden, daß aus den Verbindungsdaten (Artikel 10) unverzüglich die für die Gebührenermittlung relevanten Gebührendaten (Artikel 9) errechnet und alle übrigen Daten gelöscht werden. Auch die Gebührendaten müssen nach Errechnung der Gebühren unverzüglich gelöscht werden, es sei denn, der Teilnehmer hat eine weitere Speicherung — z. B. zur Erstellung eines Einzelgebührennachweises — gewünscht. Der Einzelgebührennachweis sollte am zweckmäßigsten nur erkennen lassen, zu welchem Ort eine Verbindung bestanden hat; zumindest muß die Rufnummer des Angerufenen deutlich verkürzt sein. Anrufe zu Stellen, die telefonisch Gesundheitsberatung und Lebenshilfe geben, dürfen aus dem Einzelgebührennachweis nicht zu erkennen sein. Mit Rücksicht darauf, daß einer Telefonnummer nicht ohne weiteres anzusehen ist, welche Ziffern das Ortsnetz bezeichnen, ist die im Richtlinienentwurf vorgesehene Kürzung der Zielnummer um vier Ziffern eine sinnvolle Lösung.

Zu begrüßen ist in Artikel 12 die Regelung des Entwurfs, daß die Anzeige der Rufnummer des Anrufers beim Angerufenen nicht nur ständig, sondern auch von Fall zu Fall unterdrückt werden kann.

Ich habe den beteiligten Bundesministerien meine Anregungen mitgeteilt und gebeten, sie in die Stellungnahme der Bundesregierung einzubeziehen.

9 Verkehrswesen

9.1 Zentrales Verkehrsinformationssystem (ZEVIS)

Über die noch vorhandenen Probleme des Aufbaus, des Betriebs und der Nutzung des Zentralen Verkehrsinformationssystems habe ich berichtet (zuletzt 12. TB S. 47 ff.). Auch im Berichtszeitraum dienten Kontrollen beim Kraftfahrt-Bundesamt und Bundeskriminalamt, bei der Grenzschutzdirektion Koblenz sowie beim Zollkriminalinstitut Köln vornehmlich dazu, Erkenntnisse über die bisher mit dem System gemachten Erfahrungen zu gewinnen, über die dem Deutschen Bundestag im Jahr 1991 zu berichten ist.

Soweit sich bisher abzeichnet, werden in diesem Erfahrungsbericht Vorschläge für die Behebung bisher erkannter Schwachstellen unterbreitet und Hinweise für eine zukünftige bessere Ausgestaltung des Systems gemacht werden. Dazu können auch Vorschläge zur Änderung gesetzlicher Vorschriften, insbesondere des Straßenverkehrsgesetzes, gehören. Zusammen mit den Landesbeauftragten für den Datenschutz, die ebenfalls Kontrollen durchgeführt haben, habe ich konzeptionelle datenschutzrechtliche Überlegungen erarbeitet, die an den BMV herangetragen werden. Der Erfahrungsbericht wird sich voraussichtlich mit

- den Voraussetzungen für den Zugang zum System,
- den erforderlichen technischen und organisatorischen Sicherungen,
- dem Verfahren und dem Umfang zu erteilender Auskünfte sowie
- der Pflicht zur Aufzeichnung von Abrufen

befassen.

9.1.1 Nutzung durch das Bundeskriminalamt

Über die bei einer Kontrolle der ZEVIS-Nutzung durch das Bundeskriminalamt (BKA) festgestellte Notwendigkeit von Vorgaben für die Abrufpraxis und Dokumentation habe ich berichtet (12. TB S. 49 f.). Das BKA hat nach erneuter Diskussion hierüber dem

nicht mehr widersprochen und meine ersten Vorschläge akzeptiert. Ich werde mit dem BKA Inhalt und Form dieser Handlungsanweisung erörtern.

ZEVIS-Abrufe zu Schulungszwecken

Bei einer weiteren Kontrolle habe ich festgestellt, daß das BKA zu Schulungszwecken über ZEVIS im automatisierten Verfahren online auf Fahrzeug- und Halterdaten zugegriffen hat, obwohl das Kraftfahrt-Bundesamt hierfür separate Schulungsdaten zur Verfügung stellt, mit denen derartige Abrufe simuliert und damit geübt werden können. Das BKA hat diese Abrufpraxis eingeräumt, jedoch darauf hingewiesen, daß der Zugriff entweder nur auf „eigene" Daten oder aber mit Daten der zu Unterweisenden mit deren ausdrücklicher Genehmigung erfolgt sei, demnach nicht auf Fremddaten zugegriffen worden sei; es habe diese Praxis daher für zulässig gehalten.

Unter „eigenen" Daten hat das BKA Daten von Personen verstanden, die es in einem anderen Zusammenhang bereits erhoben hatte. Deren Abruf für Schulungszwecke stellte aber eine durch das Straßenverkehrsgesetz nicht gedeckte zweckfremde Nutzung von Fahrzeug- und Halterdaten dar.

Ich habe davon abgesehen, diese gegen § 36 StVG in Verbindung mit § 3 BDSG verstoßende Datenübermittlung gemäß § 20 Abs. 1 BDSG zu beanstanden, weil die personenbezogenen Daten der Fahrzeughalter aufgrund der durchgeführten Abrufe nur einem begrenzten Kreis von zur Verschwiegenheit verpflichteten Polizeibeamten zugänglich wurden und eine anderweitige Nutzung oder Weitergabe ausgeschlossen werden konnte. Das BKA hat diese Schulungspraxis aufgrund meiner Bedenken nunmehr eingestellt.

Datenübermittlung an ausländische Dienststellen

Ich habe weiter festgestellt, daß das BKA über ZEVIS abgefragte Fahrzeug- und Halterdaten auch an Empfänger im Ausland übermittelt. Diese Praxis wirft einige Probleme auf.

Soweit das BKA ZEVIS-Erkenntnisse unmittelbar an deutsche Auslandsvertretungen zur Entlastung von deutschen Staatsangehörigen in ausländischen Haftanstalten übermittelt, habe ich keine Bedenken, dies als Datenübermittlung an inländische Dienststellen unter den Voraussetzungen des § 36 StVG zuzulassen. Das gleiche dürfte gelten für die Übermittlung von ZEVIS-Daten an deutsche Rauschgiftverbindungsbeamte des BKA im Ausland zur Durchführung deutscher Ermittlungsverfahren. Das Amt sollte jedoch durch Verfahrensregelungen sicherstellen, daß die anfragende Stelle und der Zweck der Anfrage festgestellt werden können, der Empfänger der Daten auf das Erfordernis der Zweckbindung hingewiesen und die Einhaltung dieser Regeln auch kontrolliert wird.

Probleme bereitet die Rechtslage in den Fällen der Übermittlung von ZEVIS-Erkenntnissen ins Ausland, in denen das BKA im Rahmen der ihm gesetzlich übertragenen Aufgabe als nationales Zentralbüro für Interpol tätig wird; als solches hat es einen Informationsaustausch mit ausländischen Stellen durchzuführen. Hieraus ergibt sich auch die Berechtigung des Amtes, unter Beachtung des § 36 StVG ZEVIS-Abrufe durchzuführen. Dies tut es häufig schon deshalb, um bei Zweifeln über den Wohnsitz von Kfz-Haltern das für die weitere Bearbeitung ausländischer Anfragen zuständige Landeskriminalamt feststellen zu können. Auch dies halte ich für zulässig. Problematisch wird es aber dann, wenn das BKA — nach Weiterleitung der Anfragen an die Landeskriminalämter, die ihrerseits ZEVIS-Ermittlungen anstellen und über das Ergebnis berichten — die Daten, möglicherweise zusammen mit eigenen Erkenntnissen, an die anfragende Stelle ins Ausland weiter übermittelt. Ich habe festgestellt, daß dabei vom KBA die für solche Fälle in § 37 Abs. 2 bis 4 StVG gesetzlich vorgesehenen besonderen Verfahrensregeln (spezielle Prüfung der Zulässigkeit dieser Übermittlung, Hinweis an den Empfänger auf die besondere Zweckbindung, Unterrichtung des Betroffenen, soweit dies geboten ist) nicht eingehalten werden. Das BKA sieht sich lediglich als „Vermittlungsstelle" der Landeskriminalämter und meint, die besonderen Übermittlungsregeln schon deshalb nicht einhalten zu müssen, weil diese nur die „Registerbehörden", also örtliche und zentrale Fahrzeugregister, verpflichten. Dies trifft nach dem Wortlaut des § 37 in der Tat zu. Die Registerbehörden wiederum können sich darauf berufen, daß sie selbst in den beschriebenen Fällen nicht ins Ausland übermitteln. Insofern sind auch sie nicht von der Bestimmung des § 37 StVG erfaßt; sie können auch nicht wissen, welche Informationen letztlich das BKA verlassen.

Bei dieser Sachlage läuft § 37 StVG größtenteils leer. Dies entspricht nicht Sinn und Zweck der Vorschrift und muß deshalb vermieden werden. Die Verpflichtung zur Einhaltung der besonderen Verfahrensregeln muß nicht nur für die Registerbehörden, sondern auch für alle sonstigen Stellen bestehen, die Fahrzeug- und Halterdaten ins Ausland übermitteln. Ich werde die Bundesregierung bitten, bei nächster Gelegenheit eine entsprechende gesetzliche Klarstellung zu veranlassen. Bis dahin sollte das Bundeskriminalamt eine dem Sinn und Zweck des § 37 StVG entsprechende Übermittlungspraxis pflegen. Deshalb habe ich das BKA gebeten, durch neue Verfahrensregeln beim Informationsaustausch mit Interpol-Stellen dafür zu sorgen, daß die in § 37 Abs. 2 bis 4 StVG enthaltenen datenschutzrechtlichen Anforderungen — unabhängig vom Adressaten der Bestimmung — in entsprechender Anwendung der Vorschrift und unter Berücksichtigung des künftigen § 17 des neuen Bundesdatenschutzgesetzes eingehalten werden.

9.1.2 Nutzung durch die Grenzschutzdirektion und das Zollkriminalinstitut

Bei Kontrollen der ZEVIS-Abrufe durch die Grenzschutzdirektion Koblenz und das Zollkriminalinstitut Köln habe ich keine Probleme festgestellt. Positiv herauszustellen ist, daß die Zentralstelle der Grenzschutzdirektion, die als zentrale Informations-Sammelstelle bei Verdacht Grenzfahndungen einleitet, nicht nur die gesetzlich vorgeschriebene Auswahlpro-

tokollierung, sondern jeden in diesem Zusammenhang erforderlichen ZEVIS-Abruf in den Ermittlungsakten dokumentiert.

Eine hundertprozentige Zusatzprotokollierung nimmt auch das Zollkriminalinstitut Köln vor, das als koordinierende Stelle für die Zollfahndungsämter und aufgrund von internationalen Rechtshilfeersuchen ausländischer Zolldienststellen ZEVIS-Abrufe durchführt. Hierzu hat das Zollkriminalinstitut Handlungsanweisungen erlassen.

Diese aus meiner Sicht vorbildliche Praxis sollte — mit den erforderlichen Anpassungen je nach Aufgabenstellung — auch von anderen abrufberechtigten Dienststellen übernommen werden.

9.2 Luftfahrt

9.2.1 Luftverkehrsgesetz

Bei den Beratungen über das Zehnte Gesetz zur Änderung des Luftverkehrsgesetzes bin ich im Berichtszeitraum intensiv beteiligt worden. Dabei sind nicht alle meine Vorstellungen berücksichtigt worden. Nachdem das Gesetz vom Bundespräsidenten nicht ausgefertigt worden ist, werde ich bei den anstehenden Neuberatungen des Vorhabens meine ursprünglichen Wünsche erneut vortragen.

Dies gilt zum Beispiel für meinen Formulierungsvorschlag zur Führung des Hauptflugbuches durch die Flugplatzhalter. Mit dem Bundesminister für Verkehr besteht Einigkeit darüber, diese bisher auf eine Auflage im Rahmen der Genehmigung zum Betrieb eines Flugplatzes gestützte Verpflichtung zur Aufzeichnung von Daten über Starts und Landungen auf eine normative Grundlage zu stellen (vgl. 12. TB S. 52). Hierzu hatte ich eine Ergänzung des Luftverkehrsgesetzes vorgeschlagen, die sich inhaltlich an dem üblichen Wortlaut der von den Genehmigungsbehörden ausgesprochenen Auflagen orientierte. Der Bundesminister für Verkehr möchte hingegen die Zuständigkeit für die Führung des Hauptflugbuches auf die Luftaufsichtsbehörden der Länder verlagern und hat hierzu Änderungen der Luftverkehrsordnung und der Luftverkehrs-Zulassungsverordnung vorgesehen. Gegen eine derartige Aufzeichnungspflicht normaler Flugbetriebsdaten durch eine überwachende Behörde habe ich grundsätzliche Bedenken geltend gemacht, da die Daten dort in aller Regel für die Aufgabenerfüllung nicht benötigt und lediglich auf Vorrat gesammelt werden; es muß — wie bisher — genügen, daß das Luftaufsichtspersonal den Flugbetrieb überwacht. Darüber hinaus sind die vorgesehenen Regelungen — die aus meiner Sicht eine Änderung des Luftverkehrsgesetzes voraussetzen — datenschutzrechtlich lückenhaft.

Die in der vergangenen Legislaturperiode gefundene datenschutzrechtliche Regelung über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Flugsicherungsbetriebsdienste und die flugsicherungstechnischen Dienste beruht auf einer von mir vorgeschlagenen Formulierung. Sie sollte in dieser Form auch bei einem Gesetz in der 12. Legislaturperiode vorgesehen werden.

Im Gegensatz hierzu waren meine Bemühungen, die Regelung für die Überprüfung des Personals im sicherheitsempfindlichen Bereich der entsprechenden Bestimmung des Atomgesetzes nachzubilden, bei der Beratung des Gesetzes nur teilweise erfolgreich. Deshalb begrüße ich, daß der Bundesminister des Innern im Rahmen eines Gesetzes zur Übertragung der Aufgaben der Luftsicherheit auf den Bundesgrenzschutz eine neue Formulierung für die Sicherheitsüberprüfung des in sicherheitsempfindlichen Bereichen auf Flughäfen tätigen Personals vorgelegt hat, die meiner ursprünglichen Konzeption entspricht und datenschutzrechtliche Belange berücksichtigt.

9.2.2 Sonstige luftrechtliche Defizite

Der Bundesminister für Verkehr ist mit der Behebung von mir seit langem bemängelter datenschutzrechtlicher Defizite weiter im Verzug. Bereits 1984 hatte ich gesetzliche Regelungen für die Führung der Datensammlung über Luftfahrer — die die Daten der Flugerlaubnisse und -berechtigungen sowie der einschlägigen rechtskräftigen Entscheidungen in Straf-, Bußgeld- und Verwaltungsverfahren enthält — gefordert. Der Bundesminister für Verkehr hat die Notwendigkeit einer entsprechenden Novellierung grundsätzlich anerkannt (vgl. zuletzt 12. TB S. 52). Er hat jedoch auch im Berichtsjahr keinerlei Regelungsvorschläge gemacht und dies zuletzt mit anderen Prioritäten, Arbeitszeitverkürzungen und Einsparungen in den Personalbereichen seines Hauses begründet. Ich bedauere, daß das Ministerium auch nach mehr als sechs Jahren weiterhin untätig geblieben ist, zumal die erwähnten Datensammlungen zum Teil sensible Daten enthalten. Es droht die Gefahr, daß sie ohne eine ausreichende gesetzliche Grundlage nicht mehr weitergeführt werden dürfen.

Ich habe auch seit langem gefordert, eine rechtliche Grundlage für die Erhebung, Speicherung und Übermittlung von personenbezogenen Informationen durch die Flugunfalluntersuchungsstelle des Luftfahrt-Bundesamtes zu schaffen (vgl. 12. TB S. 52). Der Bundesminister für Verkehr hat auch insoweit noch keine Entwürfe vorgelegt. Er hat dies mit den Schwierigkeiten der Materie begründet. Dies überzeugt nicht. Es ist dringend erforderlich, möglichst bald Entwürfe einer Verordnung über die Untersuchung von Flugunfällen oder Störungen beim Betrieb von Luftfahrzeugen sowie einer ergänzenden Verwaltungsvorschrift zu erarbeiten.

9.3 Bundesbahn

9.3.1 Schwarzfahrerdatei

Die Speicherung personenbezogener Daten strafunmündiger Kinder bei Schwarzfahrten im Verbundverkehr durch die Deutsche Bundesbahn nach Zahlung

des erhöhten Beförderungsentgelts hatte ich im Vorjahre beanstandet (vgl. 12. TB S. 52f.). Im Laufe des Berichtsjahres konnte erfreulicherweise in Verhandlungen mit der Deutschen Bundesbahn eine einvernehmliche Lösung gefunden werden. Danach werden die Eltern — entgegen der bisherigen Praxis — bereits in jedem Einzelfall einer festgestellten Schwarzfahrt in einem mit mir abgestimmten Schreiben von der Bundesbahn um Zahlung des erhöhten Beförderungsentgelts sowie um Belehrung ihrer Kinder gebeten. Zugleich wird den Eltern angekündigt, daß die Daten ihrer Kinder nach Abwicklung des Zahlungsvorganges gelöscht werden.

Damit sind meine bisherigen datenschutzrechtlichen Bedenken ausgeräumt. Ich hoffe, daß sich das Verfahren bei allen Verkehrsträgern durchsetzen wird. Die Deutsche Bundesbahn hat mir mittlerweile mitgeteilt, daß es aufgrund der neuen Regelung bisher keine Beschwerden gegeben habe, so daß davon auszugehen ist, daß sie auch von den Betroffenen akzeptiert wird.

9.3.2 Bestellschein „Familien-Paß für kinderreiche Familien"

Die Deutsche Bundesbahn läßt sich — worauf mich ein Petent aufmerksam gemacht hat — auf dem Bestellschein für einen Familien-Paß für kinderreiche Familien von dem Antragsteller die Kindergeldberechtigung u. a. durch Angabe der Kindergeld bewilligenden Stelle und der Kindergeld-Nummer bestätigen. Diese Angaben konnte die Verkaufsstelle in zweifelhaften Fällen durch Rückfrage bei der vom Besteller genannten Kindergeldstelle nachprüfen. Ich habe die Bundesbahn darauf hingewiesen, daß die Kindergeld bewilligenden Stellen zur Einhaltung des Sozialgeheimnisses verpflichtet sind und Auskünfte nur mit ausdrücklicher Zustimmung des Anspruchsberechtigten erteilen dürfen. Die Bundesbahn hat mir daraufhin mitgeteilt, daß die Überprüfung inzwischen eingestellt worden sei; es genüge, daß der Besteller in Zweifelsfällen seine Angaben durch Vorlage einer entsprechenden Bescheinigung der Kindergeld bewilligenden Stelle oder des Familienstammbuchs belege. Auf meine Bitte wird die Bundesbahn diese — datenschutzrechtlich unbedenkliche — Verfahrensweise bei der Neugestaltung des Antragsvordruckes im Jahr 1991 festschreiben.

10 Statistik

10.1 Mikrozensusgesetz

Die Ablösung des im Jahre 1990 auslaufenden Mikrozensusgesetzes von 1985 durch ein neues Gesetz, das Mikrozensuserhebungen für den kommenden Fünf-Jahreszeitraum ermöglicht, war bis zum Ende des Berichtsjahres politisch heftig umstritten. Während die Fachressorts daran interessiert waren, daß die bisher vom Mikrozensus erfaßten Erhebungen in gleicher Weise auch im kommenden Zeitraum fortgeführt werden, versuchte das Bundesministerium des Innern auf der Basis seines Verlängerungsentwurfes, über den ich in meinem 12. Tätigkeitsbericht (S. 55) berichtet habe, einzelne Erhebungsbereiche zu streichen und die Zahl der Erhebungen mit Auskunftspflicht zu reduzieren. Der Bundesrat hat beides kritisiert. Ich habe demgegenüber das Bundesministerium des Innern unterstützt, weil ich in dessen Entwurf einen weiteren begrüßenswerten Schritt in Richtung auf die Freiwilligkeit der Beantwortung statistischer Fragen und zum Verzicht auf nicht unbedingt erforderliche Erhebungsmerkmale erblicke. Ich teile vor allem nicht die im Bundesrat zum Ausdruck gebrachte Sorge der Bundesländer, daß der Verzicht auf die Auskunftspflicht erhebliche Antwortausfälle mit der Folge einer Verzerrung der Statistik nach sich ziehen wird. Jede zwangsweise Inanspruchnahme des Bürgers bei der Erhebung seiner Daten stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung des einzelnen dar; in Übereinstimmung mit dem Volkszählungsurteil des Bundesverfassungsgerichts sollten nur diejenigen Angaben zwangsweise erhoben werden, bei denen der Zweck der Statistik mit freiwilligen Auskünften nicht erreicht werden kann.

Das noch kurz vor Ende der Legislaturperiode zustande gekommene Gesetz zur Änderung des Gesetzes zur Durchführung einer Repräsentativstatistik über die Bevölkerung und den Arbeitsmarkt (Mikrozensusgesetz), dem der Bundesrat nur zugestimmt hat, um den Fortbestand der Mikrozensuserhebung zu gewährleisten, bewegt sich erfreulicherweise in die skizzierte Richtung. Konnten im Gesetz von 1985 vier Erhebungsbereiche freiwillig beantwortet werden, so sind es im neuen Gesetz sechs weitere, nämlich die Fragen nach

- zusätzlichem privaten Krankenversicherungsschutz
- Schulabschluß und Berufsausbildung
- Aufenthaltsdauer und Familienangehörigen bei Ausländern
- Verkehrsmittel und Zeitaufwand für den Weg zur Arbeitsstätte
- Behinderteneigenschaft
- Altersvorsorge und Lebensversicherung.

Hinzu kommt, daß die Gebäude- und Wohnungsstichprobe und die Erhebung zu Urlaubs- und Erholungsreisen weggefallen sind. Schließlich sieht das Gesetz auch die ursprünglich erwogenen Testerhebungen zwecks Prüfung eines verfeinerten Erhebungsverfahrens nicht mehr vor.

Insgesamt sehe ich in dem neuen Mikrozensusgesetz einen datenschutzrechtlich erfreulichen Fortschritt.

10.2 JUSTIS

Die Entwicklungsphase des Justizstatistik-Informationssystems (JUSTIS) des Bundesministers der Justiz (s. 11. TB S. 46) ist mittlerweile abgeschlossen. Das zunächst nur auf die Erfassung von Zivilsachen beschränkte System ist inzwischen auf Strafsachen erweitert worden. Es ist beabsichtigt, künftig auch Daten der Verwaltungsgerichte in das Informationssystem aufzunehmen. Hatten während der Erprobungs-

phase nur der Bundesminister der Justiz und der Justizminister des Landes Nordrhein-Westfalen Zugriff auf die Daten aus JUSTIS, ist diese Möglichkeit nun allen Landesjustizverwaltungen eröffnet worden. Zur Zeit gibt es Überlegungen, im beschränkten Umfange auch der wissenschaftlichen Forschung Zugriffsmöglichkeiten auf Daten aus JUSTIS zu gewähren.

An einer neuerlichen Demonstration des Betriebes von JUSTIS habe ich teilgenommen. Dabei hat sich gezeigt, daß die Anonymität von an Gerichtsverfahren beteiligten Personen nicht hinreichend gesichert ist. Zwar werden die Daten über den Personalstand auf der Ebene der OLG-Bezirke aggregiert, im übrigen werden aber die Angaben über Gerichtsverfahren auf Amtsgerichtsebene ausgewiesen. Dabei können möglicherweise Rückschlüsse auf ein bestimmtes Entscheidungsverhalten eines Richters — mit Hilfe weiterer Quellen — gezogen werden.

Deutlich wurde dies, als während der Demonstration eine Verlaufsstatistik aufgerufen wurde, die die Praxis eines kleinen Amtsgerichts in Entmündigungssachen wegen Trunksucht in den siebziger Jahren darstellte. Anhand des Handbuches der Justiz konnte festgestellt werden, daß ein halbes Jahr, bevor sich an diesem Gericht die Entmündigungen wegen Trunksucht verdreifachten, ein neuer Richter seinen Dienst aufgenommen hatte. Ob dieser Richter mit Entmündigungssachen betraut und für die signifikante Erhöhung der Entmündigungen ursächlich war, kann durch Einsicht in den entsprechenden Geschäftsverteilungsplan dieses Gerichtes geklärt werden.

Nach diesem Ergebnis habe ich gefordert, daß der Zugriff auf das System eingeschränkt wird. Es sollte nur diejenige Justizverwaltung Daten abrufen können, die sie zur Erfüllung ihrer eigenen fachlichen Aufgaben benötigt. Ein Zugriff jeder Landesjustizverwaltung auf den gesamten Datenbestand ist für eine Geschäftsstatistik weder erforderlich noch zweckmäßig. Die Daten sollten auch auf Landgerichtsebene — nicht auf der eines Amtsgerichts — zusammengefaßt werden. Falls derartige Schritte nicht getan werden, muß JUSTIS durch ein entsprechendes Statistikgesetz geregelt werden, da sonst kein ausreichender Schutz für die Betroffenen besteht. Wenn es nämlich Zweck des Systems ist, auf der Grundlage von Einzeldatensätzen statistische Auswertungen über Gerichtsverfahren bundesweit vornehmen zu können und Abrufe aller Justizminister einschließlich des BMJ für Zwecke der Gesetzgebung ermöglicht werden sollen, handelt es sich bei JUSTIS tatsächlich um eine Bundesstatistik. Nach § 5 Abs. 1 Satz 1 Bundesstatistikgesetz dürfen Bundesstatistiken aber grundsätzlich nur durch ein Gesetz angeordnet werden. Ein Statistikgesetz für JUSTIS müßte sicherstellen, daß anfragenden Stellen nur anonymisierte statistische Ergebnisse zugänglich gemacht werden.

10.3 Volkszählung 1987

Wie in meinem Zehnten Tätigkeitsbericht (S. 55) angekündigt, habe ich im Statistischen Bundesamt die Einhaltung des Datenschutzes bei der Übermittlung von Einzelangaben im Zusammenhang mit der Durchführung des Volkszählungsgesetzes 1987 (VZG) kontrolliert. Anhaltspunkte für einen Verstoß gegen datenschutzrechtliche Bestimmungen habe ich nicht festgestellt.

Zur 1%-Stichprobe nach § 14 Abs. 6 VZG habe ich festgestellt, daß bis auf die beiden größten Bundesländer alle Statistischen Landesämter dem Statistischen Bundesamt Einzeldatensätze geliefert haben, die bei jedem Merkmal mit einem jeweils bestimmten Faktor hochgerechnet wurden, um repräsentatives Datenmaterial zu erhalten. Unter den gelieferten Datensätzen befinden sich vermutlich auch solche, die nach § 11 Abs. 1 Satz 1 VZG vervollständigt worden waren, weil die zu Befragenden entweder bei der Erhebung nicht anwesend waren oder die Volkszählung boykottiert hatten. Bei diesen Datensätzen wurden die in § 11 Abs. 1 Satz 1 VZG nicht genannten Merkmale durch ein entsprechendes Merkmal aus einem fremden Datensatz ergänzt. Einige Statistische Landesämter haben diese Datensätze durch ein Kennzeichen markiert. Weil diese Markierung nicht überall erfolgt, gehe ich davon aus, daß die vorgesehenen Sonderaufbereitungen nach § 14 Abs. 6 VZG auch ohne diese Kennzeichnungen vorgenommen werden können. Um die Entstehung einer Datei mutmaßlicher Volkszählungsboykotteure aus den anonymisierten Datensätzen von vornherein unmöglich zu machen, habe ich empfohlen, in der Stichprobe auf die Kennzeichnung vervollständigter Datensätze zu verzichten.

Ich konnte feststellen, daß das Statistische Bundesamt Gemeinden in der Regel keine Einzelangaben nach § 14 Abs. 1 VZG mitteilt. Das Statistische Bundesamt übermittelt und veröffentlicht statistische Ergebnisse nur auf Kreisebene. Angaben, die weniger als fünfzig Einzelfälle betreffen, werden nicht veröffentlicht. Das ist aus meiner Sicht eine erfreuliche datenschutzgerechte Entscheidung. Gegen die beabsichtigte Veröffentlichung der Volkszählungsergebnisse auf Standarddisketten bestehen keine datenschutzrechtlichen Bedenken .

Von der Befugnis nach § 12 Abs. 5 Satz 6 VZG, zur Aktualisierung der im Statistischen Bundesamt geführten Kartei im Produzierenden Gewerbe bestimmte Einzelangaben zu erhalten, hat das Bundesamt keinen Gebrauch gemacht. Die Statistischen Landesämter stellen dem Bundesamt vielmehr die aktualisierte Kartei zur Verfügung, aus der man die auf der Volkszählung beruhenden Bestandteile nicht erkennen kann. Datenschutzrechtliche Probleme habe ich insoweit nicht feststellen können.

10.4 Strafverfolgungsstatistikgesetz

Der Bundesminister der Justiz hat inzwischen den Entwurf eines Strafverfolgungsstatistikgesetzes erneut überarbeitet; den in meinem Zwölften Tätigkeitsbericht (S. 56f.) vorgebrachten Bedenken trägt der Entwurf zum größten Teil Rechnung.

Der ursprünglich gewählte Weg der Übermittlung statistischer Daten an das Bundeszentralregister, gegen den ich im Hinblick auf den verfassungsrechtlich gebotenen Grundsatz der Trennung von Statistik und

Verwaltungsvollzug datenschutzrechtliche Bedenken geäußert hatte, soll nicht mehr beschritten werden. Nunmehr sollen die Geschäftsstellen der Gerichte und Staatsanwaltschaften die erhobenen statistischen Daten unmittelbar an die Statistischen Landesämter übermitteln.

Der Entwurf sieht allerdings immer noch vor, die Geschäftsnummer des Gerichts oder der Staatsanwaltschaft als Hilfsmerkmal zu erheben. Da mit Hilfe der Geschäftsnummer der Zugang zu den Gerichtsakten und damit zur Person des Betroffenen ermöglicht wird, sollte auf dieses Hilfsmerkmal verzichtet werden. Es stellt sich zudem die Frage, ob die Erhebung der Geschäftsnummer bei der zukünftigen elektronischen Erstellung der Mitteilung an die Statistischen Landesämter für die Plausibilitätskontrolle überhaupt noch erforderlich ist.

Ich habe den Bundesminister der Justiz ferner gebeten, auf die von ihm erwogene Vorschrift zu verzichten, wonach an Forschungseinrichtungen für wissenschaftliche Zwecke Angaben über die aktenführende Stelle und die Anzahl der für das Forschungsvorhaben in Betracht kommenden Strafverfolgungsakten übermittelt werden können und zu diesem Zweck die Statistischen Landesämter die entsprechenden Hilfs- und Erhebungsmerkmale für die Dauer von vier Jahren aufbewahren dürfen. Dieses Verfahren widerspricht der auf das Volkszählungsurteil zurückgehenden Verpflichtung, die Hilfsmerkmale nach Abschluß der Plausibilitätsprüfung sogleich zu löschen (§ 12 Abs. 1 Bundesstatistikgesetz).

10.5 EG-Statistikverordnung

Der Rat der Europäischen Gemeinschaften hat die Verordnung über die Übermittlung von unter die Geheimhaltungspflicht fallenden Informationen an das Statistische Amt der Europäischen Gemeinschaften (EG-Statistikverordnung) vom 11. Juni 1990 beschlossen. Der Bundesminister des Innern hat mich bei den Entwurfsberatungen beteiligt. Zu meinem Bedauern konnten nicht alle von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung vom 26./27. Oktober 1989 (s. 12. TB S. 111) vorgebrachten Anregungen und Bedenken berücksichtigt werden.

Die Verordnung ermächtigt die zuständigen nationalen Stellen, dem Statistischen Amt der Europäischen Gemeinschaften auch vertrauliche statistische Daten zu übermitteln, die aufgrund anderer Rechtsvorschriften für bestimmte statistische Zwecke (z. B. für die Produktions-, Industrie- und Außenhandelsstatistik) erhoben worden sind. Die Übermittlung derartiger Daten darf in der Regel nur in einer eine direkte Identifizierung der statistischen Einheiten ausschließenden Weise erfolgen; in — allerdings die Bundesrepublik Deutschland nicht berührenden — Ausnahmefällen ist auch die Übermittlung von statistischen Daten in direkt identifizierbarer Form zulässig. Die von der Datenschutzkonferenz geforderten Sanktionsmöglichkeiten für eine etwaige Verletzung des Statistikgeheimnisses im Bereich der EG gibt es noch nicht. Weiterhin fehlt es immer noch an einer unabhängigen Datenschutzkontrolle auf Gemeinschaftsebene. Immerhin ist die Kommission der Europäischen Gemeinschaften ermächtigt worden, alle erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen zu treffen, um die vertrauliche Behandlung der statistischen Daten zu gewährleisten. Die Mitgliedstaaten ihrerseits sind verpflichtet, bis zum 1. Januar 1992 geeignete Maßnahmen zu treffen, um eine Verletzung des Statistikgeheimnisses — auch durch Personal der EG — ahnden zu können. Die EG-Statistikverordnung stellt einen ersten Schritt für den Datenschutz im Bereich Statistik auf europäischer Ebene dar.

11 Wissenschaft und Forschung

11.1 Kontrolle und Beratung des Bundesarchivs

Im Berichtszeitraum habe ich den Umgang mit personenbezogenen Daten sowie die automatisierte Datenverarbeitung im Bundesarchiv kontrolliert. Im Vordergrund der Prüfung stand der Umgang mit dem seit drei Jahren geltenden neuen Bundesarchivgesetz. Gewichtige datenschutzrechtliche Probleme habe ich nicht feststellen können.

Die Archivierung elektronischer Datenträger, mit der augenblicklich erst begonnen wird, ist noch nicht geregelt. Ich habe darauf hingewiesen, daß hierfür eine adäquate Organisation (von der Eingangsprüfung über die Registrierung bis zur Zuführung zum Archivbestand) geschaffen werden muß. Die Stellungnahme des Bundesarchivs hierzu liegt noch nicht vor.

11.2 Forschungsvorhaben „Anonymisierung"

Das Forschungsvorhaben der Universität Mannheim, das ich in meinem 11. (S. 48) und 12. Tätigkeitsbericht (S. 58) dargestellt hatte, ist im Berichtsjahr abgeschlossen worden. Es wurde von einem projektbegleitenden Beirat betreut, dem auch meine Dienststelle angehört hat. Die Ergebnisse sollen Mitte dieses Jahres in der Schriftenreihe des Statistischen Bundesamtes vorgestellt werden.

Ziel des Forschungsprojektes war es zu klären, wann faktische Anonymisierung i. S. des § 16 Abs. 6 Bundesstatistikgesetz (BStatG) als Voraussetzung der Weitergabe von Einzelangaben durch die Statistischen Ämter an die Wissenschaft angenommen werden kann. Im Rahmen des Forschungsvorhabens wurden 170 000 Einzeldatensätze aus dem Mikrozensus des Landes NordrheinWestfalen unter Fortlassung der Hilfsmerkmale (Name und Anschrift) verwendet. Die Forscher der Universität Mannheim versuchten anschließend, anhand von Zusatzwissen die Personen, denen die Datensätze zuzuordnen waren, zu reidentifizieren. Dabei wurden „Kürschners Gelehrtenkalender 1987" repräsentativ für öffentlich zugängliche Informationsquellen und eine repräsentative sozialwissenschaftliche Erhebung herangezogen. Als Reidentifikationstechniken wurden sowohl einfache Zuordnungsverfahren (Sortier- oder Selektionsroutinen), als auch komplexe Techniken, wie z. B. ein von der Ge-

sellschaft für Mathematik und Datenverarbeitung (GMD) entwickeltes Reidentifikationsverfahren, angewandt.

Bei den Reidentifizierungsversuchen aus dem Gelehrtenkalender (8 000 Fälle) wurden dessen Datensätze 16 unterschiedlichen Vercodungsvarianten unterzogen. Ein einfaches Zuordnungsverfahren führte zu dem Ergebnis, daß 14 Fälle aus dem Gelehrtenkalender den Datensätzen aus dem Mikrozensus zugeordnet wurden. Die Überprüfung dieser Zuordnungen durch den im Rahmen des Forschungsprojekts eingesetzten Treuhänder ergab jedoch, daß nur in vier Fällen tatsächlich Personenidentität vorlag. Bei der Verwendung der sehr viel aufwendigeren Technik der GMD wurden entgegen allen Erwartungen ebenfalls lediglich 14 Zuordnungen gefunden, von denen sich nach der Überprüfung durch den Treuhänder nur drei als korrekt erwiesen. Dieses Ergebnis erstaunt vor allem deshalb, weil nach Feststellung des Treuhänders tatsächlich 53 Personen, deren Daten im Gelehrtenkalender vorhanden waren, auch am Mikrozensus teilgenommen hatten.

Die Reidentifizierungsversuche mit der sozialwissenschaftlichen Erhebung wurden an Hand von 2 685 Fällen durchgeführt. Bei der einfachen Zuordnungstechnik wurden 35 Zuordnungen als angeblich „eindeutig" gefunden. Die Überprüfung durch den Treuhänder ergab allerdings, daß in keinem einzigen Fall die Zuordnung korrekt war. Keine der 10 Personen, die nach Feststellung des Treuhänders sowohl an der sozialwissenschaftlichen Studie als auch am Mikrozensus teilgenommen hatten, wurde somit tatsächlich reidentifiziert. Wegen des damit verbundenen hohen Aufwands und der entsprechenden Kosten wurde auf einen Deanonymisierungsversuch mit der komplexen GMD-Technik verzichtet.

Bei allen Reidentifizierungsversuchen überstiegen die Kosten und der Arbeitsaufwand, der für die Zuordnungen betrieben werden mußte — ohne sicher sein zu können, daß sie erfolgreich waren —, bei weitem den Betrag, der für eine anderweitige Informationsbeschaffung (z. B. durch Befragungen) aufzuwenden gewesen wäre.

Die bisher bekannten Ergebnisse des Forschungsvorhabens zeigen allerdings, daß in besonders gelagerten, sehr seltenen Einzelfällen eine Reidentifizierung mit verhältnismäßig geringem Aufwand nicht ausgeschlossen werden kann. Das ist etwa dann der Fall, wenn gezielt nach einer Person im Datenbestand gesucht wird, die einer sehr kleinen Gruppe angehört (z. B. Bundesminister, Landesbeauftragte für den Datenschutz).

Daher empfiehlt die Forschungsgruppe der Universität Mannheim für die Übermittlung faktisch anonymer Daten zusätzlich:

- Vertragliche Bindung des Empfängers faktisch anonymer Daten, wobei u. a. Einzelheiten der Datennutzung und Nutzungskontrolle, der Datensicherung und Datenlöschung sowie die Verwirkung einer Vertragsstrafe bei Reidentifizierungsversuchen zu vereinbaren sind,
- Geheimhaltung der örtlichen Umsetzung der Stichprobenpläne beim Vollzug der amtlichen Statistik,
- Systemfreie Anordnung der Daten: Eine systematische Anordnung der Datensätze erhöht das Identifikationsrisiko, sofern ein potentieller Angreifer das Organisationsprinzip kennt.
- Vergröberung der regionalen Gliederung und der Erhebungsmerkmale,
- Aggregierung von Einzelangaben,
- Weitergabe nur von Stichproben aus den Erhebungen an die Wissenschaft.

Nach den Ergebnissen der wissenschaftlichen Untersuchung hat es den Anschein, daß „faktische Anonymität" bei der Übermittlung von Einzelangaben aus amtlichen Statistiken an die Wissenschaft i. S. von § 16 Abs. 6 BStatG angenommen werden kann, wenn die vorgenannten Bedingungen eingehalten werden.

Der zuständige Arbeitskreis der Konferenz der Datenschutzbeauftragten des Bundes und der Länder wird im Laufe dieses Jahres das Ergebnis des Forschungsprojekts beraten.

12 Sozialwesen — Allgemeines

12.1 Kinder- und Jugendhilfegesetz

Das Gesetz zur Neuordnung des Kinder- und Jugendhilferechts (Kinder- und Jugendhilfegesetz — KJHG) ist inzwischen verabschiedet worden und am 1. Januar 1991 in Kraft getreten. Meinen Anregungen, über die ich im 12. Tätigkeitsbericht berichtet hatte (S. 62), wurde voll Rechnung getragen und der ursprüngliche Entwurf um ein gesondertes Kapitel bereichsspezifischer Datenschutzregelungen ergänzt.

So wurden

- der Anwendungsbereich der Datenschutzvorschriften festgelegt,
- die Datenerhebung geregelt und der Grundsatz festgeschrieben, daß personenbezogene Daten beim Betroffenen zu erheben sind und ohne dessen Mitwirkung nur in den abschließend aufgeführten Ausnahmefällen erhoben werden dürfen,
- die Datenspeicherung in Akten und auf sonstigen Datenträgern geregelt und die Zulässigkeit der Zusammenführung von Daten, die zur Erfüllung unterschiedlicher Aufgaben erhoben worden sind, eingegrenzt,
- das Zweckbindungsprinzip festgeschrieben und die Offenbarungsbefugnis konkretisiert,
- die Offenbarungsbefugnis zusätzlich im Hinblick auf solche Daten, die im Rahmen persönlicher und erzieherischer Hilfe anvertraut worden sind, begrenzt,
- die Datenlöschung und Datensperrung geregelt,
- das Auskunfts- und Einsichtsrecht der Betroffenen auch für Daten in Akten normiert und

— besondere Datenschutzregelungen für den Bereich der Amtspflegschaft und Amtsvormundschaft getroffen.

Dieses aus der Sicht des Datenschutzes vorbildliche Ergebnis, das auch publizistisch so gewürdigt wurde, ist das Ergebnis einer besonders guten Zusammenarbeit aller Beteiligten im letzten Stadium des Gesetzgebungsverfahrens.

12.2 Grundsatz der Ersterhebung beim Betroffenen

Im Rahmen einer Eingabe hat mich die Frage beschäftigt, ob der Datenerhebung des Sozialleistungsträgers beim Betroffenen Vorrang vor einer Beschaffung seiner Daten bei dritten Stellen, insbesondere im Wege der Amtshilfe, zukommt.

Die Erhebung personenbezogener Daten durch Behörden stellt einen Eingriff in das Recht auf informationelle Selbstbestimmung der betroffenen Bürger dar. Nach dem Volkszählungsurteil des Bundesverfassungsgerichts wäre eine Rechtsordnung nicht verfassungsgemäß, bei der der Bürger nicht mehr erkennen kann, wer was wann und bei welcher Gelegenheit über ihn weiß. Schon dieser Grundsatz erfordert es, Informationen grundsätzlich beim Betroffenen selbst zu erheben. Abweichungen vom Grundsatz der Ersterhebung beim Betroffenen, der inzwischen Eingang in § 62 Abs. 2 KJHG und § 13 Abs. 2 des am 1. Juni 1991 in Kraft tretenden Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes gefunden hat sowie auch von § 60 Abs. 1 Ziff. 1, 2. Alternative SGB I reflektiert wird, bedürfen als Eingriff in das Recht auf informationelle Selbstbestimmung einer normenklaren gesetzlichen Grundlage.

Der Bundesminister für Arbeit und Sozialordnung vertritt demgegenüber die Auffassung, § 60 SGB I enthalte lediglich die Verpflichtung, Tatsachen, die für die Leistung erheblich sind, anzugeben, darüber hinaus aber keine Aussage über die Rangfolge der Erhebung. Die Wege einer Erhebung beim Betroffenen oder bei Dritten seien als gleichberechtigt anzusehen.

Der vom Bundesminister für Arbeit und Sozialordnung übermittelte erste Entwurf einer Neuregelung der datenschutzrechtlichen Vorschriften des Sozialgesetzbuches, der vor allem dessen Weiterentwicklung unter Berücksichtigung des neuen Bundesdatenschutzgesetzes dienen soll, hat das Problem aufgegriffen. Der Vorschlag des Entwurfs bedarf noch einer eingehenden Erörterung.

12.3 Offenbarung von Gesundheitsdaten der Versicherten durch Sozialleistungsträger in sozialgerichtlichen Verfahren

In einer Eingabe wurde ich um datenschutzrechtliche Bewertung folgenden Sachverhalts gebeten: In einem Rechtsstreit vor dem Sozialgericht wegen der Weitergewährung einer Verletztendauerrente hatte die beklagte Berufsgenossenschaft ärztliche Stellungnahmen von nicht bei ihr beschäftigten Ärzten zu den vom Gericht veranlaßten Sachverständigengutachten eingeholt, obwohl die Petentin der Offenbarung ihrer bei der Begutachtung gewonnenen Daten ausdrücklich widersprochen hatte. Der Hauptverband der gewerblichen Berufsgenossenschaften e. V. sah diese Offenbarung in einer Stellungnahme mir gegenüber als nach § 69 Abs. 1 Nr. 1 SGB X zulässig an; die Einschränkung des § 76 SGB X komme nicht zum Zuge, da die Voraussetzungen für eine Offenbarung nach § 203 StGB vorlägen. Dem Anspruch der Berufsgenossenschaft auf rechtliches Gehör gebühre Vorrang vor dem Interesse der Petentin auf Geheimhaltung ihrer medizinischen Gutachtendaten.

Ich habe die Weitergabe medizinischer gerichtlicher Gutachten durch Sozialversicherungsträger während des Sozialgerichtverfahrens an externe Gutachter gegen den Widerspruch des Betroffenen als unzulässig bewertet und mich damit im Ergebnis der Stellungnahme des Bundesversicherungsamtes und dem Urteil des Sozialgerichts Duisburg angeschlossen, vor dem der Rechtsstreit anhängig war. Zur Begründung habe ich ausgeführt, daß dahingestellt bleiben könne, ob die Zulässigkeit der Offenbarung bereits deswegen an § 69 Abs. 1 Nr. 1 SGB scheitert, weil die Offenbarung für die Aufgabenerfüllung der Berufsgenossenschaft nicht erforderlich ist. Denn der Widerspruch des Betroffenen macht die Weitergabe des Gutachtens durch die Berufsgenossenschaft nach § 76 SGB X unzulässig. Es liegt insbesondere keine der Voraussetzungen vor, unter denen Ärzte ausnahmsweise nicht durch das Patientengeheimnis im Sinne des § 203 Abs. 1 StGB an einer Offenbarung gehindert sind.

Eine Verletzung des Anspruchs der anderen Prozeßpartei auf rechtliches Gehör tritt dadurch nicht ein. Nach § 62 Sozialgerichtsgesetz hat jeder Prozeßbeteiligte Anspruch darauf, rechtserhebliche Begutachtungsdaten durch sachverständige Gutachter prüfen zu lassen. Wird dies durch den Widerspruch des Betroffenen unmöglich gemacht, so ist die Verwertung des Gutachtens als Beweismittel nicht zulässig. Dies geht, wie das Sozialgericht Duisburg zu Recht festgestellt hat, zu Lasten desjenigen, der die Darlegungslast trägt.

In diesem Zusammenhang habe ich erneut die Auffassung vertreten, daß der Betroffene über die Absicht der Übersendung des Gutachtens an außenstehende Dritte und seine Widerspruchsmöglichkeit nach § 76 Abs. 2 SGB X aufzuklären ist; widrigenfalls ist eine Offenbarung unzulässig, auch wenn der Betroffene (noch) nicht ausdrücklich widersprochen hat (vgl. 9. TB S.49ff.). Diese Auffassung entspricht auch der des Innenausschusses des Deutschen Bundestages der erklärt hat, das Widerspruchsrecht nach § 76 Abs. 2 SGB X könne nur wahrgenommen werden, wenn der Betroffene von der beabsichtigten Offenbarung wisse (BT-Drucksache 10/1719).

12.4 Doppelfunktion des internen Datenschutzbeauftragten

Eine Eingabe richtete sich dagegen, daß bei einer Betriebskrankenkasse deren stellvertretender Ge-

schäftsführer gleichzeitig die Funktion des internen Datenschutzbeauftragten ausübte. Die sich aus dieser Doppelfunktion ergebende Interessenkollision und die damit möglicherweise nicht mehr gewährleistete Unabhängigkeit der Aufgabenwahrnehmung des Datenschutzbeauftragten haben mich veranlaßt, der betroffenen Krankenkasse eine Neuorganisation zu empfehlen. Ein interner Datenschutzbeauftragter muß, will er seiner Aufgabenstellung gerecht werden, u. U. auch mit aller Entschiedenheit auf der strikten Einhaltung der gesetzlich definierten Grenzen für die Verarbeitung und Nutzung personenbezogener Daten bestehen. Leitende Mitarbeiter einer Krankenkasse haben auch andere Gesichtspunkte zu berücksichtigen, deren Verwirklichung auf Zielkonflikte mit dem Datenschutz stoßen kann. Deshalb besteht die Gefahr, daß diese Gesichtspunkte schon in die datenschutzrechtliche Bearbeitung einfließen, wenn ein leitender Mitarbeiter die Aufgabe des Datenschutzbeauftragten wahrnimmt. Hinzu kommt, daß der interne Datenschutzbeauftragte bei der ordnungsgemäßen Erledigung seiner Beratungs- und Kontrollaufgaben auch Kenntnis von personenbezogenen Daten der Kassenmitarbeiter erhalten kann. Soweit es sich dabei um deren Versichertendaten handelt, dürfen diese gemäß § 284 Abs. 4 SGB V Personen, die kasseninterne Personalentscheidungen treffen oder daran mitwirken können, nicht zugänglich sein oder diesen Personen von Zugriffsberechtigten offenbart werden.

Da mit der Funktion eines stellvertretenden Geschäftsführers stets auch Personalkompetenzen verbunden sind, ist die Verbindung mit dem Amt des internen Datenschutzbeauftragten auch unter diesem Aspekt unzulässig.

Die betroffene Krankenkasse hat auf meine Anregung hin den bisherigen internen Datenschutzbeauftragten abberufen und den Innenrevisor der Kasse mit diesen Aufgaben betraut. Dies ist eine akzeptable Lösung, die auch häufig praktiziert wird.

13 Arbeitsverwaltung

— Kontrolle eines Arbeitsamtes —

Die im Laufe des Berichtsjahres durchgeführte Kontrolle in einem Arbeitsamt erbrachte folgende Ergebnisse:

— Im Verfahren „coArb" der Arbeitsvermittlung waren u. a. die folgenden Äußerungen einer Petentin gegenüber ihrem Arbeitsvermittler gespeichert: „Der Arbeitsberater solle sich bitte um seine Langzeitarbeitslosen kümmern.", „Stasi-Methoden". Der Beratungsvermerk eines Maßnahmeteilnehmers enthielt die Aussage „Wegen destruktiven und unsozialen Verhaltens kann eine weitere Teilnahme . . . den anderen Teilnehmern nicht mehr zugemutet werden."

  Gemäß § 79 Abs. 1 Satz 1 SGB X in Verbindung mit § 9 Abs. 1 BDSG ist das Speichern personenbezogener Daten zulässig, wenn es zur rechtmäßigen Erfüllung in der Zuständigkeit der speichernden Stelle liegender Aufgaben erforderlich ist.

  Die Erforderlichkeit der Speicherung der genannten personenbezogenen Daten für eine spätere Vermittlung in eine Arbeit konnte mir von den Vertretern der Bundesanstalt für Arbeit nicht hinreichend begründet werden. Die spontanen Unmutsäußerungen der Petentin, deren persönliche Unzufriedenheit sich bereits aus dem übrigen Wortlaut der Beratungsvermerke ergab, enthalten keine grundsätzliche Aussagekraft für die Beurteilung der fachlichen oder persönlichen Eignung der Arbeitssuchenden. Sie können erfahrungsgemäß die schlechte Gesprächsatmosphäre kennzeichnen, die wiederum von beiden Gesprächspartnern beeinflußt sein kann. Die Eintragung „destruktives und unsoziales Verhalten" beinhaltet eine pauschale negative Kennzeichnung des Betroffenen. Da der Gesamtinhalt des individuellen Beratungsgespräches nur der beteiligten Vermittlungsfachkraft bekannt wird und diese ihn unter Zugrundelegung persönlicher subjektiver Maßstäbe zusammenfaßt, besteht die Gefahr, daß ein Stellvertreter oder Nachfolger des Vermittlers dem Betroffenen voreingenommen gegenübertritt. In diesem Zusammenhang ist auch zu berücksichtigen, daß der Personenkreis der zugriffsberechtigten Mitarbeiter durch die Einführung des Systems „coArb" faktisch auf alle Mitarbeiter der Vermittlungsabteilung erweitert worden ist.

  Die Bundesanstalt für Arbeit beurteilt diese Beratungsnotizen als für ihre Arbeit unentbehrlich. Die wörtlich wiedergegebenen Äußerungen enthielten u. a. vermittlungsrelevante Informationen zum Verhalten der Arbeitsuchenden im Rahmen von Vorstellungsgesprächen bei Arbeitgebern.

  Mit dieser Haltung setzt die Bundesanstalt sich in Gegensatz zu einer bundesweit geltenden Verwaltungsvorschrift, mit der sie das Verfahren der Erhebung und Speicherung personenbezogener Daten in der Abteilung Arbeitsvermittlung/Arbeitsberatung grundsätzlich datenschutzgerecht geregelt hat. Danach dürfen Arbeit- und Ratsuchende nicht negativ gekennzeichnet werden. Subjektive Eindrücke und Wertungen sind nicht in Dateien festzuhalten. Die oben dargestellte Praxis ist mit diesen Regelungen nicht zu vereinbaren.

  Die Bundesanstalt hat zwar meine Feststellungen zum Anlaß genommen, die betroffenen Führungskräfte noch einmal auf die Problematik hinzuweisen; das Thema soll außerdem in das Schulungskonzept für die Mitarbeiter aus dem Beitrittsgebiet aufgenommen werden. Eine verbindliche Zusicherung, die Speicherungspraxis im System „coArb" künftig strikt an den eindeutigen Vorschriften ihres Runderlasses auszurichten und Notizen der oben dargestellten Art nicht mehr vorzunehmen hat die BA mir allerdings bisher nicht erteilt. Ich werde kontrollieren, ob die Bundesanstalt die mit ihrer eigenen Verwaltungsvorschrift unvereinbare Praxis fortsetzt und gegebenenfalls auf deren Änderung dringen.

— Im Rahmen der Kontrolle wurde weiterhin festgestellt, daß Inhalte einzelner Beratungsvermerke im System „coArb" von der zuständigen Vermittlungsfachkraft nicht gelöscht werden können. Es besteht lediglich die Möglichkeit, Korrekturvermerke zu speichern; in Ausnahmefällen kann das gesamte Bewerberangebot gelöscht und anschließend verändert wieder eingegeben werden. Die Bundesanstalt begründet dieses Verfahren mit dem dokumentarischen Wert der Beratungsinhalte. Außerdem sollen Manipulationen ausgeschlossen werden.

Ich habe diese Regelung unter Berücksichtigung der Vorschrift des § 84 SGB X als datenschutzrechtlich problematisch beurteilt. Danach ist jeder Sozialleistungsträger verpflichtet, personenbezogene Daten zu löschen, soweit ihre Kenntnis zur rechtmäßigen Erfüllung seiner Aufgaben nicht mehr erforderlich ist und kein Grund zu der Annahme besteht, daß durch die Löschung schutzwürdige Belange des Betroffenen beeinträchtigt werden. Löschen bedeutet gemäß § 2 Abs. 2 Ziff. 4 BDSG das Unkenntlichmachen gespeicherter Daten (ebenso § 3 Abs. 5 Nr. 5 BDSG neu). In Fällen eines Löschungsgebotes muß die speichernde Stelle deshalb einen Zustand herstellen, in dem sie die betreffende Information nicht mehr aus von ihr gespeicherten Daten gewinnen kann.

Das Verfahren „coArb" erfüllt die Voraussetzungen für ein Löschen nicht. Auch in Fällen, in denen sich nachträglich herausstellt, daß nicht erforderliche oder unrichtige personenbezogene Daten gespeichert wurden, lassen diese sich nicht unkenntlich machen. Daraus können Nachteile für Betroffene entstehen.

Die bestehende Löschungsmöglichkeit des gesamten Bewerberangebotes ist im Regelfall nicht durchführbar und wird nur ausnahmsweise praktiziert. Um der Löschungspflicht nach § 84 SGB X nachkommen zu können, müssen folglich differenzierende technische und organisatorische Maßnahmen im Sinne des § 6 Abs. 1 BDSG und der Anlage dazu vorgesehen werden.

Ich habe daher dringend empfohlen, Löschungsmöglichkeiten auch für einzelne Vermerke vorzusehen. Soweit diese aus Beweissicherungsgründen dem Arbeitsberater/Hauptvermittler selbst nicht eingeräumt werden soll, habe ich angeregt, geeignete Mitarbeiter — etwa den fachlich zuständigen Abschnitts- oder Abteilungsleiter — mit Löschungsbefugnissen auszustatten, wie dies in anderen Bereichen der Sozialverwaltung bereits praktiziert wird.

— Anhand von vier Einzelfällen habe ich ferner die internen Zugriffsmöglichkeiten auf Daten von Mitarbeitern eines Arbeitsamtes überprüft, die vorher Leistungen von diesem Arbeitsamt erhalten haben.

Im Falle der Einstellung früherer Leistungsempfänger durch das Arbeitsamt wird eine Sperrung der im *System coLei* gespeicherten Leistungsdaten, mit Ausnahme einiger Stammdaten, für die Dauer der Beschäftigung in der Dienststelle veranlaßt. Die Prüfung bestätigte die ordnungsgemäße Sperrung der Leistungsdaten.

Zugriffsmöglichkeiten auf die in den *Leistungsakten* dieser Mitarbeiter gespeicherten personenbezogenen Daten hatten zum Zeitpunkt der Kontrolle insbesondere die ca. 15 bis 20 Mitarbeiter der zuständigen Leistungsgruppe. Da hinsichtlich der Leistungsakten von Mitarbeitern von einem höheren Mißbrauchsrisiko ausgegangen werden muß, habe ich empfohlen, die Anzahl der Mitarbeiter, die Einblick in die Leistungsakten von Mitarbeitern nehmen dürfen, zu verringern. Auch sollten für solche Leistungsakten zusätzliche Sicherungsmaßnahmen vorgesehen werden, etwa durch zentrale Aufbewahrung einer begrenzten Anzahl von Leistungsakten bei einem bestimmten Mitarbeiter der Leistungsabteilung. Zugriffe sollten jeweils dokumentiert werden und nur mit besonderer Begründung möglich sein.

Daraufhin hat die Bundesanstalt für Arbeit diese Thematik in einem bundesweiten Runderlaß neu geregelt. Nach diesem sind die Leistungsakten von Mitarbeitern, die ehemals Leistungsempfänger waren, beim zuständigen Gruppen-/Abschnittsleiter aufzubewahren. Eine Dokumentation der Zugriffe auf diese Daten ist nicht vorgesehen.

Unter Hinweis auf den Inhalt des § 284 Abs. 4 Gesundheitsreformgesetz sowie die Neufassung des § 35 SGB I aufgrund des Rentenreformgesetzes habe ich gegen die neue Regelung erhebliche datenschutzrechtliche Bedenken vorgetragen. Nach den vorgenannten gesetzlichen Regelungen dürfen Personen, die Personalentscheidungen treffen „oder daran mitwirken können", nicht auf die personenbezogenen Daten der Beschäftigten zugreifen können. Ich habe weiterhin darauf hingewiesen, daß auch der Arbeits- und Sozial-Ausschuß des Deutschen Bundestages in seiner Stellungnahme zu meinem 8. und 9. Tätigkeitsbericht davon ausgeht, daß weder dem Arbeitgeber selbst noch einem anderen Vorgesetzen, noch einem Angehörigen der Personalverwaltung Kenntnisse von personenbezogenen Daten eines Betriebsangehörigen offenbart werden dürfen, die dem Sozialgeheimnis unterliegen (vgl. BT-Drucksache 11/8200, S. 5).

Ich habe deshalb empfohlen, die Leistungsakten der Mitarbeiter zentral bei einem Sachbearbeiter der Leistungsgruppe oder der Widerspruchstelle aufzubewahren und in Zweifelsfällen den Leiter der Widerspruchstelle entscheiden zu lassen. Unter der Voraussetzung, daß dieses Verfahren sichergestellt ist, kann nach meiner Auffassung auf die sonst notwendige Protokollierung der Zugriffe auf die in den Akten enthaltenen Leistungsdaten verzichtet werden.

Die Bundesanstalt für Arbeit hat zugesagt, meinem Anliegen zu entsprechen und will das Verfahren in meinem Sinne regeln.

— Auch das Verfahren der Aufbewahrung amtsärztlicher Gutachten in Leistungsakten habe ich mir näher angesehen. Bei der Prüfung einiger Leistungsakten wurde festgestellt, daß sich in den Akten jeweils Durchschläge des Vordrucks „Antrag auf ärztliche Begutachtung" sowie des Vordrucks „Ärztliches Gutachten" befanden. Die ärztlichen Gutachten enthielten u. a. detaillierte ärztliche Diagnosen sowie Angaben über Gesundheitsstörungen.

Begründet wurde dies damit, daß der Sachbearbeiter der Leistungsabteilung die Stellungnahme des Ärztlichen Dienstes zur Entscheidung über die Verfügbarkeit und eine etwaige Sperrzeit benötige. In diesem Zusammenhang überprüfe er u. a. die Plausibilität der von der Abteilung Arbeitsvermittlung/Arbeitsberatung an den Ärztlichen Dienst gestellten Fragen.

Das Speichern personenbezogener Daten ist gemäß § 79 Abs. 1 Satz 1 SGB X i. V. m. § 9 Abs. 1 BDSG nur in dem Umfang zulässig, in dem es zur rechtmäßigen Erfüllung der Aufgaben der jeweiligen Stelle erforderlich ist. Unter Berücksichtigung des „funktionalen Behördenbegriffs" (vgl. u. a. Urteil des Oberverwaltungsgerichts für die Länder Niedersachsen und Schleswig-Holstein vom 12. Januar 1989 in RDV 1989, Heft 5/6) dürfen nach Maßgabe der am 1. Januar 1992 in Kraft tretenden Ergänzung des § 35 Abs. 1 Satz 2 SGB I auch intern den verschiedenen Stellen eines Leistungsträgers nur diejenigen personenbezogenen Daten zugänglich gemacht werden, die diese zur Erledigung ihrer speziellen Aufgabe benötigen.

Detaillierte Angaben über Gesundheitsstörungen oder ärztliche Diagnosen (z. B. „Zustand nach Milzentfernung, Hüftgelenksverschleiß rechts mit Schmerzen, Rücken- und Gelenkverschleiß mit Schmerzsymptomatik, chronisch asthmoide Bronchitis bei Lungenemphysem") sind für die Aufgabenerfüllung der Leistungsverwaltung nicht erforderlich. Auch ist zu beachten, daß dem Sachbearbeiter der Leistungsabteilung medizinische Kenntnisse im Regelfall fehlen; eine sachgerechte Auswertung der ärztlichen Feststellungen dürfte ihm kaum möglich sein. Ich habe empfohlen, auf eine Mitteilung dieser Daten an die Leistungsabteilung (beispielsweise durch Reduzierung der Felder in der für die Leistungsabteilung bestimmten Durchschrift) künftig zu verzichten.

Die Hauptstelle der Bundesanstalt für Arbeit hält demgegenüber die Kenntnis von amtsärztlichen Diagnosen und Gesundheitsstörungen auch für die Arbeit der Leistungsabteilung (etwa als Grundlage für eine geänderte Leistungsbemessung) für erforderlich. Sie hat sich daher gegen eine Reduzierung der Angaben im Arztgutachten ausgesprochen.

— Aus Anlaß früherer Eingaben habe ich mich mit der Verwendung überholter Vordrucke beschäftigt. So enthielt der Vordruck KG 13 a („Auskunftsersuchen nach § 19 des Bundeskindergeldgesetzes") in der Auflage 12/84 die mit dem Ausforschungsverbot des § 1758 BGB unvereinbare Frage nach einer Adoption. Auf meine Initiative hin hatte die Hauptstelle der Bundesanstalt für Arbeit die Arbeitsämter in mehreren Runderlassen angewiesen, die seit Januar 1986 überholte alte Auflage des o. a. Vordrucks nicht mehr zu verwenden.

Aufgrund einer erneuten Eingabe wurde ich darauf aufmerksam, daß der überholte und durch eine korrigierte Neuauflage ersetzte Vordruck in einem anderen Arbeitsamt auch noch im Jahre 1989 verwendet wurde. Die Bundesanstalt für Arbeit räumte dies ein und teilte mir mit, es handele sich um einen bedauerlichen Einzelfall.

Ich habe daraufhin die Verwendung des Vordrucks auch 1990 überprüft. In den überprüften 13 Kindergeldakten wurde der angesprochene Vordruck in acht Fällen seit dem Januar 1986 verwandt. Ich habe festgestellt, daß in vier dieser insgesamt acht relevanten Fälle der überholte Vordruck, Auflage 12/84, von verschiedenen Mitarbeitern des Arbeitsamts ausgegeben worden war (u. a. noch im Juli 1989 sowie im Februar 1990). Eine Überprüfung der Vordruckbestände im Materiallager sowie in zwei Leistungsstellen ergab keinerlei Hinweise auf eine weitere Aufbewahrung der überholten Auflage.

Nach diesen Feststellungen im Arbeitsamt handelte es sich bei der Verwendung des überholten Vordrucks im Eingabefall also nicht — wie die Bundesanstalt erklärt hatte — um einen Einzelfall. Ich habe dies als Verstoß gegen eine andere Vorschrift über den Datenschutz — hier gegen das in § 1758 BGB verankerte Ausforschungsverbot — beanstandet.

Ich habe der Bundesanstalt für Arbeit dringend empfohlen, das Verfahren — insbesondere in Fällen alter Vordrucke mit unzulässigem Inhalt — so zu ändern, daß derartige Vordrucke mit sofortiger Wirkung nicht mehr verwendet werden.

Die Bundesanstalt für Arbeit hat daraufhin ihre nachgeordneten Dienststellen angewiesen, über den Vollzug der Aussonderung der Auflage 12/84 des Vordrucks zu berichten. Sie hat mir im übrigen mitgeteilt, sie beabsichtige, ihr Vordruckwesen im Sinne einer stärkeren Zentralisierung neu zu regeln. Ein entsprechendes Projekt sei bereits angelaufen, mit ersten Ergebnissen sei Mitte 1991 zu rechnen.

Ich habe diese Absicht begrüßt und werde die weitere Entwicklung aufmerksam verfolgen.

14 Krankenversicherung

14.1 Einzelfragen des Gesundheits-Reformgesetzes (SGB V)

Bei der Umsetzung des Gesundheits-Reformgesetzes in die Praxis haben sich einige Zweifelsfragen ergeben, die ich mit dem BMA, teilweise auch mit den Spitzenverbänden der Krankenkassen und der Kas-

senärztlichen Bundesvereinigung, erörtert habe. Dabei wurden folgende Ergebnisse erzielt:

— Gegenstand zahlreicher Eingaben und öffentlicher Erörterung war im Berichtszeitraum die bis zum Inkrafttreten des Gesundheits-Reformgesetzes zulässige Praxis der Angabe von *Diagnosen auf Krankenscheinen* und ihrer Übermittlung mit diesen an kassenärztliche Vereinigungen und Krankenkassen. Das Gesundheits-Reformgesetz enthält keine eindeutige Befugnisnorm für die Offenbarung von Diagnosen in diesem Zusammenhang; das hat zu Meinungsverschiedenheiten darüber geführt, ob eine solche Angabe eine Verletzung des nach § 203 StGB geschützten Patientengeheimnisses darstellt.

  Bei meiner Erörterung des Problems mit dem Bundesminister für Arbeit und Sozialordnung und Vertretern der Spitzenverbände der Krankenkassen und der Kassenärztlichen Bundesvereinigung hat sich als übereinstimmende Auffassung ergeben, daß Diagnoseangaben auf Krankenscheinen zur Beschreibung der ärztlichen Leistung im Sinne des § 295 Abs. 1 SGB V jedenfalls insoweit erforderlich sein können, als sich diese nicht oder nicht mit hinreichender Deutlichkeit aus der Leistungsbeschreibung im Gebührenverzeichnis für ärztliche Leistungen ergeben. Dasselbe gilt für die Abrechnung von Sonderleistungen.

  Der Bundesminister für Arbeit und Sozialordnung hat zur Klarstellung eine entsprechende Ergänzung des § 295 Abs. 1 SGB V in Aussicht gestellt. Die Spitzenverbände der Krankenkassen und die kassenärztliche Bundesvereinigung haben zugesagt, entsprechend der ihnen in Absatz 3 dieser Vorschrift eingeräumten Befugnis die Übermittlungspflichten der Ärzte so schnell wie möglich im einzelnen festzulegen. Daraufhin habe ich mich bereit erklärt, eine entsprechend begrenzte und unter den vorerwähnten Gesichtspunkten plausible Übermittlungspraxis bis zu der ins Auge gefaßten kurzfristigen Gesetzesänderung datenschutzrechtlich zu tolerieren. Im übrigen wird dieses Abrechnungsverfahren mit der Einführung der Krankenversichertenkarte, die ab 1. Januar 1992 den Krankenschein ersetzen soll, ohnehin geändert (vgl. Bilanz Nr. 33).

— Die *Übersendung von Krankenhausentlassungsberichten (sog. Arztbriefe) an die Krankenkassen* ist mit § 301 SGB V nicht vereinbar, soweit die Berichte Daten enthalten, die über den gesetzlichen Datenkatalog hinausgehen. Die von den Krankenkassen gewünschte Prüfung ihrer Leistungspflicht kann durch Einschaltung des Medizinischen Dienstes nach §§ 275, 276 SGB V ermöglicht werden. Im Hinblick darauf, daß § 276 Abs. 4 SGB V es dem Medizinischen Dienst ohnehin erlaubt, im Einzelfall in den Krankenhäusern die Krankenunterlagen einzusehen, kann als Kompromißlösung für die Übergangszeit eine Übersendung von Krankenhausentlassungsberichten in dem unbedingt erforderlichen Umfang an den Medizinischen Dienst toleriert werden. Der BMA hat auch insoweit eine einzelfallbezogene gesetzliche Klarstellung — etwa in § 276 Abs. 2 oder 4 SGB V zugesagt.

— Zulässigkeit der *Datenübermittlung zur Durchführung von Qualitätsprüfungen* (§§ 136, 298 SGB V)

  Die gesetzliche Regelung des GRG bedarf insoweit ebenfalls einer Klarstellung, um eine eindeutige Befugnis für die notwendige Übermittlung personenbezogener Daten zu schaffen. Mit dem BMA besteht Einigkeit darüber, § 298 SGB V etwa wie folgt zu ergänzen: „Im Rahmen eines Prüfverfahrens ist die versichertenbeziehbare Übermittlung von Angaben über ärztliche oder ärztlich verordnete Leistungen zulässig, soweit die Wirtschaftlichkeit *oder Qualität* der ärztlichen Behandlungs- oder Verordnungsweise im Einzelfall zu beurteilen ist".

Der kurz vor Redaktionsschluß bei mir eingegangene erste Entwurf eines Gesetzes zur Änderung von Vorschriften des Sozialgesetzbuches enthält u. a. Vorschläge zur Regelung dieser Fragen, die zum Teil noch einer vertiefenden Erörterung bedürfen.

14.2 Studentische Krankenversicherung

— Fragen zur Beurteilung des Versicherungsverhältnisses —

Durch das Gesundheits-Reformgesetz (SGB V) wurde in § 5 Abs. 1 Nr. 9 SGB V die Dauer der Krankenversicherungspflicht von Studenten im Regelfall auf den Abschluß des 14. Fachsemesters, längstens aber die Vollendung des 30. Lebensjahres beschränkt. Darüber hinaus sind Studenten nur dann versicherungspflichtig, wenn die Art der Ausbildung oder familiäre sowie persönliche Gründe, insbesondere der Erwerb der Zugangsvoraussetzungen in einer Ausbildungsstelle des 2. Bildungsweges, die Überschreitung der Altersgrenze oder eine längere Fachstudienzeit rechtfertigen. Ein Petent hatte sich in einer Eingabe darüber beschwert, daß ihm auch Fragen nach studienverlängernden Gründen gestellt worden waren, obwohl er weder das 14. Fachsemester noch das 30. Lebensjahr erreicht hatte.

Ich habe gegenüber der betroffenen Krankenkasse darauf hingewiesen, daß die Fragen nach studienverlängernden Gründen nur dann zu beantworten sind, wenn die vorgenannten Zeitgrenzen überschritten sind, und daß hierauf im Fragebogen zur Prüfung der Versicherungspflicht von Studenten aufmerksam zu machen ist. Als bessere Alternative sollte für diesen Personenkreis ein gesonderter Vordruck entwickelt und verwendet werden. Eine Antwort der Krankenkasse stand bei Redaktionsschluß noch aus.

14.3 Fragebogen zur Prüfung der Familienversicherung

Aufgrund der Eingabe einer Petentin, die sich durch einzelne an ihren Sohn gerichtete Fragen über die Einkommens- und Versicherungsverhältnisse der El-

tern „ausgeforscht" sah, habe ich mich mit dem Fragebogen zur Prüfung der Familienversicherung befaßt. Im Hinblick auf das in § 1758 BGB enthaltene Ausforschungsverbot habe ich die in dem von der betroffenen Krankenkasse verwendeten Fragebogen enthaltene differenzierende Fragestellung nach leiblichen Eltern/Adoptiveltern zur Klärung des Anspruches nach § 10 Abs. 1 i. V. m. Abs. 3 SGB V als Risiko für die Wahrung des Adoptionsgeheimnisses bewertet. Ich habe gemeinsam mit der von dem Eingabevorgang betroffenen Krankenkasse eine Formulierung erarbeitet, die das Mißverständnis vermeiden soll, der betroffene Familienangehörige hätte den Status seiner Eltern — ob leibliche oder Adoptiveltern — zu offenbaren.

Ich habe auch gegenüber den Spitzenverbänden der Krankenkassen auf diese Problematik hingewiesen und darum gebeten, daß bei der Gestaltung von Fragebögen zur Prüfung der Familienversicherung auch nur der Anschein einer Verpflichtung vermieden wird anzugeben, ob die Eltern Adoptiveltern sind.

14.4 Information der Versicherten und behandelnden Ärzte über Kosten der ärztlichen Behandlung und Arzneikosten

Die Betriebskrankenkasse (BKK) Mercedes-Benz beabsichtigt, durch regelmäßige Informationen ihrer Versicherten und Ärzte über die Kosten für ärztliche Behandlungen und Arzneimittel deren Kostenbewußtsein zu fördern und mehr Transparenz in das Kostengeschehen zu bringen.

Unter Berücksichtigung der Regelung des § 305 SGB V habe ich gegen das beabsichtigte Informationsverfahren keine datenschutzrechtlichen Bedenken erhoben, soweit sichergestellt ist, daß Versicherte und Ärzte jeweils nur über ihre eigenen Daten unterrichtet werden. Die BKK hat entsprechend folgende Bestimmung in ihre Satzung aufgenommen:

„Soweit verfügbar, erteilt die Betriebskrankenkasse dem Versicherten auf Antrag oder im Rahmen besonderer Maßnahmen auch Gruppen von Versicherten Auskunft über die Art und die Kosten der gewährten Leistungen.

Bei Einzelanträgen soll der Versicherte den oder die in Anspruch genommenen Leistungserbringer angeben."

Ich würde mich freuen, wenn andere Krankenkassen diesem Beispiel folgen würden.

15 Rentenversicherung

— Kontrolle der Bundesversicherungsanstalt für Angestellte —

Im Gesetzgebungsverfahren zum Rentenreformgesetz 1992 wurde auch die Frage heftig diskutiert, ob die in § 148 Abs. 3 SGB VI enthaltene Rahmenregelung über die Möglichkeit der Einrichtung von Online-Verbindungen mit ausländischen Leistungsträgern im Hinblick auf den unterschiedlichen Datenschutzstandard in den Empfängerstaaten mit datenschutzrechtlichen Grundsätzen vereinbar ist (vgl. 12. TB S. 69 ff.).

Ich habe dies zum Anlaß genommen, eine Kontrolle der seit einiger Zeit bestehenden Online-Verbindung zwischen der BfA und der Pensionsversicherungsanstalt (PVAngG) Wien durchzuführen. In diesem Verfahren wird der PVAng ein Direktzugriff auf Konten von Versicherten der BfA eingeräumt. Hierüber habe ich bereits in meinem 6. TB S. 33 berichtet.

Ich konnte feststellen, daß die BfA die Möglichkeit eines Direktzugriffs — wie schon bei der Einrichtung vorgesehen — immer von der Vorlage einer Einwilligungserklärung des Betroffenen bei der PVAng abhängig macht. Durch entsprechende Zugriffssicherungen wird auch gewährleistet, daß nur bestimmte, speziell befugte Mitarbeiter der österreichischen Pensionsversicherungsanstalt für Angestellte die Zugriffsmögkeit haben. Zudem werden entsprechende automatisierte Abrufe dokumentiert. Stichproben haben ergeben, daß Direktzugriffe auf die Datenbestände der BfA nur aus solchen Anlässen durchgeführt worden waren, die von dem gegenseitigen Sozialversicherungsabkommen gedeckt sind. Die Direktabfrage ist auch nur im erforderlichen Umfang möglich. So werden z. B. bei einer Online-Abfrage die gespeicherten Entgeltangaben aus dem Versicherungsverlauf unterdrückt, also nicht mitübermittelt.

Bei der in den meisten Fällen auch noch erforderlichen schriftlichen Übermittlung der Daten wurde diese Einschränkung hingegen nicht beachtet. Ich habe darauf hingewirkt, daß bei der Übersendung von Versicherungsverläufen — soweit diese als ergänzender Nachweis erforderlich sind (z. B. für das Rentenverfahren) — künftig nicht erforderliche Angaben nicht mehr übermittelt werden. Die BfA hat eine Änderung der entsprechenden Verfahrensweise zugesagt.

Die o. g. Inhalte datenschutzrechtlicher Anforderungen, insbesondere die Zugriffssicherheit und -dokumentation sowie die Begrenzung der übermittelten Daten auf das für die Aufgabenerfüllung des Versicherungsträgers des anderen Vertragsstaates erforderliche Maß habe ich in Abstimmung mit dem Bayerischen Landesbeauftragten für den Datenschutz auch für die neu eingerichtete, sich in der Anlaufphase befindliche Online-Verbindung zwischen der als Verbindungsstelle der Landesversicherungsanstalten tätigen LVA Schwaben in Augsburg und der italienischen Rentenversicherungsanstalt (INPS) in Rom gefordert. Die Bereitschaft, auf diese Forderungen einzugehen, wurde bereits signalisiert.

16 Unfallversicherung

16.1 Organisationsdienst für nachgehende Untersuchungen (ODIN)

Das Übereinkommen Nr. 139 der Internationalen Arbeitsorganisation (IAO) vom 24. Juni 1974 über die Verhütung und Bekämpfung der durch krebserzeugende Stoffe und Einwirkungen verursachten Berufs-

gefahren wurde durch Gesetz vom 13. Mai 1976 (BGBl. II 1976, S. 577) deutsches Recht. Die darin geforderten Maßnahmen wurden durch die Gefahrstoffverordnung und durch Unfallverhütungsvorschriften (UVV), insbesondere durch die UVV „Arbeitsmedizinische Vorsorge", umgesetzt. Nach den §§ 11—13 dieser UVV sollen sich Arbeitnehmer auch *nach* einer Tätigkeit, bei der sie über einen bestimmten Umfang hinaus (Auslöseschwelle) mit krebserzeugenden Stoffen in Berührung gekommen waren, auf deren Auswirkungen hin untersuchen lassen.

Grundsätzlich obliegt während der „aktiven" Beschäftigungszeit des Arbeitnehmers dem Arbeitgeber die Pflicht, die Teilnahme an den ärztlichen Untersuchungen — auch im Hinblick auf die Berührung mit krebserregenden Stoffen — zu überwachen. Nach dem Ausscheiden des betroffenen Arbeitnehmers aus dem Unternehmen wird die Sicherstellung der Nachuntersuchung durch den Arbeitgeber und dem für das frühere Unternehmen zuständigen Unfallversicherungsträger erheblich schwieriger. Zum einen bestehen zwischen dem bisherigen Arbeitgeber und dem ausgeschiedenen Arbeitnehmer möglicherweise keine Kontakte mehr, zum anderen können sich aus Branchen- oder Ortswechseln andere berufsgenossenschaftliche Zuständigkeiten ergeben. Das hat dazu geführt, daß die Unfallversicherungsträger durch eine entsprechende Vereinbarung eine zentrale Stelle — ODIN — geschaffen haben. Dort sollen u. a. Beschäftigungszeiten, in denen der Betroffene mit krebserzeugenden Stoffen oberhalb der jeweiligen Auslöseschwelle in Berührung gekommen ist, sowie damit zusammenhängende weitere personenbezogene Daten (Adresse, Arbeitgeber, usw.) auf Lebenszeit gespeichert werden. Die zentrale Stelle soll mit Hilfe der Datei die nachgehenden Untersuchungen koordinieren und sicherstellen. Darüber hinaus dokumentiert die Datei Informationen, die für mögliche künftige Leistungsansprüche der Arbeitnehmer von erheblicher Bedeutung sind. Sie ermöglicht schließlich statistische Auswertungen, auf die bei der Bewertung von Berufskrankheiten zurückgegriffen werden kann.

Aus datenschutzrechtlicher Sicht stellte sich die Frage, ob die oben dargestellten Regelungen in Verbindung mit § 708 RVO als Rechtsgrundlage für die damit verbundene Einrichtung einer bundesweiten Datei mit einer erwarteten Größenordnung von über 20 Mio. Arbeitnehmern ausreichen. Ich habe diese Frage grundsätzlich bejaht, jedoch neben einer stärkeren Betonung der Verantwortlichkeit der Unfallversicherungsträger, die durch Vereinbarung der Berufsgenossenschaft Chemie die Aufgabe übertragen haben, ODIN zu führen, eine Errichtungsanordnung für die Datei gefordert. Diese stellt die Aufgaben von ODIN dar und sichert die Transparenz der gespeicherten Daten. Ich habe ferner gefordert, die zu erfassenden Daten zu konkretisieren. Etwaige Klartext-Zusätze sind auf solche Angaben einzugrenzen, die zur Erläuterung der in der Errichtungsanordnung ausdrücklich genannten Daten dienen. Eine besondere Geheimhaltungsdienstanweisung und die organisatorische Trennung ODINS vom räumlichen und personellen Bereich der BG Chemie — unterstützt durch Maßnahmen des Zugriffschutzes — gewährleisten, daß keine Aufgabenvermengung zwischen ODIN und der BG Chemie eintreten kann. Damit kann ein möglichst hoher Datenschutzstandard eingehalten werden, der speziell an den Aufgaben von ODIN orientiert ist.

Die von ODIN eingerichtete Datei enthält keine Diagnosen. Die Rückläufe über Nachuntersuchungen können aber „Anhaltspunkte von medizinischer Qualität" enthalten. Diese Rückläufe geben allerdings nur Auskunft darüber, ob die arbeitsmedizinische Untersuchung ein positives, ein negatives oder ein fragliches Ergebnis mit der Notwendigkeit weiterer Aufklärung ergeben hat. Wird festgestellt, daß durch Berührung mit krebsauslösenden Stoffen eine gesundheitliche Beeinträchtigung eingetreten oder möglich ist, übernimmt der für den Entschädigungssachverhalt/Leistungsfall zuständige Unfallversicherungsträger die weitere Betreuung. Nur dieser erhält auch die medizinischen Untersuchungergebnisse. Ergibt die Untersuchung keinen Befund, setzt ODIN die terminliche Überwachung für Nachfolgeuntersuchungen fort.

Im Gegensatz zur arbeitsmedizinischen Vorsorgeuntersuchung während der „aktiven" Tätigkeit ist die nachgehende Untersuchung für die (früheren) Arbeitnehmer freiwillig. Ich habe darauf hingewirkt, daß dies gegenüber den Betroffenen stärker verdeutlicht wird. Sie werden um ihre Einwilligung in die Begutachtung durch einen von der Berufsgenossenschaft beauftragten Arzt und die hierzu erforderliche Offenbarung ihrer personenbezogenen Daten gebeten. Darüber hinaus wird ihnen die Möglichkeit eingeräumt, die Untersuchung durch einen anderen geeigneten Arzt zu wählen.

Ich habe die durchführende BG Chemie gebeten, mich über den weiteren Ausbau von ODIN sowie neue Entwicklungen oder Verfahrensabläufe zu unterrichten. Datenschutzrechtlich von besonderem Interesse dürfte in diesem Zusammenhang insbesondere sein, welche automatisierten Auswertungsverfahren für die Erforschung von Berufskrankheiten oder Zusammenhängen von Gefahrstoffen am Arbeitsplatz und von Gesundheitsschäden installiert werden.

16.2 Kontrolle der Berufsgenossenschaft der chemischen Industrie

Im Berichtsjahr habe ich eine datenschutzrechtliche Kontrolle bei der Berufsgenossenschaft der chemischen Industrie, Heidelberg (BG Chemie), durchgeführt.

Die BG Chemie ist ein bundesweiter Träger der gesetzlichen Unfallversicherung mit ca. einer Million Versicherten und ca. 10 000 Mitgliedern (Unternehmer der chemischen Industrie). Ihre Aufgaben erledigt sie in der Hauptverwaltung Heidelberg und sechs Bezirksverwaltungen.

Die Organisation des Datenschutzes ließ insbesondere Mängel der internen Datenschutzkontrolle erkennen. Die festgestellten Defizite haben ihre Ursache teilweise darin, daß der Datenschutzbeauftragte neben dieser Funktion auch noch die Aufgaben eines

Abteilungsleiters wahrnehmen mußte. Daraus ergab sich eine so hohe Gesamtbelastung, daß der Datenschutz fast zwangsläufig zu kurz kommen mußte.

Die Dienstanweisung für die Geheimhaltung der Sozialdaten war bei der kontrollierten BG unvollständig; das gleiche galt für die Dateienübersicht und die Registermeldungen nach § 19 Abs. 4 Satz 1 BDSG.

Die Berufsgenossenschaft hat zugesagt, festgestellte Defizite kurzfristig zu beseitigen und auch die Überwachung des Datenschutzes und der Datensicherung stärker als bisher vorzunehmen; Kontrollen sollen dokumentiert werden und in entsprechende Berichte an die Geschäftsleitung einfließen.

Nicht aufgegriffen hat die BG meine Empfehlung, auf Bezirksverwaltungsebene „Ansprechpartner" — gewissermaßen als „verlängerten" Arm des internen Datenschutzbeauftragten — zu benennen. Aufgrund der gegliederten Struktur der Berufsgenossenschaft mit mehreren Bezirksverwaltungen halte ich dies weiterhin für erforderlich. Darüber hinaus habe ich eine datenschutzrechtliche Schulung der Mitarbeiterinnen/Mitarbeiter als notwendig angesehen. Diesen sollten insbesondere die entsprechenden Materialien (Dienstanweisungen) als Arbeitsunterlage zur Verfügung gestellt werden.

Im Rahmen der automatisierten Datenverarbeitung der BG Chemie war es bislang möglich, eine unbegrenzte Anzahl von Paßworteingaben zu versuchen, ohne daß dies systembedingt verhindert wurde. Die BG Chemie wird die Möglichkeit der Installation einer Abbruchprozedur prüfen.

Eine Überprüfung der Verfahrensweise der Poststelle der Hauptverwaltung der BG ergab, daß dort auch die an die Bezirksverwaltung Heidelberg adressierte Post geöffnet wurde. Unterlagen mit sensiblen Daten wurden offen in Laufmappen oder Metallkörben zur Bezirksverwaltung transportiert. Eine schriftliche Dienstanweisung für die Behandlung der Post existierte nicht.

Ich habe empfohlen, das Posteingangsverfahren schriftlich zu regeln. Insbesondere medizinische Gutachten sollten verschlossen transportiert werden. Darüber hinaus sollte die Öffnung der an die Bezirksverwaltung gerichteten Post deren eigenen Mitarbeitern vorbehalten bleiben, um die Möglichkeit einer unbefugten Kenntnisnahme durch Mitarbeiter der Hauptverwaltung auszuschließen.

Im Rahmen der Kontrolle habe ich festgestellt, daß in den Versichertenakten der BG Chemie komplette ärztliche Gutachten abgeheftet werden. Sämtliche ärztliche Gutachten gelangen darüber hinaus bei Eingang dem Bezirksgeschäftsführer und dessen Stellvertreter zur Kenntnis.

Die BG begründete dieses Verfahren mit der Notwendigkeit einer vollständigen Auswertung der medizinischen Aussagen durch den Sachbearbeiter. Darüber hinaus sei eine Kenntnisnahme durch den Geschäftsführer und dessen Stellvertreter zur Beurteilung der Eignung der Gutachter für die Zwecke der Berufsgenossenschaft erforderlich. Diese Begründung erscheint plausibel. Die Vorteile, die sich für den Versichertern aus dem praktizierten Verfahren ergeben, dürften die datenschutzrechtlichen Risiken überwiegen.

Ich habe die datenschutzgerechte Organisation der Beihilfesachbearbeitung der BG Chemie begrüßt. Diese hat innerhalb der Personalabteilung eine eigenständige Beihilfe-Arbeitsgruppe geschaffen. Der Abteilungsleiter besitzt keinerlei Zugriffsrechte auf die Beihilfeunterlagen und die automatisiert gespeicherten Beihilfedaten. In Zweifelsfragen entscheidet die Arbeitsgruppe. Lediglich in Ausnahmefällen, etwa in rechtlichen Grundsatzfragen, entscheidet der Abteilungsleiter Personal auf der Grundlage ihm anonymisiert vorgelegter Unterlagen.

Die Erörterung der durch die Kontrolle der BG aufgeworfenen Fragen ist noch nicht abgeschlossen.

16.3 Offenbarung toxikologischer Blutanalysedaten von Arbeitnehmern an die Presse

Der Redakteur einer süddeutschen Tageszeitung hat mich um die datenschutzrechtliche Bewertung eines Sachverhalts gebeten, der mich mit einer ungewöhnlichen, für den Bereich des Sozialwesens untypischen Problematik konfrontierte: Seine Zeitung berichtet seit Jahren über die Dioxinverseuchung auf dem Werksgelände und in der Nachbarschaft eines metallverarbeitenden Betriebes in einer süddeutschen Stadt. Nachdem bekanntgeworden war, daß die zuständige Berufsgenossenschaft bei ehemaligen Arbeitnehmern des Betriebes Dioxin-Blutfettanalysen hatte anfertigen lassen, ersuchte die Tageszeitung um die Bekanntgabe von 10 anonymisierten Analyseergebnissen. Dies lehnte die Berufsgenossenschaft ab. Sie räumte zwar ein, daß es sich eindeutig um anonymisierte Daten handelte, deren Offenbarung schutzwürdige Belange der in die Untersuchung einbezogenen ehemaligen Arbeitnehmer nicht beeinträchtige. Sie sah sich an der erwünschten Übermittlung jedoch durch die Vorschrift des § 35 Abs. 4 SGB I gehindert, da die Analyseergebnisse Betriebs- und Geschäftsgeheimnisse seien und eine der Offenbarungsvoraussetzungen der §§ 67 ff. SGB X, insbesondere eine Einwilligung des Unternehmens, nicht vorliege. Die Berufsgenossenschaft deutete mir jedoch ihre Bereitschaft zur Übermittlung der Analyseergebnisse an die Presse für den Fall an, daß ich eine Verletzung des Sozialgeheimnisses für ausgeschlossen hielte.

Nachdem die Berufsgenossenschaft eingeräumt hatte, daß abgesicherte Erkenntnisse über die (mögliche) Belastung ehemaliger Arbeitnehmer des Unternehmens mit Dioxinrückständen von der Presse verbreitet worden waren und sich bestätigt hatte, daß das Betriebsunternehmen bereits im Jahre 1986 jede Produktions- und Vertriebstätigkeit eingestellt hatte, von einer Drittfirma übernommen worden war und nach Aussage ihres heutigen Geschäftsführers „faktisch mittellos" ist, habe ich die Auffassung vertreten, daß § 35 Abs. 4 SGB I der Übermittlung der Analyseergebnisse an die Presse nicht entgegensteht. Es wäre nämlich davon auszugehen, daß ein schützenswertes wirtschaftliches Geheimhaltungsinteresse des betroffenen Unternehmens zumindest nicht mehr vorlag. Die Dioxin-Belastung wenigstens einiger ehemaliger Mit-

arbeiter der betroffenen Firma war in der Öffentlichkeit bekannt und damit offenkundig geworden. Sobald eine Information, die üblicherweise vertraulich behandelt zu werden pflegt, offenkundig wird, stellt sie kein „Geheimnis" mehr dar. Hinzu kam, daß eine Wettbewerbsrelevanz jedenfalls nicht mehr gegeben war; denn von einer Teilhabe an einem wie auch immer gestalteten „Markt" könnte nicht mehr die Rede sein, so daß ein wirtschaftliches Interesse an der Geheimhaltung nicht mehr bestand.

In diesem Zusammenhang war auch die EG-Richtlinie vom 7. Juni 1990 über den freien Zugang zu Informationen über die Umwelt (Nr. 76 10/90) zu beachten, die darauf abzielt, „den freien Zugang zu den bei den Behörden vorhandenen Informationen über die Umwelt sowie die Verbreitung dieser Informationen zu gewährleisten und die grundlegenden Bedingungen festzulegen, unter denen derartige Informationen zugänglich gemacht werden sollen" (Artikel I). Zu den Umweltinformationen zählen nach Maßgabe der Entschließung des Europäischen Parlaments vom 13. April 1987 (Dok. A 2-30/87, S. 7) insbesondere „... Gesundheitsrisiken am Arbeitsplatz und in der Umwelt durch Chemikalien, Fasern, Strahlen, Lärm; ...".

Trotz mehrfacher Erinnerungen hat die Berufsgenossenschaft hierzu bislang nicht, wie erbeten, Stellung genommen und mitgeteilt, ob sie grundsätzlich bereit ist, die Analyseergebnisse der Öffentlichkeit zur Verfügung zu stellen.

17 Bundeskriminalamt, Bundesgrenzschutz

17.1 Gesetzgebungsvorhaben

Die Datenerhebung, -verarbeitung und -nutzung durch das Bundeskriminalamt und den Bundesgrenzschutz sollen auf eine neue gesetzliche Grundlage gestellt werden, die den Anforderungen des Volkszählungsurteils des Bundesverfassungsgerichts aus dem Jahre 1983 entspricht. Im Berichtsjahr sind mir die Referentenentwürfe zu einem „Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten" (BKAG) und eines „Gesetzes zur Änderung des Bundesgrenzschutzgesetzes" (BGSG) zugegangen. In meinen Stellungnahmen habe ich Vorschläge zur Verbesserung des bereichsspezifischen Datenschutzes gemacht. Ein Schwerpunkt war dabei der Schutz des Persönlichkeitsrechts von Personen, die nicht einer Straftat verdächtig und nicht für eine konkrete Gefahr verantwortlich sind. Insoweit sollte eine Datenerhebung und -speicherung über einzelne Personen grundsätzlich nur stattfinden, wenn tatsächliche Anhaltspunkte für die Begehung von möglichst konkret zu beschreibenden Straftaten mit erheblicher Bedeutung oder für eine konkrete Verwicklung in einen Gefahrensachverhalt sprechen, eine andere Möglichkeit zur Klärung des Sachverhalts nicht besteht sowie die Erhebung und Verarbeitung der Daten dem Betroffenen zugemutet werden kann. Insgesamt ist die Verarbeitung von Daten über nicht verdächtige Personen wie Anzeigende, Hinweisgeber, Kontakt- und Begleitpersonen, Geschädigte und Gefährdete, durch einschränkende Regelung der Speichervoraussetzungen und der Nutzung in engen Grenzen zu halten. Die Aufgabe des Bundeskriminalamtes, als Zentralstelle personenbezogene Daten zu sammeln und für andere Polizeibehörden bereitzustellen, sollte zudem auf die länderübergreifende und internationale Kriminalität begrenzt sein. Allenfalls für konkret zu benennende spezielle Deliktsbereiche, die ihrer Eigenart nach eine umfassendere Zentralstellenspeicherung gebieten, sollten Ausnahmen zugelassen werden.

Kurz vor Redaktionsschluß ist mir der Entwurf eines Gesetzes zur Änderung des Bundesgrenzschutzgesetzes zugegangen, mit dem dem Bundesgrenzschutz die Aufgaben der bisherigen Bahnpolizei übertragen werden sollen. Leider enthält der Gesetzentwurf nicht die seit langem erforderlichen bereichsspezifischen Regelungen über die Datenverarbeitung durch den Bundesgrenzschutz. Eine so bedeutsame Erweiterung der Aufgaben des BGS, wie sie der Entwurf vorsieht, sollte — wenn irgend möglich — nicht ohne solche Vorschriften verabschiedet werden.

17.2 Umgang mit Daten aus Telefonüberwachungsmaßnahmen beim BKA

Der ehemalige Hessische Minister des Innern, Milde, gab im Berichtsjahr öffentlich vor dem Hessischen Landtag Informationen aus einem Protokoll über ein Telefongespräch bekannt, das vom BKA überwacht worden war. Dieser Fall gab Anlaß, das Verfahren der Telefonüberwachung und den Umgang mit den daraus gewonnenen Informationen beim BKA zu überprüfen. Dabei konnte ich im konkreten Fall keinen Verstoß des BKA gegen datenschutzrechtliche Vorschriften feststellen, der ursächlich für die Bekanntgabe hätte sein können. Das BKA hatte im Auftrag der zuständigen hessischen Staatsanwaltschaft Ermittlungen durchgeführt und auf Grund richterlicher Anordnung Telefongespräche überwacht. Im Rahmen eines von der Staatsanwaltschaft ausdrücklich gebilligten Informationsaustausches hatte das BKA das Protokoll an die Frankfurter Polizei weitergeleitet. Von dort war die Information an das Hessische Ministerium des Innern und den Minister gelangt. Meine Prüfung hat aber ergeben, daß es dringend erforderlich ist, das Verfahren bei der Durchführung von Telefonabhörmaßnahmen und der Weitergabe von Informationen aus solchen Maßnahmen durch das BKA datenschutzrechtlich klar zu regeln und damit zu verbesssern. In dieser Auffassung bin ich mit dem Bundesminister des Innern und dem Bundeskriminalamt grundsätzlich einig. Das BKA plant, organisatorische und technische Maßnahmen zur Sicherung der personenbezogenen Daten aus Überwachungen des Fernmeldeverkehrs in einer Dienstanordnung festzulegen.

Dies begrüße ich, halte allerdings darüber hinaus Regelungen für erforderlich, die den Informationsfluß begrenzen. Ich habe nämlich festgestellt, daß die mit der Durchführung der Abhörmaßnahme betraute

Stelle des BKA Informationen aus der Maßnahme an die Leitung des Amtes weitergegeben hatte, obwohl dazu kein konkreter dienstlicher Anlaß bestanden hatte. Die Weitergabe von Informationen aus Maßnahmen zur Überwachung des Post- und Fernmeldeverkehrs zu Zwecken der Dienst- und Fachaufsicht ist im Lichte des Artikel 10 des Grundgesetzes zu sehen. Sie ist deshalb auf Fälle zu beschränken, in denen eine im konkreten Fall vorgesehene Maßnahme der Dienst- und Fachaufsicht die Kenntnis der Informationen erforderlich macht. Die Problematik wird noch mit den beteiligten Stellen erörtert. Ferner werde ich im Rahmen meiner Zuständigkeit darauf hinwirken, daß Anordnungen der Staatsanwaltschaft zur Weitergabe von Informationen aus Fernmeldeüberwachungsmaßnahmen nur für den Einzelfall und schriftlich getroffen werden. Nur so lassen sich Unklarheiten darüber, ob eine Übermittlung solcher Informationen einer Weisung der Staatsanwaltschaft tatsächlich entsprochen hat, vermeiden.

17.3 Zugriff von Landespolizeibehörden auf die Aktennachweisdatei BKA-AN

Das BKA unterhält im Rahmen des polizeilichen Informationssystems INPOL die Aktennachweisdatei BKA-AN neben der Datei Kriminalaktennachweis (KAN). Während der KAN Kriminalakten über schwerwiegende und überregional bedeutsame Delikte für Polizeidienststellen des Bundes und der Länder nachweist, wird in der Datei BKA-AN jeder Vorgang erfaßt, der irgendeine polizeiliche Relevanz aufweist. Im Gegensatz zum KAN, der eine Verbunddatei mit der Möglichkeit des unmittelbaren Abrufs für die Bundes- und Landespolizeidienststellen ist, handelt es sich bei der Datei BKA-AN um eine Datei, aus der in der Regel nur konventionell Daten übermittelt werden. Solange jedoch noch nicht alle Bundesländer am KAN-Verbund teilnahmen, wurden auch Polizeidienststellen der Länder zum direkten Abruf aus der Datei BKA-AN zugelassen. Dies hatte ich seit 1983 kritisiert, ohne daß Konsequenzen gezogen wurden. Auf meine im Mai 1990 ausgesprochene förmliche Beanstandung hin ist der direkte Zugriff der Polizeidienststellen der Länder auf die Daten in der Datei BKA-AN auf die Fälle beschränkt worden, in denen das System erkennungsdienstliches Material nachweist. Diese Lösung halte ich datenschutzrechtlich für befriedigend. Der verbleibende Zugriff betrifft erkennungsdienstliches Material, das nicht in der Zentralstellendatei Erkennungsdienst erfaßt ist, weil es aus der Zeit vor der Inbetriebnahme dieser Datei stammt und dort auch bisher nicht nachträglich erfaßt worden ist.

Nur zur Vermeidung von Mißverständnissen weise ich darauf hin, daß die weitgehende Beendigung des unmittelbaren Zugriffs der Polizeidienststellen der Länder auf die Datei BKA-AN keinerlei Auswirkungen auf die Bekämpfung der überregionalen Kriminalität, insbesondere des Terrorismus, hat. Dafür stehen die Datei KAN und besondere Dateien — wie z. B. APIS — zur Verfügung, auf die die Polizeidienststellen der Länder unmittelbar Zugriff haben.

17.4 Datenabfrage zur Besucherkontrolle beim BKA

Das BKA hat sein Verfahren zur Besucherkontrolle (s. 12. Tätigkeitsbericht S. 74) verbessert. Daten von Besuchern werden in den Dateien des BKA nur noch abgefragt, wenn es zwingend erforderlich erscheint, daß sie den inneren Sicherheitsbereich des Amtes betreten. Der Besucher wird dann um schriftliche Einwilligung ersucht. Der Zutritt zum inneren Sicherheitsbereich des Amtes bleibt verwehrt, wenn der Besucher die Einwilligung nicht erteilt oder die Abfrage Erkenntnisse mit terroristischen oder extremistischen Bezügen zutage fördert. Der Besuchte wird nicht über den Inhalt der Erkenntnisse informiert.

Trotz dieser Verbesserungen bleibt die Regelung hinter meinen Vorschlägen zurück. Wenn gespeicherte Daten nicht auf ihre konkrete Sicherheitsrelevanz überprüft werden, kann es zu sachlich unbegründeten Zurückweisungen kommen, wie gerade der Fall gezeigt hat, der Anlaß der Beanstandung war (s. 12. Tätigkeitsbericht S. 74).

18 Zollkriminalinstitut

Datenerhebung, -verarbeitung und -nutzung durch das Zollkriminalinstitut, das in ein Zollkriminalamt umgewandelt werden soll, sollen im Finanzverwaltungsgesetz geregelt werden. Im Unterschied zur bisherigen Rechtslage, in der entsprechende Regelungen durch Rechtsverordnung vorgesehen sind, soll jetzt der Gesetzgeber selbst über die wesentlichen Gesichtspunkte der Datenverarbeitung entscheiden. Dies halte ich für eine gebotene Konsequenz aus dem Volkszählungsurteil des Bundesverfassungsgerichts.

Der Entwurf des Finanzverwaltungsgesetzes sieht auch eine Regelung für das Datenverarbeitungssystem KOBRA vor, das bereits am 1. April 1991 auf der Grundlage des bisherigen Finanzverwaltungsgesetzes in Betrieb genommen worden ist. Dieses Datenverarbeitungssystem ist eine in ihrer Qualität neuartige Form der Datenverarbeitung zur Überwachung des Außenwirtschaftsverkehrs. Es eröffnet u. a. die Möglichkeit zur zollfahndungsrechtlichen Auswertung von Daten über Personen, die am Außenwirtschaftsverkehr teilnehmen und kann so als eine Art Verdachtsverdichtungsinstrument für Delikte auf dem Gebiet des Außenwirtschaftsverkehrs genutzt werden. Damit erfährt der Grundsatz der Trennung des normalen Verwaltungsvollzuges von der polizeilichen Kontrolle eine deutliche Durchbrechnung. Darüber hinaus soll dem künftigen Zollkriminalamt nach dem inzwischen vom Bundestag beschlossenen Gesetz zur Änderung des Außenwirtschaftsgesetzes die Befugnis eingeräumt werden, in das Brief-, Post- und Fernmeldegeheimnis einzugreifen, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, daß vorsätzliche Straftaten von erheblicher Bedeutung nach dem Außenwirtschaftsgesetz oder dem Kriegswaffenkontrollgesetz geplant werden. Das Verfahren ist zum größten Teil mit der Regelung des § 100a StPO vergleichbar. Damit werden die Kompetenzen des künftigen Zollkriminalamts bei Vorfeldermittlungen um

die Befugnis zum Einsatz eines tief in die Privatsphäre eindringenden nachrichtendienstlichen Mittels erweitert. Zur Einschätzung der besonderen Gefahren, die derartige Befugnisse für die Privatsphäre von Bürgern mit sich bringen können, müssen diese auch im Zusammenhang gesehen werden. Aus Daten des normalen Verwaltungsvollzuges können Verdachtsmomente gewonnen, auf diese Verdachtsmomente kann eine Überwachung des Brief-, Post- und Fernmeldeverkehrs gestützt und deren Ergebnisse können als Grundlage von Exekutivmaßnahmen nach dem Strafverfolgungsrecht verwendet werden.

Ich habe deutlich gemacht, daß es — unbeschadet der Notwendigkeit einer effektiven Kontrolle des Außenwirtschaftsverkehrs mit sensiblen Gütern — entscheidend darauf ankommt, ob und inwieweit tatsächlich ein Defizit in der Vorfeldaufklärung besteht und die vorgesehenen zusätzlichen Befugnisse auch wirklich geeignet sind, ein etwa bestehendes Manko zu beseitigen. Die Bundesregierung hat dies bei der Erörterung des Gesetzentwurfs zur Änderung des Außenwirtschaftsgesetzes dargelegt. Verdeckte Datenerhebungsbefugnisse und der Umgang mit so gewonnenen Daten müssen unter Beachtung des Rechts auf informationelle Selbstbestimmung besonders sorgfältig und normenklar auf das wirklich Unerläßliche eingegrenzt und soweit irgend möglich in die Systematik unserer Rechtsordnung eingepaßt werden. So sollten die neuen Befugnisse keinesfalls bei Anhaltspunkten für Fahrlässigkeitsdaten zulässig sein, denn auch § 100 a StPO läßt Überwachungen des Post- und Fernmeldeverkehrs nur beim Verdacht vorsätzlich begangener Straftaten zu. Das beschlossene Gesetz trägt dieser Forderung Rechnung und hat auch die Möglichkeit, Anschlüsse juristischer Personen oder von Personenvereinigungen abzuhören, auf die Anschlüsse beschränkt, die — nach tatsächlichen Anhaltspunkten — zu den vom Gesetz mißbilligten Zwecken benutzt werden. Der Bundestag hat auch meinen Vorschlag aufgegriffen, die Erhebungsbefugnisse zunächst nur für eine bestimmte Zeit (bis 31. Dezember 1994) vorzusehen. Damit ist gewährleistet, daß der Gesetzgeber nach Ablauf dieser Frist aufgrund der bis dahin gemachten Erfahrungen erneut darüber entscheidet, ob die Befugnis zu derart intensiven Eingriffen noch weiter bestehen bleiben muß. Der Bundesrat hat wegen der vorgesehenen Erweiterung der Befugnisse zu Abhörmaßnahmen den Vermittlungsausschuß angerufen. Das Gesetzgebungsverfahren war bei Redaktionsschluß noch nicht abgeschlossen.

Hinsichtlich des Datenverarbeitungssystems KOBRA habe ich zur Begrenzung polizeilicher Nutzungen in meiner Stellungnahme zur Inbetriebnahme des Systems u. a. vorgeschlagen, eine systematische Auswertung des in KOBRA gespeicherten Datenbestandes über Ausfuhren oder von Teilen davon nur dann für die polizeilichen Zwecke der Verhütung und Verfolgung von Delikten vorzunehmen, wenn es sich um ein Delikt mit erheblicher Bedeutung handelt. Eine Nutzung der Daten zu diesen polizeilichen Zwecken im Einzelfall sollte nur zulässig sein, wenn tatsächliche Anhaltspunkte befürchten lassen, daß ein Delikt mit erheblicher Bedeutung begangen werden soll oder wenn Tatverdacht vorliegt.

19 Bundesamt für Verfassungsschutz

19.1 Bundesverfassungsschutzgesetz

Das neue Bundesverfassungsschutzgesetz ist zusammen mit dem MAD-Gesetz und dem BND-Gesetz als Teil des „Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes" (s. 26.) am 30. Dezember 1990 in Kraft getreten. Die Konferenz der Datenschutzbeauftragten von Bund und Ländern und ich haben zu einem während der parlamentarischen Beratungen erreichten Zwischenstand des Gesetzentwurfs noch einmal Stellung genommen (s. Anlage 3). Bei der Beratung des Gesetzentwurfs konnten im Bundestag und Bundesrat gegenüber den ursprünglichen Entwürfen (s. hierzu 11. TB S. 66 f.), datenschutzrechtliche Verbesserungen erzielt werden.

- Das neue Gesetz präzisiert im Sinne einer größeren Normenklarheit nunmehr die Aufgaben des BfV, in dem es die Begriffe „Bestrebungen gegen den Bestand des Bundes oder eines Landes", „Bestrebungen gegen die Sicherheit des Bundes oder eines Landes" und „Bestrebungen gegen die freiheitliche demokratische Grundordnung" definiert.

- Die Befugnis, amtliche Register einzusehen, bei deren Wahrnehmung die personenbezogenen Daten vieler Nichtverdächtiger erhoben werden können, wird nicht unterschiedslos für die Erfüllung aller Aufgaben des BfV, sondern nur für bestimmte Sachbereiche (z. B. Spionageabwehr, Terrorismusbeobachtung) gewährt.

- Die Regelungen über die gemeinsamen Verbunddateien der Verfassungsschutzbehörden sind präziser gefaßt worden. Sie dürfen als Textdateien oder mit weiteren im Gesetz nicht ausdrücklich vorgesehenen Daten nur für bestimmte, eng umgrenzte Anwendungsgebiete geführt werden.

- Das Gesetz regelt besser als der Entwurf die besonderen Formen der Datenerhebung durch das Bundesamt für Verfassungsschutz. Es läßt insbesondere den Einsatz technischer Mittel zur heimlichen Ton- und Bildaufzeichnung in Wohnungen nur unter sehr engen Voraussetzungen zu.

- Für manuelle Datensammlungen wie Karteien und Akten sind einschränkende Regelungen, insbesondere zum Minderjährigenschutz, in das Gesetz aufgenommen worden.

- Das Gesetz schreibt vor, daß für jede automatisierte Datei eine Dateianordnung zu erlassen ist, deren wesentlicher Inhalt festgelegt ist. Die Dateianordnung bedarf der Zustimmung des Bundesministers des Innern. Der Bundesbeauftragte für den Datenschutz ist vorher anzuhören.

- Gesetzlich geregelt sind jetzt auch die Rahmenfristen für die Überprüfung und Löschung gespeicherter Daten. Gespeicherte Daten sind spätestens nach fünf Jahren darauf zu überprüfen, ob sie zu berichtigen oder zu löschen sind. Spätestens zehn Jahre nach der letzten gespeicherten relevanten

Information sind sie — ausgenommen im Falle der Spionage — grundsätzlich zu löschen.

— Das Recht des Bürgers auf Auskunft über beim Bundesamt für Verfassungsschutz über ihn gespeicherte Daten ist jetzt im Verfassungsschutzgesetz — nicht mehr im Bundesdatenschutzgesetz — geregelt. Nach der Absicht des Gesetzgebers sollte das Auskunftsrecht des Bürgers verbessert werden. Ich fürchte, daß diese Absicht nicht oder kaum erreicht worden ist. Ursache dafür ist, daß eine Auskunftserteilung durch das BfV überhaupt nur in Betracht kommt, wenn der Bürger auf einen „konkreten Sachverhalt" hinweist und ein „besonderes Interesse" an der Auskunft darlegt. Gegen diese Regelung hatte ich Bedenken erhoben, deren Richtigkeit ich durch die inzwischen gewonnenen ersten Erfahrungen bestätigt sehe. Sie führt nämlich dazu, daß der Bürger dem BfV detaillierte Angaben über persönliche Lebensumstände preisgeben muß, um Auskunft über gespeicherte Daten zu erhalten. Das scheuen viele Bürger. Nach meinem Eindruck hat die Regelung kaum eine Verbesserung der Auskunftspraxis gebracht. Erbittet ein Bürger Auskunft ohne einen konkreten Sachverhalt und ein besonderes Interesse an der Auskunft darzulegen, erhält er vom BfV in aller Regel einen formelhaften Bescheid, und dies auch dann, wenn keiner der besonderen Gründe vorliegt, die das BfV im Interesse seiner Aufgabenerfüllung zur Verweigerung der Auskunft berechtigen.

  Daß auch eine Regelung im Sinne meines Vorschlags möglich ist, zeigt § 18 des neuen Hessischen Verfassungsschutzgesetzes, der das Auskunftsrecht des Bürgers nicht von der Darlegung eines konkreten Sachverhalts und eines besonderen Interesses an der Auskunft abhängig macht. Ein gewiß unverdächtiger Zeuge, nämlich der Präsident des Hessischen Landesamtes für Verfassungsschutz, hat kürzlich in einer öffentlichen Veranstaltung erklärt, mit diesem Gesetz ließe sich vernünftig arbeiten.

Ich habe auch bedauert, daß mein Vorschlag, die Erhebung von Daten bei Nichtverdächtigen — besonders mit Hilfe sogenannter nachrichtendienstlicher Mittel — an strengere Voraussetzungen zu binden, nicht übernommen worden ist. Das Hessische Verfassungsschutzgesetz, bei dessen Vorbereitung ich als Sachverständiger gehört worden bin, enthält eine solche Regelung. Und auch auf diese bezieht sich das oben wiedergegebene Urteil des Präsidenten des Hessischen Landesamtes für Verfassungsschutz.

Trotz dieser Bedenken stellt das neue Verfassungsschutzgesetz einen deutlichen Fortschritt dar.

Die gleichzeitig verabschiedeten Gesetze über den MAD und den BND haben für die Tätigkeit dieser beiden Dienste endlich eine Rechtsgrundlage geschaffen. Da die Gesetze für die Befugnisse dieser Dienste und die Rechte der Bürger weitgehend auf das Verfassungsschutzgesetz verweisen, gilt das obige Gesamturteil im wesentlichen auch für sie.

19.2 Sicherheitsüberprüfung

Bereits in meinem 6. Tätigkeitsbericht (S. 42) hatte ich über die Einbeziehung von Unterlagen des Anerkennungsverfahren von Kriegsdienstverweigerern in die Sicherheitsüberprüfung berichtet.

Bei einer Querschnittsprüfung der Abteilung V des Bundesamtes für Verfassungsschutz die für Sicherheitsüberprüfungen zuständig ist, hatte ich seinerzeit festgestellt, daß sich entweder Kopien aus den Akten des Anerkennungsverfahrens für Kriegsdienstverweigerer oder vom Bundesamt für Verfassungsschutz gefertigte inhaltliche Wiedergaben hieraus in den Sicherheitsüberprüfungsakten der betroffenen Bediensteten befanden. Die Eingabe eines Petenten gab mir nunmehr Anlaß, diesem Problem erneut nachzugehen. Der Petent erklärte mir, daß er zwar sein Einverständnis gegenüber dem Bundesamt für Verfassungsschutz erklärt habe, die Akten des Anerkennungsverfahrens im Rahmen der Sicherheitsüberprüfung beizuziehen, jedoch nicht dazu, diese Akten zu seiner Sicherheitsüberprüfungsakte zu übernehmen. Die Aufnahme von Unterlagen über das Anerkennungsverfahren in die Sicherheitsüberprüfungsakte ist deshalb sehr problematisch, weil dadurch sehr persönliche, das Gewissen betreffende Informationen sehr viel länger aufbewahrt werden als es nach dem Kriegsdienstverweigerungsgesetz zulässig ist. Derartige Unterlagen in den Sicherheitsüberprüfungsakten werden weder nach Ablauf des Jahres, in dem der Betroffene das 32. Lebensjahr vollendet (bei anerkannten Kriegsdienstverweigerern, die nicht zum Zivildienst herangezogen werden), vernichtet, noch — nach § 2 Abs. 6 des Kriegsdienstverweigerungs-Neuordnungsgesetzes mit Ausnahme des Anerkennungsbescheides — spätestens sechs Monate nach Ableistung des Zivildienstes, sondern — nach § 16 Abs. 4 der Sicherheitsrichtlinien — erst fünf Jahre nach dem Ausscheiden einer Person aus einer sicherheitsempfindlichen Tätigkeit, wenn sie nicht nach den „Richtlinien der Bundesregierung für die Abgabe von Verschlußsachen an das Geheimarchiv des Bundesarchivs" an das Geheimarchiv abzugeben sind. Eine entsprechende Regelung gilt auch für die beim Bundesamt für Verfassungsschutz vorhandenen Unterlagen. Eine besondere Regelung für Informationen aus dem Anerkennungsverfahren besteht nicht.

Nach der Regelung des § 16 der Sicherheitsrichtlinien können demzufolge Informationen aus dem Anerkennungsverfahren in Sicherheitsüberprüfungsakten länger aufbewahrt werden, als es nach der spezialgesetzlichen Regelung für das Anerkennungsverfahren zulässig ist. Ich konnte den Bundesminister des Innern und den Bundesminister für Jugend, Familie, Frauen und Gesundheit davon überzeugen, daß die Regelung des Kriegsdienstverweigerungs-Neuordnungsgesetzes sinngemäß auch auf die im Rahmen des Geheimschutzverfahrens übermittelten Informationen anzuwenden ist. Zukünftig wird das Bundesamt für Verfassungsschutz keine Kopien aus den Anerkennungsunterlagen mehr zu Sicherheitsüberprüfungsakten nehmen. Aktenvermerke zu Sachverhalten aus diesen Akten werden nur noch bis zur Abgabe des Votums des Bundesamtes für Verfassungsschutz an den Geheimschutzbeauftragten, sicherheitsrelevante Infor-

mationen bis zum Abschluß der Sicherheitsüberprüfung aufbewahrt. Die notwendige rückwirkende Bereinigung der Sicherheitsüberprüfungsakten will das Bundesamt für Verfassungsschutz bis spätestens Ende 1996 erledigen.

19.3 Übermittlung von Erkenntnissen im Rahmen von Sicherheitsüberprüfungen

Eine Petentin hatte sich darüber beschwert, daß der für sie zuständige Geheimschutzbeauftragte einer obersten Bundesbehörde ihr im Rahmen einer Sicherheitsüberprüfung der untersten Stufe (Dateianfrage), der sie sich zu unterziehen hatte, Erkenntnisse des BfV über ihren früheren Ehemann vorgehalten hatte, die erst nach der Ehescheidung angefallen waren.

Meine Überprüfung des Vorgangs ergab, daß das BfV dem Geheimschutzbeauftragten eine Erkenntniszusammenstellung übermittelt hatte, die neben irrelevanten und später gelöschten Informationen über die Petentin auch umfangreiche Erkenntnisse über deren früheren Ehemann enthielt. Durch die bei der Übermittlung gewählten Formulierungen wurde auch noch der falsche Eindruck des Fortbestands der Ehe hervorgerufen. Insoweit waren die übermittelten Angaben objektiv falsch und damit zugleich ungeeignet, den Übermittlungszweck zu erfüllen. Bei der Sensibilität der Daten hätte sich das BfV — etwa durch Rückfrage beim Geheimschutzbeauftragten — vergewissern müssen, ob die eheliche Verbindung zwischen der Petentin und ihrem früheren Ehemann noch bestand. Jedenfalls hätte es den Bestand der Ehe nicht als feststehendes Faktum übermitteln dürfen, sondern darauf hinweisen müssen, daß vor einer Verwendung und Mitteilung an Außenstehende eine Aktualisierung geboten ist. Dieser Sorgfaltspflicht ist das BfV nicht nachgekommen.

Ich habe daher die Übermittlung der Daten an den Geheimschutzbeauftragten wegen Verstoßes gegen § 3 BDSG und gegen § 1 der Verschlußsachenanweisung beanstandet.

Im Interesse der Verbesserung des Verfahrens begrüße ich es, daß der Bundesminister des Innern das BfV angewiesen hat, künftig vor der Übermittlung von Erkenntnissen über den Partner des Überprüften den aktuellen Familienstand über den zuständigen Geheimschutzbeauftragten feststellen zu lassen.

20 Bundesnachrichtendienst (BND)

— Im Rahmen einer *Kontrolle beim Bundesnachrichtendienst* wurden neben fachspezifischen Fragen des Datenschutzes bei der Entwicklung von IT-Verfahren auch nachrichtendienstliche Besonderheiten bei Bewerbungs- und Einstellungsverfahren sowie datenschutzbezogene Regelungen bestimmter Fachbereiche erörtert.

  Die breit angelegte Kontrolle ergab einige datenschutzrechtliche Mängel, die ich gegenüber dem Staatssekretär beim Bundeskanzleramt beanstandet habe. Aus Gründen der Geheimhaltung kann in diesem, der Öffentlichkeit zugänglichen Bericht nicht konkret auf diese Mängel eingegangen werden.

  Ich begrüße sehr, daß Bundeskanzleramt und Bundesnachrichtendienst nicht nur die sich aus den Beanstandungen ergebenden konkreten Korrekturen vornehmen wollen, sondern auch meine weiteren Empfehlungen zur Verbesserung des Datenschutzes bereitwillig und nahezu vollständig aufgegriffen haben. Dabei ist insbesondere die beabsichtigte bedeutende personelle Verstärkung der Organisationseinheit des internen Datenschutzes hervorzuheben, die es erlauben wird, künftig die weitere Erforderlichkeit von Datenspeicherungen besser und in angemessenen Zeitabständen zu überprüfen.

— Wieder haben mich mehrere Bürger ersucht, im Zusammenhang mit ihrer Person beim Bundesnachrichtendienst Kontrollen durchzuführen. In zwei Fällen hat der Bundesnachrichtendienst nach Eingang meiner *Anfragen* die *über* die *Petenten* gespeicherten Daten gelöscht und die entsprechenden Aktenunterlagen vernichtet, bevor ich die Möglichkeit hatte, die Fälle zu kontrollieren. Ich habe diese Vorgehensweise beanstandet, weil sie mich außerstande gesetzt hat, meiner gesetzlichen Kontrollverpflichtung nachzukommen. Nach § 19 Abs. 3 Nr. 1 BDSG (alt) wäre es Pflicht des Bundesnachrichtendienstes gewesen, mir auf Wunsch in die zum Zeitpunkt meiner Anfragen bestehenden Unterlagen Einsicht zu gewähren. Darüber hinaus war der Bundesnachrichtendienst nach § 14 Abs. 3 BDSG nicht zur Löschung der Daten der Petenten befugt, weil wegen meiner Anfragen Grund zu der Annahme bestand, daß durch die Löschung schutzwürdige Belange der Petenten beeinträchtigt werden. Zu diesen Belangen zählt auch das nach § 21 BDSG jedermann zustehende Recht, den Bundesbeauftragten für den Datenschutz anzurufen. Dieses Recht läuft ins Leere, wenn während des Prüfungsvorgangs relevante Unterlagen vernichtet werden.

  Der Bundesnachrichtendienst hat seine Vorgehensweise verteidigt, aber zugesichert, künftig Daten und Aktenunterlagen solange aufzubewahren, bis mir die Möglichkeit zur Kontrolle gegeben war.

21 Verteidigung

21.1 Medizinische und psychologische Untersuchungen und Tests

Im Rahmen der Beratungen des Entwurfs eines Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften (BT-Drucksache 11/7390 [neu], s. 7.1) war für mich auch die dort vorgesehene Regelung zur Ergänzung des Soldatengesetzes von besonderem Interesse, die sich mit der Behandlung der Unterlagen über bei Soldaten durchgeführte medizinische und psychologische Untersuchungen und Tests befaßte. Solche Unterlagen fallen z. B. bei ärztlichen Untersuchungen auf die körperliche Tauglichkeit des Wehrpflichtigen

im Rahmen der Musterung und bei der Eignungs- und Verwendungsprüfung, mit deren Hilfe die Eignung der wehrdienstfähigen Wehrpflichtigen für bestimmte Verwendungen bei der Bundeswehr festgestellt werden soll, an.

Der Entwurf sah u. a. bereits vor, daß

- von den Unterlagen über medizinische und psychologische Untersuchungen und Tests im Rahmen der Personalführung und -bearbeitung nur die *Ergebnisse* automatisiert verarbeitet und genutzt werden dürfen, soweit sie die Verwendungs- und die Dienstfähigkeit des Soldaten betreffen,

- eine Verarbeitung psychologischer Daten auch in automatisierten Dateien zu dem Zweck gestattet sein sollte, die Aussagefähigkeit der psychologischen Eignungsfeststellungsverfahren zu bewerten und zu verbessern.

In Beratungen mit dem Bundesminister der Verteidigung und dem für den Gesetzentwurf insgesamt federführenden Bundesminister des Innern konnte ich Übereinstimmung über folgende wesentliche Verbesserungen und Präzisierungen des Regierungsentwurfs erreichen, die ich auch bereits weitgehend den Vorsitzenden des Innen- und des Verteidigungsausschusses unterbreitet hatte:

- Die Verarbeitung der bei medizinischen und psychologischen Untersuchungen und Tests anfallenden vielfältigen Daten — die angesichts des Umfangs dieser Daten auch den Einsatz automatisierter Datenverarbeitung umfaßt — muß *abgeschottet* im jeweiligen Dienst der Bundeswehr erfolgen.

- An die für die Personalführung und -bearbeitung zuständigen Stellen der Bundeswehr dürfen im erforderlichen Rahmen *nur die Ergebnisse* der Untersuchungen und Tests gelangen.

- Zur Verbesserung der Aussagefähigkeit der psychologischen Eignungsfeststellungsverfahren darf der *Psychologische Dienst* in der Regel *nur Stichproben* aus Daten über psychologische Untersuchungen und Tests verarbeiten. Zu diesem Zweck dürfen dem Psychologischen Dienst auf sein Ersuchen die erforderlichen tatsächlichen Bewährungsdaten übermittelt werden, soweit sie sich auf die Ergebnisse der vorangegangenen Untersuchungen und Tests beziehen, deren Aussagefähigkeit verbessert werden soll.

- Die an den Psychologischen Dienst übermittelten Daten sollen mindestens den gleichen Schutz genießen, den das Bundesdatenschutzgesetz bei der vergleichbaren Verwendung personenbezogener Daten für Zwecke der wissenschaftlichen Forschung gewährt. Damit sind diese Daten zu anonymisieren, sobald dies nach dem Zweck der Verarbeitung — Verbesserung der Aussagefähigkeit des Eignungsfeststellungsverfahrens — möglich ist.

Die abgesprochenen Verbesserungen des Gesetzentwurfs wurden nicht verwirklicht, weil dieser nicht mehr verabschiedet wurde. Inzwischen hat die Bundesregierung den Gesetzentwurf der vergangenen Legislaturperiode unverändert neu eingebracht. Ich gehe davon aus, daß das erzielte Einvernehmen über die vorzunehmenden Änderungen fortbesteht und die oben dargestellten Verbesserungen im Laufe des Gesetzgebungsverfahrens noch eingearbeitet werden.

21.2 Verwendung privater Personalcomputer bei einer Heimatschutzbrigade

Ein Petent hat in einer Eingabe die Nutzung eines privaten Personalcomputers (PC) für dienstliche Zwecke in einer Heimatschutzbrigade gerügt. Bei einer Kontrolle habe ich festgestellt, daß dort zu einem früheren Zeitpunkt tatsächlich zwei privat beschaffte PC aufgestellt waren:

- einer im Dienstzimmer des Leiters

- ein zweiter in dessen Geschäftszimmer.

Der private PC im Dienstzimmer des Leiters befand sich zum Kontrollzeitpunkt aufgrund eines entsprechenden Befehles nicht mehr in den Räumen der Einheit. Dementsprechend konnte nicht mehr festgestellt werden, inwieweit auf der Festplatte dieses Rechners sowie auf noch vorhandenen privaten Disketten, bei denen es sich vermutlich um Sicherungskopien der Festplatte handelte, personenbezogene Daten von Soldaten gespeichert worden waren. Der zweite PC war inzwischen ordnungsgemäß in den Bestand der Dienststelle aufgenommen. Hierbei handelte es sich um ein Gerät mit dem Betriebssystem MS-DOS. Auf der Festplatte befanden sich neben den Systemen, die von der Schreibkraft benutzt wurden, auch eine Reihe von Software-Paketen, deren Herkunft unklar war und die zur Aufgabenerfüllung nicht erforderlich waren, sowie einige alte Dateien aus dem Textverarbeitungssystem. Die aktuellen Dateien, die zum Teil auch personenbezogene Daten enthielten, waren ausnahmslos auf Disketten abgelegt.

Der BMVg hat für seinen Geschäftsbereich Richtlinien zum Einsatz von Kleinrechnern erlassen, wonach deren Verwendung für die Personalführung und -bearbeitung außerhalb hierfür bestehender DV-Verfahren bis zum Erlaß gesonderter Regelungen unzulässig ist; dasselbe ist generell für die Verwendung *privater* Kleinrechner und *privater* Programme für dienstliche Zwecke bestimmt. Meine Feststellungen ergaben, daß in der Einheit die Problematik zwar durchaus erkannt war, die getroffenen Maßnahmen jedoch nicht ausreichten, um eine Trennung von dienstlicher und privater Datenverarbeitung, insbesondere Datenspeicherung, zu gewährleisten. Um dies sicherzustellen, wurde auf meine Empfehlung hin veranlaßt, daß

- dem Eigentümer des privaten PC und der privaten Disketten befohlen wurde, dienstliche personenbezogene Daten sowohl auf der Festplatte als auch auf den Disketten zu löschen und

- der im Geschäftszimmer der Einheit betriebene PC zwischenzeitlich überprüft und die zur Aufgabenerfüllung nicht erforderliche Software sowie die

Software unbekannter Herkunft von der Festplatte gelöscht wurden.

Ich erwarte, daß die vom BMVg in Aussicht gestellten Regelungen für den Einsatz von PC bald getroffen und etwaige vergleichbare Mängel an anderen Stellen dann von diesen bereits selbst besser erkannt und beseitigt werden.

21.3 Militärischer Abschirmdienst (MAD)

Im 12. Tätigkeitsbericht (S. 81) habe ich über die Bereinigung der gesamten Datenbestände der Abwehrbereiche 1 (Sicherheitsüberprüfung), 2 (verfassungsfeindliche Kräfte) und 3 (Spionageabwehr) des Militärischen Abschirmdienstes berichtet. Der Bundesminister der Verteidigung hat mir nunmehr mitgeteilt, daß die Bereinigung von Datensätzen zu Altaktenvorgängen im Bereich der personellen Sicherheit abgeschlossen ist. Die Datenbestände des Abwehrbereichs 2 sind ebenfalls überwiegend in bezug auf ihre Relevanz für die weitere Aufrechterhaltung der Speicherung durchgesehen worden. Der Abwehrbereich 2 hat lediglich noch die archivierten Akten, bei denen zwar die Dateispeicherung gelöscht wurde, aber die Akteneinsicht/Vernichtung aus Zeitgründen noch nicht durchgeführt werden konnte, nach Auswertekriterien zu prüfen. Im Abwehrbereich 3 wurde ebenfalls die Bereinigung der Personendatensätze aus Ermittlungsvorgängen zum Jahresende 1990 abgeschlossen. Einige Datensätze, die einen bestimmten Personenkreis betreffen, wurden vor Löschung dem Abwehrbereich 1 zugeleitet, damit von dort unter dem Gesichtspunkt der personellen Sicherheit abschließend die mögliche weitere Relevanz beurteilt werden kann. Soweit personenbezogene Daten aus Operationen des Militärischen Abwehrdienstes gespeichert wurden, hat die durchgeführte Bestandsbereinigung dazu geführt, daß nunmehr 80 % der ehemals gespeicherten Datensätze gelöscht wurden. Der Bundesminister der Verteidigung hat zugesichert, mir in Kürze mitzuteilen, wann die Bereinigungssaktion endgültig abgeschlossen sein wird.

21.4 Regelungen für Sicherheitsüberprüfungen bei der Bundeswehr

Das Bundeskabinett hat für Bedienstete des Bundes im Mai 1988 die Sicherheitsrichtlinien in Kraft gesetzt. Diese sehen vor, daß in besonders begründeten Fällen jede oberste Bundesbehörde für ihren Geschäftsbereich abweichende Regelungen erlassen kann, wenn dadurch die Wirksamkeit des personellen Geheimschutzes nicht beeinträchtigt und die Grundsätze dieser Richtlinien beachtet werden.

Wegen der Größe und der strukturellen Besonderheiten der Bundeswehr gelten die allgemeinen Sicherheitsrichtlinien nicht für den Bereich des Bundesministers der Verteidigung. Dieser hat mit Rücksicht auf die neuen Sicherheitsrichtlinien die bisher bestehende zentrale Dienstvorschrift über die Sicherheitsüberprüfung in seinem Geschäftsbereich überarbeitet. Hierbei wurde ich beteiligt und konnte meine Vorstellungen einbringen. Das hat dazu geführt, daß die neue Dienstvorschrift unter Datenschutzaspekten einen deutlichen Fortschritt darstellt.

Der Bundesminister der Verteidigung ist mir allerdings in der Frage der Zweckbindung der angefallenen Informationen aus der Sicherheitsüberprüfung nicht gefolgt. Die neue Regelung sieht vor, daß die anfallenden Informationen zwar vertraulich zu behandeln sind; sie dürfen jedoch außer für die mit der Sicherheitsüberprüfung verfolgten Zwecke des Geheimschutzes oder Zwecke des Verfassungsschutzes auch für Zwecke der straf- oder disziplinarrechtlichen Verfolgung sowie erforderliche dienst- oder arbeitsrechtliche Maßnahmen und für parlamentarische Untersuchungen genutzt und weitergegeben werden. Dies bedeutet, daß Informationen aus der Sicherheitsüberprüfung grundsätzlich auch an mit anderen Aufgaben betraute Abteilungen des Verfassungsschutzes übermittelt werden dürfen. Ich hatte eine restriktivere Verwendungsregelung angeregt. Der Bundesminister der Verteidigung beruft sich darauf, daß § 12 Abs. 3 der Sicherheitsrichtlinien auch keine strengere Zweckbindung vorsieht.

Weiterhin hatte ich angeregt, bei der Festlegung sicherheitsempfindlicher Bereiche im Bundesministerium der Verteidigung zu differenzieren. Es sollte noch einmal überprüft werden, ob es wirklich erforderlich ist, jede Person, die in dessen Geschäftsbereich ihren Dienst verrichtet, einer Sicherheitsüberprüfung zu unterziehen. Die Anzahl der zu Überprüfenden könnte hierdurch reduziert und ein erheblicher Beitrag zur Verwaltungsvereinfachung sowie zur Beschleunigung von Einstellungsverfahren geleistet werden. Das entspräche auch der seit einiger Zeit geübten Praxis der übrigen Bundesbehörden. Der Bundesminister der Verteidigung lehnt dies ab, weil sein Geschäftsbereich in besonderem Maße Ziel gegnerischer Nachrichtendienste sei.

Die angesprochenen Fragen werden bei der Ausarbeitung eines Geheimschutzgesetzes, die ich in der neuen Legislaturperiode erwarte, noch einmal zu erörtern sein.

22 Wirtschaftsverwaltung

22.1 Änderung gewerberechtlicher Vorschriften

Über einen Gesetzesentwurf des Bundesministers für Wirtschaft zur Änderung datenschutzrechtlich relevanter Vorschriften im Gewerberecht habe ich berichtet (12. TB S. 81 f). Hierzu habe ich zwischenzeitlich konkrete Alternativen formuliert. Kernpunkte meiner Anregungen betreffen die Wahrung des Steuer- und des Sozialgeheimnisses sowie die besonderen Informationssammlungen in zentralen Registern.

Der Gesetzesentwurf sieht vor, daß der Datenerhebung durch die Gewerbeaufsicht weder das Steuer- noch das Sozialgeheimnis entgegenstehen sollen. Ich habe den Bundesminister für Wirtschaft darauf hingewiesen, daß schon aus Gründen der Gesetzessystematik eine Durchbrechung des Sozialgeheimnisses in der

Gewerbeordnung ausscheidet, weil dies nur im Sozialgesetzbuch geregelt werden kann. Eine generelle Durchbrechung des Steuergeheimnisses ohne jede Differenzierung hinsichtlich der unterschiedlichen Sachverhalte, wie im Gesetzesentwurf vorgesehen, wäre außerordentlilch bedenklich. Ich sehe keine fachlichen Gründe, die es rechtfertigen könnten, den bestehenden Datenschutz-Standard abzusenken, der in dieser Frage im wesentlichen durch die Rechtsprechung des Bundesfinanzhofes konkretisiert ist. Gegen eine normenklare Übernahme der von der Rechtsprechung herausgearbeiteten Grundsätze hätte ich keine Bedenken; sie wäre sogar zu begrüßen. Demzufolge habe ich eine Regelung vorgeschlagen, die den in § 30 Abs. 4 Nr. 5 der Abgabenordnung verwendeten unbestimmten Rechtsbegriff des „zwingenden öffentlichen Interesses" unter Berücksichtigung der hierzu ergangenen Rechtsprechung des Bundesfinanzhofs bereichsspezifisch konkretisiert.

Der vorliegende Entwurf sieht vor, daß Gewerbeaufsichtsbehörden Informationen, die bislang über hierzu eingerichtete Register — wie Gewerberegister oder Bundeszentralregister — bezogen wurden, in Zukunft auch unmittelbar bei den jeweiligen öffentlichen Stellen (insbesondere Gerichte, Behörden) erheben können. Die Register stellen in sich wohlabgewogene Informationsbereitstellungs-Systeme dar, die über zahlreiche Filter gewährleisten, daß dem Entscheidungsträger nur solche Informationen zugeführt werden, die er für eine sachorientierte Entscheidung benötigt. So enthalten beispielsweise die Regelungen zum Gewerbezentralregister detaillierte Vorschriften, welche Informationen dort überhaupt zu speichern sind (beispielsweise nur bestimmte Bußgeldentscheidungen, und auch diese erst dann, wenn sie rechtskräftig sind), zu welchen Zwecken sie an wen übermittelt werden dürfen und unter welchen Voraussetzungen sie wieder zu löschen sind. Auch das Bundeszentralregistergesetz enthält verschiedene Regelungen zur Sicherung der Persönlichkeitsrechte (abgestufte Informationszugriffe).

Alle diese Freiheitsrechte sichernden Restriktionen im Informationsfluß liefen leer, wenn eine Erhebung von sachlich vom Register erfaßten Daten an diesem vorbei zugelassen würde.

Der vorliegende Gesetzentwurf ist darüber hinaus unvollständig, weil er keine Änderungen weiterer Vorschriften des Gewerberechts vorsieht, die nach dem vor mehr als sieben Jahren ergangenen Volkszählungsurteil des Bundesverfassungsgerichts dringend einer Überarbeitung bedürfen. Beispiele habe ich in meinem 12. Tätigkeitsbericht (S. 81f.) genannt.

22.2 Berufsrecht der Steuerberater

Das Fünfte Gesetz zur Änderung des Steuerberatungsgesetzes hat in einem dem § 10 des Steuerberatungsgesetzes angefügten neuen Absatz 2 eine allgemeine Rechtsgrundlage für die Übermittlung personenbezogener Daten, insbesondere von Steuerberatern und Steuerbevollmächtigten, für berufsrechtliche Zwecke geschaffen. Der Entwurf orientierte sich ursprünglich an der entsprechenden Vorschrift im Berufsrecht der Rechtsanwälte (§ 36 a Abs. 3 der Bundesrechtsanwaltsordnung), die unter meiner Mitwirkung formuliert worden war. Diese Fassung habe ich als ausgewogen und datenschutzrechtlich akzeptabel bewertet, insbesondere im Hinblick auf den vorgesehenen Satz 2, nach dem die Übermittlung einschränkungslos unterbleiben sollte, wenn ihr besondere gesetzliche Verwendungsregelungen entgegenstehen. Auf Anregung des Bundesrats ist dieser Übermittlungsausschluß in der Fassung des verabschiedeten Gesetzes durch einen Halbsatz eingeschränkt worden, wonach dies nicht für das Steuergeheimnis nach § 30 der Abgabenordnung (AO) gilt. Gegen diese Anregung hatte ich Bedenken angeführt und statt dessen vorgeschlagen, eine Übermittlung nur für den Fall zuzulassen, daß daran ein „zwingendes öffentliches Interesse" im Sinne von § 30 Abs. 4 Nr. 5 AO besteht. Es hätte klargestellt werden können, daß ein solches „zwingendes" öffentliches Interesse erreicht ist, wenn die zu übermittelnden Umstände von solchem Gewicht sind, daß sie einen Widerruf der Bestellung zum Steuerberater rechtfertigen.

Leider sind meine Bedenken vom Bundesminister der Finanzen nicht aufgegriffen worden. Die letztlich beschlossene Fassung ändert aber nichts daran, daß eine Übermittlung nur dann erfolgen darf, wenn die im erhalten gebliebenen Satz 1 der Vorschrift aufgestellten Voraussetzungen erfüllt sind. Danach ist eine Übermittlung, die schutzwürdige Belange des Betroffenen beeinträchtigt, nur dann zulässig, wenn das öffentliche Interesse das Geheimhaltungsinteresse des Betroffenen überwiegt; hierbei ist auch zu berücksichtigen, daß Informationen, die dem Steuergeheimnis unterliegen, besonders zu schützen sind; dies ist bei der vorgesehenen Abwägung zu beachten. Im Hinblick hierauf habe ich davon abgesehen, meinen Änderungswunsch weiterzuverfolgen.

Eine weitere Neuerung ist, daß mit einem eingefügten § 37 d nunmehr im Steuerberatungsgesetz selbst eine ausdrückliche Regelung über die vom Bewerber für die Steuerberaterprüfung zu machenden Angaben getroffen ist. Nach dem neuen Recht wird die Informationserhebung über einen Fragebogen erfolgen. An weiteren Unterlagen können nur Nachweise verlangt werden. Hierdurch ist klargestellt, daß vom Bewerber insbesondere auch kein Lebenslauf gefordert werden kann, wogegen ich mich schon bisher ausgesprochen habe. Auch der Verordnungsgeber kann nicht ermächtigt sein, eine solche Befugnis zu begründen, zumal mit einem „lückenlosen Lebenslauf mit genauen Angaben über Person und beruflichen Werdegang" (so die Bestimmung der derzeitigen Durchführungsverordnung) auch Daten erhoben werden, die für die Zulassungsentscheidung nicht erforderlich sind. Bei der nunmehr anstehenden Anpassung der Durchführungsverordnung ist dies zu berücksichtigen.

Unbefriedigend ist, daß die Pflichtmitteilung über die Bestellung des Leiters einer Beratungsstelle eines Lohnsteuerhilfevereins künftig nicht nur — wie bisher — den Nachweis enthalten muß, daß der Beratungsstellenleiter mindestens drei Jahre auf dem Gebiet des Lohnsteuerwesens hauptberuflich tätig ge-

wesen ist, sondern auch, daß „er sich nicht so verhalten hat, daß die Besorgnis begründet ist, er werde die Pflichten des Lohnsteuerhilfevereins nicht erfüllen". Damit wird nunmehr ein Negativnachweis gefordert, der praktisch nicht möglich ist. In der nun anzupassenden Durchführungsverordnung wird eine sachgerechte Auslegung dieser problematischen Bestimmung erfolgen müssen. In Betracht käme eine Regelung, den Nachweis über die persönliche Zuverlässigkeit durch Vorlage eines polizeilichen Führungszeugnisses zu erbringen, was auch der Finanzausschuß des Bundestages in seinem Bericht zum Fünften Gesetz zur Änderung des Steuerberatungsgesetzes erwähnt.

22.3 Berufsrecht der Wirtschaftsprüfer

Bezogen auf das Berufsrecht der Wirtschaftsprüfer sind im Rahmen eines vorgesehenen Dritten Gesetzes zur Änderung der Wirtschaftsprüferordnung ähnliche Probleme aufgeworfen, wie unter 22.2 für den Bereich der Steuerberater dargelegt. Die entsprechende Durchführungsverordnung (Prüfungsordnung für Wirtschaftsprüfer) enthält derzeit noch eine Bestimmung, wonach dem Antrag auf Zulassung zur Wirtschaftsprüfer-Prüfung ein „lückenloser Lebenslauf" beizufügen ist. In neueren Prüfungsordnungen für Eignungsprüfungen als Wirtschaftsprüfer, die die Prüfungsdurchführung für solche Bewerber aus dem Bereich der neuen Bundesländer und der EG regeln, die dort schon eine einschlägige Vorbildung erlangt hatten, ist das Wort „lückenlos" nicht übernommen. Dies ist ein erster zu begrüßender Schritt.

23 Umweltschutz

23.1 Zugang zu Umweltinformationen

Am 7. Juni 1990 ist die Richtlinie des Rates der Europäischen Gemeinschaften über den freien Zugang zu Informationen über die Umwelt (Nr. 7610/90) verabschiedet worden. Die Richtlinie hat das Ziel, jedermann in der Gemeinschaft einen grundsätzlich freien Zugang zu den bei den Behörden verfügbaren umweltbezogenen Informationen zu eröffnen. Als Richtlinie ist die Bestimmung an die Mitgliedsstaaten gerichtet, die nun ihrerseits nationale Gesetze schaffen müssen, die die Grundsätze der Richtlinie umsetzen.

Die Richtlinie gestattet es den Mitgliedsstaaten, in ihren Umsetzungsgesetzen vorzusehen, daß ein Auskunftsantrag abgelehnt werden kann, wenn „die Vertraulichkeit personenbezogener Daten und/oder Akten" berührt ist. Im Rahmen meiner Beteiligung hatte ich mit dem Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit Einvernehmen erreicht, daß der möglicherweise mißverständliche Zusatz „die Vertraulichkeit" aus dem Entwurf der EG-Kommission zu streichen sei, um klarzustellen, daß personenbezogene Daten vom Grundsatz her vertraulich sind. Ich bedauere, daß diese Änderung nicht durchgesetzt worden ist.

Auf der Basis der verabschiedeten Richtlinie wird es nunmehr darauf ankommen, den Grundsatz der allgemeinen Vertraulichkeit personenbezogener Daten im deutschen Umsetzungsgesetz klar zum Ausdruck zu bringen. Ein Entwurf zu einem solchen Gesetz liegt mir noch nicht vor.

23.2 Europäisches Umweltinformationsnetz

Am 7. Mai 1990 hat der Rat der Europäischen Gemeinschaften eine Verordnung zur Errichtung einer Europäischen Umweltagentur und eines Europäischen Umweltinformations- und Umweltbeobachtungsnetzes verabschiedet, die unmittelbar in jedem Mitgliedstaat gilt.

Die Verordnung bezweckt eine Sammlung, Aufbereitung und Analyse von Umweltdaten auf europäischer Ebene, um objektive, zuverlässige und vergleichbare Informationen zu erhalten, die es ermöglichen, die auf dem Gebiet des Umweltschutzes unentbehrlichen Maßnahmen zu ergreifen und eine angemessene Unterrichtung der Öffentlichkeit über den Zustand der Umwelt sicherzustellen. Hierzu werden u. a. bestehende nationale Informationssysteme miteinander vernetzt. Damit sind umfangreiche grenzüberschreitende Datenflüsse eröffnet, die — wenn auch nur am Rande — auch personenbezogene Daten enthalten. Ich habe deshalb betont, daß seitens deutscher Stellen eine Übermittlung personenbezogener Daten an Stellen außerhalb des Anwendungsbereiches deutscher Datenschutzregelungen nur unter der Voraussetzung erfolgen darf, daß auch der Empfänger aufgrund des für ihn geltenden Rechts bei der Informationsverwendung Datenschutzregelungen unterliegt, die mindestens dem der Datenschutzkonvention des Europarats entsprechen.

Ein derartiger Datenschutzstandard ist derzeit auf EG-Ebene jedoch noch nicht in allen Mitgliedstaaten gesichert. Der Bundesumweltminister hat mir mitgeteilt, er werde den Datenschutzvorschriften des Bundesstatistikgesetzes und der jeweiligen Fachgesetze (z. B. des Bundes-Imissionsschutzgesetzes), die er durch die EG-Verordnung nicht verdrängt sieht, dadurch Rechnung tragen, daß er personenbezogene Daten nur nach Maßgabe dieser Bestimmungen für das Europäische Umweltinformationsnetz bereitstellt. Ich begrüße diese Position.

24 Landwirtschaft

24.1 EG-Informationssystem „Wiedereinziehung zu Unrecht gezahlter Agrarsubventionen"

Seit 1972 ist eine EG-Verordnung „betreffend die Unregelmäßigkeiten und die Wiedereinziehung zu Unrecht gezahlter Beträge im Rahmen der Finanzierung der gemeinsamen Agrarpolitik sowie die Einrichtung eines einschlägigen Informationssystems" in Kraft. In ihrer bislang geltenden Fassung sieht diese Verordnung vor, daß die Mitgliedstaaten der EG-Kommission periodisch eine anonymisierte Aufstellung über Unregelmäßigkeiten, die Gegenstand einer ersten

amtlichen oder gerichtlichen Feststellung gewesen sind, übermitteln. Diese Mitteilung soll nach einem nun vorliegenden Änderungsentwurf künftig personenbeziehbar erfolgen.

Ich habe Zweifel geäußert, ob die vorgesehene Einführung der Personenbeziehbarkeit erforderlich ist. Der im Verfahren auf Seiten der Bundesrepublik Deutschland federführende Bundesminister der Finanzen hat aber darauf hingewiesen, daß diese Änderung durch konkrete Vorfälle fachlich veranlaßt ist. In der Vergangenheit seien einzelne Fälle unrechtmäßigen Subventionsbezugs erst verzögert und durch glückliche Umstände aufgeklärt worden, die bei Zusammenführung der in den Mitgliedsstaaten vorhandenen Informationen frühzeitiger und problemfreier hätten entdeckt werden können.

Die mir vorgetragenen Argumente sind plausibel. Es muß jedoch sichergestellt sein, daß die Übermittlung nur dann erfolgt, wenn sie im Einzelfall tatsächlich erforderlich ist. Ein französischer Vorschlag, wonach von der Mitteilung solche Fälle ausgenommen sein sollen, „wo die Mitteilung zur Verfolgung der Unregelmäßigkeiten nicht nützlich ist", weist dabei in die richtige Richtung und hat gute Aussicht, in die endgültige Änderungsverordnung einzugehen. Das Erforderlichkeitsprinzip sollte allerdings noch klarer und als postive Übermittlungsvoraussetzung formuliert werden.

Ferner sieht der Änderungsvorschlag vor, daß neben bereits derzeit erfolgenden Mitteilungen über gerichtliche oder verwaltungsmäßige Wiedereinziehungsverfahren künftig zusätzlich die zur Anwendung von Strafmaßnahmen infolge von Unregelmäßigkeiten eingeleiteten Gerichts- und Verwaltungsverfahren mitzuteilen sind. Derartige Mitteilungen verlangen nach datenschutzrechtlichen Begleitregelungen. Ich habe dem Bundesminister der Finanzen empfohlen, insoweit — orientiert am vorliegenden Entwurf eines Justizmitteilungsgesetzes — ergänzende Regelungen zu erwirken, die die Wahrung von Verhältnismäßigkeitsgrundsatz, Zweckbindung und Gewährung rechtlichen Gehörs sichern. Da es sich bei der durch die vorgeschriebenen Mitteilungen entstehenden Datei praktisch um eine Art Strafregister handeln würde, sind auch angemessene Bestimmungen über die Löschung von Eintragungen in die Datei unerläßlich. Ich habe auch dazu Vorschläge unterbreitet.

Schließlich ist vorgesehen, daß Bedienstete der Kommission an Untersuchungen teilnehmen können, die von Bediensteten der einzelstaatlichen Verwaltungen in Ausübung ihres Amtes zur Feststellung einer Unregelmäßigkeit durchgeführt werden; die Kommission versteht unter solchen Untersuchungen auch Strafverfahren. Hierzu ist zu bemerken, daß die spezifischen Erhebungsbefugnisse und Erhebungszwangsmittel im Strafverfahren nur für Zwecke des Strafverfahrens genutzt werden dürfen. Aus diesem Grunde bin ich gegen jedwede Beteiligung der Kommission an Strafverfahren, soweit diese nicht öffentlich sind. Insbesondere muß eine Teilnahme der Kommission an Vernehmungen und Hausdurchsuchungen ausscheiden.

24.2 Wasserverbandsgesetz

Der Regierungsentwurf des 1990 verabschiedeten Gesetzes über Wasser- und Bodenverbände sah vor, daß im Rahmen der öffentlichen Bekanntmachung der beabsichtigten Errichtung eines Wasser- und Bodenverbandes auch ein Verzeichnis derjenigen, die Beteiligte dieses Verbandes werden sollen, auszulegen ist. Mit dem Verzeichnis wären nicht nur Name und Anschrift, sondern — aus dem Bekanntmachungskontext — weitere personenbezogene Daten der Betroffenen der Allgemeinheit uneingeschränkt zugänglich gewesen. Damit wäre nämlich zugleich publiziert, daß die Betroffenen die gesetzlichen Beteiligungsvoraussetzungen erfüllen, beispielsweise indem sie Eigentümer eines im räumlichen Wirkungsbereich des Verbandes belegenen Grundstücks sind.

Ich habe den Bundesminister für Ernährung, Landwirtschaft und Forsten darauf hingewiesen, daß diese Beeinträchtigung der informationellen Selbstbestimmung nicht erforderlich ist.

Die Auslegung des Verzeichnisses derjenigen, die Beteiligte werden sollen, bezweckt im wesentlichen, diesen Betroffenen vor einer konstitutiven, behördlichen Feststellung ihrer Beteiligten-Eigenschaft rechtliches Gehör zu gewähren und ihnen die Möglichkeit der Vorbereitung von Anträgen zu geben. Dieser Zweck kann noch besser durch eine individuelle Benachrichtigung der Betroffenen erreicht werden. Bloße Erwägungen der Verwaltungsökonomie rechtfertigen keinen Eingriff in die informationelle Selbstbestimmung durch eine öffentliche Zustellung, soweit eine gewöhnliche Zustellung möglich ist.

Die Bundesregierung war jedoch nicht bereit, meinen Bedenken in vollem Umfange Rechnung zu tragen. Aus pragmatischen Erwägungen habe ich daraufhin hilfweise vorgeschlagen, eine Regelung in das Gesetz aufzunehmen, wonach die Einsicht in das Verzeichnis nur unter den Voraussetzungen zulässig ist, nach denen Grundbucheinsicht gewährt wird, also nur bei Darlegung eines berechtigten Interesses. Dem lag die Erwägung zugrunde, daß im wesentlichen grundbuchmäßig erfaßte Daten offenbart werden und insofern ohnehin die — beschränkte — Publizität des Grundbuchs besteht.

Mein an § 12 Abs. 1 Satz 1 der Grundbuchordnung orientierter Kompromißvorschlag ist in § 14 Abs. 1 Satz 2 des Wasserverbandsgesetzes berücksichtigt.

24.3 Meisterprüfung

Im Rahmen der Meisterprüfung im Weinbau wird nach geltendem Recht von Prüfungsteilnehmern grundsätzlich verlangt, dem Prüfungsausschuß eine Betriebs- und Entwicklungsanalyse über einen existierenden Betrieb abzuliefern. In einer im Entwurf vorliegenden Verordnung für die Meisterprüfung für den Beruf Landwirt werden ähnliche Anforderungen aufgestellt, wobei ausdrücklich bestimmt wird, daß die Hausarbeit über den Betrieb zu erstellen ist, in dem der Prüfungsteilnehmer tätig ist. Im letztgenannten Verordnungsentwurf ist nicht mehr vorgesehen,

daß — wie bisher und für Winzer auch weiterhin — ausnahmsweise eine andere Prüfungsaufgabe gestellt werden kann, wenn die Erteilung der grundsätzlich geforderten betriebswirtschaftlichen Arbeit nicht möglich ist.

In den Prüfungsausschüssen für die anerkannten Ausbildungsberufe der Landwirtschaft können nach den Regelungen in den Ländern derzeit auch Konkurrenten des Prüflings und des Betriebs, in dem er tätig ist, als Prüfer mitwirken.

Insbesondere vor diesem Hintergrund halte ich es für datenschutzrechtlich sehr problematisch, daß ein Prüfungsteilnehmer gezwungen ist, detaillierte Angaben über einen — unter Umständen sogar seinen eigenen künftigen — Betrieb zu offenbaren. Zwar unterliegen die Prüfungsausschußmitglieder einer — strafrechtlich bewehrten — Verschwiegenheitspflicht. Dies schließt jedoch nicht die Gefahr aus, daß die in der Prüfung erhobenen Informationen über den Betrieb zu Wettbewerbszwecken vom konkurrierenden Prüfungsausschußmitglied selbst genutzt werden. Den Prüfungsteilnehmern sollte deshalb die Wahlmöglichkeit eingeräumt werden, eine Hausarbeit über einen anderen Gegenstand, beispielsweise einen fiktiven Betrieb, abzuliefern.

Ich werde in diesem Sinne weiterhin auf eine Überarbeitung der Winzermeisterprüfungsverordnung und der Landwirte-Meisterprüfungsverordnung hinwirken.

25 Datensicherung

25.1 Aktivitäten der Bundesregierung

In meinem 12. Tätigkeitsbericht konnte ich über Bemühungen der Bundesregierung berichten, eine Stelle zu schaffen, die durch Forschung, Entwicklung, Beurteilung, Zertifizierung und Beratung einen seit langem notwendigen Beitrag zur Sicherheit in der Informationstechnik leisten soll. Die Verabschiedung des Gesetzes über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und die zum 1. Januar 1991 erfolgte Errichtung dieses Amtes sind entscheidende Schritte auf dem Weg, dieses Ziel zu erreichen. Ich begrüße besonders, daß das neue Amt aufgrund einer gegen Ende der parlamentarischen Beratungen erreichten Erweiterung seiner gesetzlichen Aufgaben nun auch die Beratung der Anwender von Informationstechnik entsprechend dem Bedarf durchführen kann.

Für die Erfüllung der Aufgaben des neuen Amtes hat dessen Vorläuferorganisation, die Zentralstelle für Sicherheit in der Informationstechnik (ZSI), bereits wesentliche Vorarbeiten geleistet. Dazu gehören

- die Herausgabe von IT-Sicherheitskriterien und die Bemühungen um einen internationalen Konsens über solche Kriterien,
- die Herausgabe eines Evaluationshandbuchs, das sich in erster Linie an Hersteller wendet, die entsprechende Produkte zertifizieren lassen möchten, sowie an Stellen, die bei der Zertifizierung mitwirken wollen, sowie
- der für den Anwender sehr wichtige Beginn der Bewertung und Zertifizierung von praktisch einsetzbaren Produkten (s. 25.2.1.)

Leider hat sich die Fertigstellung des zur Unterstützung der Anwender geplanten IT-Sicherheitshandbuches so verzögert, daß seine Veröffentlichung erst im Frühsommer 1991 möglich sein wird. Damit fehlt immer noch eine lange erwartete Hilfe für den Anwender. Zwar ist der Teil dieses Handbuches, der sich mit den Hinweisen zum sicheren Einsatz von Personalcomputern beschäftigt, vorab veröffentlicht worden; die noch immer eher abwartende Haltung vieler Anwender konnte damit aber noch nicht grundlegend verändert werden. Eine solche Änderung ist aber dringend geboten. Denn für viele Anwendungen könnten wesentliche Sicherheitsmängel mit der verfügbaren Technik und meist sogar mit nur wenig Mühe behoben werden, wenn die Anwender nur anfingen, sich ernsthaft um die Sicherheit ihrer Informationsverarbeitung zu kümmern. Dies zeigen meine Kontrollen (s. 25.2.2) ebenso wie die Untersuchungen des Bundesrechnungshofes.

25.2 Personalcomputer

Die erheblichen Anforderungen an meine Dienststelle belasten auch die Kapazität für Kontrollen und Beratungen hinsichtlich der Datensicherheit. Deshalb habe ich meine Aktivitäten wie schon im Vorjahr im wesentlichen auf den Einsatz von Personalcomputern (PC) konzentriert, weil hier nach allen Erfahrungen die Defizite am größten, Beratungen und Kontrollen also am nötigsten sind.

25.2.1 PC-Sicherheitsprodukte

Die in meinem Zwölften Tätigkeitsbericht beschriebene Entwicklung im Bereich der Datensicherheit für Personalcomputer hat sich im Berichtsjahr fortgesetzt. Eine Vielzahl von Produkten zur Verbesserung der Sicherheit von Personalcomputern wird inzwischen angeboten. Darunter befinden sich sowohl reine Softwarelösungen als auch reine Hardwarelösungen, aber auch Kombinationen von beiden. Der Überblick für den Benutzer ist nach wie vor schwierig. Dieser ist weitgehend auf Marktübersichten in Fachzeitschriften angewiesen, um ein für seine Anwendung geeignetes Produkt zu finden. Weil es dem einzelnen Anwender häufig schwerfallen wird, die erreichte Sicherheit zu beurteilen, begrüße ich, daß die ZSI (ab 1. Januar 1991: BSI) zur Prüfung und Zertifizierung solcher Produkte in der Lage ist und sie auch bereits durchgeführt hat. Einen ersten Erfolg stellt die Zertifizierung des für PC mit dem Betriebssystem MS-DOS ab Version 4.0 einsetzbaren Produktes „SAFEGUARD" dar.

Ebenfalls noch von der ZSI wurde in Zusammenarbeit mit einer Firma für Industrieelektronik die Kryptobaugruppe DVAT (Datenverschlüsselung auf AT-Rechnern) entwickelt, die innerhalb der Bundesver-

waltung verbreitet zum Einsatz kommen soll. Diese steckbare Karte wird aber nur für Anwendungen im Rahmen der Verschlußsachenanweisung (VSA), die durch einen Geheimschutzbeauftragten betreut werden, freigegeben. Sie kann in stand-alone-PC der Typen IBM XT und IBM AT sowie dazu kompatiblen PC anderer Hersteller eingesetzt werden. In Verbindung mit einem abstrahlgeschützten Gerät ist auch die Verarbeitung von Daten zulässig, die VS-Vertraulich (und höher) eingestuft sind. Der Anwender muß dem BSI den Verbleib der Baugruppe nachweisen.

Die Karte bewirkt eine Zwangsverschlüsselung der Festplatte und der Disketten; gleichwohl besteht die kennwortgeschützte Möglichkeit, unverschlüsselte Disketten zu lesen. Leider führt die Kryptobaugruppe keine Benutzerverwaltung durch. Sollen mehrere Benutzer am selben PC arbeiten, müssen sie daher gegenüber dem PC mit dieser Karte alle als derselbe Benutzer erscheinen und dasselbe Paßwort benutzen.

Daß gelegentlich in standardmäßig gelieferten Programmen auch noch immer gefährliche Schwachstellen zu finden sind, zeigt das folgende Beispiel: Der Emulator eines bekannten deutschen Herstellers, unter dem PC in einer UNIX-Anlage betrieben werden können, enthält auch die Funktion eines sogenannten „Auto-log-in". Damit kann ein Benutzer seine Anmeldung bei dem UNIX-Rechner protokollieren und dieses Protokoll bei künftigen Anmeldungen „auf Knopfdruck" ablaufen lassen. Er erspart sich damit die Eingabe von Benutzernamen und Paßwort. Dies stellt eine erhebliche Schwachstelle dar, da auch ein Angreifer, der sich Zugang zu dem PC verschaffen kann, in die Lage versetzt wird, sich bei dem UNIX-System als bekannter Benutzer anzumelden. Verschärft wird dieser Mangel durch die Tatsache, daß der befugte Benutzer nicht erkennen kann, ob seine Anmeldung beim System protokolliert wird oder nicht. Eine Rückfrage bei dem Hersteller hat ergeben, daß dieses „Trojanische Pferd" in der neuen Version des Emulators nicht mehr vorhanden ist.

25.2.2 Ergebnisse von Kontrollen der PC-Sicherheit

Auch in diesem Berichtszeitraum mußte ich feststellen, daß die Sicherheit des PC-Einsatzes bei den kontrollierten Stellen des Bundes häufig unzureichend gewährleistet war. Es gibt zwar auch ermutigende Anzeichen dafür, daß dieser Zustand änderbar ist, trotzdem ist das Gesamtbild noch immer schlecht. Die Hauptursache dafür ist, daß die Verantwortlichen sich um diese Fragen nicht oder nur unzureichend kümmern; deshalb treten im Prinzip bereits bekannte Schwächen fast überall immer wieder neu auf.

Typische und wichtige Feststellungen aus einzelnen Kontrollen waren:

PARLAKOM

Nachdem ich vom Ältestenrat des Deutschen Bundestages um eine Stellungnahme zu PARLAKOM gebeten worden war, habe ich in den vergangenen Jahren die Bundestagsverwaltung wiederholt beraten und darüber, zuletzt in meinem Zwölften Tätigkeitsbericht (s. S. 18ff.), berichtet. Dabei konnte ich feststellen, daß bei dem Einsatz von Arbeitsplatzcomputern auch Fragen der Sicherheit sorgfältig beachtet wurden.

Anläßlich einer Sendung des ARD-Magazins „Monitor" über angebliche Mängel der Datensicherheit bei PARLAKOM hat mich der Direktor des Deutschen Bundestages erneut um eine Stellungnahme gebeten. Die Untersuchung eines für den Einsatz typischen und mit den entsprechenden Programmen versehenen Gerätes ergab, daß ein Zugriff von außen, so wie er von „Monitor" gezeigt worden war, nicht möglich ist, die behauptete Schwachstelle also nicht besteht.

Für einen Angreifer der — wenn auch nur vorübergehend — über ein PARLAKOM-Gerät verfügen kann, ist jedoch ein Eindringen in die Dateien dieses Geräts möglich. Da es sich bei den Daten auf der Festplatte des PC u. a. um Anschriften von Ansprechpartnern der Bundestagsabgeordneten handelt, habe ich dringend den Einsatz der Kryptobaugruppe DVAT (s. 25.2.1) empfohlen.

— Verbesserungen im BMU

Die nach der Kontrolle des PC-Einsatzes im Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit zugesagte Beseitigung der Mängel, über die ich in meinem Zwölften Tätigkeitsbericht (S. 87f.) berichtet habe, ist inzwischen nahezu abgeschlossen. Der BMU hat mir zu Anfang des Berichtsjahres mitgeteilt, die Einbindung der PC, deren ungeregelten Einsatz ich beanstandet hatte, in das bei ihm bestehende Netz werde angestrebt. Zur Zeit erlaube die Kapazität des Zentralrechners dieses Vorgehen jedoch nicht.

Eine Rückfrage hat ergeben, daß eine neue Anlage beim BMU installiert wird; die Einbindung aller PC ist fast abgeschlossen.

— PC-Einsatz bei der Fahndungsunion

Weil schon am 1. Juli 1990 die Personenkontrollen an der innerdeutschen Grenze aufgehoben wurden, haben die damals noch bestehenden beiden deutschen Staaten eine Fahndungsunion beschlossen, in deren Rahmen polizeiliche Fahndungsdaten ausgetauscht wurden. Dabei bestand das Problem, daß die kommunikationstechnische Infrastruktur in der früheren DDR eine zuverlässige Online-Verbindung nicht ermöglichte. Deshalb war (und ist) zur Datenversorgung der Polizeidienststellen im Gebiet der früheren DDR der Einsatz von PC geboten, deren Daten durch in kurzen Abständen erfolgende Aktualisierung stets möglichst aktuell gehalten werden.

Aufgrund einer vertraglichen Vereinbarung zwischen den beiden deutschen Staaten wurde mir schon vor dem Beitritt die datenschutzrechtliche Kontrolle dieser Datenverarbeitung übertragen (s. auch 2.3). Deshalb habe ich schon vor dem 3. Oktober 1990 beim Zentralen Kriminalinstitut (ZKI) und der Zentralstelle für kriminalistische Informationsverarbeitung (ZSKI)

in Ostberlin sowie beim Bezirkskriminalamt Potsdam einen Beratungs- und Kontrollbesuch durchgeführt. Untersucht wurde der Einsatz von Einzelplatzsystemen (PC) im Rahmen der Fahndungsunion.

Das BKA Wiesbaden übermittelt an das ZSKI die notwendigen Daten des Anfangsbestandes, der auf die Festplatten der auszuliefernden PC für die einzelnen Dienststellen eingetragen wird. Die Bestände werden mit Hilfe von Disketten aktualisiert, die im Rahmen meist ohnehin erfolgender Kurierfahrten zugestellt werden. Das dabei eingesetzte Diskettenverwaltungssystem ist ausreichend sicher. Auch das organisatorische Umfeld (z. B. Objektschutz) bietet ungewöhnlich guten Schutz. Die technische Sicherheit des eigentlichen Verfahrens war im Zeitpunkt der Kontrolle dagegen gering, denn die bekannten Mängel beim Einsatz von Personalcomputern (s. insbesondere 12. TB S. 87 ff.) waren auch hier vorhanden. Im Hinblick auf die Tatsache, daß sich die Mängel angesichts des besonders sicheren organisatorischen Umfeldes weniger auswirken dürften, und weil es sich um eine Übergangslösung handelt, habe ich meine Bedenken gegen das Verfahren zurückgestellt und lediglich einige einfach umzusetzende Verbesserungsmaßnahmen vorgeschlagen.

— PC-Einsatz im Bahnhof

Im Berichtszeitraum habe ich den PC-Einsatz in einem Bahnhof der Deutschen Bundesbahn kontrolliert.

Dieser Bahnhof gehört zu einer Stadt mit weniger als 100 000 Einwohnern und ist nur mit einem Rechner mit fünf Terminals und einem angeschlossenen PC sowie einem eigenständig betriebenen PC ausgestattet.

Auf dem Terminalrechner wird in erster Linie die örtliche Personaldatenverarbeitung (ÖPDV) betrieben. Daneben laufen eine Bürokommunikationsanwendung mit Textverarbeitung, Kalender und Büro-Mail sowie ein Pilotprojekt betreffend die Ablauforganisation in der Dienststelle.

Der angeschlossene PC hat Zugriff auf das Bürokommunikationssystem und wird für die Textverarbeitung benötigt, mit der auch Dateien mit personenbezogenen Daten geführt werden.

Mit dem stand-alone-PC wird in erster Linie Textverarbeitung durchgeführt. Daneben existieren Kalkulationsprogramme und Datenbankanwendungen.

Die Übersicht über die Art der gespeicherten personenbezogenen Daten (§ 15 BDSG) entsprach im Kontrollzeitpunkt hinsichtlich Vollständigkeit und Detailtiefe den Anforderungen. Ein leitender Mitarbeiter des Bahnhofs war als Datenschutzbeauftragter eingesetzt.

Die Unterbringung der Datenverarbeitungsanlagen war nicht ausreichend sicher, weil der entsprechende Raum von dem offenen Bereich für das Publikum und die im Schichtdienst wechselnden Mitarbeiter nicht genügend abgegrenzt war.

Die Disketten, auf denen immerhin jeweils der Inhalt von mehreren hundert Schreibmaschinenseiten Platz hat, wurden wohl wegen ihres geringen Preises als Verbrauchsmaterial behandelt. Es existierte keine Nachweisführung der eingesetzten Datenträger; diese waren uneinheitlich oder überhaupt nicht gekennzeichnet. Inventuren waren bisher noch nicht durchgeführt worden. Es war auch nicht bekannt, wie viele Disketten vorhanden sein mußten. Darüber hinaus wurden die Disketten zwar in verschließbaren Behältnissen aufbewahrt, diese jedoch in den Diensträumen in einfachen Büroschränken gelagert. Bei Diebstahl, Brand oder anderen Havarien wären die entsprechenden Anwendungssysteme arbeitsunfähig geworden.

Die Zugriffsberechtigung und der Paßwortschutz des Terminalrechners waren insoweit unzureichend gestaltet, als die Benutzertabelle neben den berechtigten Nutzern der Dienststelle auch Systemzugänge für Wartungspersonal sowie einige unklare Systemzugänge enthielt. Bei der Paßwortprüfung waren zehn Fehlversuche noch zulässig.

Die beiden Personalcomputer waren nicht mit Sicherheitssoftware ausgestattet. Die Festplatten beider Rechner enthielten Software unklarer Herkunft, die teilweise „versteckt" gespeichert worden waren. Dem kundigen Nutzer dieser Software wären damit leicht beliebige Manipulationen möglich geworden. Da in solchen Fällen der Verdacht auf sogenannte „Raubkopien" nicht auszuschließen ist, besteht auch die Gefahr der Infizierung der Systeme durch Computerviren o.ä.

Wegen dieser und einiger anderer Mängel habe ich dringend empfohlen, daß der zentrale Systemdienst der Deutschen Bundesbahn sich des Einsatzes von Arbeitsplatzcomputern auf Bahnhöfen annimmt, damit die bestehenden Regelungen auch hier eingehalten werden.

— Unzureichender Zugriffsschutz

Eine der im Berichtsjahr kontrollierten PC-Anwendungen im Geschäftsbereich des Auswärtigen Amtes verfügte über etwa 15 PC, die untereinander (lokal) durch ein Netz verbunden waren. Meine Kontrolle förderte, obwohl in dieser Behörde sowohl von der Aufgabenstellung als auch von den Umgebungsbedingungen her Sicherheitsmaßnahmen geboten waren, einen unvertretbar leichtfertigen Umgang mit den Zugriffsberechtigungen zu Tage. Der wesentliche Schutzmechanismus bestand darin, daß im Prinzip jeder Berechtigte sich durch ein nur ihm bekanntes Paßwort dem PC gegenüber als berechtigt ausweisen mußte. Trotzdem benutzte keiner der etwa 20 Berechtigten ein Paßwort, in dem Buchstaben und Ziffern gemischt vorkamen, und zehn Paßwörter bestanden aus nur drei Zeichen. Unter den gewählten Paßwörtern befanden sich Vornamen oder andere gebräuchliche Wörter, wie z. B. „Urlaub". Es gab nicht nur einen „Eingang" für die Wartung, sondern auch einen befugten Benutzer mit dem Namen „test" und mit dem Paßwort „test". Derartige „Hintertüren" sind in

der Fachwelt allgemein bekannt. Jeder Systemverwalter sollte sie unverzüglich aus seinen Benutzertabellen entfernen.

Schwachstellen dieser Art, die ich ganz ähnlich auch an anderen Stellen angetroffen habe, lassen sich mit wenig Mühe von den für Sicherheit Verantwortlichen in den einzelnen Stellen finden und beseitigen. Es ist als Organisationsversagen zu bewerten, wenn dies noch immer nicht erfolgt.

25.2.3 Regelungen für den PC-Einsatz

Die in meinem Zwölften Tätigkeitsbericht enthaltenen Empfehlungen und sonstigen Hinweise sind von einigen Stellen in der Weise aufgegriffen worden, daß sie für ihren Verantwortungsbereich daran orientierte Regelungen erlassen haben. Insbesondere die DBP Postdienst hat nach Beratungen mit ihrem Hauptpersonalrat, an denen ich beteiligt war, eine sachgerechte Vorgabe für den PC-Einsatz im Postdienst geschaffen: Ähnliche Regelungen bereitet die DBP TELEKOM für ihren Bereich vor.

Soweit das von mir vorgeschlagene Schema zur Erfassung und Beschreibung des PC-Einsatzes (12. TB Anlage 11 S. 113ff.) verwendet wird, hat es sich als zweckmäßig erwiesen. Daran ändert auch die Feststellung einer Behörde nichts, daß dieses Mittel zwar nützlich, mit seiner Anwendung aber auch ein deutlich spürbarer Aufwand verbunden ist. Denn in dieser Behörde waren über 300 Geräte zu erfassen, so daß entsprechend umfangreiche Anstrengungen durchaus geboten waren, um einen ordnungsgemäßen Einsatz einer so großen Zahl von PC zu gewährleisten.

Zum ordnungsgemäßen Einsatz von Arbeitsplatzcomputern gehört auch eine dem Personalvertretungsrecht entsprechende Lösung der Mitbestimmungsfrage. Denn in den Systemen werden häufig intern Verwaltungsdateien geführt, die im normalen Ablauf auch für den Benutzer nicht besonders in Erscheinung treten, die aber trotzdem für Zwecke der Verhaltens- und Leistungskontrolle genutzt werden können. So werden z. B. in Textverarbeitungssystemen in der Regel Dateien geführt, denen der Autor, die Schreibkraft, das Datum der ersten Eingabe, das Datum der letzten Bearbeitung und die Textlänge entnommen werden können. Die einfachste und im allgemeinen auch sachgerechteste Lösung des Mitbestimmungsproblems ist eine Vereinbarung, mit der die Nutzung dieser Daten für Zwecke der Verhaltens- und Leistungskontrolle mit Ausnahme von etwaigen Auswertungen zu Datenschutz- und Datensicherungsprüfungen ausgeschlossen wird. Solche Lösungen sind auch deswegen sinnvoll, weil die Auswertung dieser Daten den konventionellen Methoden der Verhaltens- und Leistungsbeurteilung unterlegen ist und so kontrollierte Mitarbeiter mit vergleichsweise wenig Aufwand diese Dateien und ihre Auswertung durch vom System „zählbare", für die Erfüllung ihrer Aufgaben aber nutzlose Aktivitäten leicht beeinflussen können.

25.2.4 Weiterverwendung von PC der ehemaligen DDR

Jahrelang wurde den Fragen von Datenschutz und Datensicherheit in der DDR kaum Aufmerksamkeit geschenkt. Ausgehend von der herrschenden politischen Auffassung sah man nur wenig Anlaß, solche Themen in Theorie und Praxis aufzugreifen.

Erst im Frühjahr 1989 wurde mit dem Gesetzblatt der Deutschen Demokratischen Republik vom 22. März 1989 eine „Anordnung zur Gewährleistung der Datensicherheit" erlassen. Sie sollte die Grundlage für Maßnahmen zu Sicherheit, Ordnung und Geheimnisschutz bei der Informationsverarbeitung bilden. Etwa seit Mitte der achtziger Jahre war auch das Institut für Datensicherheit der Hochschule für Ökonomie Berlin zunehmend mit Lehrgängen zu den genannten Themen an die Öffentlichkeit getreten. Hier wurden jedoch in erster Linie Fragen der äußeren Sicherheit von Rechenzentren und dezentral organisierten EDV-Installationen behandelt; Sicherheitssoftware existierte kaum und war deshalb nur in geringem Umfang Gegenstand der Lehrgänge. Datenschutz im Sinne von Persönlichkeitsschutz wurde entsprechend der herrschenden Staats- und Gesellschaftsauffassung als nicht notwendig erachtet.

Für die unter diesen Umständen entwickelten DV-Anwendungen der ehemaligen DDR sind die Anforderungen der jetzt geltenden Datenschutzvorschriften nur schwer erfüllbar. Im Anwendungsbereich von Großrechnern werden jedoch ohnehin grundlegende Umstellungen erfolgen, teils weil der Einsatz der jetzt verfügbaren Geräte wirtschaftlicher ist und deshalb veraltete Systeme ersetzt werden, teils weil die Änderungen in der Verwaltungsstruktur radikale Änderungen der großen DV-Anwendungen erzwingen. Beides trifft auf PC-Anwendungen weit weniger zu, so daß noch für einige Jahre mit der Weiternutzung von PC aus DDR-Produktion zu rechnen ist.

Mit dem Beitritt der fünf Länder und Ost-Berlins zur Bundesrepublik Deutschland gelangte u. a. auch der Bestand an Groß-, Mittel- und Kleinrechentechnik der bisherigen Verwaltung in den Bereich von Behörden und Dienststellen des Bundes, der Länder und der Kommunen sowie der privaten Wirtschaft.

Über PC-Technik aus der Produktion der ehemaligen DDR habe ich mich im Rechenzentrum der Außenstelle des BMI in Ost-Berlin informiert. Dort sind einige der am häufigsten in den fünf neuen Ländern und Ost-Berlin eingesetzten PC-Typen vorhanden.

Als sogenannte Büro- bzw. Arbeitsplatzcomputer sind heute noch relativ häufig die Typen A 5120, A 5130 und A 1715 anzutreffen. Das sind typische 8-bit-Rechner mit in der Regel 64 kBytes RAM, einem oder mehreren Diskettenlaufwerken (8-Zoll oder 5¼-Zoll), ohne Festplatte, aber zum Teil mit Magnetbandlaufwerk und monochromem Bildschirm. Drucker und — teilweise — Plotter sind anschließbar.Die Rechner A 7100 und A 7150 stellen Zwischenschritte zur Entwicklung eines DDR-Rechners auf XT-Niveau dar. Allerdings wurden sie nur in relativ geringen Stückzahlen hergestellt und dürften daher keine große Verbreitung gefunden haben. Es sind 16-bit-Rechner, in der Regel mit 320 kBytes RAM, je nach Ausstattung

mit 30 bis 50-MBytes-Festplatte, Diskettenlaufwerken und mono- bzw. polychromem Bildschirm. Anschließbar sind Drucker und Plotter.

Der Rechner EC 1834 hat das Niveau der Geräteklasse PC/XT. Er sollte in der zweiten Hälfte der achtziger Jahre (ca. ab 1987) in zunehmendem Maße flächendeckend in die öffentliche Verwaltung eingeführt werden. Fehlende Produktionskapazitäten ließen jedoch nie die geplanten Stückzahlen erreichen; trotzdem dürfte er relativ verbreitet sein. Es handelt sich um einen 16-bit-Rechner mit 256 kBytes RAM (erweiterbar um 384 kBytes auf maximal 640 kBytes), Diskettenlaufwerken und einer Festplatte mit je nach Ausstattung 20 bis 80 MBytes. Angeschlossen werden können Bildschirm (mono- bzw. polychrom), Drucker, Plotter, andere PC EC 1834 oder PC A 5120 oder A 1715 oder Modems zur Datenfernübertragung.

Die auf diesen Rechnern eingesetzten Betriebssysteme SCP 1520 und DCP sind nach den Anwendungshinweisen kompatibel zum Betriebssystem CP/M der Firma Digital Research Corporation/USA bzw. MS-DOS, mindestens Version 3.30. Programmiersprachen sind im allgemeinen BASIC und TURBO-PASCAL.

Hauptanwendungsgebiete der genannten Rechner waren

- CAD-Anwendungen,
- Softwareentwicklung,
- betriebswirtschaftliche Aufgaben (z. B. Buchung, Planung, Fakturierung, Abrechnung),
- wissenschaftlich-technische Rechnungen,
- Textverarbeitung und
- Datenbankanwendungen.

Als Standardsoftware wurde für die Textverarbeitung das Paket TEXT in verschiedenen Ausbaustufen, welches aus den entsprechenden Versionen von WORDSTAR abgeleitet ist, genutzt. Bezüglich der Datenbankanwendungen handelt es sich um das relationale Datenbankbetriebssystem REDABAS als Derivat von dBaseII und folgende. Auf den untersuchten Rechnern waren auch Software-Pakete wie z. B. Norton-Utilities oder POWER und diverse Computerspiele in den Originalversionen vorhanden und lauffähig. Das alles zeigt, daß diese Rechner mit hoher Wahrscheinlichkeit auch unter den lizensierten Ausgaben der Original-Betriebssysteme mit der entsprechenden Standardsoftware einsatzfähig sein werden. Damit wäre auch der Einsatz geeigneter Sicherheitssoftware möglich.

Damit ich mich mit den Einzelheiten, die für die Kontrolle und Beratung beim Einsatz dieser PC wesentlich sind, näher vertraut machen kann, hat mir der Bundesminister des Innern einige dieser Geräte aus den Beständen des Ministeriums des Innern der ehemaligen DDR überlassen.

25.3 Behördeninterne Telekommunikationsanlagen

Bereits jetzt hat ein großer Teil der Behörden und sonstigen öffentlichen Stellen des Bundes seine konventionellen Telefonanlagen („Telefonnebenstellenanlagen") durch moderne, digitalisierte „Telekommunikationsanlagen" (TK-Anlagen) ersetzt. Dieser Generationenwechsel bringt eine Reihe überzeugender Vorteile: nicht nur die Qualität und die Zuverlässigkeit der Funktion erhöhen sich, sondern zusätzliche Leistungsmerkmale und Dienste werden nutzbar, so daß Telefonieren heute meistens nur eine von mehreren Funktionen der TK-Anlage ist, die auch für Bildschirmtext, Telefax, Teletex usw. genutzt werden kann.

Die Zentrale einer modernen TK-Anlage gleicht nicht nur äußerlich einer ADV-Anlage, sie enthält die gleichen Funktionselemente und bringt daher für die Belange der Benutzer — Anrufer und Angerufener — dieselben Gefährdungen mit sich. Dabei spielt es keine Rolle, ob die Anlage „lediglich" digitalisiert, bereits ISDN-fähig oder gar als ISDN-TK-Anlage geschaltet ist.

In meinem Zwölften Tätigkeitsbericht (S. 89ff.) hatte ich bereits auf die besonderen Probleme hingewiesen, die sich im Zusammenhang mit Wartung und Fernwartung von TK-Anlagen ergeben. Ich hatte dabei betont, daß es besonderer technischer und organisatorischer Vorkehrungen bedarf, um die in den TK-Anlagen gespeicherten personenbezogenen Daten — insbesondere über die Telefonverbindungen selbst — vor dem (auch unbeabsichtigten) Zugriff durch Behördenfremde zu schützen.

Auch zu der Frage, welche Daten wie lange in TK-Anlagen gespeichert werden dürfen und welche Auswertungen dieser Daten zulässig sind, habe ich in meinen Tätigkeitsberichten (zuletzt im 12. TB, S. 32) Stellung genommen.

Ob und mit welchem Aufwand die Sicherheits- und Verarbeitungsanforderungen erfüllbar sind, entscheidet sich im wesentlichen bei der Beschaffung der TK-Anlagen. Deshalb bedauere ich, daß eine wichtige Vorgabe für die Verarbeitung von Verbindungsdaten in TK-Anlagen von Bundesdienststellen, die „Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Bundesverwaltung (Dienstanschlußvorschriften — DAV —)" des Bundesministers der Finanzen, noch immer nicht in der überarbeiteten Form verkündet wurde (s. 7.2)

Generell ist darauf zu achten, daß die zur Erfüllung der (hoffentlich bald geltenden) DAV erforderlichen Leistungsmerkmale der TK-Anlage nicht nur im Prospekt stehen, sondern vom Lieferanten auch vertraglich zugesichert werden. Dies gilt besonders für die Möglichkeit, bestimmte Angaben in den Verbindungsdatensätzen zu unterdrücken (z. B. Zeitpunkt des Gespräches, letzte Ziffern der Zielrufnummern usw.), weil solche Leistungsmerkmale erforderlich sind, um die Anforderungen der DAV und unter Umständen noch weitergehender Dienstvereinbarungen zu erfüllen.

Gespeicherte Verbindungsdaten sind geeignet, für eine Verhaltens- oder Leistungskontrolle der Bediensteten verwendet zu werden. Daher ist bereits vor der Beschaffung einer TK-Anlage der Personalrat über die Einzelheiten der geplanten Verarbeitungen und Nutzungen zu informieren, damit er seine Rechte nach den Bundespersonalvertretungs- oder Betriebsverfassungsgesetz wahrnehmen kann.

Für ein Rundschreiben an die obersten Bundesbehörden habe ich Hinweise zu diesem Problembereich erstellt, die diesem Bericht als Anlage 12 beigefügt sind.

25.4 Sicherheit bei Telefax-Übertragungen

Unabhängig vom Einsatz moderner Telekommunikationsanlagen hat sich der Telefaxdienst ausgebreitet, weil die entsprechenden Endgeräte an alten wie an neuen Vermittlungsanlagen praktisch wie Telefone betrieben werden können. Die vergleichsweise niedrigen Installations- und Betriebskosten von Telefax-Endgeräten, die hohen Übertragungsgeschwindigkeiten und daraus resultierende niedrige Übertragungskosten sowie nicht zuletzt die relativ leicht zu erlernende Handhabung führten in den letzten Jahren zu hohen Zuwachsraten.

Aber gerade die Vorteile des Telefaxdienstes und besonders die Tatsache, daß beliebige Vorlagen schnell übertragen und beim Empfänger sofort originaltreu — und offen! — ausgedruckt werden, lassen bei Dokumenten mit personenbezogenem Inhalt Probleme entstehen. Diese können im wesentlichen aus drei Aspekten erwachsen:

- Das Anwählen des Partners ist fehleranfällig, deshalb ist nicht ohne weiteres gewährleistet, daß die Sendung am richtigen Gerät ankommt.
- Durch gebührensparendes zeitversetztes Senden, durch abweichende Arbeitszeiten beim Empfänger oder durch andere Verschiebungen kann eine Sendung zu einer Zeit beim Empfänger ankommen, zu der dort eine sofortige sichere Behandlung nicht möglich ist.
- Auch während der regelmäßigen Arbeitszeit entspricht die Behandlung ankommender Telefax-Sendungen beim Empfänger erfahrungsgemäß nicht unbedingt den Sicherheitsmaßstäben, die der Absender für seine Sendung für angemessen hält.

Deshalb sollte bei der Übermittlung personenbezogener Daten, insbesondere solcher, die sich auf gesundheitliche Verhältnisse, strafbare Handlungen, Ordnungswidrigkeiten, religiöse oder politische Anschauungen sowie auf arbeitsrechtliche Rechtsverhältnisse beziehen, Vorsorge getroffen werden, um die Rechte der Betroffenen zu wahren. Vorkehrungen zur Datensicherung müssen insbesondere das Risiko begrenzen, daß der Inhalt einer Telefax-Sendung Unbefugten zur Kenntnis gelangt.

In einem Rundschreiben an die obersten Bundesbehörden habe ich deshalb ausführliche Hinweise für die sichere Nutzung der Telefaxgeräte und der Telefaxanlagen gegeben und das Muster eines Merkblatts versandt (siehe Anlage 13).

26 Entwicklung des allgemeinen Datenschutzrechts

Das neue Bundesdatenschutzgesetz, das als Artikel 1 des Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes am 20. Dezember verkündet worden ist und am 1. Juni 1991 in Kraft treten wird, schließt die Diskussion über die Novellierung des allgemeinen Datenschutzrechts, an der sich im Berichtsjahr sowohl die Datenschutzkonferenz (siehe Entschließung Anlage 3) als auch ich mit einer schriftlichen Stellungnahme gegenüber dem Innenausschuß des Deutschen Bundestages noch einmal beteiligt haben, vorläufig ab. Über das langwierige Gesetzgebungsverfahren und über meine Stellungnahmen zu den Gesetzentwürfen habe ich in den vergangenen Jahren ausführlich berichtet.

Das neue Gesetz enthält für den öffentlichen Bereich eine Reihe von erfreulichen — auch konzeptionellen — Verbesserungen. Das Gesetz ist insgesamt übersichtlicher geworden. Für die öffentlichen wie für die nicht-öffentlichen Stellen werden die Rechtsgrundlagen der Datenverarbeitung, die Rechte der Betroffenen und die Datenschutzkontrolle jeweils in einem besonderen Unterabschnitt des Zweiten (öffentliche Stellen) und Dritten (nicht-öffentliche Stellen) Abschnitts zusammengefaßt. Der Vierte Abschnitt enthält erstmals Sonderbestimmungen zur Datenverarbeitung durch Forschungseinrichtungen und zum Datenschutz im Bereich der Medien.

Der Anwendungsbereich des Gesetzes ist für die Datenverarbeitung der öffentlichen Stellen erheblich ausgeweitet worden. Als Zweck des Gesetzes ist jetzt — klarstellend — eindeutig der Schutz des Persönlichkeitsrechts des einzelnen beim Umgang mit seinen personenbezogenen Daten bestimmt. Im öffentlichen Bereich ist künftig auch die Verarbeitung personenbezogener Daten in Akten vom Gesetz umfaßt. Auch Datenerhebung und Datennutzung werden geregelt. Grundsätzlich fällt jeder Umgang öffentlicher Stellen mit personenbezogenen Daten, angefangen von der Datenerhebung über die Datenverarbeitung — sei es automatisiert oder manuell dateigebunden, sei es in Akten — bis hin zur Nutzung der Daten in den Anwendungsbereich des Gesetzes.

Die *Begriffsbestimmungen* sind erweitert worden. Neben der Definition der bekannten Verarbeitungsphasen (Speichern, Verändern, Übermitteln, Löschen) ist jetzt auch eine Bestimmung der Begriffe „Erheben", „Sperren", „Nutzen" und „Anonymisieren" aufgenommen worden. Der jetzt vorwiegend nur noch für die Anwendbarkeit des Gesetzes im nicht-öffentlichen Bereich bedeutsame Begriff der *Datei* wurde weiterentwickelt. Entscheidendes Kriterium für den Dateibegriff bei automatisierten Verfahren ist nur noch die Auswertbarkeit des Datenbestandes. Damit wird Forderungen der Datenschutzbeauftragten entsprochen. Für nicht-automatisierte Verfahren bleibt es dabei, daß der Dateibegriff nur erfüllt ist, wenn der

Datenbestand nach bestimmten Merkmalen umgeordnet werden kann.

Gegenüber öffentlichen Stellen hat der Betroffene künftig einen vom *Verschulden unabhängigen Schadensersatzanspruch*; wenn durch eine unzulässige oder unrichtige automatisierte Datenverarbeitung ein Schaden verursacht wurde (Gefährdungshaftung). Bei schweren Verletzungen des Persönlichkeitsrechts hat der Betroffene sogar einen Anspruch auf Erstattung eines Nichtvermögensschadens (Schmerzensgeld). Nicht-öffentliche Stellen haben für Schäden, die sie durch eine unzulässige oder unrichtige automatisierte Datenverarbeitung verursachen, weiterhin Schadensersatz nach dem Verschuldensprinzip zu leisten; allerdings ist zugunsten des Betroffenen eine Beweislastumkehr vorgesehen, die zumindest verfahrensmäßig in ihrer Wirkung der Regelung für den öfentlichen Bereich nahekommen dürfte.

Erstmals ist in das BDSG eine Grundnorm darüber aufgenommen worden, unter welchen Voraussetzungen *automatisierte Abrufverfahren* eingerichtet werden dürfen. Die Zulässigkeit solcher Verfahren wird von deren Angemessenheit im Hinblick auf die schutzwürdigen Belange der Betroffenen und die von den beteiligten Stellen damit verfolgten Zwecke abhängig gemacht. Für die öffentlichen Stellen des Bundes besteht die Pflicht, den BfD über die Einrichtung eines solchen Verfahrens sowie über dessen Anlaß und Zweck, die Datenempfänger, die Art der zu übermittelnden Daten und die getroffenen Datensicherungsmaßnahmen zu unterrichten. Auf diese Weise wird eine hinreichende Mitprüfung bereits bei der Schaffung solcher Verfahren sichergestellt.

Erstmals regelt das BDSG auch die *Datenerhebung*. Damit wird ebenfalls langjährigen Forderungen der Datenschutzbeauftragten entsprochen. Es gilt der Grundsatz, daß personenbezogene Daten beim Betroffenen zu erheben sind, und zwar unter Hinweis auf den Erhebungszweck sowie die der Erhebung zugrundeliegende Rechtsvorschrift oder die Freiwilligkeit der Angaben. Sollen Daten ohne Mitwirkung des Betroffenen erhoben werden, ist das nur unter eingeschränkten Voraussetzungen zulässig. Eine ähnlich differenzierte Erhebungsregelung fehlt indessen für den nicht-öffentlichen Bereich, wo die Erhebung lediglich unter den ohnehin geltenden Grundsatz von Treu und Glauben gestellt wird.

Datenspeicherung, Veränderung und *Nutzung* werden in einen gemeinsamen Erlaubnistatbestand zusammengefaßt, in den der Grundsatz der *Zweckbindung* verstärkt Eingang gefunden hat. Speicherung, Veränderung und Nutzung personenbezogener Daten werden grundsätzlich an den Erhebungszweck oder — soweit keine Erhebung vorausgegangen ist — an den Speicherungszweck gebunden. Zweckänderungen sind nur eingeschränkt zulässig, wenn bestimmte Ausnahmetatbestände erfüllt sind. Die *Datenübermittlung* wird ebenfalls differenziert unter Betonung des Zweckbindungsgrundsatzes geregelt.

Das BDSG enthält erfreulicherweise für den öffentlichen Bereich auch eine Bestimmung über den *internationalen Datenverkehr*. Grenzüberschreitende Datenübermittlung ist unter den gleichen Voraussetzungen, die auch für Datenübermittlungen an nicht-öffentliche Stellen gelten, grundsätzlich zulässig. Der Empfänger im Ausland ist darauf hinzuweisen, daß die übermittelten Daten nur zu dem Zweck verarbeitet oder genutzt werden dürfen, zu dem sie ihm übermittelt worden sind.

Auch die *Rechte der Bürger* sind verbessert worden. Das Auskunftsrecht des Betroffenen — gegenüber den Nachrichtendiensten des Bundes ist es jetzt nicht mehr im BDSG, sondern in den betroffenen Fachgesetzen geregelt — erstreckt sich auch auf Herkunft und Empfänger der zu seiner Person gespeicherten Daten sowie den Speicherungszweck und gilt auch für Datenspeicherungen in Akten. Die bisher schon weitgehend übliche Unentgeltlichkeit der Auskunft wird jetzt im Gesetz verankert, jedoch ist im nicht-öffentlichen Bereich eine einschränkende Ausnahmeregelung zugunsten von Kreditinformationssystemen vorgesehen.

Berichtigung und Sperrung von Daten werden für den öffentlichen Bereich differenziert auch für Daten in Akten geregelt. Personenbezogene Daten in Dateien, die nicht mehr gebraucht werden, sind jetzt grundsätzlich zu löschen. Für bestimmte Tatbestände tritt an die Stelle der Löschung eine Sperrung. Ohne Einwilligung des Betroffenen ist die Nutzung gesperrter Daten nur in engen Ausnahmefällen zulässig. Auch regelmäßige Datenempfänger sind grundsätzlich von einer Berichtigung, Sperrung oder Löschung personenbezogener Daten zu unterrichten, wenn dies zur Wahrung schutzwürdiger Interessen des Betroffenen erforderlich ist.

Die *Rechtstellung des BfD* ist verstärkt worden. Er wird künftig mit mehr als der Hälfte der gesetzlichen Zahl der Mitglieder des Bundestages gewählt. Zum Schutz des Vertrauensverhältnisses mit dem Bürger besitzen er und seine Mitarbeiter künftig ein Zeugnisverweigerungsrecht über Personen und Tatsachen, die ihnen in der Eigenschaft als BfD anvertraut worden sind. Besonders erfreulich ist die Klarstellung, daß die Kontrolle durch den BfD umfassend ist. Auch Akten unterliegen seiner Kontrolle, wenn er — z. B. durch eine Petenteneingabe — Anhaltspunkte dafür hat, daß die Erhebung, Verarbeitung oder Nutzung von Daten das Persönlichkeitsrecht des Betroffenen verletzt. Die Kontrolle erstreckt sich ausdrücklich auch auf personenbezogene Daten, die einem besonderen Berufs- oder Amtsgeheimnis, dem Steuergeheimnis oder dem Post- und Fernmeldegeheimnis unterliegen. Eine Kontrolle des Inhalts des Post- und Fernmeldeverkehrs kommt allerdings nicht in Betracht. Von der Kontrolle ausgenommen sind personenbezogene Daten im Zusammenhang mit Verfahren nach dem Artikel 10 des Grundgesetzes sowie bestimmte Fälle, in denen der Betroffene einer Kontrolle durch den BfD diesem gegenüber widerspricht. Über dieses Widerspruchsrecht hat die speichernde Stelle den Betroffenen zu unterrichten. Das Kontrollrecht des BfD ist aber von der Unterichtung nicht abhängig. Deshalb kann die speichernde Stelle dem Bundesbeauftragten nicht entgegenhalten, sie habe den Betroffenen noch nicht unterrichtet.

Die Datenverarbeitung für *Zwecke der wissenschaftlichen Forschung* ist zum Teil an verschiedenen Stellen

des Gesetzes bei den jeweiligen Verarbeitungsvorschriften geregelt. Daneben enthält § 40 des Gesetzes eine zusammenfassende Bestimmung mit besonderen Verfahrensmodalitäten und einer absoluten Bindung der für die wissenschaftliche Forschung zur Verfügung gestellten Daten an diesen Zweck. Die Datenverarbeitung zu Forschungszwecken wird insgesamt erleichtert, ohne daß es zugleich zu einer nicht hinnehmbaren Schwächung des Persönlichkeitsschutzes kommt.

Das *Medienprivileg* bleibt erhalten. Die Position des Betroffenen gegenüber Medien wird allerdings verbessert. Gegendarstellungen sind zu den Akten zu nehmen und für diesselbe Zeit wie diese aufzubewahren. Außerdem werden dem Betroffenen ein eingeschränktes Auskunftsrecht und ein Berichtigungsanspruch gegeben.

Im *nicht-öffentlichen Bereich* hat eine entsprechende Weiterentwicklung des Datenschutzrechts nicht stattgefunden. Es bleibt hier für die Anwendung des Gesetzes bei der Bindung des Datenschutzes an die Datenverarbeitung in Dateien. Auch die Verarbeitungsgrundlagen sind nicht zugunsten der Betroffenen verbessert worden. Lediglich das Auskunftsrecht ist erweitert. Positiv ist anzumerken, daß die interne (betriebliche) und externe Datenschutzkontrolle verbessert worden sind. Dadurch werden allerdings die Mängel der materiellen Regelung nicht kompensiert. Es wird deshalb in Zukunft vermehrt bereichsspezifischer Gesetze auch für den nichtöffentlichen Bereich bedürfen, um in sensiblen Bereichen, wie z. B. bei Arbeitnehmern, in der Versicherungs- und Kreditwirtschaft sowie bei der Tätigkeit von Auskunfteien, einen angemessenen Datenschutz zu gewährleisten.

27 Nicht-öffentlicher Bereich

An dem ständigen Meinungs- und Erfahrungsaustausch der Datenschutzaufsichtsbehörden der Länder (Düsseldorfer Kreis) habe ich mich weiterhin beteiligt. Neben einer Vielzahl von Einzelproblemen standen im Berichtsjahr vor dem Hintergrund der Vollendung des europäischen Binnenmarktes vermehrt Fragen des grenzüberschreitenden Datenverkehrs im Vordergrund. Die Unternehmen der Privatwirtschaft, für die der Austausch personenbezogener Daten mit Stellen im Ausland erhebliche geschäftliche Bedeutung haben kann, sind besonders daran interessiert, Modelle zu entwickeln, die eine grenzüberschreitende Datenverarbeitung auch dann zulassen, wenn im Empfängerland kein gleichwertiger Datenschutz besteht. Ein sogenanntes Vertragsmodell, bei dem sich der Empfänger der übermittelnden Stelle gegenüber vertraglich verpflichtet, zum Schutz des Betroffenen einen bestimmten Datenschutzstandard einzuhalten, ist von den Aufsichtsbehörden als eine mögliche Lösung angesehen worden. Die Diskussion zeigt, daß es für die Unternehmen dringlich ist, möglichst bald einheitliche Rahmenbedingungen für den Datenschutz zumindest in der Europäischen Gemeinschaften vorzufinden.

Die Datenschutzpraxis in den Unternehmen stand im übrigen unter dem Eindruck der Diskussion über das neue Datenschutzgesetz und dessen Auswirkungen für den betrieblichen Datenschutz. Nach dem Eindruck, den ich insbesondere bei verschiedenen Verbänden und auf der jährlichen Datenschutzfachtagung der Gesellschaft für Datenschutz und Datensicherung (GDD) gewonnen habe, wird das neue Gesetz rasch in die betriebliche Praxis umgesetzt werden. Die Wirtschaft begrüßt natürlich, daß es für den nichtöffentlichen Bereich nicht zu einer Erstreckung des Datenschutzes auf die Datenverarbeitung in Akten gekommen ist und Verschärfungen der materiellen Datenschutzregelungen weitgehend ausgeblieben sind. Die im Gesetz vorgesehene Stärkung der betrieblichen Datenschutzbeauftragten stößt auf Zustimmung.

28 Internationales

Mit der Vorlage eines „Vorschlags für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" (SYN 287) durch die Kommission der Europäischen Gemeinschaften am 13. September 1990 hat die EG endlich auf dem Gebiet des Datenschutzes die Initiative ergriffen. Ich sehe darin nicht zuletzt einen Erfolg der internationalen Zusammenarbeit der Datenschutzbeauftragten, die im Jahr zuvor mit ihrer auf der 13. Internationalen Datenschutzkonferenz in Berlin gefaßten Entschließung nachdrücklich unterstrichen hatten, wie dringlich die Schaffung eines europäischen Datenschutzes ist (vgl. 12. TB 27.1 und 27.3 sowie Anlage 12). Aber auch das datenschutzrechtliche Vorangehen der Benelux-Länder, Frankreichs und der Bundesrepublik Deutschland im Rahmen des Schengener Übereinkommens (vgl. 12. TB 27.6) hat die Gemeinschaft zum Handeln veranlaßt und zugleich wichtige inhaltliche Vorgaben geliefert. Erfreulich ist aber nicht nur die Tatsache, daß die Europäische Gemeinschaft nach vielen Jahren des Zögerns nunmehr aktiv geworden ist, sondern auch die inhaltliche Linie, die der Kommissionsvorschlag verfolgt. Hervorzuheben ist zunächst, daß die Kommission sich nicht auf den erwähnten Richtlinienentwurf beschränkt hat, sondern in einem Paket zugleich weitere Maßnahmen vorgeschlagen hat, die das Ziel haben, eine datenschutzrechtliche Gesamtkonzeption für den Bereich der EG zu verwirklichen. Es handelt sich dabei zunächst um den „Entwurf einer Entschließung der im Rat vereinigten Vertreter der Regierung der Mitgliedstaaten der Europäischen Gemeinschaften", welche das Ziel verfolgt, die Grundsätze der Richtlinie auf die Dateien des öffentlichen Bereichs auszudehnen, für die diese wegen der begrenzten Kompetenzen der Gemeinschaft nicht gilt. Damit soll eine Selbstverpflichtung der Mitgliedstaaten herbeigeführt werden, die nationale Gesetzgebung mindestens dem durch die Richtlinie gesetzten europäischen Standard anzupassen, womit zugleich der Vorteil eines weitgehend homogenen Datenschutzes innerhalb der EG verbunden wäre. Ein weiterer Teil des Pakets ist die „Erklärung der Kommission betreffend die Anwendung der Grundsätze der Richtlinie zum Schutz von Personen bei der Verarbeitung personenbezogener Daten auf

die Organe und Einrichtungen der Europäischen Gemeinschaften". Darin ist vorgesehen, daß die Kommission die erforderlichen Maßnahmen trifft oder vorschlägt, um die Grundsätze auch für die eigenen Organe und Einrichtungen der Gemeinschaft verbindlich zu machen. Die Kommission hat sich mit der Vorlage des Pakets bereits verpflichtet, in der Zwischenzeit die Bestimmungen der Richtlinie auf ihre eigenen Dateien anzuwenden. Sie hat sich damit in eindrucksvoller Weise an die Spitze der Entwicklung gestellt. Die Datenschutzbeauftragten der Mitgliedstaaten werden die Kommission zweifellos in ihrem Bemühen unterstützen, die sich jetzt zeigende Vorreiterrolle überzeugend auszufüllen.

Weiterhin umfaßt das Paket noch Initiativen auf dem technischen Sektor. Der „Vorschlag für eine Richtlinie des Rates zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Kommunikationsnetzen, insbesondere im diensteintegrierenden digitalen Telekommunikationsnetz (ISDN) und in öffentlichen digitalen Mobilfunknetzen" (SYN 288) enthält eine bereichsspezifische Regelung des Datenschutzes für die Telekommunikation. Die Kommission bekennt sich damit zur Notwendigkeit bereichsspezifischer Datenschutzregelungen für einzelne zum Schutz des Persönlichkeitsrechts der Betroffenen besonders wichtige Sektoren. Zum Datenschutz in der Telekommunikation hat die Internationale Konferenz der Datenschutzbeauftragten Anforderungen definiert (Beschluß der Konferenz vom 19. September 1990, s. Anlage 11), die für die weitere Beratung des Richtlinien-Entwurfs große Bedeutung haben. Weiterhin hat die Kommission dem Rat die Annahme eines Zwei-Jahres-Aktionsprogramms im Bereich der Sicherheit der Informationssysteme vorgeschlagen. Damit sollen eine globale Strategie und konzertierte Aktionen in den Bereichen Technologie, Normen und Verfahren zur Genehmigung und Prüfung gefördert werden.

Schließlich wurde dem Rat ein Beschluß empfohlen, der auf den Beitritt der Europäischen Gemeinschaft zum Datenschutzübereinkommen des Europarats zielt. Dies ist folgerichtig, weil der Regelungsansatz der Kommission auf den Grundsätzen der Europaratskonvention aufbaut; ein Beitritt der EG zu diesen Übereinkommen wäre darüber hinaus ein Instrument, das die datenschutzrechtlichen Beziehungen der Gemeinschaft zu Drittländern, die die Europaratskonvention ratifiziert haben, in einheitlicher Weise regeln könnte.

Konzeptionell geht der EG-Entwurf in zwei Punkten über die Europarats-Konvention hinaus. Er umfaßt neben der automatisierten auch die manuelle Verarbeitung personenbezogener Daten (nach der Europarats-Konvention nur optional), und er verpflichtet die Mitgliedsstaaten zur Einrichtung von Datenschutzbehörden, deren Spitzen überdies gemeinsam ein europäisches Datenschutz-Organ bilden sollen. Der Richtlinien-Entwurf greift in vielfältiger Weise auf Datenschutzregelungen der Mitgliedsländer, insbesondere auf das britische, französische und deutsche Datenschutzgesetz, zurück.

Die Datenschutzbeauftragten der EG-Länder haben den Entwurf gemeinsam beraten und Gespräche mit dem Vizepräsidenten der Kommission Bangemann und mit Experten der Kommission aufgenommen. Dabei hat sich gezeigt, daß zwischen den europäischen Datenschutzbeauftragten Konsens in der grundsätzlich positiven Beurteilung des Entwurfs besteht, aber ebenso auch der Wunsch nach Verbesserungen. Die Datenschutzbeauftragten der EG-Länder haben im übrigen vereinbart, zur Behandlung der EG-spezifischen Fragen künftig einen regelmäßigen Meinungs- und Erfahrungsaustausch zu pflegen.

Gemeinsam mit den Landesbeauftragten für den Datenschutz habe ich im Januar 1991 eine Stellungnahme zu dem Richtlinienentwurf abgegeben (s. Anlage 9). Verbesserungen sind vor allem in folgenden Punkten notwendig, um nicht unter dem in den Mitgliedsstaaten schon erreichten Niveau zu bleiben:

- Anwendung auf alle Unterlagen mit personenbezogenen Daten
- Verstärkung des Zweckbindungsgrundsatzes,
- Datenerhebung vorrangig beim Betroffenen selbst,
- besserer Schutz beim Datenexport in Drittländer,
- Stärkung der vorgesehenen europäischen Datenschutzinstanz und
- Einrichtung einer Datenschutzinstanz für die Einrichtungen der Gemeinschaft.

Die Datenschutzrichtlinie der EG eröffnet eine qualitativ neue Phase für den Datenschutz in Europa. Mir kommt es deshalb besonders darauf an, die Weichen so zu stellen, daß der Datenschutz auch künftig entsprechend den technologischen, ökonomischen und sozialen Änderungen fortentwickelt werden kann. Die Organisation des Datenschutzes auf der europäischen Ebene hat daher für mich hohe Priorität. Für die künftige Entwicklung ebenso wichtig ist es aber, daß die Mitgliedsstaaten auch den für nationale Initiativen erforderlichen Spielraum behalten. Zumal im bereichsspezifischen Datenschutz gibt es in den einzelnen Ländern unterschiedliche Schwerpunkte in der Anwendung der Informationstechnologie wie auch in der rechtlichen und sozialen Wertung. Deshalb muß in der Richtlinie klargestellt werden, daß sie nur einen datenschutzrechtlichen Mindeststandard vorschreibt und nationalen Regelungen, die einen noch besseren Datenschutz gewährleisten, nicht im Wege steht.

Ich hoffe, daß die Richtlinie noch im zeitlichen Zusammenhang mit der Vollendung des Binnenmarktes zu Beginn des Jahres 1993 in Kraft gesetzt werden kann.

Das bereits erwähnte Zusatzübereinkommen zum Schengener Übereinkommen (zum Inhalt und den datenschutzrechtlichen Problemen vgl. 12. TB Abschnitt 27.6 sowie Anlage 6) ist Mitte des Jahres 1990

von den Regierungen der Vertragsstaaten unterzeichnet worden und steht jetzt zur Ratifizierung an. Die vor einem Jahr noch bestehenden Lücken des Datenschutzes beim manuellen Umgang mit personenbezogenen Daten, auf die ich hingewiesen hatte (12. TB a.a.O.), wurden noch beseitigt. Auch wenn dies nicht in vollem Umfang im Sinne meiner Vorstellungen geschehen ist, bin ich doch mit dem von der Bundesregierung in den Verhandlungen mit den Partnerstaaten erreichten Ergebnis zufrieden. Das im Zusatzübereinkommen vorgesehene internationale Datenschutzgremium wird zu kontrollieren und zu beurteilen haben, ob die getroffenen Regelungen und deren praktische Anwendung durch die Vertragsstaaten auf Dauer den datenschutzrechtlichen Anforderungen genügen.

Die im Jahre 1989 von der Menschenrechtskommission der Vereinten Nationen beschlossenen „Richtlinien betreffend personenbezogene Daten in automatisierten Dateien" wurden mit geringfügigen Änderungen im Berichtsjahr von der Generalversammlung verabschiedet (vgl. 12. TB Abschnitt 27.4, mit Text in der Anlage 14). Es ist zu wünschen, daß von diesen Richtlinien der Vereinten Nationen neue Anstöße zur weltweiten Verbreitung des Datenschutzes ausgehen.

Der Zeitpunkt, in dem der Europarat die Datenschutzkonvention zur Zeichnung ausgelegt hat, jährt sich 1991 zum zehnten Male. Aus diesem Anlaß hat die Internationale Konferenz der Datenschutzbeauftragten gern die Einladung der Generalsekretärin des Europarats angenommen, die Jahreskonferenz 1991 am Sitz des Europarats in Straßburg abzuhalten. Die Bedeutung des Datenschutzes für die Menschenrechte wird eines der tragenden Themen dieser Konferenz sein.

29 Aus zurückliegenden Tätigkeitsberichten — Bilanz —

1. Zur Verbesserung des *Melderechtsrahmengesetzes* habe ich in den vergangenen Jahren verschiedene Anregungen gegeben (8. TB S. 10, 12. TB S. 20f.). Der Bundesminister des Innern hatte bisher nur wenige meiner Anregungen übernommen. Im Lauf des Berichtsjahres habe ich aber erreicht, daß in dem Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes eine Präzisierung der Hotel- und Krankenhausmeldepflicht vorgesehen wurde, die meinen und auch den Bedenken der Konferenz der Datenschutzbeauftragten (s. Anlage 6) zumindest entgegen kam. Danach darf die Polizei diese Angaben nur noch unter bestimmen Bedingungen bezogen auf den Einzelfall nutzen. Ferner sollte für alle Bürger ein Widerspruchsrecht gegen die Übermittlung ihrer Daten an politische Parteien im Zusammenhang mit Wahlen eingeräumt werden. Nach dem jetzt noch gültigen Melderechtsrahmengesetz können alle Parteien im Zusammenhang mit Wahlen zum Deutschen Bundestag oder zum Europäischen Parlament Auskunft aus dem Melderegister über Vor- und Familiennamen, akademischen Grad und Anschriften von Wahlberechtigten erhalten. Leider konnte der Gesetzentwurf in der vergangenen Legislaturperiode nicht mehr abschließend behandelt werden. Ich hoffe, daß er unter Berücksichtigung aller Anregungen aus den Reihen des Datenschutzes in der laufenden Legislaturperiode wieder eingebracht wird.

2. Gegenüber dem Entwurf des BMJ für ein *Justizmitteilungsgesetz* habe ich insbesondere die generalklauselartigen Bestimmungen kritisiert, die Anlaß und Umfang der vorgesehenen Datenverarbeitung nicht hinreichend deutlich erkennen ließen (10. TB S. 23). In meiner Stellungnahme zu dem inzwischen überarbeiteten Entwurf des BMJ für ein Justizmitteilungsgesetz habe ich zwar Verbesserungen anerkannt, aber erneut die immer noch nicht ausreichende Normenklarheit bemängelt.

3. Zu den Entwürfen eines Gesetzes zur Änderung von Vorschriften über das *Schuldnerverzeichnis* sowie einer Verordnung über die Erteilung von Abdrucken und Listen aus dem Schuldnerverzeichnis habe ich als wesentliches Problem die Weitergabe von Schuldnerlisten durch die Empfänger von Abdrucken aus dem Schuldnerverzeichnis, d. h. durch die Kammern (z. B. Industrie- und Handelskammern, Handwerkskammern), an ihre Mitglieder herausgestellt (10. TB S. 24f.). Im Berichtsjahr 1990 hat der Bundesrat bei der Beratung des von der Bundesregierung eingebrachten Entwurfs eines Gesetzes zur Änderung von Vorschriften über das Schuldnerverzeichnis gefordert klarzustellen, ob die „Errichtung und Führung *zentraler* bundesweiter Schuldnerverzeichnisse durch Private" zulässig sein sollen. Dies bestätigt eine bereits früher von mir geäußerte Forderung. Die Bundesregierung hat den in der vergangenen Legislaturperiode nicht mehr verabschiedeten Entwurf inzwischen in unveränderter Form neu eingebracht.

4. Gegen die vom BMJ inzwischen ausdrücklich gebilligte Auslegung des § 829 ZPO und die darauf beruhende Praxis, in Pfändungs- und Überweisungsbeschlüsse auch mehrere *Drittschuldner* aufzunehmen, habe ich eingehend meine Bedenken dargelegt, die sich auf den Wortlaut der Vorschrift und darauf stützen, daß mit dem derzeit geübten Verfahren die Drittschuldner jeweils Kenntnis von den anderen Drittschuldnern erhalten (12. TB S. 25f.). Auch nach meinem Hinweis auf die gegenteilige Praxis der Finanzbehörden zu dem entsprechenden § 309 AO hält der BMJ an seiner Auffassung fest. Ich werde mich weiterhin nachdrücklich dafür einsetzen, daß die datenschutzrechtlich bedenkliche Praxis beseitigt wird.

5. Über datenschutzrechtliche Bedenken gegen die im Entwurf eines *Rechtspflege-Vereinfachungsgesetzes* vorgesehene unzureichende Regelung der Ermittlungsbefugnisse des Gerichtsvollziehers anläßlich der Zwangsvollstreckung habe ich berichtet (12. TB S. 26). Der im — inzwischen verabschiedeten — Rechtspflege-Vereinfachungsgesetz enthaltene § 806a ZPO (neu) trägt meinem

Anliegen insofern Rechnung, als er normenklar die Befragung der zum Hausstand des Schuldners gehörenden erwachsenen Personen durch den Gerichtsvollzieher regelt.

6. Die Zusammenfassung mehrerer Entscheidungen in *Ehescheidungsverbundurteilen* (Scheidung/Umgang mit dem ehelichen Kind/Zugewinnausgleich u. a.) erzeugt datenschutzrechtliche Probleme, wenn solche Urteile Behörden vorgelegt oder dem Gerichtsvollzieher für Zwecke der Zwangsvollstreckung übergeben werden, weil diese Stellen nicht den gesamten Inhalt eines solchen Verbundurteils kennen müssen (12. TB S. 27). Der BMJ sieht keinen Bedarf für Änderungen der Zivilprozeßordnung. Die von ihm vorgetragenen Gründe überzeugen nicht.

7. Auf die im Entwurf einer *Steuerdaten-Abruf-Verordnung* noch offene Frage der Eingrenzung der Möglichkeit, besonders ermächtigten Amtsträgern der Oberfinanzdirektionen die Berechtigung zum Abruf von Daten der Finanzämter im automatisierten Verfahren zu erteilen, habe ich hingewiesen (12. TB S. 29f., 30). Nachdem inzwischen mit drei entsprechenden Fallgruppen (z. B. Bearbeitung von Beschwerden und Billigkeitsmaßnahmen) ein datenschutzrechtlich vertretbarer Rahmen erarbeitet werden konnte, innerhalb dessen solche Abrufberechtigungen erteilt werden dürfen, hoffe ich, daß die für den Datenschutz beim Abruf von Steuerdaten wichtige Rechtsverordnung in absehbarer Zeit in Kraft treten wird.

8. Für die *Mitteilungspflichten von Behörden an Finanzbehörden*, z. B. über Zahlungen, gibt es bisher keine Rechtsgrundlage (11. TB S. 22f., 23). Wie der BMF mir mitteilte, konnte die vorbereitete Rechtsverordnung nach § 93a AO wegen starker Belastung durch Aufgaben im Zusammenhang mit der Wiedervereinigung bisher nicht weiterverfolgt werden. Vor dem Hintergrund, daß — wie der BMF weiterhin mitteilte — nach der gemeinsamen Auffassung der Vertreter der obersten Finanzbehörden des Bundes und der Länder keine Rechtsgrundlage für eine Fortführung der Kontrollmitteilungsverfahren besteht, habe ich gefordert, daß der BMF entsprechend dem Beispiel einiger Länder unverzüglich die Verwaltungsanweisung, mit der die Kontrollmitteilungen angeordnet werden, aufhebt.

9. Ich habe Bedenken dagegen erhoben, daß Gerichte, Notare und Behörden im Rahmen ihrer *Anzeigepflicht nach dem Erbschaftsteuergesetz und dem Grunderwerbsteuergesetz* den Finanzbehörden vollständige beglaubigte Abschriften von Urkunden, wie zum Beispiel von Verfügungen von Todes wegen oder von Grundstückskaufverträgen, zu übersenden haben. Auf diese Weise werden den Finanzbehörden zum Teil personenbezogene Daten übermittelt, die sie zur Aufgabenerfüllung nicht benötigen (12. TB S. 30). Der BMF und der ebenfalls von mir eingeschaltete Präsident der Bundesnotarkammer sind der Ansicht, auf die Übersendung der vollständigen Abschriften könne nicht verzichtet werden. Ich bleibe bemüht, dennoch eine datenschutzrechtlich angemessenere Lösung zu erreichen.

10. § 2 Abs. 1 des *Wohnungsbindungsgesetzes* regelt nicht klar, welche personenbezogenen Daten bei der Erfassung öffentlich geförderter Wohnungen erhoben und verarbeitet werden dürfen (10. TB S. 20). Meine Anregungen hierzu sind in dem am 30. Mai 1990 in Kraft getretenen Wohnungsbindungsänderungsgesetz leider nicht berücksichtigt worden, obwohl der Bundesminister für Raumordnung, Bauwesen und Städtebau hierzu früher seine grundsätzliche Bereitschaft erklärt hatte.

11. Über die Frage, ob *Personalvertretungen* sich an den Bundesbeauftragten für den Datenschutz wenden können (und umgekehrt), habe ich bereits mehrfach berichtet (u. a. 12. TB, S. 32). Das Bundesverwaltungsgericht hat in seinem Beschluß vom 8. November 1989 — 6 P 7.87 — festgestellt, daß der Personalrat, wenn es um die Gewinnung erforderlicher Informationen geht, nicht ausschließlich auf die Unterrichtung durch die Dienststelle verwiesen ist. Damit wird meine Auffassung bestätigt, daß der Personalrat sich auch an den Bundesbeauftragten für den Datenschutz wenden kann.

    In der vorgenannten Entscheidung hat das Bundesverwaltungsgericht auch meine Auffassung (vgl. 10. TB S. 31) bestätigt, daß bei der Einführung von automatisierten Verfahren, die zu einer Leistungs- und Verhaltenskontrolle führen können, ein Informationsanspruch der Personalvertretung über das technische System einschließlich des Betriebsprogramms und etwaiger Anwendungsprogramme sowie über die Verknüpfungsmöglichkeiten mit anderen Systemen besteht. Dies verlange in der Regel die Übergabe entsprechender Hard- und Software-Beschreibungen, die lückenlos sein müßten. Die Dienststelle habe den Personalrat über alle gespeicherten Datenfelder mit Personaldaten zu informieren und Arbeitsweise sowie Verwendungszusammenhänge der Programme einschließlich der Möglichkeit der Verknüpfung der Datenfelder offenzulegen. Soweit bei neuartigen, komplizierten und langwierig entwickelten Systemen von den Beteiligten Datenschutzinstitutionen eingeschaltet worden seien, sei die Personalvertretung auch über das dabei erzielte Ergebnis der Überprüfung zu unterrichten.

12. Über die *Telefondatenverarbeitung bei der Deutschen Genossenschaftsbank* (DG-Bank) (12. TB S. 32) habe ich Gespräche geführt. Danach ist folgende konstruktive Lösung erkennbar:

    Sämtliche Daten aus der Telefondatenerfassung werden nunmehr nur noch zwei Monate gespeichert und Buchungsunterlagen entsprechend den gesetzlichen Bestimmungen aufbewahrt.

    Das derzeit in der Frankfurter Zentrale der DG-Bank praktizierte Telefondatenerfassungsverfahren wird nur noch für einen Übergangszeitraum bis zum Umzug in ein neues Dienstgebäude im Jahre 1992 beibehalten. In der Übergangszeit ha-

ben die Mitarbeiter die Möglichkeit, die Aufzeichnung der Telefondaten ihrer Privatgespräche durch Benutzung der öffentlichen Fernsprecher im Dienstgebäude zu verhindern.

Die DG-Bank hat mir zugesagt, daß die Telefondatenverarbeitung im neuen Dienstgebäude — sofern nicht schon zu einem früheren Zeitpunkt auf eine neue Anlage umgeschaltet wird — allen meinen Forderungen sowie den Anforderungen der neuen Dienstanschlußvorschriften (vgl. hierzu 7.2) entsprechen wird.

13. Über meine Beteiligung an der Konzeption des Systems „Dezentrale Leistungs- und Kostenrechnung bei der Deutschen Bundespost *(DELKOS)*" habe ich berichtet (12. TB S.32f.). Zwischenzeitlich haben die Unternehmen DBP TELEKOM, DBP POSTDIENST, DBP POSTBANK inhaltsgleiche Dienstvereinbarungen mit dem jeweiligen Hauptpersonalrat abgeschlossen. In diese sind meine Empfehlungen umfassend eingeflossen. Am 1. September 1990 hat der Probebetrieb von DELKOS begonnen.

14. Auf die Notwendigkeit eines eigenen Antragsrechts für berücksichtigungsfähige Familienangehörige im *Beihilfeverfahren* habe ich hingewiesen (12. TB S. 33ff.). In seinem Beitrag zur Stellungnahme der Bundesregierung zu meinem 12. Tätigkeitsbericht hat der Bundesminister des Innern zum Ausdruck gebracht, daß ein weitergehendes Zugeständnis im Hinblick auf die von mir als Schritt in die richtige Richtung gewürdigte Verfahrensregelung nicht in Aussicht gestellt werden könne. Ich bedauere dies und werde mich in Zusammenarbeit mit den Landesbeauftragten für den Datenschutz weiterhin für eine datenschutzgerechte Lösung einsetzen.

15. Im Zusammenhang mit dem Beurteilungsbogen der BfA (s. 12. TB, S. 34) hat die Personalvertretung der BfA inzwischen einen Entwurf zur Änderung der *Beurteilungsrichtlinien* erarbeitet, der in Übereinstimmung mit meinem Vorschlag auf die Bewertung der äußeren Erscheinung des Bediensteten verzichtet. Die BfA selbst hat mir mitgeteilt, meiner Anregung, auf das Merkmal „Äußere Erscheinung" schon vorab zu verzichten, könne auch nach erneuter Prüfung nicht entsprochen werden. Sie begründet dies mit der Möglichkeit, daß die Mitarbeiter Kontakte nach außen haben könnten. Insoweit sei das Ansehen der BfA in der Öffentlichkeit zu berücksichtigen. Ich halte dies nach wie vor nicht für überzeugend.

16. Im Berichtszeitraum teilte die Physikalisch-Technische Bundesanstalt (PTB) Braunschweig mit, die Erklärung eines Verzichts auf freie Abfragemöglichkeiten bei ihrer *automatisierten Personaldatenverarbeitung* (12. TB S. 35) beruhe auf einem Mißverständnis. Um eine effiziente Sachbearbeitung gewährleisten zu können, seien vielmehr eingeschränkte freie Abfragemöglichkeiten notwendig. Ich bin nach wie vor nicht von der Notwendigkeit solcher, wenn auch eingeschränkten, freien Abfragemöglichkeiten überzeugt und habe demgemäß erneut gefordert, darauf zu verzichten.

17. Auf die Absicht des Bundesministers für Post und Telekommunikation, *Wartezonen* vor Postschaltern einzurichten, habe ich hingewiesen (11. TB S. 36). Zwischenzeitlich ist in einem Betriebsversuch der Einsatz einer Acrylglassäule als Trennelement gestestet worden. Die begleitende Kundenbefragung hat dabei ergeben, daß dieser zusätzliche Hinweis auf die Diskretionszone von den Kunden positiv aufgenommen wird. Die Post hat mir angekündigt, sie werde aufgrund dieses Ergebnisses die Hinweissäule in allen dazu in Frage kommenden Postämtern einsetzen.

18. Die nicht erforderliche *Speicherung der Verbindungsdaten* aller von ISDN-Anschlüssen aus gewählten Telefongespräche für über drei Monate habe ich beanstandet (12. TB S. 39ff.). Der rechtswidrige Zustand bestand im Berichtsjahr fort. Die Speicherung von Verbindungsdaten durch die Deutsche Bundespost — TELEKOM soll jetzt in der gemäß § 30 Abs. 2 des Postverfassungsgesetzes zu erlassenden Rechtsverordnung geregelt werden (siehe 8.1.3).

19. Ich habe bedauert, daß es nicht möglich war, in die Planungen des paneuropäischen Mobilfunknetzes *(D-Netz)* rechtzeitig Vorstellungen des Datenschutzes einzubringen (12. TB S. 42). Die mir inzwischen bekanntgewordenen Vereinbarungen, die ohne Rücksicht auf die Rechtslage getroffen wurden, übertreffen meine Befürchtungen (siehe dazu Nr. 8.7 in diesem Bericht).

20. In Zusammenhang mit einer Datenschutzkontrolle des *Sprachboxdienstes* hatte ich der Deutschen Bundespost TELEKOM eine Reihe von Empfehlungen und Anregungen zur Verbesserung der Datensicherung gegeben (12. TB S. 43f.). Ich habe es begrüßt, daß für den Betriebsversuch die meisten Punkte aufgegriffen und umgesetzt wurden. In welchem Maße auch das nachfolgende System des Wirkbetriebes den Erfordernissen des Datenschutzes entspricht, werde ich zu gegebener Zeit überprüfen.

21. Auf die Risiken, die mit dem Einsatz des neuen Fernwirkdienstes *TEMEX* zur Erfassung von Verbrauchsdaten für Elektrizität, Wasser, Gas und Wärme verbunden sind, habe ich hingewiesen (12. TB S. 44f.). Wie erwartet, hat der Bundesminister für Wirtschaft Entwürfe für Datenschutzvorschriften in den Allgemeinen Versorgungsbedingungen für Tarifkunden vorgelegt, die sowohl den Forderungen des Datenschutzes als auch den Interessen der Versorgungsunternehmen an modernen, auch den Umweltschutz berücksichtigenden Tarifen gerecht werden.

22. Auf Defizite bei der Organisation des Datenschutzes durch die *Bundesanstalt für Straßenwesen* habe ich hingewiesen (11. TB S. 38f.). Die Bundesanstalt hat mir inzwischen den Entwurf einer Datenschutz-Dienstanweisung zugeleitet, mit dem die festgestellten Mängel beseitigt werden sollen. Die endgültige Fassung des Entwurfs, der

noch geändert und ergänzt werden muß, stimme ich derzeit mit dem Amt ab.

23. Die automatisierte *Verkehrszentralregister-Auskunft* zur Beurteilung der Kraftfahrverwendungsfähigkeit der Wehrpflichtigen und zur statistischen Auswertung von Unfallmeldungen bei der Bundeswehr (10. TB S. 48) wird zukünftig so durchgeführt, daß die Verkehrszentralregister-Auskünfte in der Zentralen Militärkraftfahrtstelle selbst ausgewertet werden und den Einheitsführern grundsätzlich nur das Ergebnis mitgeteilt wird. Der Bundesminister für Verteidigung hat mir dargelegt, daß die in der Unfallstatistik gespeicherten Daten keinen Personenbezug mehr aufweisen.

24. Über die Notwendigkeit normenklarer gesetzlicher Regelungen für die Datenverarbeitung des *Verkehrszentralregisters* sowie einer Entscheidung zur Kooperation zwischen Bundeszentralregister und Verkehrszentralregister habe ich mehrfach berichtet (zuletzt 12. TB S. 50f.). Nach Mitteilung des Bundesministers für Verkehr konnten die Arbeiten an der Novellierung der in Betracht kommenden Vorschriften 1990 wegen der dringenden Arbeiten am Einigungsvertrag und dessen Umsetzung nicht fortgeführt werden.

25. Das Kraftfahrt-Bundesamt versucht insbesondere durch Einrichtung einer Fehlerdatenbank und vorrangige Bearbeitung fehlerhafter Meldungen der Zulassungsstellen, die Aktualität und *Qualität des Zentralen Fahrzeugregisters* wesentlich zu verbessern (vgl. hierzu 11. TB S. 38).

26. Über die notwendige Verbesserung der bisher unzureichenden gesetzlichen Regelungen für die Erhebung und Verarbeitung von *Fahrerlaubnisdaten* habe ich berichtet (12. TB S. 51). Der bereits im Jahre 1988 angekündigte Gesetzentwurf soll nach Mitteilung des Bundesministers für Verkehr in dieser Legislaturperiode erarbeitet werden.

27. Für die Veröffentlichung von personenbezogenen Daten der Eigentümer von *Luftfahrzeugen*, die im Rahmen der Verkehrszulassung erhoben und in der Luftfahrzeugrolle eingetragen sind, habe ich eine ausreichende gesetzliche Grundlage gefordert (vgl. 12. TB S. 51f.). Mit dem Bundesminister für Verkehr habe ich mittlerweile den Entwurf eines Gesetzes zur Änderung des Luftfahrt-Bundesamt-Gesetzes und der Luftverkehrs-Zulassungsordnung abgestimmt; er entspricht meinen Erwartungen. Ich hoffe, daß der Entwurf in Kürze verabschiedet wird.

28. Durch Artikel 37 des Rechtsbereinigungsgesetzes vom 28. Juni 1990 ist § 27 Abs. 2 des *Luftverkehrsgesetzes* — Erlaubniserteilung zur Herstellung und zum Vertrieb von Luftbildern — aufgehoben worden. Mit Fortfall dieser Rechtsvorschrift ist ein Ansatzpunkt für meine Bemühungen (12. TB S. 52), auch in diesem Bereich den Schutz des Persönlichkeitsrechts Betroffener zu verbessern, weggefallen. Dies kann nichts an der Forderung ändern, daß auch bei der Herstellung, Aufbereitung und Übermittlung von stehenden und beweglichen Bildern die Privatsphäre der Bürger beachtet werden muß. Das neue Bundesdatenschutzgesetz, das die Anknüpfung an Dateien in weiten Bereichen aufgegeben hat, kann hierfür eine gewisse Hilfestellung geben.

29. Das Gesetz über die *Statistik im Handwerk*, über das ich in meinem 11. Tätigkeitsbericht (S. 42) berichtet hatte, ist in der abgelaufenen Legislaturperiode nicht verabschiedet worden.

30. Das Gesetz über die *Statistik der Straßenverkehrsunfälle* ist im Berichtszeitraum vom Deutschen Bundestag verabschiedet worden und zum 1. Januar 1991 in Kraft getreten. Meine datenschutzrechtlichen Bedenken gegen Vorschläge des Bundesrates, Einzelangaben an bestimmte Landesbehörden weiterzugeben, über die ich an anderer Stelle berichtet habe (11. TB S. 43f., 12. TB S. 98), wurden berücksichtigt.

31. Über meine Bedenken gegen die Aufnahme der Matrikel-Nummer als Hilfsmerkmal im *Hochschulstatistikgesetz* habe ich berichtet (12. TB S. 56). Ich habe bei dem mittlerweile verabschiedeten Gesetz erreicht, daß die Matrikel-Nummer nach Abschluß der Plausibilitätsprüfung zu löschen ist.

32. Die Möglichkeit einer *Zusammenführung* der aufgrund *von* einzelnen Wirtschafts- und Umweltstatistikgesetzen gewonnenen *statistischen Erhebungen* ist inzwischen durch Ergänzung des § 13 und Einfügung eines neuen § 13 a in das Bundesstatistikgesetz in datenschutzrechtlich befriedigender Weise (vgl. im einzelnen 12. TB S. 53f.) neu geregelt worden.

33. Der Bundesminister für Raumordnung, Bauwesen und Städtebau hat den Entwurf eines Gesetzes über die Durchführung einer Repräsentativstatistik auf dem Gebiet des Wohnungswesens *(Gebäude- und Wohnungsstichprobengesetz)*, gegen den ich einzelne Bedenken geäußert hatte (12. TB S. 55f.), nicht weiter verfolgt. Eine entsprechende Erhebung wurde auch nicht wieder in das Mikrozensusgesetz eingefügt (siehe dazu Nr. 10a). Der BMBau beabsichtigt jedoch, den Gesetzentwurf in der neuen Legislaturperiode wieder einzubringen.

34. Die in § 291 SGB V (Gesundheitsreformgesetz) enthaltene Regelung über die Einführung und Gestaltung der *Krankenversichertenkarte* habe ich beschrieben (11. TB S. 55f.). In Zusammenarbeit mit den Spitzenverbänden der Krankenkassen habe ich zwischenzeitlich darauf hingewirkt, daß bei der Einführung der Krankenversichertenkarte keine Daten erhoben, gespeichert oder übermittelt werden, die für den Betroffenen nicht erkennbar sind. So darf die maschinenlesbare Zone (Magnetstreifenfeld) der Krankenversichertenkarte nur personenbezogene Daten enthalten, die auch auf der Kartenvorderseite in Klarschrift vorgesehen sind. Dem Karteninhaber wird das Recht eingeräumt, sich auf Wunsch den Inhalt des Magnetstreifens aufzeigen zu lassen. Die Versendung der Karten hat grundsätzlich getrennt an jeden Versicherten zu erfolgen. Bei Familienangehörigen in häuslicher Gemeinschaft dürfen die

Karten gemeinsam versandt werden, wenn der Versicherte keinen entgegenstehenden Wunsch geäußert hat und ein solcher auch aus anderen Umständen nicht erkennbar ist. Die Krankenversichertenkarte löst ab 1. Januar 1992 den Krankenschein ab.

35. Bei der Vorbereitung der Verordnung zur Bestimmung des Musters und des Inhalts des *Sozialversicherungsausweises*, (12. TB S. 59), seiner Ausstattung mit einem Lichtbild und der Form der Eintragungen (Sozialversicherungsausweis-Verordnung) habe ich u. a. erreicht, daß

    — auf die ursprünglich vorgesehene Aufnahme der Unterschrift des Ausweisinhabers verzichtet wurde,

    — ein Merkblatt erarbeitet wurde, das diejenigen Arbeitnehmer, die aufgrund ihrer Branchenzugehörigkeit einen Ausweis mit einem Lichtbild bei sich zu führen haben, über die besondere Rechtslage informiert,

    — die Vordrucknummer, die der Sozialversicherungsausweis als fortlaufendes Merkmal aus drucktechnischen Gründen erhält, keine Angaben über den Beschäftigten enhalten darf.

36. Auf die Notwendigkeit einer besonders geschützten Aufbewahrung und Behandlung von Arztgutachten und Befundberichten habe ich die *See-Berufsgenossenschaft — Seekasse* hingewiesen (12. TB S. 59f.). Die See-Berufsgenossenschaft-Seekasse hat meine Anregung aufgegriffen und für den Renten- und Rehabilitationsbereich der Seekasse eine verschließbare Gutachten-Teilakte zur Aufbewahrung solcher Unterlagen eingeführt. Die Öffnung dieser Akte durch den jeweils befugten Bearbeiter ist zu dokumentieren. Das Verfahren hierzu wurde in einer besonderen Dienstanweisung geregelt.

37. Das Direktorium der Deutschen Bundespost, Dienststelle Sozialangelegenheiten, hat das *Sozialamt der Deutschen Bundespost (SAP)* zwischenzeitlich angewiesen, in seinem neu bezogenen Dienstgebäude jeweils eine eigene Posteingangsstelle, einen eigenen Botendienst sowie eine eigene Postabgangsstelle für jede dem SAP unterstehende Selbstverwaltungseinrichtung zu schaffen (vgl. 12. TB S. 60). Außerdem soll ermöglicht werden, daß der Schriftverkehr einzelner Selbstverwaltungseinrichtungen, soweit er einem besonderen Vertrauensschutz unterliegt, dienststellenintern gefertigt werden kann. Ich habe diese datenschutzfreundlichen Regelungen begrüßt.

38. Die Bundesknappschaft hat Anregungen zur Aufgabenwahrnehmung durch die ehrenamtlich tätigen *Knappschaftsältesten* (12. TB S. 60) aufgegriffen. Schriftstücke werden in Zukunft durch Knappschaftsälteste nur noch in verschlossenen Umschlägen zugestellt. In der Geschäftsordnung soll geregelt werden, daß auf Wunsch des Versicherten Schriftstücke auch durch die Post zugestellt werden.

39. Zur *Durchführung von Außenprüfungen* im Sinne des § 132a AFG durch die Bundesanstalt für Arbeit (s. 12. TB S. 64f.) hat mir der Bundesminister für Arbeit und Sozialordnung mitgeteilt, Außenprüfungen seien nur effizient, wenn ihnen ein umfassendes Prüfungsrecht zugrundeliege. Dazu müßten auch automatisierte Verfahren zum Abgleich von Dateien der Beschäftigten eines überprüften Betriebes mit Dateien der Bundesanstalt für Arbeit eingesetzt werden. Der BMA beabsichtigt, eine klarstellende Ergänzung des § 132a AFG vorzuschlagen.

40. Über die *Auskunftspflicht unterhaltsverpflichteter Personen* im Verfahren der Gewährung von Arbeitslosenhilfe habe ich bereits mehrfach berichtet (u. a. 12. TB, S. 65ff.). Der Bundesminister für Arbeit und Sozialordnung hat die Bundesanstalt für Arbeit zwischenzeitlich gebeten, in den Fällen des § 137 Abs. 1a AFG die Höhe des zu berücksichtigenden Einkommens zu schätzen, falls Angehörige die erforderlichen Angaben nicht freiwillig machen. Nach dieser Vorschrift gilt der Arbeitslose als nicht bedürftig, soweit er auf berücksichtigungsfähige Ansprüche gegenüber Unterhaltsverpflichteten verzichtet oder Handlungen unterlassen hat, die Voraussetzung für das Entstehen oder Fortbestehen eines derartigen Anspruchs sind. Ich werde die Auswirkungen dieser Praxis aufmerksam verfolgen, weil der geschilderte Sachverhalt immer wieder Anlaß zu Eingaben von Bürgern, insbesondere von Eltern Arbeitsloser, ist.

41. Die *Kaufmännische Krankenkasse Hannover* (KKH) hat auf Grund meiner Empfehlungen zur Bearbeitung von Beihilfevorgängen (12. TB S. 68ff.) zwischenzeitlich die Bearbeitung der Beihilfe vollständig von der Personalverwaltung getrennt; die Bearbeitung erfolgt in einer eigenen Bearbeitungsstelle für die Leistungsangelegenheiten der bei der KKH versicherten Mitarbeiter und deren Angehörige. Über Widersprüche in Beihilfeangelegenheiten entscheidet ein bei der KKH tätiger Jurist, der an Personalentscheidungen nicht beteiligt ist und auf seine Geheimhaltungspflicht auch gegenüber Vorgesetzten schriftlich hingewiesen wurde.

42. Meinen Bedenken zu den Datenverarbeitungsprogrammen KLINAIDS (multizentrische Studie zum Verlauf der HIV-Infektion) und KLIMACS (klinisch-medizinische Analysen — Computer System) wurde erfreulicherweise Rechnung getragen (siehe 12. TB S. 71f.). Beide Programmpakete dürfen in Kliniken nur noch im Zusammenhang mit einer Sicherheitssoftware eingesetzt werden, und zu beiden gibt es Empfehlungen, die Datenschutzanforderungen einschließlich Sicherheitsanforderungen für den Anwender der Programme festlegen. Damit ist bundesseitig für KLINAIDS und KLIMACS ein sicherer Rahmen geschaffen worden, mit dem meine Bedenken ausgeräumt wurden. Details für die Anforderungen müssen jedoch für die jeweilige Klinik unter Einbeziehung der Landesbeauftragten für den Datenschutz bestimmt werden. Die betroffenen Ministerien haben mir zugesagt, mich weiterhin über die

Entwicklung der Projekte und deren Einsatz auf dem laufenden zu halten.

43. Im Bundesgesundheitsamt, im Robert-Koch-Institut und im *AIDS-Zentrum* wurden meine Empfehlungen für einen sicheren Einsatz von MS-DOS-geführten Arbeitsplatzrechnern einschließlich einer sicheren Umgebung hierfür mittlerweile umgesetzt (siehe 12. TB S. 72).

44. Im 12. TB habe ich mich zu den mit einem *Krebsregister* verbundenen rechtlichen Problemen geäußert (S. 71). Im Berichtszeitraum hat der Bundesminister für Gesundheit umfassende Überlegungen für die Schaffung eines Bundeskrebsregistersgesetzes angestellt. Im Rahmen der Besprechungen hierzu habe ich auf meine im 12. TB wiedergegebene Position verwiesen, wonach aus der Sicht des Datenschutzes ein nicht-personenbezogenes Krebsregister wünschenswert sei. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission hat mich hierin unterstützt (siehe Anlage 7). Die Notwendigkeit einer gesetzlichen Regelung ist durch die Existenz des Nationalen Krebsregisters der früheren DDR besonders aktuell geworden (s. 2.12). Ein Referentenentwurf für ein Bundeskrebsregistergesetz lag bis Redaktionsschluß nicht vor.

45. Anläßlich einer Prüfung der Abteilung Staatsschutz des Bundeskriminalamts hatte ich die Speicherung und Verarbeitung personenbezogener Daten im *Nachrichtendienstlichen Informationssystem (NADIS)* der Verfassungsschutzbehörden beanstandet. Der Bundesminister des Innern hatte diese Beanstandung zurückgewiesen (10. TB S. 78, 11. TB S. 64f.). Da das neue Verfassungsschutzgesetz eine solche Datenverarbeitung des BKA in NADIS nicht mehr zuläßt, habe ich noch vor Inkrafttreten dieses Gesetzes beim BMI nachgefragt, ob und welche Maßnahmen ergriffen worden seien, um dem neuen Gesetz zu entsprechen. Daraufhin hat er mir mitgeteilt, daß das Bundeskriminalamt alle Tätigkeiten in NADIS mit Ablauf des 31. Oktober 1990 eingestellt hat und der Datenbestand des BKA in NADIS am 8. November 1990 vom Bundesamt für Verfassungsschutz gelöscht worden ist.

46. Auf datenschutzrechtliche Probleme der Verfassungsschutz-Verbunddatei *ADOS* (Adressen und Objekte Ost) habe ich hingewiesen (12. TB S. 78f.) Nach Mitteilung des BMI ist die Datei inzwischen aufgelöst.

47. Das Bereithalten von Daten der *zollrechtlichen Überwachung* zum Abruf beim innerdeutschen Flugverkehr durch die Berliner Polizei habe ich wegen Verstoßes gegen § 3 BDSG i.V.m. § 2 Abs. 2 Nr. 2 BDSG und gegen das Steuergeheimnis nach § 30 Abgabenordnung beanstandet (vgl. 12. TB S. 76f.). Nachdem der Bundesminister der Finanzen und die Dienststellen der Berliner Polizei meine rechtliche Bewertung teilten, ist der Zugriff im Mai 1990 beendet worden. Nach der Vereinigung Deutschlands werden Kontrollen des innerdeutschen Flugverkehrs in Berlin nicht mehr durchgeführt.

48. Auf meine Beanstandung hin wurden beim Streitkräfteamt geführte Dateien mit Daten und Äußerungen von Personen, die aus der Sicht der *Psychologischen Verteidigung* als besonders bedeutsam angesehen wurden, vernichtet, da hierfür eine Rechtsgrundlage nicht vorhanden war und die rechtmäßige Erfüllung der Aufgaben des Amtes diese Dateien nicht erforderte (12. TB S. 79). Wie zwischenzeitlich der Presse zu entnehmen war, wurde am 1. Juli 1990 das für Psychologische Verteidigung zuständige Leitreferat beim BMVg aufgelöst. Die Zentrale Dienstvorschrift für die Psychologische Verteidigung, die im Zusammenhang mit der oben genannten Führung der Dateien Bedeutung hatte, wurde außer Kraft gesetzt. Damit kann die Wiederholung eines entsprechenden Vorgangs als ausgeschlossen gelten.

49. Ich habe darüber berichtet, daß das *Bundesaufsichtsamt für das Versicherungswesen* im Rahmen von Mitteilungen der Versicherungen über Unregelmäßigkeiten im Außendienst auch personenbezogene Daten von Außendienstmitarbeitern erhebt (s. 12. TB S.82). Der Bundesminister der Finanzen war weiterhin nicht bereit, diese nicht erforderlichen Datenerhebungen abzustellen. Dies habe ich im März 1991 förmlich beanstandet.

50. Mit dem Bundesminister der Finanzen habe ich weiter die Frage erörtert, ob § 81 des *Versicherungsaufsichtsgesetzes* eine normenklare Rechtsgrundlage für die Erhebung und Speicherung personenbezogener Daten über Vorstandsmitglieder von Versicherungsgesellschaften durch das Bundesaufsichtsamt für das Versicherungswesen darstellt (vgl. 12. TB S. 82). Er ist bisher nur bereit, bei nächster Gelegenheit zu prüfen, ob die Vorschrift entsprechend geändert werden muß.

51. Die anläßlich einer Kontrolle beim *Bundesaufsichtsamt für das Kreditwesen* festgestellten datenschutzrechtlichen Mängel wurden infolge der kooperativen Haltung des Bundesaufsichtsamtes bis auf einen Fragenbereich sehr zügig geklärt (12. TB S. 82f). Auch die verbliebenen Fragen zur technischen und organisatorischen Datensicherung im Zusammenhang mit einem online-Zugriff des Bundesaufsichtsamtes auf einige Datenbanken der Deutschen Bundesbank wurden zwischenzeitlich befriedigend gelöst.

52. In meinem Elften Tätigkeitsbericht (S. 75f.) habe ich nicht erforderliche Datenübermittlungen aus *Einfuhrkontrollmeldungen* an Verwertungsgesellschaften gerügt und auf eine beabsichtigte Neuregelung hingewiesen. Diese ist mittlerweile in der Fünften Verordnung zur Änderung der Außenwirtschaftsverordnung in befriedigender Weise getroffen worden.

53. Die Gesetzentwürfe zur Verbesserung der *Außenwirtschaftskontrolle* (12. TB S. 83) sind zwischenzeitlich in Kraft getreten. Die von mir dargestellten datenschutzrechtlichen Kompromisse sind durch ergänzende Regelungen im Außenwirtschaftsgesetz, im Atomgesetz und im Finanzver-

waltungsgesetz berücksichtigt worden. Das Instrumentarium der Außenwirtschaftskontrolle wurde inzwischen noch weiter vervollständigt (siehe oben 18).

54. In einem ergänzenden Beschluß hat der Deutsche Bundestag bei Verabschiedung des Gesetzes über die *Umweltverträglichkeitsprüfung* von der Bundesregierung Gesetzentwürfe erbeten zur Sicherung der informationellen Selbstbestimmung in solchen Verfahren, die der Entscheidung über die Zulässigkeit von Vorhaben unter dem Gesichtspunkt der Umweltverträglichkeit dienen und die unter Einbeziehung der Öffentlichkeit durchgeführt werden (12. TB S. 83f.). Regierungsentwürfe hierzu liegen bislang nicht vor. Den Beginn der 12. Legislaturperiode nehme ich zum Anlaß, nachdrücklich solche datenschutzrechtlich erforderlichen Nachbesserungen zu fordern.

55. In den Entwürfen eines *Ernährungssicherstellungsgesetzes* und eines *Ernährungsvorsorgegesetzes*, über die ich berichtet habe (12. TB S. 84), konnte ich im Rahmen der Ausschußberatungen des Deutschen Bundestages weitere datenschutzrechtliche Verbesserungen durchsetzen. Der Kreis der Auskunftsverpflichteteten ist — unter dem Gesichtspunkt der Erforderlichkeit — noch klarer abgegrenzt worden. Es ist auch sichergestellt, daß nicht etwa eine Art paralleles Melderegister auf Vorrat geführt wird; Übermittlungen der Meldebehörden dürfen zur Ernährungsvorsorge erst nach Feststellung einer Versorgungskrise durch die Bundesregierung, zur Ernährungssicherstellung erst nach Feststellung des Spannungs- oder Verteidigungsfalles oder nach besonderer Zustimmung durch den Bundestag erfolgen.

56. In meinem 11. TB (S. 78f.) und meinem 12. TB (S. 92) habe ich ausführlich zum Entwurf eines *Gesetzes über Verbraucherkredite* berichtet. Die konkreten mit dem Bundesminister der Justiz abgestimmten Vorschläge zur Verbesserung des Datenschutzes in diesem Gesetz wurden vom Deutschen Bundestag leider nicht übernommen. Der federführende Rechtsausschuß, dem ich meine Vorschläge schriftlich übermittelt hatte, ist — mir wenig verständlich — in seiner Beschlußempfehlung zu diesem Gesetz nicht einmal darauf eingegangen, daß es fachlich unbedenkliche Vorschläge zur Verbesserung des Datenschutzes gegeben hat und warum er diese ablehnte. Das Gesetz über Verbraucherkredite vom 17. Dezember 1990 wurde im Bundesgesetzblatt I S. 2840 verkündet.

Anlage 1 (zu 2.2 und 2.5.1)

Vorläufige Regelung zur Behandlung von Unterlagen des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit

(Anlage I Kapitel II Sachgebiet B Abschnitt II Nr. 2 Buchstabe b des Einigungsvertrages vom 31. August 1990 i. V. m. Artikel 1 des Einigungsvertragsgesetzes vom 23. September 1990, BGBl. 1990 II S. 885, 912f.)

Die vom ehemaligen Staatssicherheitsdienst der Deutschen Demokratischen Republik rechts- und verfassungswidrig gewonnenen personenbezogenen Informationen betreffen eine Vielzahl von Bürgern aus ganz Deutschland. Die Aufbewahrung, Nutzung und Sicherung dieser Unterlagen bedarf wegen der damit verbundenen erheblichen Eingriffe in Grundrechtspositionen einer umfassenden gesetzlichen Regelung durch den gesamtdeutschen Gesetzgeber. Die Vertragsparteien empfehlen den gesetzgebenden Körperschaften dabei die Grundsätze zu berücksichtigen, wie sie in dem von der Volkskammer am 24. August 1990 verabschiedeten Gesetz über die Sicherung und Nutzung der personenbezogenen Daten des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit zum Ausdruck gekommen sind. Bis dahin gelten vom Wirksamwerden des Beitritts an für die Behandlung von Unterlagen des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit der Deutschen Demokratischen Republik anstelle der Vorschriften des Bundesarchivgesetzes die folgenden besonderen Vorschriften:

§ 1

(1) Die Dateien und Unterlagen des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit der Deutschen Demokratischen Republik, die personenbezogene Daten enthalten, sind bis zu einer endgültigen gesetzlichen Regelung durch einen Sonderbeauftragten der Bundesregierung in sichere Verwahrung zu nehmen und gegen unbefugten Zugriff zu sichern. Der Sonderbeauftragte wird auf Vorschlag des Ministerrates der Deutschen Demokratischen Republik, der der Zustimmung der Volkskammer bedarf, bis spätestens zum 2. Oktober 1990 von der Bundesregierung berufen. Sein Ständiger Vertreter ist der Präsident des Bundesarchivs.

(2) Der Sonderbeauftragte ist in der Ausübung dieses Amtes unabhängig und untersteht der Rechtsaufsicht der Bundesregierung. Er ist speichernde Stelle im Sinne des Bundesdatenschutzgesetzes.

(3) Der Sonderbeauftragte wird durch einen von der Bundesregierung zu bestellenden Beirat beraten. Der Beirat besteht aus fünf Personen, von denen mindestens drei ihren Hauptwohnsitz zum Zeitpunkt des Wirksamwerdens des Beitritts in dem in Artikel 3 des Vertrages genannten Gebiet haben müssen.

(4) Der Sonderbeauftragte wird bei der Wahrnehmung seiner Aufgaben durch das Bundesarchiv und den Bundesbeauftragten für den Datenschutz unterstützt. In wichtigen Angelegenheiten ist der Bundesbeauftragte für den Datenschutz vorher zu hören.

§ 2

(1) Die in § 1 genannten Dateien und Unterlagen sind gesperrt. Ihre Löschung ist unzulässig. Die Lagerung erfolgt zentral in dem in Artikel 3 des Vertrages genannten Gebiet. Die personenbezogenen Daten dürfen nur für folgende Zwecke übermittelt und genutzt werden, soweit dies unerläßlich und nicht bis zu einer abschließenden gesetzlichen Regelung aufschiebbar ist:

1. für Zwecke der Wiedergutmachung und der Rehabilitierung von Betroffenen,
2. zur Feststellung einer offiziellen oder inoffiziellen Tätigkeit für das ehemalige Ministerium für Staatssicherheit/Amt für Nationale Sicherheit der Deutschen Demokratischen Republik und zwar
   a) für die Überprüfung von Abgeordneten und Kandidaten für parlamentarische Mandate mit Zustimmung der Betroffenen,
   b) für die Weiterverwendung von Personen im öffentlichen Dienst (Anlage I Kapitel XIX Sachgebiet A Abschnitt III Nr. 1) mit deren Kenntnis und
   c) für die Einstellung von Personen in den öffentlichen Dienst und für Sicherheitsüberprüfungen mit Zustimmung der Betroffenen,
3. zur Verfolgung von Straftaten im Zusammenhang mit der Tätigkeit des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit der Deutschen Demokratischen Republik und
4. zur Aufklärung und Verfolgung der in Artikel 1 § 2 Abs. 1 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Gesetz zu Artikel 10 des Grundgesetzes) genannten Straftaten durch Strafverfolgungsbehörden und andere Behörden im Rahmen ihrer gesetzlichen Aufgaben.

(2) Der Sonderbeauftragte darf für diese Zwecke an die zuständigen Stellen Auskünfte erteilen. Die Herausgabe von Unterlagen und die Einsicht in Unterlagen ist nur in dem erforderlichen Umfang und nur soweit zulässig, wie die Erteilung von Auskünften für den Zweck nicht ausreicht. Der Empfänger darf die Daten nur zu dem Zweck verarbeiten und nutzen, zu dem sie ihm übermittelt worden sind. Sind die benötigten personenbezogenen Daten mit weiteren Daten des Betroffenen oder eines Dritten in Akten so verbun-

den, daß eine Trennung nicht oder nur mit unvertretbarem Aufwand möglich ist, ist die Herausgabe von Unterlagen oder die Einsichtgewährung auch hinsichtlich dieser Daten zulässig, soweit nicht berechtigte Interessen des Betroffenen oder des Dritten an deren Geheimhaltung überwiegen; eine Nutzung dieser Daten ist unzulässig.

§ 3

Den Betroffenen ist für die in § 2 Abs. 1 Nr. 1 genannten Zwecke sowie zur Abwehr einer gegenwärtigen oder drohenden Verletzung ihres Persönlichkeitsrechtes Auskunft über die zu ihrer Person vorhandenen Daten zu erteilen, soweit dies zur Verfolgung ihrer Rechte unerläßlich und unaufschiebbar ist. Die Auskunft ist so zu erteilen, daß überwiegende schutzwürdige Interessen Dritter nicht beeinträchtigt werden.

§ 4

Der Umgang mit den vorhandenen Dateien und Unterlagen, insbesondere ihre Sicherung gegen unbefugten Zugriff, ihre Nutzung und die Auskunftserteilung an Betroffene unterliegen der Kontrolle des Bundesbeauftragten für den Datenschutz.

§ 5

Im übrigen gelten die Vorschriften des Bundesdatenschutzgesetzes.

Anlage 2 (zu 2.5.1 und 2.5.2)

Vereinbarung zwischen der Bundesrepublik Deutschland und der Deutschen Demokratischen Republik zur Durchführung und Auslegung des Einigungsvertrags („Ergänzungsvereinbarung")

(Vereinbarung vom 18. September 1990 i. V. m. Artikel 1 des Gesetzes vom 23. September 1990, BGBl. 1990 II S. 885, 1239)

Artikel 1

Zu der Frage der weiteren Vorgehensweise hinsichtlich der vom ehemaligen Staatssicherheitsdienst der Deutschen Demokratischen Republik gewonnenen personenbezogenen Informationen stellen die Regierungen der beiden Vertragsparteien übereinstimmend fest:

1. Sie erwarten, daß der gesamtdeutsche Gesetzgeber die Grundsätze, wie sie in dem von der Volkskammer am 24. August 1990 verabschiedeten Gesetz über die Sicherung und Nutzung der personenbezogenen Daten des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit zum Ausdruck kommen, umfassend berücksichtigt.

2. Sie erwarten, daß der gesamtdeutsche Gesetzgeber die Voraussetzungen dafür schafft, daß die politische, historische und juristische Aufarbeitung der Tätigkeit des ehemaligen Ministeriums für Staatssicherheit/Amtes für Nationale Sicherheit gewährleistet bleibt.

3. Sie gehen davon aus, daß ein angemessener Ausgleich zwischen

   — der politischen, historischen und juristischen Aufarbeitung,

   — der Sicherung der individuellen Rechte der Betroffenen und

   — dem gebotenen Schutz des einzelnen vor unbefugter Verwendung seiner persönlichen Daten

   geschaffen wird.

4. Sie gehen davon aus, daß von den in Artikel 1 des Einigungsvertrags genannten Ländern bestellte Beauftragte den Sonderbeauftragten bei der Erfüllung seiner gesetzlichen Aufgaben beraten und unterstützen, damit die Interessen der Bürger der neuen Bundesländer in besonderer Weise Berücksichtigung finden.

5. Sie stellen Einvernehmen darüber fest, daß bei zentraler Verwaltung die sichere Verwahrung, Archivierung und Nutzung der Unterlagen zentral und regional erfolgen kann. In wichtigen Angelegenheiten der sicheren Verwahrung, Archivierung und Nutzung der Unterlagen soll sich der Sonderbeauftragte mit dem Beauftragten des jeweiligen Landes ins Benehmen setzen.

6. Sie gehen davon aus, daß so bald wie möglich den Betroffenen ein Auskunftsrecht — unter Wahrung der schutzwürdigen Interessen Dritter — eingeräumt wird.

7. Sie gehen davon aus, daß der Sonderbeauftragte unverzüglich eine Benutzerordnung erläßt, die die gesetzlichen Vorgaben ausfüllt. Mit dieser Benutzerordnung werden zugleich Inhalt, Art und Umfang der Beratung und Unterstützung durch die Landesbeauftragten näher bestimmt.

8. Sie gehen davon aus, daß bis auf die unumgängliche Mitwirkung bei der Aufklärung und Verfolgung von Straftaten entsprechend § 2 Abs. 1 Nr. 4 der Maßgabe b) zum Bundesarchivgesetz die Nutzung oder Übermittlung von Daten für nachrichtendienstliche Zwecke ausgeschlossen wird. Der Bundesminister des Innern wird das Bundesamt für Verfassungsschutz anweisen, bis zum Erlaß der in Nummer 7 genannten Benutzerordnung keine diesbezüglichen Anfragen an den Sonderbeauftragten zu richten. Die verwendeten Informationen aus den Akten sind so zu kennzeichnen, daß Art, Umfang und Herkunft der übermittelten Daten kontrollierbar und eine abschließende gesetzgeberische Entscheidung über den Verbleib der Daten möglich bleibt.

9. Die Regierungen der beiden Vertragsparteien gehen davon aus, daß die Gesetzgebungsarbeit zur endgültigen Regelung dieser Materie unverzüglich nach dem 3. Oktober 1990 aufgenommen wird. Dabei soll das Volkskammergesetz in Verbindung mit dem Einigungsvertrag als Grundlage dienen.

Anlage 3 (zu 26 und 19.1)

Entschließung der 39. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 — gegen die Stimme Bayerns — zum Datenschutzgesetz und zum Bundesverfassungsschutzgesetz

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz (gegen die Stimme Bayerns) begrüßt die mit den am 13. März 1990 vorgelegten Vorschläge der Koalitionsfraktionen verbundene Absicht, die längst fällige Novellierung des Bundesdatenschutzgesetzes und des Bundesverfassungsschutzgesetzes noch rechtzeitig vor dem Ende der Legislaturperiode zu verabschieden.

Die Vorschläge zum *Bundesdatenschutzgesetz* beseitigen eine Reihe von Schwächen des Regierungsentwurfes. Hervorzuheben ist insoweit

- daß nunmehr für den öffentlichen Bereich die Verarbeitung personenbezogener Daten in Akten und die Datenerhebung durch öffentliche Stellen in den Geltungsbereich des Bundesdatenschutzgesetzes einbezogen werden,
- daß künftig der Bundesbeauftragte für den Datenschutz durch das Parlament gewählt werden soll,
- daß der Betroffene bei Ablehnung der Auskunftserteilung darauf hingewiesen wird, daß er sich an den Bundesbeauftragten für den Datenschutz wenden kann.

Demgegenüber weisen auch die Vorschläge noch Schwächen und Defizite auf. Dazu gehören u. a.:

- Die unzureichende Kontrollbefugnis des Bundesbeauftragten für den Datenschutz bei der Datenverarbeitung in Akten,
- ein Widerspruchsvorbehalt für die Betroffenen gegen eine Kontrolle ihrer Daten durch den Bundesbeauftragten für den Datenschutz, der systematische Prüfungen gefährdet und deshalb entbehrlich ist, weil es für die Datenschutzbeauftragten schon immer selbstverständlich war, die Daten von Betroffenen nicht gegen deren erklärten Willen in Kontrollen einzubeziehen,
- die verfassungswidrige Erstreckung des Widerspruchsvorbehaltes in der Neufassung auf die Landesbeauftragten für den Datenschutz,
- das Fehlen eines gesonderten Gesetzesvorbehaltes für die Einrichtung von Direktzugriffsverfahren in besonders sensiblen Bereichen,
- der zu weite Katalog erlaubter Zweckänderungen und die unzureichende Unterrichtung des Betroffenen über die Zweckänderung.

Im Bereich der Datenverarbeitung durch nichtöffentliche Stellen verschlechtern einzelne vorgeschlagene Regelungen die Rechte der Betroffenen im Vergleich zum geltenden Gesetz, etwa bei der Übermittlung von Daten an den Adressenhandel. Sie bleiben im übrigen weit hinter den Vorschlägen für den öffentlichen Bereich zurück. Weder die Verarbeitung in Akten noch die Datenerhebung werden einbezogen. Auch die höchst unzureichenden Kontrollbefugnisse der Datenschutzaufsichtsbehörden sind nicht wesentlich verbessert worden.

Schließlich erinnern die Datenschutzbeauftragten an ihre früheren Forderungen nach bereichsspezifischen Regelungen für die Verarbeitung von Arbeitnehmerdaten sowie von Regelungen für den Kredit- und Versicherungsbereich.

Zu den Vorschlägen der Koalition für das *Bundesverfassungsschutzgesetz* stellen die Datenschutzbeauftragten des Bundes und der Länder fest:

Die Vorschläge bringen gegenüber dem Vorentwurf der Bundesregierung Verbesserungen. Dies gilt insbesondere für:

- Den Schutz des in Wohnungen nichtöffentlich gesprochenen Wortes vor heimlichem Mithören und Aufzeichnen,
- die Einschränkung der Speicherung von Daten über Minderjährige,
- die konkretisierenden und einschränkenden Regelungen für den Einsatz nachrichtendienstlicher Mittel,
- die präzise Definition der „Bestrebungen" gegen die freiheitlich-demokratische Grundordnung,
- die Anknüpfung der Sammlung und Verarbeitung von Daten an das Vorliegen tatsächlicher Voraussetzungen.

Hingegen sind u. a. folgende datenschutzrechtliche Anforderungen noch nicht erfüllt:

- Die Befugnisse zur Datenverarbeitung müssen differenziert den unterschiedlichen Aufgaben zugeordnet werden.
- Die Datenspeicherung ist nicht so präzise geregelt, daß der Bürger dem Gesetz entnehmen kann, unter welchen in seiner Person liegenden Voraussetzungen der Verfassungsschutz über ihn Daten speichern darf.
- Die Zweckbindung der Daten innerhalb des Verfassungsschutzes ist nicht gewährleistet.
- Das Auskunftsrecht des Bürgers auch gegenüber den Verfassungsschutzbehörden wird zwar nunmehr erstmals anerkannt. Die vorgeschlagene Regelung schränkt aber den Auskunftsanspruch zu sehr ein. So wird dem Bürger eine Pflicht zur Begründung seines Auskunftsersuchens auferlegt,

während die Ablehnung der Auskunft unter keinen Umständen begründet werden muß.

- Die vorgesehenen Regelungen zur Sicherheitsüberprüfung ersetzen nicht eine bereichsspezifische, präzise Rechtsgrundlage in einem Geheimschutzgesetz für das Überprüfungsverfahren.

Die Datenschutzbeauftragten gehen davon aus und halten es für notwendig, daß die bestehenden Mängel der Gesetzentwürfe in den anstehenden Parlamentsberatungen behoben und ihre Anregungen aufgegriffen werden.

Anlage 4 (zu 2.1)

Entschließung der 39. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 22./23. März 1990 zum Datenschutz im deutsch-deutschen Verhältnis

1. Das Engagement der Bevölkerung in der DDR für den Schutz ihrer personenbezogenen Daten z. B. beim Staatssicherheitsdienst zeigt, wie elementar die Persönlichkeitsrechte von den Bürgern in der DDR verstanden werden und daß sie das Recht auf informationelle Selbstbestimmung als Teil des allgemeinen Selbstbestimmungsrechts wahrnehmen.

   Die Konferenz der Datenschutzbeauftragten begrüßt Bemühungen, auch in der DDR angemessene Datenschutzregelungen zu schaffen.

2. Obwohl in der DDR keine hinreichenden Datenschutzregelungen bestehen, werden bereits jetzt mehr personenbezogene Daten als früher ausgetauscht. Dieser Datentransfer wird noch zunehmen. Aktuelle Anlässe, wie der Austausch von Daten bei Verkehrsunfällen sowie im Rahmen der Gefahrenabwehr und der Strafverfolgung, haben in der Öffentlichkeit besondere Aufmerksamkeit gefunden.

   Der Prozeß der sozialen, wirtschaftlichen und politischen Einigung führt zu verstärktem grenzüberschreitenden Datenverkehr, z. B. im Sozialrecht, im Melderecht, im Versicherungs- und Kreditrecht. Dies wirft Fragen des Datenschutzes auf. Für die Bundesrepublik Deutschland gelten das allgemeine Datenschutzrecht und besondere Gesetze wie z. B. das Gesetz über die innerdeutsche Rechts- und Amtshilfe in Strafsachen vom 2. Mai 1953 sowie Vereinbarungen.

   Bei der Verwirklichung technischer Maßnahmen, insbesondere bei dem Ausbau der Telekommunikationsdienste und bei der automatisierten Datenverarbeitung, muß der Datenschutz beachtet werden.

3. Die Datenschutzkonferenz hält es für geboten, daß der Austausch personenbezogener Daten zwischen Behörden und öffentlichen Stellen in der Bundesrepublik Deutschland und in der Deutschen Demokratischen Republik erst durchgeführt wird, wenn gewährleistet ist, daß nach folgenden Grundsätzen verfahren wird:

   - Die Grundsätze des Übereinkommens des Europarates über den Schutz des Menschen bei der Verarbeitung personenbezogener Daten vom 28. Januar 1981 sind zu beachten.
   - Die Übermittlung personenbezogener Informationen unterbleibt, soweit Grund zu der Annahme besteht, daß dadurch gegen den Zweck eines Gesetzes der Bundesrepublik Deutschland verstoßen würde oder schutzwürdige Belange bei den betroffenen Personen beeinträchtigt würden. Die Übermittlung personenbezogener Informationen unterbleibt insbesondere dann, wenn Grund zu der Annahme besteht, daß die Verwendung der übermittelten Informationen nicht in Einklang mit rechtsstaatlichen Grundsätzen steht oder dem Betroffenen aus der Verwendung der Informationen erhebliche Nachteile erwachsen, die im Widerspruch zu rechtsstaatlichen Grundsätzen stehen.
   - Der Empfänger darf personenbezogene Informationen nur zu dem durch die übermittelnde Stelle angegebenen Zweck und unter den von ihr vorgeschriebenen Bedingungen nutzen.
   - Personenbezogene Informationen dürfen ausschließlich an die in den Abkommen oder Absprachen genannten Behörden übermittelt werden. Eine Übermittlung an andere Stellen darf nur mit vorheriger Zustimmung der übermittelnden Stelle erfolgen.
   - Der Empfänger unterrichtet die übermittelnde Stelle und den zuständigen Datenschutzbeauftragten auf Ersuchen über die Verwendung der übermittelten Informationen und über die dadurch erzielten Ergebnisse.
   - Die übermittelnde Stelle ist verpflichtet, auf die Richtigkeit der zu übermittelnden Informationen zu achten. Erweist sich, daß unrichtige oder zu vernichtende personenbezogene Informationen übermittelt worden sind, so ist dies dem Empfänger unverzüglich mitzuteilen. Dieser ist verpflichtet, die Berichtigung oder Vernichtung vorzunehmen.
   - Dem Betroffenen ist auf Antrag über die zu seiner Person vorhandenen Informationen sowie über den vorgesehenen Verwendungszweck Auskunft zu erteilen. Eine Verpflichtung zur Auskunftserteilung besteht nicht, soweit eine Abwägung ergibt, daß eine Auskunft den Verwendungszweck oder schutzwürdige Interessen Dritter gefährden würde.
   - Die Übermittlung und der Empfang personenbezogener Informationen sind aktenkundig zu machen.
   - Zur Gewährleistung dieser Grundsätze sind die verfahrensmäßigen Sicherungen vorzusehen. Dazu kann es gehören, besondere Stellen mit der Datenübermittlung zu beauftragen. Die Kontrolle der Datenübermittlung durch unabhängige Datenschutzbeauftragte muß gewährleistet sein.

4. Die Verarbeitung personenbezogener Daten bei den Sicherheitsbehörden der Bundesrepublik Deutschland muß im Hinblick auf die politischen Veränderungen in der DDR und im übrigen Mittel- und Osteuropa über die bereits getroffenen Maßnahmen hinaus überprüft werden. Diese Notwendigkeit besteht u. a. bei:

   — dem Verfahren der Sicherheitsüberprüfung,

   — der Datenerhebung und Datenübermittlung des Bundesgrenzschutzes anläßlich von Grenzkontrollen an die Nachrichtendienste,

   — der Bereinigung der Datensammlungen der Verfassungsschutzbehörden.

Anlage 5 (zu 4.1)

Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. Juni 1990 — gegen die Stimme Bayerns — zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität

Die Konferenz der Datenschutzbeauftragten hat schwerwiegende datenschutzrechtliche Bedenken gegen die Ausweitung der polizeilichen Ermittlungsbefugnisse in der Strafprozeßordnung, wie sie mit dem vom Bundesrat vorgelegten Gesetzentwurf zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität (OrgKG) beabsichtigt ist.

Erstmals werden in die Strafprozeßordnung Regelungen zur Rasterfahndung, zum Einsatz Verdeckter Ermittler sowie von Wanzen und Richtmikrofonen und heimlichen Film- und Fotoaufnahmen eingefügt. Die Konferenz der Datenschutzbeauftragten verkennt nicht, daß bestimmte Erscheinungsformen von Kriminalität im Interesse des Schutzes der Bürger besondere Ermittlungsmethoden erforderlich machen können. Der vorgelegte Entwurf regelt jedoch nicht nur neue Eingriffsbefugnisse zur Bekämpfung des illegalen Rauschgifthandels und sonstiger organisierter Kriminalität — die im übrigen nicht definiert wird —, sondern soll tief in die Privatsphäre der Bürger eingreifende Fahndungs- und Ermittlungsmethoden in das Strafverfahrensrecht allgemein einführen.

Gegen den vorliegenden Entwurf bestehen insbesondere folgende datenschutzrechtliche Bedenken:

- Die vorgesehenen Eingriffsbefugnisse der Strafverfolgungsbehörden werden an den konturenlosen Begriff „Straftaten von erheblicher Bedeutung" geknüpft. Damit dürfte nach der Begründung des Gesetzentwurfs in der Praxis allenfalls die Kleinkriminalität ausscheiden. So soll z. B. auch die *Rasterfahndung* für eine Vielzahl von Delikten außerhalb organisierter Kriminalität zugelassen werden. Dies erscheint besonders bedenklich, weil gerade diese Form der Fahndung unbescholtene Bürger in großer Zahl unvermeidlich mit einbezieht und sie in der Folge Ziel weiterer Ermittlungen werden können.
- Tief in die Privatsphäre eindringende Ermittlungsmethoden werden nicht hinreichend präzisiert und sind großenteils unverhältnismäßig: So dürfen ohne Wissen des Betroffenen zur Aufklärung *jeder Straftat* — sogar in Wohnungen hinein — „Lichtbilder und Bildaufzeichnungen" aufgenommen sowie „besondere Sichthilfen" eingesetzt werden.
- Maßnahmen, wie Einsatz von Peilsendern, Richtmikrofonen, Wanzen und sonstiger Überwachungstechniken können sich auch gegen dritte *unverdächtige Personen* richten, wenn „aufgrund bestimmter Tatsachen" anzunehmen ist, „daß sie mit dem Täter in Verbindung stehen oder eine solche Verbindung hergestellt wird". Es bleibt völlig offen, wie das Tatbestandsmerkmal der „Verbindung" eingegrenzt werden soll. Foto- und Filmaufnahmen von Unbeteiligten sind bereits zulässig, wenn sie für Ermittlungen „geeignet" sind. Damit kann kein Bürger vorhersehen, ob und wann er hiervon betroffen sein kann. Ohne Kenntnis der gegen ihn gerichteten Eingriffe kann er im Regelfall nicht einmal Rechtsschutz erlangen.
- Die Möglichkeiten der Telefonüberwachung werden über das vertretbare Maß hinaus ausgeweitet.
- Bedenken richten sich ferner dagegen, bei besonderen Ermittlungsmaßnahmen auf die vorherige *richterliche Kontrolle* zu verzichten und durch Eilkompetenzen die Entscheidung der diese Maßnahmen selbst durchführenden Polizei zu übertragen. Nicht einmal die nachträgliche richterliche Kontrolle ist in jedem Fall zwingend vorgesehen.

Im Gegensatz zu den erweiterten Befugnissen der Strafverfolgungsbehörden sind Regelungen zum Schutz oder im Interesse der Betroffenen nur unzureichend vorgesehen. Die mit besonderen Ermittlungsmethoden für besondere Strafverfolgungszwecke erhobenen Daten dürfen für zu weitgehende andere Zwecke verwendet werden. So sind z. B. die Begriffe „Zwecke der staatsanwaltschaftlichen Vorgangsverwaltung" und „Zwecke der Rechtspflege" zu unbestimmt. Es fehlen weiterhin ausreichende Bestimmungen zum Auskunftsrecht des Betroffenen und zur Löschung.

Zusammenfassend ist festzustellen, daß dieser Entwurf selbst hinter den datenschutzrechtlichen Ansätzen, wie sie etwa noch im Entwurf des Strafverfahrensänderungsgesetzes 1989 enthalten waren, zurückbleibt.

Die Konferenz der Datenschutzbeauftragten fordert den Deutschen Bundestag auf, diese Vorschläge des Gesetzentwurfs abzulehnen und die unterbrochenen Arbeiten an der umfassenden datenschutzrechtlichen Novellierung der Strafprozeßordnung, die dringend geboten ist, wieder aufzunehmen. Hierzu haben die Datenschutzbeauftragten wiederholt konkrete Vorschläge vorgelegt.

Anlage 6 (zu 29 Nr. 1)

Entschließung der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 — gegen die Stimme Bayerns mit Ausnahme des letzten Absatzes — zur Neuregelung des Melderechtsrahmengesetzes

Der dem Deutschen Bundestag vorliegende Entwurf eines Ersten Gesetzes zur Änderung des Melderechtsrahmengesetzes hält weiter an der Hotel- und Krankenhausmeldepflicht fest. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz hat erhebliche Bedenken, ob dem Bund die Gesetzgebungskompetenz zur Regelung dieser Frage zusteht. In jedem Fall ist zu bedenken:

Zweck der allgemeinen Meldepflicht ist es, die Identität der Einwohner und deren Wohnungen festzustellen und diese Basisinformation für die Bewältigung einer Vielzahl von Verwaltungsaufgaben zur Verfügung zu stellen. Bei einem kurzfristigen Aufenthalt in einem Hotel oder Krankenhaus entfällt dieser Zweck. Lediglich die Polizei hat ein Interesse an der Feststellung dieser Tatsachen. Schon deshalb paßt die Hotel- und Krankenhausmeldepflicht nicht in die Systematik des Melderechts, es handelt sich vielmehr um materielles Polizeirecht.

Polizeiliche Datenverarbeitung setzt voraus, daß Gefahren abgewendet oder Straftaten verfolgt bzw. verhütet werden sollen. Hotelgäste und Krankenhauspatienten können jedoch nicht schlechthin als Gefahrenquellen oder (potentielle) Straftäter angesehen werden. Vielmehr ist zu berücksichtigen, daß es sich im Regelfall um Bürger handelt, die ein Recht darauf haben, von polizeilichen Ermittlungen unbehelligt zu bleiben.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder und die Datenschutzkommission Rheinland-Pfalz ist darüber hinaus der Auffassung, daß den Bürgern in allen Meldegesetzen ein Widerspruchsrecht gegen die Weitergabe ihrer Daten an politische Parteien und Wählergruppen zum Zwecke der Wahlwerbung eingeräumt werden muß.

Gegenstimme Bayern mit Ausnahme des letzten Absatzes.

Anlage 7 (zu 2.12 und 29 Nr. 44)

Entschließung der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 zur Erarbeitung von Krebsregistergesetzen in Bund oder Ländern

1. Die Datenschutzbeauftragten haben schon in ihren Entschließungen vom 14. Dezember 1981 und 27. April 1982 zur Schaffung gesetzlicher Grundlagen für die Errichtung und Führung bevölkerungsbezogener epidemiologischer Krebsregister Stellung genommen. Wenn sich der Gesetzgeber zugunsten solcher Register, deren Nutzen auch unter Medizinern nicht unumstritten ist, entscheiden sollte, entspricht es dem gesetzlichen Auftrag der Datenschutzbeauftragten darauf zu achten, daß die Errichtung und Führung solcher Register in einer Weise geschieht, die auf das Persönlichkeitsrecht der Krebskranken in größtmöglichem Umfang Rücksicht nimmt.

2. Würde den Ärzten die Befugnis eingeräumt, ihre Krebskranken in jedem Fall ohne deren Einwilligung mit Namen an ein solches Register zu melden, würde dies einen äußerst schwerwiegenden Eingriff in deren durch Artikel 1 i. V. m. Artikel 2 Abs. 1 GG geschütztes Persönlichkeitsrecht darstellen, eine weitere Durchbrechung der ärztlichen Schweigepflicht zur Folge haben und damit das Arzt-/Patientenverhältnis erheblich belasten. Die Krebskranken würden ohne ihre Einwilligung zentral in einem Register gespeichert werden und zwar so, daß die registerführende Stelle feststellen kann, welche Personen an Krebs erkrankt und zum Register gemeldet worden sind.

Die Datenschutzbeauftragten sind deshalb der Auffassung, daß die Einrichtung eines Krebsregisters auf einer solchen Grundlage (Melderechtsmodell) nicht in Betracht kommt. Sie sind nach wie vor der Meinung, daß das Krebsregister nur mit Einwilligung der Patienten oder auf anonymer Basis geführt werden können. Für beides gibt es bereits Modelle (Einwilligungsmodell und dezentrales Verschlüsselungsmodell). Die Datenschutzbeauftragten sehen in diesen Modellen gangbare Wege zur Führung bevölkerungsbezogener Krebsregister, die auch noch fortentwickelt werden können.

Sollten weitere Modelle, die das Persönlichkeitsrecht der Krebskranken in gleicher Weise wahren, weiterentwickelt werden, sind die Datenschutzbeauftragten selbstverständlich bereit, auch sié in Erwägung zu ziehen.

Anlage 8 (zu 1.5)

Entschließung der 40. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 4./5. Oktober 1990 — bei Stimmenthaltung Bayerns — zur Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes

Wegen der dynamischen technischen Entwicklung auf dem Gebiet der Telekommunikation ist es dringlich, das Grundrecht auf freie Entfaltung der Persönlichkeit gegen neue Gefährdungen zu schützen. Den Risiken für das Recht auf unbeobachtete Kommunikation muß rechtzeitig begegnet werden:

- Die Einführung von ISDN macht es möglich, daß auch nach Beendigung von Telefongesprächen über einen bestimmten Zeitraum gespeichert wird, wer wann mit wem wie lange telefoniert hat.
- Der zunehmende Einsatz von Funkdiensten im Telekommunikationsverkehr (z. B. mobile Telefone, Satellitenkommunikation) ist mit der Speicherung von noch mehr Daten über die Telefonverbindungen verbunden und erleichtert die Möglichkeit des Abhörens und Aufzeichnens der Gesprächsinhalte.
- Zunehmend stehen Abhöranlagen zur Verfügung, mit denen aus der Masse der geführten Telefongespräche bestimmte Telefonate gezielt herausgegriffen, aufgezeichnet und nach bestimmten Gesichtspunkten ausgewertet und gespeichert werden können.

Das Grundgesetz läßt Einschränkungen des Fernmeldegeheimnisses unter gewissen Voraussetzungen auf gesetzlicher Grundlage zu. In den vergangenen Jahren hat der Gesetzgeber diese Eingriffsmöglichkeiten mehrmals erweitert und hierbei alle Telekommunikationsdienste (wie z. B. Telefax und Btx) einbezogen. Zudem hat die Rechtsprechung den Anwendungsbereich extensiv ausgelegt. Vor diesem Hintergrund ist es erforderlich:

- Die gesetzlichen Regelungen präziser und enger zu fassen,
- bei Entwicklung, Auswahl und Einsatz von Telekommunikationstechniken darauf zu achten, daß bei deren Betrieb die Speicherung personenbezogener Daten nach Dauer und Umfang auf das wirklich notwendige Maß beschränkt wird,
- erlaubte Eingriffe in das Grundrecht nach Artikel 10 auf das unerläßliche Maß zu beschränken und eine strenge Zweckbindung der dabei gewonnenen Daten sicherzustellen,
- eine wirksame Kontrolle solcher Eingriffe durch geeignete technisch-organisatorische Maßnahmen zu gewährleisten.

Neben die Ausweitung der Möglichkeit der Überwachung der Telekommunikation treten zunehmend weitere Techniken der heimlichen Datenerhebung (z. B. durch Videoaufnahmen, Abhörgeräte, Richtmikrofone), durch die das Recht auf ungestörte Kommunikation auch außerhalb des Fernmeldebereiches gefährdet ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, daß der Gesetzgeber diesen Gefährdungen des Rechts auf informationelle Selbstbestimmung seine Aufmerksamkeit zuwendet. Sie unterstützt in diesem Zusammenhang die Einwände der Bundesregierung in deren Stellungnahme zum Gesetzentwurf des Bundesrates zur Bekämpfung der organisierten Kriminalität. Die Datenschutzbeauftragten sehen in der Stärkung des Schutzes des Brief-, Post- und Fernmeldegeheimnisses sowie des nichtöffentlich gesprochenen Wortes einen Schwerpunkt ihrer weiteren Arbeit.

Enthaltung: Bayern

Anlage 9 (zu 28)

Entschließung der Sonderkonferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 29. Januar 1991 zum Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten

I.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in der Vergangenheit zu wiederholten Malen die Untätigkeit der Europäischen Gemeinschaft im Bereich des Datenschutzes kritisiert. Kernpunkt dieser Kritik war die Befürchtung, daß die Dynamik der wirtschaftlichen Entwicklung in Richtung auf den vollendeten Binnenmarkt zu einem „informationellen Großraum" mit einem engen Netzwerk grenzüberschreitender Datenflüsse führt, ohne daß gleichzeitig der Grundrechtsschutz in der Gemeinschaft bei der Verarbeitung und dem Austausch persönlicher Daten gewährleistet wird.

II.

Daher begrüßt die Konferenz, daß die EG-Kommission im Juli 1990 den „Vorschlag für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" vorgelegt hat. Der Kommissionsvorschlag geht in einer Reihe von Punkten über die Konvention des Europarats zum Datenschutz von 1980 hinaus und berücksichtigt insoweit die technische und rechtliche Entwicklung des vergangenen Jahrzehnts. Positiv bewertet die Konferenz vor allem die Intention des Entwurfs, den Datenschutz in der EG nicht auf dem kleinsten gemeinsamen Nenner, sondern auf einem möglichst hohen Niveau zu harmonisieren. Sie legt allerdings entscheidenden Wert darauf, daß die Mitgliedstaaten die Möglichkeit behalten, den Datenschutz in der nationalen Gesetzgebung weiterzuentwickeln.

III.

Zahlreiche bewährte Vorschriften und Instrumente aus dem deutschen Datenschutzrecht sind in den Richtlinientext aufgenommen worden. Die Bewertung der einzelnen Bestimmungen des Richtlinienentwurfs kann jedoch nicht isoliert aus dem Blickwinkel des deutschen Datenschutzrechts erfolgen. Jeder nationale Gesetzgeber muß bei Rechtsharmonisierung auf europäischer Ebene bereit sein, einzelne seiner Regelungen auf dem Hintergrund der Erfahrungen und Vorstellungen anderer Mitgliedstaaten in Frage zu stellen. Zur Abstimmung der Auffassungen auf EG-Ebene besteht ein intensiver Meinungsaustausch zwischen der Konferenz und den Datenschutzinstitutionen der Partnerländer.

IV.

Die Konferenz hält, abgesehen von der Bereinigung von redaktionellen Unstimmigkeiten, einige Änderungen im Richtlinienvorschlag für notwendig, um die Gleichwertigkeit des Schutzes auf dem Niveau, das die Mitgliedsländer mit bestehender Datenschutzgesetzgebung bereits erreicht haben, sicherzustellen. Folgende Korrekturen sind dabei vorrangig:

1. Datenschutz muß, jedenfalls im Bereich der öffentlichen Verwaltung, für alle Unterlagen mit personenbezogenen Daten gelten. Die in der Richtlinie vorgesehene Beschränkung des Anwendungsbereichs auf die Verarbeitung personenbezogener Daten in „Dateien" ist ebenso technisch überholt wie Anlaß zu einer Fülle von Interpretationsproblemen.

2. Für die Verwendung und Weitergabe persönlicher Daten muß das Prinzip strikter Zweckbindung gelten und ausdrücklich statuiert werden. Wenn der Entwurf die bloße Vereinbarkeit der Zwecke von Erhebung, Speicherung und Übermittlung genügen läßt, werden inakzeptable Verarbeitungsfreiräume eröffnet; die Transparenz des Datenumgangs geht für den einzelnen verloren.

3. Der Anspruch auf Auskunft über die gespeicherten Daten ist das elementarste Individualrecht der Betroffenen. Nur gravierende Interessen der Allgemeinheit oder Dritter dürfen im Ausnahmefall diesen Auskunftsanspruch einschränken. Der im Entwurf vorgesehene Katalog von Fällen der Auskunftsverweigerung muß daher deutlich vermindert werden.

4. Der Forderung des Entwurfs, daß die Erhebung von Daten nur „nach Treu und Glauben" erfolgen darf, kann uneingeschränkt zugestimmt werden. Doch muß dieses Prinzip im Interesse des einzelnen konkretisiert werden. Es gilt klarzustellen, daß persönliche Angaben vorrangig beim Betroffenen selbst zu erheben sind. Die Ausnahmefälle, in denen Informationen ohne Kenntnis des Betroffenen beschafft werden dürfen, sollten soweit wie möglich in der Richtlinie konkret benannt werden.

5. Der Datenschutz der EG-Bürger darf nicht an den Gemeinschaftsgrenzen haltmachen. Ziel der Richtlinie muß neben der EG-internen Harmonisierung auch sein, den Schutz des Betroffenen beim Datenexport in Drittländer zu gewährleisten. Dies setzt voraus, daß im Empfängerland ein dem EG-Standard gleichwertiges Datenschutzniveau besteht. Daß der Richtlinienentwurf sich mit einem „angemessenen" Schutz im Zielland zufriedengibt, genügt nicht. Notwendig ist schließlich, das Verfahren zur Feststellung des Datenschutzstandards in

Drittländern übersichtlich und praktikabel auszugestalten.

6. Auf der EG-Ebene bedarf es einer unabhängigen Datenschutzinstanz, die alle EG-Organe in Datenschutzfragen berät und für die Überwachung der Einhaltung sowie die einheitliche Anwendung der Richtlinie sorgt. Die im Richtlinienvorschlag vorgesehene „Gruppe für den Schutz personenbezogener Daten" erfüllt — betrachtet man ihre Struktur, Aufgaben und Kompetenzen — diese Anforderungen nicht. Die Unabhängigkeit der Datenschutzkontrolle auf EG-Ebene wird in Zweifel gezogen, wenn den Vorsitz nicht ein gewähltes Mitglied dieser — aus den nationalen Datenschutzorganen zusammengesetzten — „Gruppe", sondern ein Vertreter der EG-Kommission führt. Klargestellt werden muß weiter, daß das Votum der „Gruppe" im vorhinein bei allen den Datenschutz betreffenden Initiativen und Entwürfen der Kommission einzuholen ist. Ansprechpartner der „Gruppe" darf nicht ausschließlich die EG-Kommission, sondern muß auch das Europäische Parlament sein.

7. Da die Kommission die entsprechende Anwendung der Richtlinie auf die personenbezogene Datenverarbeitung ihrer eigenen Dienststellen beschlossen hat, muß sie auch umgehend für eine unabhängige Kontrolle dieses Bereichs Sorge tragen.

V.

Die Konferenz weist darauf hin, daß die vorliegende Richtlinie durch Regelungen für besondere Anwendungsbereiche ergänzt werden muß. Sie sind insbesondere für den Arbeitnehmer- und Sozialdatenschutz vordringlich. Die Kommission sollte schon jetzt ihre Bereitschaft erklären, entsprechende Regelungen zu treffen, und möglichst bald erste Vorschläge vorlegen.

VI.

Die Konferenz begrüßt die Gesprächsbereitschaft der Kommission und geht davon aus, daß der bereits begonnene Dialog zu einer substantiellen Verbesserung des Richtlinienvorschlags führen wird. Die Konferenz wird diese Entschließung der EG-Kommission, dem Europäischen Parlament sowie der Bundesregierung zuleiten. Informiert werden ebenfalls die Datenschutzkontrollinstitutionen der Partnerländer in der Gemeinschaft.

Anlage 10 (zu 8.1.3)

Entschließung der 41. Konferenz der Datenschutzbeauftragten des Bundes und der Länder und der Datenschutzkommission Rheinland-Pfalz vom 8. März 1991 zu Telekommunikation und Datenschutz

I.

Die Telekommunikation hat außerordentlich stark an Bedeutung gewonnen und ersetzt häufig den Brief oder auch das persönliche Gespräch: Über die dreißig Millionen deutschen Telefone werden monatlich rund drei Milliarden Gespräche geführt. Für die Privatsphäre des Bürgers in einer freiheitlichen Gesellschaft ist es unverzichtbar, daß Telefongespräche unkontrolliert und unbeobachtet geführt werden können. Von existentieller Bedeutung wird dies, wenn der Bürger in Notlagen gerät, aus denen er sich nur mit vertraulicher Beratung und Hilfe befreien kann. Daher unterstützen sowohl die Kirchen als auch Hilfs- und Beratungsorganisationen die Forderung, das „Grundrecht auf unbeobachtete Kommunikation" zu sichern.

Dieser Forderung muß die technische Ausgestaltung der Telekommunikationsnetze und -dienste folgen, und die rechtlichen Regelungen müssen diesen sich aus der Verfassung ergebenden Auftrag erfüllen. Der Gesetzgeber hat in dem am 1. Juli 1989 in Kraft getretenen Poststrukturgesetz die Bundesregierung aufgefordert, „Rechtsverordnungen zum Schutz personenbezogener Daten der am Fernmeldeverkehr Beteiligten" zu erlassen. Der Ausschuß für Post und Telekommunikation und der Innenausschuß des Deutschen Bundestages haben mehrfach den Schutz des Fernmeldegeheimnisses angemahnt.

Die vom Bundesminister für Post und Telekommunikation vorgelegten Entwürfe von Verordnungen über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (TDSV) und über den Datenschutz für Unternehmen, die Telekommunikationsdienstleistungen erbringen (UDSV), widersprechen in wesentlichen Punkten dem Grundrecht auf unbeobachtete Kommunikation. Dabei ist besonders unverständlich, daß der Bundesminister von bereits früher gemachten Zusagen an den Deutschen Bundestag wieder abgerückt ist.

Die Entwürfe bleiben in wichtigen Punkten unter dem Datenschutzniveau, das von der EG-Kommission in ihrem Richtlinienentwurf zum Schutz personenbezogener Daten und der Privatsphäre in öffentlichen digitalen Telekommunikationsnetzen für den europäischen Binnenmarkt angestrebt wird.

II.

Ein wesentlicher Mangel besteht in der beabsichtigten Vollerfassung aller Verbindungsdaten von Telefongesprächen: Für jedes Telefonat soll bis zur Versendung der Entgeltrechnung bei der Deutschen Bundespost TELEKOM festgehalten werden dürfen, wer wann wie lange und mit wem telefoniert hat, nach Wahl des Kunden achtzig Tage darüber hinaus. Eine monatliche Auflistung dieser dem Fernmeldegeheimnis unterliegenden Informationen (Einzelentgeltnachweis) sollen Kunden — auch Arbeitgeber — auf Wunsch erhalten können. Außerdem können nach § 12 Fernmeldeanlagengesetz (FAG) auch Gerichte und Staatsanwaltschaften bei strafrechtlichen Ermittlungen jeder Art, also auch bei Bagatelldelikten, ohne besondere Voraussetzungen auf diese Daten zugreifen.

Abzulehnen ist auch die vorgesehene Beschränkung des Kunden auf die Alternative, daß von einem Anschluß die Telefonnummer des Anrufers immer oder nie beim Angerufenen angezeigt wird. Dem Recht auf informationelle Selbstbestimmung entspricht es, daß der Anrufer in jedem Einzelfall entscheiden kann, ob seine Rufnummer beim Angerufenen angezeigt wird. Umgekehrt hat jeder Angerufene selbstverständlich das Recht, nur Gespräche entgegenzunehmen, bei denen die Nummer des Anrufers angezeigt wird.

III.

Die Datenschutzbeauftragten fordern:

1. Alle — durch die computergesteuerte Vermittlungstechnik entstehenden — Verbindungsdaten sind nach dem Ende der Verbindung mit folgender Maßgabe unverzüglich zu löschen:

   In die Entgeltdatenverarbeitung dürfen nur diejenigen Daten eingehen, die zur Berechnung der Entgelte in Summenform unerläßlich sind. Auf Antrag des Kunden darf zur Prüfung der Richtigkeit des in Rechnung gestellten Entgelts oder zur Erstellung des Einzelentgeltnachweises die Rufnummer des Angerufenen nur in einer zumindest um die letzten vier Ziffern verkürzten Form gespeichert werden. Die Daten sind spätestens achtzig Tage nach dem Absenden der Entgeltrechnung zu löschen.

   Die Entscheidung des Kunden über die Form der Abrechnung muß auch bei der Abrechnung zwischen verschiedenen Netzbetreibern respektiert werden.

2. Die Erstellung von „Kommunikationsprofilen", die Aussagen über das persönliche Telefonierverhalten des Bürgers und die Nutzung anderer Telekommunikationsdienste enthalten, muß ausgeschlossen sein.

3. Bei der Anzeige der Rufnummer des Anrufers beim Angerufenen müssen beide die Wahlmöglichkeit

haben, diese Anzeige entweder auf Dauer oder im Einzelfall „auf Knopfdruck" zu unterdrücken.

4. Ausnahmen von diesen Grundsätzen — zum Beispiel zur Aufklärung telefonischer Bedrohungen oder in Notfällen — müssen begründet, ausdrücklich geregelt und für den Betroffenen transparent sein.

5. Die Konferenz bekräftigt ihre Forderung (Beschluß vom 4./5. Oktober 1990), Eingriffe in das grundgesetzlich geschützte Fernmeldegeheimnis (Artikel 10 GG) auf das unerläßliche Maß zu beschränken und insbesondere nicht schon im Bereich der Bagatellkriminalität zuzulassen. Die Regelung des § 12 FAG hat im Zuge der technischen Entwicklung eine verfassungsrechtlich bedenkliche neue Qualität erhalten, da sie nunmehr auch die bei Einsatz neuer Kommunikationstechniken anfallenden Abrechnungs-, Verbindungs-, Nutzungs- und Inhaltsdaten umfaßt. Statt im FAG sollten die Eingriffsmöglichkeiten in das Fernmeldegeheimnis im Rahmen der Strafverfolgung — schon aus Gründen der Normenklarheit — in der Strafprozeßordnung unter engen Voraussetzungen und Beschränkungen abschließend geregelt werden.

Anlage 11 (zu 28)

Beschluß der 12. Internationalen Konferenz der Datenschutzbeauftragten in Paris (19. September 1990) zu Problemen öffentlicher Telekommunikationsnetze und des Kabelfernsehens

(Übersetzung)

Nachdem die XII. Internationale Konferenz der Datenschutzbeauftragten in ihrer Entschließung vom 31. August 1989 allgemeine Grundsätze zu dienste-integrierenden digitalen Netzen (ISDN) aufgestellt hat, begrüßt sie den zweiten Bericht der Arbeitsgruppe „Telekommunikation und Medien", der zeigt, daß diese Grundsätze konkretisiert und auf der technischen Ebene garantiert werden sollten. Diese Grundsätze sind auf jede Form der Telekommunikation einschließlich analoger Formen und bestimmter Formen massenmedialer Kommunikation (insbesondere Kabelfernsehen) anzuwenden. Öffentliche und private Netzbetreiber sollten diese Prinzipien ebenso verwirklichen wie Anbieter von Telekommunikationsdiensten.

I. Teilnehmerverzeichnisse

Verzeichnisse von Teilnehmern an Telekommunikationsdiensten sind inzwischen weltweit die wichtigsten öffentlich verfügbaren personenbezogenen Dateien. Die Konferenz stellt mit Sorge fest, wie schwierig es ist, die Nutzung dieser Daten weltweit zu kontrollieren. Die Risiken nehmen durch den Verkauf der Teilnehmerverzeichnisse auf elektronischen Datenträgern zu.

Personenbezogene Daten, die von Netzbetreibern erhoben und gespeichert werden, müssen dem Zweck entsprechen, dem Betroffenen einen Telekommunikationsdienst zur Verfügung zu stellen und ihm den Zugang zum Netz zu ermöglichen; die Daten müssen für diesen Zweck erheblich sein und dürfen nicht darüber hinausgehen.

Ein Teilnehmerverzeichnis sollte nur solche personenbezogenen Daten enthalten, die unbedingt zur hinreichend sicheren Identifikation bestimmter Teilnehmer erforderlich sind. Die Teilnehmer haben auch das Recht, einen Hinweis auf ihr Geschlecht (und auf ihren Wohnort) *) auszuschließen. Andererseits schließt dies die Veröffentlichung zusätzlicher Daten auf Wunsch des Teilnehmers nicht aus.

Teilnehmer haben das Recht, gebührenfrei und ohne Begründung den Eintrag ihrer Daten in ein Teilnehmerverzeichnis auszuschließen.

Bei der Erhebung von Bestandsdaten sollte der Netzbetreiber den Betroffenen vollständig darüber aufklären, ob er zur Aufnahme seiner Daten in ein Teilnehmerverzeichnis unabhängig von der Form der Veröffentlichung verpflichtet ist oder nicht.

*) bezüglich des Klammerzusatzes bestehen unterschiedliche Auffassungen

Bestandsdaten, die einen Mitbenutzer des Endgerätes betreffen, dürfen nur mit dessen Zustimmung in ein Teilnehmerverzeichnis aufgenommen werden.

Die Weitergabe von Bestandsdaten durch einen Netzbetreiber an Dritte zu Werbezwecken darf nur mit der freiwilligen und informierten Zustimmung des Betroffenen erfolgen, es sei denn, dieser hat nach innerstaatlichem Recht die Möglichkeit, der Weitergabe zu widersprechen.

Bestandsdaten von Teilnehmern, die einen Eintrag in das Teilnehmerverzeichnis ausgeschlossen oder sich entschieden haben, ihren Namen nicht für Werbezwecke nutzen zu lassen, sollten in keinem Fall an Dritte weitergegeben werden.

Besondere Aufmerksamkeit muß der höchsten räumlichen Ebene gewidmet werden, auf der dem Verzeichnis Teilnehmerdaten entnommen werden können.

Die Konferenz betrachtet mit Sorge die wachsenden Gefahren der telefonischen Direktwerbung und wird diese Probleme eingehender untersuchen.

II. Anzeige der vom Anrufer benutzten Rufnummer

Die Einführung einer Einrichtung, die die Anzeige der Nummer des vom Anrufer benutzten Anschlusses am Endgerät des angerufenen Teilnehmers vor der Herstellung der Verbindung ermöglicht, wirft ernste Fragen des Schutzes der Privatsphäre auf.

Es ist wichtig, den Schutz der Privatsphäre des einzelnen Teilnehmers — der anrufenden und der angerufenen Person — mit den Erfordernissen der Kommunikationsfreiheit in Einklang zu bringen. Dies wird durch die Beachtung der folgenden Grundsätze erreicht:

Der Anrufer muß die Möglichkeit haben, durch eine einfache technische Vorrichtung im Einzelfall zu entscheiden, ob er seine Rufnummer anzeigen lassen will oder nicht, auf die Gefahr hin, daß sein Anruf von der angerufenen Person nicht entgegengenommen wird.

Dieses Verfahren zur Unterdrückung der Rufnummernanzeige muß für den Teilnehmer gebührenfrei sein.

Bei der Anwendung dieser Grundsätze sollen die folgenden Maßnahmen getroffen werden:

Teilnehmer müssen das Recht haben, gebührenfrei in das Teilnehmerverzeichnis einen Hinweis darauf aufnehmen zu lassen, daß sie kein Verfahren zur Anzeige der vom Anrufer benutzten Rufnummer anwenden.

Es ist notwendig, die Offenbarung übermittelter Informationen über den Anrufer an Dritte einzuschränken.

Ausnahmsweise darf die Unterdrückung der Rufnummernanzeige entsprechend dem innerstaatlichen Recht außer Kraft gesetzt werden, wenn Personen über Notruf die Feuerwehr oder den Notarzt anrufen.

Der Netzbetreiber kann die Unterdrückung der Rufnummernanzeige auch außer Kraft setzen, um auf Antrag der angerufenen Person den Urheber belästigender Anrufe festzustellen.

Diese Grundsätze sollen bei der Abwicklung internationaler Telefongespräche in gleicher Weise beachtet werden.

III. Mobilfunk

Netzbetreiber, die ein Mobilfunknetz betreiben und anbieten, sollten Teilnehmer über die Sicherheitsrisiken informieren, die normalerweise — insbesondere bei fehlender Verschlüsselung der übermittelten Nachrichten — mit der Benutzung eines Mobilfunknetzes verbunden sind. Der Betreiber sollte dem Teilnehmer vor allem empfehlen, das Mobilfunknetz nicht zur Übermittlung vertraulicher Nachrichten zu benutzen, solange Probleme der Datensicherheit bestehen.

Netzbetreiber sollten verpflichtet sein, den Teilnehmern an Mobilfunknetz wirksame Verschlüsselungsverfahren anzubieten.

Wirksame technische Vorkehrungen sollen getroffen werden, um den unbefugten Netzzugang über mobile Endgeräte zu verhindern.

Die Speicherung von Verbindungsdaten muß strikt auf den kurzen Zeitraum des Verbindungsaufbaus zwischen Teilnehmer und Netz beschränkt werden. Das Tarifsystem soll so gestaltet werden, daß die Orte, an denen Mobiltelefone benutzt worden sind, nicht Teil der Abrechnungsdaten sind. Besondere Beachtung verdient die Frage, inwieweit die Speicherung der vollständigen Rufnummer der angerufenen Person für Abrechnungszwecke notwendig ist.

IV. Gebührenabrechnung

Inwieweit die Speicherung der vollständigen Nummer des angerufenen Teilnehmers für Zwecke der Gebührenabrechnung im allgemeinen erforderlich ist, sollte noch näher untersucht werden.

V. Kabelfernsehen

Die Speicherung individueller Zuschauerprofile durch Kabelfernsehgesellschaften, die einzeln abrufbare („pay per view") Programme anbieten, ist ein Eingriff in die Privatsphäre des Kunden.

Deshalb sollten Kabelfernsehgesellschaften „pay per view"-Programme nur dann anbieten, wenn die Kunden eine praktikable und wirtschaftliche Möglichkeit (z. B. im voraus bezahlte Karten oder Decoder) haben, die Programme zu empfangen, ohne daß zuschauerbezogene Information gespeichert werden.

Messungen der Sehbeteiligung und Tantiemen dürfen nicht auf der Grundlage zuschauerbezogener Daten berechnet werden.

Die Konferenz befürchtet, daß in naher Zukunft im Bereich des Kabelfernsehens zahlreiche Datenschutzprobleme entstehen werden und wird die Entwicklung deshalb eingehend überwachen.

Anlage 12 (zu 25.3)

Hinweise zur Beschaffung und zum Betrieb digitaler TK-Anlagen

1. Personenbezogene Daten

In TK-Anlagen werden im Regelfall zwei Arten personenbezogener Daten gespeichert und verarbeitet:

— *Anschlußdaten*

Für jeden Anschluß (Telefon, Telefax usw.) werden administrative Anschlußdaten gespeichert: Name des Anschlußinhabers, Art der Berechtigung, Kurzwahlziele (d. h., oft gewählte private und dienstliche Telefonnummern), Geheimnummer des elektronischen Telefonschlosses, zuletzt gewählte Verbindung usw. Diese Daten werden überwiegend von einem Systemverwalter — meist Mitarbeiter der Hausverwaltung — am Betriebsterminal eingegeben und ggf. geändert.

— *Verbindungsdaten*

Für jede abgehende Verbindung wird automatisch ein Datensatz gespeichert, der neben der Rufnummer des Anrufers und des Angerufenen, auch Angaben über Zeitpunkt, Dauer und Art der Verbindung (Telefon, Telefax usw.) enthält. Meist enthält die TK-Anlage bereits in der Erstausstattung Programme, die eine vielfache Auswertung dieser Verbindungsdaten gestatten. So können nicht nur etwa monatliche Listen zur Abrechnung der Privatgespräche erzeugt werden, sondern die Verbindungsdaten können auch zur Erstellung von „Hit-Listen" benutzt werden (Wer hat die längsten, teuersten und häufigsten Gespräche geführt? Mit welchem Anschluß wurde am häufigsten telefoniert?). Die möglichen Programme sollten *vollständig* dokumentiert und

nur dann und in dem Umfange gespeichert sein, wie dies *erforderlich* ist (siehe auch 4).

2. Zulässigkeit der Datenverarbeitung

Auch die Verarbeitung personenbezogener Daten in TK-Anlagen unterliegt den Zulässigkeitsvoraussetzungen des Bundesdatenschutzgesetzes und hat dessen Sicherheitsanforderungen zu erfüllen. Darüber hinaus sind jedoch wesentlich die Bestimmungen zu beachten, die insoweit das Verhältnis zwischen Bediensteten und Dienstherrn bzw. Arbeitgeber regeln. Insbesondere sind dies die „Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Bundesverwaltung (Dienstanschlußvorschriften — DAV —)" des Bundesministers der Finanzen sowie die einschlägigen Vereinbarungen zwischen Dienstherrn und Bediensteten, in der Regel in Form von Dienstvereinbarungen. Aus Sicht des Datenschutzes können nur solche Datenerhebungen und -verarbeitungen als erforderlich und somit zulässig angesehen werden, die von diesen Vorschriften *gefordert* werden; weitergehende Erhebungen und Verarbeitungen können nur mit Einwilligung der Betroffenen erfolgen.

3. Dienstanschlußvorschriften

Hier ist darauf zu achten, daß die zur Erfüllung der DAV erforderlichen Leistungsmerkmale der TK-Anlage nicht nur im Prospekt stehen, sondern vom Lieferanten auch vertraglich zugesichert werden. Dies gilt insbesondere für die Möglichkeit, bestimmte Angaben in den Verbindungsdatensätzen zu unterdrükken (z. B. Zeitpunkt des Gespräches, letzte Ziffern der Zielrufnummern usw.), die von den DAV nicht gefordert werden und deren Zulässigkeit sich auch nicht aus einer Dienstvereinbarung ergibt.

4. Mitwirkung der Personalvertretung

Jedenfalls die Verbindungsdaten sind geeignet, für eine Verhaltens- oder Leistungskontrolle der Bediensteten verwendet zu werden. Daher ist bereits vor der Beschaffung einer TK-Anlage der Personalrat über die Einzelheiten der geplanten Verarbeitungen und Nutzungen zu informieren, damit er seine Rechte nach den Bundespersonalvertretungs- oder Betriebsverfassungsgesetz wahrnehmen kann.

5. Dienstliche Verbindungen

Eine Vollspeicherung, d. h. eine Speicherung aller Verbindungsdaten einschl. der vollständigen Rufnummer des Angerufenen *der Dienstgespräche und -verbindungen* ist nur zulässig, wenn diese Daten für eine Kontrolle der durchgeführten Verbindungen im Rahmen einer Fach- oder Dienstaufsicht oder für eine Datenschutzkontrolle benötigt werden. Die Daten dürfen nur für diese Zwecke verwendet und nicht mit anderen automatisierten Personaldateien verknüpft werden. Sie dürfen nur den mit der Kontrolle beauftragten Personen zugänglich gemacht werden und sind nach Abschluß der Kontrolle — spätestens nach einer festzulegenden Frist — zu löschen.

6. Private Verbindungen

Bei *Privatgesprächen und -verbindungen* ist die Verbindungsdatenspeicherung nur in dem Umfange zulässig, in dem sie zur Überprüfung der vom Arbeitgeber oder Dienstherrn erstellten Telefonrechnung durch den Bediensteten erforderlich ist und eine Dienstvereinbarung dies bestimmt. Für die Rufnummer des Angerufenen ist dabei in der Regel die Orts-

netzkennzahl ausreichend. Wenn mehr gespeichert werden soll, muß die Anschlußnummer schon bei der Speicherung soweit gekürzt werden, daß eine Identifizierung des Angerufenen nicht mehr möglich ist, also etwa um die letzten drei Ziffern. Daten über Privatgespräche dürfen nur zum Nachweis der Gespräche für den Betroffenen sowie zur Abrechnung der Gebühren verwendet werden; sie dürfen nur dem Betroffenen (direkt) zur Verfügung gestellt werden. Sie sind zu löschen, sobald die Gebühren ohne Vorbehalt bezahlt worden sind.

7. Datensicherung

Die gespeicherten personenbezogenen Daten — insbesondere die Verbindungsdaten — sind gegen unbefugte Einsichtnahme und Veränderung technisch und organisatorisch zu sichern; das Betriebsterminal darf *nur* dem Systemverwalter zugänglich sein.

Die Berechtigung, Daten einzugeben, zu löschen oder zu verändern, ist auf den Systemverwalter zu begrenzen und durch ein individuelles Paßwort abzusichern; für den Vertretungsfall kann dieses mit versiegeltem Umschlag aufbewahrt werden.

8. Wartung, Fernwartung

(Vgl. 12. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, 24.3)

Fernwartung sollte nur dann zugelassen werden, wenn sichergestellt ist, daß

1. ein Zugriff durch das Fernwartungszentrum auf die TK-Anlage auch im Einzelfall nur unter Mitwirkung des Systemverwalters (z. B. durch Betätigen eines Schalters, Freigabe am Betriebsterminal usw.) möglich ist *und*
2. bei einem solchen Zugriff keine Möglichkeit besteht, personenbezogene Daten der Behörde einzusehen, zu ändern oder zu kopieren. Die Lieferfirma sollte daher die betreffenden Programme schriftlich erläutern und den Nichtzugriff auf personenbezogene Daten vertraglich bestätigen.

Programme, bei denen der Zugriff auf personenbezogene Daten unerläßlich ist, dürfen nur am Betriebsterminal und ebenfalls unter Mitwirkung des Systemverwalters im Einzelfall zu starten sein.

9. Paßwörter

Unbefugte Einsichtnahme und Veränderung der gespeicherten personenbezogenen Daten sind nur zu verhindern, wenn diese in der TK-Anlage „sorgfältig verschlossen" aufbewahrt werden. Dazu müssen ein etwa vorhandener (mechanischer) Schlüssel gesichert aufbewahrt und seine Verwendung geregelt werden. Im allgemeinen sind TK-Anlagen auch durch Paßwörter geschützt, wobei häufig mehrere „User" — z. B. „Betreiber" (= Behörde) und „Wartung" — eingerichtet sind, für die unterschiedliche Paßwörter mit unterschiedlichen Berechtigungen bestehen müssen.

Entsprechende vollständige Erläuterungen sollten stets mitgeliefert werden. Anzahl und Berechtigungsumfang der Paßwörter sollten auf das Unerläßliche beschränkt werden: Im Regelfall reichen hierfür zwei Paßwörter aus, wobei das eine den Betreiber (mit seinen besonderen Zugriffsmöglichkeiten — auch auf personenbezogene Daten), das andere die Wartungsfirma kennzeichnet. Auch letzteres sollte durch die Behörde festgelegt werden, wobei zu beachten ist, daß viele (auch ADV-)Hersteller für ihre Wartungsorganisation ein einheitliches, oft bundesweit geltendes Paßwort festgelegt haben; dies kann nicht toleriert werden.

Anlage 13 (zu 25.4)

Datenschutz bei Telefaxübermittlungen

1. Organisatorische Regelungen

Die Nutzung des Telefaxgerätes bzw. der Telefaxanlage sollte durch Dienstanweisung geregelt werden. Dabei sollten insbesondere die grundsätzlichen Voraussetzungen für eine Nutzung, die erforderlichen Sicherheitsvorkehrungen sowie die Verantwortlichkeiten festgelegt werden.

2. Fernmeldegeheimnis

Nach den Vorschriften des Fernmeldeanlagengesetzes ist „jeder, der eine für den öffentlichen Verkehr bestimmte Fernmeldeanlage betreibt, beaufsichtigt, bedient oder sonst bei ihrem Betrieb tätig ist, zur Wahrung des Fernmeldegeheimnisses verpflichtet." Dies gilt auch z. B. für Bedienstete, die ein eingegangenes Telefax dem Gerät entnehmen, um es dem Empfänger zuzuleiten oder die die Sende-/Empfangsprotokolle (s. 3.) ausdrucken lassen und verwalten. Die Bediensteten sollten auf die Bedeutung des Fernmeldegeheimnisses, insbesondere die Folgen eines Verstoßes hingewiesen werden.

3. Sende-/Empfangsprotokolle

Telefaxgeräte erzeugen automatisch und/oder auf Wunsch Sende-/Empfangsprotokolle, die bezüglich jedes Vorganges u. a. Zeitpunkt der Sendung bzw. des Empfangs und die Anschlußkennung der anderen Station enthalten. Diese Daten unterliegen dem besonderen Schutz des Fernmeldegeheimnisses. Die Sende-/Empfangsprotokolle müssen daher entsprechend sorgfältig behandelt werden: Ein Ausdruck durch Unbefugte sollte verhindert, jedenfalls verboten werden; die Einsichtnahme sollte geregelt, die Protokolle sorgfältig und gesichert aufbewahrt werden.

4. Kenntnisnahme durch Unbefugte

Weil Telefaxsendungen beim erreichten Empfänger offen ankommen, ist bei der Versendung besondere Sorgfalt geboten. Vor der Absendung muß deshalb die Gültigkeit der bekannten Anschlußnummer gewährleistet sein. Dabei ist stets zu berücksichtigen, daß eine Telefaxsendung ebenso wie ein Telefongespräch u. U. von Unbefugten „abgehört" werden kann!

4.1 Anschlußkennung des Empfängers

Durch Falschwahl sowohl beim Absender als auch im Übertragungsnetz der Deutschen Bundespost kann es dazu kommen, daß ein anderer als der gewünschte Anschluß erreicht wird. Zudem kann sich, da freigewordene Anschlußnummern durch die Post sofort wieder neu vergeben werden, hinter einer bekannten und auch richtig angewählten Anschlußnummer unerwartet ein anderer Partner verbergen. Bei jeder Sendung ist deshalb zu überprüfen, ob auch tatsächlich der richtige Anschluß/Partner erreicht wird: Nahezu jedes Gerät sendet — wenn es von einem anderen Gerät aus angewählt wird — die eigene Anschlußkennung an dieses zurück. Sie besteht aus einem numerischen Teil, z. B. „49 228 1899550" und im allgemeinen einem Textteil, z. B. „Bundesdatenschutz, Bonn 2". Bei Absendung eines Telefax sollte daher stets die Rücksendung der Kennung des angewählten Gerätes abgewartet und diese überprüft werden. Bei fehlender Übereinstimmung sollte im Zweifelsfall die Sendung sofort abgebrochen werden.

4.2 Zeitversetzte Sendungen

Bei Sendungen ins Ausland ist die Ortszeit zu überprüfen. Es ist je nach Art des Inhalts sicherzustellen, daß ein Telefax dort nicht außerhalb der Dienstzeit ankommt und somit durch Unbefugte Einsicht genommen werden könnte. Dieser Gesichtspunkt ist auch im Inland dann zu beachten, wenn ein Telefax nicht sofort abgesandt, sondern von der Möglichkeit der *zeitversetzten* Sendung Gebrauch gemacht wird.

4.3 Anrufumleitung, -weiterschaltung

Für Telefaxgeräte, die in Kommunikationsanlagen (Telefonanlagen) eingesetzt sind, kann — soweit vorhanden — die Möglichkeit der Anrufumleitung und -weiterschaltung genutzt werden. Dies kann dazu führen, daß eine Sendung bei einem (anderen als dem angewählten) Empfangsgerät ankommt, das in einem fachlich unzuständigen Bereich aufgestellt ist. Dadurch könnte es zu einer datenschutzrechtlich unzulässigen Übermittlung kommen. Dieses Risiko kann nur durch Überprüfung der rückgesendeten Kennung ausgeschlossen werden (s. oben 4.1).

4.4 Besonders schutzbedürftige Daten

Wegen der bestehenden Risiken sollten besonders schutzbedürftige Daten, insbesondere solche, die sich auf

- strafbare Handlungen,
- Ordnungswidrigkeiten,
- religiöse oder politische Anschauungen sowie
- bei Übermittlung durch den Arbeitgeber auf arbeitsrechtliche Rechtsverhältnisse

beziehen, nur dann per Telefax übermittelt werden, wenn dies von der Eilbedürftigkeit her geboten und durch besondere Vorkehrungen sichergestellt ist, daß die Sendung (nur) dem Richtigen zugeht. Neben der Beachtung dieser Hinweise ist es geboten, unmittelbar vor der Sendung eine telefonische Vereinbarung möglichst auch über persönliche Entgegennahme der Sendung zu treffen.

5. Dokumentation, Vollständigkeit

Jeder Sendung sollte ein Vorblatt vorangefügt werden, welches Absender, dessen Telefax- und Telefonnummer (für Rückrufe) sowie die Gesamtanzahl der gesendeten Seiten ausweist. Es sollte möglichst für jede einzelne Sendung ein Sendeprotokoll erzeugt und dies dem Vorgang beigefügt werden. Soweit das Gerät eine gesendete Seite durch einen Verifikationsstempel als solche kennzeichnet, sollte die Funktionsfähigkeit dieser Vorrichtung sichergestellt sein.

6. Erhalt der Verfügbarkeiten

Bei Ausfall der Netzstromversorgung können die Speicherinhalte des Gerätes (teilweise) gelöscht werden. Dadurch können — sofern vorhanden — Seitenspeicher (für Gruppensendungen usw.) oder Ziel- und Gruppenwahlnummern gelöscht oder unrichtig werden. Dies ist von Zeit zu Zeit, bei bekanntgewordenem Netzausfall in jedem Fall, zu überprüfen.

7. Räumliche Unterbringung

Telefaxgeräte sollten in solchen Räumen untergebracht werden, die nicht nur ausreichend gesichert sind, sondern für die sichergestellt ist, daß eine Telefaxsendung nicht unbeobachtet ankommt und von Unbefugten entnommen oder eingesehen werden kann.

Anlage

Datenschutz bei Telefax

1. Sie tragen die Verantwortung für die durch Sie übermittelten personenbezogenen Daten; prüfen Sie daher genau deren Sensibilität.
2. Beachten Sie die für Ihre Behörde/Dienststelle geltenden Anweisungen für die Nutzung des Telefax-Dienstes.
3. Nutzen Sie *nach Möglichkeit* alle der Sicherheit dienenden Einrichtungen des Gerätes, insbesondere die Anzeige des erreichten Gerätes (s. Nummer 4)!
4. Vergewissern Sie sich vor einer Sendung, ob der Adressat noch unter der Ihnen bekannten Anschlußnummer erreichbar ist.
5. Verständigen Sie sich vor der Absendung besonders sensibler Daten mit dem Adressaten über den konkreten Zeitpunkt der Übermittlung!
6. Gewährleisten Sie — möglichst durch persönliche Anwesenheit am Gerät — während der Übertragung von Dokumenten mit personenbezogenen Daten, daß kein Unbefugter in diese Einsicht nehmen kann.
7. Verständigen Sie sich nach Empfang einer Sendung mit Ihrem Partner über aufgetretene Mängel und ggf. deren Behebung.
8. Erleichtern Sie sich und Ihren Partnern die Nachweisführung:
   - Vorblatt der Behörde/Dienststelle benutzen,
   - Aussagekräftiges „Logo" vorprogrammieren,
   - Blattnumerierung der Kopien,
   - Originale mit Verifikationsstempel versehen,
   - Journalfunktion nutzen.
9. Faxübertragungen sind „abhörbar": Was am Telefon nicht gesagt werden darf, darf auch nicht gefaxt werden!
10. Beachten Sie bei der Nutzung von Fernkopierern auf PC-Basis neben den erweiterten Möglichkeiten auch die damit verbundenen Risiken; verständigen Sie sich darüber mit Ihrem Datenschutzbeauftragten.

Sachregister

Abkürzungsverzeichnis

2. BMeldDÜV	Zweite Meldedaten-Übermittlungsverordnung des Bundes
AA	Auswärtiges Amt
ADOS	Adressen und Objekte Ost
AFG	Arbeitsförderungsgesetz
AFWoG	Gesetz über den Abbau der Fehlsubventionierung im Wohnungswesen
AIDS	Acquired Immune Deficiency Syndrome
AO	Abgabenordnung
APC	Arbeitsplatzcomputer
APIS	Arbeitsdatei PIOS innere Sicherheit
AT	Advanced Technology
AuslG	Ausländergesetz
AWV	Arbeitsgemeinschaft für wirtschaftliche Verwaltung
AZR	Ausländerzentralregister
AZRG	Gesetz über das Ausländerzentralregister
BA	Bundesanstalt für Arbeit
BAG	Bundesarbeitsgericht
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl	Bundesgesetzblatt
BGSG	Bundesgrenzschutzgesetz
BKA	Bundeskriminalamt
BKA-AN	BKA-Aktennachweisdatei
BKK	Betriebskrankenkasse
BMA	Bundesminister für Arbeit und Sozialordnung
BMBau	Bundesminister für Raumodnung, Bauwesen und Städtebau
BMF	Bundesminister der Finanzen
BMI	Bundesminister des Innern
BMJ	Bundesminister der Justiz
BML	Bundesminister für Ernährung, Landwirtschaft und Forsten
BMP	Bundesminister für das Post- und Fernmeldewesen
BMPT	Bundesminister für Post und Telekommunikation
BMU	Bundesminister für Umwelt, Naturschutz und Reaktorsicherheit
BMV	Bundesminister für Verkehr
BMVg	Bundesminister der Verteidigung
BMWi	Bundesminister für Wirtschaft
BND	Bundesnachrichtendienst
BPersVG	Bundespersonalvertretungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStatG	Bundesstatistikgesetz
BT-Drs.	Bundestags-Drucksache
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerwG	Bundesverwaltungsgesetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
CAD	Computer Aided Design
coArb	computerunterstützte Arbeitsverwaltung
CP/M	Control Program for Microcomputer
DAV	Dienstanschlußvorschriften
DB	Deutsche Bundesbahn
DBP	Deutsche Bundespost
DDR	Deutsche Demokratische Republik

DDR StG	Strafgesetzbuch der DDR
DEVO/DÜVO	Datenerfassungsverordnung/Datenübermittlungsverordnung
DV/dv	Datenverarbeitung
DVAT	Datenverschlüsselung auf AT-Rechner
DORA	Dialogorientiertes Auswertungs- und Rechnersystem
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EMD-Technik	Edelmetall-Motor-Drehwähler-Technik (der DBP)
ETSI	European Telekommunikations Standards Institute
GBl.DDR	Gesetzblatt der DDR
GG	Grundgesetz
GLKA	Gemeinsames Landeskriminalamt der fünf neuen Bundesländer
GMBl	Gemeinsames Ministerialblatt
GMD	Gesellschaft für Mathematik und Datenverarbeitung
GRG	Gesundheits-Reformgesetz
IAO	Internationale Arbeitsorganisation
INPOL	Informationssystem der Polizei
ISDN	Integrated Services Digital Network
IT	Informationstechnik
ITG	Informationstechnische Gesellschaft
JUSTIS	Justiz-Informationssystem
KAN	Kriminalaktennachweis
KBA	Kraftfahrt-Bundesamt
KBytes	Kilobytes = 1024 Bit
KG	Kindergeld
KJHG	Kinder- und Jugendhilfegesetz
KOBRA	Kontrolle bei den Ausfuhren
LVA	Landesversicherungsanstalt
MAD	Militärischer Abschirmdienst
MfS	Ministerium für Staatssicherheit/Amt für nationale Sicherheit
MoU	Memorandum of Understanding, Vermerk über Übereinstimmung
MRRG	Melderechtsrahmengesetz
MS-DOS	Microsoft Disc Operating System
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenzeitschrift
NVA	Nationale Volksarmee
NTT, KDD, AT&T	Telefongesellschaften
ODIN	Organisationsdienst für nachgehende Untersuchungen
ÖPDV	örtliche Personaldatenverarbeitung
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität
PARLAKOM	Parlamentskommunikationssystem
PC	Personalcomputer
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PIN	persönliche Identifikationsnummer
PK	Personenkennziffer
PKZ	Personenkennzahl
RAM	Random Access Memory
RDV	Recht der Datenverarbeitung (Zeitschrift)
RVO	Reichsversicherungsordnung
SAP	Sozialamt der Deutschen Bundespost
SED	Sozialistische Einheitspartei Deutschlands
SGB I	Sozialgesetzbuch Erstes Buch
SGB IV	Sozialgesetzbuch Viertes Buch
SGB V	Sozialgesetzbuch Fünftes Buch (Gesundheitsreformgesetz)
SGB VI	Sozialgesetzbuch Sechstes Buch (Rentenversicherung)
SGB X	Sozialgesetzbuch Zehntes Buch
SIM	Subscriber Identity Module

SPUDOK	Spurendokumentationssystem
Stasi	Staatssicherheitsdienst
StGB	Strafgesetzbuch
StPO	Strafprozeßordnung
StVG	Straßenverkehrsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
TB	Tätigkeitsbericht *)
Telefax	Telefon Faksimile (telephonisch übertragene Fernkopie)
TEMEX	Telemetry Exchange
THA	Treuhandanstalt
TKO	Telekommunikationsordnung
UVV	Unfallverhütungsvorschriften
VSA	Verschlußsachenanweisung
VZG	Volkszählungsgesetz
VZR	Verkehrszentralregister
WEWIS	Wehrersatzwesen-Informationssystem
XT	Extended Technology
ZER	Zentrales Einwohnerregister
ZEVIS	Zentrales Verkehrsinformationssystem
ZKI	Zollkriminalinstitut
ZKA	Zentrales Kriminalamt
ZPO	Zivilprozeßordnung
ZSKI	Zentralstelle für Kriminalistische Informationsverarbeitung

*) Erster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/2460
Zweiter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 8/3570
Dritter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/93
Vierter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/1243
Fünfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 9/2386
Sechster Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/877
Siebenter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/2777
Achter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/4690
Neunter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 10/6816
Zehnter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/1693
Elfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/3932
Zwölfter Tätigkeitsbericht ist erschienen als Bundestags-Drucksache Nr. 11/6458