Deutscher Bundestag
13. Wahlperiode

Drucksache 13/1150

18. 04. 95

Sachgebiet 204

Unterrichtung

durch den Bundesbeauftragten für den Datenschutz

Tätigkeitsbericht 1993 und 1994 des Bundesbeauftragten für den Datenschutz – 15. Tätigkeitsbericht – gemäß § 26 Abs. 1 des Bundesdatenschutzgesetzes

Gliederung

Zugeleitet mit Schreiben des Bundesbeauftragten für den Datenschutz vom 13. April 1995 – L – 111/17 – gemäß § 19 Abs. 2 des Bundesdatenschutzgesetzes.

Seite

Abbildungsverzeichnis

1 Einführung

1.1 Datenschutz auf dem Prüfstand

Datenautobahn und Multimedia sind Stichworte, die auf bahnbrechende Technikinnovationen in der nahen Zukunft hinweisen. Fachleute sprechen von einer neuen Phase des „Informationszeitalters". Auch die Medien befassen sich bereits intensiv mit den Neuerungen.

Unter den Bürgerinnen und Bürgern besteht offenbar noch große Unkenntnis über diese neue Entwicklung und damit auch Nachholbedarf, sie darauf vorzubereiten. Nach einer aktuellen Umfrage der Europäischen Kommission ist beinahe nur jede dritte der befragten Personen in Deutschland mit den Begriffen „Informationsgesellschaft" oder „Datenautobahn" vertraut. Mehr als die Hälfte sieht das Privatleben durch die neuen Technologien gefährdet. Auf die Frage schließlich, ob „neue Informations- und Kommunikationstechnologien mehr individuelle Freiheit mit sich bringen", werden die Deutschen nur noch von einem anderen EU-Mitgliedsland an Skepsis übertroffen.

Durch diese Umwälzungen sind neue, besondere Auswirkungen auch beim Persönlichkeitsrecht der Bürgerinnen und Bürger zu erwarten. In einer völlig neuen Dimension werden z. B. Unternehmen Kundendaten sammeln und zu Kundenprofilen verarbeiten. Die Konzeption des Datenschutzes steht damit auf dem Prüfstand. Mit den Technikerneuerungen stellen sich an den Datenschutz umfassende Fragen, die einer Antwort bedürfen. Außer Frage für mich steht, daß sich der Datenschutz nicht gegen diese Entwicklungen stellen darf und die neue Kommunikationstechnik schneller kommen wird, als von manchen erwartet. Um so intensiver und energischer muß daher die Diskussion in Staat, Wirtschaft und Gesellschaft geführt werden, welche Konsequenzen und Perspektiven für den Datenschutz damit verbunden sind.

1.2 Anlaß für eine Bestandsaufnahme

Anlaß für eine Bestandsaufnahme des Datenschutzes und seiner Entwicklungen bestand im Berichtszeitraum nach 10 Jahren des sog. Volkszählungsurteils vom 15. Dezember 1983 des Bundesverfassungsgerichts. Damit hat das Bundesverfassungsgericht ein für das Persönlichkeitsrecht wegweisendes Urteil gesprochen. Es war entscheidend für die Entwicklung des Datenschutzes in Deutschland. Mit dem Urteil hat das Bundesverfassungsgericht den Datenschutz als „Recht auf informationale Selbstbestimmung", d. h. als informationsspezifisches Grundrecht interpretiert. Damit trägt es den in allen gesellschaftlichen Bereichen zu beobachtenden Entwicklungen Rechnung, die mit dem Stichwort „Informationsgesellschaft" gekennzeichnet werden. Das Urteil hat klargestellt, daß grundsätzlich jeder Bürger selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen hat. Nur im überwiegenden Allgemeininteresse sind Einschränkungen dieses Rechts zulässig. Sie bedürfen einer verfassungsgemäßen gesetzlichen Grundlage. In den vergangenen 10 Jahren hat der Gesetzgeber – diesen verfassungsrechtlichen Vorgaben folgend – nicht nur die Datenschutzgesetze in Bund und Ländern verbessert und erweitert, sondern auch zahlreiche Spezialbestimmungen auf teilweise hohem Datenschutzniveau geschaffen. Auf einigen Gebieten stehen allerdings datenschutzrechtliche Vorschriften noch aus, die die Befugnisse der Behörden, Gerichte und Wirtschaftsunternehmen einerseits und die Rechte des Einzelnen deutlich gegeneinander abgrenzen. In Deutschland wurde seit dem Volkszählungsurteil relativ viel erreicht. Studien belegen, daß der Datenschutz ein hohes Maß an Akzeptanz gewonnen hat und für die meisten zur Normalität geworden ist. Eine Gesamtbilanz des Datenschutzes kann daher insgesamt und grundsätzlich als erfreulich bezeichnet werden.

Vor 17 Jahren wurde das Amt des Bundesbeauftragten für den Datenschutz eingerichtet. Für mich als Bundesbeauftragten ist dieser 15. Tätigkeitsbericht zugleich der erste, den ich dem Deutschen Bundestag und der Öffentlichkeit vorlege. Ich danke meinen Vorgängern und allen meinen Mitarbeitern, daß sie nach aufreibender Pionierarbeit die Belange des Datenschutzes beharrlich vertreten haben und für das Persönlichkeitsrecht unserer Bürgerinnen und Bürger erfolgreich eingetreten sind. Die feste Verankerung des Datenschutzes in unserem rechtsstaatlichen System bestätigt auch die jährliche IPOS-Umfrage zu aktuellen Fragen der Innenpolitik, nach der der Bundesbeauftragte für den Datenschutz zu den wichtigsten Einrichtungen des Bundes gezählt wird. Seine Einrichtung steht längst nicht mehr in Frage. Auch die etwa 3 000 Anfragen und Eingaben von Bürgern pro Jahr beim Bundesbeauftragten bestätigen den hohen Stellenwert und das hohe Interesse am Datenschutz. Sorge bereitet mir allerdings, wenn Bürger ihren Namen aus Angst vor Nachteilen z. B. in der Krankenversicherung zur Weiterverwendung nicht angeben wollen. Ob zu Recht oder nicht – diese Fälle zeigen, daß das Vertrauen in den freiheitlich, demokratischen Rechtsstaat weiter gestärkt werden muß.

1.3 Eine gute Gelegenheit versäumt

Wenn auch die verfassungsrechtliche Dimension des Datenschutzes heute unbestritten ist, hätte ich es dennoch für einen besonderen Gewinn gehalten, wenn das Recht auf informationelle Selbstbestimmung ausdrücklich in das Grundgesetz aufgenommen worden wäre. Gegenüber den Bürgerinnen und Bürgern wäre damit auch in der Verfassung zum Ausdruck gebracht worden, daß ihr Recht auf informationelle Selbstbestimmung in gleicher Weise wie die traditionellen Grundrechte garantiert ist. Zu meinem Bedauern hat der entsprechende mehrheitliche Wunsch in der gemeinsamen Verfassungskommission, den Datenschutz in das Grundgesetz aufzunehmen, nur deshalb nicht die notwendige Zweidrittelmehrheit gefunden, weil dies angesichts der klaren und unangefochtenen Rechtsprechung des Bundesverfassungsgerichts und der auch insoweit festen Verankerung des Datenschutzes in der Verfassungswirklichkeit als nicht unabdingbar angesehen wur-

de. Die Verfassungsgeber der neuen Länder waren insoweit aufgeschlossener und haben, wenn auch mit unterschiedlichen Formulierungen und unterschiedlichem Regelungsumfang, die Problematik des Umgangs mit der modernen Informationstechnik unter dem Gesichtspunkt der Selbstbestimmung angesprochen. Sie sind damit den Verfassungen einer Reihe europäischer Staaten gefolgt. Für das Grundgesetz wurde allerdings eine gute Gelegenheit für eine zeitgemäße Erweiterung des Grundrechtskatalogs versäumt (siehe auch Nr. 31.1).

1.4 Harmonisierter Datenschutz in Europa auf gutem Wege

Der Europäische Binnenmarkt und die Weiterentwicklung der Europäischen Union sind ohne einen europäischen Datenschutz undenkbar. Die Freizügigkeit von Personen und Dienstleistungen sowie der ungeheuren Waren- und Kapitalströme im europäischen Wirtschaftsraum wird in immer höherem Maße von umfassenden personenbezogenen Datenflüssen begleitet. Der Binnenmarkt entwickelt sich damit mehr und mehr auch zu einer Informations- und Datengemeinschaft, Europa verwandelt sich mithin in einen informationellen Großraum. Wir teilen daher mit unseren europäischen Nachbarn die Überzeugung, daß wir den Datenschutz in Europa harmonisieren müssen. Während der deutschen EU-Präsidentschaft habe ich als Vorsitzender der Ratsgruppe „Wirtschaftsfragen/Datenschutz" die schwierigen Verhandlungen über die EG-Datenschutzrichtlinie fortgeführt. Trotz größter Meinungsunterschiede wurde am Ende ein gemeinsamer Kompromiß gefunden. Mich erfüllt daher besondere Freude, daß der Rat für Wirtschafts- und Finanzfragen am 20. Februar 1995 den Gemeinsamen Standpunkt zur Richtlinie verabschiedet hat. Damit wurde ein wichtiger Meilenstein auf dem Wege eines europäischen Datenschutzes auf hohem Niveau erreicht. Nach Öffnung der innereuropäischen Grenzen ist ein europäischer Datenschutz in harmonisierter, rechtsangeglichener Form dringender denn je, um den erforderlichen und gewünschten freien Datenverkehr zu ermöglichen, um Wettbewerbsverzerrungen innerhalb der Gemeinschaft zu vermeiden und das bestehende unterschiedliche Datenschutzniveau in den einzelnen Mitgliedsstaaten aufzuheben. Hierzu trägt die Richtlinie in entscheidender Weise bei. Für die Bürgerinnen und Bürger Europas werden hierdurch u. a. umfassende Auskunfts- und Informationsrechte geschaffen. Die Richtlinie wurde inzwischen dem Europäischen Parlament zur 2. Lesung übermittelt. Stimmt das Parlament zu, stehen dem Inkrafttreten der Richtlinie keine Hindernisse mehr im Wege. Zwar gibt die Richtlinie nur einen Kompromiß wieder. Er ist jedoch nicht vermeidbar, weil in Europa nicht nur viele Nationen, sondern auch unterschiedliche Rechtskreise ihre Anerkennung und Identifikation finden wollen. Im deutschen Recht wird es nach Inkrafttreten der Richtlinie keinen grundlegenden Wandel geben. Den Anwendern wird damit eine flächendeckende kostenintensive Umstellung erspart bleiben. Insoweit kommt das anerkannt hohe Datenschutzniveau in Deutschland allen Beteiligten zugute. Als wesentlich ist hervorzuheben, daß die Richtlinie einen hochentwickelten nationalen Datenschutzstandard unberührt läßt und eine Weiterentwicklung des Datenschutzes in den Mitgliedsländern ermöglicht. Damit können Mitgliedsstaaten mit besonders strengen Schutzvorschriften diese beibehalten und sich auch künftig als Notar für weitere Verbesserungen befähigen. Besondere Regelungen wurden auch für den Arbeitnehmer- und Sozialdatenschutz getroffen; entsprechende Daten dürfen grundsätzlich nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden.

Ich fordere alle Beteiligten im weiteren europäischen Gesetzgebungsverfahren auf, im Interesse der europäischen Bürgerinnen und Bürger weiter zielstrebig daran zu arbeiten, daß die Richtlinie baldmöglichst in Kraft tritt (siehe auch Nr. 33.1).

1.5 Kontroll- und Überwachungsinstrumentarien – Datenabgleiche und ihre Grenzen

Ein zentrales Thema für den Datenschutz ist die seit den letzten Jahren feststellbare Zunahme der Kontroll- und Überwachungsverfahren. Allein im Bereich der Sozialleistungen wurden mehr als ein Dutzend solcher Kontrollverfahren eingeführt. Ziel dieser verstärkten Kontrollen ist, Leistungsmißbrauch aufzudecken und darüber hinaus illegale Beschäftigung einzudämmen. Diese Ziele und ihre Erreichung sind grundsätzlich legitim und unterstützenswert. Andererseits ist zu befürchten, daß immer mehr pauschalierte Datenübermittlungen und Datenabgleiche zwischen den Leistungträgern den Beitragszahler und Leistungsbezieher zum bloßen Objekt der Datensysteme machen. Wie sensibel die Betroffenen hierauf reagieren, hat auch die öffentliche Diskussion um die Nachforderungen von Krankenkassenbeiträgen im Rentenverfahren Ende 1994 gezeigt.

Die Einführung entsprechender Verfahren kann daher nur an enge restriktive Voraussetzungen geknüpft sein. Im einzelnen muß insbesondere dargelegt werden, daß die Datenabgleiche zur Zielerreichung unabdingbar erforderlich sind und keine, das Persönlichkeitsrecht weniger beeinträchtigende Lösungen möglich sind. Im Mittelpunkt der öffentlichen Diskussion stehen naturgemäß stärker die Forderungen nach Bekämpfung des Leistungsmißbrauchs. Ich würde es begrüßen, wenn in dieser Diskussion mindestens ebenso intensiv der Grundsatz der Verhältnismäßigkeit diskutiert würde. Die zulässige Grenze dieser Verfahren liegt in jedem Falle beim Übermaßverbot. Dabei ist auch zu berücksichtigen, daß es eine immer wieder feststellbare Eigenart der Verwaltungen ist, mehr Daten über den Betroffenen zu sammeln, als für die Aufgabenwahrnehmung erforderlich ist.

Noch bevor sich die Tendenz zur weiteren Kontrolle und Überwachung fortsetzen wird, wofür es Anzeichen gibt, ist es aus meiner Sicht an der Zeit, die eingeführten Datenabgleichsverfahren in ihrer praktischen Bedeutung und Auswirkung auf den Verhältnismäßigkeits- und Erforderlichkeitsgrundsatz zu überprüfen. Nicht nur die Erfolge in der Mißbrauchsbekämpfung dürfen die ihnen zukommende gewich-

tige Rolle spielen; ein ebenso starkes Gewicht muß das Persönlichkeitsrecht der Betroffenen erhalten. Aus meiner Sicht muß dies auch schon in der öffentlichen Diskussion zum Ausdruck kommen.

Ein wesentlicher datenschutzrechtlicher Mangel der pauschalierten Datenübermittlungen und Datenabgleiche besteht darin, daß bei nahezu keinem Verfahren bislang eine ausdrückliche Unterrichtung der Betroffenen erfolgt. Dies wird zumeist damit begründet, daß es zum ureigenen Aufgabenbereich des Sozialleistungsträgers gehöre, Leistungsmißbrauch durch Kontrollen aufzudecken und zu verhindern. Jeder Betroffene müßte daher mit solchen Kontrollen auch im Wege des Datenabgleiches rechnen. In dieser allgemeinen Form kann ich dieser Ansicht nicht folgen. Sie wird dem Recht des Einzelnen auf informationelle Selbstbestimmung nicht gerecht. Es sollte vielmehr – auch aus Gründen der Prävention – sichergestellt werden, daß durch geeignete Verfahren die Informationsrechte der Beitragszahler und Leistungsempfänger gewahrt werden. Auch würden Akzeptanz und Vertrauen in den Staat hierdurch steigen. Der größte Teil der Kritik in der genannten Rentendiskussion Ende 1994 wäre hierdurch erspart geblieben.

1.6 Chipkarten – viele Probleme noch ungelöst

In der heutigen Gesellschaft herrscht ein Informationsfluß wie noch nie zuvor. Längst wird die elektronische Form der Information der herkömmlichen vorgezogen. Die schnelle Verfügbarkeit und Verarbeitbarkeit der Informationen sind die Gründe hierfür. In diesem Wettstreit führt besonders die Chipkarte den Siegeszug an. Dabei verfügen lediglich die sog. intelligenten Speicherkarten über bestimmte Sicherheitsfunktionen (z. B. Pin- oder Echtheitsprüfung). Diese Sicherheitsmechanismen werden zwar ständig erweitert, der entscheidende Durchbruch ist bislang allerdings ausgeblieben. Trotz erheblicher Verbesserungen der Sicherheitsmechanismen sind einige Probleme immer noch ungelöst:

- Beispiel: das „Pin-Problem"
  Mit der starken Zunahme der Karten in naher Zukunft wird sich kaum noch jemand die vielen verschiedenen Pins der vielen Karten für die verschiedenen Bereiche merken können. Dies wird spürbaren Einfluß auf die Sicherheit der Kartenbenutzung haben. Das Problem kann wohl nur durch die Verwendung biometrischer Merkmale (z. B. Fingerabdruck) gelöst werden, wird dann aber noch datenschutzrechtlich vertieft zu diskutieren sein.

Wenn es nicht gelingt, die Datenschutzprobleme zu lösen, die mit der Verbreitung der Chipkarten verbunden sind, werden gravierende Probleme für das Persönlichkeitsrecht der Nutzer auftreten. Hierzu müssen sowohl die zur Sicherheit einer Karte notwendigen technischen und organisatorischen Maßnahmen als auch die rechtlichen Rahmenbedingungen geschaffen werden. Die Diskussionen über die künftige Verarbeitung von Gesundheitsdaten und den Schutz der Patienten vor einer Bloßstellung sind seit Einführung der Krankenversicherungskarte sprunghaft angestiegen. Dabei hat sich gezeigt, daß es durchaus sachgerecht war, die Datenspeicherung auf der Krankenversicherungskarte und ihre Nutzung gesetzlich eng zu begrenzen (siehe auch Nr. 12.4). Bis jetzt sind zu viele Fragen offen, als daß man den Einsatz von Chipkarten als Träger von Gesundheitsinformationen über seinen Inhaber generell empfehlen könnte. Bei der Lösung der Probleme ist Eile geboten. Denn die Technik dazu ist nicht nur im Prinzip verfügbar, sondern mit vielen Millionen von Karten und Tausenden von Lesegeräten in den Arztpraxen bereits eingeführt. Zugleich werden von Verbänden und Unternehmen Versuche mit Gesundheitsdatenkarten geplant oder schon durchgeführt.

Zu den offenen Problemen gehört z. B. daß die Gesundheitsdaten auf einer Karte im Besitz des Inhabers nicht der ärztlichen Schweigepflicht unterliegen. Einige Probleme lassen sich sicherlich technisch und organisatorisch lösen, für andere muß der Gesetzgeber die richtigen Rahmenbedingungen vorgeben. Hierfür fordere ich, daß im Zuge der bei Ärzten, Apothekern und Krankenkassen geführten Feldversuchen mit allgemeinen Gesundheitsdaten nicht nur technische und wirtschaftliche Gewinne im Vordergrund stehen, sondern auch die ethischen und datenschutzrechtlichen Fragen gleiches Gewicht erhalten (siehe auch Nrn. 17.3 und 30.1).

1.7 Sicherheitsbereich: Vor dem Ruf nach neuen Gesetzen erst vorhandene Gesetze auf Wirksamkeit überprüfen

Im Spannungsfeld von Sicherheitsaufgaben und Datenschutz wird die Diskussion nicht selten von emotionalen Äußerungen belastet. Undifferenzierte Vorwürfe, wie z. B. Datenschutz behindere die Kriminalitätsbekämpfung, können dabei zunächst den Blick für Fragen des Datenschutzes verstellen. Bisher jedoch habe ich in keinem Fall davon erfahren, daß eine konkrete datenschutzrechtliche Regelung sich aufgrund der gewonnenen Erfahrungen als wirkliches Hindernis für eine effektive Strafverfolgung erwiesen hat. In diesem Zusammenhang kann die Fragestellung nicht lauten, ob Sicherheit vor Datenschutz oder Datenschutz vor Sicherheit geht. Die Bürgerinnen und Bürger haben sowohl ein Recht darauf, daß sie sich vor Verbrechen sicher fühlen können als auch darauf, daß ihr Recht auf Privatsphäre nicht beeinträchtigt wird. Beide Belange müssen aus Sicht des Bürgers miteinander im Einklang stehen. Der Bundesbeauftragte für den Datenschutz ist jederzeit zu Gesprächen und auch zur Mitverantwortung bereit, wenn es darum gehen sollte, datenschutzrechtliche Schranken für ein Tätigwerden der Strafverfolgungsbehörden bei der Kriminalitätsbekämpfung zu erörtern und – wenn möglich – zu beheben.

Nach langen politischen Kontroversen während der parlamentarischen Beratungen und nach Einschaltung des Vermittlungsausschusses ist am 1. Dezember 1994 das Verbrechensbekämpfungsgesetz in Kraft getreten. Sogleich wurde gefordert, in der neuen Legislaturperiode ein „Verbrechensbekämpfungsgesetz II" zu schaffen. Hierbei wurde die Forderung laut, auch das Abhören mutmaßlicher Gangsterwohnungen müsse ermöglicht werden.

Wiederholt habe ich hierzu Stellung genommen. Ich habe nie Bedenken dagegen geäußert, in einem eng begrenzten Bereich auch ein Eindringen in den Schutzbereich der Wohnung zuzulassen, wenn damit das Ziel verfolgt wird, erhebliche Gefahren für die Existenz und die Menschenwürde anderer abzuwehren. Bei aller Bedeutung, die der Durchsetzung des staatlichen Strafanspruchs zukommt, halte ich jedoch einen Eingriff in das durch die Menschenwürde geschützte private Refugium eines Menschen allein für den Zweck der Strafverfolgung mit dem Menschenbild des Grundgesetzes nicht für vereinbar. Dies sage ich auch aufgrund der bisherigen Erfahrungen mit der Telefonüberwachung. Der Lauschangriff auf die Wohnung würde in der weit überwiegenden Mehrzahl unschuldige Bürger treffen.

Mit Blick auf die in jüngster Zeit in Kraft getretenen Gesetze, wie das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und andere Erscheinungsformen der organisierten Kriminalität, das Geldwäschegesetz und das Verbrechensbekämpfungsgesetz, appelliere ich an den Gesetzgeber, keine weiteren offenen oder verdeckten Überwachungsmöglichkeiten und Meldepflichten zum Zwecke der Durchsetzung des staatlichen Strafanspruchs zu schaffen. Zunächst einmal müssen mit dem neu geschaffenen gesetzlichen Instrumentarium Erfahrungen gesammelt werden. Das Bundesverfassungsgericht hat im Volkszählungsurteil gefordert, daß der Gesetzgeber *„ungewissen Auswirkungen eines Gesetzes dadurch Rechnung tragen muß, daß er die ihm zugänglichen Erkenntnisquellen ausschöpft, um die Auswirkungen so zuverlässig wie möglich abschätzen zu können. ... Der Gesetzgeber kann aufgrund veränderter Umstände zur Nachbesserung einer ursprünglich verfassungsgemäßen Regelung gehalten sein."* In diesem Sinne hoffe ich auf eine stärkere Erprobung und Überprüfung des vorhandenen Instrumentariums. Das bisherige Wissen darüber ist gegenwärtig jedenfalls noch unzureichend. Daher sollten sich vor weitergehenden Forderungen einer Einschränkung des Rechts auf informationelle Selbstbestimmung sowohl Legislative als auch Exekutive in diesem sensiblen Bereich einer Erfolgskontrolle stellen (siehe auch Nr. 4.1).

1.8 Mehr vertrauensbildende Maßnahmen im Sicherheitsbereich

In der Diskussion um die Eingriffsbefugnisse der Strafverfolgungsbehörden habe ich mehrfach neue, vertrauensbildende Maßnahmen für eine Stärkung des Persönlichkeitsrechts gefordert. Diese Forderung wiederhole ich nachdrücklich. Nach der Strafprozeßordnung (§ 100a) darf ein Telefon für Zwecke der Strafverfolgung überwacht werden. Der Katalog der Straftaten, die diese Überwachung erlauben, ist zuletzt im Verbrechensbekämpfungsgesetz erweitert worden. So sehr dies für eine wirksame Verbrechensbekämpfung notwendig ist, so sehr sprechen andere Gründe dafür, das Persönlichkeitsrecht im Ausgleich hierfür zu stärken. Solche vertrauensbildenden Maßnahmen könnten sein:

- Jährliche Berichterstattung an den Deutschen Bundestag über Anlaß, Verlauf und Ergebnisse der Telefonüberwachung
- Verbesserung des Verfahrens der richterlichen Anordnung: Die Zustimmung zur Überwachungsmaßnahme müßte umfassend begründet werden. Nur bestimmte Richter sollten über den Antrag auf Überwachung entscheiden; damit bliebe die Verantwortung bis zur Beendigung der Maßnahme an diesen Richter gebunden.

In den USA konnten mit entprechenden Regelungen überaus positive Erfahrungen gesammelt werden.

Vertrauensbildende Maßnahmen hatte ich auch in einem anderen Zusammenhang gefordert. Mit dem Verbrechensbekämpfungsgesetz wurde das Gesetz zu Art. 10 GG geändert und die Befugnis der Fernmeldeaufklärung des BND erweitert. Im Falle von Erkenntnissen z. B. über die internationale Drogenkriminalität oder den Terrorismus hat der Bundesnachrichtendienst Informationen an die Polizei weiterzugeben. U. a. hatte ich empfohlen, eine angemessene Übermittlungsschwelle im Gesetz ausdrücklich vorzusehen und durch den Entscheidungsvorbehalt einer unabhängigen Institution (Strafrichter oder G-10-Kommission) zu sichern. Leider ist diese Empfehlung so wenig aufgegriffen worden wie mein Vorschlag einer besseren Datenschutzkontrolle. Gegenwärtig sehe ich eine effektive Datenschutzkontrolle nicht gewährleistet (siehe auch Nrn. 4.1.1, 28.1 und 28.2).

1.9 „Gläserner Ausländer"? „Gläserner Asylbewerber"?

Am 1. Oktober 1994 ist das Gesetz über das Ausländerzentralregister in Kraft getreten. Seit vielen Jahren hatten die Datenschutzbeauftragten von Bund und Ländern gefordert, für dieses Register gesetzliche Grundlagen zu schaffen, die den Eingriff in das Persönlichkeitsrecht von Ausländern verbindlich festlegen. Im Zuge der parlamentarischen Beratungen hat es von allen Seiten z. T. heftige Kritik gegeben. Einige Stimmen sprachen vom „Gläsernen Ausländer".

Meine Bedenken richteten sich im wesentlichen gegen den Informationsverbund des Registers mit der Polizei, den Strafverfolgungsorganen und den Nachrichtendiensten. Damit werden auch im Ausländerzentralregister Erkenntnisse der Sicherheitsbehörden zu Ausländern gespeichert, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie bestimmte Straftaten planen, begehen oder begangen haben. Polizei und Verfassungsschutzbehörden haben dazu jedoch ihre eigenen Informationssysteme. Deren Vernetzung via Ausländerzentralregister widerspricht m. E. dem verfassungsrechtlichen Gebot zur Trennung von Polizei und Nachrichtendiensten. Zu meinem Bedauern wurde hierauf nicht verzichtet. Ich hoffe aber, daß – wie es in den Ausschußberatungen zum Ausdruck gekommen ist – es bei diesem einen „Sündenfall" bleibt. In anderen wichtigen Punkten läßt sich aber eine durchaus zufriedenstellende Bilanz meiner Bemühungen ziehen.

Eine ähnliche, in Teilen polarisierende Diskussion wird z.Zt. zum Thema „Asylcard" geführt, deren Einführung in einer sog. Machbarkeitsstudie geprüft werden soll. Hätten hierzu die politischen Ideengeber und Planer schon in einem sehr frühen Stadium deutlich gemacht, wie sie hierbei das grundgesetzliche Gebot von der Unantastbarkeit der Menschenwürde achten und schützen wollen, wäre vieles an scharfer Kritik erspart geblieben (siehe auch Nr. 3.1).

1.10 Spion im Auto?

Im Auftrag des Bundesministeriums für Verkehr werden derzeit Systeme zur automatischen Erhebung von Straßenbenutzungsgebühren erprobt. Mit der Einführung solcher Systeme besteht die Gefahr, daß personenbezogene Daten über den Aufenthaltsort von Millionen Verkehrsteilnehmern erhoben und verarbeitet werden. Derartige Datensammlungen wären aus datenschutzrechtlicher Sicht nicht akzeptabel. Kaum ein Thema wie dieses hat daher die veröffentlichte Meinung im Berichtszeitraum beschäftigt. Mit besonderer Befriedigung habe ich festgestellt, daß der Bundesverkehrsminister im Unterschied zu seinem Amtsvorgänger deutlich unterstrichen hat, daß nur ein datenschutzgerecht ausgestaltetes Mautsystem in Frage kommt. Ich begrüße sehr, daß auch alle anderen Beteiligten diesen Grundsatz akzeptieren. Die Versuche werden im Frühjahr 1995 abgeschlossen. Erst dann können zuverlässige Aussagen über die einsetzbare Technik getroffen werden. Einige Datenschutzforderungen zeichnen sich schon jetzt ab:

- Die Technik muß so verläßlich sein, daß nicht zur Sicherheit und für alle Fälle Aufzeichnungen über jede Fahrt gespeichert werden.
- Die Verkehrsteilnehmer dürfen nicht gezwungen werden, einen lückenlosen Nachweis über ihre Fahrten zu führen.
- Kontrolliert werden darf nur, wenn Anhaltspunkte dafür bestehen, daß Gebühren nicht entrichtet wurden (siehe auch Nr. 18.1).

1.11 Telekommunikation: Einheitliche Datenschutzkontrolle auch künftig unerläßlich

Mit dem Gesetzpaket zur Postreform II, das zum 1. Januar 1995 in Kraft getreten ist, wurde meine Zuständigkeit für die Deutsche Bundespost Telekom hinsichtlich der Einhaltung von datenschutzrechtlichen Vorschriften wegen deren Monopolstellung bis Ende 1997 verlängert. Zum Ende der Monopole soll sie dagegen entfallen. Aus datenschutzrechtlicher Sicht wäre dies wegen der hohen Sensibilität der im Telekommunikationsbereich anfallenden Daten und ihres besonderen grundrechtlichen Schutzes durch das Fernmeldegeheimnis in Art. 10 GG von großem Nachteil für den Bürger. Vor allem gäbe es keine vorbeugende Kontrolle mehr, die Datenschutzaufsicht würde regional zersplittert.

Im Deutschen Bundestag wurden meine Bedenken geteilt. Der Ausschuß für Post und Telekommunikation empfahl der Bundesregierung eindringlich, daß in Absprache mit den Bundesländern eine zentrale Kontrollstelle für den Datenschutz bestimmt werden soll. In diesem Sinne fordere ich das Bundesministerium für Post und Telekommunikation auf, die Arbeiten hieran nicht auf die lange Bank zu schieben, sondern das Vorhaben voranzubringen (siehe auch Nr. 20.1).

1.12 Sozialdatenschutz: In der Praxis noch vielfach Lücken

Am 1. Juli 1994 ist das 2. SGB-Änderungsgesetz in Kraft getreten. Es enthält eine weitgehend abschließende bereichsspezifische Regelung des Sozialdatenschutzes im Zehnten Buch des Sozialgesetzbuches. Wenn auch nicht alle meine Anliegen sich in dem Gesetz wiederfinden, begrüße ich insgesamt die neue Regelung.

Auch in diesem Tätigkeitsbericht hat der Sozialdatenschutz den größeren Anteil. Die vielen Einzelfälle zeigen, daß es einzelnen Sozialleistungsträgern oftmals an der nötigen Aufgeschlossenheit gegenüber den datenschutzrechtlichen Prinzipien mangelt. In der Praxis sehe ich hier noch viel Handlungsbedarf. Für mich ist der Sozialdatenschutz ein ganz besonderes Anliegen, handelt es sich doch bei den Betroffenen häufig um die sozial schwächeren Menschen in unserer Gesellschaft. Auch bei den an mich gerichteten vielen Eingaben handelt sich überwiegend um Probleme aus dem Sozialdatenschutz. Allzuoft werden hinter dem Rücken der Versicherten Daten erhoben und verarbeitet. Datenschutzrechtliche Prinzipien, wie der Ersterhebungsgrundsatz und das Transparenzgebot, müssen in der Praxis vielfach noch ihre Anerkennung und Durchsetzung finden.

In dieser Legislaturperiode will die Bundesregierung Gesetzentwürfe zu den Bereichen Unfallversicherung (SGB VII) und Rehabilitations- und Schwerbehindertenrecht (SGB IX) vorlegen. Bei den Gesetzesberatungen werde ich darauf drängen, daß diese Gesetze den datenschutzrechtlichen Anforderungen gerecht werden (siehe auch Nrn. 10.1 und 14.1).

1.13 Lücken in der Datenschutzgesetzgebung

In der Datenschutzgesetzgebung bestehen in einigen Gebieten nach wie vor erhebliche Lücken. Bereichsspezifische gesetzliche Regelungen fehlen z. B. im Justiz- und Finanzbereich und im Arbeitnehmerrecht.

- **Arbeitnehmerdatenschutz – ein bislang verschlepptes Thema**

  Der Arbeitnehmerdatenschutz bedarf dringlich bereichsspezifischer Regelungen. Das Bundesdatenschutzgesetz ist hierfür zu allgemein und nicht ausreichend. Selbst einfache Einzelfragen, wie die firmeninterne Bekanntgabe von Krankheitszeiten oder Ausbildungsergebnissen oder die Auskunft des bisherigen an den künftigen Arbeitgeber werfen erhebliche Auslegungsprobleme auf. Die Art und Weise, wie ein Arbeitgeber mit den personenbezogenen Daten von Arbeitnehmern umgehen darf, muß der Tatsache Rechnung tragen, daß der Arbeitnehmer seinem Arbeitgeber in aller Regel

als der sozial schwächere Vertragspartner gegenübersteht. Die Freiwilligkeit der Einwilligung ist da eher zweifelhaft.

Für Beamte gelten seit über zwei Jahren bereichsspezifische Datenschutzregelungen. Niemand wird behaupten wollen, für die Angestellten und Arbeiter des öffentlichen Dienstes oder für die Arbeitnehmer in der freien Wirtschaft sei der Ausbau des Datenschutzes weniger dringlich. Für die neue Legislaturperiode hat die Bundesregierung einen entsprechenden Gesetzentwurf angekündigt. Es ist dringend zu wünschen, daß das Vorhaben nunmehr energisch aufgegriffen wird (siehe auch Nr. 32.4).

– **Datenschutzrechtliche Regelungen im Strafverfahrensbereich nicht länger aufschieben**

Der Schutz des Persönlichkeitsrechts im Strafverfahrensrecht ist nach wie vor unzureichend. Dabei geht es nicht nur um Daten der Täter oder Tatverdächtigen, sondern ebenso um Daten von Verbrechensopfern, Tatzeugen und Unbeteiligten, oft ermittelt unter Zeugniszwang und unter Eingriff in die Privatsphäre. Beispiele hierfür sind medizinische und psychologische Gutachten sowie Abhörprotokolle aus Telefonüberwachungen. Es fehlen Regelungen über die Erteilung von Aktenauskünften und Akteneinsicht sowie die Übermittlung von Erkenntnissen für wissenschaftliche Zwecke – Defizite, die keineswegs nur Beschuldigte, sondern oft einschneidend auch Opfer und Zeugen betreffen. Es fehlen Regelungen über die Fahndung, insbesondere die Öffentlichkeitsfahndung oder durch Einschaltung der Medien, so z. B. zur Ermittlung des Aufenthalts eines Zeugen. Es verstärkt sich der Eindruck, daß es politisch leichter und schneller geht, neue Eingriffsbefugnisse für Staatsanwaltschaften und Polizei zu schaffen, daß es aber sehr lange Zeit braucht, wenn es um die Rechte Betroffener auf sorgfältigen Umgang mit ihren oft sehr sensiblen personenbezogenen Daten geht (siehe auch Nr. 4.2).

Zu den datenschutzrechtlichen Enttäuschungen der zurückliegenden Legislaturperiode zählt ferner, daß die unter Gesichtspunkten des Datenschutzes unerläßlichen Regelungen über den Einsatz gentechnischer Methoden im Strafverfahren nicht getroffen wurden. Für die neue Legislaturperiode hoffe ich, daß die für die Strafverfolgungsorgane sowie für die Betroffenen immer wichtiger werdende rechtliche Klarheit in dieser Frage geschaffen wird (siehe auch Nr. 4.2.2).

– **Justizmitteilungen aus gerichtlichen und staatsanwaltlichen Verfahren an andere Stellen ohne gesetzliche Grundlage**

Seit Jahren fordern die Datenschutzbeauftragten des Bundes und der Länder die dringlich notwendige gesetzliche Grundlage für sog. Justizmitteilungen, d. h. Mitteilungen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften aus den dortigen Verfahren ohne Ersuchen an Gerichte, Behörden und sonstige öffentliche Stellen für andere Zwecke als die des jeweiligen Verfahrens. Justizmitteilungen in Strafsachen bedeuten für den Betroffenen oftmals einen erheblichen Eingriff in sein Persönlichkeitsrecht, wenn diese z. B. zur Rücknahme der Zulassung zur Ausübung eines Handwerks oder zur Untersagung einer ehrenamtlichen Tätigkeit führen können. Ähnliches gilt in Zivilsachen, so z. B. über Mitteilungen in Konkurs- und Vergleichsverfahren an das Finanzamt und die Sozialversicherungsträger, damit sie ihre Forderungen in diesen Verfahren geltend machen können.

Ich bedaure sehr, daß es bisher nicht gelungen ist, diesen Bereich entsprechend den Vorgaben des Volkszählungsurteils zu regeln und einzugrenzen. Hier kommt es entscheidend auch auf den Grundsatz der Transparenz der Datenverarbeitung an, daß nämlich jeder wissen können muß, wer was bei welcher Gelegenheit über ihn weiß. (siehe auch Nr. 4.10).

– **Finanzbereich: Abgabenordnung braucht Datenschutzregelungen**

Die datenschutzrechtlichen Vorschriften der Abgabenordnung stammen noch aus dem Jahre 1977 und entsprechen weder den Anforderungen des geltenden Datenschutzrechts noch den Vorgaben des Bundesverfassungsgerichts zum Recht auf informationelle Selbstbestimmung. Unter diesem Gesichtspunkt sind insbesondere die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Ausgestaltung der Rechte der Betroffenen unzureichend geregelt. Dies gilt auch für die Durchbrechung des Steuergeheimnisses. So muß z. B. bei der Datenübermittlung zur Durchführung von Strafverfahren, die keine Steuerstraftaten betreffen, dem Grundsatz der Verhältnismäßigkeit strikt Rechnung getragen werden. Darüber hinaus ist – auch im Interesse der Praxis der Finanzverwaltung – eine Vereinheitlichung der datenschutzrechtlichen Terminologie dringend geboten.

Seit mehreren Jahren bin ich mit Unterstützung der Landesbeauftragten für den Datenschutz und des Bundesministeriums der Justiz um eine entsprechende Verbesserung der Rechtslage bemüht. Bisher war es leider jedoch nicht möglich, das Bundesministerium der Finanzen dazu zu bewegen, die Abgabenordnung den datenschutzrechtlichen Erfordernissen anzupassen (siehe auch Nr. 5.1).

1.14 Beratungen und Kontrollen, insbesondere Beanstandungen

Zu zahlreichen Gesetzesvorhaben und datenschutzrechtlichen Fragen habe ich Bundesbehörden und sonstige öffentliche Stellen des Bundes beraten. Daneben habe ich Informations- und Kontrollbesuche

durchgeführt. Die von mir kontrollierten Stellen sind in Anlage 1 aufgeführt.

Nach dem Bundesdatenschutzgesetz muß ich Verstöße gegen datenschutzrechtliche Vorschriften förmlich beanstanden (§ 25 BDSG). Von einer Beanstandung kann ich u. a. absehen, wenn die Verstöße oder Mängel von geringer Bedeutung sind. Von dem Mittel der Beanstandung machte ich eher zurückhaltend Gebrauch, da es meine "schwerste Waffe" ist. Die Zahl der festgestellten Mängel oder Verstöße entspricht wieder der im 14. TB genannten.

Zu den Beanstandungen im einzelnen siehe Anlage 2.

2 Datenschutz beim Deutschen Bundestag

In meinem 14. TB (S. 32 Nr. 3.1) hatte ich berichtet, daß den Fraktionen und Gruppen des Deutschen Bundestages ein Entwurf zur Ergänzung seiner Geschäftsordnung um eine **Datenschutzordnung** und – damit zusammenhängend – ein Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes vorliegt. Hiermit sollen eigenständige datenschutzrechtliche Regelungen geschaffen werden, die – in Anlehnung an das Bundesdatenschutzgesetz – den besonderen Belangen **parlamentarischer Tätigkeit** Rechnung tragen. Die Beratungen über die Entwürfe haben in der 12. Wahlperiode zu keinem abschließenden Ergebnis geführt. Ich halte es für geboten, in der neuen Legislaturperiode die Beratungen hierüber wieder aufzunehmen und klare datenschutzrechtliche Grundlagen für den parlamentarischen Bereich zu schaffen.

Unabhängig hiervon bin ich gern der Bitte um Beratung im parlamentarischen Bereich gefolgt. Der 2. Untersuchungsausschuß **„Treuhandanstalt"** des Deutschen Bundestags hat mich dazu gehört, wie der Schutz der Privat- und Geschäftsgeheimnisse in den von der Bundesregierung angeforderten Akten der Treuhandanstalt und in anderen Akten zu gewährleisten ist (vgl. BT-Drs. 12/8404 S. 28 f.). Außerdem bin ich vom Sekretariat der Enquete-Kommission **„Aufarbeitung von Geschichte und Folgen der SED-Diktatur in Deutschland"** um Beratung bei der Vorbereitung einer Verlagspublikation gebeten worden. Damit sollen die von der Kommission in Auftrag gegebenen Expertisen und Berichte (einschließlich Abdrucken von Dokumenten und Aktenauszügen) veröffentlicht werden. Diese Unterlagen enthalten eine Vielzahl personenbezogener Daten. Für einen Teil der Unterlagen war das Stasi-Unterlagen-Gesetz (StUG) heranzuziehen, insbesondere § 32 Abs. 3, der ausdrückliche Regelungen für die Veröffentlichung personenbezogener Daten trifft; für die Veröffentlichung anderer Unterlagen konnten diese Regelungen entsprechend herangezogen werden. Ich habe dargelegt

- daß außer im Falle ausdrücklicher Einwilligung eine Veröffentlichung personenbezogener Informationen von Betroffenen oder Dritten i. S. des Stasi-Unterlagen-Gesetzes unzulässig ist;
- daß Informationen über „Personen der Zeitgeschichte, Inhaber politischer Funktionen oder Amtsträger in Ausübung ihres Amtes, soweit sie nicht Betroffene oder Dritte sind" (vgl. § 32 Abs. 3 Nr. 2 StUG) solche sind, die deren zeitgeschichtliches, politisches oder amtliches Wirken betreffen, und daß Angaben über die Privatsphäre dieser Personen durchweg nicht hierzu zählen; solche Angaben seien auch in bezug auf Mitarbeiter und Begünstigte des Staatssicherheitsdienstes im Sinne des § 32 Abs. 3 Nr. 2 StUG von der Veröffentlichung auszuschließen;
- daß in jedem Falle der **parlamentarische Auftrag** der Enquete-Kommission einerseits und die **schutzwürdigen Interessen** der in Betracht kommenden Personen andererseits vor einer Veröffentlichung gegeneinander abzuwägen sind.

Anhand dieser Leitlinien wurden Einzelfälle erörtert. Das Sekretariat erklärte, man werde die datenschutzrechtlichen Empfehlungen in die Überlegungen zur Veröffentlichung einbeziehen.

3 Innere Verwaltung und Auswärtiger Dienst

3.1 Ausländerzentralregister

3.1.1 Endlich: AZR-Gesetz

Am 1. Oktober 1994 ist das Gesetz über das Ausländerzentralregister in Kraft getreten. Es ist unter Gesichtspunkten des Datenschutzes eines der bedeutendsten sowohl im Berichtszeitraum als auch in der letzten Legislaturperiode. Unterstützt von den Landesbeauftragten für den Datenschutz hatte ich seit mehr als einem Jahrzehnt immer wieder gefordert, für dieses Register gesetzliche Regelungen zu schaffen, die den Eingriff in das Persönlichkeitsrecht von Ausländern verbindlich festlegen (siehe hierzu auch Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 – Anlage 7 –).

Die Vorbereitung dieses Gesetzes habe ich von Anfang an mit großer Intensität begleitet (zuletzt 14. TB S. 33 ff.). In diesem Zusammenhang möchte ich die gute Zusammenarbeit mit den beteiligten Ressorts und dem Bundesverwaltungsamt als Registerbehörde besonders hervorheben.

Das Gesetz ist schon vor seinem Inkrafttreten von vielen Seiten kritisiert worden. Meine Bedenken richteten sich im wesentlichen gegen den Informationsverbund des Registers mit der Polizei, den Strafverfolgungsorganen und den Nachrichtendiensten. Damit werden auch im AZR Erkenntnisse der Sicherheitsbehörden zu Personen gespeichert, bei denen Anhaltspunkte für den Verdacht bestehen, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben (§ 2 Abs. 2 Nr. 7 AZRG). Polizei und Verfassungsschutzbehörden haben dazu jedoch ihre eigenen Informationssysteme. Deren Vernetzung via AZR widerspricht dem verfassungsrechtlichen Gebot zur Trennung von Polizei und Nachrichtendiensten.

Diese Speicherung hat das Bundesministerium des Innern nicht nur mit Erfordernissen der Kriminalitätsbekämpfung begründet, sondern auch mit einem In-

formationsbedarf der Ausländerbehörden und Auslandsvertretungen z. B. bei der Visaerteilung und der Verlängerung von Aufenthaltsgenehmigungen. Die Speicherung im AZR sei notwendig, da die Ausländerbehörden und die Auslandsvertretungen keinen Zugriff auf das polizeiliche Informationssystem INPOL haben und – wie das BMI in den Ausschußberatungen vorgetragen hat – auch nicht erhalten sollen. Meiner Forderung, nur diesen Stellen den Zugriff auf diese Daten im AZR einzuräumen, wurde dagegen nicht entsprochen.

Weiterhin habe ich den automatisierten Zugriff von Nachrichtendiensten auf im AZR gespeicherte Daten (§ 22 Abs. 1 Nr. 8 AZRG) als bedenklich problematisiert, auch wenn dieser auf die Stelle, die die Daten übermittelt hat, auf Geschäftszeichen und auf Personalien des betroffenen Ausländers reduziert ist. U. a. habe ich darauf hingewiesen, daß der Gesetzgeber in der Vergangenheit selbst restriktive Ansätze der Zulassung von Nachrichtendiensten zu automatisierten Abrufverfahren abgelehnt hat. Ich bedauere, daß meine Empfehlung, hierauf auch mit Blick auf das AZR zu verzichten, nicht aufgenommen wurde. Ich hoffe, daß – wie es in den Ausschußberatungen zum Ausdruck gekommen ist – es bei diesem einen „Sündenfall" bleibt.

In anderen wichtigen Punkten läßt sich aber eine durchaus befriedigende Bilanz meiner Bemühungen ziehen:

- Entgegen den Vorstellungen des Bundesrats hat sich die Auffassung durchgesetzt, daß nicht jeder Polizeibeamte auf jedes an die Registerbehörde gerichtete Ersuchen alle über den Ausländer im AZR gespeicherte Daten benötigt – eine Frage nicht nur des Datenschutzes, sondern auch der Arbeitsökonomie. Ich habe mich nachdrücklich für eine Lösung eingesetzt, wie der Gesetzgeber sie nunmehr verabschiedet hat (§ 16 AZRG), nämlich ein mehrstufiges Verfahren der Datenübermittlung an die Polizeivollzugsbehörden und Staatsanwaltschaften, in dem nicht alle Daten automatisiert abgerufen werden können.
- Entgegen den Vorstellungen des Bundesrats hat der Gesetzgeber daran festgehalten, daß Protokolldaten ausschließlich für die Zwecke der Auskünfte an den Betroffenen, der Unterrichtung über Berichtigung, Löschung oder Sperrung von Daten, der Sicherstellung des ordnungsgemäßen Betriebes der Datenverarbeitungsanlage und der Datenschutzkontrolle, nicht aber für Fahndungszwecke verfügbar sind (§§ 9 Abs. 2 und 13 Abs. 2 AZRG). Ich hoffe sehr, daß diese an die Prinzipien des § 14 Abs. 4 BDSG angelehnte Entscheidung auch zukünftig bei anderen Rechtsnormen wegweisend ist.
- Auch die Regelung zur Erteilung von Gruppenauskünften ist überwiegend befriedigend. Da Gruppenauskünfte immer auch einen Eingriff in das informationelle Selbstbestimmungsrecht unbeteiligter Personen bedeuten, begrüße ich, daß hier – gegen Vorstellungen des Bundesrats – datenschutzrechtlich akzeptable Regelungen geschaffen wurden. Danach sind z.B Gruppenauskünfte nicht „zur Verfolgung von Straftaten" schlechthin zugelassen, sondern „zur Verfolgung eines Verbrechens oder einer anderen Straftat, von der aufgrund tatsächlicher Anhaltspunkte anzunehmen ist, daß sie gewerbs- oder gewohnheitsmäßig von einem Bandenmitglied oder in anderer Weise organisiert begangen wird" (§ 12 Abs. 1 Satz 1 Nr. 2 b AZRG).
- Die Verpflichtung der Registerbehörde, im automatisierten Abrufverfahren sicherzustellen, daß die einzelnen abrufberechtigten Stellen Daten nur in dem Umfang abrufen können, der dem angegebenen Verwendungszweck entspricht (§ 22 Abs. 4 AZRG), geht auf meine Empfehlung zurück.
- Erfolgreich mitwirken konnte ich auch bei der Schaffung der Vorschrift über die „Übermittlung und Veränderung von Daten im Wege der Direkteingabe" (§ 7 AZRG).

3.1.2 Verordnung zur Durchführung des AZR-Gesetzes

Wie beim Ausländerzentralregistergesetz hat mich das Bundesministerium des Innern auch an der Vorbereitung einer Verordnung zur Durchführung des Ausländerzentralregistergesetzes schon in einem frühen Stadium beteiligt. Dabei konnte ich sowohl durch schriftliche Stellungnahmen als auch durch die Teilnahme an Besprechungen im Rahmen der Ressort- und Länderabstimmungen datenschutzrechtliche Verbesserungen des Entwurfs erreichen. Besonders wichtig war mir die inhaltliche Präzisierung der Datenübermittlungen an und durch die Registerbehörde, das Bundesverwaltungsamt. Wegen der engen Zweckbindungsregelungen des Gesetzes waren besonders genau abgefaßte Regelungen über die verschiedenen Verwendungszwecke der Daten erforderlich. Weitere Beispiele für Verbesserungen sind die Regelungen über die Auskunftserteilung an den Betroffen und über die Möglichkeit, eigene Daten im Register sperren zu lassen.

Die Kontrolle und Beratung der Registerbehörde hinsichtlich der Vorschriften des Gesetzes und der Verordnung wird ein Schwerpunkt meiner zukünftigen Arbeit sein.

3.2 Asylverfahren

3.2.1 Kontrolle und Beratung des Bundesamtes für die Anerkennung ausländischer Flüchtlinge und seiner Außenstellen

Ein starkes Anwachsen der Asylbewerberzahlen, die zum 1. Juli 1993 erneut geänderten gesetzlichen Vorgaben, mit der die Antragstellung von den Ausländerbehörden zum Bundesamt für die Anerkennung ausländischer Flüchtlinge verlagert wurde, sowie die Vorbereitung auf das anzuwendende Ausländerzentralregistergesetz waren beim Bundesamt und seinen Außenstellen Anlaß für die Einführung einer vernetzten elektronischen Datenverarbeitung mit Hilfe des Systems ASYLON. Die Verarbeitung personenbezogener Daten habe ich sowohl bei der Zentrale des Bundesamtes in Nürnberg als auch bei Außenstellen der Behörde kontrolliert.

Mein besonderes Augenmerk galt hierbei der Richtigkeit der in ASYLON zu erhebenden Daten des

Asylbewerbers. Ich halte es für sachgerecht, daß sich der Bearbeiter des Asylantrages zunächst durch eine Abfrage des Ausländerzentralregisters Klarheit darüber verschafft, ob der Asylbewerber bereits an anderer Stelle in der Bundesrepublik Deutschland in Erscheinung getreten ist. In diesem Zusammenhang hat der Bearbeiter – bei Vergleich der vom Ausländerzentralregister angegebenen Personalien (§ 10 Abs. 3 AZRG) mit den jeweils vorliegenden Personendaten des Antragstellers – eine nicht immer leichte Identitätsentscheidung zu treffen. Eine ähnliche Problematik ergibt sich auch bei der Nutzung des Systems ASYLON, wenn festgestellt wird, ob der Asylbewerber bereits einen Asylantrag gestellt hat. Für diese Arbeitsschritte habe ich Hinweise und Anregungen gegeben. Das Bundesministerium des Innern und das Bundesamt sind meinen Empfehlungen erfreulicherweise nachgekommen. So hat das Bundesamt durch Schulungen und verbesserte Dienstanweisungen die Information und die Kenntnis der Mitarbeiter über die Anwendung beider Systeme gefestigt.

Aufgrund der seit Juli 1992 geänderten Vorschrift des § 16 AsylVfG (s. 14. TB S. 35f.) werden Asylbewerber, die älter als 14 Jahre sind, zur Sicherung ihrer Identität erkennungsdienstlich behandelt. Die Abnahme der Abdrucke aller Finger durch das BAFl erfolgt auf demselben Formular-Muster, welches das Bundeskriminalamt für die erkennungsdienstliche Behandlung von mutmaßlichen Straftätern benutzt. Dieses Fingerabdruckblatt, das das BAFl dem Bundeskriminalamt zur Auswertung im Automatisierten Fingerabdrucksystem (AFIS) zuleitet, enthält außer den für die Identitätsfeststellung zwingend erforderlichen Angaben auch weitere Datenfelder, z. B. zum Familienstand, zum Beruf, zum Ehegatten und sogar zu den Eltern des Antragstellers. Ich vermag die Bedeutung solcher Angaben zum Zwecke der Feststellung der Identität des Asylbewerbers nicht zu erkennen und habe empfohlen, auf diese Datenfelder im Vordruck zu verzichten. Das Bundesministerium des Innern hat bislang meiner Empfehlung nicht entsprochen, vielmehr darauf hingewiesen, daß die in Rede stehenden Felder für die Bearbeitung von Übernahmegesuchen der Vertragsstaaten des Schengener und Dubliner Übereinkommens (hierzu siehe auch nachfolgend Nr. 3.2.2) an Bedeutung gewinnen könnten. Diese Vermutung rechtfertigt die Erhebung dieser Daten nicht. Ich halte daher meine Forderung nach Verzicht dieser Datenerhebung aufrecht.

Im Regelfall wird ein Asylbewerber durch den Einzelentscheider des Bundesamtes angehört, bevor das Auswertungsergebnis des Zehn-Finger-Abdruckblattes durch das Bundeskriminalamt vorliegt. Ich halte dies für unbefriedigend, da anzunehmen ist, daß eine Anhörung einen gänzlich anderen Verlauf nehmen würde und einen anderen Inhalt hätte, wenn dem Einzelentscheider schon bei deren Beginn bekannt wäre, daß Tatsachen vorliegen, die auf eine Identitätstäuschung und somit auf einen offensichtlich unbegründeten Asylantrag (§ 30 Abs. 3 Nr. 2 AsylVfG) hindeuten. Das Bundesministerium des Innern hat dazu bemerkt, eine Unterrichtung des Einzelentscheiders über das Auswertungsergebnis vor der Anhörung würde den Ablauf des Asylverfahrens erheblich verzögern und dem Beschleunigungszweck des Asylverfahrensgesetzes entgegenwirken. Ich habe die Hoffnung, daß meiner Empfehlung doch noch entsprochen wird, da das Bundesministerium davon ausgeht, daß die Auswertungszeit des Bundeskriminalamtes und die sich anschließende Unterrichtung des Bundesamtes für die Anerkennung ausländischer Flüchtlinge zukünftig verkürzt werden kann.

In verschiedenen Verfahrensschritten habe ich Auswertungsunterlagen – auch mit Personenbezug – vorgefunden, die statistischen Anforderungen dienen. Das Bundesministerium des Innern hat mir mitgeteilt, daß künftig die Form der Datenerfassung für Geschäftsstatistiken ohne personenbezogene Daten lediglich anhand von Sachständen erfolgen soll. Ich werde dies verfolgen.

3.2.2 Übermittlung von Asylbewerberdaten ins Ausland

Die Übermittlung von Daten von Asylbewerbern ins Ausland war weiterhin auch Gegenstand öffentlicher Diskussion (siehe hierzu auch 14. TB S. 35f.). Leider haben sich meine Vorstellungen nicht durchgesetzt, im Interesse des Asylsuchenden und seiner Angehörigen im Asylverfahren Kontakte zum Herkunftsland bzw. Verfolgerstaat grundsätzlich nur mit Zustimmung des Betroffenen zuzulassen. Immerhin ist in der Vorschrift des § 7 Abs. 2 Satz 2 Asylverfahrensgesetz eine Regelung getroffen, die bei der Datenerhebung bei ausländischen Behörden auf eine Vermeidung der Beeinträchtigung schutzwürdiger Interessen des Betroffenen zielt. Bei meinem Kontroll- und Beratungsbesuchen beim Bundesamt für die Anerkennung ausländischer Flüchtlinge und seinen Außenstellen ging es mir besonders um das Verhältnis dieser Regelung zu einer anderen datenschutzrechtlich bedeutsamen Vorschrift des Asylverfahrensgesetzes. Nach dem seit Juli 1993 geltenden § 43b AsylVfG hat für Ausländer, die in einer Aufnahmeeinrichtung zu wohnen verpflichtet sind, das Bundesministerium des Innern oder die von ihm bestimmte Stelle die Heimreisedokumente im Wege der Amtshilfe zu beschaffen. Die erforderlichen Maßnahmen sind zum frühestmöglichen Zeitpunkt zu treffen. Übereinstimmend mit dem örtlichen Vertreter des UNHCR habe ich darauf hingewiesen, daß die Regelung des § 7 Abs. 2 Satz 2 AsylVfG als gesetzgeberische Leitlinie auch für die Datenübermittlung an das Herkunftsland bei Anwendung des § 43b AsylVfG verstanden werden muß. In meinen Empfehlungen an das Bundesministerium des Innern habe ich Überlegungen widersprochen, daß einseitig die von der jeweiligen ausländischen Vertretung „gestellten Bedingungen" bei der Beantragung der Heimreisedokumente „zu beachten" sind. Die Beschaffung der Heimreisedokumente ist nicht lediglich eine innere Angelegenheit zwischen dem Ausländer und seinem Heimatstaat, in die sich die Bundesrepublik nicht einmischen dürfte. Berührt sind vielmehr nach meinem Verständnis völkerrechtliche Ansprüche im zwischenstaatlichen Verhältnis zwischen der Bundesrepublik und dem Heimatstaat, deren Bedingungen – in den Antragsvordrucken der jeweiligen Auslands-

vertretung – nicht einseitig bestimmt werden. Vor diesem Hintergrund habe ich nachdrücklich die an das Auswärtige Amt gerichtete Bitte des Bundesministeriums des Innern unterstützt, in Verhandlungen mit den jeweiligen Botschaften „eine Neutralisierung der Antragsvordrucke zu erreichen".

Vorsorglich habe ich auch darauf hingewiesen, daß – unbeschadet des gesetzlichen Gebotes, die erforderlichen Maßnahmen „zum frühestmöglichen Zeitpunkt zu treffen" – § 43b AsylVfG Stellen der Bundesrepublik einen Kontakt zu der Vertretung des ausländischen Staates zum Zwecke der Beschaffung von Heimreisedokumenten in Fällen nicht erlaubt, in denen eine Heimreise nicht oder noch nicht in Betracht kommt. Dementsprechend habe ich die im BAFl bestehende Verfahrensregelung unterstrichen, daß diese Behörde ausgefüllte Anträge auf Beschaffung von Heimreisedokumenten nicht aus der Hand gibt, bevor nicht nach erfolgter Anhörung das Votum des Einzelentscheiders „offensichtlich unbegründet" oder „unbeachtlich" lautet.

Andere bedeutsame Aspekte der Übermittlung von Asylbewerberdaten ins Ausland enthalten folgende internationale Übereinkommen: Nach dem Übereinkommen vom 19. Juli 1990 zur Durchführung des Übereinkommens von Schengen vom 14. Juni 1985 (Titel II, Kap. 7, Art. 38 Abs. 5) und dem Dubliner Übereinkommen vom 15. Juni 1990 (Art. 15 Abs. 5) dürfen die zu übermittelnden personenbezogenen Informationen nur zu den in diesen Übereinkommen näher bestimmten asylrechtlichen Zwecken verwendet werden. Nach Inkrafttreten des Dubliner Übereinkommens dürfen aufgrund des sog. Bonner Protokolls (vgl. BT-Drs. 13/24 vom 18. November 1994) die asylrechtlichen Regelungen des Schengener Durchführungsübereinkommens nicht mehr angewandt werden. Beide Übereinkommen regeln auch, daß neben näher bestimmten anderen Personalien auch „sonstige zur Identifizierung des Asylbewerbers erforderliche Angaben" an die jeweilige Behörde der ausländischen Vertragspartei übermittelt bzw. von dieser entgegengenommen werden dürfen. Das können im Einzelfall auch Fingerabdrucke sein, wie in einem Gutachten des Juristischen Dienstes des Rates der Europäischen Gemeinschaften vom 18. März 1993 – 5546/93 – JUR25 – dargelegt wird. Hierzu wird vertreten, daß diese oft das einzige effiziente Mittel zur sicheren Identifizierung des Asylbewerbers wären. Die in den genannten Übereinkommen enthaltenen Zweckbindungsregelungen haben durch die Ratifizierungsgesetze normativen Rang. Somit ist den Vertragsparteien eine zweckändernde Verwendung der auszutauschenden Asylbewerberdaten, also auch von Fingerabdrucken, für Zwecke der Strafverfolgung und Gefahrenabwehr nicht erlaubt. Anders läßt es § 16 Abs. 5 Asylverfahrensgesetz in bezug auf in der Bundesrepublik gestellte Asylanträge zu. Zu den *„einzuleitenden Maßnahmen"*, die die Vertragsparteien im *Vorgriff* auf die Inkraftsetzung der Übereinkommen zu treffen haben (vgl. hierzu Einigung der Schengener Vertragspartner vom 18. Oktober 1993 in Paris, Bulletin der Bundesregierung vom 26. Oktober 1993 S. 1028), sollten – so empfehle ich nachdrücklich – Vorkehrungen zur Gewährleistung der genannten Zweckbindungsregelungen gehören.

Bei den auch auf internationaler Ebene laufenden Überlegungen, unter dem Begriff EURODAC ein europäisches automatisches Fingerabdruckidentifizierungssystem zu schaffen, geht es um mehr als die zwischen zwei Vertragsstaaten im Einzelfall erforderliche Übermittlung von Fingerabdruckdaten zur Identifizierung des Asylbewerbers mit dem Ziel, den für die Prüfung des Asylantrags zuständigen Vertragsstaat zu bestimmen und die Prüfung des Antrags vorzunehmen: EURODAC soll Fingerabdruckdaten aller Asylbewerber in den Mitgliedstaaten allen diesen Staaten zugänglich machen. Damit soll EURODAC das mit den vorgenannten Übereinkommen angestrebte Ziel absichern, asylsuchenden Flüchtlingen europaweit nur ein Anerkennungsverfahren zu gewähren. Ich schließe mich aber nachdrücklich der von der Bundesregierung vertretenen Auffassung an, daß für EURODAC eine eigene Konvention geschaffen werden muß. Die Entwicklung einer spezifischen Rechtsgrundlage halte ich auch für den Fall erforderlich, daß EURODAC als dezentrales System konzipiert werden sollte. Ich teile die auch von anderen Mitgliedstaaten der Europäischen Union ausgesprochene Besorgnis über die Gefahren von Vernetzungen von EURODAC mit anderen Zielen oder polizeilichen Datenbanken und die Verwendung von Asylbewerberdaten für verfahrensfremde Zwecke. Aus meiner Sicht ist zum Schutz der Asylbewerberdaten zumindest ein Datenschutzstandard wie in den vorgenannten Übereinkommen anzustreben.

3.3 Verwendung erkennungsdienstlicher Daten von Bürgerkriegsflüchtlingen

Die – auch in den Medien geführte – Diskussion, ob und inwieweit Bürgerkriegsflüchtlinge wie Asylbewerber zu behandeln sind, berührt auch Fragen des Schutzes der Persönlichkeitsrechte der Betroffenen. Hierzu zählt vor allem die erkennungsdienstliche Behandlung von Bürgerkriegsflüchtlingen und die Verwendung solcher Daten.

Die Innenministerkonferenz hat in ihrer Sitzung am 6./7. Mai 1994 zum Thema „Anwendung von Verfahrens- und Leistungsregeln für Asylbewerber auf Bürgerkriegsflüchtlinge (Mißbrauchsverhütung)" folgenden Beschluß gefaßt:

> *„Die Innenminister und Senatoren der Länder bitten die Bundesregierung, durch eine entsprechende Änderung des Ausländergesetzes die generelle erkennungsdienstliche Behandlung auch von Bürgerkriegsflüchtlingen zu ermöglichen. Bis zu der erforderlichen Rechtsänderung sind die vorhandenen Möglichkeiten nach § 41 des Ausländergesetzes konsequent auszuschöpfen."*

Für mich war zunächst auf der Basis geltenden Rechts die Feststellung wichtig, daß § 16 des Asylverfahrensgesetzes auf Bürgerkriegsflüchtlinge nicht anwendbar ist; hiernach dürfen lediglich Asylsuchende erkennungsdienstlich behandelt werden.

Eine andere Frage ist, wie dies in Zukunft sein soll. Nach Informationen aus dem Bundesministerium des Innern wird eine gesetzliche Regelung angestrebt,

die eine erkennungsdienstliche Behandlung von Bürgerkriegflüchtlingen ermöglichen soll. Grund hierfür seien zahlreiche Fälle aufgedeckter Mehrfachidentitäten und gefälschter Personaldokumente. Ursache für diese Erkennisse dürfte sein, daß in Folge von Kriegswirren im ehemaligen Jugoslawien auch Vordrucke und Personalausweise amtlicher Stellen ehemaliger jugoslawischer und auch bosnischer Behörden in falsche Hände geraten sind. In vielen Fällen habe sich gezeigt, daß es ehemaligen Asylbewerbern gelungen sei, sich nach negativ abgeschlossenem Verfahren unter anderer Identität als vermeintlicher Bürgerkriegsflüchtling ein neues Aufenthaltsrecht – und damit verbundene Sozialleistungen – zu erschleichen. Diese Gründe überzeugen mich nicht, denn auch für die Zukunft müßte die Regelung des § 41 Ausländergesetz (AuslG) ausreichen, die erkennungsdienstliche Maßnahmen im Einzelfall dann erlaubt, wenn Zweifel über die Person oder die Staatsangehörigkeit des Ausländers bestehen und diese Zweifel nicht mit vertretbarem Aufwand in anderer Weise ausgeräumt werden können. Gegen die pauschale erkennungsdienstliche Behandlung aller Bürgerkriegsflüchtlinge – egal wann, unter welchen Umständen und aus welcher Gegend der Welt sie kommen – habe ich erhebliche Bedenken.

Auch wenn man Bürgerkriegsflüchtlinge erkennungsdienstlichen Maßnahmen dann unterzieht, wenn sich Identitätszweifel in anderer Weise nicht ausräumen lassen, stellt sich die weitere Frage, ob diese erkennungsdienstlichen Daten, insbesondere auch ihre Fingerabdrucke, beim Bundeskriminalamt zweckändernd – nach dem Muster des § 16 Abs. 5 AsylVfG bzw. des § 78 Abs. 3 AuslG – zur Aufklärung von Straftaten in gleichem Maße zur Verfügung stehen sollen, wie Daten anderer Ausländer und als potentielle Straftäter erkannter Personen. Mit Blick auf die besondere Situation von Bürgerkriegsflüchtlingen trete ich dafür ein, sich hierbei auf einen Katalog schwerer Straftaten und Straftaten im Zusammenhang mit der Erlangung des Status eines Bügerkriegsflüchtlings zu beschränken.

3.4 Kontrolle und Beratung des Bundesverwaltungsamtes und seiner Außenstellen bei der Durchführung des Aussiedleraufnahmeverfahrens

Am 1. Januar 1993 ist das Gesetz zur Bereinigung von Kriegsfolgengesetzen (Kriegsfolgenbereinigungsgesetz – KfbG) in Kraft getreten, das das Gesetz über die Angelegenheiten der Vertriebenen und Flüchtlinge (Bundesvertriebenengesetz – BVFG) aus dem Jahre 1953 an die heutigen Gegebenheiten nach der Herstellung der Deutschen Einheit anpaßt.

Mit der Einführung des Begriffes „Spätaussiedler" und der vereinfachten Aufnahme als Ehegatte oder Abkömmling wurden rechtliche Rahmenbedingungen geschaffen, die es ermöglichen, den Antrag auf Aufnahme in seinem Umfang deutlich zu reduzieren, was meinem langjährigen Anliegen entspricht (vgl. 14. TB S. 41 f.). Das Bundesministerium des Innern hat in Zusammenarbeit mit dem Bundesverwaltungsamt einen nunmehr – immer noch – 20seitigen Fragebogen entwickelt, der die Erhebung personenbezogener Daten auf den für die Entscheidung erforderlichen Rahmen begrenzt. Dieser Fragebogen dient der Verwaltungsvereinfachung und erfüllt den Zweck, das Aufnahmeverfahren zu beschleunigen; er dient zugleich dem Datenschutz und verhindert die Abfrage personenbezogener Daten, die für das Verfahren nicht erforderlich sind. Nur wer als Ehegatte oder Abkömmling selbst die Spätaussiedlereigenschaft erwerben will, muß ergänzend noch einen 8seitigen Zusatzfragebogen ausfüllen.

Die veränderte Rechtslage habe ich zum Anlaß genommen, zwei Außenstellen des Bundesverwaltungsamtes zu kontrollieren. Ich habe hierbei erfreulicherweise festgestellt, daß meine früher gegebenen Empfehlungen zwischenzeitlich im wesentlichen umgesetzt worden sind. Das Bundesverwaltungsamt setzt für die Aufgabenerfüllung des Aussiedleraufnahmeverfahrens eine umfangreiche Datenverarbeitung ein. Mit Ausnahme der Prüfung des schriftlichen Antrages arbeitet das Bundesverwaltungsamt weitgehend papierlos, d. h. die notwendigen Daten werden in einem Datenverarbeitungssystem vorgehalten, ein Textverarbeitungssystem dient der Erstellung von Individualtexten, der Aufnahmebescheid und der Registrier- und Verteilschein werden automatisiert erstellt. Das Bundesverwaltungsamt hat inzwischen technische Maßnahmen getroffen, die meinen Empfehlungen zur Paßwortgestaltung und zum Sicherheitsmanagement (Anlage 13 zum 14. TB S. 193) weitestgehend entsprechen.

Hervorzuheben ist auch, daß die Laufkarte für Spätaussiedler nunmehr in allen Außenstellen des Bundesverwaltungsamtes einheitlich gestaltet ist. Es ist für den Antragsteller erkennbar, welche Stellen als Teil des Registrier- und Verteilungsverfahrens aufzusuchen sind (zur Beteiligung der Nachrichtendienste s. Nr. 26.3).

3.5 Kontrolle und Beratung des Bundesverwaltungsamtes – Außenstelle Gießen – bezüglich Altdaten aus der Aufnahme von Übersiedlern aus der ehemaligen DDR

Auch fünf Jahre nach der Wende gehen heute noch bis zu 200 schriftliche Anfragen monatlich zu Übersiedlerdaten beim Bundesverwaltungsamt ein. Hierbei handelt es sich hauptsächlich um Auskunftsersuchen öffentlicher Stellen (z. B. Rentenversicherungsträger, Vertriebenenämter, Gerichte etc.), die zur Erfüllung ihrer Aufgaben Auskünfte aus der Übersiedlerakte benötigen. Häufig wendet sich auch der Betroffene an die ehemalige Bundesaufnahmestelle und bittet um Auskünfte, die sich in der Regel auf genaue, in der Aufnahmeakte vorhandene Angaben z. B. zum Einreisedatum oder frühere Anschriften in der ehemaligen DDR beziehen. Diese Information benötigt der Betroffene typischerweise zur Durchführung anderer Verwaltungsverfahren wie z. B. Rentenangelegenheiten. In einigen Fällen wenden sich auch Verwandte oder Bekannte an die ehemalige Bundesaufnahmestelle in der Hoffnung, durch die erbetene Auskunft den jetzigen Wohnort des Betroffenen ausfindig machen zu können.

Mangels einer bereichsspezifischen Rechtsgrundlage hat das Bundesverwaltungsamt jedes Auskunftsbegehren auf die rechtliche Zulässigkeit nach dem Bundesdatenschutzgesetz zu prüfen. Auch in Gesprächen mit den Mitarbeitern der Außenstelle Gießen habe ich festgestellt, daß die vorhandene Arbeitsanweisung des Bundesverwaltungsamtes zur Durchführung der Rest- und Folgeaufgaben Lücken enthielt. Insbesondere fehlten Hinweise zum Verständnis des Gesetzesbegriffes der schutzwürdigen Interessen des Betroffenen (§ 16 Abs. 1 Nr. 2 BDSG) bei Auskunftserteilung an nicht-öffentliche Stellen, wie z. B. Verwandte. Aufgrund meiner Beratung hat das Bundesverwaltungsamt inzwischen eine neue Arbeitsanweisung erstellt, die dem Schutz der Persönlichkeitsrechte der Betroffenen in vollem Umfang gerecht wird. Als Ergebnis meiner Kontrolle sind auch die technischen und organisatorischen Maßnahmen zur Datensicherung verbessert worden.

3.6 Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR

3.6.1 Änderungen des Stasi-Unterlagen-Gesetzes

Die auf Erfahrungen von nunmehr mehr als drei Jahren gestützte Bewertung, daß sich das Stasi-Unterlagengesetz im wesentlichen bewährt hat, wird von mir aus der Sicht meiner datenschutzrechtlichen Kontroll- und Beratungsaufgabe geteilt. Hierzu steht nicht im Widerspruch, daß zu Einzelfragen Verbesserungen und Ergänzungen notwendig sind. Anstöße hierzu habe ich bereits in meinem 14. Tätigkeitsbericht (S. 36 ff.) gegeben. Ich begrüße insofern Überlegungen aus dem Hause des Bundesbeauftragten für die Stasi-Unterlagen (BStU), für die Verwendung von Daten über eine lange zurückliegende Stasi-Verstrikkung eine zeitliche Grenze zu setzen. Dies geht in die gleiche Richtung wie von mir unter Hinweis auf im Bundeszentralregistergesetz verankerte Resozialisierungsgedanken gegebene Empfehlungen, dem Zeitablauf seit Beendigung der Stasi-Mitarbeit Rechnung zu tragen.

Nach dem zwischenzeitlich geänderten Stasi-Unterlagen-Gesetz (StUÄndG vom 22. Februar 1994) darf der BStU zur Erfüllung seiner Aufgaben aus dem – inzwischen aufgelösten – Zentralen Einwohnerregister der ehemaligen DDR das Personenkennzeichen und bestimmte damit verbundene Identifizierungsdaten (Name, Vorname, Geburtsname, sonstige Namen, Geburtsort, letzte Anschrift, Merkmal „verstorben") nutzen. Diese Ergänzung entspricht meinen Empfehlungen (14. TB S. 20 f. und 38 f.). Ebenso halte ich die in der Gesetzesänderung zugelassene Übermittlung dieser Daten an Gerichte und Strafverfolgungsbehörden für gerechtfertigt.

Auch das Zweite Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes (2. StUÄndG vom 26. Juli 1994) habe ich unterstützt. Wiederholte Hinweise der Medien auf das Vorhandensein von Stasi-Informationen aus ausländischen Geheimdienstunterlagen in der Bundesrepublik haben bewußt gemacht, das Konzept der Vollständigkeit des Archivs des BStU mit Nachdruck durchzusetzen. Ich habe bei dieser Gelegenheit das vorherrschende Verständnis des § 6 StUG über den Begriff der Stasi-Unterlagen in Frage gestellt, Kopien von Stasi-Unterlagen, die beim Staatssicherheitsdienst entstanden sind, als Stasi-Unterlagen anzusehen, Kopien, die durch andere Stellen hergestellt sind, aber nicht. Mit der Gesetzesänderung ist es zwar beim herkömmlichen Verständnis des Begriffs der Stasi-Unterlagen geblieben. Die ohnehin schon bestehende Pflicht, auch Duplikate an den BStU herauszugeben (§§ 8 Abs. 1 und 9 Abs. 2 StUG) ist durch entsprechende Anzeigepflichten ergänzt worden (in § 7 Abs. 1 und Abs. 3 StUG), die sich bislang nur auf Originalunterlagen bezogen: Der BStU erhält danach Kenntnis vom Vorhandensein auch von Duplikaten und kann somit deren Herausgabe verlangen.

3.6.2 Kontrolle und Beratung des BStU und seiner Außenstellen

Im Berichtszeitraum habe ich wieder sowohl die Zentrale des BStU in Berlin als auch mehrere Außenstellen beraten und kontrolliert.

Erfreulicherweise hat sich die räumliche wie die personelle Situation des BStU erheblich verbessert, so daß auch die äußere Sicherung der Unterlagen deutlich erhöht wurde. Durch zusätzliches Personal konnten weitere Unterlagen erschlossen werden.

In der Behörde des BStU wird den Belangen des Datenschutzes große Bedeutung zugemessen. Meine im 14. Tätigkeitsbericht (S. 38 ff.) dargestellten Empfehlungen wurden umgesetzt.

Eine Thematik, die mich während meiner Kontrollen wiederholt beschäftigt hat, ist die erforderliche Trennung der Sachgebiete „Verwendung von Stasi-Unterlagen" und „Archivwesen" innerhalb der Zentrale und der Außenstellen. Mir kommt es darauf an, daß die Mitarbeiter des Archivs nicht mehr personenbezogene Daten, z. B. des Akteneinsicht begehrenden Antragstellers, zur Kenntnis erhalten, als sie zur Recherche im Archiv benötigen. Umgekehrt muß ausgeschlossen werden, daß sich Mitarbeiter der Fachbereiche „Akteneinsicht" und „Auskünfte an öffentliche und nicht-öffentliche Stellen" im Archiv bei den Karteikarten oder Akten „selbst bedienen". Der BStU teilt meine Auffassung und hat entsprechend meinen Empfehlungen die strikte Trennung durch eine Reihe organisatorischer Maßnahmen sichergestellt.

Seiner sog. Nachberichtspflicht gemäß § 4 Abs. 3 StUG, nach der erteilte Auskünfte berichtigt werden müssen, die sich z. B. durch das Auffinden neuer Unterlagen im nachhinein als unrichtig erweisen, konnte der BStU auch bis heute u. a. aus technischen und organisatorischen Gründen nur in äußerst geringem Umfang nachkommen. Der Plan, eine automatisiert geführte Datei „Nachrecherche" aufzubauen, wurde mittlerweile fallengelassen. Dafür wurde die Datei „Elektronisches Personenregister" (EPR) eingerichtet. EPR führt zwei verschiedene Datenbestände zusammen: Bei den Datenbeständen handelt es sich zum einen um die Daten aus mehr als 80 dezentralen Einzelkarteien, die in den Dienststellen des ehemaligen Staatssicherheitsdienstes angelegt wurden und aufgrund ihrer Vielzahl und Größe bisher

kaum für Recherchen genutzt werden konnten. Zum anderen werden die Personendaten in das EPR eingegeben, die bei der Erschließung der in den MfS-Diensteinheiten aufgefundenen Aktenbestände ermittelt werden. Das Verfahren EPR ist so angelegt, daß der gesamte Datenbestand auch für nachträgliche Abgleiche mit den Daten der bereits beauskunfteten und registrierten Personen genutzt werden kann. Ich begrüße dieses Konzept des BStU, weil er damit seiner Nachberichtspflicht besser nachkommen kann.

Ein anderes Problem im Zusammenhang mit der Nachberichtspflicht ist, daß zwischen Erstauskunft und dem Erschließen neuer Unterlagen, was zu einer Nachberichtigung führen kann, oft ein längerer Zeitraum liegt. So haben sich mehrere Bürger beklagt, daß trotz eines Wechsels des Arbeitsplatzes Nachberichtigungen vom BStU dem früheren Arbeitgeber erteilt wurden. Ich habe dem BStU daher dringend empfohlen, vor der Übermittlung einer berichtigten Auskunft an den Empfänger der Erstübermittlung bei diesem anzufragen, ob ein Informationserfordernis weiterhin besteht oder durch Zeitablauf inzwischen erledigt ist. Der BStU hat mir zugesagt, zukünftig so zu verfahren.

3.6.3 Unzulässig: Verpflichtung zur sog. Selbstauskunft

Die Luftfahrtbehörden können nach § 29 d des Luftverkehrsgesetzes (LuftVG) die Zuverlässigkeit von dort näher bezeichneten Personen mit deren Zustimmung überprüfen. Die Vorschrift gilt für jeden, der Zugang zu sicherheitsempfindlichen Bereichen und Anlagen hat oder dem es als Angehöriger von Flugplatz- und Luftfahrtunternehmen möglich ist, die Sicherheit des Luftverkehrs zu beeinträchtigen. Von einem Landesbeauftragten für den Datenschutz bin ich darauf aufmerksam gemacht worden, daß im zuständigen Landesministerium die Auffassung bestand, daß die Zuverlässigkeitsüberprüfung nach dem Verkehrsgesetz nicht als eine Überprüfung im Sinne der §§ 20 und 21 jeweils Absatz 1 Nr. 6 g StUG für Zwecke einer Sicherheitsüberprüfung verstanden werden könne. Das Ministerium hatte deshalb ein Formular entwickelt, das den Arbeitnehmer verpflichtete, eine „Selbstauskunft" beim Bundesbeauftragten für die Stasi-Unterlagen einzuholen: Er sollte sich verpflichten, „unverzüglich bei der Behörde Gauck gemäß § 3 i.V.m. §§ 12, 16 StUG im Rahmen des § 6 Abs. 4 StUG Auskunft zu erbitten" und diese „seinem Arbeitgeber unverzüglich vorzulegen".

Ich habe darauf hingewiesen, daß das Stasi-Unterlagen-Gesetz die Verwendung von Stasi-Unterlagen für Zwecke öffentlicher und nicht-öffentlicher Stellen in den §§ 19 ff. und 32 ff. abschließend regelt und das Verfahren der „Selbstauskunft" als unzulässige Gesetzesumgehung gekennzeichnet. Dem Bundesbeauftragten für die Stasi-Unterlagen habe ich empfohlen, Anträge auf Selbstauskunft, die erkennbar diesem Zwecke dienen, unter Gesichtspunkten des Mißbrauchs abzulehnen.

Inzwischen hat sich die Auffassung durchgesetzt, daß die §§ 20 und 21 jeweils Abs. 1 Nr. 6 g StUG auf die genannte Überprüfung nach dem Luftverkehrsgesetz – ebenso wie bezüglich der Überprüfung nach § 12 b Atomgesetz – anwendbar sind. Ich habe mich mit Erfolg dafür eingesetzt, in der Zuverlässigkeitsüberprüfungsverordnung zum Luftverkehrsgesetz klarzustellen, daß eine Regelanfrage beim BStU nicht stattfindet, die Luftfahrtbehörde ein Auskunftsersuchen vielmehr nur dann stellt, „wenn dies für die Beurteilung der Zuverlässigkeit erforderlich ist". Abfragen sollen also nur dann erfolgen, wenn es wahrscheinlich ist, daß das Ergebnis der Abfrage zur Beurteilung der Zuverlässigkeit beitragen kann. Hierbei ist auch das spezifische Sicherheitsrisiko, das sich im Hinblick auf den späteren Einsatz- und Verantwortungsbereich ergibt, zu berücksichtigen. Durch den Verzicht auf eine generelle Abfrage werden Anfragen über Personen vermieden, bei denen z. B. aufgrund ihres Lebenslaufes oder Lebensalters keine Angaben in den Unterlagen bei der Gauck-Behörde zu erwarten sind.

Für verkehrsrechtliche und für atomrechtliche Überprüfungen dürfte sich die sogenannte Selbstauskunft somit auch mangels Bedarfs erledigt haben. Wichtig bleibt mir aber der allgemeine datenschutzrechtliche Hinweis, daß – bei allem Respekt vor möglichen Informationsanliegen öffentlicher und nicht-öffentlicher Stellen – das Stasi-Unterlagen-Gesetz die Verwendung von Stasi-Unterlagen nur für in diesem Gesetz abschließend bestimmte Zwecke zugelassen hat und diese Grenzlinie nicht durch die „Verpflichtung zur Selbstauskunft" überschritten werden darf. Dieses Prinzip gilt auch nach dem Bundeszentralregistergesetz für die Verwendung unbeschränkter Auskünfte (§§ 42 Abs. 1 i. V. m. 41 Abs. 1 BZRG) und auch für das neue Ausländerzentralregistergesetz (§§ 15 ff. AZRG). Die vorliegende Problematik gibt daher Anlaß, es generell in Erinnerung zu bringen.

3.7 Ordensangelegenheiten – Datenerhebung ohne Mitwirkung des Betroffenen

Vor einer Entscheidung über die Verleihung von Orden und Ehrenzeichen der Bundesrepublik Deutschland werden personenbezogene Daten des Betroffenen in einem nicht unerheblichen Umfang erhoben und verarbeitet, worauf auch die Landesbeauftragten für den Datenschutz hingewiesen haben. Hierfür gibt es in dem einschlägigen Gesetz über Titel, Orden und Ehrenzeichen vom 26. Juli 1957 keine ausreichende Rechtsgrundlage.

Vor dem Vorschlag einer Ordensverleihung wird regelmäßig die Ordenswürdigkeit des Betroffenen geprüft. Dies bedeutet z. B. für Beschäftigte im öffentlichen Dienst, daß die Personalakte vom Dienstherrn mit Blick auf diese Eigenschaft ausgewertet wird. Aber auch soweit es sich nicht um Beschäftigte im öffentlichen Dienst handelt, werden von der vorschlagsberechtigten Behörde eine Vielzahl von personenbezogenen Daten bei Dritten erhoben. Der Dienstvorgesetzte oder der Arbeitgeber werden aufgefordert, eine allgemeine Stellungnahme über den Betroffenen abzugeben. Regelmäßig wird ein Aus-

zug aus dem Bundeszentralregister über den Betroffenen eingeholt, denn eine Verurteilung wegen eines Verbrechens schließt eine Auszeichnung mit dem Verdienstorden aus. Außerdem werden in der Praxis oft Auskünfte vom Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR, ggf. beim Document-Center in Berlin sowie bei den Verfassungsschutzämtern oder beim Bundesnachrichtendienst herangezogen. Auch Befragungen in der Nachbarschaft durch die vorschlagsberechtigte Behörde sind nicht ausgeschlossen. Kommt sie zu dem Ergebnis, daß der Betroffene ordenswürdig ist, schlägt sie ihn zur Verleihung eines Verdienstordens dem Chef des Bundespräsidialamtes vor. Der Bundespräsident entscheidet letztendlich, ob diesem Vorschlag entsprochen wird.

Erst jetzt erfährt der Betroffene davon, daß ihm ein Verdienstorden der Bundesrepublik Deutschland verliehen werden soll. Allerdings erfährt er nicht, welche personenbezogene Daten über ihn wann, von wem und bei welcher Stelle im Vorfeld der avisierten Ordensverleihung erhoben worden sind.

Ich halte diese Verfahrensweise bei der Vorbereitung der Ordensverleihung in mehrfacher Hinsicht für datenschutzrechtlich bedenklich. Das geschilderte Verfahren entspricht insgesamt nicht den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Grundsätzen zur informationellen Selbstbestimmung. Hiernach muß ein Betroffener nachvollziehen können, welche Daten bei welchen Stellen zu welchem Zweck über ihn erhoben wurden. Doch weder bei der Vorbereitung der Ordensverleihung noch danach wird dies dem Betroffenen mitgeteilt. Auch mit Blick auf die Möglichkeit, daß der Betroffene den Orden oder die Auszeichnung gar nicht entgegennehmen will, halte ich die Datenerhebung bei den verschiedensten Stellen und die damit verbundene Vorratsdatenhaltung ohne vorherige Information des Betroffenen für nicht zulässig. Ich bin der Auffassung, daß Personalaktendaten von Beamten auf der Grundlage von § 90 d Abs. 1 Bundesbeamtengesetz an den Chef des Bundespräsidialamtes nicht weitergegeben werden dürfen. Aus diesem Grunde befürworte ich ein Verfahren, bei dem der Betroffene vor Einleitung des Vorschlagverfahrens zu den beabsichtigten Datenerhebungen um seine Einwilligung gefragt wird. Ich verkenne nicht, daß hierdurch ggf. Erwartungen geweckt werden, die eventuell nicht erfüllt werden.

Ich habe dem Bundesministerium des Innern empfohlen, eine bereichspezifische Regelung in das Ordensgesetz aufzunehmen, wonach der Betroffene vor Beginn des Ordensvergabeverfahrens über Art und Umfang der Datenerhebung ausführlich informiert wird. Der Beginn des Verfahrens sollte von der Einwilligung des Betroffenen abhängig gemacht werden. Das Bundesministerium des Innern hat mir geantwortet, es halte die Aufnahme einer bereichsspezifischen Datenschutzregelung in das Gesetz über Titel, Orden und Ehrenzeichen für nicht erforderlich. Ich halte bei diesem Diskussionsstand eine politische Entscheidung für notwendig.

3.8 Probleme bei der Herstellung von Personalausweisen und Pässen

Die Bundesdruckerei – bislang eine nachgeordnete Behörde des Bundesministeriums für Post und Telekommunikation – wurde mit Wirkung vom 1. Juli 1994 in eine Gesellschaft mit beschränkter Haftung umgewandelt, deren Anteile zu 100% der Bundesrepublik Deutschland gehören. Aufgrund dieser Besitzverhältnisse und nach § 2 Abs. 1 und 3 i.V. m. §§ 24 Abs. 1 und 26 Abs. 3 BDSG bin ich für die datenschutzrechtliche Kontrolle und Beratung der Bundesdruckerei auch weiterhin zuständig. Das BMPT teilt diese Auffassung bisher leider nicht.

Im Rahmen meiner Tätigkeit bin ich auf folgende Probleme gestoßen:

- Bereits früher (11. TB S. 17f., 12. TB S. 23f.) habe ich kritisiert, daß die Bundesdruckerei von den Paßbehörden Anträge zur Herstellung von Pässen erhält, die neben den zur Herstellung der fälschungssicheren Paßkarte erforderlichen personenbezogenen Daten auch solche Daten enthalten, die auf den Seiten 1 bis 3 des Reisepasses eingetragen werden. Hierbei handelt es sich sowohl um Wohnort, Größe, Augenfarbe und eventuelle Ordens- oder Künstlernamen des Antragstellers als auch um die Daten von Kindern unter 16 Jahren, die auf Wunsch des Antragstellers in den Paß eingetragen werden können. Diese Daten mußten bislang von den Paßbehörden selbst in die Seiten 1 bis 3 des Reisepasses eingetragen werden, da die Bundesdruckerei dazu technisch nicht in der Lage war. Sie erhielt also mehr Daten, als sie zur Herstellung des Dokuments benötigte. Seit April 1993 kann die Bundesdruckerei nunmehr technisch die Beschriftung der Seiten 1 bis 3 des Reisepasses bei der Paßherstellung selbst vornehmen. Sie bietet dies den Paßbehörden als „zusätzliche Serviceleistung" an. Dabei stellt sich die grundsätzliche Frage, mit welchen Daten die Bundesdruckerei verpflichtet ist, den Paß herzustellen. Nach meinem Verständnis des § 16 Abs. 3 des Paßgesetzes bezieht sich die Herstellungspflicht der Bundesdruckerei jedenfalls auf die in § 4 Abs. 1 und 2 dieses Gesetzes genannten Daten, zu denen auch die eben genannten – auf Seite 1 des Reisepasses einzutragenden – Daten über Größe, Wohnort, Augenfarbe und eventuelle Ordens- oder Künstlernamen zählen. Eine Wahlmöglichkeit eröffnet § 4 Abs. 3 des Paßgesetzes nur bezüglich der Daten von Kindern unter 16 Jahren. Nur insofern kann von einer „Serviceleistung" der Bundesdruckerei die Rede sein und nur dann, wenn diese Serviceleistung in Anspruch genommen wird, dürfen die Daten von Kindern von der Paßbehörde an die Bundesdruckerei übermittelt werden.

  Ich habe der Bundesdruckerei nachdrücklich empfohlen, ihrer Herstellungspflicht vollständig zu genügen.

- Schon im Februar 1993 habe ich die Bundesdruckerei zu ihrer Absicht beraten, den Ausweisbehörden eine zentrale Vernichtung ungültig gewordener Personaldokumente anzubieten. Seit Oktober 1993 können diejenigen Behörden, die an diesem

Verfahren teilnehmen wollen, bei der Bundesdruckerei spezielle Versandtaschen bestellen, die dem Transport der zu vernichtenden Personaldokumente dienen. Wie ich im September 1994 festgestellt habe, waren diese Taschen, die der Bundesdruckerei in großem Umfang als selbständige Postsendungen zugeschickt wurden, bei ihrem Eingang in der Bundesdruckerei vielfach erheblich beschädigt. Bei einer Stichprobe konnte ich aus einer solchen Versandtasche – ohne den Klebeverschluß zu öffnen – deren Inhalt mit unentwerteten noch gültigen DDR-Personalausweisen entnehmen. Ich habe weiter festgestellt, daß auch bei unbeschädigten Versandtaschen Dokumente problemlos und ohne Spuren zu hinterlassen entnommen werden konnten, da der Klebeverschluß leicht zu öffnen und ebenso leicht wieder zu verschließen war. Eine weitere Stichprobe ergab, daß in einer Versandtasche neben der überwiegenden Zahl von entwerteten Personaldokumenten auch ein nicht entwerteter noch gültiger maschinenlesbarer Personalausweis enthalten war.

Ich habe der Bundesdruckerei unter Hinweis auf ihre Verpflichtung zu Maßnahmen der Datensicherheit (§ 9 BDSG) dringend empfohlen, das derzeit praktizierte Verfahren entweder sofort einzustellen oder derart zu ändern, daß die Ausweisbehörden der Bundesdruckerei nur entwertete Personaldokumente zur Vernichtung zusenden dürfen. Der Transport der Versandtaschen sollte nur in den Plastiktaschen erfolgen, die sich seit Jahren beim Versand der Ausweisunterlagen als sicher bewährt haben.

Die Bundesdruckerei ist meinen Empfehlungen gefolgt: Ich werde die Wirksamkeit des geänderten Verfahrens weiter kontrollieren.

3.9 Kontaktpflegedateien und APC-Sicherheit bei Auslandsvertretungen

Die deutschen Auslandsvertretungen erheben zur Erfüllung der ihnen mit Art. 3 des Wiener Übereinkommens über diplomatische Beziehungen (WÜD) und Art. 5 des Wiener Übereinkommens über konsularische Beziehungen (WÜK) übertragenen Aufgaben Daten zu Personen, mit denen dienstlicher Kontakt hergestellt und gepflegt wird. Die Angaben werden in sogenannten **Kontaktpflegedateien** gespeichert. Für eine automatisierte Verarbeitung dieser Daten hat das Auswärtige Amt das DV-Programm PERsonenbezogenes DateienSYstem (PERSY) entwickelt und den Auslandsvertretungen zur Verfügung gestellt. Anläßlich eines früheren Beratungs- und Kontrollbesuchs bei einer Auslandsvertretung hatte ich dem Auswärtigen Amt empfohlen, das PERSY-Programm nachzubessern. Insbesondere ging es mir damals darum, den Katalog der personenbezogenen Daten auf das zur Aufgabenerfüllung erforderliche Maß zu beschränken. Dies sollte bevorzugt in der Weise geschehen, daß darüber hinausgehende Angaben schon beim Eingabeversuch vom Programm zurückgewiesen werden oder – wo das nicht möglich ist (z. B. bei sog. Freitextfeldern) – möglichst genau vorgegeben wird, welche Informationen zu den Kontaktpersonen gespeichert werden dürfen.

Das Auswärtige Amt hat das PERSY-Programm zur Version 2.0 weiterentwickelt und die Auslandsvertretungen im August 1993 damit ausgestattet. Meine Vorschläge zur Verbesserung des Datenschutzes sind darin zum großen Teil berücksichtigt worden, so daß die Auslandsvertretungen für ihre Kontaktpflegedateien nunmehr über ein DV-Programm verfügen, das datenschutzrechtlichen Anforderungen entspricht.

In meinem 14. Tätigkeitsbericht (S. 15, 45) hatte ich **Sicherheitsmängel beim Einsatz von Arbeitsplatzcomputern** (APC) in Auslandsvertretungen beanstandet. Das Auswärtige Amt hatte die von mir geforderten zusätzlichen Sicherheitsmaßnahmen zunächst als zu aufwendig und unverhältnismäßig angesehen. Inzwischen hat es mir mitgeteilt, daß die wenigen noch im Einsatz befindlichen APC älterer Bauart ohne ausreichenden Zugangsschutz – wo erforderlich – mit einigen Sicherheitskomponenten nachgerüstet worden seien und im übrigen nicht mehr für eine Verarbeitung personenbezogener Daten verwendet würden.

4 Rechtswesen

4.1 Verbrechensbekämpfungsgesetz

4.1.1 Erfolgskontrolle von polizeilichen Befugnissen

Am 1. Dezember 1994 ist das **Verbrechensbekämpfungsgesetz** in Kraft getreten. Kaum hatte es im Vermittlungsausschuß seine endgültige Textfassung erhalten, wurde schon gefordert, in der neuen Legislaturperiode ein „Verbrechensbekämpfungsgesetz II" zu schaffen. Das Ergebnis der Bemühungen im Vermittlungsausschuß sei lediglich eine Richtungsangabe und ein Einstieg, auch das Abhören mutmaßlicher Gangsterwohnungen müsse ermöglicht werden. Ich wiederhole hierzu meine in meinem 14. Tätigkeitsbericht (S. 47 f.) abgegebene Stellungnahme. Aufgrund der bisherigen Erfahrungen auch mit der Telefonüberwachung weise ich darauf hin: Der Lauschangriff auf die Wohnung – das durch die Menschenwürde geschützte private Refugium eines Menschen – trifft in der weit überwiegenden Mehrzahl unschuldige Bürger.

Mit Blick auf die in jüngster Zeit in Kraft getretenen Gesetze, wie **das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität** (OrgKG), das Geldwäschegesetz und das Verbrechensbekämpfungsgesetz appelliere ich erneut an den Gesetzgeber, keine weiteren offenen oder verdeckten Überwachungsmöglichkeiten und Meldepflichten zum Zwecke der Durchsetzung des staatliches Strafanspruchs zu schaffen. Zunächst einmal müssen mit dem neu geschaffenen gesetzlichen Instrumentarium Erfahrungen gesammelt werden. Das vorhandene Instrumentarium muß erst erprobt werden, ehe durch immer neue Forderungen das Recht auf informationelle Selbstbestimmung weiter eingeschränkt wird.

In diesem Zusammenhang bin ich Äußerungen nachgegangen, daß die Erwartungen sich nicht erfüllt hätten, die sich an das Instrument der Rasterfahndung (§§ 98 aff. StPO) geknüpft haben, und von dieser Eingriffsmöglichkeit zunehmend weniger Gebrauch gemacht werde. Auf meine Frage nach konkreteren Erfahrungen und auch zahlenmäßigen Angaben hat das Bundesministerium der Justiz auf die Grenzen seiner Zuständigkeiten und Möglichkeiten hingewiesen. Ähnliche Hinweise auf die Schwierigkeit „gesonderter Erhebungen seitens der Landesjustizverwaltungen" und deren Aufwand mit Blick auf die ohnehin bestehende starke Belastung der Staatsanwaltschaften und Gerichte finden sich auch in Antworten der Bundesregierung über den Einsatz anderer besonderer strafprozessualer Ermittlungsbefugnisse, wie z. B. die Telefonüberwachung und deren Ergebnisse (vgl. z. B. BT-Drs. 12/8306 vom 20. Juli 1994).

Das bisherige Wissen darüber ist lückenhaft und unzureichend. Auch wenn einzuräumen ist, daß Ermittlungserfolge oft nicht monokausal auf den Einsatz einzelner Ermittlungsinstrumente, vielmehr auf das Zusammenspiel unterschiedlicher Maßnahmen zurückzuführen sind, sollten sich Gesetzgeber wie auch Rechtsanwender in diesem sensiblen Bereich einer Erfolgskontrolle stellen. Dies gilt für den Erhalt bestehender und die Schaffung neuer Eingriffsbefugnisse ebenso wie für die Rechtsanwendung im Einzelfall.

Nach der Strafprozeßordnung darf ein Telefon für Zwecke der Strafverfolgung überwacht werden (§ 100a StPO). Das Gesetz nennt die Straftaten, die eine solche Überwachung rechtfertigen. Dieser Straftatenkatalog ist erweitert worden, z. B. um Schlepperkriminalität.

Mit Nachdruck hatte ich gefordert, die Strafprozeßordnung um vertrauensbildende Maßnahmen zu ergänzen, um andererseits das Persönlichkeitsrecht für einen notwendigen Ausgleich zu stärken. Solche vertrauensbildenden Maßnahmen könnten sein:

- Jährliche Berichterstattung an den Deutschen Bundestag über Anlaß, Verlauf und Ergebnisse der Telefonüberwachung: Hierzu gehört z. B. wieviele Personen betroffen waren, wieviele Strafverfahren eingeleitet und wieviele Gespräche überwacht/mitgehört wurden.
- Verbesserung des Verfahrens der richterlichen Anordnung: Aus meiner Sicht müßte insbesondere die Zustimmung zur Maßnahme umfassend begründet werden. Ebenso sollten z. B. nur bestimmte Richter über den Antrag auf Überwachung entscheiden, so daß die Verantwortung bis zum Schluß der Maßnahme an diesen Richter gebunden bleibt.

Diese Vorschläge tragen dazu bei, Vertrauen in staatliche Eingriffsmaßnahmen zu schaffen, und sind auch geeignet, den Erfolg dieser Eingriffe nachzuweisen.

Zu Fragen der Erfolgskontrolle bei der Wahrnehmung polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26./27. September 1994 den Beschluß „Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen" gefaßt (Anlage 9).

4.1.2 Länderübergreifendes staatsanwaltschaftliches Verfahrensregister

Mit dem Verbrechensbekämpfungsgesetz wurden auch Regelungen für ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister beim Generalbundesanwalt als Registerbehörde (§§ 474 ff. StPO) geschaffen.

Dieses Register stellt in gewisser Weise eine Ergänzung zum Bundeszentralregister dar: Werden dort hauptsächlich rechtskräftige Verurteilungen gespeichert, so sollen in das neue Register Daten eingetragen werden, die für die Staatsanwaltschaften im Ermittlungsverfahren und während eines laufenden Gerichtsverfahrens von Bedeutung sein können. Dabei handelt es sich um die Personendaten des Beschuldigten und, soweit erforderlich, andere zur Identifizierung geeignete Merkmale (wie etwa besondere körperliche Merkmale und unveränderliche Kennzeichen – siehe hierzu näheres Nr. 4.2.2 –), die zuständige Stelle und das Aktenzeichen, die Tatzeiten, die Tatvorwürfe durch Angabe der gesetzlichen Vorschriften und die nähere Bezeichnung der Straftaten, die Einleitung des Verfahrens sowie Verfahrenserledigungen bei der Staatsanwaltschaft und bei Gericht nebst Angabe der gesetzlichen Vorschriften. Diese Daten dürfen nur für Strafverfahren gespeichert und verändert werden. Auskünfte aus dem Verfahrensregister dürfen nur Strafverfolgungsbehörden für Zwecke eines Strafverfahrens erteilt werden.

Die Konzeption des neuen Verfahrensregisters habe ich grundsätzlich unterstützt. Es soll die Ermittlung überörtlicher Täter und die Prüfung der Haftvoraussetzungen insbesondere wegen Wiederholungsgefahr erleichtern. Darüber hinaus soll es dazu beitragen, Doppelverfahren zu vermeiden, Sammelverfahren frühzeitig zu bilden, zuverlässige Grundlagen für Verfahrenseinstellungen zu schaffen und gerichtliche Entscheidungen in allen Verfahrensstadien sachgerecht vorzubereiten. Dadurch sollen unnötige Belastungen von Beschuldigten durch unkoordinierte Strafverfolgung vermieden werden. Problematisch ist jedoch der konzeptionelle Ansatz, die Daten des Betroffenen auch bei einem rechtskräftigen Freispruch oder einer Verfahrenseinstellung mangels hinreichenden Tatverdachts mindestens zwei Jahre zu speichern (§ 476 Abs. 2 StPO); siehe hierzu den Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 „Informationsverarbeitung im Strafverfahren" (Anlage 8). Bei der Beobachtung der Erfahrungen mit dem Verbrechensbekämpfungsgesetz (vgl. oben Nr. 4.1.1) sollte dieser Punkt besondere Aufmerksamkeit finden.

Bereits im Vorfeld des Gesetzgebungsverfahrens habe ich gegenüber dem Bundesministerium der Justiz wiederholt deutlich gemacht, daß Spontanmitteilungen, d. h. Datenübermittlungen seitens der Register-

behörde an Staatsanwaltschaften ohne entsprechendes Ersuchen der Staatsanwaltschaften, in bezug auf ihre Erforderlichkeit kritischer Prüfung und gesetzgeberischer Entscheidung bedürfen. Dies ist besonders wichtig, da bei Mitteilungen auf Ersuchen – im Gegensatz zu Spontanmitteilungen – die Erforderlichkeit einer Anfrage durch die anfragende Stelle überprüft wird. Der Spontanmitteilung kommt mithin eine andere Eingriffsqualität als der Mitteilung auf Ersuchen zu.

In einer Reihe von Rechtsetzungsmaßnahmen ist die Bedeutung dieser Unterscheidung erkannt und mit deutlicher Unterstützung durch das Bundesministerium der Justiz weiter ausgebaut worden. Als Beispiele nenne ich die ausdrückliche Regelung der Zulässigkeit von Spontanmitteilungen als Sonderfall im Stasi-Unterlagen-Gesetz sowie Regelungen im Ausländergesetz, die diese Differenzierung ebenfalls enthalten. Entsprechendes gilt auch für die Regelungen im Ausländerzentralregister, wonach eine Übermittlung von Daten an die Registerbehörde eine *vorhergehende Abfrage* des Registers obligatorisch danach voraussetzt, ob im Register bereits ein Datensatz besteht.

Ich habe bei der Vorbereitung einer Errichtungsanordnung für das länderübergreifende staatsanwaltschaftliche Verfahrensregister das Bundesministerium der Justiz darauf hingewiesen, daß Spontanmitteilungen durch die Registerbehörde durch den Gesetzestext nicht gedeckt sind. Dies wird bereits durch die Verwendung des Begriffes „Auskunft" im neuen § 474 Abs. 3 Satz 2 StPO deutlich. Eine Auskunft setzt definitionsgemäß ein Ersuchen voraus. Das ergibt sich auch aus der Verwendung dieses Begriffes in anderen Vorschriften, etwa im Bundeszentralregistergesetz oder im Bundesverfassungsschutzgesetz.

Zu dem mir bei Redaktionsschluß vorliegenden Entwurf dieser Errichtungsanordnung habe ich u. a. empfohlen:

- Bezüglich der Regelungen über die Übermittlungsmedien bei der Übermittlung von der Registerbehörde an die Auskunftsempfänger habe ich wegen der vergleichbaren Problematik auf die Regelungen verwiesen, wie sie in der Verordnung zur Durchführung des Ausländerzentralregistergesetzes vorgesehen sind. Dies gilt z. B. auch für telefonische Auskünfte der Registerbehörde. Hier halte ich eine Formulierung für datenschutzrechtlich vertretbar, die fernmündliche Übermittlungen dann zuläßt, wenn die mit einer anderen Übermittlungsart verbundene zeitliche Verzögerung aus dringenden dienstlichen Gründen nicht vertretbar ist und die Registerbehörde sich zuvor über die Identität der ersuchenden Person und über deren Zugehörigkeit zur ersuchenden Strafverfolgungsbehörde Gewißheit verschafft hat.
- Bezüglich bislang fehlender Regelungen über die Medien, mit denen Daten an die Registerbehörde übermittelt werden, habe ich wegen der Verwendung maschinell verwertbarer Datenträger auf die vorgesehenen Verfahrensregelungen für das Ausländerzentralregister verwiesen.

4.2. Enttäuschte Erwartungen: Ausstehende datenschutzrechtliche Regelungen im Strafverfahrensbereich

4.2.1 Strafverfahrensänderungsgesetz u. a.

Der Schutz des Persönlichkeitsrechts durch strafverfahrensrechtliche Regelungen ist nach wie vor unzureichend. Dabei geht es nicht nur um die personenbezogenen Daten von „Gangstern" oder auch nur von Verdächtigen, sondern ebenso um Daten von Verbrechensopfern, Tatzeugen und Unbeteiligten, oft ermittelt unter Zeugniszwang und Eingriff in die Privatsphäre der Betroffenen. Beispiele hierfür sind medizinische und psychologische Gutachten sowie Abhörprotokolle aus Telefonüberwachungen. Es fehlen Regelungen über die Erteilung von Aktenauskünften und Akteneinsicht für Gerichte, Staatsanwaltschaften, Behörden und Privatpersonen sowie die Übermittlung von Erkenntnissen für wissenschaftliche Zwecke – Defizite, die keineswegs nur Beschuldigte, sondern, oft einschneidend, auch Opfer und Zeugen betreffen. Es fehlen Regelungen über die Fahndung, insbesondere die Fahndung in der Öffentlichkeit und durch Inanspruchnahme von Publikationsorganen, so z. B. zur Ermittlung des Aufenthalts eines Zeugen. Es fehlen – mit Blick auch auf minderjährige Opfer sowie auf jugendliche und heranwachsende Tatverdächtige – Regelungen über die Informationserteilung durch Strafverfolgungsorgane an die Presse. Es fehlen Regelungen über die längerfristige Observation – eine Maßnahme, die sich nicht nur gegen Beschuldigte, sondern auch gegen andere Personen richten kann. Immer noch fehlt ein Justizmitteilungsgesetz, das Antwort auf die Frage gibt, wann und in welchem Umfang Strafverfahrensdaten durch Spontanmitteilungen der Gerichte oder Staatsanwaltschaften einer Verwendung für andere Zwekke (z. B. für dienstrechtliche Entscheidungen) zugeführt werden dürfen (vgl. Nr. 4.10).

Die Bilanz meiner Bemühungen in diesem Bereich im Berichtszeitraum ist negativ wie im Rückblick auf die vergangene Legislaturperiode insgesamt. Es verstärkt sich der Eindruck, daß es schneller geht, zusätzliche Eingriffsbefugnisse für Staatsanwaltschaften und Polizei zu schaffen, daß es aber lange braucht, wenn es um die Rechte Betroffener auf sorgfältigen Umgang mit ihren oft sehr sensiblen personenbezogenen Daten geht. Dabei besteht über die Problemfelder, zu denen es auch wegen des Volkszählungsurteils des Bundesverfassungsgerichts dringender gesetzgeberischer Entscheidung bedarf, zwischen dem Bundesministerium der Justiz und mir weitestgehendes Einvernehmen. Woran es mit Blick auf die unter dem Arbeitstitel „Rest-StVÄG" (Regelungsinhalte eines Strafverfahrensänderungsgesetzes, die nicht schon durch das OrgKG oder das Verbrechensbekämpfungsgesetz eine gesetzgeberische Aussage gefunden haben) seit etwa Herbst 1991 laufenden Bemühungen bislang offenbar fehlte, ist, daß es bisher nicht gelungen ist, „die fortbestehenden Meinungsunterschiede in den sich schwierig und kompliziert gestaltenden Einzelabstimmungen zu überwinden und alsbald einen Regierungsentwurf vorzulegen". In diesem Appell an den Gesetzgeber sehe ich mich durch meine Kollegen in den Ländern

unterstützt. Im einzelnen nehme ich auf die als Anlagen 5 und 10 beigefügten einstimmigen Beschlüsse der Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit den Titeln „Informationsverarbeitung im Strafverfahren" und „Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz" Bezug.

Als Folge einer fehlenden Regelungsinitiative des Bundes sehe ich den vom Bundesrat am 14. Oktober 1994 beschlossenen Entwurf eines Strafverfahrensänderungsgesetzes 1994 (StVÄG 1994, BR-Drs. 620/94 vom 14. Juni 1994). Zur Einbringung dieses Entwurfs im Bundesrat hat es auch öffentliche Erklärungen von Landesbeauftragten für den Datenschutz gegeben. Ich teile die Hinweise auf die Erforderlichkeit neuer Impulse für die gesetzgeberischen Bemühungen zur Schaffung der dringend notwendigen bereichsspezifischen Regelungen des Datenschutzes im Strafverfahren. Ebenso bin ich der Auffassung, daß der Entwurf unter Gesichtspunkten des Datenschutzes gründlicher Überarbeitung und Nachbesserung bedarf.

4.2.2 Genomanalyse im Strafverfahren

Zu den datenschutzrechtlichen Enttäuschungen der zurückliegenden Legislaturperiode zählt, daß die unter Gesichtspunkten des Datenschutzes unerläßlichen Regelungen über den Einsatz gentechnischer Methoden im Strafverfahren nicht getroffen wurden. Für die neue Legislaturperiode hoffe ich, daß die für die Strafverfolgungsorgane sowie für die Betroffenen immer wichtiger werdende rechtliche Klarheit in dieser Frage geschaffen wird.

Dabei könnte an den früheren Gesetzentwurf der Bundesregierung Entwurf eines ... Strafverfahrensänderungsgesetzes – DNA-Analyse „genetischer Fingerabdruck" – BT-Drs. 12/7266 –, angeknüpft werden. Leider hat dieser in der Stellungnahme des Bundesrats (BR-Drs. 729/93 Beschluß – vom 26. November 1993) mehr datenschutzrechtliche Verschlechterungen als Verbesserungen erfahren.

Meine wichtigsten Empfehlungen zur Neufassung des Entwurfs sind:

- Zweckbindungs- und Vernichtungsregelungen sind nicht nur bezüglich des für die Untersuchung verwendeten Materials, sondern auch für deren Ergebnisse zu schaffen. Ein Hinweis – wie er sich in der früheren Entwurfsbegründung findet –, die Verwendung von Untersuchungsergebnissen in anderen als Strafverfahren sei grundsätzlich möglich, ist unzureichend. Dabei wird als „Untersuchungsergebnis" ganz offensichtlich mehr als die Antwort auf das Untersuchungsziel verstanden, mehr also als die durch Vergleich zweier Proben getroffene Schlußfolgerung über das Bestehen oder Nichtbestehen einer Abstammung oder der Erzeugung oder Nichterzeugung des Spurenmaterials durch den Beschuldigten oder den Verletzten. Gemeint ist vielmehr offenbar ein Untersuchungsbefund, der sich in einem Muster und/oder einer verformelten Aussage darstellt. Die Verwendung von in Akten befindlichen Untersuchungsergebnissen für andere als das „zugrunde liegende oder andere anhängige Strafverfahren" wird jedenfalls dann sehr problematisch, wenn man an die – offenbar im Fortschreiten begriffenen – Möglichkeiten der Digitalisierung der Untersuchungsergebnisse denkt. Diese Problematik steht im Mittelpunkt der Besorgnisse der Bürger, die sich hierzu äußern.

  Dies wird deutlich auch vor dem Hintergrund der Regelungen des Verbrechensbekämpfungsgesetzes über ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister, das in § 474 Abs. 2 Nr. 1 StPO vorsieht, im Register neben „Personendaten des Beschuldigten" auch „soweit erforderlich, andere zur Identifizierung geeignete Merkmale" zu speichern. Die zu schaffenden gesetzlichen Regelungen über die Genomanalyse im Strafverfahren müssen eine Antwort auf die Frage geben, ob hierzu auch genomanalytische Untersuchungsergebnisse zählen, und jedenfalls die Speicherung in anderen automatisierten Dateien als dem in § 474 StPO genannten Register ausschließen.

  Was die Verwendung in „anderen als Strafverfahren" anbelangt, so sollte eine Aussage hierzu ebenfalls nicht der Entwurfsbegründung überlassen werden. Soweit daran gedacht ist, die in den Akten des Strafverfahrens dokumentierten Ergebnisse einer mittels DNA-Analyse durchgeführten Abstammungsuntersuchung in einem Zivilrechtsstreit zu verwenden, sollte hierzu eine Aussage durch Rechtsnormen getroffen werden.

- Im Gegensatz zur bisherigen Stellungnahme des Bundesrates sollte an der im früheren Regierungsentwurf vorgesehenen Bestimmung des Sachverständigen durch schriftliche Anordnung des Richters festgehalten werden. Umso mehr dann, wenn auf eine normative Entscheidung über zulässige Methoden molekulargenetischer Untersuchungen wie auch auf die Bestimmung der jeweils anzuwendenden Methode durch richterliche Anordnung verzichtet wird, sehe ich hierin ein Minimum an verfahrensrechtlicher Sicherung.

  Zur organisatorischen Sicherung der vorgesehenen Verwendungsbeschränkungen sollten für die Untersuchung nur Amtsträger in Betracht kommen, die nicht der ermittlungsführenden Behörde oder einer Organisationseinheit angehören, die von der ermittlungsführenden Dienststelle organisatorisch und sachlich getrennt ist. In dieser Regelung des früheren Entwurfs sehe ich einen akzeptablen Kompromiß, der nicht in Frage gestellt werden sollte.

- Auch an der Vorstellung des früheren Regierungsentwurfs, daß das Untersuchungsverfahren anonymisiert, d. h. unter einer Code-Bezeichnung, zu laufen hat, sollte festgehalten werden. Ich sehe hierin ein unverzichtbares Element verfahrensrechtlicher Sicherheitsvorkehrungen. Die vom Bundesrat angestrebte Reduzierung auf lediglich eine „Teilanonymisierung" zum Zwecke einer „Plausibilitätskontrolle" durch den Sachverständigen ist mir nicht einleuchtend: Soll der Sachverständige z. B. vorläufige Erkenntnisse etwa über

einen Spurenfund bewerten und zum Maßstab für die Richtigkeit seines Untersuchungsergebnisses machen? Eine Erforderlichkeit für die Erfüllung seines Auftrages, nämlich die Antwort auf das Untersuchungsziel – die durch Vergleich zweier Proben getroffene bejahende oder verneinende Schlußfolgerung über das Bestehen oder Nichtbestehen einer Abstammung oder der Erzeugung oder Nichterzeugung des Spurenmaterials durch den Beschuldigten oder den Verletzten – vermag ich nicht zu erkennen.

Ich hoffe auf eine Entscheidung des Gesetzgebers in dieser Legislaturperiode.

4.3 Weitere Empfehlungen für den Persönlichkeitsschutz im Strafverfahren

Um das Persönlichkeitsrecht im Strafverfahren zu schützen, empfehle ich desweiteren folgende gesetzlichen Verbesserungen (siehe auch 14. TB S. 50):

a) Besserer Schutz personenbezogener Daten im Rahmen von Gerichtsverfahren

Nach § 174 Abs. 3 Gerichtsverfassungsgesetz kann das Gericht bei einer Verhandlung, die aus in diesem Gesetz näher bezeichneten Gründen (z. B. bei der Erörterung von Umständen aus dem persönlichen Lebensbereich eines Prozeßbeteiligten, sofern durch die öffentliche Erörterung überwiegende schutzwürdige Interessen verletzt würden) unter Ausschluß der Öffentlichkeit stattfindet, „den anwesenden Personen die Geheimhaltung von Tatsachen, die durch die Verhandlung oder durch ein die Sache betreffendes amtliches Schriftstück zu ihrer Kenntnis gelangen", durch Beschluß zur Pflicht machen. Unter „anwesenden Personen" sind insbesondere auch die Parteien und ihre Anwälte zu verstehen. Ein Verstoß gegen die auferlegte Geheimhaltungspflicht ist strafrechtlich sanktioniert (§ 353 d Ziffer 2 StGB). Diese Regelungen stellen sicher, daß der Ausschluß der Öffentlichkeit nicht im **nachhinein** dadurch unterlaufen wird, daß **nach** der Verhandlung die erörterten Umstände durch Weitergabe seitens eines der anwesenden Beteiligten nach außen dringen.

Zu dieser Thematik hat sich das Bayerische Staatsministerium der Justiz mit begrüßenswerten Vorschlägen an das Bundesministerium der Justiz gewandt, den Schutz des Persönlichkeitsrechts auf das **Vorfeld** der Verhandlung zu erweitern. Ich teile die Überzeugung, daß ein Bedürfnis besteht, die Regelung des § 174 Abs. 3 Gerichtsverfassungsgesetz auf diejenigen Fälle auszudehnen, in denen eine öffentliche Verhandlung **nicht stattfindet** und daher ein Ausschluß der Öffentlichkeit nicht in Betracht kommt. Vor dem Hintergrund mitunter spektakulärer Auftritte einzelner Rechtsanwälte noch vor Beginn der Verhandlung trete ich darüber hinaus dafür ein, daß die Schweigepflicht auch schon in einem Verfahrensstadium auferlegt werden kann, in dem es **noch nicht** zu einer mündlichen Verhandlung gekommen ist. Für die Wahrung des Persönlichkeitsrechts eines Prozeßbeteiligten kann es zu spät sein, wenn bei der mündlichen Verhandlung, in der z. B. ein über ihn erstelltes ärztliches Gutachten erörtert wird, die Öffentlichkeit ausgeschlossen und das Schweigegebot des § 174 Abs. 3 Gerichtsverfassungsgesetz erlassen wird. Denn schon zuvor ist das Gutachten dem jeweiligen Prozeßgegner bzw. dessen Prozeßbevollmächtigten in Wahrung des Rechts auf rechtliches Gehör und zur Vorbereitung der Verhandlung zugegangen.

Meinem Anliegen läßt sich mit geringem gesetzgeberischen Aufwand dadurch entsprechen, indem das zuständige Gericht die Möglichkeit erhält, das Schweigegebot unter den ansonsten gegebenen Voraussetzungen des § 174 Abs. 3 Gerichtsverfassungsgesetz auch dann zu erlassen, wenn im Falle einer mündlichen Verhandlung die Voraussetzungen für den Ausschluß der Öffentlichkeit gegeben wären. Das Erfordernis einer gerichtlichen Entscheidung im Einzelfall stellt sicher, daß die widerstreitenden Interessen jeweils konkret gegeneinander abgewogen werden können.

In Ergänzung dieser Erweiterung des § 174 Gerichtsverfassungsgesetz habe ich eine Strafbewehrung gesetzlicher Zweckbindungsregelungen angeregt. Dem liegt die aus Eingaben gewonnene Erkenntnis zugrunde, daß der Schutz der durch Akteneinsicht erlangten personenbezogenen Daten vor zweckwidriger Verwendung bisher nicht ausreicht. Dabei ist diese Problematik nicht allein auf Strafverfahren beschränkt. Ich habe vorgeschlagen, den Straftatbestand „Verbotene Mitteilungen über Gerichtsverhandlungen" (§ 353 d StGB) durch folgende Ziffer 4 zu ergänzen:

– Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer ... *„4. entgegen einer gesetzlichen Zweckbindungsregelung personenbezogene Daten, die ihm aus Akten oder Dateien des Gerichts, der Staatsanwaltschaft oder anderer Behörden zur Kenntnis gelangt sind, verwendet".*

Eine Antwort aus dem Bundesministerium der Justiz steht bislang noch aus.

b) Gleiche Bedingungen für die Zeugnisverweigerung und Beschlagnahmeverbote

Bei einer Kontrolle des Instituts für Wehrmedizinalstatistik und Berichtswesen bin ich auf Sachverhalte gestoßen, die aus meiner Sicht eine Überprüfung geltender Strafverfahrensvorschriften nahelegen: In einem Fall hatte eine Staatsanwaltschaft im Zusammenhang mit einem Banküberfall Blutgruppenunterlagen eines ehemaligen Soldaten beschlagnahmen wollen. Das Institut hatte sich geweigert, die Unterlagen herauszugeben. In einem anderen Fall, einem „Mordverdachtsfall", hatte ein Amtsgericht die Beschlagnahme von im Institut befindlichen medizinischen Dokumenten angeordnet. Unter Hinweis auf die Regelungen der Strafprozeßordnung wurde seitens des Instituts die Ansicht geäußert, im Institut gelagerte medizinische Dokumente würden der Beschlagnahme nicht unterliegen. Man ging davon aus, sich bei der Weigerung, in Strafverfahren medizinische

Unterlagen herauszugeben, auf die Wahrung des Arztgeheimnisses berufen zu können.

Nach meinem Verständnis stellt sich die Rechtslage für beide Fälle wie folgt dar: Anders als das Zeugnisverweigerungsrecht des § 53 StPO gelten die Beschlagnahmeverbote des § 97 StPO nur dann, wenn sich das Strafverfahren gerade gegen den Klienten/Patienten des Zeugnisverweigerungsberechtigten **als Beschuldigten** richtet. Eine allgemeine Freistellung von der Beschlagnahme, entsprechend dem allgemeinen Zeugnisverweigerungsrecht nach § 53 StPO, besteht nicht. Die Beschuldigteneigenschaft der an dem Vertrauensverhältnis als Klient/Patient beteiligten Person ist konstitutiv für das Eingreifen der Beschlagnahmeverbote des § 97 StPO. Nicht anwendbar ist § 97 StPO, wenn die Ermittlungen zunächst gegen Unbekannt geführt werden oder das Strafverfahren sich gegen Dritte richtet.

Dies bedeutet, daß in beiden Beispielsfällen die Beurteilung der Rechtmäßigkeit einer eventuellen Verweigerung der Herausgabe der Unterlagen davon abhing, ob es sich um Unterlagen von Beschuldigten handelte. In beiden Fällen aber hätten Mitarbeiter des Instituts in ihrer Eigenschaft als Ärzte sich ohne weiteres bei einer Vernehmung gegenüber der Staatsanwaltschaft und vor Gericht auf ihr Zeugnisverweigerungsrecht berufen können. Ich sehe hierin einen Wertungswiderspruch.

c) Fernmeldegeheimnis für Mail- und Voiceboxen?

Ein ständig an Bedeutung gewinnendes Problem ist die Frage der Beachtung des Fernmeldegeheimnisses durch staatliche Stellen im Rahmen von Hausdurchsuchungen bei Betreibern von Mail- und Voiceboxen. Tatsächlich hat die Verwendung von Mail- und Voiceboxen unterschiedlichster Ausgestaltung durch private, nicht-gewerbliche Betreiber deutlich zugenommen.

Hierbei geht es um folgendes: In Mailboxen werden elektronische Schriftstücke abgelegt, in Voiceboxen Sprache. Die Boxen sind Bestandteil von Computernetzen und über diese zugänglich. Der Kreis der Benutzer, die Zugang haben, ist unterschiedlich. Die Boxen können allen Benutzern zugänglich sein, dann sind sie öffentlich und erfüllen die Funktion eines schwarzen Brettes. Der Zugang kann aber auch auf Benutzergruppen oder gar einzelne Benutzer begrenzt sein; solche Boxen wirken dann wie Briefkästen. Ein Systemoperator legt nach den Wünschen des Inhabers der jeweiligen Box fest, welche anderen Benutzer Zugang haben. Darüber hinaus kontrolliert er stichprobenweise den Inhalt der Boxen.

Die datenschutzrechtliche Problematik beginnt hier bereits bei der notwendigen Klärung der Frage, ob und inwieweit es sich bei den hier stattfindenden Datenübermittlungen um Fernmeldeverkehr im Sinne der §§ 100a, 100b StPO handelt, um Datenübermittlungen also, deren Überwachung nur unter bestimmten, vom Gesetzgeber genau festgelegten Voraussetzungen zulässig ist. Aus meiner Sicht ist von besonderem Interesse, ob neben dem unmittelbaren Übermittlungsvorgang des Einlesens und Auslesens von Informationen in Mail- und Voiceboxen auch die dazwischenliegende Phase der Speicherung dieser Informationen in den Boxen als Fernmeldeverkehr anzusehen ist. Die erheblichen Auswirkungen der Beantwortung dieser Frage sowohl für Betreiber als auch für Nutzer derartiger Systeme sind offensichtlich.

Zu diesen gerade auch wegen der Vielgestaltigkeit der technisch möglichen Varianten noch weitgehend ungeklärten Rechtsfragen habe ich mit meinen Kollegen in den Ländern und mit dem Bundesministerium der Justiz Gespräche aufgenommen. Möglicherweise wird es schon aus Gründen der Rechtssicherheit unumgänglich sein, eine neue, normenklare und bereichsspezifische Regelung zu schaffen.

Bezüglich der technischen Aspekte der Mail- und Voiceboxen weise ich im übrigen auf Nr. 20.2.11 hin.

4.4 Bundeszentralregister

4.4.1 Das Bundeszentralregister und die Vorbereitung der Wahlen 1994

Ende 1993 ging mir der Entwurf der Fraktionen der CDU/CSU und F.D.P. zur Änderung des Bundeszentralregistergesetzes zu (3. BZRÄndG, Bundestagsdrucksache 12/6380). Ausgangsproblem war, daß in den Melderegistern der Gemeinden in den neuen Bundesländern Ausschlüsse vom Wahlrecht oder der Wählbarkeit nicht oder nur unvollständig vermerkt waren, so daß zu befürchten stand, die Wahlen 1994 ließen sich nicht ordnungsgemäß vorbereiten. Gemeinden der neuen Bundesländer haben daraufhin beim Bundeszentralregister Behördenführungszeugnisse für ihre wahlberechtigten Bürgerinnen und Bürger beantragt, um so die Wahlen vorbereiten und die Melderegister vervollständigen zu können. Dies wäre auf einen „flächendeckenden" Abgleich zwischen Melderegister und Bundeszentralregister hinausgelaufen. Mit Erlaß des Bundesministeriums der Justiz vom 5. Oktober 1993, von dem ich erst im Januar 1994 erfuhr, war die Erteilung derartiger Behördenführungszeugnisse durch den Generalbundesanwalt mit der Begründung gestoppt worden, § 31 Bundeszentralregistergesetz trage einen solchen Abgleich nicht.

Erhebliche Bedenken mußte ich aber gegen das Konzept des seinerzeitigen Regelungsentwurfs geltend machen:

- So war den Innenministerien der neuen Länder eine besondere Filterfunktion zugedacht. Ihnen sollten Zehntausende von sog. Positiv-Auskünften der Registerbehörde – d. h. Behördenführungszeugnisse mit Eintragungen über Vorstrafen – zugehen. Die Innenressorts benötigen die Zeugnisse in diesem Zusammenhang aber für ihre eigene Aufgabenerfüllung nicht. Auch befürchtete ich, daß angesichts der zu erwartenden Belastungen die Innenministerien ihre Filterfunktion auf die Kreisebene (Landratsämter) verlagern würden. Das Konzept, Auskunftsinhalte, die Wahlrecht oder

Wählbarkeit nicht betreffen, nicht der örtlichen Ebene bekanntwerden zu lassen, wäre damit vollends in Frage gestellt gewesen.

- Regelungstechnisch mangelhaft war auch die Entwurfsformulierung, nicht wahlrechtsrelevante Eintragungen seien „unkenntlich zu machen". Sie war so zu verstehen, daß nach der Übermittlung an die örtlichen Behörden in einem Führungszeugnis Angaben über Wahlrecht oder Wählbarkeit erkennbar geblieben, das Führungszeugnis aber mit allen anderen Angaben „geschwärzt" weitergereicht worden wäre.

Mit diesem Konzept hätten viele Stellen und Personen erfahren, ob es zu Wahlberechtigten Eintragungen im Bundeszentralregister gibt. Eine Kontrolle des ordnungsgemäßen Umgangs mit diesen Kenntnissen wäre m.E. nicht möglich gewesen.

Aufgrund auch der heftigen öffentlichen Diskussion wurde schließlich ein Gesetz verabschiedet, das datenschutzgerecht ist. Dabei wurden meine Verbesserungsvorschläge übernommen:

- Die Filterfunktion für **Auskünfte über das aktive Wahlrecht** wurde durch das Bundeszentralregister selbst wahrgenommen. Seine Auskunft beschränkte sich auf Eintragungen, aus denen sich lediglich ein Ausschluß der betroffenen Personen vom Wahlrecht ergibt (§ 69 BZRG).

- Dieses in bezug auf das aktive Wahlrecht formulierte datenschutzrechtliche Konzept hat sich allerdings nicht hinsichtlich der Wählbarkeit (passives Wahlrecht) verwirklichen lassen. Nach Erklärungen der Vertreter des Bundeszentralregisters bestand programmtechnisch keine Möglichkeit, Eintragungen, die sich nur auf die **Wählbarkeit** beziehen, lückenlos im Registerbestand zu erkennen. Die Mittlerfunktion der Innenressorts wurde aber auf die – relativ überschaubare – Zahl der Bewerber der Wahl des Jahres 1994 beschränkt. Ausdrücklich wurde festgelegt, daß die Innenministerien Führungszeugnisse nicht – auch nicht mit Schwärzungen – an die Meldebehörden weiterleiten durften. Den zuständigen Meldebehörden wurde nur der wählbarkeitsrelevante Eintrag mitgeteilt.

Die Einhaltung der Vorschriften dieses Gesetzes durch den Generalbundesanwalt – Dienststelle Bundeszentralregister – habe ich im Mai 1994 kontrolliert und mich durch eine Vielzahl von Stichproben davon überzeugt, daß die Registerbehörde den gesetzlichen Vorgaben entsprechend verfahren ist. Den hierbei von mir gegebenen Empfehlungen zur Erhöhung der Sicherheit bei der Übermittlung der Auskunftsersuchen und bei der Löschung der benutzten Magnetbänder ist die Registerbehörde gefolgt.

4.4.2 Novellierung des Bundeszentralregistergesetzes

Die beginnende neue Legislaturperiode gibt Anlaß, an die Notwendigkeit datenschutzrechtlicher Verbesserungen des Bundeszentralregistergesetzes zu erinnern. Der Deutsche Bundestag hat schon 1986 eine entsprechende Aufforderung an die Bundesregierung gerichtet (siehe auch 11. TB S. 19 f).

Insbesondere die geltende Fassung der §§ 41 Abs. 1 Nr. 2 und 43 BZRG und die hierauf gestützte Praxis bedürfen einer dringenden Überprüfung. Eine Datenübermittlung im überwiegenden Allgemeininteresse an eine oberste Bundes- oder Landesbehörde ist nicht erforderlich, wenn ihr nur der Umstand zugrunde liegt, daß das Gesetz einer nachgeordneten oder ihrer Aufsicht unterstehenden Behörde nicht die Möglichkeit einer unbeschränkten Auskunft durch den Generalbundesanwalt – Dienststelle Bundeszentralregister – gibt. Angesichts divergierender Rechtsauffassungen in der Praxis habe ich empfohlen, das Recht oberster Bundes- und Landesbehörden auf unbeschränkte Auskunft aus dem Bundeszentralregister nach § 41 Abs. 1 Nr. 2 BZRG ausdrücklich dahingehend zu beschränken, daß ein Auskunftsersuchen nur zur Erfüllung eigener Aufgaben zulässig ist, nicht aber zur Erfüllung von Aufgaben einer nachgeordneten oder ihrer Aufsicht unterstehenden Behörde. Hierbei bleibt die Frage unberührt, inwieweit die oberste Bundes- oder Landesbehörde eine einzelne Angelegenheit einer nachgeordneten Behörde im Rahmen der Rechts- oder Fachaufsicht zu einer eigenen Aufgabe machen kann. Schon auf der Basis des geltenden § 43 BZRG ausgeschlossen ist jedenfalls, daß eine oberste Bundes- oder Landesbehörde immer dann eine solche Auskunft zum Zwecke der Weitergabe einholt, wenn eine ihr nachgeordnete oder ihrer Aufsicht unterstehende Behörde eine bestimmte Aufgabe zu erfüllen hat, die ihrer Art nach sich wiederholt. Meine Empfehlung wird auch durch das in § 41 Abs. 4 BZRG betonte Prinzip der Zweckbindung unterstützt: Danach dürfen Daten auch nicht über Dritte beschafft werden, die mit dieser Aufgabe nichts zu tun haben. Meine Empfehlung muß zwangsläufig mit einer Prüfung der Erforderlichkeit einer Erweiterung des Kataloges des § 41 Abs. 1 BZRG zugunsten einzelner Behörden verbunden werden. So schließe ich z. B. nicht aus, daß bei der Vergabe von Spitzenfunktionen im Kredit- und Versicherungsgewerbe ein Führungszeugnis nicht immer ausreichen kann.

4.4.3 Identitätsfindung bei Anwendung des Bundeszentralregistergesetzes

Ein Schwerpunkt meiner Kontroll- und Beratungstätigkeit beim Generalbundesanwalt – Dienststelle Bundeszentralregister – war, wie zuverlässig die Identitätsfindung sowohl beim Speichern von im Register einzutragenden Informationen (§§ 3 ff. BZRG) als auch bei der Auskunftserteilung (§§ 30 ff., §§ 41, 42 BZRG) ist. Hierbei war eine zentrale Frage, inwieweit in den Massenverfahren der Registerbehörde diese Entscheidungen maschinell, d. h. ohne intellektuelle Mitwirkung eines Sachbearbeiters, getroffen werden können und dürfen.

a) Einspeichern einer Mitteilung

Das Datenbankprogramm der Registerbehörde bietet die Möglichkeit, eingehende Mitteilungen über Personen einem bereits vorhandenen Personendatensatz zuzuordnen oder einen neuen Personendatensatz anzulegen. Hierzu sind die drei Suchmerkmale Vorname, Geburtsname und Geburtsdatum zwingend vorgeschrieben. Diese Angaben werden in einem ersten Schritt phonetisch

verschlüsselt. Der Phonetik ist zusätzlich eine von der Registerbehörde eigens erstellte Vornamen-Tabelle vorangestellt; hier werden z. B. der Vorname „Josef" mit den Vornamen „Jupp" oder „Sepp" gleichgestellt. Die phonetische Verschlüsselung wird mit allen in der Datenbank bereits vorhandenen phonetischen Verschlüsselungen abgeglichen. Trifft eine Verschlüsselung auf eine bereits vorhandene identische in der Datenbank, wird in einem zweiten Schritt auf den gespeicherten, unverschlüsselten Datensatz zurückgegriffen. Der einzuspeichernde Datensatz wird dann mit dem gefundenen Datensatz auf Zeichenübereinstimmung verglichen. Dies bedeutet, daß der Geburtsname, mindestens ein Vorname sowie das Geburtsdatum exakt übereinstimmen müssen. Bei exakter Zeichenübereinstimmung wird die eingehende Mitteilung dem bestehenden Datensatz hinzugespeichert. Bei Abweichungen wird ein neuer Datensatz angelegt.

Sind in der einzuspeichernden Mitteilung und in dem gefundenen Datensatz mehr als die drei Mindestangaben vorhanden (wie z. B. Geburtsort oder Geburtsname der Mutter), werden auch diese auf Zeichengleichheit bzw. auf phonetischen Gleichklang verglichen. Auch hier steht für die Entscheidung auf Basis der Zeichengleichheit des Geburtsortes ein Unterprogramm zur Verfügung, welches z. B. den Ortsteil Bad Godesberg mit dem Ort Bonn gleichsetzt.

In einer Entscheidungstabelle hat die Registerbehörde Wertigkeiten für die exakte Zeichengleichheit und die phonetische Übereinstimmung festgelegt. Im Vergleich der einzelnen Datenfelder eines einzuspeichernden Datensatzes mit einem gefundenen Datensatz ergibt sich so eine Gesamtpunktzahl, die wiederum mit zwei Schwellenwerten verglichen wird, die aus Erfahrungswerten der Registerbehörde resultieren. Ergibt die Addition der einzelnen Werte eine größere Summe als der obere Schwellenwert, wird die einzuspeichernde Mitteilung automatisch dem bestehenden Datensatz zugespeichert. Bei einer geringeren Summe im Vergleich zu dem unteren Schwellenwert wird ein neuer Datensatz angelegt. Befindet sich die Gesamtpunktzahl zwischen beiden Stellenwerten, ist eine automatische Speicherung nicht möglich. Diese Fallkonstellationen müssen vom Sachbearbeiter individuell bearbeitet werden. Der Sachbearbeiter leitet Nachermittlungen bei der mitteilenden Stelle hinsichtlich der fehlenden oder unklaren Angaben ein, um zu einem späteren Zeitpunkt nach Antwort dieser Stelle den einzuspeichernden Datensatz einem bereits bestehenden zuzuführen oder einen neuen Datensatz anzulegen.

Das von der Registerbehörde verwendete Datenbankprogramm stellt nach meiner Bewertung eine ausreichende Sicherheit dafür dar, daß eine automatische Zusammenführung nur in solchen Fällen geschieht, in denen der Mensch bei Vorliegen der entsprechenden Angaben zu den Suchmerkmalen auch nicht anders als die Maschine entscheiden würde. Unbedenklich erscheinen mir auch die Fälle, in denen eine Zusammenführung ausgeschlossen und ein weiterer Datensatz neben dem bereits vorhandenen angelegt wird. Ich begrüße, daß in Zweifelsfällen die intellektuelle Entscheidung eines Sachbearbeiters und somit eine Identitätsentscheidung nur auf der Basis von Nachermittlungen bei der mitteilenden Stelle herbeigeführt wird.

b) Auskunftserteilung

Unter Gesichtspunkten des Datenschutzes steht die zuverlässige Identitätsfindung bei der Auskunftserteilung im Mittelpunkt der Aufgaben der Registerbehörde. Ich habe im Rahmen meiner Kontrolle festgestellt, daß die Anforderungen an eine bejahende Identitätsentscheidung bei der automatischen Auskunftserteilung noch höher sind als bei der automatischen Einspeicherung. Ähnlich wie beim Einspeichern eines Datensatzes werden zunächst die notwendigen Suchmerkmale gebildet und mit den in der Datenbank vorhandenen verglichen. Findet sich zu dem Anfragedatensatz mit seinen drei Mindestangaben – Vorname, Geburtsname, Geburtsdatum – in der Datenbank kein vergleichbarer Datensatz, erfolgt automatisch die sog. Negativ-Auskunft „kein Eintrag". Etwa zwei Drittel sämtlicher Anfragen führen zu einer Negativ-Auskunft.

Trifft der Anfragedatensatz auf einen Bestandsdatensatz, werden in einem zweiten Schritt die einzelnen Felder wiederum auf zeichengetreue Übereinstimmung verglichen. Im Unterschied zu der Zuspeicherung, bei dem – neben der exakten Zeichengleichheit von Geburtsname und Geburtsdatum – lediglich ein Vorname zeichengleich vorhanden sein muß, sind die Anforderungen an positive Identitätsentscheidungen bei der Auskunft insofern höher, als alle Vornamen des Anfragedatensatzes mit denen des Bestandsdatensatzes übereinstimmen müssen. Ein Beispiel soll dies verdeutlichen: Sind im eingegangenen Datensatz zwei Vornamen angegeben (z. B. Hans Georg) und ist im Bestandsdatensatz nur ein Vorname (z. B. Hans) gespeichert, so erfolgt zwar eine automatische Zuspeicherung, aber keine automatische Auskunftserteilung. In solchen Fällen dagegen, in denen im Anfragedatensatz nur ein Vorname (z. B. Hans) angegeben ist und im Bestandsdatensatz neben diesen zeichengleichen auch ein weiterer (z. B. Hans Georg) gespeichert ist, wird die Auskunft automatisch erteilt. Auch hier ist festzuhalten, daß ein Mensch bei Vorliegen dieser Informationen hinsichtlich der Identität des Betroffenen nicht anders entscheiden würde als die Maschine.

Sobald beim Vergleich des Bestandsdatensatzes mit dem Anfragedatensatz Abweichungen bei nur einem der drei Mindestangaben auftreten, werden Anfragedatensatz und Bestandsdatensatz dem Sachbearbeiter an seiner Datensichtstation angezeigt. Er entscheidet dann, ob eine Auskunft erteilt wird. Nach Informationen der Registerbehörde bedürfen etwa ein Viertel der Auskunftsersuchen einer zusätzlichen Überprüfung durch Sachbearbeiter. Blickt man nicht auf die Auskunftsersuchen insgesamt, sondern nur auf die erteilten Positiv-

Auskünfte (Auskunft über eine oder mehrere strafrechtliche Verurteilungen), so habe ich festgestellt, daß bei lediglich 6 bis 8 % aller Anfragen Positiv-Auskünfte automatisch erteilt werden.

Bei genauer Betrachtung der von der Registerbehörde verwandten Programme zur Identitätsfindung läßt sich feststellen, daß schon bei geringsten Zweifeln nicht die Entscheidung von der Maschine getroffen, sondern von der intellektuellen Entscheidung eines Sachbearbeiters abhängig gemacht wird. Umgekehrt ist dort der Einsatz des Computers sinnvoll, wo die Arbeitsanweisung an den Bearbeiter nicht anders lauten kann als die Programmierung des Computers. Die Praxis bestätigt, daß die automatisierte Datenverarbeitung in dem Massenverfahren bei der Registerbehörde zu einer erhöhten Sicherheit der Entscheidung bei der Identitätsfindung führt. Mir sind im Berichtszeitraum keine Fälle bekanntgeworden, die auf eine fehlerhafte automatische Zuspeicherung oder automatische Auskunft schließen lassen. Das automatisierte Verfahren bei der Registerbehörde könnte noch sicherer werden, wenn die mitteilenden und auskunftssuchenden Stellen der Registerbehörde exakte und vollständige Identifizierungsdaten liefern würden, so daß sich Nachermittlungen durch die Registerbehörde auf ein Minimum reduzieren ließen.

4.5 Weitergabe personenbezogener Daten an gemeinnützige Einrichtungen bei Geldauflagen im Strafverfahren

Wird ein Strafverfahren eingestellt und mit der Auflage versehen, einen Geldbetrag zugunsten einer gemeinnützigen Organisation zu zahlen, ist es gängige Praxis von Staatsanwaltschaften und Gerichten, den Zahlungseingang durch diese gemeinnützigen Einrichtungen überwachen zu lassen. Zu diesem Zweck werden die personenbezogenen Daten des Verurteilten den entsprechenden Organisationen übermittelt. Auch durch die Verwendung von allgemein üblichen Überweisungsträgern erhalten diese Institutionen personenbezogene Daten des Verurteilten.

Ich halte diese Praxis für datenschutzrechtlich bedenklich. Die einschlägigen Vorschriften regeln zwar die Einstellung von Strafverfahren nach Erfüllung von Auflagen, sind jedoch keine ausreichende bereichsspezifische Regelung für die Übermittlung personenbezogener Daten an nicht-öffentliche Stellen wie eben die gemeinnützigen Organisationen. Nach den allgemeinen datenschutzrechtlichen Vorschriften (§ 16 Abs. 1 Nr. 1 i.V. m. § 14 Abs. 2 Nr. 7 BDSG bzw. vergleichbaren Vorschriften der Länder) ist eine Übermittlung nur zulässig, wenn dies einerseits zur Erfüllung der Aufgaben der übermittelnden Stelle und andererseits zur Vollstreckung oder zum Vollzug von Strafen erforderlich ist. Hier fehlt es aus meiner Sicht an der Erforderlichkeit der Durchführung des beschriebenen Verfahrens.

Unterstützt von Kollegen in den Ländern habe ich mich daher mit folgenden alternativen Lösungsvorschlägen an das Bundesministerium der Justiz gewandt:

Alternative 1:

Das Bußgeld wird an die Landeshauptkasse/Gerichtskasse überwiesen, wo auch der Zahlungseingang überwacht wird. Die gemeinnützigen Einrichtungen erhalten dann anonymisiert den festgesetzten Betrag.

Alternative 2:

Es werden Überweisungsträger verwendet, bei denen der Beleg für die empfangende gemeinnützige Organisation keine personenbezogenen Daten, sondern z. B. nur ein Codewort enthält. Die Überwachung des Zahlungseingangs durch die gemeinnützigen Institutionen wäre anhand von anonymisierten Listen ebenfalls möglich.

Das Bundesministerium der Justiz sieht das Erfordernis einer datenschutzrechtlichen Absicherung und hat den Landesjustizverwaltungen folgenden Formulierungsvorschlag zur Diskussion gestellt:

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

Dieser Formulierungsvorschlag entspricht nicht meinen Vorschlägen: Ich habe gegenüber dem Bundesministerium der Justiz betont, daß es nach meinem Grundrechtsverständnis als zusätzliche Sanktion von nicht geringem Gewicht angesehen werden muß, die über das eigentliche vom Gesetzgeber verfolgte Ziel hinausgeht, dem Betroffenen ein finanzielles Opfer aufzuerlegen, wenn eine gemeinnützige Organisation von persönlichen Verhältnissen Betroffener erfährt. Der Zahlungsauflage darf nicht gleichzeitig eine Prangerfunktion innewohnen. Sie hat keinen Strafcharakter und soll die Resozialisierung des Betroffenen erleichtern, die aber gerade durch die Offenlegung der Tatsache verhindert werden kann, daß gegen den Betroffenen ermittelt wurde und daß wenigstens „zureichende tatsächliche Anhaltspunkte" für eine Straftat vorlagen. Mag im Falle der Erbringung gemeinnütziger Leistungen – etwa Arbeit in einem Tierheim oder Krankenhaus – die Offenlegung persönlicher Verhältnisse unausweichlich mit dem Vollzug verbunden sein; ein zwingender Bestandteil der Geldzahlung ist die Offenbarung persönlicher Verhältnisse jedenfalls nicht.

Ich habe daher das Bundesministerium der Justiz gebeten, seinen Formulierungsvorschlag zurückzuziehen und statt dessen meine Lösungvorschläge mit den Landesjustizverwaltungen zu diskutieren.

4.6 Durchführung des Geldwäschegesetzes

Im Zusammenhang mit dem Geldwäschegesetz haben sich viele Bürger an mich gewandt. Ihren Eingaben läßt sich eine erhebliche Verunsicherung entnehmen, die vor allem auf der in diesem Ausmaß völlig neuen Einbeziehung privater Dritter, nämlich der Banken, in die Belange der Strafverfolgung beruht (siehe auch 14. TB S. 46f.) Die Praxis und der Erfolg dieses Gesetzes, gerade mit Blick auf die im Geldwäschegesetz vorgeschriebenen Datenerhebungen durch private Dritte, ist mit besonderer Aufmerksamkeit zu verfolgen.

Viele Bürger haben auch auf folgendes Problem hingewiesen: Das Geldwäschegesetz verpflichtet Banken unter bestimmten Voraussetzungen (Beispiel: Bareinzahlung von 20 000,– DM oder mehr) den Betroffenen zu identifizieren und im Rahmen dieser Identifizierung erhobene Daten aufzuzeichnen und aufzubewahren. Viele Banken erfüllen diese Aufzeichnungspflicht, indem sie die gesamten ihnen von ihren Kunden zur Feststellung der Identität vorgelegten Dokumente kopieren. Mein Einwand richtet sich hier nicht gegen das Kopieren der Daten; dies ist vom Gesetzgeber ausdrücklich als Aufzeichnungsart vorgesehen. Ausdrücklich hat aber der Gesetzgeber gesagt, was er unter Identifizieren im Sinne des Geldwäschegesetzes versteht: *„das Feststellen des Namens aufgrund eines Personalausweises oder Reisepasses sowie des Geburtsdatums und der Anschrift, soweit sie darin enthalten sind, und das Feststellen von Art, Nummer und ausstellender Behörde des amtlichen Ausweises"*. Die Banken können sich daher trotz der möglicherweise mißverständlichen Formulierung des Gesetzes nicht auf eine Verpflichtung durch das Geldwäschegesetz berufen, andere personenbezogene Daten als die zu kopieren, die zur Identifizierung erforderlich sind.

4.7 Grundbuch

4.7.1 Grundbucheinsicht und ihre Protokollierung

Der Entwurf für das Ende 1993 in Kraft getretene Gesetz zur Vereinfachung und Beschleunigung registerrechtlicher und anderer Verfahren (Registerverfahrenbeschleunigungsgesetz – RegVBG –; BGBl. 1993 I S. 2182ff.) enthielt ursprünglich auch Regelungen zur Ergänzung des § 12 Grundbuchordnung (GBO) um Bestimmungen zur Einsichtnahme in das Grundbuch. Wegen der unterschiedlichen Belange des Datenschutzes einerseits und der Praxis der Landesjustizverwaltungen andererseits war eine Einigung hierzu kurzfristig nicht möglich. Das Bundesministerium der Justiz nahm daher diese aus der Sicht des Datenschutzes wichtigen Vorschläge aus dem Entwurf heraus und will sie in einer „Verordnung zur Änderung des Grundbucheinsichtsrechts" durch Neufassung und Ergänzung der §§ 43ff. Grundbuchverfügung (GBVerf) regeln. Ein Entwurf hierfür wird im BMJ vorbereitet.

In meiner Stellungnahme gegenüber dem BMJ zu § 12 GBO der Entwurfsfassung zum Registerverfahrenbeschleunigungsgesetz hatte ich mich vor allem für die Regelung folgender Punkte eingesetzt, die ich auch bei der Beratung der angekündigten Verordnung besonders im Auge behalten werde:

– **Protokollierung der Grundbucheinsicht**

Das Grundbuch enthält eine Vielzahl personenbezogener Daten über Eigentumsverhältnisse oder finanzielle Belastungen. Deshalb ist zu Recht die Einsichtnahme nach § 12 Abs. 1 GBO nur demjenigen gestattet, der ein berechtigtes Interesse hierfür darlegt. Zum Schutz des Persönlichkeitsrechts auf informationelle Selbstbestimmung eines Eigentümers gehört aber auch, daß er nachprüfen kann, wer was wann durch die Einsichtnahme in das Grundbuch über ihn erfahren hat. Hierzu ist es erforderlich, daß die Einsichtnahme in das Grundbuch protokolliert wird. Bisher wurde häufig eingewendet, dies verursache erheblichen Verwaltungsaufwand. Im Interesse des Schutzes der Rechte des Betroffenen halte ich einen gewissen Mehraufwand aber für hinnehmbar. Zudem wird in einigen Bundesländern bereits ein entsprechendes Verfahren praktiziert. Eine spürbare Verringerung des Aufwands dürfte sich darüber hinaus beim Einsatz von Informationstechnik – insbesondere im Zusammenhang mit der z. T. unmittelbar bevorstehenden Einführung des maschinell gestützten Grundbuchs – ergeben.

– **Beschränkung des Umfangs der Einsicht**

Die Einsicht in das Grundbuch darf nur soweit gewährt werden, wie das dargelegte berechtigte Interesse reicht. Der ursprüngliche Entwurf des Registerverfahrenbeschleunigungsgesetzes enthielt bereits eine Regelung, die dies berücksichtigt. Die Beschränkung der Einsichtnahme auf einzelne Teile des Grundbuchs ist ohne großen Verwaltungsaufwand durchführbar, z. B. durch Abdecken bestimmter Eintragungen oder Fertigen von Teilauszügen aus dem Grundbuch. Auch in diesem Fall wird nach meiner Auffassung der Einsatz der Informationstechnik in größerem Maße zu einer Arbeitsentlastung beitragen.

– **Zweckbindung der durch Einsicht übermittelten Daten**

Von Bedeutung ist auch die Frage der Verwendung der durch Einsicht erhaltenen personenbezogenen Daten durch den Empfänger. Der Entwurf des Registerverfahrenbeschleunigungsgesetzes enthielt erfreulicherweise auch insoweit eine Regelung. Hiernach sollte der Empfänger der Daten verpflichtet sein, sie nur für den Zweck zu verwenden, für den sie ihm übermittelt wurden. Außerdem sah der Entwurf eine Verpflichtung des Grundbuchamts vor, den Empfänger auf die Einhaltung der Zweckbestimmung der Datenübermittlung hinzuweisen.

Ich hoffe, daß der angekündigte Verordnungsentwurf bald vorgelegt wird.

4.7.2 Grundbucheinsicht durch die Presse?

Mit der Frage, ob auch die Presse das Grundbuch einsehen kann, war ich aufgrund einer Verfassungsbeschwerde befaßt. Das Bundesverfassungsgericht hatte mir Gelegenheit zur Stellungnahme gegeben.

Die Einsicht des Grundbuchs ist nach § 12 Abs. 1 Satz 1 Grundbuchordnung jedem gestattet, der ein berechtigtes Interesse darlegt. Ich habe mich gegenüber dem Bundesverfassungsgericht dahingehend geäußert, es komme entscheidend darauf an, ob das Informationsinteresse der Presse als ein berechtigtes Interesse i. S. dieser Vorschrift angesehen werden kann. Der ursprüngliche Zweck der Führung der Grundbücher ist es, den **privaten** grundstücksbezogenen Rechtsverkehr zu unterstützen; hieran sind auch das Einsichtsrecht in das Grundbuch und die darin eingetragenen personenbezogenen Daten ausgerichtet. Dagegen geht das Informationsbedürfnis der Presse in eine andere Richtung. Es dient der Unterrichtung der Öffentlichkeit.

Der Entscheidung des Bundesverfassungsgerichts sehe ich mit großem Interesse entgegen.

4.7.3 Grundbucheinsicht bei Miteigentum

Ein Grundpfandrecht (Hypothek, Grundschuld) an einem herrschenden Grundstück erstreckt sich vielfach auch auf Miteigentumsanteile an einem sog. dienenden Grundstück, wie z. B. gemeinsamen Zugangswegen oder Abstellplätzen. Ist für das dienende Grundstück ein besonderes Grundbuchblatt angelegt worden, muß das an dem herrschenden Grundstück bestehende Grundpfandrecht auch dort eingetragen werden. Für andere Miteigentümer des dienenden Grundstücks wird dann bei Einsicht in dieses Grundbuchblatt ersichtlich, wie das herrschende Grundstück belastet ist. In früheren Tätigkeitsberichten hatte ich mehrfach über meine Bemühungen gegenüber dem Bundesministerium der Justiz um eine Lösung berichtet, die verhindern sollte, daß durch die Bekanntgabe des Inhalts von Grundbuchauszügen schutzwürdige Belange von Grundstückseigentümern verletzt werden, die gleichzeitig Miteigentümer dienender Grundstücke sind (5. TB S. 22, 6. TB S. 15, 7. TB S. 16).

Die im Rahmen des Registerverfahrenbeschleunigungsgesetzes vorgenommene Änderung der Grundbuchordnung – GBO – (BGBl. 1993 I S. 2182 ff.) hat nunmehr „im Hinblick auch auf einen besseren Datenschutz" (BT-Drs. 12/5553, S. 54) das Verfahren zur Eintragung von Miteigentumsanteilen im Grundbuch (§ 3 GBO) modifiziert. Im Ergebnis sollen hiernach künftig Grundbuchblätter für dienendes Miteigentum nur noch in Ausnahmefällen angelegt werden; der Miteigentumsanteil an solchen Grundstükken soll regelmäßig beim herrschenden Grundstück des jeweiligen Miteigentümers eingetragen werden. Bisher galt dies nur, wenn dies zur Erleichterung des Rechtsverkehrs angezeigt war. Nunmehr ist umgekehrt die Buchung des Miteigentumsanteils beim herrschenden Grundstück lediglich ausgeschlossen, wenn dadurch eine wesentliche Erschwerung des Rechtsverkehrs oder der Grundbuchführung zu besorgen ist (vgl. § 3 Abs. 4, 6, 7 GBO). Damit entfällt bereits weitgehend – mangels eines gemeinschaftlichen Grundbuchblattes – die **Möglichkeit**, daß Miteigentümer Kenntnis von der Belastung eines herrschenden Grundstücks eines anderen Miteigentümers erhalten. Die Beachtung des oben unter Nr. 4.7.1, 2. Anstrich, dargelegten Grundsatzes, daß eine Grundbucheinsicht nur in dem Umfang zulässig ist, der sich aus dem berechtigten Interesse ergibt, sollte in den verbleibenden Ausnahmefällen von Grundbuchblättern für gemeinschaftliches dienendes Eigentum ebenfalls unzulässige Kenntnisnahmen durch Miteigentümer verhindern.

4.8 Schuldnerverzeichnis

Das Schuldnerverzeichnis dient dem Schutz des redlichen Geschäftsverkehrs. Es enthält Daten der Personen, die eine eidesstattliche Versicherung über ihr Vermögen abgegeben haben oder gegen die zur Erzwingung dieser Versicherung die Haft angeordnet worden ist. Aus datenschutzrechtlicher Sicht dürfen diese Daten aber nur insoweit an Dritte bekanntgegeben werden, als dies im Hinblick auf den Zweck des Verzeichnisses erforderlich ist. Entsprechende Verfahrensregelungen, die dem Schutz des Persönlichkeitsrechts des Schuldners Rechnung tragen, fehlten jedoch bisher.

Nachdem ich unter Beteiligung der Landesbeauftragten für den Datenschutz lange Zeit mit dem Bundesministerium der Justiz Lösungsansätze und Entwürfe für eine sachgerechte Regelung diskutiert (vgl. zuletzt 14. TB S. 161) und schließlich zu dem Regierungsentwurf für ein entsprechendes Gesetz (BT-Drs. 12/193) gegenüber dem Rechtsausschuß des Deutschen Bundestages Stellung genommen habe, ist nunmehr am 1. Januar 1995 das Gesetz zur Änderung von Vorschriften über das Schuldnerverzeichnis (BGBl. 1994 I S. 1566 f.) in Kraft getreten.

In diesem Gesetz sehe ich ein gutes Ergebnis auch meines langjährigen Dialogs mit dem BMJ. Es legt konkret die **Zwecke** fest, für die die Daten des Schuldnerverzeichnisses verwendet werden dürfen. Es trifft eingehende Regelungen über die Abgabe von **Abdrucken** des Verzeichnisses an Kammern und – unter besonderen Voraussetzungen – an andere Antragsteller sowie über die Überlassung von **Listen** an Mitglieder von Kammern; es legt ausdrücklich fest, daß die Abdrucke, Listen und ebenso erteilte Einzelauskünfte **vertraulich** zu behandeln sind; es regelt die **Löschung** der Daten auch bei deren Empfängern. Weiterhin sieht es die Auskunftserteilung auch im **automatisierten Abrufverfahren** und die Möglichkeit **anlaßfreier Kontrolle** bei Beziehern von Abdrucken vor, die z. B. zentrale bundesweite oder regionale Schuldnerverzeichnisse errichtet haben. Dasselbe gilt für andere Bezieher von Abdrucken und Listen des Schuldnerverzeichnisses.

In der ergänzenden Verordnung über das Schuldnerverzeichnis (SchuVVO, BGBl. 1994 I S. 3822), an deren Erarbeitung ich ebenfalls beteiligt war, werden nähere Regelungen u. a. zur Auskunftserteilung im automatisierten Abrufverfahren durch die Bezieher von Abdrucken getroffen. Nachdem die auch datenschutzgerechten gesetzlichen Voraussetzungen ge-

schaffen sind, liegt es nunmehr an der Praxis, anhand dieser Festlegungen mit den Daten der im Schuldnerverzeichnis eingetragenen Schuldner in einer Weise umzugehen, wie es deren Persönlichkeitsrecht erfordert.

4.9 Prozeßkostenhilfe

Bereits früher (3. TB S. 20, 4. TB S. 44) habe ich mich mit einer datenschutzrechtlichen Problematik befaßt, die jährlich 350 000 bis 400 000 Bürger betrifft, die einen Antrag auf Prozeßkostenhilfe stellen. Bei einem solchen Antrag muß der Antragsteller jeweils seine persönlichen und wirtschaftlichen Verhältnisse (Familienverhältnisse, Beruf, Vermögen, Einkommen und Lasten) gegenüber dem Gericht offenlegen. Bisher fehlte es jedoch an einer gesetzlichen Regelung darüber, ob dem Prozeßgegner insoweit ein Recht auf Anhörung und Akteneinsicht zusteht. Die Frage war selbst nach einem Beschluß des Bundesgerichtshofs aus dem Jahre 1983 (BGHZ 89, 65ff.), der ein solches Recht verneinte, nicht unumstritten. Das Bundesverfassungsgericht hat die hieran anknüpfende Rechtsprechung des Bundesgerichtshofs schließlich bestätigt (BVerfG NJW 1991, 2078). Aus datenschutzrechtlicher Sicht bedeutet die Unterrichtung des Gegners über die persönlichen und wirtschaftlichen Verhältnisse des Antragstellers ohne dessen Einwilligung einen nicht erforderlichen und damit unzulässigen Eingriff in sein Persönlichkeitsrecht. Seit Jahren habe ich daher eine eindeutige gesetzliche Regelung gefordert.

Am 1. Januar 1995 ist nunmehr das Prozeßkostenhilfeänderungsgesetz in Kraft getreten, das in § 117 Abs. 2 Satz 2 ZPO (neu) festlegt, daß die Erklärung und die Belege über die persönlichen und wirtschaftlichen Verhältnisse dem Gegner nur mit Zustimmung des Antragstellers zugänglich gemacht werden dürfen (BGBl. 1994 I S. 2954f.).

Gegenüber einer im Regierungsentwurf für das Prozeßkostenhilfeänderungsgesetz (BT-Drs. 12/6963) enthaltenen weiteren Ergänzung der Zivilprozeßordnung (§ 127 Abs. 1 Satz 3 ZPO – neu –, a.a.O. S. 5), daß dem Gegner die Gründe der Entscheidung des Prozeßkostenhilfeverfahrens nur mit Zustimmung des Antragstellers zugänglich gemacht werden dürfen, soweit sie Angaben über dessen persönliche und wirtschaftliche Verhältnisse enthalten, hatte der Bundesrat Bedenken erhoben (a. a. O. S. 25, dort Nr. 5). Insbesondere wegen der schutzwürdigen Belange des Antragstellers habe ich mich gegenüber dem Rechtsausschuß des Deutschen Bundestages nachdrücklich für die von der Bundesregierung vorgeschlagene Regelung eingesetzt. Ich begrüße es, daß diese Regelung in die Zivilprozeßordnung eingefügt wurde.

4.10 Justizmitteilungen aus gerichtlichen und staatsanwaltschaftlichen Verfahren an andere Stellen

Die Datenschutzbeauftragten des Bundes und der Länder fordern seit Jahren die dringlich notwendige **gesetzliche Grundlage** für die Mitteilungen der Gerichte der ordentlichen Gerichtsbarkeit und der Staatsanwaltschaften aus den dortigen Verfahren (Justizmitteilungen) ohne Ersuchen (sog. Spontanmitteilungen) an Gerichte, Behörden und sonstige öffentliche Stellen für andere Zwecke als die des jeweiligen Verfahrens. Die Bundesregierung hatte dem 12. Deutschen Bundestag hierzu einen Gesetzentwurf vorgelegt; in meinem 14. TB (Seite 53f.) habe ich hierüber eingehend berichtet. Leider ist der Regierungsentwurf auch in der vergangenen Legislaturperiode nicht verabschiedet worden.

Justizmitteilungen in **Strafsachen** bedeuten für den Betroffenen oftmals einen erheblichen Eingriff in sein Persönlichkeitsrecht, wenn diese z. B. zur Rücknahme der Zulassung zur Ausübung eines Handwerks oder zur Untersagung einer ehrenamtlichen Tätigkeit führen können. Ähnliches gilt in **Zivilsachen,** so z. B. für Mitteilungen in Konkurs- und Vergleichsverfahren an das Finanzamt und die Sozialversicherungsträger, damit sie ihre Forderungen in diesem Verfahren geltend machen können.

Ich bedaure sehr, daß es bisher nicht gelungen ist, diesen Bereich entsprechend den Vorgaben des Volkszählungsurteils (BVerfGE 65,1 ff., 44) zu regeln und einzugrenzen. Wie aus dem Bundesministerium der Justiz zu erfahren ist, soll in dieser Legislaturperiode erneut ein Gesetzentwurf eingebracht werden. Ich halte dies für dringend erforderlich. Mein Anliegen wird von meinen Kollegen in den Ländern geteilt und in einem gemeinsamen Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt (vgl. Anlage 10 und oben Nr. 4.2.1).

4.11 Mehrzahl von Drittschuldnern

Meine Bedenken gegen **einheitliche** Pfändungs- und Überweisungsbeschlüsse gegenüber einer Mehrzahl von Drittschuldnern habe ich zuletzt im 14. TB (S. 162) dargelegt. Dort hatte ich auch eine Stellungnahme gegenüber dem Bundesministerium der Justiz zu einem – gerade entgegengesetzten – Vorschlag der mit der Überarbeitung des Zwangsvollstreckungsrechts betrauten Arbeitsgruppe der Justizministerkonferenz angekündigt; dieser sah vor, § 829 Abs. 1 ZPO dahingehend zu ergänzen, daß die Pfändung mehrerer Geldforderungen gegen verschiedene Drittschuldner auf Antrag des Gläubigers durch „einheitlichen Beschluß" ausgesprochen werden „soll". Ich habe demgegenüber darauf hingewiesen, ein solcher Grundsatz gefährde – da nicht erforderlich – das Persönlichkeitsrecht der betroffenen Drittschuldner (z. B. der Patienten eines Arztes), die auf diese Weise voneinander Kenntnis erhalten; das einzige von der Arbeitsgruppe angeführte Beispiel für die Notwendigkeit einer Zusammenfassung der Drittschuldner im Hinblick auf gegenseitige Unterrichtung in einem Beschluß, nämlich die Pfändung und Zusammenrechnung mehrerer Arbeitseinkommen, überzeugt demgegenüber nicht als Begründung für den **regelmäßigen** Erlaß einheitlicher Pfändungsbeschlüsse. Die Arbeitsgruppe folgte meinen Bedenken nicht. Vielmehr wurde in einem Gesetzentwurf des Bundesrates für eine 2. Zwangsvollstreckungsnovelle der

Vorschlag der Arbeitsgruppe dahingehend verdeutlicht, daß die Grundregel eines einheitlichen Beschlusses nur gelte, „soweit dies für Zwecke der Vollstreckung geboten erscheint und kein Grund zu der Annahme besteht, daß schutzwürdige Interessen der Drittschuldner entgegenstehen (BT-Drs. 12/8314 S. 6 Nr. 21 Buchst. a). Diese datenschutzrechtlich zwar bessere Fassung halte ich noch für unzureichend, da sie unzutreffend von der Grundregel einheitlicher Beschlüsse ausgeht.

In meiner Stellungnahme hierzu gegenüber dem Bundesministerium der Justiz habe ich daher die Formulierung vorgeschlagen: „Die Pfändung mehrerer Geldforderungen gegen verschiedene Drittschuldner darf auf Antrag des Gläubigers durch einheitlichen Beschluß ausgesprochen werden, soweit dies für Zwecke der Vollstreckung erforderlich ist und kein Grund zu der Annahme besteht, daß schutzwürdige Interessen der Drittschuldner entgegenstehen". Diese Fassung geht vom Grundsatz **getrennter** Pfändungsbeschlüsse aus und gibt der Praxis Spielraum für einheitliche Beschlüsse mit der Maßgabe, daß diese vorher jeweils prüft, ob hierfür im Einzelfall überhaupt ein Erfordernis besteht und ob schutzwürdige Interessen der Drittschuldner entgegenstehen. Eine entsprechende Regelung sollte im übrigen auch in § 835 ZPO für den Fall erst nachträglicher Überweisung von Geldforderungen mehrerer Drittschuldner an den Gläubiger aufgenommen werden.

Der Gesetzentwurf des Bundesrates wurde in der abgelaufenen Wahlperiode nicht mehr verabschiedet, inzwischen aber unverändert wieder eingebracht (BR-Drs. 1083/94 (Beschluß)). In meiner Stellungnahme gegenüber dem BMJ im Hinblick auf die erneut abzugebende Gegenäußerung der Bundesregierung habe ich mein datenschutzrechtliches Anliegen wiederholt. Ich werde die weiteren Beratungen aufmerksam verfolgen.

5 Finanzwesen

5.1 Bereichsspezifischer Datenschutz in der Abgabenordnung

Im 14. TB (S. 54 f.) habe ich über den Entwurf eines Gesetzes zur Änderung der Abgabenordnung (AOÄG 1994) und darin enthaltene Vorschläge für datenschutzrechtliche Verbesserungen berichtet. Nachdem die Abgabenordnung inzwischen mit dem **Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz (StMBG)** vom 21. Dezember 1993 (BGBl. I S. 2310, 2344) um einige vom Bundesministerium der Finanzen für notwendig erachtete Vorschriften aus diesem Entwurf ergänzt worden ist, hat das BMF die Arbeiten hieran nicht fortgeführt. Nach seiner Ansicht besteht „kein Handlungsbedarf mehr in datenschutzrechtlicher Hinsicht". Auch die mit dem Entwurf seinerzeit angestrebte Anwendung einheitlichen Datenschutzrechts in Verfahren nach der Abgabenordnung wird vom BMF nicht weiter verfolgt, da sich die Datenschutzgesetzgebung von Bund und Ländern nach seiner Auffassung inzwischen ausreichend angenähert hat.

Gegen einige mit dem StMBG herbeigeführte Änderungen der Abgabenordnung habe ich während des Gesetzgebungsverfahrens Bedenken erhoben. Das BMF habe ich zugleich gebeten, die Arbeiten zum bereichsspezifischen Datenschutz in der Abgabenordnung fortzusetzen. Eine große Zahl von Landesbeauftragten für den Datenschutz hat sich entsprechend an die zuständigen Finanzressorts der Länder gewandt. Das Bundesministerium der Justiz hat mein Anliegen nachdrücklich unterstützt.

Leider ist das BMF bislang nicht bereit, meinem Anliegen zur Neuregelung des bereichsspezifischen Datenschutzes in der Abgabenordnung zu folgen. Ich werde deshalb – nach Abstimmung mit den Landesbeauftragten für den Datenschutz – erneut an das BMF herantreten und ihm insbesondere folgende **Vorschläge zur Änderung und Ergänzung der Abgabenordnung** unterbreiten:

- Die Vorschrift über das Steuergeheimnis (§ 30 AO) ist entsprechend den Vorgaben des Bundesverfassungsgerichts im sog. Volkszählungsurteil (BVerfGE 65,1 ff., 45) so zu fassen, daß die **Bindung** erhobener oder gespeicherter personenbezogener Daten **an den Erhebungs-/Speicherzweck** ausdrücklich festgelegt wird; ebenso sind die Voraussetzungen und Grenzen einer **zweckändernden Verarbeitung oder Nutzung** dieser Daten eindeutig vorzugeben.
- Die nach § 30 Abs. 2 AO **geschützten Angaben** über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher oder juristischer Personen sowie über nicht rechtsfähige Personenvereinigungen, Vermögensmassen und Betriebs- oder Geschäftsgeheimnisse sollten datenschutzrechtlich gleichbehandelt werden.
- Die Tatbestände einer zulässigen **Durchbrechung des Steuergeheimnisses im zwingenden öffentlichen Interesse** (§ 30 Abs. 4 Nr. 5 AO) sind gesetzlich abschließend festzulegen.
- Die in § 31 Abs. 3 AO i.d.F. des StMBG vorgesehene Möglichkeit der zweckändernden Verwendung von **Steuerdaten von Grundstückseigentümern** ist enger zu fassen.
- Die Abgabenordnung bedarf dringend einer Regelung darüber, ob und ggf. unter welchen Voraussetzungen eine **Verarbeitung von Steuerdaten im Auftrag** durch private Dritte zulässig ist.
- Die mit dem StMBG eingeführte Erlaubnis zur **Sammlung geschützter Daten** durch die Finanzverwaltung (§ 88 a AO) bedarf sachgerechter Einschränkung und Präzisierung.
- Die in § 105 AO vorgesehene regelmäßige **Durchbrechung der Verpflichtung zur Amtsverschwiegenheit** zugunsten der Finanzbehörden ist dahingehend einzuschränken, daß sie nur in ausdrücklich geregelten Fällen zugelassen wird.
- Es sollte klargestellt werden, inwieweit die **allgemeinen Vorschriften des Bundesdatenschutzgesetzes bzw. der Landesdatenschutzgesetze** anzuwenden sind, wenn die Abgabenordnung keine bereichsspezifische Regelung vorsieht.

5.2 Kontrollmitteilungen von Hauptzollämtern an Finanzämter

Bei Beratungs- und Kontrollbesuchen habe ich festgestellt, daß von Hauptzollämtern sog. Kontrollmitteilungen mit personenbezogenen Angaben aus unterschiedlichen Verfahren an die für die Beteiligten zuständigen Finanzämter übermittelt wurden.

Die Übermittlung personenbezogener Daten wäre in diesen Fällen zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Hauptzollamts oder des betreffenden Finanzamts liegenden Aufgaben erforderlich wäre **und** die gesetzlichen Voraussetzungen für eine zweckändernde Nutzung dieser Daten durch die Finanzämter zu steuerlichen Zwecken vorlägen, §§ 4, 15 Abs. 1 i. V. m. 14 Abs. 2 BDSG. Für die von mir kontrollierten Verfahren traf dies nicht zu: Zur Erfüllung der den Hauptzollämtern übertragenen Aufgaben sind Mitteilungen an die Finanzämter nicht erforderlich. Die Finanzämter ihrerseits haben die zur Feststellung eines für die Besteuerung erheblichen Sachverhalts erforderlichen Auskünfte grundsätzlich von den Beteiligten selbst einzuholen, § 93 Abs. 1 Satz 3 Abgabenordnung (AO). Einer Übermittlung **regelmäßiger Kontrollmitteilungen** durch Hauptzollämter zur Erfüllung der den Finanzämtern obliegenden Aufgaben bedarf es daher nicht. Ebenso fehlt es an einer Rechtsvorschrift, die eine zweckändernde Nutzung der bei den Hauptzollämtern gespeicherten Daten durch die Finanzämter vorsieht oder zwingend voraussetzt, § 14 Abs. 2 Nr. 1 BDSG.

Ich habe die Übermittlung dieser Kontrollmitteilungen nach § 25 Abs. 1 BDSG beanstandet. Das BMF teilt meine Auffassung, daß es für diese Übermittlungen an einer bereichsspezifischen Rechtsgrundlage fehlt. Es hat mir mitgeteilt, die beanstandeten Übermittlungen seien inzwischen eingestellt worden. Gleichwohl halte man Kontrollmitteilungen an die Finanzämter weiterhin für erforderlich und – jedenfalls zum Teil – nach den Amtshilfevorschriften der Abgabenordnung (§§ 111 ff. AO) auch für zulässig. Die vom BMF hierzu vorgetragenen Gründe haben mich nicht überzeugt. Ich werde die Praxis von Kontrollmitteilungen auch bei künftigen Beratungs- und Kontrollbesuchen im Bereich der Bundesfinanzverwaltung aufmerksam beobachten.

5.3 Eintragung der Kirchensteuermerkmale des Ehegatten auf der Lohnsteuerkarte

Bis einschließlich 1994 trug die Gemeinde auf der Lohnsteuerkarte für die Einbehaltung und Abführung der Kirchensteuer durch den Arbeitgeber neben der Angabe der Religionszugehörigkeit des Arbeitnehmers stets auch für den Ehegatten ein, ob und welcher zur Erhebung von Kirchensteuer berechtigten Religionsgesellschaft er angehörte. Der Arbeitgeber benötigt Angaben über die Religionszugehörigkeit des Ehegatten für Zwecke der Kirchensteuererhebung aber nur, wenn der Arbeitnehmer und der Ehegatte verschiedenen erhebungsberechtigten Religionsgesellschaften angehören. In diesem Fall wird der vom Arbeitgeber abgeführte Betrag je zur Hälfte auf beide Religionsgesellschaften aufgeteilt.

Zunächst hatte ein Landesbeauftragter für den Datenschutz gegenüber einem Landesfinanzministerium Bedenken erhoben, daß über den genannten Fall hinaus Angaben zur Konfession des Ehegatten auf der Lohnsteuerkarte eingetragen werden. Er hatte zu Recht dargelegt, daß Eintragungen über die Religionszugehörigkeit des Ehegatten und die damit verbundene Offenbarung dieses personenbezogenen Datums gegenüber dem Arbeitgeber im Hinblick auf Artikel 140 GG i.V. m. Art. 136 Abs. 3, 137 Abs. 6 Weimarer Reichsverfassung nur insoweit vertretbar sind, als dies für die Erhebung und Abführung der Kirchensteuer tatsächlich erforderlich ist.

Bei Erörterung dieses Anliegens schlug das Bundesministerium der Finanzen zunächst nur vor, von Eintragungen über die Konfession des Ehegatten abzusehen, wenn der Arbeitnehmer keiner erhebungsberechtigten Religionsgesellschaft angehört. Mit dem BMF konnte schließlich Übereinstimmung dahingehend erzielt werden, daß datenschutzrechtlich eine Eintragung der Religionszugehörigkeit des Ehegatten nur bei konfessionsverschiedenen Ehen vertretbar ist. Nach Abstimmung mit den obersten Finanzbehörden der Länder legte das BMF daraufhin in den Vorgaben für die Ausstellung der Lohnsteuerkarte 1995 (Bundessteuerblatt 1994 I S. 455 f.) fest, daß die Religionszugehörigkeit des Ehegatten eines Arbeitnehmers von der ausstellenden Gemeinde nur noch auf der Lohnsteuerkarte eingetragen wird, wenn beide Eheleute unterschiedlichen erhebungsberechtigten Religionsgesellschaften angehören.

5.4 Musterklausel zum Datenschutz für Doppelbesteuerungsabkommen

Mit zwischenstaatlichen Doppelbesteuerungsabkommen soll eine mehrfache Besteuerung desselben Steuergegenstands (z. B. des Einkommens) durch zwei Staaten vermieden oder eingeschränkt werden. Die von der Bundesrepublik Deutschland zu diesem Zweck mit vielen Staaten abgeschlossenen Abkommen sehen regelmäßig einen Austausch der steuerlich erheblichen Daten zwischen den Vertragspartnern vor. Um die mit dem grenzüberschreitenden Informationsaustausch verbundenen Gefährdungen des Persönlichkeitsrechts der betroffenen Steuerpflichtigen zu begrenzen, müssen ausreichende Bestimmungen zum Schutz personenbezogener Daten in die Doppelbesteuerungsabkommen aufgenommen werden.

Hierzu hat das Bundesministerium der Justiz dem Bundesministerium der Finanzen eine Datenschutzklausel vorgeschlagen. Die Musterklausel sieht insbesondere vor, daß

- die übermittelnde Stelle darauf zu achten hat, daß die Übermittlung personenbezogener Daten erforderlich und verhältnismäßig ist, und die zu übermittelnden Daten richtig sind oder ggf. unverzüglich berichtigt werden,
- personenbezogene Daten grundsätzlich nur an die zuständigen Stellen übermittelt und nur zu dem mit dem Abkommen erstrebten Zweck verwendet werden dürfen,

- der Betroffene Auskunft über die zu seiner Person übermittelten Daten erhalten kann, soweit keine Auskunftsverweigerungsgründe entgegenstehen,
- personenbezogene Daten zu löschen sind, sobald sie nicht mehr benötigt werden, und
- die Daten wirksam gegen unbefugten Zugang, unbefugte Veränderung sowie unbefugte Bekanntgabe zu schützen sind.

Das BMF hat hiergegen eingewandt, die Aufnahme so umfangreicher Datenschutzklauseln in Amtshilfevereinbarungen „gleich welcher Art" sei „weder erforderlich noch zweckmäßig". Man müsse zwischen Abkommen unterscheiden, die einen eingeschränkten Datenaustausch vorsehen (z. B. mit Entwicklungsländern) und solchen, die einen erweiterten oder umfassenden Informationsaustausch zulassen (z. B. mit Industriestaaten bzw. mit einigen westeuropäischen Staaten).

Ich habe gegenüber den beteiligten Ressorts zu dieser Frage Stellung genommen. Dabei bin ich der Argumentation des BMF teilweise gefolgt: Ich halte es für sachgerecht, Art und Umfang der zu vereinbarenden Datenschutzregelungen von den besonderen Gegebenheiten des jeweiligen Abkommens (vorgesehener Umfang des Datenaustauschs, Datenschutzstandard im innerstaatlichen Recht des Partnerstaats) abhängig zu machen. Da andererseits auch das BMF eine einheitliche Datenschutzklausel für alle derartigen Abkommen anstrebt, halte ich es für erforderlich, in eine solche Musterklausel Datenschutzvorkehrungen aufzunehmen, die nicht hinter dem für den innergemeinschaftlichen Datenaustausch weitgehend erreichten Standard nach dem Vorbild des Schengener Durchführungsübereinkommens zurückbleiben. Die vom BMJ vorgeschlagene Musterklausel entspricht im wesentlichen diesem Standard.

Erfreulicherweise konnte mit dem BMF Einvernehmen darüber erzielt werden, diese Klausel mit einigen redaktionellen Änderungen als Muster für Doppelbesteuerungsabkommen zu verwenden. Darüber hinaus hat das BMF zugesagt, an die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) heranzutreten, um auf eine entsprechende Änderung des OECD-Muster-Doppelbesteuerungsabkommens hinzuwirken.

5.5 Amtshilfe unter den EU-Staaten im Bereich der Verbrauchsteuern

Im 14. TB (S. 56 f.) hatte ich über die Einbeziehung der **Verbrauchsteuern** auf Mineralöl, Alkohol, alkoholische Getränke und Tabakwaren in den Geltungsbereich der EG-Amtshilfe-Richtlinie und über die entsprechende Ergänzung des EG-Amtshilfe-Gesetzes (EG-AH-G) berichtet. Das Bundesministerium der Finanzen hat mir inzwischen einen Entwurf zur Änderung der Richtlinie über das allgemeine System der Verbrauchsteuern („System-Richtlinie") zur Stellungnahme übersandt. Der Entwurf zielt darauf ab, einen Informationsaustausch unter den Mitgliedstaaten bei verbrauchsteuerrechtlichen **Stichprobenkontrollen** einzuführen. Die damit zusammenhängenden Datenschutzfragen habe ich mit dem BMF auf der Grundlage verschiedener Textfassungen des Entwurfs mehrfach erörtert und hierzu Stellungnahmen abgegeben. Insbesondere wollte ich sichergestellt wissen, daß nach der beabsichtigten Ergänzung der System-Richtlinie

- ausschließlich zur Durchführung verbrauchsteuerrechtlicher Kontrollen erforderliche Daten erhoben und übermittelt werden dürfen, und
- die in der EG-Amtshilfe-Richtlinie enthaltenen Datenschutzbestimmungen sowie die innerstaatlichen Regelungen des EG-Amtshilfe-Gesetzes auf diesen Informationsaustausch anzuwenden sind.

Das BMF hat meine Vorschläge aufgegriffen, in die Verhandlungen der damit befaßten EG-Ratsgruppe eingebracht und mir mitgeteilt, der Text des Richtlinien-Entwurfs berücksichtige diese Vorschläge. Ich hoffe, daß sie in die endgültige Fassung der System-Richtlinie aufgenommen werden und damit ein datenschutzrechtlich befriedigendes Ergebnis erreicht wird.

Unabhängig davon hat das BMF die Frage an mich herangetragen, ob gegen eine Erweiterung des **Bestätigungsverfahrens nach § 2a Abs. 6 EG-AH-G** datenschutzrechtliche Bedenken bestehen. In diesem Verfahren wird einem Wirtschaftsbeteiligten bisher auf Antrag von der Finanzbehörde mitgeteilt, ob die – ihm bereits bekannte – Verbrauchsteueridentifikationsnummer eines Geschäftspartners gültig ist. Diese Information wird für die steuerliche Abwicklung des innergemeinschaftlichen Verkehrs mit verbrauchsteuerpflichtigen Waren benötigt. Das BMF ist von Vertretern der Wirtschaft gebeten worden, im Bestätigungsverfahren zuzulassen, daß die Finanzbehörden den Wirtschaftsbeteiligten die Verbrauchsteueridentifikationsnummer ihrer Geschäftspartner nicht nur **bestätigen,** sondern auf Anfrage auch **offenbaren.**

Ich habe das BMF in meiner Stellungnahme darauf hingewiesen, daß ich einen zwingenden Grund für eine solche Erweiterung des Bestätigungsverfahrens nicht erkennen kann, weil sich die Wirtschaftsbeteiligten diese Information von ihrem jeweiligen Geschäftspartner selbst geben lassen können und – gerade in deren Interesse – auch geben lassen sollen. Die Kenntnis der Verbrauchsteueridentifikationsnummer läßt nämlich nach Auskunft des BMF Rückschlüsse auf die für den Betroffenen zuständige Finanzbehörde und auf Art und Umfang seiner verbrauchsteuerrechtlichen Berechtigungen zu. Mit ihrer Preisgabe durch die Finanzbehörde würde somit eine Informationsmöglichkeit über steuerliche Verhältnisse Dritter geschaffen, die weit über die gesetzlich vorgesehene Bestätigung der Gültigkeit dieser Nummer hinausginge.

Ich habe dem BMF empfohlen, im Interesse des Persönlichkeitsschutzes von einer Erweiterung des Bestätigungsverfahrens jedenfalls dann abzusehen, wenn seitens der interessierten Wirtschaftsvertreter nicht nachgewiesen wird, daß sie zwingend erforderlich ist. Eine Entscheidung des BMF steht noch aus.

5.6 EG-Zollinformationssystem – EG-ZIS –

Die mit der Einrichtung einer den Mitgliedstaaten zugänglichen **zentralen Datenbank zur Bekämpfung von Zuwiderhandlungen gegen die EG-Zoll- und Agrarregelungen (EG-Zollinformationssystem – EG-ZIS –)** verbundenen datenschutzrechtlichen Fragen habe ich im 14. TB (S. 57) aufgezeigt. Die Beratungen über eine neue EG-Amtshilfe-Verordnung für den Zollbereich, die dem EG-ZIS als Rechtsgrundlage dienen soll, haben inzwischen zu einer Einigung im Rat über einen gemeinsamen Text geführt, der dem Europäischen Parlament zur Stellungnahme vorgelegt wird.

Für die **automatisierte Datenverarbeitung** im EG-ZIS sind weitgehend die datenschutzrechtlichen Regelungen in den Verordnungsentwurf aufgenommen worden, die im Entwurf des „Übereinkommens über den Einsatz der Informationstechnologie im Zollbereich" für das Zollinformationssystem der EU-Mitgliedstaaten zur Bekämpfung von Zuwiderhandlungen gegen nationale Vorschriften vorgesehen sind (s. Nr. 25.2). Damit würde für den Bereich der automatisierten Datenverarbeitung ein hoher Datenschutzstandard nach dem Vorbild des Schengener Durchführungsübereinkommens verwirklicht.

Der Entwurf einer neuen EG-Amtshilfe-Verordnung für den Zollbereich sieht neben der Einrichtung eines EG-ZIS auch vor, daß in erheblichem Umfang personenbezogene Daten zwischen den Mitgliedstaaten untereinander und von diesen mit der EG-Kommission in **nicht-automatisierten Verfahren** ausgetauscht werden. Das Ziel, auch diesen konventionellen Datenaustausch nach den entsprechenden Vorschriften des Schengener Durchführungsübereinkommens zu regeln, konnte nur zum Teil erreicht werden: Nach Art. 42 des Verordnungsentwurfs sollen zwar die Bestimmungen für die automatisierte Datenverarbeitung für die nicht-automatisierte Datenverarbeitung gelten. Damit würde ein dem Schengen-Standard vergleichbares Datenschutzniveau gewährleistet. Die Mitgliedstaaten, die dem Schengener Abkommen nicht beigetreten sind (Vereinigtes Königreich, Irland und Dänemark), haben diese Regelung aber nicht akzeptiert, sondern darauf bestanden, von der Anwendung dieser Vorschrift ausgenommen zu werden. Das Bundesministerium der Finanzen hat mit Unterstützung des Bundesministeriums der Justiz und meiner Beteiligung mehrere Kompromißvorschläge für eine Regelung des konventionellen Datenaustauschs erarbeitet. Zuletzt hat das BMJ angeregt, die datenschutzrechtlichen Vorkehrungen des „Dubliner Asylübereinkommens", das von allen Mitgliedstaaten unterzeichnet worden ist, zu übernehmen. Diese entsprechen weitgehend dem Standard des Schengener Durchführungsübereinkommens. Obwohl dieser Vorschlag auch von den Datenschutzbeauftragten der EU-Staaten befürwortet wurde (s. Anlage 18), konnte leider auch hierüber keine Einigung erzielt werden.

Nach der nunmehr im Verordnungsentwurf vorgesehenen Regelung gilt Art. 42 für die Mitgliedstaaten, die dem Schengener Abkommen beigetreten sind, sowie für die neuen EU-Staaten Österreich und Finnland uneingeschränkt. In einer Übergangsregelung (Art. 53) werden die vorgenannten Nicht-Schengen-Staaten von der Anwendung dieser Vorschrift ausgenommen. Der neue Mitgliedstaat Schweden wurde auf seinen Wunsch in die Übergangsregelung einbezogen. Für diese Staaten sollen die Bestimmungen für den nicht-automatisierten Datenaustausch erst dann gelten, wenn es eine entsprechende Gemeinschaftsregelung (z. B. Datenschutzrichtlinie) gibt, die Art. 42 des Verordnungsentwurfs entbehrlich macht. Wenn nach Ablauf von fünf Jahren eine solche Gemeinschaftsregelung noch nicht anwendbar ist, wird die EG-Kommission einen Bericht ggf. mit entsprechenden Vorschlägen erstellen. Die übrigen Mitgliedstaaten und die EG-Kommission können allerdings bereits jetzt die Mitteilung personenbezogener Daten an diese Staaten von der Beachtung datenschutzrechtlicher Auflagen abhängig machen.

Ich habe Verständnis dafür, daß die Bundesregierung diesen Kompromiß akzeptiert hat, um die Verabschiedung der Verordnung nicht weiter zu verzögern. Dennoch bleibt zu bedauern, daß die von der klaren Mehrheit der EU-Staaten gewünschte umfassende Regelung nicht durchsetzbar war und somit auf längere Zeit im Verhältnis zu vier Mitgliedstaaten eine lückenhafte Lösung in Kauf genommen werden muß, bei der die Gefahr einer Umgehung des Datenschutzes nicht auszuschließen ist.

5.7 Abkommen der EG mit Drittländern über die Amtshilfe im Zollbereich

Die Kooperation der EG mit Drittstaaten sieht regelmäßig in sog. **Protokollen über die Amtshilfe im Zollbereich** einen Austausch personenbezogener Daten mit diesen Drittländern vor (siehe auch 14. TB, S. 57). Die von der EG-Kommission in die Protokollentwürfe aufgenommenen Datenschutzbestimmungen sind bei allen Abkommen weitgehend gleich. Zu den Amtshilfeprotokollen für mehrere Abkommensentwürfe (z. B. mit der Türkei, Kanada und Korea) habe ich gegenüber dem Bundesministerium der Finanzen schriftlich Stellung genommen. Mit meinen Verbesserungsvorschlägen habe ich insbesondere darauf hingewiesen, daß ich es für unvertretbar halte, einen Austausch personenbezogener Daten mit Drittstaaten zuzulassen, solange die hierfür vorgesehenen datenschutzrechtlichen Vorkehrungen weit hinter dem für den innergemeinschaftlichen Datenaustausch erreichten Standard zurückbleiben.

Das BMF hat meine Vorschläge zur Nachbesserung der Amtshilfeprotokolle aufgegriffen und mich an den Beratungen der mit den Drittlandsabkommen befaßten EG-Ratsgruppe beteiligt. Zu den **Abkommen mit der Türkei und Kanada** konnten die Protokollentwürfe zumindest in folgenden Punkten verbessert werden:

- In die Begriffsbestimmungen wird eine Definition der „personenbezogenen Daten" aufgenommen („... alle Informationen, die eine bestimmte oder bestimmbare natürliche Person betreffen").
- Eine zweckändernde Verwendung übermittelter Daten ist nur mit schriftlicher Einwilligung der

übermittelnden Behörde und ggf. unter von ihr auferlegten Beschränkungen zulässig.

- Die Vertragsparteien müssen mindestens ein Schutzniveau gewährleisten, das sich an die Grundsätze des Übereinkommens Nr. 108 des Europarats zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten anlehnt.

Den weitergehenden Vorschlag des Bundesministeriums der Justiz, die Datenschutzvorschriften des „Dubliner Asylübereinkommens" (vgl. auch Nr. 5.6) in die Abkommen der EG mit **Kanada und Korea** zu übernehmen, hatte das BMF in die Beratungen der Ratsgruppe eingebracht. Mangels Unterstützung durch andere Mitgliedstaaten und die EG-Kommission konnte über den Vorschlag der deutschen Delegation aber keine Einigung erzielt werden. Ich bedaure, daß für den Datenverkehr der EG mit Drittstaaten keine ausreichende Absicherung der Persönlichkeitsrechte der Betroffenen in den Amtshilfeprotokollen durchsetzbar war.

5.8 Abschriften von Urkunden an Finanzbehörden

Sowohl nach dem Grunderwerbsteuergesetz als auch nach dem Erbschaftsteuer- und Schenkungsteuergesetz übersenden Gerichte, Notare und Behörden den Finanzbehörden im Rahmen ihrer Anzeigepflicht vollständige beglaubigte Abschriften von Urkunden, wie z. B. von Grundstückskaufverträgen oder von Testamenten. Ich habe gegenüber dem Bundesministerium für Finanzen Bedenken erhoben, weil die entsprechenden Vorschriften den Grundsatz des § 93 Abs. 1 Satz 3 Abgabenordnung verdrängen; hiernach ist der Steuerpflichtige von den Finanzbehörden regelmäßig selbst über den ihn betreffenden steuerlich erheblichen Sachverhalt zu befragen. Ich habe deshalb empfohlen, daß sich die Gerichte, Behörden und Notare auf eine Anzeige beschränken. Die Finanzbehörden können dann den für die Besteuerung maßgeblichen Sachverhalt beim Steuerpflichtigen selbst aufklären (vgl. zuletzt 14. TB S. 58).

Das BMF hat hierzu wie folgt Stellung genommen:

- Bei notariellen Verträgen, insbesondere Verträgen über die Veräußerung von **Grundstücken,** werde der Notar üblicherweise beauftragt, die Behörden zu unterrichten, die einen Anspruch auf Benachrichtigung vom Vertragsschluß haben. Die Vertragspartner akzeptierten dieses Verfahren gern, weil es ihnen einen „lästigen Schriftverkehr" mit Behörden erspare.
- Bei der Übersendung **letztwilliger Verfügungen** sei nicht jeder zunächst als rein privat erscheinende Bestandteil einer Urkunde für die steuerliche Bewertung bedeutungslos. Dies sei z. B. dann nicht der Fall, wenn die Verfügung erkennen lasse, daß mit einer Anfechtung eines Testaments zu rechnen sei, die den steuerlich relevanten Sachverhalt verändern könne.

Diesen Überlegungen kann ich mich insoweit anschließen, als dargelegt wird, die Übermittlung der Urkunden an die Finanzämter entspreche regelmäßig dem Willen der Betroffenen. Allerdings halte ich Durchbrechungen des Grundsatzes, daß zur Klärung des steuerlich bedeutsamen Sachverhalts zunächst der Steuerpflichtige selbst befragt werden soll, nach wie vor für bedenklich und nur in begründeten Ausnahmefällen für zulässig. Ich werde die Angelegenheit mit den Landesbeauftragten für den Datenschutz erörtern, aus deren Kreis die Problematik an mich herangetragen worden ist.

5.9 Zahlungsaufforderung in verschlossenem Umschlag für abwesenden Vollstreckungsschuldner

Wenn ein Vollziehungsbeamter eines Hauptzollamtes weder den Vollstreckungsschuldner noch einen erwachsenen Mitbewohner oder einen Bevollmächtigten antrifft, soll er die Wohnung in der Regel erst dann gewaltsam öffnen, nachdem er eine entsprechende Ankündigung und eine Zahlungsaufforderung in einem Umschlag verschlossen z. B. durch Einwurf in den Briefkasten „niedergelegt hat".

Weil ein Petent abwesend war, hatte ein Vollziehungsbeamter die an ihn gerichtete Zahlungsaufforderung der unter der angegebenen Anschrift anwesenden Vermieterin unverschlossen übergeben. Das hierzu von mir eingeschaltete Bundesministerium der Finanzen machte geltend, die angetroffene Person habe sich als Lebensgefährtin des Petenten zu erkennen gegeben. Dieser gegenüber habe sich der Vollziehungsbeamte nach § 285 Abs. 2 AO durch Vorzeigen des Vollstreckungsauftrags als zur Durchführung der Vollstreckung ermächtigt ausweisen können. Die unverschlossen übergebene Zahlungsaufforderung enthalte keine weitergehenden schuldnerbezogenen Daten als der Vollstreckungsauftrag. Ich habe das BMF demgegenüber darauf hingewiesen, daß diese Überlegung nicht überzeugt. Sie läßt unberücksichtigt, daß das Verschließen der Zahlungsaufforderung in einem Umschlag sicherstellen soll, daß sie z. B. nicht durch Unbefugte zur Kenntnis genommen oder möglicherweise auch kopiert wird, bevor sie der Schuldner schließlich in Händen hat. Dem entspricht es, daß die Zahlungsaufforderung auch dann in einem Umschlag zu verschließen ist, wenn sie in den Briefkasten des Schuldners eingeworfen wird. Für den von der Vollziehungsanweisung nicht geregelten Fall, daß der Vollziehungsbeamte bei Abwesenheit des Vollstreckungsschuldners eine andere Person antrifft und dieser die Zahlungsaufforderung übergibt, könne nichts anderes gelten. Das BMF hat daraufhin in einem Erlaß ausdrücklich geregelt, daß die Zahlungsaufforderung ausnahmslos in einem verschlossenen Umschlag zu hinterlassen ist, „so z. B. auch dann, wenn sie einer angetroffenen anderen Person als dem Vollstreckungsschuldner ausgehändigt" wird.

5.10 Offenbarung steuerlicher Verhältnisse an Bausparkassen bei Beantragung einer Wohnungsbauprämie

Das derzeitige Verfahren nach dem Wohnungsbau-Prämiengesetz zwingt den Bausparer dazu, bei Beantragung einer Wohnungsbauprämie gegenüber der Bausparkasse Steuerdaten zu offenbaren, die dort für

die Bescheinigung prämienbegünstigter Aufwendungen nicht benötigt werden. Er muß z. B. angeben, ob ihm ein Einkommensteuerbescheid erteilt worden ist, ob sein Einkommen die festgelegte Höchstgrenze überschreitet, ob und ggf. welche Kindschaftsverhältnisse zu berücksichtigen sind, ob eine Steuererklärung abgegeben wird und ob er mit anderen Bausparkassen weitere Verträge abgeschlossen hat.

Der Arbeitskreis „Steuerverwaltung" der Datenschutzbeauftragten des Bundes und der Länder hat das gegenwärtige Antragsverfahren als datenschutzrechtlich unverhältnismäßige Belastung der Bausparer angesehen. Landesbeauftragte für den Datenschutz haben deshalb zur Änderung des Verfahrens vorgeschlagen:

Die Bausparkasse bescheinigt dem Steuerpflichtigen die Höhe der prämienbegünstigten Aufwendungen und ggf. die Prämienhöhe. Der Steuerpflichtige reicht seinen Antrag auf Wohnungsbauprämie zusammen mit dieser Bescheinigung beim Finanzamt ein. Das Finanzamt setzt die Höhe der Prämie fest und teilt sie der Bausparkasse mit.

Eine entsprechende Neuregelung des Antragsverfahrens würde eine Änderung des Wohnungsbau-Prämiengesetzes erfordern. Da beim Bundesministerium der Finanzen eine Arbeitsgruppe mit der Konzeption eines EDV-Verfahrens für die Wohnungsbauprämienstellen der Finanzämter befaßt ist, habe ich die Vorschläge zur Änderung des Gesetzes zusammen mit Anregungen zur Gestaltung eines datenschutzrechtlich unbedenklichen EDV-Verfahrens an das Bundesministerium der Finanzen herangetragen. Das BMF hat mir zugesagt, nach Anhörung der zuständigen Landesressorts auf die Angelegenheit zurückzukommen.

5.11 Mitteilungsverordnung

Der im 14. TB (S. 58) behandelte Entwurf einer Rechtsverordnung nach § 93a AO ist am 1. Januar 1994 in Kraft getreten (BGBl. 1993 I S. 1554). Diese „Verordnung über Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten" **Mitteilungsverordnung** (MV) ist inzwischen bereits geändert worden (BGBl. 1994 I S. 3848).

Zu einem Punkt des Entwurfs für die Änderungsverordnung hatte ich Bedenken erhoben. Zunächst war vorgesehen, § 8 Abs. 3 MV ohne jegliche Einschränkung dahin gehend zu ergänzen, daß die Mitteilungspflicht auch durch Übersendung einer Mehrausfertigung oder eines Abdrucks des Bescheids erfüllt werden kann. Diese Regelung hätte als Folge die bisherige Festlegung in § 8 Abs. 3 MV, welche Daten im einzelnen an die Finanzbehörden zu übermitteln sind, unterlaufen. Die beabsichtigte Änderung hätte dazu geführt, daß den Finanzbehörden mehr personenbezogene Daten übermittelt worden wären, als diese zur Aufgabenerfüllung benötigen. Das BMF hat erfreulicherweise meinen Vorschlag aufgegriffen. Danach dürfen auch bei einer Übersendung von Mehrausfertigungen oder Abdrucken nicht mehr personenbezogene Daten übermittelt werden, als es die bisherige Regelung des § 8 Abs. 3 MV vorsieht. Der Bundesrat hat der entsprechenden Fassung des § 8 Abs. 3 MV zugestimmt.

6 Wirtschaft

6.1 Datenabgleichverfahren in der Gewerbeordnung

Das Gesetz zur Änderung der Gewerbeordnung und sonstiger gewerberechtlicher Vorschriften (siehe 14. TB S. 59) ist am Ende der letzten Legislaturperiode in Kraft getreten. Neben den von mir begrüßten Regelungen über die Erhebung und Verarbeitung personenbezogener Daten bei den Gewerbeaufsichtsämtern wurden im Gesetzgebungsverfahren auf Wunsch der Länder mehrere Datenabgleichverfahren in das Gesetz aufgenommen. So sollen die Gewerbeanzeigen an die Zentrale Vermittlungsstelle nach § 117 Bundessozialhilfegesetz (BSHG) und die Bundesanstalt für Arbeit übermittelt werden, um zu verhindern, daß ein Gewerbetreibender unberechtigt Leistungen nach dem BSHG oder den AFG erhält. Derartige Datenabgleichverfahren, von deren Notwendigkeit ich noch nicht überzeugt bin, bestätigen meine Sorge, was die Entwicklung einer immer intensiver werdenden Kontrolle und Überwachung der Bürger anlangt (s. 14. TB S. 10 ff. und oben Nr. 1.5)

6.2 Datenschutz in der Handwerksordnung – ein gelungenes Gemeinschaftswerk

Vom Zentralverband des Deutschen Handwerks wurde ich im Rahmen der Novellierung der Handwerksordnung um Beratung bei der Ausgestaltung der datenschutzrechtlichen Vorschriften gebeten. In vorbildlicher Zusammenarbeit mit den Ministerien für Wirtschaft und Justiz, Handwerksvertretern und den Ländern konnten sachgerechte Vorschriften über die Daten erreicht werden, die über Handwerker, Ausbilder und Auszubildende gespeichert und gegebenenfalls weitergegeben werden dürfen. Das Gesetz ist am 1.1.1994 in Kraft getreten.

6.3 Fahndung im Bestand des Bundesausfuhramtes

Die Genehmigung von Ausfuhren ist bisweilen ein sensibles Geschäft. Das Bundesausfuhramt (BAFA) als Genehmigungsbehörde und das Zollkriminalamt als Ermittler gehen dabei zwar mit wenigen, deshalb aber nicht weniger schutzwürdigen Personendaten um. Vom Bundeswirtschaftsministerium wurde ich daher um Beratung gebeten, als es darum ging, den Datenfluß zwischen den beiden Behörden durch die im Außenwirtschaftsgesetz vorgesehene Vereinbarung zu regeln. Ich habe dazu Vorschläge unterbreitet, nach denen einerseits dem Zollkriminalamt die Daten des BAFA im Einzelfall so zur Verfügung stünden, daß es den Verdachtsfällen nachgehen kann, andererseits entsprechend der Auflage des Gesetzgebers nicht die Gesamtheit der

Daten zum Gegenstand der Zollfahndung wird. Eine auf der Grundlage dieser Vorschläge erarbeitete Vereinbarung wird gegenwärtig zwischen den Beteiligten abgestimmt.

7 Bau- und Wohnungswesen

7.1 Wohnungsbauförderung

Das Bundesministerium für Raumordnung, Bauwesen und Städtebau hat mich bei den Beratungen zur Neuregelung der Wohnungsbauförderung (Wohnungsbauförderungsgesetz 1994) auf der Basis des Mietereinkommens beteiligt. Eine neue Förderungsart soll dem Investor eine angemessene Mieteinnahme dadurch garantieren, daß der Mieter einen einkommensabhängigen Teil der Miete zahlt und der Rest als öffentlicher Zuschuß zur Miete gezahlt wird. Anders als beim Wohngeld ist die Förderung objektbezogen und der Vermieter, nicht der Mieter, hat Anspruch auf den Zuschuß. Erhält der Vermieter den Zuschuß direkt, so kann er daraus ungefähr die Höhe des Mietereinkommens ableiten, obwohl diese Information für ihn nicht erforderlich ist. Dies ist datenschutzrechtlich vertretbar, weil der Vermieter aus der Förderungsbewilligung einen Anspruch auf diesen Zuschuß hat.

Das Ziel der Förderung wird aber auch erreicht, wenn der Zuschuß über den Mieter geleitet wird. Für den Fall, daß die Länder diesem Verfahren den Vorzug geben, würde erreicht, daß dem Vermieter – pünktliche und vollständige Zahlung der gesamten Miete durch den Mieter vorausgesetzt – im Bewilligungsbescheid nur die Tatsache der Förderung mitgeteilt wird.

Meine Beteiligung führte auch dazu, daß bei begründetem Zweifel an der Richtigkeit der Angaben des Wohnungsinhabers oder Antragstellers die Behörde vor einer Nachfrage bei den Finanzbehörden oder dem Arbeitgeber dem Betroffenen Gelegenheit zur Stellungnahme zu geben hat.

7.2 Datenschutz für Verpächter

Dem Deutschen Bundestag lag ein Gesetzentwurf über eine Änderung des Bundeskleingartengesetzes vor, auf den ich erst durch eine Eingabe betroffener Bürger aufmerksam wurde. Es waren Verpächter von Flächen im Obst- und Gemüseanbau, deren ortsüblich erzielte Pachtzinsen als Berechnungsmaßstab für die Obergrenze der Kleingartenpacht erhoben werden. Befürchtet wurde, daß in den Fällen, in denen am Ort nur wenige Personen für diesen Zweck Land verpachten, aus den festgelegten Höchstpachten Rückschlüsse auf das aus der Verpachtung erzielte Einkommen möglich wären. Ich habe geraten, in diesen Fällen zusätzlich die Ergebnisse von Erhebungen in vergleichbaren Gemeinden mit einzubeziehen. Dem ist der Gesetzgeber in § 5 Abs. 2 des Bundeskleingartengesetzes gefolgt.

8 Landwirtschaft

8.1 Verwaltungs- und Kontrollsysteme der EG-Beihilfen – InVeKoS

In meinem 14. Tätigkeitsbericht hatte ich über das Integrierte Verwaltungs- und Kontrollsystem für bestimmte landwirtschaftliche Beihilfen (InVeKoS) berichtet, das zur Durchführung, aber auch zur Kontrolle von Förderungsmaßnahmen der EG eingeführt wurde. Die Datenschutzbeauftragten des Bundes und der Länder haben sich anläßlich ihrer 46. Datenschutzkonferenz mit dem Thema befaßt (s. auch Anlage 3).

Der Aufbau von InVeKoS macht in den Ländern mittlerweile Fortschritte, wenn auch der jeweilige Stand recht unterschiedlich ist. Eine durch die EG-InVeKoS-Verordnungen vorgesehene Überwachung der landwirtschaftlichen Flächen, für die eine EG-Beihilfe beantragt wurde, wird in fast allen EU-Mitgliedstaaten praktiziert. In der Bundesrepublik wurden im Jahr 1993 in drei und 1994 in vier Bundesländern von privaten Unternehmen die Beihilfeanträge aufgrund von Satellitenaufnahmen überprüft. In weiteren zwei Bundesländern wurden hierfür Luftaufnahmen herangezogen.

Regelmäßig erhält die Bundeskasse als einzige Stelle des Bundes personenbezogene Daten aus InVeKoS von den in den Ländern zuständigen Behörden, und zwar in Form von Auszahlungslisten und -bändern. Das BML erhält zur Weitermeldung an die EG-Kommission aus den Ländern lediglich aggregierte Daten und gibt diese als Bundesergebnis aufbereitet in Tabellenform weiter. An Stellen der Kommission der Europäischen Gemeinschaften werden personenbezogene Daten aus InVeKoS nicht übermittelt. Ausnahmsweise können allerdings bei Kontrollen der zuständigen Stellen der Länder durch die Europäische Kommission Angaben aus den Beihilfeanträgen Mitarbeitern der Kommission bekannt werden.

8.2 Datenschutz für Fischer

Das Bundesministerium für Ernährung, Landwirtschaft und Forsten (BML) bat mich um Beratung bei der Formulierung datenschutzrechtlicher Normen in einer EG-Verordnung auf dem Gebiet der Fischerei. Mit der inzwischen verabschiedeten Verordnung wird eine umfassende Kontrollregelung für die gemeinsame Fischereipolitik der Gemeinschaft eingeführt. Wie bei solchen Kontrollverfahren üblich, erwartet die Gemeinschaft die Einrichtung umfassender Datenaustauschverfahren und räumt sich selbst das Recht zur Einsichtnahme in nationale Unterlagen und Register ein. Weil eine eigenständige Datenschutzregelung für die Gemeinschaftsorgane noch immer fehlt, mußte die Verordnung gewährleisten, daß die deutschen Fischer gegenüber der EG nicht schlechter gestellt werden, als gegenüber deutschen oder anderen staatlichen Behörden, für die jeweils nationale Datenschutzvorschriften gelten. Dieses Ziel wurde in Art. 37 der Verordnung dank einer vorbildlichen Zusammenarbeit mit der Verhandlungsdelegation des BML erreicht.

8.3 Kein Datenschutz beim Sortenschutz?

Durch eine Eingabe wurde ich darauf hingewiesen, daß die Datenschutzregelungen im Entwurf einer „Verordnung des Rates über den gemeinschaftlichen Sortenschutz" unklar waren. Auf meine rund fünf Monate vor Verabschiedung der Verordnung an das BMWi gerichtete Bitte, zu bestimmten Fragen der geplanten Norm Stellung zu nehmen, erhielt ich erst einen Monat nach deren Verabschiedung ein Schreiben, in dem das Ministerium zu einigen schwer verständlichen datenschutzrechtlichen Regelungen erklärende Hinweise und Interpretationen gab. Zwar hätte meine Beteiligung für die Verhandlungsführer mehr Aufwand bedeutet, aber es wäre vermutlich gelungen, die Datenschutzrechte der Landwirte in diesem Fall ähnlich klar wie die der Fischer (s. o. Nr. 8.2) zu regeln.

9 Personaldaten

9.1 Probleme beim Umgang mit Personal- und Bewerberdaten

9.1.1 Personalfragebögen

Mit Personalfragebögen werden durch Dienstherrn und Arbeitgeber umfangreiche Datenerhebungen bei Bewerbern und Beschäftigten durchgeführt. Auch dies zeigt den dringenden Bedarf für ein Arbeitnehmer-Datenschutzgesetz. In vielen Fällen konnte ich feststellen, daß oftmals weit mehr als die erforderlichen Angaben, d. h. unzulässigerweise, erhoben werden (siehe auch 14. TB S. 66 ff.).

9.1.1.1 Stiftung Preußischer Kulturbesitz – erfreuliche Fortschritte

Bei einer Kontrolle der Stiftung habe ich u. a. festgestellt, daß dort ein Personalfragebogen mit sehr umfangreichen Datenerhebungen verwendet wird. Im Hinblick auf den Erforderlichkeitsgrundsatz habe ich gegen etliche dieser Fragen Bedenken erhoben. Diese Bedenken hat die Stiftung aufgegriffen und mir mitgeteilt, daß sie sich künftig grundsätzlich an dem Personalfragebogen des BMI orientieren wird. Damit wird auf einige bisher gestellte Fragen verzichtet, so z. B. auf die Frage bei Kindern nach ehelich, nicht ehelich, Adoptiv-, Stief- und Pflegekindern.

Bei den Fragen insbesondere nach laufenden Strafverfahren sowie nach Bestrafungen und Disziplinarmaßnahmen aber auch bei den Angaben über wirtschaftliche Verhältnisse des Bewerbers besteht hingegen auch weiterhin Diskussionsbedarf. Soweit Angaben über wirtschaftliche Verhältnisse im Einzelfall zulässigerweise erfragt werden dürfen, weil sie für den konkreten Arbeitsplatz von Bedeutung sind, ist m.E. dabei soweit wie möglich auf objektive Kriterien abzustellen. Bislang wurde folgende Frage verwendet: „Sind Ihre wirtschaftlichen Verhältnisse geordnet, d. h. können Sie bei angemessener Lebenshaltung Ihre bestehenden Zahlungsverpflichtungen erfüllen?". Diese Formulierung ist aus meiner Sicht unzulässig, weil sie zu allgemein ist. Je nach subjektivem Empfinden und Einschätzen kann bei gleichem Sachverhalt diese Frage von einem Bewerber mit „Ja" und von einem anderen mit „Nein" beantwortet werden. Unter Berücksichtigung, daß die Beantwortung mit „Nein" in der Regel negative Konsequenzen im Hinblick auf eine Einstellung hat, muß eine neue Formulierung gefunden werden, die eine Gleichbehandlung der Bewerber sicherstellt.

9.1.1.2 Fragebogen zur Erhebung von Gesundheitsdaten durch die Deutsche Bundespost – Postamt Weimar

Unter der Schlagzeile „Intime Fragen an das Personal" hatte ich aus der Presse erfahren, daß im Bereich der Generaldirektion Postdienst, Direktion Erfurt, ein Gesundheitsfragebogen ausgegeben wurde, in dem die Mitarbeiter u. a. nach persönlichen und familiären Krankheitsgeschichten (z. B. Geschlechtskrankheiten, Menstruationsverlauf, Einnahme von Antibabypillen, Gemütserkrankungen) befragt wurden.

Nach Auskunft der Direktion Erfurt wurde der Fragebogen bei Einstellungsuntersuchungen in 2 Postämtern im Rahmen einer Sonderuntersuchung zur Feststellung der Bildschirmtauglichkeit von der Personalstelle ausgegeben, um die Durchführung der Untersuchung zu beschleunigen und um zugleich „lückenhafte ärztliche Akten zu vervollständigen". Der ausgefüllte Fragebogen sei jedoch von den Betroffenen persönlich an den untersuchenden Arzt ausgehändigt worden. Im übrigen entspreche die Erhebung von Anamnesedaten der üblichen ärztlichen Praxis und sei im Rahmen des § 13 Abs. 1 BDSG in dem erforderlichen Umfang auch zulässig.

Ich habe die Generaldirektion Postdienst darauf hingewiesen, daß nach § 12 Abs. 4 i.V. m. § 28 Abs. 1 Satz 2 BDSG die Speicherung von personenbezogenen Daten nur zulässig ist, wenn sie nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Der mit dem Neunten Gesetz zur Änderung dienstrechtlicher Vorschriften eingeführte Grundsatz, daß ein Dienstherr personenbezogene Daten über Beamte nur erheben darf, soweit dies zur Begründung, Durchführung, Beendigung oder Abwicklung des Dienstverhältnisses oder zur Durchführung organisatorischer, personeller und sozialer Maßnahmen, insbesondere auch zu Zwecken der Personalplanung und des Personaleinsatzes erforderlich ist oder eine Rechtsvorschrift dies erlaubt, gilt auch für Angestellte und Arbeiter (vgl. Nr. 9.13). Aus diesen Gründen habe ich die Generaldirektion Postdienst gebeten, die bereits ausgefüllten und dem Ärztlichen Dienst zugeleiteten Fragebögen zu vernichten und keine weitere Datenspeicherung und -verwertung vorzunehmen.

Die Generaldirektion Postdienst hat mir daraufhin versichert, daß der in die Diskussion geratene Fragebogen nicht mehr verwendet wird und in den Fällen, in denen er in der Vergangenheit verwendet worden sei, aus den Akten entfernt wurde. Anläßlich einer Fortbildungsveranstaltung für alle Postbetriebsärzte beim Sozialamt der Deutschen Bundespost seien die Grundsatzproblematik der ärztlichen Fragebögen und die Einzelheiten eines datenschutzgerechten

Verfahrens erörtert worden. Danach sei im Zuge der Neustrukturierung des Postbetriebsärztlichen Dienstes insbesondere beabsichtigt, einen für alle Betriebsärzte geltenden einheitlichen Fragebogen einzuführen.

9.1.1.3 Personalfragebögen nur noch mit Genehmigung zulässig

„Alle Jahre wieder – Neugieriger Postweihnachtsmann stellt unerlaubte Fragen auf Einstellungsfragebögen". Mit dieser Schlagzeile in einer Tageszeitung sowie wegen mehrerer Eingaben wurde ich auf Fragebögen aufmerksam, die im Zusammenhang mit Bewerbungen für Aushilfskräfte u. a. unzulässige Fragen nach Familienverhältnissen (geschieden oder zum Unterhalt verpflichtet), Gewicht, Körpergröße, ansteckende Krankheiten enthielten. Im vorliegenden Fall ging es um die Einstellung von Aushilfskräften für die Verteilung der Weihnachtspost. Nach Mitteilung der Generaldirektion Postdienst, die die Unzulässigkeit der Fragen teilweise einräumte, werden die Personalfragebögen von den Postämtern selbst entworfen. Nach dem Neunten Gesetz zur Änderung dienstrechtlicher Vorschriften bedürfen Fragebögen, mit denen personenbezogene Daten über Bewerber, Bedienstete und ehemalige Bedienstete erhoben werden sollen, seit 1. Januar 1994 der Genehmigung durch die zuständige oberste Dienstbehörde. Danach dürfen die bisherigen Fragebögen seit diesem Zeitpunkt nicht mehr ohne die Genehmigung der obersten Dienstbehörde verwendet werden (vgl. § 90 Abs. 4 Satz 2 BBG). Dies gilt für Beamte, Angestellte und Arbeiter gleichermaßen (s. Nr. 9.13).

Mehrfach habe ich festgestellt, daß sich Dienststellen bereits von Bewerbern zu Beginn von Auswahlverfahren den gesamten Personalbogen (Personalfragebogen), teilweise sogar den Besoldungsbogen ausfüllen lassen. Dies ist mit den Grundsätzen des Datenschutzes auf der Grundlage des BDSG und des BBG in der Fassung des Neunten Dienstrechtsänderungsgesetzes nicht vereinbar. Vielmehr ist bei der Gestaltung von Bewerberfragebögen von entscheidender Bedeutung, in welchem Stadium des Bewerbungs- und Einstellungsverfahrens Fragen an Bewerber gerichtet werden. Dabei lassen sich sowohl bei der Einstellung einer Gruppe von Bewerbern – wie im vorliegenden Fall – als auch bei Einstellungsverfahren nach konkreter Ausschreibung im allgemeinen eine erste Phase bis zur Vorauswahl der grundsätzlich geeigneten Bewerber und eine zweite Phase unterscheiden, in der die endgültige Auswahlentscheidung getroffen wird (vgl. auch 14. TB S. 66 ff.).

Aus den genannten Grundsätzen ergibt sich für Dienstherren die Verpflichtung, schon bei der Gestaltung von Personalfragebögen die datenschutzrechtlichen Grenzen für die Erhebung der Daten nach den Kriterien der Erforderlichkeit und Zweckbestimmung möglichst eng zu ziehen. Die gleichen Maßstäbe sind von den obersten Dienstbehörden im Genehmigungsverfahren der Personalfragebögen für den jeweiligen Zuständigkeitsbereich zu beachten.

Die mir bisher vorgelegten Personalfragebögen veranlassen mich, den öffentlichen Stellen im Rahmen meiner Zuständigkeit zu empfehlen, in ihren Bereichen einheitliche Fragebögen für den jeweiligen Verwendungszweck, z. B. für Bewerber (getrennt nach den einzelnen Bewerbungsphasen), Besoldung, Kindergeld, Ortszuschlag, vorzugeben.

9.1.2 Führung und Inhalt von Personalakten

Zur Personalakte gehören alle Unterlagen einschließlich der in Dateien gespeicherten, die den Mitarbeiter betreffen, soweit sie mit seinem Dienst- oder Arbeitsverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Andere Unterlagen dürfen in die Personalakte nicht aufgenommen werden. Dies ist für Beamte nunmehr ausdrücklich in § 90 Abs. 1 BBG festgeschrieben. Es gibt keinen sachlichen Grund, bei den Angestellten und Arbeitern anders zu verfahren. Des weiteren darf für jeden Mitarbeiter nur eine Personalakte geführt werden, d. h. „geheime Personalakten" sind verboten.

9.1.2.1 Personalnebenakten in den Landes- und Bezirksgeschäftsstellen der DAK

Anläßlich einer Kontrolle bei der Deutschen Angestellten Krankenkasse (DAK) wurde mir bekannt, daß in deren Landesgeschäftsstellen sog. „Personalnebenakten" geführt werden. Diese enthalten insbesondere Korrespondenzen im Zusammenhang mit Personalangelegenheiten. Diese Akten werden im Vorzimmer des Landesgeschäftsführers in einem verschlossenen Schrank aufbewahrt. Außer dem Landesgeschäftsführer haben auch die Vorzimmerkräfte zu ihnen Zugang.

Ich habe gegenüber der DAK Bedenken dahin gehend geäußert, ob diese Personalnebenakten für die Personalverwaltung oder -wirtschaft im Bereich der DAK erforderlich und damit datenschutzrechtlich zulässig sind.

Die Führung von Nebenakten ist eng zu begrenzen. Die Zulässigkeit setzt voraus, daß mehrere personalverwaltende Behörden für den Beamten zuständig sind oder die personalverwaltende Behörde nicht mit der Beschäftigungsbehörde identisch ist, was bei einem mehrstufigen Verwaltungsaufbau häufig der Fall ist.

Auf die zweite Alternative hat sich die DAK berufen. Die Landesgeschäftsführer hätten Personalbefugnisse. Dazu gehöre z. B. die Einstellung, Höhergruppierung und Versetzung von Mitarbeitern bis zu einer bestimmten Vergütungsgruppe. Zur Abwicklung und Durchführung dieser Personalaufgaben bedürfe der Landesgeschäftsführer daher bestimmter Unterlagen vor Ort, um ein wirtschaftliches und sparsames Verwaltungshandeln sicherzustellen. Dies müsse gerade auch im Hinblick auf die zu führende Korrespondenz mit den Mitarbeitern gelten oder im Hinblick auf Anfragen von diesen. Auch hätten nur solche Mitarbeiter Zugang zu den Personalnebenakten, die Informationen hieraus für ihre Aufgabenerfüllung benötigen.

Unter Berücksichtigung der von der DAK vorgetragenen Argumente halte ich die Führung der Perso-

nalnebenakten in den Landesgeschäftsstellen aus datenschutzrechtlicher Sicht für vertretbar. Ferner muß sichergestellt sein, daß die betroffenen Mitarbeiter wissen, daß es solche Nebenakten gibt, um von ihrem Einsichtsrecht Gebrauch machen zu können. Dies wird dadurch erreicht, daß in die Grundakte ein vollständiges Verzeichnis aller Teil- und Nebenakten aufzunehmen ist, wie es in § 90 Abs. 2 letzter Satz BBG für Personalakten von Beamten vorgesehen ist. Die DAK wird meine Forderung umsetzen.

9.1.2.2 Offene Informationen über den Gesundheitszustand von BGS-Mitarbeitern in Akten des Bundesverwaltungsamtes

Im Bundesverwaltungsamt (BVA) werden Lehrgänge durchgeführt, in denen dienstuntauglich gewordene Vollzugsbeamte des Bundesgrenzschutzes (BGS) auf eine Übernahme in den Allgemeinen Verwaltungsdienst des Bundes vorbereitet werden. Anläßlich einer Kontrolle stellte ich fest, daß hierzu dem BVA seitens des BMI sowohl die zuständigen Personalakten wie auch sog. „Sachakten" überlassen wurden, die Unterlagen über die Dienstuntauglichkeit des jeweiligen Beamten enthielten.

In diesen Sachakten befanden sich u. a. – offen – ärztliche Gutachten. Ein grenzschutzärztliches Gutachten enthielt beispielsweise die Diagnose „Angstneurotisch-depressives Syndrom". Des weiteren fanden sich Gutachten der Vorgesetzten der BGS-Beamten zur Übernahme in den allgemeinen Verwaltungsdienst. Die Sachakten waren den Mitarbeitern des BVA, die mit der Durchführung der Lehrgänge betraut waren, zugänglich.

Diese Verfahrensweise ist mit dem Vertraulichkeitsgebot von Personal- und Gesundheitsdaten nicht zu vereinbaren. Da nach Auskunft des BVA diese Akten für die Durchführung der Lehrgänge und damit für die Aufgabenerfüllung des BVA auch nicht erforderlich waren, wurde mir zugesichert, auf die Übersendung dieser Sachakten durch das BMI in Zukunft zu verzichten.

Darüber hinaus hat mir das BVA versichert, daß künftig Bescheide mit Angaben über den Gesundheitszustand der Beamten in verschlossenen und versiegelten Umschlägen aufbewahrt und nur von dem mit der Verteilung der Planstellen befaßten Sachbearbeitern oder dem zuständigen Referatsleiter geöffnet werden dürfen.

9.1.2.3 Fortlaufende Numerierung der Patientenakten abgelehnt

Anläßlich einer Kontrolle des Umgangs mit Patientenakten beim Ärztlichen und Sozialen Dienst im Bundesministerium der Verteidigung (vgl. zuletzt 13. TB 7.3. S. 44) war meine Forderung, die Blätter der Patientenakten fortlaufend zu numerieren (paginieren), zunächst mit der Begründung abgelehnt worden, daß dies weder erforderlich noch durchführbar sei. Außerdem wurde angeführt, daß bei einer Paginierung der Patient den Eindruck gewinnen könne, ihm würden widerrechtlich Teile seiner Patientenakte vorenthalten, wenn hieraus nur für den behandelnden Arzt bestimmte Aufzeichnungen oder dem Patienten gegebenenfalls nachteilige Gutachten entnommen würden.

Diese Argumentation halte ich nicht für überzeugend, weil alle den Mitarbeiter betreffenden Unterlagen in die Patientenakte aufzunehmen sind und auch daraus grundsätzlich nicht wieder entfernt werden dürfen. Sollte dies im Ausnahmefall dennoch zulässig sein, so ist dies in der Akte zu vermerken.

Mit der Entnahme bestimmter Aufzeichnungen oder Gutachten wäre das Recht des Mitarbeiters auf Einsicht in seine vollständigen Unterlagen eingeschränkt. Die Möglichkeit einer Beschränkung der Akteneinsicht für Patienten- und Personalakten von Beamten ist aber weitgehend ausgeschlossen. § 90 c Abs. 1 i.V. m. Abs. 4 BBG legt eindeutig fest, daß der Beamte, auch nach Beendigung des Beamtenverhältnisses, ein Recht auf Einsicht in seine vollständigen Unterlagen hat.

Da das Bundesministerium der Verteidigung meine Forderung, die Patientenakten fortlaufend zu numerieren, ablehnte, habe ich dies gem. § 25 Abs. 1 BDSG als einen Verstoß gegen § 9 BDSG beanstandet.

Meine Auffassung zur Paginierung vertritt offenbar auch das Bundesministerium des Innern, das in einem Erlaß zur Anlage und Führung von Personalakten ausgeführt hat: „Grundakte und Teilakten sind für sich getrennt **durchlaufend mit arabischen Ziffern fälschungssicher zu numerieren.**

9.1.2.4 Streikvermerke in Personalakten des Bundesverteidigungsministeriums

In einer Tageszeitung vom 07.01.1993 war unter anderem zu lesen: „Verteidigungsministerium verstößt gegen Datenschutz. In den Akten von Angestellten ist deren Teilnahme an Streiks festgehalten und nach Ablauf der gesetzlichen Verjährungsfrist nicht gelöscht worden."

Die Aufbewahrung von Streikvermerken in Personalakten ist mit datenschutzrechtlichen Grundsätzen nicht vereinbar. Sie ist nach der Rechtsprechung des Bundesarbeitsgerichts (vgl. Urteil vom 13. April 1988 – 5 AZR 537/86) für die Aufgabenerfüllung der Personalverwaltung nicht erforderlich und darüber hinaus geeignet, den Mitarbeiter in seiner beruflichen Entwicklungsmöglichkeit fortwirkend zu beeinträchtigen.

Dem entspricht auch eine Weisung des Bundesverteidigungsministeriums, das bestätigte, dagegen habe die Standortverwaltung Bonn verstoßen, was aber einen Einzelfall darstelle. Bei Arbeitskampfmaßnahmen würden lediglich Änderungsmeldungen erstellt und dem zuständigen Wehrbereichsgebührnisamt als zahlungsbegründende Unterlagen übersandt. Diese Änderungsmeldungen würden dort in den Teilakten „Vergütung/Lohn" aufbewahrt. Dies sei erforderlich, um gegenüber den Rentenversicherungsträgern Auskünfte über entstandene Fehlzeiten geben zu können.

Bei einer Kontrolle der Standortverwaltung in Bonn konnten schließlich keine Streikvermerke festgestellt werden.

Die Teilakten Vergütung/Lohn enthalten überwiegend zahlungsbegründende Unterlagen. Die Nachweise von für die Unterbrechung einer Vergütungs-/Lohnzahlung und für die Rentenversicherung relevanten Abwesenheitszeiten unterliegen der Rechnungsprüfung und sind entsprechend aufzubewahren. Das Bundesministerium der Verteidigung hat mir zugesichert, hierfür eine entsprechende Weisung zu erlassen.

9.1.2.5 Aufbewahrung von Unterlagen in Personalakten

In Eingaben wurden u. a. datenschutzrechtliche Bedenken im Hinblick auf folgenden Inhalt von Personalakten vorgetragen:

- Psychologische Stellungnahme aus einem Eignungstest für die Einstellung in den Vorbereitungsdienst
- Amtsärztliches Zeugnis für die Berufung in das Beamtenverhältnis auf Widerruf und auf Lebenszeit
- Schriftverkehr mit dem Personalrat über dessen Zustimmung zur Einstellung und Ernennung

Für die Zuordnung zur Personalakte ist insoweit von Bedeutung:

Sowohl die psychologische Stellungnahme als auch das amtsärztliche Zeugnis zur Einstellung in das Beamtenverhältnis auf Widerruf stellen einen Nachweis zur Erfüllung der Einstellungsvoraussetzungen dar und müssen in der Personalakte dokumentiert bleiben. Das gleiche gilt für das amtsärztliche Zeugnis zur Übernahme in das Beamtenverhältnis auf Lebenszeit.

Diese Unterlagen enthalten in der Regel höchst sensible personenbezogene Informationen, die nicht für jede Personalentscheidung von Bedeutung sind und dann auch nicht zur Kenntnis genommen werden dürfen. Psychologische Stellungnahmen, ärztliche Gutachten und andere Unterlagen mit ähnlich sensiblen personenbezogenen Daten sind daher in der Personalakte in verschlossenen Umschlägen, die mit dem entsprechenden Aufdruck (z. B. „Arztsache") zu versehen sind, aufzubewahren und nur im Bedarfsfall zu öffnen. Die Öffnung ist in der Weise zu dokumentieren, daß deutlich wird, wann und durch wen sie vorgenommen wurde.

Im Hinblick auf den Schriftverkehr mit dem Personalrat gilt folgendes: Die Zustimmung ist ein Wirksamkeitserfordernis für die beabsichtigte Übernahme in das Beamtenverhältnis auf Widerruf oder auf Lebenszeit (vgl. §§ 75 Abs. 1 Nr. 1 und 76 Abs. 1 Nr. 1 BPersVG). Das Zustimmungsschreiben steht somit in einem unmittelbaren inneren Zusammenhang mit dem Dienstverhältnis des Betroffenen (vgl. § 90 Abs. 1 BBG) und verbleibt daher in der Personalakte.

Die Abbildung 1 soll einen Hinweis für die richtige Zuordnung von Unterlagen geben.

9.1.3 Bewerberunterlagen

Sie gehören zunächst nicht zu den Personalakten im Sinne des § 90 Abs. 1 BBG. Sie werden oder sind nur Bestandteile von Personalakten, wenn und soweit sie in einem inneren Zusammenhang zu einem vorhandenen Beamtenverhältnis stehen oder zur Begründung eines Beamtenverhältnisses geführt haben oder Bestandteil eines beendeten Beamtenverhältnisses geworden sind. Liegt keiner dieser Ausnahmefälle vor, unterliegen Bewerberunterlagen nicht den Schutzvorschriften der §§ 90 ff. BBG, insbesondere nicht dem Einsichtsrecht des Betroffenen und den Löschungsfristen.

9.1.3.1 Abgelehnte Bewerber sollen ihre Unterlagen zurückerhalten

Ein Petent hatte sich an mich gewandt, weil ihm vom Geheimen Staatsarchiv der Stiftung Preußischer Kulturbesitz die vollständigen Bewerbungsunterlagen nicht zurückgesandt wurden. Mittlerweile konnte erreicht werden, daß die Hauptverwaltung der Stiftung das Geheime Staatsarchiv im konkreten Fall angewiesen hat, alle Unterlagen – einschließlich der Fragebögen – bei Nichtberücksichtigung an den Bewerber zurückzusenden.

Aus datenschutzrechtlicher Sicht war es bedenklich, daß die Bewerberschreiben nicht zurückgegeben wurden. Diese Schreiben enthalten oftmals sensible Angaben über Qualifikationen, Fähigkeiten, Werdegang etc. der Betroffenen. Die Speicherung dieser Daten ist jedoch im Falle einer endgültig abgelehnten Bewerbung für die Aufgabenerfüllung der Stiftung nicht mehr erforderlich.

9.1.3.2 Bewerbung an das Bundesamt für die Anerkennung ausländischer Flüchtlinge – Unterlagen zurückerhalten vom Bundesamt für Verfassungsschutz

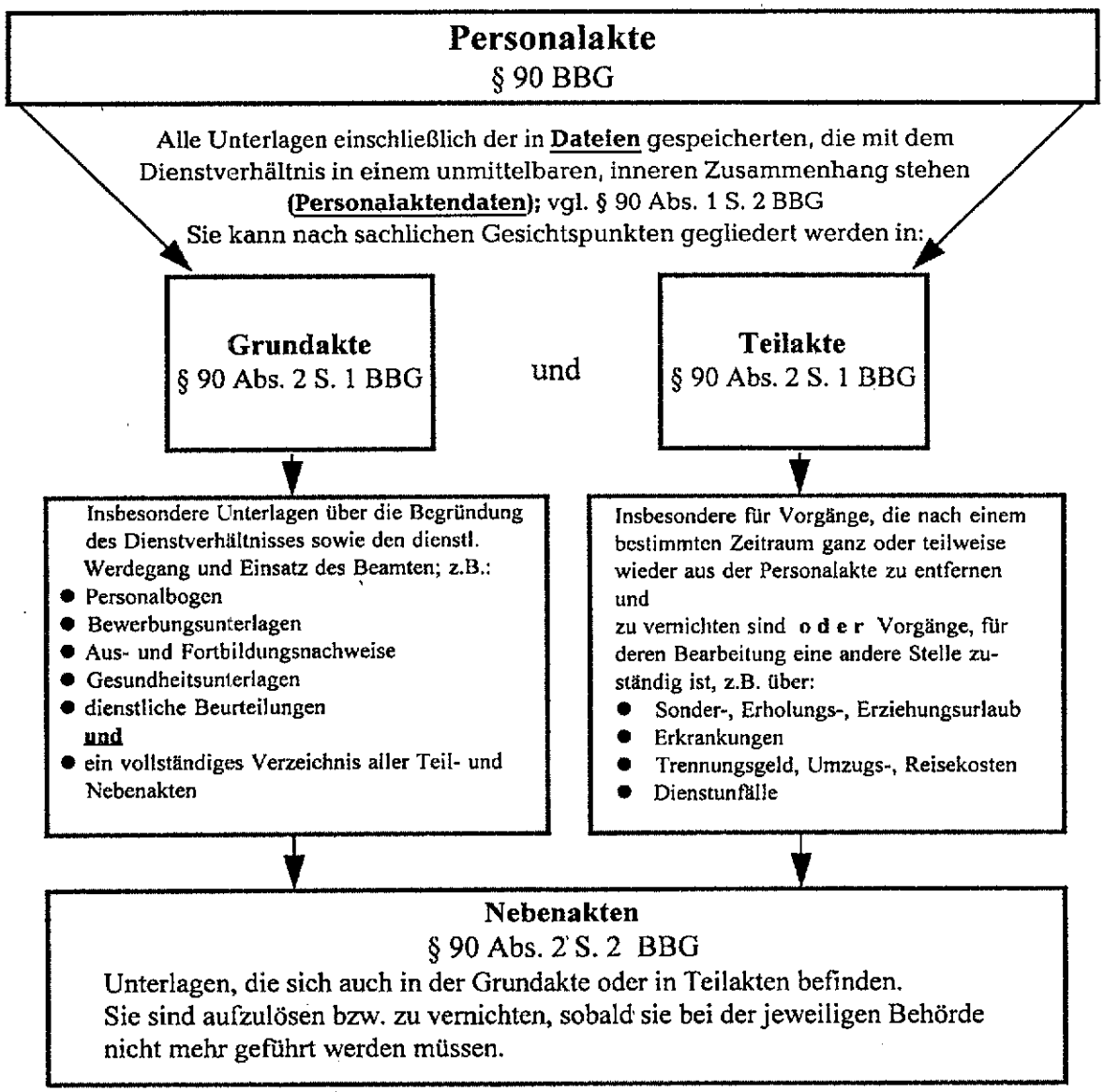
Ein Mitarbeiter aus dem nachgeordneten Bereich eines Bundesministeriums hatte sich aufgrund einer Stellenausschreibung beim BAFl beworben. Nachdem er die Bewerbung zurückgenommen hatte, bekam er seine Unterlagen vom Bundesamt für Verfassungsschutz zurückgesandt. Der Betroffene vermutete eine mißbräuchliche Verwendung seiner Bewerbungsunterlagen.

Dieses Verfahren beruhte letztlich auf einem Beschluß des Bundeskabinetts vom 21. Oktober 1992. Danach wurde eine vorübergehende personelle Unterstützung des BAFl durch insgesamt 1 300 Beschäftigte aller Bundesressorts beschlossen. Mit der verwaltungsmäßigen Abwicklung dieser Abordnungsaktion hatte das Bundesministerium des Innern für Beschäftigte des mittleren Dienstes das BfV beauftragt. Die Bearbeitung der Bewerbungen oblag dort einer ausschließlich für diese Hilfsaktion eingerichteten Arbeitsgruppe. Ihre Mitglieder wurden von ihren bisherigen Aufgaben vollständig freigestellt. Die von dem Petenten eingereichten Bewerbungsunterlagen wurden vom BAFl zuständigkeitshalber an diese Arbeitsgruppe im BfV weitergeleitet.

Aus meiner Sicht habe ich gegen die Weitergabe der Bewerbungsunterlagen vom BAFl an das BfV

Abbildung 1

„Personalakte § 90 BBG"



Darf nur angelegt werden

- wenn die personalverwaltende Behörde ***nicht*** zugleich Beschäftigungsbehörde ist

oder

- wenn mehrere personalverwaltende Behörden (z.B. zentrale Besoldungsstelle) für den Beamten zuständig sind.

Sie dürfen ***nur*** solche Unterlagen enthalten, die
a) in der Grund- oder Teilakte enthalten sind und
b) deren Kenntnis zur rechtmäßigen Aufgabenerfüllung der betreffenden Behörde unerläßlich ist.

Wichtig: 1. Aus dem Grundsatz der **Abschottung** von Unterlagen (§ 90a BBG) ergibt sich, daß Beihilfeunterlagen nicht in die Nebenakte aufgenommen werden dürfen.
2. Spezifische Regelungen für die **automatisierte Personaldatenverarbeitung** enthält § 90g BBG.

im vorliegenden Fall grundsätzlich keine Bedenken. Dieses Verfahren war notwendig, um entsprechende Personalentscheidungen zügig vornehmen zu können.

Demgegenüber ist es jedoch mit dem datenschutzrechtlichen Transparenzgebot nicht vereinbar, daß dem Petenten keine entsprechende Abgabenachricht erteilt und er nicht über die näheren Umstände der Bearbeitung seiner Bewerbung aufgeklärt wurde. Um in vergleichbaren Ausnahmesituationen künftig ein bewerberfreundliches Verfahren sicherzustellen, bat ich das BMI, dafür Sorge zu tragen, daß Bewerber entsprechend benachrichtigt werden.

9.2 Weitergabe von Personalunterlagen

Die Weitergabe von Personalakten oder auch von Informationen daraus ist stets mit besonderer Zurückhaltung zu behandeln. Das Persönlichkeitsrecht der betroffenen Mitarbeiter erfordert eine weitgehende Geheimhaltung der Personalakten. Das Personalaktengeheimnis wirkt sich damit rechtlich erheblich stärker aus als das allgemeine Amtsgeheimnis.

9.2.1 Urteil eines Arbeitsgerichtes als Grundlage für HBV-Flugblatt

In einem Urteil des Arbeitsgerichtes Hamburg wurde der Deutschen Angestellten Krankenkasse (DAK) als Antragsgegnerin im Wege der einstweiligen Verfügung aufgegeben, einen Mitarbeiter – der sich als Petent an mich gewandt hatte – zu unveränderten Arbeitsbedingungen weiter zu beschäftigen. Das Urteil, das in den Entscheidungsgründen auf das Verhalten und die Persönlichkeit des Petenten eingeht, wurde an die Gewerkschaft Handel, Banken und Versicherungen (HBV) – nach dortigen Angaben – anonym weitergeleitet.

Die HBV erstellte auf der Grundlage des Urteils ein Flugblatt mit personenbezogenen Daten über den Petenten. Dieser war darin zwar nicht namentlich genannt, durch die Angabe der Bezirksgeschäftsstelle, einschließlich der Funktion, in der er dort tätig ist, war er jedoch für Angehörige der DAK mühelos bestimmbar (§ 3 Abs. 1 BDSG). Das Rundschreiben wurde in der DAK bundesweit verteilt.

Der Inhalt des Urteils des Arbeitsgerichts Hamburg steht in einem inneren und unmittelbaren Zusammenhang mit dem Arbeitsverhältnis des Petenten. Es gehört damit in die Personalakte. Mangels Rechtsvorschrift oder Einwilligung des Betroffenen ist seine Weitergabe als eine unzulässige Datenübermittlung und damit als Verstoß gegen § 4 Abs. 1 BDSG zu werten.

Die Offenbarung von personenbezogenen Daten ist auch dann unzulässig, wenn diese in einem öffentlich verkündeten Urteil eines Gerichts enthalten sind und von einer Prozeßpartei an Dritte weitergegeben werden. Die Öffentlichkeit des Verfahrens gilt nur für die Verhandlung vor dem erkennenden Gericht; sie soll das Vertrauen in die Rechtspflege stärken, also nach außen wirken. Sie umfaßt jedoch nicht den Text des in aller Regel erst nachträglich verfaßten, schriftlichen Urteils. Dieses ist – anders als die Verhandlung – keine allgemein zugängliche Quelle im Sinne des § 28 Abs. 1 Nr. 3 BDSG. Der Urteilstext ist grundsätzlich nur dazu bestimmt, den Parteien des Verfahrens zugestellt zu werden, um diesen eine weitere, gegebenenfalls gerichtliche Nachprüfung der Entscheidung zu ermöglichen.

Aufgrund der Kontrollergebnisse konnte der Verstoß einer bestimmten Person im vorliegenden Fall nicht zugeordnet werden. Die Frage, ob die Übermittlung des Urteils durch ein Organisationsverschulden von der DAK zu verantworten war, konnte nicht abschließend beantwortet werden.

Einer datenschutzrechtlichen Bewertung der Veröffentlichung der personenbezogenen Daten des Petenten durch die HBV in dem Flugblatt habe ich mich enthalten, da sich mein Zuständigkeitsbereich nicht auf die HBV erstreckt. Die Bezirksregierung Köln, die für die Einhaltung des Datenschutzes bei der HBV zuständig ist, hat mir in diesem Zusammenhang mitgeteilt, daß im Rahmen einer datenschutzrechtlichen Überprüfung der HBV nicht feststellbar war, wer das Urteil des Arbeitsgerichtes Hamburg an die HBV übermittelt hat.

9.2.2 Außenstehenden wird bekannt, daß ein Disziplinarverfahren anhängig ist

Gegen einen Petenten war ein Disziplinarverfahren anhängig, weil der Verdacht eines gravierenden Dienstvergehens bestand. Nach seiner Zurruhesetzung wurde die teilweise Einbehaltung der Ruhestandsbezüge gem. § 92 Abs. 3 BDO verfügt. Gemäß der Darstellung des Dienstherrn, der Deutschen Bundesbahn, hat die Einleitungsbehörde unter Berücksichtigung der wirtschaftlichen Verhältnisse des Petenten nach pflichtgemäßem Ermessen entschieden, in welchem Umfang Dienst- oder Ruhestandsbezüge einzubehalten sind. Es ergaben sich in diesem Zusammenhang Unstimmigkeiten im Hinblick auf die Wohnverhältnisse des Petenten. Aus Zweckmäßigkeitsgründen wurde daher die Verwaltung seiner Heimatgemeinde im Hinblick auf die Amtshilfeverpflichtung gem. § 20 BDO um die entsprechende Auskunft ersucht. Die Gemeinde hat diese Auskunft auch erteilt.

Seitens der Deutschen Bundesbahn stellt die Anfrage bei der Gemeindeverwaltung eine Datenerhebung, zugleich auch eine Datenübermittlung dar, da der Gemeindeverwaltung das anhängige Disziplinarverfahren mitgeteilt wurde.

Die Datenerhebung durch die Deutsche Bundesbahn unmittelbar bei der Gemeindeverwaltung war aus datenschutzrechtlicher Sicht gem. § 90 Abs. 4 BBG in Verbindung mit § 13 Abs. 2 BDSG zulässig. Danach darf der Dienstherr personenbezogene Daten über Beamte u. a. erheben, soweit dies zur Durchführung oder Abwicklung des Dienstverhältnisses erforderlich ist. Dies ist vorliegend erfüllt, da die Deutsche Bundesbahn bei der Entscheidung über die Höhe der Einbehaltung der Ruhestandsbezüge gem. § 92 Abs. 3 BDO die wirtschaftlichen Verhältnisse des Petenten zu berücksichtigen hatte. Hierfür war es notwendig, seine Wohnverhältnisse und die damit zu-

sammenhängenden Kosten, insbesondere die Trennung nach privaten und geschäftlichen Kosten im einzelnen festzustellen.

Des weiteren liegt kein Verstoß gegen den Ersterhebungsgrundsatz des § 13 Abs. 2 Satz 1 BDSG vor. Denn ohne Mitwirkung des Petenten dürfen die Daten auch dann erhoben werden, wenn die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen oder Stellen als ihm selbst erforderlich macht (§ 13 Abs. 2 Satz 2 Nr. 2 a BDSG). Der Petent hatte monatliche Fixkosten für Strom-, Wasser- und Kanalgebühren in Höhe von mehr als 500 DM geltend gemacht. Bezogen auf seinen 2-Personen-Haushalt erschien der Deutschen Bundesbahn dieser Betrag zu hoch. Sie war somit berechtigt, als Dienstherr im Rahmen pflichtgemäßen Ermessens den für die Aufklärung des Disziplinarvorgangs erforderlichen Sachverhalt zu erforschen.

Der Petent hat mir gegenüber auch vorgetragen, daß er in einer kleinen Gemeinde wohnt und vermeiden möchte, daß seine Disziplinarsache durch Indiskretion „Dorfgespräch" wird. Aber auch unter Berücksichtigung des hier zum Ausdruck kommenden Vertraulichkeitsgrundsatzes bei Personalakten war die DB berechtigt, der Gemeindeverwaltung mitzuteilen, daß gegen den Petenten ein Disziplinarverfahren anhängig ist. Dies ergibt sich aus der Vorschrift des § 20 Satz 1 BDO. Danach ist die Gemeindeverwaltung verpflichtet, für die DB in Disziplinarsachen Rechts- und Amtshilfe zu leisten. Die Übermittlung von personenbezogenen Daten im Wege der Amtshilfe ist immer nur dann zulässig, wenn es hierfür eine gesetzliche Grundlage gibt. Damit die Gemeindeverwaltung eine Entscheidung treffen konnte, ob sie dem Amtshilfeersuchen der Deutschen Bundesbahn nachkommt, mußte sie daher wissen, aus welchem Grund diese Anfrage erfolgt. Nur so konnte sie entscheiden, ob es für die Übermittlung der personenbezogenen Daten eine Rechtsgrundlage – hier § 20 BDO – gibt.

9.2.3 Offenbarung von Personaldaten an den Bundesrechnungshof

Der Bundesrechnungshof hatte eine Beförderungsentscheidung und deren Vollzug in einem Bundesministerium beanstandet. Aus dieser Beanstandung ergab sich als Konsequenz die Einleitung eines disziplinarrechtlichen Ermittlungsverfahrens gegen verschiedene Mitarbeiter des Ministeriums, die an der Personalmaßnahme mitgewirkt hatten. Nach Abschluß der Ermittlungen sah der beauftragte Ermittlungsführer keinen Anlaß für disziplinarrechtliches Handeln und stellte das Ermittlungsverfahren ein. Daraufhin bat der Bundesrechnungshof zur weiteren Prüfung der Angelegenheit um eine Übersendung der Ermittlungsakten zur Einsichtnahme.

Bei den Ermittlungsakten handelt es sich nicht um Personal-, sondern um sog. Sachakten, auch wenn ggf. Personaldaten enthalten sind. Die Ermittlungsakten dienen besonderen, von der Person und dem Dienstverhältnis des einzelnen Beamten sachlich zu trennenden Zwecken. Damit sind die Vorschriften, insbesondere der §§ 90 ff. des Bundesbeamtengesetzes (BBG), grundsätzlich nicht einschlägig, sondern die Regelungen des Bundesdatenschutzgesetzes.

Ich halte eine entsprechende Übersendung aus datenschutzrechtlicher Sicht grundsätzlich für zulässig. Rechtsgrundlage hierfür ist § 95 Abs. 1 der Bundeshaushaltsordnung (BHO). Danach sind dem Bundesrechnungshof Unterlagen, die er zur Erfüllung seiner Aufgaben für erforderlich hält, auf Verlangen innerhalb einer bestimmten Frist zu übersenden oder seinen Beauftragten vorzulegen. Maßgebendes Kriterium für die Zulässigkeit der Datenübermittlung an den Bundesrechnungshof ist also, ob diese Übermittlung für die Erfüllung der in seiner Zuständigkeit liegenden Aufgaben erforderlich ist. Ob die Überprüfung der Ermittlungsakten zu den Aufgaben des Bundesrechnungshofes (§§ 88 ff. BHO) gehört, ist eine Fachfrage und abschließend von diesem zu beantworten.

Eine Einschränkung der Zulässigkeit der Datenübermittlung – abhängig von den Umständen des Einzelfalles – könnte im übrigen allenfalls dann und insoweit bestehen, als ein kontrollfreier politischer Kernbereich der Exekutive betroffen ist.

Die Rechtslage ist anders zu beurteilen, wenn es um die Einsichtnahme von Mitarbeitern des Bundesrechnungshofes in Personalakten im Sinne des § 90 Abs. 1 BBG geht. Das Bundesbeamtengesetz enthält keine ausdrückliche Rechtsgrundlage zur Einsichtnahme von Personalakten durch den Bundesrechnungshof. § 95 BHO regelt lediglich in allgemeiner Form, daß Unterlagen, die der Bundesrechnungshof zur Erfüllung seiner Aufgaben für erforderlich hält, ihm auf Verlangen vorzulegen sind. Auf die Sonderproblematik von Personalaktendaten geht die Bestimmung nicht ein.

Ich habe im 10. Tätigkeitsbericht (Seite 61) im Hinblick auf Sozialdaten die Auffassung geteilt, daß der verfassungsmäßige Prüfungsauftrag des Bundesrechnungshofes (Art. 114 GG) das notwendige Zugriffsrecht auch auf Vorgänge und Daten umfaßt, die einer besonderen Geheimhaltung unterliegen, und daher die Offenbarung solcher Vorgänge und Daten an den Bundesrechnungshof einer einfachgesetzlichen Regelung im Sozialgesetzbuch entzogen ist. Unter Zugrundelegung dieser Rechtsansicht komme ich auch bei Personalakten zu dem Ergebnis, daß der verfassungsmäßige Prüfungsauftrag des Bundesrechnungshofes jedenfalls soweit eine Rechtsgrundlage darstellt, als finanzwirksame Vorgänge in Betracht kommen. In diesem Zusammenhang hat das BMF mit Rundschreiben vom 12. Dezember 1980 festgelegt, daß sich der Bundesrechnungshof bei Vorgängen besonders vertraulicher Art (z. B. Gesundheitszeugnissen, Beurteilungen und dergleichen), die durch das von der Verfassung gewährleistete Persönlichkeitsrecht geschützt sind, gemäß den Grundsätzen der Verhältnismäßigkeit auf das unbedingt Notwendige bei Einsichtnahmen beschränkt.

Nunmehr hat sich ein Landesbeauftragter für den Datenschutz an mich gewandt und datenschutzrechtliche Bedenken gegenüber den Einsichtsrechten der Rechnungsprüfungsbehörden der Länder in Personalakten geltend gemacht. Ich werde mich dazu mit

dem Bundesministerium des Innern in Verbindung setzen und im Hinblick auf das Einsichtsrecht des Bundesrechnungshofes in Personalakten eine Ergänzung des Bundesbeamtengesetzes aus Gründen der Klarstellung erörtern.

9.2.4 Weitergabe von Personaldaten an den Petitionsausschuß

Die Oberfinanzdirektion München hatte gegen einen Mitarbeiter ein Zwangspensionierungsverfahren eingeleitet. In diesem Zusammenhang wurde u. a. ein Gutachten durch die Nervenklinik der Universität München erstellt. Mit der darin vertretenen körperlichen und geistigen Leistungseinschätzung durch den Dienstherrn war der Mitarbeiter nicht einverstanden. Er wandte sich an den Petitionsausschuß des Deutschen Bundestages, der das Bundesministerium der Finanzen um Stellungnahme bat. Dieses beschränkte sich zunächst darauf, dem Petitionsausschuß die Termine der amtsärztlichen Untersuchungen und die seinerseits gezogenen Folgerungen für die dienstliche Verwendbarkeit des betroffenen Mitarbeiters mitzuteilen. Nachdem das Ministerium erfahren hatte, daß die gutachterliche Leistungseinschätzung vom Petenten als medizinisch nicht nachgewiesen dargestellt wurde, zitierte es gegenüber dem Petitionsausschuß aus den ärztlichen Befunden und Feststellungen, „um diese unsubstantiierte Behauptung zu entkräften". Die betreffenden Stellungnahmen waren teilweise mit der Aufschrift „nicht für den Petenten bestimmte Hinweise" versehen. Mir gegenüber begründete das Ministerium dies damit, bisherige Erfahrungen hätten gezeigt, daß der Petent aufgrund seiner Persönlichkeitsstruktur zu Mißverständnissen und Überreaktionen neige, was allen Bemühungen der Verwaltung, mit ihm eine dienstliche Zukunftsperspektive zu entwickeln, zuwidergelaufen sei. Zur Rechtfertigung für die Weitergabe dieser höchst sensiblen personenbezogenen Daten an den Petitionsausschuß berief sich das Bundesministerium der Finanzen auf die Ausführungen des Petenten und darauf, daß dieser selbst ein fachärztliches Attest an den Petitionsausschuß weitergeleitet habe.

Ich habe dem Petitionsausschuß des Deutschen Bundestages und dem Bundesministerium der Finanzen mitgeteilt, daß diese Vorgehensweise mit datenschutzrechtlichen Bestimmungen nicht vereinbar ist.

Zwar vertrete ich die Meinung, daß sich eine Weitergabe von Personaldaten an den Petitionsausschuß grundsätzlich dann im Rahmen der vorgesehenen Zweckbindung hält, falls und soweit sich ein Petent selbst mit einer seine Dienststellung betreffenden Eingabe an den Petitionsausschuß wendet. Man wird in diesem Fall davon ausgehen müssen, daß er mit seiner Petition auch den Auftrag zur umfassenden Sachaufklärung verbindet. Allerdings halte ich es auch in diesen Fällen für geboten, den Petenten über die beabsichtigte Übersendung seiner Personalakte oder von Auszügen daraus zu unterrichten und ihm eine Widerspruchsmöglichkeit einzuräumen, sofern seine Einwilligung nicht schon ausdrücklich aus der Petition zu entnehmen ist. Die Weitergabe ist ausnahmsweise ohne Einverständnis zulässig, wenn sie mit dem Verhältnismäßigkeitsgrundsatz vereinbar und die Geheimhaltung daher nicht erforderlich ist. Überwiegende schutzwürdige Interessen der Allgemeinheit an der Übersendung der Personalinformationen über den Petenten an den Petitionsausschuß wurden seitens des Ministeriums jedoch nicht vorgetragen und sind auch nicht zu erkennen. Des weiteren kann allein aus der Tatsache, daß der Petent dem Petitionsausschuß selbst ein fachärztliches Attest vorgelegt hat, nicht ohne weiteres auf sein Einverständnis geschlossen werden, weitere Personalunterlagen an den Petitionsausschuß zu geben. Dies gilt insbesondere für die Teile der übermittelten Unterlagen, von deren Existenz er überhaupt keine Kenntnis hatte. Sie enthielten höchst sensible medizinische Daten über ihn, wie z. B.: „Klinisch auffällig waren eine visomotorische Verlangsamung, eine grenzwertige Beeinträchtigung des visuellen Gedächtnisses sowie eine deutliche Einschränkung von geistiger Flexibilität und Überblicksfähigkeit".

Es wäre vorliegend also geboten gewesen, den Mitarbeiter über die beabsichtigte Übersendung seiner Personalunterlagen zu unterrichten und ihm eine Widerspruchsmöglichkeit einzuräumen. Die Vorgehensweise des BMF war mit dem in § 90 Abs. 1 Satz 1 BBG normierten Vertraulichkeitsgrundsatz der Personalunterlagen mithin nicht vereinbar.

9.3 Beendigung von Arbeitsverhältnissen

Der Verlust eines Arbeitsplatzes hat für den betroffenen Arbeitnehmer häufig existentielle Bedeutung. Die Folge sind nicht selten arbeitsgerichtliche Auseinandersetzungen. Der Arbeitgeber ist daher interessiert, eine Vielzahl von Informationen über den Betroffenen zu erhalten, um die Beendigung des Arbeitsverhältnisses hinreichend begründen zu können. Dies geschieht zum einen mit dem Hinweis einer möglichst gerechten Auswahl unter mehreren Arbeitnehmern und zum anderen, um in möglichen späteren Streitverfahren ausreichend Argumente für die Entscheidung zu haben.

Zu diesem Themenkreis haben mich insbesondere das Sozialplanverfahren, die Übermittlung von Diagnoselisten bei Kündigungsentscheidungen sowie die Beteiligung der Personalräte beschäftigt.

9.3.1 – Ehemalige – Deutsche Reichsbahn gestaltet Sozialplanverfahren datenschutzgerecht

Im Rahmen von Rationalisierungsmaßnahmen bei der ehemaligen Deutschen Reichsbahn wurden – unter Beteiligung der jeweiligen Personalvertretung – Sozialpläne erarbeitet und während der Durchführung der Rationalisierungsmaßnahmen laufend nach neuen Erkenntnissen ergänzt.

Sozialpläne werden für die Mitarbeiter erstellt, deren Arbeitsplätze (Dienstposten) verlegt werden oder wegfallen oder deren Tätigkeit ihrem Umfang oder ihrem Inhalt nach sich in der Weise ändert, daß sie auf ihren bisherigen Arbeitsplätzen (Dienstposten) nicht dauernd weiterverwendet werden können. Bei diesem Verfahren werden eine Menge von personenbezogenen Daten über die Mitarbeiter erhoben und verarbeitet.

Dabei ergibt sich eine Vielzahl von datenschutzrechtlichen Problemen, wie sie sich im Bereich der DR insbesondere an folgenden Beispielen aufzeigen lassen:

- Es werden zu viele Daten über die Mitarbeiter erhoben.
- Den Betroffenen ist oftmals unklar, welche Konsequenzen eine Verweigerung von Auskünften durch sie gegenüber dem Arbeitgeber hat.
- Die Betroffenen werden im Unklaren darüber gelassen, daß nicht nur ihre eigenen Angaben, sondern auch Informationen Dritter über sie in dem Sozialplanverfahren von Bedeutung sind.
- Einzelne Begriffe in den Fragebögen sind nicht eindeutig definiert, was zu Unklarheiten bei der Beantwortung und daher ggf. zu Nachteilen für die Mitarbeiter führt.

Meine Kontrolle hatte zur Folge, daß die DR – indem sie meinen Empfehlungen folgte – ein datenschutzgerechtes Sozialplanverfahren gestaltet hat. Dabei sind insbesondere folgende datenschutzgerechte Lösungen auch von allgemeiner Bedeutung:

- Der Arbeitgeber benötigt eine Vielzahl von Informationen, um eine Sozialauswahl vornehmen zu können. Die aus dem datenschutzrechtlichen Transparenzgebot fließende Informationspflicht der Betroffenen wird zukünftig durch einen Aufklärungstext erfüllt. Damit wird dem Mitarbeiter nochmals ausdrücklich klargelegt, daß eine Verweigerung seiner Mitwirkung nicht verhindern kann, in das Sozialplanverfahren einbezogen zu werden. Des weiteren wird er darauf hingewiesen, daß unter Umständen Daten über ihn bei Dritten erhoben werden können, worüber er jedoch rechtzeitig informiert wird und Gelegenheit zur Stellungnahme erhält.
- Zwar wurde nur danach gefragt, ob der Betroffene „pflegebedürftige" Personen zu betreuen hat. Die Frage der Pflegebedürftigkeit war jedoch nicht näher erläutert. Nunmehr ist sichergestellt, daß die Personalsachbearbeiter diesen Begriff näher darlegen.
- Im Zusammenhang mit der Frage nach einer „Behinderung" dürfen keine Diagnosen mehr erhoben und gespeichert werden. Es ist nur der Grad der Behinderung auf dem Erfassungsbogen zu vermerken.
- Das Beifügen von Arbeitszeugnissen zu den Sozialplanunterlagen ist aus datenschutzrechtlicher Sicht unzulässig. Die Deutsche Reichsbahn hat veranlaßt, daß in der Vergangenheit beigefügte Arbeitszeugnisse umgehend an die jeweilige Dienststelle zurückzugeben sind.
- Die von der DR geführte Datei im Rahmen des Sozialplanverfahrens enthielt bei den Betroffenen ein Feld „Bemerkungen" für allgemeine Eintragungen. Es konnte erreicht werden, daß ein abschließender Datenkatalog über die zulässigen Eintragungen aufgestellt wurde; dies sind Angaben im Zusammenhang mit Schichtdienst, Wohneigentum, Teilzeit, Dauerkrankheit (lt. Attest), beschränkte Einsatzmöglichkeiten und Antrag auf Erwerbsunfähigkeitsrente/Altersrente. Zusätzliche Einträge, insbesondere über die Arbeitsleistung, die eine Bewertung beinhalten, sind unzulässig.

9.3.2 Diagnosen von Mitarbeitern werden für Kündigungsentscheidungen herangezogen

Die Bundesdruckerei hatte in mehreren Fällen von der Bundespost-Betriebskrankenkasse Diagnoselisten einzelner Mitarbeiter angefordert. Dies geschah auf der Grundlage von Einwilligungserklärungen der Betroffenen. Dabei handelte es sich um Mitarbeiter, bei denen die Frage einer Kündigung im Raum stand. Die Anforderungen wurden mit dem Eigeninteresse der Betroffenen begründet. Anderenfalls müßten Kündigungen allein wegen der Tatsache hoher Fehlzeiten ausgesprochen werden.

Ich habe der Bundesdruckerei mitgeteilt, daß dieses Verfahren mit datenschutzrechtlichen Bestimmungen nicht vereinbar ist. Dieser Rechtsansicht hat die Bundesdruckerei widersprochen und mitgeteilt, daß sie auch zukünftig entsprechende Ersuchen an die Betriebskrankenkasse richten wird. Daraufhin habe ich das Verhalten der Bundesdruckerei förmlich gemäß § 25 Abs. 1 BDSG als einen Verstoß gegen die §§ 13 Abs. 1, 12 Abs. 4 i.V. m. 28 Abs. 1 Satz 2 BDSG beanstandet.

Nach meiner Bewertung liegen hier unzulässige Datenerhebungen vor, weil die Diagnoselisten für die Aufgabenerfüllung der Bundesdruckerei nicht erforderlich sind. Insbesondere besteht kein Fragerecht des Arbeitgebers bezüglich der Diagnosen bei den Arbeitnehmern. Der Ausschluß eines Fragerechts gegenüber Arzt und Arbeitnehmer darf nicht durch ein Offenbarungsersuchen gegenüber der Krankenkasse umgangen werden. Denn auch von einem untersuchenden Arzt darf der Arbeitgeber nur die für den Arbeitsplatz relevanten Schlußfolgerungen erfragen, nicht jedoch beispielsweise die Untersuchungsergebnisse im einzelnen. Eine Entbindung des Arztes von der Schweigepflicht ist unzulässig, da die Grenzen des arbeitgeberseitigen Fragerechts nicht dispositiv sind. Nichts anderes kann für die Einwilligung in die Diagnoseoffenbarung durch die Krankenkasse gelten; ist schon die Datenerhebung beim Betroffenen selbst ausgeschlossen, so muß dies erst recht für eine Datenerhebung über ihn bei Dritten gelten.

Dieses Ergebnis wird auch von der Stellungnahme der Bundesregierung zu meinem 14. Tätigkeitsbericht (zu Pkt. 14.4) getragen. Dort führt die Bundesregierung u. a. aus:

„Der Rechtsauffassung des Bundesbeauftragten für den Datenschutz, daß eine Einsichtnahme in die Unfallakte aus datenschutzrechtlicher Sicht unzulässig sei, dürfte im Ergebnis zuzustimmen sein. Durch die Einsicht in die Unfallakte würde der Arbeitgeber auch ärztliche Gutachten über den Gesundheitszustand seiner Arbeitnehmer zur Kenntnis bekommen. Das Fragerecht des Arbeitgebers über den Arbeitnehmer ist – namentlich hinsichtlich seiner Erkrankungen – auf ganz bestimmte Umstände begrenzt und kann auch durch Einwilligung nicht erweitert werden. Die Begrenzung des Fragerechts begrenzt

auch sein Recht, Tatsachen über den Arbeitnehmer bei Dritten zu erheben. Würde man hier die Einwilligung des Arbeitnehmers zur Akteneinsicht als wirksam ansehen, könnten diese arbeitsrechtlichen Schranken umgangen werden."

Des weiteren enthalten die Diagnoselisten eine Vielzahl von Überschußinformationen, die in keiner Weise für die Kündigungsentscheidung erforderlich sind. Auch widerspricht dieses Verhalten der ausdrücklichen gesetzlichen Wertung des § 275 Abs. 1 Nr. 3 b SGB V und § 69 Abs. 4 SGB X, wonach keine Diagnoseangaben von den Krankenkassen an Arbeitgeber gegeben werden dürfen.

Aufgrund meiner Beanstandung hat das Bundesministerium für Post und Telekommunikation die Bundesdruckerei angewiesen, das hier in Frage stehende Verfahren entsprechend meiner Forderung einzustellen.

9.3.3 Ein Personalrat fordert im Rahmen eines Kündigungsverfahrens „Sozialdaten" über den Betroffenen

Der Oberbundesanwalt beim Bundesverwaltungsgericht hatte mich zu einem beim Bundesverwaltungsgericht anhängigen Rechtsbeschwerdeverfahren um Stellungnahme gebeten. In diesem Verfahren stellte sich die Rechtsfrage, ob einer Personalvertretung bei einer verhaltensbedingten ordentlichen Kündigung vom Dienststellenleiter im Mitwirkungsverfahren gemäß § 79 Abs. 1 BPersVG grundsätzlich auch die „Sozialdaten" des zu Kündigenden mitzuteilen sind. Gemeint waren hier nicht die Sozialdaten im sozialversicherungsrechtlichen Sinn, sondern die sozialen Lebensverhältnisse des Beschäftigten kennzeichnende Personaldaten wie z. B. Lebensalter, Familienstand und Unterhaltsverpflichtungen.

Eine generelle Übermittlung der „Sozialdaten" des zu Kündigenden, die sich nicht daran orientiert, ob diese Informationen für die Kündigungsentscheidung erforderlich sind, ist mit dem Personalaktengeheimnis und mit dem Recht auf informationelle Selbstbestimmung nicht vereinbar.

Hierbei ist zwar einerseits zu berücksichtigen, daß sich die Aufgaben und Befugnisse, die dem Personalrat gesetzlich zugewiesen sind, ausschließlich auf den internen Bereich der Dienststelle erstrecken. Das Bundesverfassungsgericht hat in einem Beschluß vom 31. August 1986 2 BvR 467/76 – ausdrücklich festgestellt, daß der (Haupt-)Personalrat keine eigene Rechtspersönlichkeit besitzt, sondern eine öffentlichrechtliche Organstellung im internen Verwaltungsaufbau hat. Demzufolge ist der Personalrat kein Dritter im Sinne von § 3 Abs. 9 BDSG. Eine Weitergabe von personenbezogenen Daten stellt somit keine Übermittlung im Sinne des § 3 Abs. 5 Nr. 3 BDSG dar.

Davon unabhängig gilt jedoch, daß es sich bei den hier in Frage stehenden „Sozialdaten" datenschutzrechtlich um Personaldaten handelt. Nach dem Rechtsgedanken der §§ 90 ff. BBG sind diese vertraulich zu behandeln und vor unbefugter Einsicht zu schützen. Dies bedeutet, daß sie auch gegenüber der Personalvertretung nur in dem Umfang weitergegeben werden dürfen, wie sie für deren Aufgabenerfüllung erforderlich sind.

Rechtlicher Ausgangspunkt für den Informationsanspruch ist hierbei § 68 Abs. 2 Sätze 1 und 2 BPersVG. Hiernach ist die Personalvertretung zur Durchführung ihrer Aufgaben rechtzeitig und umfassend zu unterrichten. Ihr sind die hierfür erforderlichen Unterlagen vorzulegen. Aus § 68 Abs. 2 BPersVG läßt sich aber keine Informationspflicht des Dienststellenleiters herleiten, die alles umfaßt, was unter den gegebenen Umständen objektiv als wissenswert angesehen werden kann. Die Informationspflicht der Dienststelle und dementsprechend der Anspruch des Personalrats sind vielmehr auf diejenigen Informationen beschränkt, die die Person des zu Kündigenden bezeichnen und darüber hinaus auf alle Umstände und vom Dienststellenleiter angestellte Erwägungen, aufgrund derer er die Kündigung für gerechtfertigt hält. Sind bestimmte „Sozialdaten" daher aus der Sicht des Dienststellenleiters für die Entscheidung über die verhaltensbedingte Kündigung nicht erforderlich, so hat er dem Personalrat solche Daten nur mitzuteilen, wenn dieser darlegt, daß sie für seine Beurteilung erforderlich sind, oder wenn der Betroffene einwilligt.

Ein über diese Erforderlichkeitsgrenze hinausgehender Informationsanspruch der Personalvertretung wäre mit dem Recht auf informationelle Selbstbestimmung der Betroffenen nicht vereinbar. Die freie Entfaltung der Persönlichkeit setzt den Schutz des einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten voraus.

Der Gekündigte muß daher im Ergebnis selbst entscheiden können, ob und ggf. welche personenbezogenen Informationen über ihn – zusätzlich zu den für die Kündigung – der Personalvertretung bekannt werden. Dies kann dadurch geschehen, daß sich die Personalvertretung im Einzelfall an den Betroffenen wendet und ihn um zusätzliche Informationen bittet. Oder die zweite Möglichkeit: Der Betroffene tritt von sich aus an die Personalvertretung heran und legt dar, welche Tatsachen aus seiner Sicht bei der Bewertung der Kündigungsentscheidung berücksichtigt werden sollten. In beiden Fällen ist dann gewährleistet, daß der Gekündigte selbst über die Weitergabe seiner – oftmals sehr sensiblen – Personaldaten, die im konkreten Fall auch seine Privatsphäre betreffen können, entscheidet. Selbst wenn er möchte, daß die Personalvertretung der Kündigung widerspricht, kann er dann bestimmen, welche Informationen er ihr hierfür zur Verfügung stellt.

9.4 Betriebsärztliche und sonstige interne Dienste, die der Schweigepflicht des § 203 StGB unterliegen

9.4.1 Inhalt und Umgang mit Patientenakten betriebs-/dienststellenintern regeln

Bei einer datenschutzrechtlichen Kontrolle (vgl. Nr. 9.1.2.3) hatte das Bundesministerium der Verteidigung zugesagt, schriftliche Regelungen für den refe-

ratsinternen Umgang mit Patientenakten von Bediensteten zu schaffen (vgl. 13. TB S. 44 f.). Die Regelungen sollten insbesondere die Zugriffsrechte der Angehörigen der zuständigen Arbeitseinheit aufgabenbezogen regeln sowie eine Dokumentation der Einzelzugriffe vorsehen, damit insbesondere Zeitpunkt, Bearbeiter und Anlaß der Bearbeitung nachvollziehbar und ggf. nachprüfbar wären.

Eine inzwischen erlassene Anordnung ist im Hinblick auf die Belehrung der Betroffenen über die ärztliche Schweigepflicht (§ 203 StGB) datenschutzrechtlich zu begrüßen. Weitere Regelungen hat das Bundesministerium der Verteidigung mit der Begründung abgelehnt, daß in der Arbeitseinheit lediglich fünf Personen im Rahmen ihrer Zuständigkeit Zugriff auf Patientenakten haben. Vertretungsregelungen würden nur innerhalb dieser Organisationseinheit gelten, so daß im Laufe eines Jahres jeder Mitarbeiter dieser Einheit theoretisch die Möglichkeit habe und aus sachlichen Gründen auch haben müsse, jede Patientenakte ggf. einmal einzusehen.

Zum Umgang mit ärztlichen Unterlagen will das Auswärtige Amt einen Erlaß mit Regelungen zur Erhebung, Verarbeitung und Nutzung solcher personenbezogenen Daten herausgeben. In einem Entwurf habe ich Verbesserungsvorschläge gemacht und meine weitere Beratung angeboten.

Im Berichtszeitraum habe ich darüber hinaus das BMI anläßlich der Neuorganisation des BGS bei der Überarbeitung des Erlasses über die Führung Ärztlicher Aufzeichnungen beraten. Hierüber konnte eine aus datenschutzrechtlicher Sicht akzeptable Lösung gefunden werden.

9.4.2 Abschottung des Sozialpsychologischen Dienstes einer obersten Bundesbehörde von der Personalabteilung

Mehrere datenschutzrechtliche Eingaben einer Petentin haben ein grundsätzliches Problem bei der Abschottung des Sozialpsychologischen Dienstes einer obersten Bundesbehörde von der Personalabteilung aufgezeigt. Ursprünglicher Anlaß der Eingabe war, daß der Sozialpsychologische Dienst dieser Bundesbehörde Mitarbeitern angeboten hat, im Bedarfsfalle für sie beratend tätig zu werden. Die bei dieser „freiwilligen" Beratung festgehaltenen Daten wurden jedoch nicht nur in die Gesundheitsakte der betreffenden Person übernommen, sondern teilweise auch an andere Stellen innerhalb der Behörde übermittelt, so z. B. an die Personalabteilung für personalwirtschaftliche Belange. Wie ich bereits früher (siehe 14. TB S. 72) ausgeführt habe, ist eine derartige Übermittlung allenfalls im Rahmen einer offiziellen Gutachtertätigkeit des Sozialpsychologischen Dienstes im Auftrag der Personalverwaltung möglich, und dies auch nur dann, wenn dem Betroffenen Zweck und Umfang der Untersuchung und der angestrebten Datenübermittlung offenbart und im einzelnen erläutert werden.

Erschwerend kommt im vorliegenden Fall hinzu, daß die Petentin die Richtigkeit der erhobenen Daten bestreitet. Ich habe daher die Behörde um Löschung der Daten gebeten. Diese Löschung wurde mit der Begründung versagt, die Daten würden ggf. zu Beweissicherungszwecken benötigt. Ich habe daraufhin sowohl der Petentin als auch der Behörde vorgeschlagen, die Daten zu sperren, so daß nur eine Nutzung zu dem angesprochenen Zweck unter Beteiligung der Petentin möglich ist. Eine Stellungnahme hierzu steht von beiden Seiten noch aus.

Auch bei der grundlegenden Fragestellung der Abschottung des Sozialpsychologischen Dienstes von der Personalabteilung wurden datenschutzrechtliche Fortschritte durch die Neufassung einer Hausverfügung für den Sozialpsychologischen Dienst erzielt. Danach wird zwischen „beratender", also durch den freiwilligen Wunsch eines Mitarbeiters veranlaßter und „beurteilender", also im dienstlichen Auftrag stattfindender Tätigkeit unterschieden. Damit wird auch dem Betroffenen erkennbar, wann mit einer Weitergabe an den Dienstherrn zu rechnen ist.

9.4.3 Schweigepflicht gilt auch gegenüber dem Dienstherrn

Sowohl im Zusammenhang mit Kontrollen bei obersten Bundesbehörden wie auch aufgrund mehrerer Eingaben wurde die Frage aufgeworfen, inwieweit ein als Gutachter eingeschalteter Arzt Einzelheiten aus Gesundheitsunterlagen eines Beamten (Diagnose, Befunde etc.) an den Dienstvorgesetzten weiterleiten darf bzw. inwieweit er hierzu verpflichtet ist.

Zur Frage der Geltung der ärztlichen Schweigepflicht (§ 203 Abs. 1 Nr. 1 StGB) gegenüber dem Dienstherrn hatte ich das Bundesministerium der Justiz um eine Stellungnahme gebeten. Im konkreten Fall war zu beantworten, ob diese Vorschrift auch auf den in einem Zwangspensionierungsverfahren nach § 44 BBG als Gutachter tätigen Arzt anwendbar ist. Das Ministerium stimmt im Ergebnis meiner Auffassung zu, daß § 203 Abs. 1 Nr. 1 StGB auch für den zum gerichtlichen oder behördlichen Sachverständigen bestellten Arzt gilt. Denn auch bei der Erstellung eines Gutachtens im Zusammenhang mit einer Maßnahme nach § 44 BBG wird der damit beauftragte Arzt „als Arzt", von dem grundsätzlich Verschwiegenheit erwartet wird, tätig. Daß der Arzt dem Untersuchten dabei erkennbar mit der Absicht gegenübertritt, die für die Erfüllung seines Gutachtenauftrages notwendigen Informationen an seinen Arbeitgeber mitzuteilen, bedeutet nicht, daß der Untersuchte vom Arzt keinerlei Verschwiegenheit erwarten kann. Auch hier muß der Untersuchte vielmehr davon ausgehen können, daß der Arzt Informationen nicht offenbart, die zur Erfüllung des Gutachtenauftrages nicht erforderlich sind, und daß er Informationen nur in dem Verfahren, in dem er bestellt worden ist, und nur an die Stelle, die ihn beauftragt hat, weitergibt. Danach darf der Arzt lediglich das Ergebnis der ärztlichen Untersuchung mitteilen; d. h. die Feststellung, ob der Beamte dienstfähig, nicht dienstfähig oder nur eingeschränkt dienstfähig (und ggf. mit welchen Einschränkungen) ist. Darüber hinausgehende Daten sind für die Aufgabenerfüllung der Personalverwaltung grundsätzlich nicht erforderlich; ihre Offenbarung ist daher unzulässig.

Gegenüber der Deutschen Bahn AG habe ich daher die Offenbarung ärztlicher Informationen durch den Oberbahnarzt gegenüber dem Dienstherrn gem. § 25 BDSG als einen Verstoß gegen das Arztgeheimnis (§ 203 StGB) beanstandet. Darüber hinaus habe ich der Deutschen Bahn AG empfohlen, dringend eine einheitliche Handhabung im Umgang mit ärztlichen Unterlagen im Bereich der Deutschen Bahn sicherzustellen.

Eine weitere, vergleichbare Fragestellung wurde aus dem Bereich der Sozialarbeiter an mich herangetragen (siehe Nr. 31.2.1).

9.5 Beihilfeverfahren

9.5.1 Beihilfe und eigenes Antragsrecht für Angehörige

Bereits früher (12. TB S. 33) hatte ich einen eigenen Beihilfeanspruch und damit ein eigenes Antragsrecht der Familienangehörigen von Beihilfeberechtigten gefordert. Der BMI hatte diese Frage in der Bund-Länder-Kommission für das Beihilferecht erörtert. Im Ergebnis wurde die Einführung eines solchen Antragsrechts mit der Begründung abgelehnt, aus der Fürsorgepflicht des Dienstherrn nach § 79 BBG ergäben sich keine eigenen Ansprüche von Angehörigen des Beihilfeberechtigten gegenüber dem Dienstherrn. Der Innenausschuß des Deutschen Bundestages hatte sich der Meinung des BMI angeschlossen.

Im Interesse der datenschutzrechtlichen Belange von Angehörigen hat das BMI folgendes Verfahren vorgeschlagen:

In der Praxis können die betreffenden Familienangehörigen ihre Belege unmittelbar der Beihilfestelle zuleiten, während der Beihilfeberechtigte hierauf lediglich pauschal Bezug nimmt, z. B. indem er angibt, daß es sich um ein Rezept handelt. Hieraus kann er dann keine weiteren Rückschlüsse ziehen. Desgleichen werden die Belege von der Beihilfestelle auch unmittelbar an das betroffene Familienmitglied zurückgesandt.

Insbesondere unter Berücksichtigung der verfassungs- und beamtenrechtlichen Argumentation des BMI halte ich dieses Verfahren für nur teilweise geeignet, auch datenschutzrechtlichen Anforderungen gerecht zu werden. Ich werde mich daher weiter für Lösungen einsetzen, die vor allem der Situation von getrennt lebenden Ehepaaren Rechnung tragen.

9.5.2 Beihilfeverfahren bei der Postbeamtenkrankenkasse

9.5.2.1 Das Beihilfeverfahren wird datenschutzgerecht geregelt

Die Beihilfesachbearbeitung bei der Postbeamtenkrankenkasse begegnet mit einer Ausnahme keinen datenschutzrechtlichen Bedenken:

Für die Entscheidung über Widersprüche gegen Beihilfeentscheidungen sind bei den Direktionen Postdienst die Stellen zuständig, die wie die jeweiligen für Personal und Soziales zuständigen Abteilungsleiter an Personalentscheidungen beteiligt sind. Dies widerspricht dem Grundsatz, daß Beihilfe- und Sozialdaten den für die Bearbeitung von Personalangelegenheiten der Betroffenen zuständigen Personen nach dem Rechtsgedanken des § 90 a BBG nicht bekannt werden dürfen.

Die Postbeamtenkrankenkasse hat mir mittlerweile zugesichert, das Widerspruchsverfahren in Beihilfeangelegenheiten so zu regeln, daß dabei Personen, die Personalentscheidungen treffen oder an diesen mitwirken können – also auch im Rahmen von Vertreterregelungen – künftig nicht mehr beteiligt werden.

9.5.2.2 Ein Vater erfährt von der Postbeamtenkrankenkasse, daß seine Tochter die Pille nimmt

Ein Frauenarzt hatte einer 16jährigen Patienten auf Kassenrezept die Pille verschrieben. Das Kassenrezept auf den Namen der Patientin wurde von der Postbeamtenkrankenkasse dem Vater als „Hauptversicherten" mit der Bitte um Kostenerstattung zugeschickt, da es nicht beihilfefähig sei. Nach Meinung des Arztes hat damit die Postbeamtenkrankenkasse sowohl ihre, wie auch seine Schweigepflicht verletzt. Er hatte der Patientin ausdrücklich zugesagt, daß ihre Eltern nichts von der Pilleneinnahme erfahren werden. Das Rezept wurde über die zuständige Apothekenabrechnungsstelle von der Apotheke der Kasse zugeleitet. Dies sieht ein Vertrag der Postbeamtenkrankenkasse mit dem Deutschen Apothekerverein e.V. so vor.

Dieses Verfahren ist unerfreulich, verstößt gegenwärtig aber nicht gegen datenschutzrechtliche Bestimmungen. Für die Bewertung aus datenschutzrechtlicher Sicht ist dabei insbesondere von Bedeutung, daß die rechtlichen Beziehungen nur zwischen den Mitgliedern selbst und der Postbeamtenkrankenkasse bestehen. Daran ändert auch nichts, daß ggf. Ehegatten und Kinder eines Mitglieds auf Antrag mitversichert werden können.

Im Rahmen des Abrechnungsverfahrens stellte die Postbeamtenkrankenkasse im vorliegenden Fall anläßlich einer Prüfung fest, daß die verschriebene Pille zum Zeitpunkt der Verordnung nicht beihilfe- und erstattungsfähig gewesen ist. Die Rückforderung geschah zurecht gegenüber dem Vater, da dieser Mitglied der Kasse ist.

Im Interesse der mitversicherten Familienangehörigen habe ich der Postbeamtenkrankenkasse empfohlen, ein Verfahren einzuführen, bei dem die Angehörigen ihre Belege unmittelbar der Beihilfestelle zuleiten können, während der Beihilfeberechtigte hierauf lediglich pauschal Bezug nimmt, z. B. indem er angibt, daß es sich um ein Rezept handelt. Desgleichen sollten die Belege von der Beihilfestelle auch unmittelbar an das betroffene Familienmitglied zurückgesandt werden. Diesem Verfahren hat die Postbeamtenkrankenkasse im Grundsatz zugestimmt, wenn vom Familienangehörigen eines Beihilfeberechtigten dies gewünscht wird (siehe auch Nr. 9.5.1).

9.6 Personalvertretung, Frauenbeauftragte und Datenschutz

9.6.1 Zugriffsrechte der Mitarbeitervertretung auf Personaldaten

Mit den Fragen, welche Personaldaten und -auskünfte die Personalvertretung zur sachgerechten Aufgabenerfüllung gem. § 68 Abs. 2 BPersVG von der Dienststelle verlangen kann, habe ich mich zuletzt in meinem 14. Tätigkeitsbericht befaßt (S. 64). Im Vordergrund der Problematik steht die Information über die Endnote der Beurteilung und der online-Direktzugriff der Personalvertretung auf Daten in einem Personalinformationssystem.

Zur Klärung datenschutzrechlich relevanter Vorfragen habe ich in einer Umfrage an alle obersten Bundesbehörden, die Deutsche Bundesbahn, die Generaldirektion Postdienst, die Postbank und die Generaldirektion Telekom der Deutschen Bundespost zu klären versucht, ob bei diesen Behörden oder in deren Geschäftsbereich ein online-Zugriffsrecht des Personalrats auf bestimmte Daten in einem Personalinformationssystem besteht sowie ob und ggf. welche Personaldaten dem Personalrat in Listenform zur Verfügung gestellt werden. Auf meine Umfrage haben 43 Dienststellen des Bundes geantwortet. Ein online-Zugriffsrecht bestand in zwei Dienststellen. In einer wurde es mittlerweile aufgegeben. In einem dieser Fälle war das Zugriffsverfahren in einer Dienstvereinbarung geregelt, im anderen liegt dem Verfahren der Beschluß der Einigungsstelle zugrunde. Bei 32 Dienststellen werden den Personalräten Personalaktendaten in Listenform zur Verfügung gestellt. Diese Listen enthalten beispielsweise die Titelbezeichnung, Name, Vorname, Geburtsdatum, Eintrittsdatum, Besoldungs- bzw. Vergütungs- und Lohngruppe, teilweise das Datum der letzten Beförderung, Dienststellung, Beschäftigungszeit, Dienstzeit, Einsatzgebiet und Sprachen (verschlüsselt) und in einem Fall auch die Endnote der letzten Beurteilung. Die Zeitabstände, in denen die Listen zur Verfügung gestellt werden, schwanken zwischen einem und zwei Monaten und einem halben Jahr. Bei den übrigen Dienststellen erhält der Personalrat einzelfallbezogen die für die Beurteilung des jeweiligen Vorganges notwendigen Unterlagen.

Vor dem Hintergrund dieses Umfrageergebnisses habe ich die Fragen der Zulässigkeit von Umfang und Form der dem Personalrat zur Verfügung zu stellenden Informationen mit den Datenschutzbeauftragten der Länder mit folgendem Ergebnis erörtert:

Nach Rechtsprechung und herrschender Meinung in der Literatur kann die Personalvertretung alle Daten und Auskünfte von der Dienststelle verlangen, die sie zur sachgerechten Aufgabenerfüllung, insbesondere der Wahrnehmung ihrer Beteiligungsrechte, benötigt. Welche Daten ihr im einzelnen zustehen, hängt von den konkreten Verhältnissen in der Dienststelle ab. Aus datenschutzrechtlicher Sicht bestehen keine Bedenken, dem Personalrat, unabhängig von Beteiligungsverfahren, bestimmte Grunddaten, die er auf Dauer benötigt, zur Verfügung zu stellen. Das gilt auch für ein Direktzugriffsverfahren.

Dieses Ergebnis wurde im Berichtszeitraum durch eine Entscheidung des Bundesverwaltungsgerichts bestätigt (Beschluß vom 26. Januar 1994 – BVerwG 6 P 21.92). Das Gericht kommt dabei u. a. zu folgenden wesentlichen Feststellungen:

- Die Informations- und Vorlagepflicht der Dienststelle gem. § 68 Abs. 2 Sätze 1 und 2 BPersVG beurteile sich allein nach Maßgabe der Vorlagefähigkeit und der Erforderlichkeit. In diesem Zusammenhang komme es auf den Standpunkt einer „objektiven Personalvertretung" an. Ausschlaggebend sei, was aus ihrer Sicht bei verständiger Würdigung als für die Aufgabenerfüllung noch bedeutsam angesehen werden kann.
- Die Vorschriften des § 68 Abs. 2 Sätze 3 und 4 BPersVG stellten dieses Ergebnis nicht in Frage. Persönlichkeitsrechte der Beschäftigten würden insbesondere nicht schon dadurch verletzt, daß dem Personalrat Stellungnahmen, Berichte und Zusammenstellungen von Daten, welche die Dienststelle zu reinen Übersichtszwecken erstellt hat sowie abschließende Bewertungen aus den dienstlichen Beurteilungen der Bewerber bekanntgegeben werden.
- In welcher Form dem Personalrat Informationen zu geben und Unterlagen vorzulegen seien – z. B. durch Einsichtnahme, vorübergehende Aushändigung oder gar Überlassung – hänge von den Umständen des Einzelfalles ab. Die unerläßlichen Informationen seien jedenfalls im Rahmen des für die Bewerber Vertretbaren unter Berücksichtigung der Erfordernisse der Geschäftsführung des Personalrats in möglichst schonender Weise zu erteilen.

9.6.2 Aufgaben und Kompetenzen der Frauenbeauftragten

Mehrfach wendeten sich Frauenbeauftragte oberster Bundesbehörden mit Anfragen und Beschwerden an mich. Sie sahen sich in der Erfüllung ihrer Aufgaben und Rechte nach Maßgabe der Frauenförderungsrichtlinie der Bundesregierung behindert. In einem Schreiben der Vorsitzenden des Interministeriellen Arbeitskreises der Frauenbeauftragten der obersten Bundesbehörden wurden insbesondere folgende Punkte hervorgehoben:

- Einzelne Ressorts verweigerten den Frauenbeauftragten die zu ihrer Aufgabenwahrnehmung notwendigen Daten. So seien für die Mitwirkung an Personalentscheidungen entscheidungsrelevante Daten aller Bewerberinnen und Bewerber unter Hinweis auf die Schutzinteressen der männlichen Mitbewerber zurückgehalten und damit eine Mitwirkung der Frauenbeauftragten unmöglich gemacht worden. Dies geschehe besonders häufig bei Personalentscheidungen für Referatsleitungspositionen. In anderen Fällen seien den Frauenbeauftragten mit gleicher Begründung sogar Angaben darüber verweigert worden, wer sich beworben habe.
- Um an Personalentscheidungen mitwirken zu können, aber auch um ihre Initiativrechte ausüben und eigene Vorschläge machen zu können, benötigten die Frauenbeauftragten neben Personal-

daten, die nur fallweise und kurzfristig zur Verfügung zu stellen seien, längerfristig auch Dienstalters-, Stellenbesetzungs- und Beförderungsplanlisten bzw. ein auf die entsprechenden Datenfelder beschränktes Leserecht in von der Personalabteilung betriebenen automatisierten Personalinformationssystemen. Derartige Informationsmöglichkeiten würden ebenfalls von einzelnen Ressorts verweigert.

Die Frauenbeauftragte, die von der Dienststelle berufen wird, nimmt Aufgaben der Dienststelle wahr. Soweit sie an Personalentscheidungen zu beteiligen ist und ihr Initiativrechte zustehen, ist sie rechtzeitig und umfassend zu unterrichten. Ihr sind die dafür erforderlichen Unterlagen frühzeitig vorzulegen und erbetene Auskünfte zu erteilen. Jedoch erst das Zweite Gleichberechtigungsgesetz (2. GleiBG) hat hierfür die eindeutige Rechtsgrundlage gebracht. Die Frauenförderungs-Richtlinie hätte den verfassungsgerichtlichen Anforderungen an einen Eingriff in das informationelle Selbstbestimmungsrecht der betroffenen Bewerber bzw. Mitarbeiter des öffentlichen Dienstes möglicherweise nicht standgehalten.

Im Hinblick auf die bisher umstrittenen Informationsrechte ist die Frauenbeauftragte damit gesetzlich im wesentlichen mit der Personalvertretung vergleichbar. Die insoweit vom Bundesverwaltungsgericht entwickelten Grundsätze (vgl. Nr. 9.6.1) gelten damit entsprechend auch für sie. Inhalt, Umfang, Form und Zeitraum der ihr zustehenden Informationen bestimmen sich jeweils nach der Erforderlichkeit für ihre gesetzliche Aufgabenerfüllung. Maßstab der Beurteilung ist dabei der Standpunkt einer dies verständig würdigenden Frauenbeauftragten.

9.7 Automatisierte Personaldatenverarbeitung

Seit längerem werden mit zunehmender Automatisierung und fortschreitender Entwicklung der modernen Informationstechnik in der Bundesverwaltung verstärkt auch Personaldaten automatisiert verarbeitet. Auf die spezifischen Gefährdungen des Persönlichkeitsrechts der Bediensteten durch die automatisierte Verarbeitung ihrer personenbezogenen Daten habe ich in zahlreichen Tätigkeitsberichten hingewiesen (etwa 8. TB, S. 16 ff.).

Bei der Einführung oder Umstellung zahlreicher automatisierter Systeme wurde ich auch im Berichtszeitraum beteiligt. Es hat sich jedoch erneut gezeigt, daß ich meinen Beratungsauftrag nach § 26 Abs. 3 BDSG nur dann wirkungsvoll erfüllen kann, wenn ich in einem frühen Entwicklungsstadium des Vorhabens eingeschaltet werde, weil dann Datenschutzaspekte noch mit dem geringsten Aufwand in die Entwicklung einfließen können.

Beispiele für eine solch frühzeitige Beteiligung sind die Personalinformations-/Personalverwaltungssysteme im BMJ, BMWi, BMV, BMU, – früheren – BMFT, in den Bereichen der Deutschen Bundespost Telekom und des Postdienstes sowie sonstige automatisierte Systeme, mit denen Mitarbeiterdaten verarbeitet werden (z. B. IT-gestützte Reisekostensysteme).

Ein Thema, das in diesem Zusammenhang immer wieder diskutiert wird, ist der Einsatz von Datenbanksprachen („freie Abfragesprachen"). Ich habe daher den obersten Bundesbehörden „Hinweise zum Einsatz von Datenbanksprachen bei der automatisierten Personaldatenverarbeitung" (siehe Anlage 19) gegeben.

Im Rahmen von Datenschutzkontrollen im Personalwesen habe ich auch die automatisierte Verarbeitung von Mitarbeiterdaten geprüft und hierbei u. a. festgestellt:

9.7.1 Geschäftsführer überwacht Termine mit Laptop

Bei der Kontrolle der Betriebskrankenkasse der Preussag AG (BKK Preussag) wurde im Büro des Geschäftsführers ein Laptop mit Diskettenlaufwerk festgestellt. Die Vorführung des Gerätes ergab, daß personenbezogene Daten der Mitarbeiter in einer Datei „Merke" gespeichert waren. Mit Hilfe dieser Datei überwachte der Stellvertretende Geschäftsführer nach seinen Angaben die termingerechte Erledigung von Aufträgen, die er Mitarbeitern und Dritten außerhalb der BKK zur Vorbereitung eigener Termine erteilt hatte.

Bei der Erörterung der datenschutzrechtlichen Problematik mit der Geschäftsführung, betroffenen Mitarbeitern und dem Betriebsrat stellte sich heraus, daß die Eignung dieser Datei zur Verhaltens- und Leistungskontrolle bisher nicht erkannt worden war.

Da der Geschäftsführer der BKK die Datei noch während der Kontrolle gelöscht und angekündigt hatte, die Terminüberwachung künftig schriftlich zu gestalten, habe ich davon abgesehen, die festgestellte unzulässige Speicherung und Nutzung von Personaldaten förmlich zu beanstanden.

9.7.2 Südwestliche Bau-Berufsgenossenschaft: Zustimmung des Personalrats fehlte

Die von der Bau-BG geführte sogenannte „Gehaltsdatei" erwies sich bei der Datenschutzkontrolle als Personalverwaltungsdatei; sie enthält neben den für die Gehaltszahlung relevanten Datenarten auch alle diejenigen, die im Zusammenhang mit Dienstzeit- und Urlaubsabrechnung erforderlich sind. Damit ist sie als geeignet zur Verhaltens- und Leistungskontrolle der Mitarbeiter anzusehen. Es stellte sich indessen heraus, daß die gemäß § 75 Abs. 3 Nr. 17 BPersVG erforderliche Zustimmung des Personalrats fehlte, die Führung der Datei mithin unzulässig war.

Nachdem die Beteiligten bei der Bau-BG noch während der Kontrolle zugesagt hatten, das Mitbestimmungsverfahren unverzüglich nachzuholen und dabei meine Empfehlungen zum Inhalt derartiger Vereinbarungen (vgl. u. a. 10. TB Nr. 7.4.3) zu berücksichtigen, habe ich von einer förmlichen Beanstandung abgesehen.

9.7.3 Personaldatenverarbeitung beim Kraftfahrt-Bundesamt

Bei der Kontrolle der automatisierten Personaldatenverarbeitung beim Kraftfahrt-Bundesamt habe ich u. a. festgestellt, daß in der dortigen Personaldatei für

die ca. 1 300 Mitarbeiter ein uneingeschränktes freies Abfragen mittels der Datenbanksprache SQL (d. h. beliebige Verknüpfung **aller** Datensatzfelder/personenbezogener Daten der Personaldatei) möglich war.

Ich habe dies aus datenschutzrechtlicher Sicht als nicht zulässig bewertet und dargelegt, daß ich nur unter bestimmten datenschutzrechtlichen Auflagen **in begründeten Einzelfällen** den **eingeschränkten** Einsatz „freier Abfragesprachen" bei der automatisierten Personaldatenverarbeitung für vertretbar halte. Ich habe in diesem Zusammenhang auf mein o.a. Rundschreiben an die obersten Bundesbehörden (siehe Anlage 19) hingewiesen.

Die Thematik wurde noch vor Ort eingehend mit den Vertretern des KBA erörtert. Das KBA hatte aufgrund meines Rundschreibens den datenschutzrechtlichen Handlungsbedarf bereits erkannt. Es bestand Einvernehmen, alle in meinem o.a. Rundschreiben genannten datenschutzrechtlichen Anforderungen schnellstmöglich umzusetzen. Ich habe dringend empfohlen, generell auf vom Anwender der Personaldatei frei formulierte Abfragen zu verzichten.

Das KBA hat mir inzwischen mitgeteilt, daß es die datenschutzrechtlichen Anforderungen erfüllen und in einer Dienstvereinbarung regeln wird. Im Rahmen meiner Beratungsaufgabe habe ich hierbei meine Unterstützung zugesagt.

Die Personaldatei enthält auch einige sog. **Bemerkungsfelder.**

Aus datenschutzrechtlicher Sicht erscheinen Bemerkungsfelder (= Freitextfelder) im Bereich der automatisierten Verarbeitung von Mitarbeiterdaten – unabhängig vom vorliegenden Fall – generell problematisch, da sie für unzulässige, nicht für die Aufgabenerfüllung erforderliche Angaben zumindest geeignet sind.

Ich habe deshalb gebeten, die Erforderlichkeit der einzelnen Bemerkungsfelder zu prüfen und nicht erforderliche Felder zu löschen. Sofern Datenfelder für die Aufgabenerfüllung unverzichtbar sind, ist in geeigneter Weise (z. B. über einen abschließenden Katalog der für die Aufgabenerfüllung erforderlichen zulässigen Eintragungen und schriftliche Anweisung an die Nutzer des Systems) sicherzustellen, daß in diesen Datenfeldern keine unzulässigen Eintragungen vorgenommen werden. Weiterhin habe ich gebeten, die Einhaltung dieser Regelungen in geeigneter Weise – beispielsweise durch den Datenschutzbeauftragten – stichprobenartig zu überprüfen.

Das KBA hat mir hierzu mitgeteilt, daß die für die Aufgabenerfüllung unverzichtbaren Bemerkungsfelder der Personaldatei über einen abschließenden Katalog – der Bestandteil der Dienstvereinbarung wird – und alle sonstigen Bemerkungs-/Freitextfelder in anderen Dateien mit Personaldaten über eine Dienstanweisung, deren Einhaltung stichprobenweise überprüft wird, geregelt werden.

Meine Kontrolle hat ferner ergeben, daß neben der o. a. Personaldatei auch in anderen Fachabteilungen drei eigene automatisierte Dateien mit Personalaktendaten von Mitarbeitern existierten.

Diese Personaldateien wurden eigenständig in den Sachgebieten erstellt und vom jeweiligen Büroleiter für dessen Aufgabe „Personalplanung, -einsatz, -betreuung" geführt.

Aus datenschutzrechtlicher Sicht habe ich die zusätzlich zur eigentlichen Personaldatei in den Fachabteilungen geführten „Personaldateien" als nicht zulässig bewertet, da sie mit zahlreichen Regelungen des Bundesbeamtengesetzes (§ 90 ff. BBG) nicht in Einklang stehen.

Ich habe dringend empfohlen, die unzulässigen Dateien in den Sachgebieten, die darüber hinaus im für die Verwaltung und Personalwirtschaft zuständigen Sachgebiet nicht bekannt waren, zu löschen.

Das KBA hat mir zugesagt, den Sachgebieten, die für deren konkrete Aufgabenerfüllung jeweils erforderlichen personenbezogenen Mitarbeiterdaten aus der Personaldatei (über eine lesende Zugriffsmöglichkeit hierauf) zur Verfügung zu stellen, dies in der Dienstvereinbarung zu regeln und die o. g. „eigenen" Personaldateien nach der Realisierung zu löschen.

9.7.4 Personaldatenverarbeitung bei einer deutschen Botschaft

Bei der Kontrolle des Personalwesens einer deutschen Botschaft habe ich u. a. festgestellt, daß teilweise parallel inhaltsgleiche Personaldateien sowohl automatisiert, als auch nicht-automatisiert geführt wurden. Gründe, die für die Erforderlichkeit für eine solche parallele Führung sprechen könnten, wurden nicht festgestellt.

Unter Hinweis auf § 35 Abs. 2 Nr. 3 BDSG, nach dem personenbezogene Daten zu löschen sind, sobald ihre Kenntnis für die Erfüllung des Zwecks der Speicherung – vorliegend Personalverwaltung – nicht mehr erforderlich ist, habe ich deshalb empfohlen, die nicht-automatisierten Personaldateien (Karteikästen mit Karteiblättern) zu löschen.

In der Personaldatei der Botschaft waren zwei Bemerkungs-/Freitextfelder vorhanden (vgl. Nr. 9.7.3). Auch hier habe ich gebeten, die Erforderlichkeit dieser Felder zu prüfen und sicherzustellen, daß in beiden Datenfeldern keine unzulässigen Eintragungen vorgenommen werden.

9.7.5 Personaldatenverarbeitung beim BAFl

Meine Prüfung der automatisierten Personaldatenverarbeitung im Bundesamt für die Anerkennung ausländischer Flüchtlinge ergab, daß zahlreiche im BAFl mit der Wahrnehmung von Personalangelegenheiten betrauten Arbeitseinheiten mit APC ausgerüstet sind. Da aber weder ein Verzeichnis der eingesetzten Datenverarbeitungsanlagen noch eine Dateien-Übersicht i. S. des § 18 Abs. 2 BDSG vorhanden waren, lagen während meiner Prüfung exakte Kenntnisse über die insgesamt eingesetzten APC und die mit APC ausgerüsteten Arbeitseinheiten ebensowenig vor wie über die Art und Zahl der auf den APC's

geführten Personaldateien. Damit war die Überwachung der ordnungsgemäßen Anwendung der Datenverarbeitungsprogramme i. S. der vorgenannten Vorschrift nicht gewährleistet.

Die Vertreter des BAFl gaben in diesem Zusammenhang zu bedenken, daß die PC-gestützte Personaldatenverarbeitung unumgänglich war, um die aufgrund politischer Vorgaben innerhalb kürzester Zeit umzusetzende Personalverstärkung von ca. 1 000 auf ca. 4 000 Mitarbeiter bewältigen zu können.

Auf meine Bitte hin wurde noch während der Kontrolle vom BAFl eine erste Bestandsaufnahme über alle in der Hauptstelle eingesetzten Personalcomputer, die automatisiert geführten Dateien mit Personaldaten, den jeweiligen Verwendungszweck und weitere Angaben veranlaßt. Mir wurde eine entsprechende Übersicht überreicht, die es dem Datenschutzbeauftragten des BAFl ermöglichen wird, die ordnungsgemäße Anwendung der automatisierten Personaldatenverarbeitung zu überprüfen und eine datenschutzgerechte Nutzung zu gewährleisten. Auch wurde mir zugesagt, die Zulässigkeit jeder einzelnen Personaldatei sofort zu überprüfen und ggf. erforderliche datenschutzrechtliche Maßnahmen einzuleiten. Hierbei wird das BAFl ein besonderes Augenmerk auf die festgestellten Sicherheitsmängel im Hinblick auf § 9 BDSG und der Anlage hierzu, das Problem der „freien Abfragesprache" sowie auf die in zahlreichen Dateien vorgefundenen Bemerkungsfelder richten.

Darüber hinaus wurde mir zugesagt, nach Abschluß der Bestandsaufnahme und datenschutzgerechter Neuordnung der Personaldatenverarbeitung alle Mitarbeiter gem. § 90 Abs. 5 BBG bzw. 33 Abs. 1 BDSG zu benachrichtigen.

Während der Kontrolle hat das BAFl vorgetragen, es sei bemüht, schnellstmöglich ein zentrales Personalinformationssystem einzuführen, das das bisherige PC-gestützte Verfahren ablösen wird.

Im Anschluß an die Datenschutzkontrolle hat das BAFl vereinbarungsgemäß den Entwurf einer Dienstanweisung zur automatisierten Personaldatenverarbeitung mit mir abgestimmt.

Im Hinblick darauf, daß das BAFl noch während der Kontrolle die von mir empfohlenen Maßnahmen zur datenschutzgerechten Gestaltung der Personaldatenverarbeitung getroffen oder eingeleitet hat und aufgrund der Tatsache, daß das BAFl allen Gesichtspunkten des Datenschutzes und der Datensicherheit bei der automatisierten Personaldatenverarbeitung gegenüber sehr aufgeschlossen ist und sich bemüht, datenschutzgerechte Lösungen in Abstimmung mit mir kurzfristig zu finden und umzusetzen, habe ich auf eine förmliche Beanstandung der festgestellten Mängel verzichtet (§ 25 Abs. 2 BDSG).

9.7.6 Mangelnde Unterstützung beanstandet

Das „Personalverwaltungssystem der Wasser- und Schiffahrtsverwaltung" war während des Berichtszeitraums Gegenstand einer Besprechung im Bundesministerium für Verkehr, in der mir die Zusage gegeben wurde, zu den erörterten Punkten der Thematik schriftlich Stellung zu nehmen und mir Ausfertigungen sämtlicher Listen/Auswertungsmöglichkeiten des Systems zuzuleiten. Trotz mehrfacher, schriftlicher Erinnerungen hatte mir das BMV weder die zugesagte Stellungnahme mit den entsprechenden Unterlagen noch eine Zwischeninformation zugeleitet.

Gemäß § 24 Abs. 4 BDSG sind die öffentlichen Stellen des Bundes verpflichtet, den Bundesbeauftragten und seine Beauftragten bei der Erfüllung ihrer Aufgaben zu unterstützen. Ich habe dieses Verhalten des BMV gem. § 25 Abs. 1 BDSG wegen mangelnder Unterstützung bei der Erfüllung meiner Aufgaben als einen Verstoß gegen § 24 Abs. 4 BDSG beanstandet.

Nach Ausspruch der Beanstandung hat das BMV vorgetragen, daß die Verzögerung auf einer „groben Verkennung von Prioritäten" beruhte und nachdrücklich bedauert, daß ich diese Auskünfte erst verspätet erhalten habe. Das BMV hat mich darüber hinaus bei der Neukonzeption des „Personalverwaltungssystems der Wasser- und Schiffahrtsverwaltung" um unterstützende Beratung gebeten. Die diesbezügliche bisherige Zusammenarbeit mit dem BMV ist sehr kooperativ.

9.8 Telefondatenverarbeitung

9.8.1 Weiterhin Probleme mit der Umsetzung der Dienstanschlußvorschriften

Im 14. Tätigkeitsbericht (Seite 64 ff.) hatte ich berichtet, daß das Bundesministerium der Finanzen die „Allgemeine Verwaltungsvorschrift über die Einrichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Bundesverwaltung (Dienstanschlußvorschriften – DAV –)" vom 1. Januar 1992 (in Kraft seit 1. Januar 1993) erlassen hat. Ich hatte dies als einen Schritt zu einer datenschutzgerechten Verarbeitung der Telefondaten der Bundesbediensteten bewertet.

Eingaben von Bundesbediensteten, Beratungswünsche von Bundesbehörden, Anfragen von Personalvertretungen sowie die zu dieser Thematik bei Datenschutzkontrollen getroffenen Feststellungen zeigen jedoch, daß es bei der Umsetzung in der Praxis Probleme gibt. Beispiele hierfür sind insbesondere die unzulässige Erhebung und Verarbeitung der Uhrzeit, der Dauer von einzelnen Telefongesprächen oder der ungekürzten Rufnummer des Angerufenen bei Privatgesprächen.

In all diesen Fällen habe ich dargelegt, daß auch die Erhebung und Verarbeitung personenbezogener Daten in Telekommunikations-Anlagen (TK-Anlagen) den Zulässigkeitsvoraussetzungen des BDSG unterliegt. Nach § 13 Abs. 1 BDSG ist das Erheben, nach § 14 Abs. 1 BDSG das Speichern, Verändern oder Nutzen personenbezogener Daten dann zulässig, wenn es zur Erfüllung der in der Zuständigkeit der erhebenden/speichernden Stelle liegenden Aufgaben **erforderlich** ist. Im Bereich der Bundesverwaltung ist in den Dienstanschlußvorschriften (DAV) **abschließend** niedergelegt, welche personenbezoge-

nen Daten bei der Telefondatenverarbeitung nachzuweisen und somit erforderlich sind.

So sieht die entsprechende Regelung der DAV u. a. eine Speicherung der Uhrzeit oder der Dauer eines Telefongespräches – unabhängig, ob dienstlich oder privat – nicht vor. Bei den privaten Verbindungen sind nur Vorwahl und/oder die um die letzten beiden Ziffern **verkürzte** Rufnummer des Angerufenen nachzuweisen.

Da die vorgenannten personenbezogenen Daten für die konkrete in der DAV geregelte Aufgabenerfüllung nicht erforderlich sind, ist ihre Erhebung oder Verarbeitung aus datenschutzrechtlicher Sicht unzulässig. Im übrigen sind diese personenbezogenen Daten zumindest geeignet, für eine Verhaltens- und/oder Leistungskontrolle der Bediensteten verwendet zu werden.

Ich werde weiterhin im Rahmen meiner gesetzlichen Zuständigkeit darauf achten, daß die Regelungen der Dienstanschlußvorschriften, die zu datenschutzrechtlichen Verbesserungen für die Mitarbeiter geführt haben, von den öffentlichen Stellen des Bundes in der Praxis eingehalten oder – sofern noch nicht geschehen – deren Telefondatenverarbeitung diesen Regelungen angepaßt werden.

Einige Beispielsfälle aus dem Berichtszeitraum belegen diese Notwendigkeit:

9.8.2 Telefondatenverarbeitung der Südwestlichen Bau-Berufsgenossenschaft

Bei einer Kontrolle der Südwestlichen Bau-Berufsgenossenschaft habe ich festgestellt, daß auch dort unzulässigerweise sowohl die Uhrzeit wie auch die Dauer der Dienstgespräche gespeichert und verarbeitet wurden. Ich habe dies als unzulässig bewertet und empfohlen, die Speicherung und Verarbeitung dieser Daten durch geeignete Maßnahmen zu unterdrücken.

Hinsichtlich der Speicherung der Uhrzeit, nicht jedoch hinsichtlich der Dauer der Telefonate ist sie meinen Empfehlungen gefolgt. Ich habe nochmals gebeten, auch hierauf zu verzichten.

Die Telefondatenverarbeitung der Privatgespräche war bei der Südwestlichen Bau-Berufsgenossenschaft korrekt geregelt.

9.8.3 Telefondatenverarbeitung im BVA

Beim Bundesverwaltungsamt Köln habe ich festgestellt, daß dort ebenfalls die Uhrzeit der einzelnen dienstlichen und privaten Telefongespräche gespeichert und verarbeitet wurde; bei den Dienstgesprächen darüber hinaus auch die jeweilige Dauer der Gespräche (in Minuten, Sekunden).

Die Verfahrensregelungen zur Telefondatenverarbeitung im BVA erlauben in Ausnahmefällen auch das Führen von privaten Telefongesprächen. Auch hierbei ist auf die Regelungen der DAV abzustellen.

Entgegen der o. a. Regelung der DAV wurden zum Zeitpunkt meiner Datenschutzkontrolle auch die vollständige Zielnummer (d. h. nicht um die beiden letzten Stellen verkürzt) erfaßt und verarbeitet.

Ich habe empfohlen, sowohl Uhrzeit als auch Dauer der Telefongespräche durch geeignete Maßnahmen zu unterdrücken und auch hinsichtlich der Zielnummer bei Privatgesprächen gem. der DAV zu verfahren.

Das BVA hat mir inzwischen mitgeteilt, daß durch eine Änderung der Software nunmehr die Telefondatenverarbeitung bei den privaten Gesprächen in allen Belangen der DAV entspricht. Zur Unterdrükkung der unzulässigen Daten (Uhrzeit, Dauer eines Gespräches) hat das BVA zwischenzeitlich Verbindung mit dem Softwareentwickler aufgenommen.

9.8.4 Anpassung an Dienstanschlußvorschriften erreicht

Auch im Kraftfahrt-Bundesamt mußte ich feststellen, daß bei den dienstlichen Ferngesprächen die exakte Uhrzeit und die Dauer der Telefonate erfaßt und verarbeitet wurden.

Ich habe es begrüßt, daß mir das KBA noch während meiner Kontrolle zugesagt hat, ab sofort auf die Erfassung und Verarbeitung von Uhrzeit und Dauer der Telefongespräche zu verzichten. Dies wurde umgehend technisch realisiert.

Ich habe darüber hinaus dem KBA generell empfohlen, das Verfahren der dortigen Telefondatenverarbeitung und die Regelungen der hierzu abgeschlossenen Dienstvereinbarung auf Grundlage der Dienstanschlußvorschriften nochmals zu überprüfen und diese – soweit erforderlich – der DAV anzupassen. Das KBA hat eine umgehende Umsetzung dieser Empfehlungen zugesagt.

9.8.5 Analoge Anwendung der Dienstanschlußvorschriften

Auch bei der Deutschen Botschaft Paris habe ich u. a. die dortige Telefondatenverarbeitung geprüft.

Die Vorschriften der DAV gelten zwar nicht unmittelbar für die Telekommunikationsanlagen bei den Auslandsvertretungen. Dennoch ist kein sachlicher Grund ersichtlich, warum die personenbezogenen Daten der bei der Botschaft eingesetzten Mitarbeiter nicht den gleichen Schutz genießen sollten wie diejenigen der Beschäftigten im Auswärtigen Amt.

Bei der Kontrolle habe ich festgestellt, daß das in der Botschaft praktizierte Verfahren in wichtigen Punkten mit den datenschutzrechtlichen Regelungen analog der DAV nicht im Einklang stand.

Ich habe es ausdrücklich begrüßt, daß noch während meines Kontrollbesuches zugesagt wurde, die datenschutzrechtlich relevanten Anforderungen analog den Dienstanschlußvorschriften in die Praxis umzusetzen.

9.9 Personaldaten in den fünf neuen Bundesländern

Nach Auflösung vieler Behörden und Betriebe im Beitrittsgebiet war es eine vorrangige Aufgabe, eine ordnungsgemäße Lagerung von Personalakten sicherzustellen, die unbefugten Zugriff ausschließt.

Die Aufbewahrung von Personalunterlagen ist meist auch im Interesse der Betroffenen erforderlich, um insbesondere rentenrechtlich relevante Tatbestände überprüfen und nachweisen zu können. Dazu ist es wichtig, daß die ehemaligen Mitarbeiter von der Existenz ihrer Personalakten und dem Aufbewahrungsort Kenntnis erlangen.

9.9.1 Sichere Aufbewahrung von Kaderakten

Ich hatte den Hinweis erhalten, in einer leerstehenden Wohnung in Berlin, die unter der Verwaltung des Bundesvermögensamtes stand, befänden sich „zentnerweise" Kaderakten der früheren DDR-Handelsgesellschaft HO. Darauf sei eine Mieterin von Nebenräumen gestoßen.

Eine Kontrolle vor Ort in Berlin bestätigte, daß eine große Zahl von Akten in den Räumen der Wohnung vorhanden war. Diese waren teilweise in offenstehenden Schränken oder an den Wänden gestapelt; teilweise waren sie geordnet, teilweise aufgerissen und auch über den Boden verteilt. Offensichtlich war die Wohnung zuvor unerlaubt zum Aufenthalt genutzt worden.

Eine stichprobenartige Kontrolle der Akten ergab, daß es sich um Kaderakten der Handelsorganisation HO der ehemaligen DDR handelte, die beispielsweise Arbeitsverträge, Lebensläufe, Beurteilungen, Versetzungsgesuche etc. enthalten.

Da dringlicher Handlungsbedarf bestand, wurden zunächst die wichtigsten Maßnahmen zur Sicherung der Akten getroffen.

Mehrere Monate später konnte ich mich in einem Depot der Treuhandanstalt davon überzeugen, daß diese Unterlagen nunmehr dort geordnet und archivmäßig aufbereitet untergebracht sind.

Eine Besichtigung dieses Aktenlagers ergab keine Hinweise auf Mängel bei der Datensicherheit. In dem Treuhanddepot sind derzeit ca. 26 km an Akten gelagert. Im Endstadium wird das Depot in Berlin ca. 6 bis 8 Millionen Nettolohnkonten von Arbeitnehmern speichern. Das Aktenlager ist sicherheitstechnisch und gegen Brandgefahr hinreichend gesichert.

Sowohl diese wie auch die künftigen Akten in dem Treuhanddepot dienen insbesondere dem Nachweis von sozialversicherungsrechtlich relevanten Daten gegenüber dem jeweils zuständigen Träger sowie der Gewährleistung eines Einsichts- und Auskunftsanspruchs der Betroffenen im Einzelfall.

Die Aufbewahrungsfrist für die gelagerten Unterlagen läuft bis zum 31. Dezember 2006. Gemäß Artikel II § 15 b SGB IV sind vorhandene Lohnunterlagen mindestens bis zu diesem Zeitpunkt aufzubewahren, sofern sie am 31. Dezember 1991 in den neuen Bundesländern vorhanden waren. Nach Aussage des Depotleiters ist es im Interesse der Betroffenen notwendig, nicht nur die Lohn-, sondern alle Personalunterlagen so lange aufzubewahren, da oftmals Anfragen der Sozialversicherungsträger sich allein mit den Lohnunterlagen nicht beantworten lassen.

Es wurde mir versichert, daß eine weitere Aufbewahrung der Unterlagen auch nach Auflösung der Treuhand gewährleistet ist. Dazu soll eine Privatgesellschaft gegründet werden, die u. a. das Depot im Auftrag der Treuhand weiterführt.

Ich habe Grund zu der Annahme, daß die Lagerung dieser Unterlagen in dem Depot in der Öffentlichkeit weitgehend unbekannt ist, was Einfluß auf die Auskunfts- und Einsichtsrechte der Betroffenen hat. Ich habe daher die Treuhand gebeten, dies in geeigneter Weise bekannt zu machen. Eine entsprechende Stellungnahme der Treuhand zu diesem Punkt liegt mir bislang allerdings noch nicht vor.

9.9.2 Geheime Kaderakten in der ehemaligen DDR

Nach mir vorliegenden Informationen sollen im Ministerium des Innern der ehemaligen DDR sog. „Zweitkaderakten" geführt worden sein. In diesen – auch „Zentralisierte Kaderakten" genannt – sollen sich zusätzlich zu den auch in der sog. „Vorzeigeakte" enthaltenen Unterlagen geheime politische und charakterliche Beurteilungen befinden. Daten dieser sog. „Zweitkaderakten" sollen u. a. auf Magnetbändern des Statistischen Bundesamtes, Außenstelle Berlin, gespeichert sein.

Meine Mitarbeiter konnten demgegenüber keine Anhaltspunkte für Magnetbänder entsprechenden Inhaltes bei der Zweigstelle Berlin finden.

Außer den Personaldaten der vom Statistischen Bundesamt übernommenen Mitarbeiter wurden keine weiteren Personaldaten festgestellt. Zwar hat die Außenstelle vom Datenverarbeitungszentrum „Statistik" (DVZ) der ehemaligen DDR, die die reine Rechenarbeit für die staatliche Zentralverwaltung für Statistik erledigte, ca. 18 000 Magnetbänder übernommen. Sie befinden/befanden sich im Rechenzentrum der Außenstelle. Nach Auskunft des Statistischen Bundesamtes enthält aber keines dieser Bänder Personaldaten; insbesondere seien keine sog. „Zweitkaderaktendaten" des ehemaligen MdI gespeichert.

Von den ca. 18 000 übernommenen Magnetbändern wurden mittlerweile ca. 12 000 vernichtet. Die Vernichtung wird von einer Privatfirma durchgeführt. Bei ca. 1 500 Bändern wurden die Daten gelöscht und die Bänder einer Weiterverwendung im Bereich des Statistischen Bundesamtes zugeführt. Ca. 4 500 Magnetbänder sind noch mit den ursprünglichen Daten vorhanden.

Die Vernichtung der Magnetbänder bzw. die Löschung der darauf befindlichen Daten wurde von der Zweigstelle Berlin in einer Aufstellung „Abbau des DVZ-Datenträgerbestandes" dokumentiert. Daraus ergeben sich keine Anhaltspunkte für eine Vernichtung/Löschung von Personaldaten.

Das Statistische Bundesamt hat mir zugesichert, mich vom Abschluß der Vernichtung/Löschung des von dem DVZ übernommenen Datenträgerbestandes zu informieren.

Auch eine stichprobenartige Kontrolle der Etikettierung der noch vorhanden 4 500 Bänder brachte keine Anhaltspunkte für die Speicherung von Personaldaten.

9.10 Die Stiftung Preußischer Kulturbesitz lehnt die Bestellung eines internen Datenschutzbeauftragten derzeit ab

Gegenüber der Stiftung habe ich unter Berufung auf §§ 18 und 9 BDSG und die allgemeine Verwaltungspraxis bei den Bundesbehörden wiederholt die Bestellung eines internen Datenschutzbeauftragten empfohlen.

Die Stiftung lehnt dies derzeit ab. Die Einhaltung des Datenschutzes sei durch die gegenwärtige Organisation sichergestellt. Im übrigen befinde sich die Stiftung in einer insbesondere einigungsbedingten Umbruchsituation, die ggf. eine Neuorganisation zur Folge habe. Ich halte es demgegenüber aber gerade im Hinblick auf die erwogene Neuorganisation für besonders zweckmäßig, die datenschutzgerechte Neuorganisation durch einen Datenschutzbeauftragten zu gewährleisten.

9.11 Unternehmensrichtlinie Telekom „Kranken-Fehlzeiten mindern"

In einer Eingabe wurden datenschutzrechtliche Bedenken wegen unzulässiger Verhaltens- und Leistungskontrollen bei der Umsetzung der Unternehmensrichtlinie Telekom zur Minderung von Krankenfehlzeiten geltend gemacht. Ziel der Richtlinie soll es nach Angaben der Generaldirektion Telekom sein, die Überwachung des Krankenstandes nach der Postreform I der eines Privatunternehmens anzupassen. Auf der Grundlage der Fragestellung, wie man den Krankenstand „positiv" beeinflussen kann, wurde mit der Richtlinie versucht, eindeutige Regelungen zur Kooperation zwischen Führungskräften und Mitarbeitern und zur Planung entsprechender Gegenmaßnahmen bei erhöhtem bzw. auffälligem Krankenstand in einzelnen Arbeitsfeldern zu schaffen.

Im Rahmen der Richtlinie soll in den Niederlassungen der Generaldirektion-Telekom u. a. stets ein aktueller Überblick über den Stand der Kranken-Fehlzeiten für jeden einzelnen Mitarbeiter einschließlich der Angaben zu Wochentagen (Montag-Freitag) und etwaigen Verbindungen mit Urlaub, arbeitsfreien Tagen, Feiertagen, Zeiten mit besonders hoher Arbeitsbeanspruchung, Tagen mit ungünstigen Arbeitsschichten etc. möglich sein. In Fällen auffälliger oder erhöhter Kranken-Fehlzeiten (z. B. 45 Kalendertage oder 5 Erkrankungen in den letzten 12 Monaten) soll die Problematik zwischen dem unmittelbaren Vorgesetzten und dem Mitarbeiter in einem Gespräch erörtert werden, wobei ein positiver Ausklang des Gesprächs anzustreben sei. Nach der Unternehmensrichtlinie kann damit auch ein Gesprächsangebot etwa in der Art „Rufen Sie uns an, wir rufen zurück" gemacht werden.

Bei Zweifel an der Dienst- bzw. Arbeitsunfähigkeit von Mitarbeitern ist die Begutachtung durch einen Amtsarzt für Beamte (vgl. § 42 Abs. 1 Satz 2 BBG) bzw. den Medizinischen Dienst der Krankenkassen für Angestellte und Arbeitnehmer (vgl. § 275 Abs. 1 Nr. 3 b SGB V) ebenso geregelt, wie ein Kranken-Gespräch mit Mitarbeitern, die in den letzten 6 Monaten mehr als 2 Monate krankheitsbedingt für den Arbeitgeber nicht zur Verfügung gestanden haben, wobei Fehlzeiten wegen Kuren, Mutterschutz, ganztägiger ärztlicher Behandlung und Zeiten eines „therapeutischen Arbeitsversuchs" ausdrücklich ausgenommen werden.

Aus datenschutzrechtlicher Sicht relevant ist in diesem Zusammenhang

a) die vorgesehene Protokollierung der Gesprächsergebnisse für die Personalakte der Betroffenen sowie

b) die Übermittlung personenbezogener Daten von Ärzten an die Personalstelle anläßlich der von dort veranlaßten Begutachtung.

Die Aufnahme von Aufzeichnungen über Fehlzeiten-Gespräche in die Personalakte halte ich aus datenschutzrechtlicher Sicht grundsätzlich für zulässig, da die Gespräche m.E. geeignet und erforderlich sind, die Diensttauglichkeit bei erhöhter oder auffälliger Kranken-Fehlzeit zu prüfen und festzustellen.

Für die Aufnahme der Vermerke über Fehlzeiten-Gespräche in die Personalakte habe ich der Generaldirektion folgende Vorgehensweise empfohlen:

1. Um das Ziel eines Fehlzeiten-Gespräches, gemeinsam mit dem Betroffenen nach den Ursachen seiner Fehlzeiten und nach Möglichkeiten zu suchen, sie abzustellen, nicht zu gefährden, sollte eine Verständigung mit dem Betroffenen darüber hergestellt werden, ob der Inhalt des Gespräches schriftlich festgehalten werden soll.

2. Sollte das in dem Vermerk festgehaltene Ergebnis des Gespräches nicht von beiden Gesprächspartnern getragen werden, ist dem Betroffenen Gelegenheit zu geben, in einer Gegendarstellung seinen Standpunkt festzuhalten. Die Gegendarstellung wird damit Teil der Notiz über das Gespräch in der Personalakte (Teilakte).

3. Die Notiz wird in der entsprechenden Teilakte über Erkrankungen 5 Jahre nach Ablauf des Jahres, in dem die Bearbeitung des einzelnen Vorgangs abgeschlossen wurde, aufbewahrt (vgl. § 90 f. Abs. 2 Satz 1 BBG) und ist dann zu vernichten oder dem Betroffenen auszuhändigen.

Was die Übermittlung personenbezogener Daten von Ärzten an die Personalstelle anläßlich der von dort veranlaßten Begutachtung anbelangt, habe ich gegenüber der Generaldirektion Telekom meine Auffassung zur Geltung der ärztlichen Schweigepflicht gegenüber dem Dienstherrn (vgl. Nr. 9.4) vertreten.

Daraus folgt, daß der Arzt auch mit Zustimmung des Betroffenen lediglich das Ergebnis der ärztlichen Untersuchung übermitteln darf; d. h. die Feststellung, ob der Betroffene für das Dienst- oder Arbeitsverhältnis bzw. für eine bestimmte Tätigkeit geeignet, nicht geeignet oder eingeschränkt (ggf. mit welchen Einschränkungen) geeignet ist. Darüber hinausgehende Daten sind für die Aufgabenerfüllung der Personalverwaltung nicht erforderlich.

9.12 Das Sozialamt der Deutschen Bundespost gibt Daten an eine Haftpflichtversicherung weiter

Ein Mitarbeiter der Deutschen Bundespost erlitt einen schweren Autounfall, war daraufhin dienstunfähig und wurde später in den vorzeitigen Ruhestand versetzt.

Das SAP wandte sich mit einem Schreiben an die Haftpflichtversicherung des Unfallgegners und teilte dieser mit, der Mitarbeiter müsse vorzeitig in den Ruhestand versetzt werden. Dies sei allerdings nicht ausschließlich Unfallfolge; Ersatzansprüche würden seitens des SAP deshalb nicht geltend gemacht.

Gegen diese Offenbarung hat sich der Petent gewandt und geltend gemacht, hierdurch sei ihm ein erheblicher finanzieller Schaden entstanden.

Die Datenweitergabe an die Haftpflichtversicherung erscheint auf den ersten Blick sehr fragwürdig. In diesem Zusammenhang ist jedoch § 87a BBG zu beachten. Werden bei Dienst- oder Privatunfällen Beamte verletzt oder getötet, so gehen bis zur Höhe der zu erbringenden Leistungen die Ersatzansprüche des Verletzten bzw. des Hinterbliebenen auf die Deutsche Bundespost über. Die übergegangenen Ersatzansprüche hat das SAP zunächst bei der gegnerischen Haftpflichtversicherung dem Grunde und der Höhe nach geltend gemacht. Aufgrund eines späteren postärztlichen Gutachtens konnten anfängliche Regreßforderungen, welche Versorgungsbezüge des Petenten zum Inhalt hatten, jedoch nicht aufrecht erhalten werden. Dies hat das SAP mit dem hier in Frage stehenden Schreiben der Haftpflichtversicherung mitgeteilt.

Allerdings – und dies ist mit datenschutzrechtlichen Bestimmungen nicht vereinbar – war die Mitteilung nicht erforderlich, der Verletzte werde vorzeitig in den Ruhestand versetzt und dies sei nicht ausschließlich Unfallfolge. Es hätte ausgereicht, die Haftpflichtversicherung darüber zu informieren, daß Ersatzansprüche seitens des SAP nicht geltend gemacht werden.

Demgegenüber hat das SAP eingewandt, ein entsprechender Informationsgehalt sei der Haftpflichtversicherung auch ohne ausdrückliche Darlegung bekannt. Voraussetzung für die Geltendmachung eines Schadensersatzes gem. §§ 823, 843 BGB, 87 a BBG nach erfolgter Zurruhesetzung eines unfallverletzten Beamten sei stets eine vorzeitige unfallbedingte Versetzung in den Ruhestand. Dennoch hat sich das SAP ausdrücklich bereit erklärt, künftig in gleichgelagerten Fällen auf derartige Offenbarungen zu verzichten und ausschließlich den Verzicht auf Regreßforderungen darzulegen.

9.13 Kein Anlaß, zwischen Personalaktenführung für Beamte, Angestellte und Arbeiter zu unterscheiden

Bei einzelnen Bundesbehörden wird die Auffassung vertreten, daß die §§ 90 bis 90 g BBG zur Personalaktenführung ausschließlich auf Beamte, nicht jedoch auf Angestellte und Arbeiter analog anzuwenden seien.

Mit dem Inkrafttreten des Neunten Gesetzes zur Änderung dienstrechtlicher Vorschriften, über das ich bereits (zuletzt im 14. TB S. 62) berichtet habe, wurde das Personalaktenrecht für Beamte weitgehend auf einem datenschutzrechtlich erfreulichen Niveau geregelt.

Mit der – aus meiner Sicht verfehlten – Regelung in § 12 Abs. 4 BDSG gelten für die Verarbeitung und Nutzung personenbezogener Daten im Zusammenhang mit Dienst- und Arbeitsverhältnissen – immer noch – die Vorschriften des Dritten Abschnitts des BDSG für den nicht-öffentlichen Bereich. Damit bleibt es formal bei einer datenschutzrechtlichen Schlechterstellung, besonders der Angestellten und Arbeiter des Bundes gegenüber Bundesbeamten.

In der Begründung zum Neunten Gesetz zur Änderung dienstrechtlicher Vorschriften hat die Bundesregierung erklärt, daß über die in diesem Entwurf vorgesehenen Bestimmungen hinaus weitere gesetzliche Maßnahmen erforderlich sind, um den Datenschutz bei Arbeits- und Dienstverhältnissen umfassend zu regeln. Sie hält die Schaffung eines allgemeinen Arbeitnehmer-Datenschutzgesetzes für besonders dringlich. Dies unterstütze ich nachdrücklich.

Sowohl das Bundesministerium des Innern als auch das Bundesministerium der Verteidigung haben auf dem Erlaßwege zumindest die Vorschriften der §§ 90 bis 90 g BBG zur Personalaktenführung für die Angestellten und Arbeitnehmer ihrer Geschäftsbereiche sinngemäß für anwendbar erklärt, soweit die §§ 13 BAT/BAT-O bzw. 13 a MTB II/MT ArbO keine eigenen Regelungen enthalten oder darin keine speziellen Interpretationen der Tarifparteien ersichtlich sind.

Bezüglich der übrigen Bundesbereiche sehe ich keinen sachlichen Grund, bis zur Schaffung eines Arbeitnehmer-Datenschutzgesetzes zwischen dem Personalaktenrecht für Beamte, Angestellte und Arbeitnehmer bei öffentlichen Arbeitgebern des Bundes zu differenzieren und damit eine Schlechterstellung der letztgenannten Gruppen hinzunehmen.

9.14 Ein Unfallversicherungsträger fordert ein ärztliches Gutachten von einem privaten Versicherungsunternehmen an – Verstoß gegen den Ersterhebungsgrundsatz

Ein Mitarbeiter der Deutschen Bundespost wurde bei der Ausübung seines Dienstes als Briefzusteller zusammengeschlagen und eine Treppe hinabgestoßen. Dabei zog er sich erhebliche Verletzungen zu. Im Auftrag des Sozialamtes der Deutschen Bundespost wurde der Mitarbeiter zur Feststellung, ob ihm als Beamter ein Unfallausgleich zusteht, fachärztlich untersucht. Da er eine Invaliditätsversicherung abgeschlossen hatte, wurde er auch im Auftrage des privaten Versicherungsunternehmens in einer unfallorthopädischen Universitätsklinik begutachtet, um die Einschränkung der Erwerbsfähigkeit im einzelnen festzustellen.

Der begutachtende Arzt der Universitätsklinik wandte sich an das Sozialamt der Deutschen Bundespost und teilte diesem mit, daß er für das private Versicherungsunternehmen ein entsprechendes Gutachten erstellt habe. Gleichzeitig erklärte er sich mit einer Einsichtnahme durch das SAP einverstanden. Daraufhin wurde dieses Gutachten auf Ersuchen des SAP diesem von dem Privatversicherer direkt zur Verfügung gestellt.

Diese Vorgehensweise verstößt gegen den in § 67 a Abs. 2 SGB X (vormals § 79 SGB X i.V. m. § 13 Abs. 2 Satz 1 BDSG) normierten Ersterhebungsgrundsatz. Danach wäre das SAP verpflichtet gewesen, sich zunächst mit dem Betroffenen in Verbindung zu setzen und ihn nach der Existenz eines entsprechenden Gutachtens zu fragen und ihn gegebenenfalls um Herausgabe desselben zu bitten. Hierzu wäre dieser aufgrund seiner Mitwirkungsobliegenheit gem. § 60 Abs. 1 SGB I grundsätzlich gehalten gewesen. Erst wenn diese Vorgehensweise nicht erfolgreich gewesen wäre, wäre zu prüfen gewesen, ob eine Ausnahme vom Prinzip der Ersterhebung nach Maßgabe des § 67 a Abs. 2 Nr. 2 SGB X in Betracht kam.

Demgegenüber hat das SAP vorgetragen, daß keine Veranlassung bestand, das Gutachten bei dem Untersuchten selbst anzufordern. Dieses sei von der privaten Versicherung und nicht von dem Untersuchten veranlaßt worden und damit sei dessen Berechtigung zur Herausgabe fraglich gewesen, da bezüglich des Gutachtens Rechtsbeziehungen lediglich zwischen Versicherung als Auftraggeber und Gutachter bestanden hätten. Des weiteren hat das SAP eingewandt, die Deutsche Bundespost als Unfallfürsorgeträger benötige in bestimmten, mit Dienstunfällen zusammenhängenden Einzelfällen umfassende Informationen von Amts wegen über den Gesundheitszustand des Verletzten. Dies sei insbesondere z. B. zur Klärung von Zusammenhangsfragen und zur Beurteilung der Minderung der Erwerbsfähigkeit erforderlich. Dazu bedürfe es grundsätzlich nicht der Einwilligung des Verletzten (§§ 69 Abs. 2, 100 SGB X, 1543 d RVO).

Die datenschutzrechtliche Bewertung wird jedoch nicht dadurch beeinflußt, daß Rechtsbeziehungen lediglich zwischen der privaten Versicherung als Auftraggeber und dem Gutachter in der Universitätsklinik bestanden. Denn die Vorschrift des § 67 a Abs. 2 SGB X soll u. a. bewirken, dem Betroffenen transparent zu machen, welche Gutachten durch das SAP für seine Entscheidungsfindung herangezogen werden. Dies wäre durch eine Anfrage bei dem Betroffenen erreicht worden. Das Prinzip der Ersterhebung ist auch nicht dadurch ausgeschlossen, daß – wie sich später herausstellte – der Petent überhaupt nicht im Besitz eines Gutachtens war bzw. aufgrund zivilrechtlicher Gesichtspunkte unter Umständen zur Herausgabe nicht berechtigt gewesen wäre.

Ich verkenne dabei nicht, daß das SAP in bestimmten mit Dienstunfällen zusammenhängenden Einzelfällen umfassende Informationen über den Gesundheitszustand des Verletzten benötigt. Die hierfür angeführten Rechtsgrundlagen können im Einzelfall allenfalls eine Übermittlungsbefugnis geben. Diese Vorschriften beseitigen indessen nicht den Ersterhebungsgrundsatz. Sie normieren nur die grundsätzliche Befugnis eines Dritten, bei Vorliegen ihrer Voraussetzungen personenbezogene Daten an das SAP zu übermitteln.

Im vorliegenden Fall habe ich von einer förmlichen Beanstandung nur deshalb abgesehen, weil seitens des SAP versichert wurde, daß das hier in Frage stehende Gutachten nicht für die Leistungsentscheidung im konkreten Fall herangezogen wurde.

9.15 Behörde verweigert mir Einsicht in einen Vorgang

Aus Anlaß einer Eingabe richtete die Südwestliche BauBG ein Anschreiben an den Hauptverband der gewerblichen Berufsgenossenschaften (HVBG), in dem sie um Prüfung des Vorgangs bat. Bei einer Kontrolle der BG wollten meine Mitarbeiter in die Kopie des Anschreibens an den HVBG Einsicht nehmen, um eine evtl. Offenbarung personenbezogener Daten des Petenten kontrollieren zu können. Diese Einsichtnahme wurde durch die Südwestlichen BauBG – auch nach ausführlicher Erörterung der Rechtslage – verweigert. Als Begründung wurde angeführt, daß dieses Anschreiben keine personenbezogenen Daten – insbesondere nicht über den Petenten – enthalte und im übrigen ausschließlich Fragen der internen Organisation der BG betreffe.

Dieses Verhalten habe ich gem. § 25 Abs. 1 BDSG als einen Verstoß gegen die in § 24 Abs. 4 BDSG festgelegte Unterstützungspflicht sowie die dort normierte Pflicht, mir Einsicht zu gewähren, beanstandet.

Gegen diese Beanstandung hat sich die BG insbesondere mit dem Argument gewandt, daß sie als Dienstherr für sich in Anspruch nehme, sich über den HVBG in einer Umstrukturierungsfrage fachlich beraten zu lassen, ohne mir von diesbezüglichen Einzelheiten Kenntnis geben zu müssen. Allein aus den Behauptungen des Petenten dürfe nicht zu Lasten des Dienstherrn ein bewußter datenschutzrechtlicher Verstoß angenommen werden.

Das Vorbringen der Südwestlichen BauBG hat mich nicht überzeugt. Es ging ausschließlich darum, gemäß meinem gesetzlichen Auftrag zu kontrollieren, ob die Vorgehensweise der Südwestlichen BauBG in diesem Zusammenhang mit datenschutzrechtlichen Bestimmungen vereinbar war. Hierfür ist eine Einsichtnahme in die Korrespondenz mit dem HVBG erforderlich. Aufgrund des Vorbringens der BG sowie der Eingabe des Petenten hatte ich hinreichende Anhaltspunkte, daß personenbezogene Informationen über ihn an den HVBG gegeben wurden. Für eine wirksame Ausübung meines Kontrollrechts war es notwendig, zu überprüfen, ob personenbezogene Informationen an den HVBG weitergegeben wurden. Mich insoweit auf die Aussage der Südwestlichen BauBG zu verlassen, ist im Interesse einer wirksamen Kontrolle nicht ausreichend.

9.16 Die Gewerkschaft der Eisenbahner Deutschlands will Daten von der Deutschen Bahn AG zur bruttoverdienstbezogenen Beitragsrechnung

Die Gewerkschaft der Eisenbahner Deutschlands (GdED) hat die ehemals festen Mitgliedsbeiträge in bruttoverdienstbezogene Beiträge umgewandelt. Hier stellte sich die Frage, inwiefern ein Datenaustausch zwischen der Deutschen Bahn AG und der GdED möglich ist, um die Beitragserhebung und -berechnung zu vereinfachen. Bei diesem Datenaustausch sollten personenbezogene Daten unter Angabe des Bruttoverdienstes von der Deutschen Bahn AG an die GdED übermittelt werden. Anfragen bezüglich dieser Thematik wurden nicht nur von der GdED, sondern auch von der Gewerkschaft Deutscher Lokomotivführer und -anwärter und von der Gewerkschaft Deutscher Bahnbeamter, Arbeiter und Angestellter im Deutschen Beamtenbund an mich gestellt.

Für die datenschutzrechtlichen Anliegen der bei der Bahn AG eingesetzten Beamten ist der BfD zuständig. Durch die Zusammenführung der Sondervermögen „Deutsche Bundesbahn" und „Deutsche Reichsbahn" zum nicht rechtsfähigen Sondervermögen „Bundeseisenbahnvermögen" wurden alle Beamten dieser bisherigen Sondervermögen dem Bundeseisenbahnvermögen zugewiesen (§§ 1 und 7 ENeuOG). Der Bahn AG wurde die Befugnis übertragen, die übernommenen Beamten in ihrem Geschäftsbetrieb zu verwenden. Insofern ist die Deutsche Bahn AG öffentliche Stelle des Bundes und der BfD zuständig, wenn die zugehörige personenbezogene Datenverarbeitung durch die Bahn AG durchgeführt wird.

Hierzu habe ich der GdED gegenüber dargelegt, daß eine Datenübermittlung zulässig ist, wenn eine wirksame Einwilligung des einzelnen Mitgliedes vorliegt. Die Einwilligung macht den Datenaustausch für die Betroffenen transparent.

Weiterhin habe ich empfohlen, die Betroffenen, die schon vor der Umstellung des Beitragsverfahrens Mitglied bei der GdED waren, durch eine allgemeine Information auf den Datenaustausch und die Möglichkeit, diesem zu widersprechen, hinzuweisen.

Als Ergebnis meiner datenschutzrechtlichen Beratungen wurde im April 1994 eine Vereinbarung zwischen der Deutschen Bahn AG und der Gewerkschaft der Eisenbahner Deutschlands abgeschlossen, in der meine Empfehlungen umgesetzt wurden.

9.17 Assessment-Center-Verfahren zur Auswahl von Führungskräften

Im 14. Tätigkeitsbericht (S. 69 f.) hatte ich bereits die Durchführung von Verfahren zur Personalauswahl und Personalförderung unter Beteiligung von Privatfirmen erörtert. Im Berichtszeitraum habe ich nunmehr die Gelegenheit genutzt, bei der Generaldirektion-Telekom die Durchführung eines Assessment-Center-Verfahrens zur Auswahl von künftigen Fach- und Führungskräften im Zusammenhang mit der Ausgliederung des Mobilfunkes aus dem Bereich der Generaldirektion Telekom in ein Tochterunternehmen zu kontrollieren.

Das Assessment-Center im eigentlichen Sinne besteht aus verschiedenen Tests, in denen die Teilnehmer in verschiedenen Situationen beobachtet werden. Die getroffenen Feststellungen werden von „Beobachtern" protokolliert, die außer dem Namen keine weiteren Einzelheiten über die Teilnehmer wissen.

Gegen die Durchführung von Assessment-Center-Verfahren habe ich aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken.

Auf der Grundlage des Assessment-Center wurde ausschließlich von Mitarbeitern – im wesentlichen Psychologen – der Telekom eine „Potentialanalyse" erstellt. Grundlage hierfür waren die Ergebnisse aus dem Assessment-Center, die durch sog. Moderatoren in Zusammenarbeit mit Beobachtern in einer Beobachterkonferenz (hier Beobachter plus Moderator) zusammengetragen und objektiviert wurden; damit sollte das Ergebnis einheitlichen Kriterien genügen. Das Gutachten (Potentialanalyse) wurde einer Personalkommission als ein Auswahlkriterium zur Verfügung gestellt. Es enthält neben Angaben über den beruflichen Werdegang insbesondere detaillierte Prognosen zur künftigen Leistungsfähigkeit des Betroffenen, so z. B.:

- *„ ... übertrug Aufgaben, ohne sich dabei an den Kompetenzen seiner Mitarbeiter zu orientieren, die er hätte selbst erledigen müssen. Er überforderte seine Mitarbeiter und gab nur unspezifische Zielsetzung."*

Das dargestellte Beispiel mag ausreichen um aufzuzeigen, daß im Assessment-Center, also in einer künstlich herbeigeführten Situation, für einen bestimmten Zweck (die Besetzung von Führungspositionen bei einem Tochterunternehmen) detaillierte, auf den Teilnehmer bezogene Aussagen getroffen werden.

Mit der Zusicherung gegenüber den Teilnehmern, ihre persönlichen Daten nur für das Auswahlverfahren zu verwenden, scheidet grundsätzlich eine Nutzung des Gutachtens für andere Zwecke aus, die bei einer Aufnahme in die Personalakte nicht auszuschließen wäre.

Obwohl die gesamten Verfahrensunterlagen zunächst als Sachakten zu qualifizieren sind, halte ich eine entsprechende Aufnahme des Gutachtens in die Personalakte auf ausdrücklichen Wunsch des Betroffenen – der häufig geäußert wurde – für zulässig. Durch diese Willensäußerung werden die im Gutachten enthaltenen Sachakten- in Personalaktendaten dahin umgewidmet, für weitere Personalentscheidungen herangezogen zu werden. Der ursprüngliche, vom Dienstherrn auf das Auswahlverfahren begrenzte Zweck wird auf eine allgemeine Verwendung als Personalaktendaten erweitert. Es muß jedoch auch hier sichergestellt sein, daß es der alleinigen und freiwilligen Entscheidung des Betroffenen überlassen bleibt, ob eine Aufnahme in die Personalakte erfolgt.

Schutzwürdige Interessen der Betroffenen sind darüber hinaus regelmäßig dann verletzt, wenn diesen keine oder nicht ausreichend Gelegenheit gegeben wurde, von ihren unabdingbaren Rechten (Einsicht, Auskunft, Berichtigung, Löschung und Sperrung) Gebrauch zu machen.

Einsicht wurde den Betroffenen von seiten der Telekom zunächst ausschließlich in den Fragebogen und das Gutachten in der Form gewährt, daß der Betroffene nach einer Identitätskontrolle mittels Personal-/Dienstausweis unter Aufsicht eines Mitarbeiters Einsicht nehmen konnte. Die Wahrnehmung des Einsichtsrechtes wurde ebenso protokolliert wie besondere Vorkommnisse. Die Fertigung von Abschriften bzw. Kopien war untersagt. Einsicht in andere aus dem Assessment-Center vorhandene Unterlagen (z. B. handschriftliche Notizen der Beobachter und Moderatoren) wurde nicht gewährt.

Ich begrüße, daß die Einsicht grundsätzlich unter Aufsicht eines zugangsberechtigten Mitarbeiters der Personalverwaltung gewährt wurde. Die Einschränkung des Einsichtsrechts durch das ausgesprochene Verbot, Auszüge, Abschriften, Notizen oder gar Ablichtungen zu fertigen, steht jedoch mit der Rechtslage nicht in Einklang.

Gem. § 90 c Abs. 4 BBG erstreckt sich das Einsichtsrecht auch auf andere Akten **(auch Sachakten),** die personenbezogene Daten über den Beamten enthalten und für sein Dienstverhältnis verarbeitet oder genutzt werden, soweit gesetzlich nichts anderes bestimmt ist. Dies schließt, soweit dienstliche Gründe nicht entgegenstehen, auch die Fertigung von Auszügen, Abschriften, Ablichtungen oder Ausdrucken ein (§ 90 c Abs. 3 Satz 2 erster Halbsatz BBG).

Was die ebenfalls noch vorhandenen, von Beobachtern, Interviewern und Moderatoren im Laufe des Assessment-Center-Verfahren gefertigten, handschriftlichen Aufzeichnungen anbelangt, so ist eine Einsichtnahme der Betroffenen meines Erachtens nur dann ausgeschlossen, wenn ihre Daten mit Daten Dritter derart verbunden sind, daß ihre Trennung nicht oder nur mit unverhältnismäßig großem Aufwand möglich ist (§ 90 c Abs. 4 Satz 2 BBG). Dies ist beispielsweise dann gegeben, wenn auf einem Blatt handschriftliche Aussagen über mehrere Teilnehmer vermerkt sind. In diesem Falle ist dem Betroffenen Auskunft zu erteilen (§ 90 c Abs. 4 Satz 3 BBG).

Im vorliegenden Fall wurde ein sog. strukturiertes Interview von Mitarbeitern eines externen Unternehmensberaters durchgeführt. Ihm diente ein mit dem Hauptpersonalrat der Telekom und dem Betriebsrat des Tochterunternehmens abgestimmter Personalfragebogen als Vorbereitungsgrundlage.

Die Erforderlichkeit des Fragenkataloges wurde damit begründet, daß das Interview auf der Grundlage der beruflichen Laufbahn der Teilnehmer (strukturiert) durchgeführt werden sollte. Die grundsätzlich mögliche Erhebung der Angaben erst im Gespräch mit dem Teilnehmer hätte die Interviewdauer wesentlich verlängert. Der Fragebogen sei zu Beginn des Auswahlverfahrens an alle Teilnehmer verschickt und dem Unternehmensberater zur Vorbereitung des Interviews zur Verfügung gestellt worden. Auf der Grundlage des daraufhin durchgeführten Interviews wurde ein „Kurzgutachten nach Interview" erstellt und der „Potentialanalyse" als eigenständiger Teil beigefügt. Nach Auskunft der Telekom befanden sich zum Kontrollzeitpunkt keinerlei Unterlagen mehr in den Händen des Unternehmensberaters.

Gegen die Durchführung des strukturierten Interviews mit dem Ziel, eine persönliche Einschätzung der Teilnehmer vornehmen zu können, habe ich aus datenschutzrechtlicher Sicht grundsätzlich keine Bedenken. Allerdings bin ich in dem von mir kontrollierten Einzelfall auf der Grundlage der eingesehenen Unterlagen von der Erforderlichkeit des strukturierten Interviews und der damit verbundenen Datenerhebung durch Dritte keineswegs überzeugt.

Der Generaldirektion Telekom habe ich empfohlen, den Bediensteten das Gutachten mit den Fragebogen nach dem endgültigen Abschluß des Verfahrens zu überlassen, da sie ohnehin Anspruch auf eine Kopie haben. Die bei der Generaldirektion Telekom aus dem Verfahren vorhandenen sonstigen Unterlagen sind sodann zu vernichten. Die Generaldirektion Telekom hat mir zugesagt, diese Empfehlungen umzusetzen.

Bei künftigen Verfahren dieser Art empfehle ich, die Informationen für die Betroffenen so transparent zu gestalten, daß die Teilnehmer ausführliche Hinweise über

- die Freiwilligkeit ihrer Teilnahme, den Ablauf bzw. die Verfahrensschritte des Assessment-Center, die Aufgaben von Beobachtern, Moderatoren und Beobachterkonferenz,
- das Gesamtgutachten und
- das Gewicht des Gutachtens bei der zu treffenden Personalentscheidung

erhalten.

Damit könnte die Akzeptanz solcher Maßnahmen bei den betroffenen Mitarbeitern erheblich gestärkt werden.

10 Sozialwesen – Allgemeines

10.1 Der Datenschutz im Sozialgesetzbuch wurde neu geregelt

Am 1. Juli 1994 ist das Zweite SGB-Änderungsgesetz in Kraft getreten. Es enthält eine weitgehend abschließende bereichsspezifische Regelung des Sozialdatenschutzes – mit nur noch wenigen Verweisungen auf das Bundesdatenschutzgesetz – im Zehnten Buch des Sozialgesetzbuches. Ich war mehr als drei Jahre an der inhaltlichen Ausgestaltung und Formulierung des Gesetzes beteiligt. Hinsichtlich der einzelnen Neuregelungen verweise ich auf meine Ausführungen im 14. Tätigkeitsbericht (S. 75).

Die Neuregelung insbesondere im § 35 SGB I und in den § 67 ff. SGB X ist insgesamt zu begrüßen, wenn auch nicht alle meine Anliegen in dem Gesetz ihren Niederschlag gefunden haben. Aufgrund erster Er-

fahrungen befürchte ich, daß bei der Anwendung insbesondere folgender Vorschriften Schwierigkeiten auftreten werden:

- Wann ist eine Ausnahme vom Ersterhebungsgrundsatz im Sinne des § 67a Abs. 2 Satz 2 SGB X zulässig?
- Welche Aufklärungs-/Prüfpflichten treffen die erhebende/übermittelnde Stelle bei der Feststellung schutzwürdiger Interessen des Betroffenen (§§ 67a Abs. 2 Satz 2, 67c Abs. 3, 68 Abs. 1 Satz 1, 75 Abs. 1 Satz 1, 77 Abs. 1 SGB X)?
- Welche Informationen umfaßt die Darlegungslast der anfordernden Stelle? In welchem Umfang muß die übermittelnde Stelle diese Angaben prüfen, um ihrer Verantwortung für die Übermittlung gemäß § 67 d Abs. 2 SGB X gerecht werden zu können?
- Reicht § 69 SGB X als Rechtsgrundlage insbesondere für automatisierte Datenabgleiche oder sind bereichsspezifische Regelungen erforderlich?
- Was ist eine „Straftat von erheblicher Bedeutung" gem. § 73 Abs. 1 SGB X, bei deren Vorliegen eine Übermittlung von Sozialdaten zulässig ist?
- In welcher Form und Intensität sind die Hinweis- und Aufklärungspflichten durch die Sozialleistungsträger umzusetzen (insbesondere nach §§ 67a Abs. 3, § 67b Abs. 2 und 76 Abs. 2 SGB X)?
- Ist § 79 SGB X geeignet, um den sich abzeichnenden vermehrten Bedarf an automatisierten Abrufverfahren künftig in datenschutzgerechte Bahnen zu lenken?

10.2 Verstoß gegen den Ersterhebungsgrundsatz – ein Querschnittsproblem in der Sozialversicherung

Weder § 13 Abs. 2 Satz 1 BDSG noch die entsprechende Vorschrift des am 1. Juli 1994 in Kraft getretenen § 67 a Abs. 2 Satz 1 SGB X haben bewirkt, daß der Ersterhebungsgrundsatz in der gesetzlichen Sozialversicherung regelmäßig beachtet wird. Mit Verstößen in Einzelfällen bin ich in allen Bereichen immer wieder befaßt.

Bei meinen langjährigen Bemühungen, dem Ersterhebungsgrundsatz im Verwaltungsverfahren der Sozialleistungsträger zu allgemeiner Durchsetzung zu verhelfen, bin ich bisher besonders vom Bundesversicherungsamt und einzelnen großen Trägern, wie der BfA und der Bundesanstalt für Arbeit unterstützt worden; sie haben diesen Grundsatz frühzeitig in ihren internen Verfahrensregelungen umgesetzt.

Dazu, wie der Grundsatz der Ersterhebung im Verhältnis zum Amtshilfe- und Amtsermittlungsprinzip in den Einzelphasen des sozialrechtlichen Verwaltungsverfahrens umzusetzen ist, hat sich im Berichtszeitraum das Bundesversicherungsamt gegenüber einem Unfallversicherungsträger geäußert; dieser hatte von ihm nach meiner Beanstandung wegen Verstoßes gegen den Ersterhebungsgrundsatz eine aufsichtsrechtliche Klarstellung erbeten. Im Hinblick auf die gründliche Kenntnis der Verwaltungspraxis des Bundesversicherungsamtes und darauf, daß dessen Stellungnahme meine Rechtsauffassung insoweit vollauf bestätigt, gebe ich diese nachfolgend wieder:

„Die ... Versicherung erfüllt nach dem Willen des Gesetzgebers eine wichtige Schutzfunktion. Nach §§ ... sind die dort aufgeführten Personengruppen kraft Gesetzes versichert, das bedeutet, daß dieser Schutz unabhängig von anderweitigen Umständen, allein durch die Erfüllung der gesetzlichen Voraussetzungen eintritt. Daraus ergibt sich für die mit der Durchführung des Verwaltungsverfahrens beauftragte Behörde die Verpflichtung, zeitnah und rechtsfehlerfrei das Vorliegen bzw. Nichtvorliegen von Voraussetzungen zu klären, an die sich als rechtliche Folgen Verwaltungsakte schließen. Bei der Ausgestaltung dieses ihr obliegenden Verwaltungsverfahrens ist sie gemäß §§ 20 und 21 SGB X gehalten, den Sachverhalt von Amts wegen zu ermitteln. Das legt ihr die Verpflichtung auf, Art und Umfang der Ermittlungen nach pflichtgemäßem Ermessen zu bestimmen. Sie hat alle für den Einzelfall bedeutsamen Umstände zu berücksichtigen ...

Das Verwaltungshandeln der Behörde steht allerdings auch unter dem Generalvorbehalt des § 13 Abs. 2 BDSG. Danach sind personenbezogene Daten zunächst bei dem Betroffenen zu erheben. Dem Bundesbeauftragten für den Datenschutz ist beizupflichten, daß der Gesetzgeber hierdurch den Grundsatz der Transparenz der Datenerhebung fördern wollte. Absatz 1 der genannten Vorschrift begrenzt den Umfang der zu erhebenden Daten auf die jeweils für die Erfüllung der Aufgaben der erhebenden Stelle erforderlichen Angaben. Nach meiner Auffassung kommen Sie dieser Verpflichtung nach, indem Sie den Betroffenen zur Vorlage von Unterlagen auffordern, die Ihnen eine rechtswirksame Entscheidung ermöglicht. Dem Bundesbeauftragten für den Datenschutz ist beizupflichten, wenn er Sie darauf hinweist, daß Sie den Betroffenen darüber informieren müssen, welche Daten zwingend für eine Entscheidung benötigt werden ...

Allerdings gilt der Grundsatz der Ersterhebung nicht uneingeschränkt. Nach Satz 2 des § 13 Abs. 2 BDSG dürfen Daten u. a. auch ohne die Mitwirkung des Betroffenen erhoben werden, wenn die zu erfüllende Verwaltungsaufgabe ihrer Art nach eine Erhebung bei anderen Personen und Stellen erforderlich macht und keine Anhaltspunkte dafür bestehen, daß überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden. Der Gesetzgeber hat somit Datenerhebung bei Dritten nicht prinzipiell ausgeschlossen, sondern lediglich an ihre Vornahme qualifizierende Voraussetzungen gebunden. Für das Verwaltungsverfahren der ... bedeutet dies, daß zunächst in einem zeitlich engen Rahmen die Vorschrift des § 13 Abs. 2 Satz 1 BDSG zum Tragen kommt, wonach die Daten ausschließlich beim Betroffenen zu erheben sind ... Erst wenn der zeitliche Rahmen verlassen wurde, ohne daß durch den Betroffenen die erforderliche Klarheit geschaffen wurde, ist die ... nach §§ 20 und 21 SGB X gehalten, zu prüfen, welche Maßnahmen von Amts wegen vorzunehmen sind. Hierzu können dann auch Erhebungen bei Dritten gehören, die dem Zwecke dienen, von dem Betroffe-

nen gemachte Angaben zu überprüfen, wenn diese nicht zweifelsfrei belegt wurden. ...".

Diese Ausführungen des Bundesversicherungsamtes gelten entsprechend für die Rechtslage nach Inkrafttreten des § 67 a SGB X, der ein zulässiges Abweichen vom Grundsatz der Ersterhebung im Hinblick darauf erschwert hat, daß das Sozialgeheimnis den regelmäßig sensiblen Sozialdaten einen besonderen Schutz verleiht.

Folgende Einzelfälle erscheinen mir vor diesem Hintergrund berichtenswert, weil sie typische Verfahrenssituationen und -praktiken kennzeichnen (zu Einzelfällen in der gesetzlichen Unfallversicherung siehe ab Nr. 14):

10.2.1 Sozialamt erfragt bei Ersatzkasse einer Sozialhilfeempfängerin Krankenhausaufenthaltszeiten

Der Datenschutzbeauftragte der BEK hatte sich im folgenden Fall mit der Bitte um datenschutzrechtliche Beratung an mich gewandt: Das Sozialamt eines Landkreises habe gebeten, die Angaben einer Sozialhilfeempfängerin über einen Krankenhausaufenthalt zu bestätigen bzw. die tatsächliche Dauer der stationären Behandlung mitzuteilen. Auf die entsprechende Rückfrage, ob die bei der BEK Versicherte ihrer Mitteilungspflicht nach § 60 Abs. 1 Nr. 1 SGB I nicht nachgekommen sei oder Zweifel an der Richtigkeit ihrer Angaben bestünden, hatte das Sozialamt geantwortet, daß dafür keine Anhaltspunkte bekannt seien. Der Datenschutzbeauftragte der BEK äußerte mir gegenüber daraufhin Zweifel an der Zulässigkeit der erbetenen Datenübermittlung.

In meiner Stellungnahme habe ich seine Zweifel bestätigt und ausgeführt, daß zu den gesetzlichen Aufgaben nach dem SGB zwar auch die Leistungen der Sozialhilfe gehören, für die die Kreise und kreisfreien Städte, die überörtlichen Träger der Sozialhilfe und, für besondere Aufgaben, die Gesundheitsämter zuständig sind (vgl. § 28 SGB I). Sowohl die gesetzlichen Krankenkassen als auch die Landkreise sind Leistungsträger im Sinne des § 12 SGB I und damit unter der Voraussetzung des § 69 SGB X gemäß § 35 Abs. 2 SGB I grundsätzlich zur Offenbarung befugt. Die Offenbarungsbefugnis selbst unterliegt jedoch dem Grundsatz der Erforderlichkeit. Diese entfällt, wenn der Betroffene seiner Auskunftspflicht gemäß § 60 Abs. 1 SGB I nachkommt. Da im vorliegenden Einzelfall vom anfragenden Sozialamt erklärt wurde, daß keine Anhaltspunkte dafür bekannt seien, daß die Sozialhilfeempfängerin ihrer Mitteilungspflicht nicht oder nicht zutreffend nachkomme, ist sie als Betroffene zunächst selbst nach einem entsprechenden Nachweis zu fragen oder ihr Einverständnis nach § 60 Abs. 1 Nr. 1 SGB I zur Erteilung der erforderlichen Auskünfte durch die BEK einzuholen.

Eine Abweichung vom Grundsatz der Ersterhebung beim Betroffenen wäre nur unter den Voraussetzungen des § 67 a Abs. 2 Satz 2 Nr. 1 SGB X zulässig, die hier ersichtlich schon deswegen nicht erfüllt sind, weil die bei der Betroffenen erhobenen Angaben die erforderlichen Informationen erbracht haben.

Die BEK hat daraufhin die erbetene Datenübermittlung abgelehnt. Die Anfrage ihres Datenschutzbeauftragten habe ich als nachahmenswertes Beispiel der Zusammenarbeit im Sinne vorsorglichen Datenschutzes ausdrücklich begrüßt.

10.2.2 Arbeitsamt erfragt bei Ersatzkasse eines Arbeitslosen den Zeitpunkt der Krankengeldzahlung

Ein Petent, der laufend Arbeitslosenhilfe bezog, wies dem Arbeitsamt durch Veränderungsanzeigen und Vorlage von Arbeitsunfähigkeitsbescheinigungen nach, daß er für eine Dauer von mehr als sechs Wochen arbeitsunfähig erkrankt war. Das Arbeitsamt gewährte ihm daraufhin weiterhin Arbeitslosenhilfe, hob deren Bewilligung jedoch nach Ablauf von sechs Wochen auf und übersandte dem Petenten eine Bescheinigung über die gewährte Arbeitslosenhilfe zur Vorlage bei seiner Krankenkasse. Auf den Widerspruch und die Klage des Petenten vor dem Sozialgericht hin fragte das Arbeitsamt vor der Klageerwiderung fernmündlich bei der Ersatzkasse des Petenten an, ob dieser tatsächlich vom Tage der Aufhebung des Bewilligungsbescheides Krankengeld erhalte. Die Ersatzkasse bestätigte dies.

Nach meiner datenschutzrechtlichen Bewertung, die ich den Beteiligten mitgeteilt habe, verstieß die Anfrage des Arbeitsamtes bei der Ersatzkasse des Petenten gegen den Grundsatz der Ersterhebung beim Betroffenen. Hinsichtlich der Übermittlung der erbetenen Angaben durch die Ersatzkasse folgt aus der Unzulässigkeit der Erhebung, daß die Übermittlung nicht erforderlich und daher von der Rechtsgrundlage des § 69 Abs. 1 Nr. 1 SGB X nicht gedeckt war.

Da die Bundesanstalt für Arbeit schon mit ihrer ersten Stellungnahme eingeräumt hatte, daß das Arbeitsamt durch die Anfrage bei der Ersatzkasse gegen das Gebot der Ersterhebung beim Betroffenen verstoßen habe, dessen Vorrang künftig aber beachten werde, habe ich auf eine förmliche Beanstandung gemäß § 25 Abs. 2 BDSG verzichtet.

10.3 Licht und Schatten bei der Gewährung von Auskunft und Einsichtnahme in Versichertenakten

Der Auskunftsanspruch der Betroffenen gegen die Leistungsträger wurde in § 83 SGB X im Rahmen des 2. SGB-Änderungsgesetzes neu geregelt. Rechtsgrundlage für die Einsichtnahme in die Akten bleibt unverändert der § 25 SGB X.

Sowohl im Bereich der Bundesanstalt für Arbeit wie auch der Bundesversicherungsanstalt für Angestellte wurden neugestaltete Verwaltungsvorschriften erlassen, die diese Rechte der Betroffenen regeln. Als beispielhaft und mustergültig erweist sich dabei der folgende Auszug aus der Regelung bei der BfA:

„Nach § 25 Abs. 1 Satz 1 SGB X hat jeder Versicherte das Recht auf Einsicht in die das Verwaltungsverfahren betreffenden Akten, soweit deren Kenntnis zur Geltendmachung oder Verteidigung seiner rechtlichen Interessen erforderlich ist.

Anträge von Versicherten, die von diesem Recht Gebrauch machen, dürfen nicht aus formalen Gründen abgelehnt werden. Durch § 19 Abs. 1 BDSG – jetzt § 83 SGB X – wird dem Versicherten das generelle Recht auf Auskunft über die zu seiner Person gespeicherten Daten eingeräumt. Das Auskunftsrecht schließt auch Daten in Akten ein (§ 1 Abs. 2 Nr. 1 BDSG). Damit besteht für jeden Versicherten letztlich ein unbeschränktes Akteneinsichtsrecht ohne Rücksicht darauf, ob ein Verwaltungsverfahren noch anhängig oder bereits abgeschlossen ist. Sofern der Versicherte selbst Akteneinsicht begehrt, kann grundsätzlich davon ausgegangen werden, daß ein rechtliches Interesse im Sinne des § 25 Abs. 1 Satz 1 SGB X vorliegt. Das Recht auf Akteneinsicht erstreckt sich auf den gesamten Vorgang und schließt ärztliche Unterlagen (z. B. Gutachten, Befundberichte und Entlassungsberichte) ein. Begehrt ein Versicherter Einsicht in ärztliche Unterlagen, ist in jedem Falle zunächst der Beratungsärztliche Dienst zu hören, ob aus medizinischer Sicht Bedenken gegen eine Offenbarung bestehen . . . Nach § 25 Abs. 2 Satz 4 SGB X wird das Recht nach Abs. 1 nicht beschränkt. Das bedeutet, dem Begehren auf Akteneinsicht ist zu entsprechen, wenn der Versicherte eine Vermittlung durch einen Arzt ablehnt und darauf besteht, selbst die Akten bzw. ärztlichen Unterlagen einzusehen. Aus den von der Rechtsprechung des BGH entwickelten zivilrechtlichen Grundsätzen zum Einsichtsrecht des Patienten in psychiatrische Krankenunterlagen kann keine Beschränkung des Rechts auf Akteneinsicht hergeleitet werden, denn für das Sozialrecht regelt § 25 SGB X die Akteneinsicht durch Beteiligte abschließend. Den Berechtigten sind auf Verlangen Ablichtungen der gewünschten Unterlagen zur Verfügung zu stellen (vgl. § 25 Abs. 5 SGB X).“

Diese Ausführungen der BfA sind besonders vorbildlich im Hinblick auf die Frage der Abhängigkeit des Einsichtsrechts von laufenden Verwaltungsverfahren und die Einsichtnahme in ärztliche/psychologische Unterlagen. Ich habe bereits mehreren anderen Trägern empfohlen, diese Regelungen entsprechend zu übernehmen.

In der Praxis treten jedoch im Hinblick auf das Einsichts- und Auskunftsrecht der Betroffenen immer wieder Probleme auf.

10.3.1 Die Einsichtnahme kann zu einer Gefährdung der Gesundheit des Betroffenen führen

Das Sozialgesetzbuch bestimmt in § 25 Abs. 2 SGB X, daß der Inhalt der Akten durch einen Arzt vermittelt werden soll, „soweit zu befürchten ist, daß die Akteneinsicht dem Beteiligten einen unverhältnismäßigen Nachteil, insbesondere an der Gesundheit, zufügen würde“ (vgl. 14. TB, S. 78). Die BfA hatte in einem derartigen Fall ein ärztliches Gutachten unmittelbar an den Hausarzt eines Versicherten gesandt. Sie ging dabei stillschweigend davon aus, daß es sich bei dem Hausarzt um einen Arzt des Vertrauens des Versicherten handelt. Im Bereich der BfA ist es ausgeschlossen, daß der Gutachteninhalt durch den Gutachterarzt selbst dem Betroffenen mitgeteilt wird. Gegen diese Vorgehensweise der BfA hat sich ein Petent gewandt.

Ich teile dessen Bedenken grundsätzlich. Denn gem. § 25 Abs. 2 letzter Satz SGB X hat letztendlich der Betroffene zu entscheiden, ob überhaupt und welcher Arzt ihm das Gutachten eröffnet und vermittelt. An eine Ausnahme von dieser Entscheidungsfreiheit kann allenfalls dann gedacht werden, wenn konkrete Anhaltspunkte dafür vorliegen, daß der Betroffene bei Kenntnisnahme des Akteninhaltes ohne ärztliche oder psychologische Begleitung akut suizidgefährdet ist – wohl ein sehr selten vorkommender Ausnahmefall.

Die Weitergabe des Gutachtens an den Hausarzt ohne Kenntnis des Betroffenen ist bedenklich. Ich habe der BfA vorgeschlagen, die Betroffenen in dem Antrag auf Einsichtsgewährung zu fragen, welcher Arzt die Einsichtsnahme begleiten soll.

Die BfA hat ihre Position zunächst damit gerechtfertigt, daß in ihrem Gesamtbereich eine einheitliche Einsichtsgewährung sicherzustellen sei. Des weiteren solle vermieden werden, daß der Gutachterarzt in die Situation kommt, Rechtsfragen entscheiden zu müssen, so z. B., ob im Einzelfall eine Einsichtnahme ausgeschlossen ist. Auch würde durch die Weitergabe des Gutachtens an den Hausarzt ohne Kenntnis des Betroffenen vermieden, daß er sich ab Kenntnis von der Weitergabe bis zur tatsächlichen Einsichtnahme über den Inhalt des Gutachtens ängstigt und so einer psychischen Streßsituation ausgesetzt sei.

Aus meiner Sicht berücksichtigen diese Argumente nicht hinreichend das Recht auf informationelle Selbstbestimmung. Deshalb habe ich zusammen mit der BfA einen Weg gefunden, der dem dargestellten Interessengegensatz aus datenschutzrechtlicher Sicht gerecht wird. Danach wird künftig bei der BfA einheitlich nur noch folgendes Verfahren maßgebend sein:

Bei einem Antrag auf Akteneinsicht, bei dem medizinische Unterlagen betroffen sind, wird ein beratender Arzt der BfA mit der Frage hinzugezogen, ob gegen die direkte Einsichtnahme im Hinblick auf § 25 Abs. 2 Satz 2 SGB X Bedenken bestehen. Entscheidet dieser, daß der Inhalt über einen Arzt vermittelt werden soll, wird der Betroffene aufgefordert, einen Arzt seines Vertrauens zu benennen. An diesen werden die betreffenden Unterlagen gesandt, damit dieser die kritischen Aspekte näher darlegen kann. Die Unterlagen werden also nicht mehr sofort dem Hausarzt übersandt in der Annahme, daß dies der Arzt des Vertrauens des Betroffenen ist. Weist der Versicherte auf sein uneingeschränktes Akteneinsichtsrecht gem. § 25 Abs. 2 letzter Satz SGB X hin, dann wird ihm die Einsicht direkt gewährt, ansonsten wird der von ihm benannte Arzt des Vertrauens hinzugezogen.

10.3.2 Betriebs- und Geschäftsgeheimnisse verhindern Auskunftsanspruch einer Arbeitnehmerin nicht

Eine freiwillig bei der Techniker-Krankenkasse (TKK) versicherte Arbeitnehmerin hatte mit ihrem – ehemaligen – Arbeitgeber vereinbart, die fälligen Beiträge zur Kranken-, Renten- und Arbeitslosenversicherung im Rahmen eines sogenannten Firmenbeitragseinzugsverfahrens an die TKK zu überweisen.

Bei diesem Verfahren werden die fälligen Beiträge durch den Arbeitgeber von dem Lohn/Gehalt abgezogen und direkt an die Krankenkasse übermittelt.

Im vorliegenden Fall hatte die Petentin den Verdacht, daß ihr ehemaliger Arbeitgeber diese Beiträge nicht oder in falscher Höhe überwiesen hatte. Sie wandte sich daher an die TKK mit der Bitte um Auskunft über die Höhe der Beiträge, die der Arbeitgeber hätte entrichten müssen. Diese Auskunft wurde ihr mit dem Hinweis auf datenschutzrechtliche Belange versagt.

Die Nachfragen eines von der Petentin beauftragten Rechtsanwaltes wurden damit beantwortet, daß das Betriebs- und Geschäftsgeheimnis des ehemaligen Arbeitgebers der Petentin, das nach § 35 Abs. 4 SGB I dem Sozialgeheimnis gleichsteht, einer Auskunft im Wege stehe.

Mir gegenüber argumentierte die TKK, daß bei einem freiwilligen Krankenversicherungsverhältnis grundsätzlich das Mitglied Beitragsschuldner sei. Anders verhalte es sich bei Vorliegen einer Firmeneinzugsermächtigung; hier sei der Arbeitgeber analog § 28 e SGB IV Beitragsschuldner für den Gesamtsozialversicherungsbeitrag (§ 28 d SGB IV). So sei bei einer Säumnis des Arbeitgebers ein Rückgriff auf den Versicherten nicht möglich. Die Daten über die Höhe der getätigten Beitragsüberweisungen fielen unter den Schutz des § 35 Abs. 4 SGB I, weshalb der Petentin nur bei Vorliegen einer Einwilligungserklärung des Arbeitgebers Auskunft erteilt werden könne.

Nach meiner Auffassung verstößt die Weigerung der TKK, Auskunft über die für die Petentin abgeführten Sozialversicherungsbeiträge zu geben, gegen den in § 83 Abs. 1 SGB X normierten Auskunftsanspruch. Die begehrte Information stellt zwar grundsätzlich ein Betriebs- und Geschäftsgeheimnis dar, welches nach § 35 Abs. 4 SGB I Sozialdaten gleichsteht. Auf diesen Geheimnisschutz kann sich der Arbeitgeber jedoch nur dann berufen, wenn er ein schützenswertes Interesse an der Geheimhaltung der Informationen hat. Zu den Betriebs- und Geschäftsgeheimnissen gehören nach der geläufigen Definition alle Informationen, die im Zusammenhang mit einem Geschäftsbetrieb stehen, nur einem begrenzten Personenkreis bekannt sind und – bei berechtigtem wirtschaftlichen Interesse an der Geheimhaltung – nach dem bekundeten Willen des Betriebsinhabers geheimgehalten werden sollen (Borchert/Hase/Walz – Gemeinschaftskommentar zum Sozialgesetzbuch, Rdnr. 20 zu § 35 SGB I und Rdnr. 39 zu § 67 SGB X). Im vorliegenden Fall ist ein berechtigtes Interesse des ehemaligen Arbeitgebers an der Geheimhaltung der für die Petentin abgeführten Sozialversicherungsbeiträge nicht ersichtlich.

Da die Petentin ausschließlich Auskunft über ihre sozialversicherungsrechtlichen Belange begehrt, ist auch unter Berücksichtigung schutzwürdiger Interessen des Arbeitgebers kein Grund für eine Verweigerung der Auskünfte erkennbar. Insbesondere kommt es hierbei nicht auf eine Einwilligung des ehemaligen Arbeitgebers und auf die Frage an, ob die begehrte Auskunft für die Erfüllung einer gesetzlichen Aufgabe der TKK oder für die Durchführung eines damit zusammenhängenden Verfahrens erforderlich ist.

Die TKK hat ergänzend mitgeteilt, daß bei ihr keine Aufzeichnungen darüber vorliegen, welche Beiträge für die Petentin gezahlt wurden. Dies sei durch den Umstand zu erklären, daß mit ihrem ehemaligen Arbeitgeber das Firmenbeitragseinzugsverfahren vereinbart und auch praktiziert wurde. Zu diesem Vorbringen habe ich das Bundesversicherungsamt um Stellungnahme gebeten.

10.3.3 Falsche Bezugnahme auf das Sozialgeheimnis

Ein Arbeitsamt hatte zunächst gegenüber einem Arbeitslosen die Einsichtnahme unter Berufung auf die Wahrung von Geschäftsgeheimnissen im Sinne von § 35 Abs. 4 SGB I verweigert.

Dieser wandte sich daraufhin an mich und teilte mit, er habe beim zuständigen Arbeitsamt die Übersendung einer Kopie der Stellungnahme seines ehemaligen Arbeitgebers zu seinem Antrag auf Gleichstellung mit Schwerbehinderten nach § 2 Schwerbehindertengesetz erbeten. Da die Firma einer Offenbarung nach § 67 SGB X nicht zugestimmt habe, habe ihm das Arbeitsamt unter Berufung auf § 35 Abs. 4 SGB I die Überlassung einer Ablichtung verweigert.

Nach erneuter Prüfung räumte die Bundesanstalt für Arbeit jedoch ein, eine Überprüfung des Vorganges habe ergeben, daß die Weitergabe der gewünschten Information keine Offenbarung im Sinne des § 35 SGB I sei, da diese nur an den Betroffenen selbst zu richten gewesen wäre.

Das Arbeitsamt gewährte daraufhin dem Petenten Akteneinsicht und händigte auch die gewünschte Ablichtung aus.

10.3.4 Kein Urheberrecht des Gutachterarztes gegen Einsichtsrecht des Betroffenen

Die Südwestliche-Bauberufsgenossenschaft verwendet in den Antwortschreiben bei Auskunfts- oder Einsichtsbegehren von Versicherten unterschiedliche Textbausteine. Einleitend weist sie darin jeweils darauf hin, daß ein Rechtsanspruch auf Akteneinsicht sowie die diesem Anspruch gleichstehende Erteilung von Ablichtungen bestimmter Aktenauszüge (z. B. Gutachten) darauf beschränkt ist, daß deren Kenntnis zur Geltendmachung oder Verteidigung rechtlicher Interessen „in dem Verfahren gegen die Berufsgenossenschaft" erforderlich sei. Ein ärztliches Gutachten dürfe zu keinem anderen Zweck verwendet werden, beispielsweise dürfe es nicht einer Versicherungsgesellschaft oder ähnlichen Stellen vorgelegt werden. Dies wird mit urheberrechtlichen Vorschriften, die den Gutachter schützen sollen, begründet. Nach dem Inhalt eines weiteren Textbausteines wird darüber hinaus die Gutachtenübersendung mit der Begründung abgelehnt, daß nicht zu erkennen sei, daß die Gutachteneinsicht tatsächlich nur dem Zweck des Geltendmachens oder der Verteidigung der rechtlichen Interessen „gegenüber der Berufsgenossenschaft" dienen solle.

Die Verweigerung eines Einsichtsrechts in derartigen Fällen durch die Südwestliche-Bauberufsgenossenschaft ist nicht rechtens. § 25 SGB X regelt abschließend das Einsichtsrecht der Betroffenen im Sozialbereich. Eine Verweigerung der Einsichtnahme kann somit nur auf § 25 Abs. 3 SGB X gestützt werden. In Betracht käme vorliegend ein Ausschluß dieses Rechts allenfalls, weil die Vorgänge wegen berechtigter Interessen dritter Personen – der Gutachterärzte – geheimgehalten werden müssen.

Dieser Ausnahmetatbestand ist aber insbesondere im Hinblick auf die Einsichtnahme in ärztliche Gutachten zu verneinen. Die Frage der Geheimhaltung ist in § 35 SGB I i.V. m. §§ 67 bis 85 SGB X für den Bereich der Sozialverwaltung abschließend geregelt. Die Berufsgenossenschaft hat hier gegenüber den Antragstellern eine Offenbarungsbefugnis nach § 69 Abs. 1 Nr. 1 SGB X. Für ihre Aufgabenerfüllung ist es erforderlich, gegenüber dem Betroffenen offenzulegen, auf welche Grundlagen sie ihre Entscheidung im Zusammenhang mit einer Berufskrankheit oder einem Arbeitsunfall stützt (vgl. § 35 SGB X).

Ein berechtigtes Interesse der Gutachter an der Geheimhaltung ihrer Gutachten ist daher gerade gegenüber den von der Begutachtung Betroffenen auszuschließen. Die ärztlichen Gutachten dienen weder den Interessen des Arztes, noch stellen sie einen Selbstzweck dar; sie sind ausschließlich dazu bestimmt, über den Gesundheitszustand eines Versicherten Aufschluß zu geben. Der Transparenzgrundsatz erfordert daher elementar, daß sich der Betroffene über den Inhalt des ausschließlich über ihn erstellten Gutachtens informieren kann.

10.3.5 Einsicht auch in Befundunterlagen von ärztlichen Gutachten

In einem weiteren Fall wünschte ein Petent vom Arbeitsamt – vergeblich – vollständigen Einblick in das dort erstellte ärztliche Gutachten einschließlich der Befundunterlagen.

Nach Auskunft des zuständigen Arbeitsamtsarztes wurde der Petent von einem Vertragsarzt des Arbeitsamtes untersucht, der das ärztliche Gutachten anschließend dem Ärztlichen Dienst des Arbeitsamtes übersandte.

Eine Ablichtung dieses Gutachtens wurde dem Petenten – allerdings ohne die von ihm gewünschten Befunddaten – überlassen.

Nach dieser Auskunft wurde die Einsicht in die Befunddaten im Hinblick auf § 25 Abs. 1 Satz 1 SGB X abgelehnt, da der Petent als Begründung angegeben habe, er benötige die Akteneinsicht bzw. eine entsprechende Kopie der Befundunterlagen für seine persönlichen Unterlagen. Ferner sei man davon ausgegangen, daß der untersuchende Vertragsarzt das Gutachten mit dem Petenten erörtert habe.

Dem Petenten sei jedoch angeboten worden, die Befundunterlagen nach einer entsprechenden Schweigepflichtentbindungserklärung seinem Hausarzt zuzuleiten, was der Petent jedoch abgelehnt habe.

Nach den von mir geführten Gesprächen ließ sich die Ablehnung der Akteneinsicht in die Befundunterlagen durch den Ärztlichen Dienst des Arbeitsamtes in erster Linie dadurch erklären, daß diesem nicht bekannt war, daß schon aufgrund der durch den Petenten ergriffenen Rechtsbehelfe die Voraussetzungen des § 25 Abs. 1 SGB X vorlagen.

Ferner bestand dahin gehend Unklarheit, daß nach herrschender Meinung, über die ich auch mit der Hauptstelle der Bundesanstalt für Arbeit Übereinstimmung erzielt hatte, § 25 SGB X im Interesse des Transparenzgebotes für den Betroffenen weit auszulegen ist.

Die Bundesanstalt für Arbeit hat in ihrer Stellungnahme meinen Ausführungen beigepflichtet und mitgeteilt, die zuständigen Stellen seien nochmals zur strikten Beachtung angehalten worden.

10.4 Leistungssachbearbeitung für Mitarbeiter der Betriebskrankenkasse vorbildlich geregelt

Anläßlich einer Kontrolle bei der Betriebskrankenkasse der Preussag AG konnte ich mich von dem im folgenden geschilderten Verfahren der Leistungssachbearbeitung für die Mitarbeiter der Betriebskrankenkasse überzeugen. Nach Darstellung der dortigen Mitarbeiter bestanden zunächst Überlegungen, die Leistungsabrechnung in eine andere Geschäftsstelle zu verlagern. Diese Verfahrensweise wurde jedoch in einer vom Betriebsrat einberufenen Betriebsversammlung abgelehnt, da die Beschäftigten der Kasse in diesem Fall zu Beratungsgesprächen von Salzgitter nach Hannover, Kiel bzw. Schüttdorf hätten fahren müssen. Daraufhin haben sich Betriebsrat und Geschäftsführung auf folgende Verfahrensweise verständigt:

Von der Betriebsversammlung wurden 7 Kollegen und Kolleginnen vorgeschlagen, von denen jeweils der männliche Kandidat und die weibliche Kandidatin mit den meisten Stimmen als die künftigen Bearbeiter von Mitarbeiterleistungsvorgängen bestimmt werden sollten. Jeder Wahlberechtigte erhielt zwei Stimmen. Die beiden in geheimer Wahl gewählten Bearbeiter wurden inzwischen von der Geschäftsführung mit der Wahrnehmung der Leistungsabrechnung betraut. Dabei können die BKK-Mitarbeiter künftig jeweils selbst bestimmten, welcher der beiden Kollegen ihre Anträge bearbeiten soll.

Ich habe diese Regelung als vorbildlich, sowohl im Hinblick auf das in § 35 Abs. 1 Satz 3 SGB I reflektierte, strikte funktional-personelle Abschottungsprinzip, als auch auf das von der BKK praktizierte Organisationsverfahren, begrüßt, da dem Recht der Mitarbeiter auf informationelle Selbstbestimmung damit in vorbildlicher Weise Rechnung getragen wird. Darüber hinaus habe ich empfohlen, das beschriebene Verfahren der Leistungsbearbeitung der Mitarbeiter der BKK in die allgemeinen Richtlinien für die Führung der Verwaltungsgeschäfte aufzunehmen.

Eine entsprechende Regelung für das Widerspruchsverfahren wurde von der BKK als verzichtbar angesehen, da bisher kein einziger Mitarbeiter Widerspruch

gegen einen Leistungsbescheid erhoben hat. Die Widerspruchsbearbeitung im Sinne der Satzung und der Geschäftsordnung für das Vorverfahren und das Einspruchsverfahren in der derzeit gültigen Form begegnet aus datenschutzrechtlicher Sicht grundsätzlichen Bedenken, da der Geschäftsführer zunächst über die Abhilfe des Widerspruchs entscheidet, bevor der Widerspruchsausschuß damit befaßt wird. Dem Widerspruchsausschuß gehört ebenfalls der Geschäftsführer oder ein von ihm Beauftragter beratend an. Ein solches Verfahren ist mit den Vorgaben des § 35 Abs. 1 Satz 3 SGB I nicht vereinbar. Eine Regelung hingegen, der zufolge über die Abhilfe eines Widerspruchs der zunächst nicht betroffene Beihilfebearbeiter und ggf. abschließend der Widerspruchsausschuß entscheidet, dem dabei aber Personen, die Personalentscheidungen treffen oder daran mitwirken können, nicht – auch nicht mit beratender Stimme – angehören dürfen, würde die vorbildliche Leistungssachbearbeitung für die Mitarbeiter der Betriebskrankenkasse vervollständigen.

10.5 Geschäftsführer einer Krankenkasse untersagt dem internen Datenschutzbeauftragten die Kontrolle der Versicherten- und Personaldaten

Der interne Datenschutzbeauftragte einer Krankenkasse wandte sich an mich mit der Bitte um datenschutzrechtliche Beratung. Er hatte der Geschäftsführung seiner Kasse angekündigt, die Führung der Versicherten- und Personaldaten der Mitarbeiter der Kasse zu kontrollieren. Daraufhin war er vom Geschäftsführer der Kasse schriftlich angewiesen worden, *„... sich außer in konkreten Fällen, die von Mitarbeitern an Sie herangetragen werden und bei denen die Zustimmung zur Einsicht in die Unterlagen impliziert ist, sich auf die Prüfung der allgemeinen Verfahrensabläufe zu beschränken"*.

Zum Problem der Befugnisse des internen gesetzlichen Datenschutzbeauftragten bei Sozialleistungsträgern im Sinne des § 81 Abs. 4 SGB X, §§ 18 Abs. 2, 36, 37 Abs. 1 BDSG analog und zu der Frage, ob und ggf. inwieweit der gesetzliche Datenschutzbeauftragte bei seiner Aufgabenerfüllung Weisungen der Geschäftsführung unterliegt, habe ich wie folgt Stellung genommen.

- Während der sog. **betriebliche** DSB nach dem Bundesdatenschutzgesetz mit einer umfassenden und nicht eingeschränkten Kontrollkompetenz ausgestattet ist (§ 37 Abs. 1 BDSG), ist dies beim sog. **behördlichen** DSB nicht der Fall; hier gibt es die grundsätzlich umfassende Kontrollkompetenz des BfD bzw. der LfD (s. hierzu auch Nr. 31.2.2).
- Anders verhält es sich im Falle von Sozialleistungsträgern im Sinne des § 12 SGB I. In diesem Bereich hat der Gesetzgeber die Einrichtung eines internen DSB gesetzlich vorgeschrieben und ihn mit demselben Status, denselben Aufgaben und Kompetenzen ausgestattet, wie sie nach §§ 36, 37 Abs. 1 BDSG für den betrieblichen DSB vorgesehen sind (§ 81 des 4 SGB X). Ausschlaggebend für die Entscheidung des Gesetzgebers, den Behörden im sozialen Bereich einen **gesetzlichen** DSB vorzuschreiben, ist die besondere Schutzwürdigkeit der meisten hier verarbeiteten personenbezogenen Daten.

  Das Kontrollrecht des gesetzlichen DSB schließt die uneingeschränkte Befugnis ein, die Einhaltung des Datenschutzes bei der Bearbeitung von Mitglieder- und Leistungsdaten der Mitarbeiter insbesondere durch Einsichtnahme in die entsprechenden Akten oder automatisierten Verarbeitungssysteme zu kontrollieren. Der besonderen Gefährdung des Rechts auf informationelle Selbstbestimmung der Mitarbeiter von Sozialleistungsträgern dadurch, daß Versichertendaten in Personalentscheidungen einfließen können, hat der Gesetzgeber in § 35 Abs. 1 Satz 3 SGB I Rechnung getragen. Danach ist die interne Weitergabe an bzw. das Zugänglichsein von Sozialdaten der Mitarbeiter oder deren Angehöriger für Personen, die Personalentscheidungen treffen oder daran mitwirken können, strikt verboten worden.

  Für die Kontrollkompetenz des gesetzlichen DSB im Bereich der Sozialleistungsträger folgt daraus, daß er die datenschutzgerechte Organisation und Bearbeitung von Mitarbeiter-Versichertendaten ebenso wie die der Mitarbeiter-Personaldaten nur dann analog § 37 Abs. 1 BDSG im Wortsinne sicherstellen kann, wenn seine Kontrollkompetenz sowohl den einen wie auch den anderen Bereich einschließt. Daraus ergibt sich, daß dem gesetzlichen DSB der Sozialleistungsträger grundsätzlich auch ein umfassendes Kontrollrecht hinsichtlich der Personalverwaltung zusteht, das die Einsichtnahme in Personalakten oder in Personaldatenverarbeitungssyteme einschließt.
- Aufgaben und Befugnisse des gesetzlichen DSB sind auch nicht durch entsprechende Weisungen der Geschäftsführung einschränkbar. Die eingangs zitierte Weisung des Geschäftsführers einer Krankenkasse ist mit der Weisungsfreiheit des gesetzlichen DSB nicht vereinbar. Denn es ist der Leitung der speichernden Stelle insbesondere untersagt, den Beauftragten durch Anweisungen aufgrund des Direktionsrechts bei seiner Arbeit zu behindern. Das Weisungsverbot berührt umgekehrt nicht die Befugnis oder Verpflichtung der Leitung der Dienststelle, den DSB anzuweisen, bestimmte Aufgaben nach Maßgabe des § 37 Abs. 1 BDSG durchzuführen. Der DSB muß zwar die Anordnungen seines Geschäftsführers befolgen, allerdings nur so lange, wie sie ihn nicht bei seiner Aufgabe behindern. Die Weisungsfreiheit ist insofern Grundbedingung einer wirklichen Überwachung.

  Andererseits bedeutet Weisungsfreiheit aber nicht zugleich Entscheidungsfreiheit. Die Entscheidungskompetenz auch in Datenschutzfragen verbleibt bei der Leitung der Dienststelle. Ihr steht damit auch das Recht zu, die Tätigkeit des DSB zu kontrollieren. In diesem Rahmen ist die Behördenleitung befugt, auch dem DSB Weisungen zu erteilen, die darauf abzielen, festgestellte Mängel zu beseitigen.
- Bei einer Kontrolle der Südwestlichen Bau-Berufsgenossenschaft zeigte sich, daß der Dienstherr dort die Weisungsfreiheit und Aufgabenstellung des

internen DSB nicht hinreichend berücksichtigt hatte. So wollte der Geschäftsführer Gespräche meiner Mitarbeiter mit dem DSB zunächst nur in seiner Gegenwart zulassen. Ich habe klargestellt, daß zum einen aus § 37 Abs. 1 Satz 2 BDSG das Recht des DSB folgt, sich unabhängig vom Wissen und Willen der Geschäftsführung unmittelbar an den BfD zu wenden, falls er dies für erforderlich hält. Zum anderen entspricht es meiner gesetzlich garantierten Unabhängigkeit, über Gegenstand und Form meiner Kontroll- und Beratungstätigkeit innerhalb des von § 24 BDSG gesteckten Rahmens selbst zu entscheiden und ggf. Einzelgespräche mit dem DSB zu führen.

10.6 Einordnung des Rehabilitations- und Schwerbehindertenrechts in das Sozialgesetzbuch

Das Bundesministerium für Arbeit und Sozialordnung hat einen Entwurf zur Einordnung des Rehabilitations- und Schwerbehindertenrechts in das Sozialgesetzbuch (Entwurf eines SGB IX) vorgelegt. Nach einer ersten Prüfung des Gesetzesvorhabens im Hinblick auf die Regelungen zum Umgang mit personenbezogenen Daten bin ich der Auffassung, daß auch in diesem Sozialgesetzbuch bereichsspezifische Regelungen über den Umgang der dort genannten Stellen mit personenbezogenen Daten zu schaffen sind. Auf entsprechende Abschnitte in bereits in Kraft getretenen Büchern des Sozialgesetzbuches (§§ 284 ff. SGB V, 147 ff. SGB VI und 61 ff. SGB VIII) habe ich hingewiesen.

Demgegenüber wird seitens des Bundesministeriums für Arbeit und Sozialordnung die Ansicht vertreten, daß die Aufnahme von bereichsübergreifenden Regelungen über den Schutz personenbezogener Daten in den Entwurf des SGB IX nicht erforderlich sei. Zur Begründung wird angeführt, daß für die verschiedenen Rehabilitationsträger über die allgemeinen Datenschutzregelungen in § 35 SGB I i.V. m. §§ 67 bis 85 SGB X hinaus trägerspezifische Datenschutzregelungen in den einzelnen Sozialleistungsbereichen – wie oben genannt – gelten. Ein Bedarf für bereichsübergreifende Regelungen sei daher nicht erkennbar.

Diese Ausführungen überzeugen mich nicht. Es ist vorgesehen, im SGB IX spezifisch das Rehabilitations- und Schwerbehindertenrecht zu regeln. Damit ergeben sich auch spezifische Erfordernisse für Regelungen, insbesondere welche personenbezogenen Daten an wen übermittelt und zu welchem Zweck sie bei den einzelnen Stellen erhoben, verarbeitet und genutzt werden dürfen. Diese Vorschriften haben sich am Inhalt der sachlichen Notwendigkeiten der Aufgaben der einzelnen im SGB IX genannten Stellen zu orientieren. Ich werde dazu mit dem Bundesministerium für Arbeit und Sozialordnung im Gespräch bleiben.

10.7 Die Pflegeversicherung – SGB XI –

Nach der Konzeption des Gesetzes wird die Pflegeversicherung als neuer Zweig der Sozialversicherung geschaffen. Träger der Pflegeversicherung sind die Pflegekassen. Deren Aufgaben werden jeweils von der Krankenkasse wahrgenommen, bei der ein Bürger krankenversichert ist. Datenschutzrechtlich ist die Pflegekasse als eigenständige speichernde Stelle anzusehen.

Aufgrund der Anlehnung an die gesetzliche Krankenversicherung orientierte sich bereits der erste, vom Bundesministerium für Arbeit und Sozialordnung (BMA) vorgelegte Entwurf des Pflegeversicherungsgesetzes nahezu vollständig an den bereichsspezifischen Datenschutzvorschriften des SGB V (Gesetzliche Krankenversicherung). Auf die datenschutzgerechte Formulierung insbesondere der folgenden Regelungen konnte ich hinwirken:

- Soweit der Versicherte durch den Medizinischen Dienst zur Feststellung der Voraussetzungen für die Einstufung als Pflegebedürftiger und damit Leistungsberechtigter zu untersuchen ist, weist das Gesetz darauf hin, daß die §§ 65, 66 SGB I unberührt bleiben (§ 18 Abs. 2 SGB XI). Dies bedeutet, daß der Versicherte nur im Rahmen der dort festgelegten Grenzen mitwirkungspflichtig ist, d. h. sich nur in diesem Rahmen untersuchen lassen muß. Der Verweis im Pflegeversicherungsgesetz stellt sicher, daß in den Fällen, in denen er nicht mitwirkungspflichtig ist, entsprechende Datenerhebungen unterbleiben und ihm dadurch keine Nachteile entstehen.
- In einer Vereinbarung der Spitzenverbände der Pflegekassen und Krankenkassen muß festgelegt werden, welche Daten von der für den Versicherten zuständigen Pflege- und Krankenkasse gemeinsam genutzt werden dürfen. Dies ist der Fall, soweit die Kranken- und die Pflegekasse dieselben Daten für die jeweils zu erfüllende Aufgabe benötigen. An der abschließenden Festlegung dieses Datenkataloges sind das BMA und ich zu beteiligen (§ 96).

10.8 Häufige Verstöße im Zusammenhang mit dem Widerspruchsrecht nach § 76 Abs. 2 Nr. 1 SGB X

Gemäß § 76 Abs 1 SGB X ist die Übermittlung von Sozialdaten, die einem Sozialleistungsträger von einem Arzt oder einer anderen in § 203 Abs. 1 und 3 Strafgesetzbuch genannten Person zugänglich gemacht worden sind, nur unter den Voraussetzungen zulässig, unter denen diese Person selbst übermittlungsbefugt wäre. Nach den zur ärztlichen Schweigepflicht entwickelten Grundsätzen ist dafür die Einwilligung des Patienten erforderlich, soweit nicht eine gesetzliche Mitteilungspflicht besteht oder die Offenbarung unter den Voraussetzungen des § 34 StGB (rechtfertigender Notstand) zum Schutze eines höheren Rechtsgutes erforderlich ist. Daneben muß die Übermittlung für die Erfüllung sozialer Aufgaben erforderlich sein (§ 69 SGB X).

Diese besondere Einschränkung der Offenbarungsbefugnis durch die Ausweitung der ärztlichen Schweigepflicht auf den Sozialleistungsträger entfällt nach § 76 Abs. 2 SGB X im Rahmen der Aufgabenerfüllung durch den Träger für medizinische

Angaben, die ihm im Zusammenhang mit einer Begutachtung wegen der Erbringung von Sozialleistungen oder wegen der Ausstellung einer Bescheinigung übermittelt worden sind. In diesen Fällen kann der Betroffene allerdings der Offenbarung widersprechen.

In der Vergangenheit ergaben sich datenschutzrechtliche Probleme häufig daraus, daß Sozialleistungsträger darauf verzichteten, den Betroffenen über sein Widerspruchsrecht zu informieren; sie beriefen sich darauf, daß dies nicht gesetzlich vorgeschrieben sei. Ich habe mit dem Bundesversicherungsamt demgegenüber stets die Auffassung vertreten, daß Leistungsträger vor einer Übermittlung von unter § 76 SGB X fallenden Daten den Betroffenen stets über die Absicht der Übermittlung aufzuklären haben. Der Deutsche Bundestag hat in einer einvernehmlichen Entschließung meine Auffassung bestätigt und ausgeführt, daß das Widerspruchsrecht nur wahrgenommen werden könne, wenn der Betroffene von der beabsichtigten Übermittlung wisse (BT-Drucksache 10/1719).

Nach der Neufassung des SGB X ist in § 76 Abs. 2 Nr. 1 nunmehr klargestellt, daß der Betroffene zu Beginn des Verwaltungsverfahrens in allgemeiner Form schriftlich auf sein Widerspruchsrecht hinzuweisen ist. Gleichwohl habe ich auch nach Inkrafttreten der Neuregelung im Berichtszeitraum Verstöße gegen die Hinweispflicht feststellen müssen: Teilweise wurde Betroffenen kein Hinweis auf ihr Widerspruchsrecht gegeben, teilweise wurden eingelegte Widersprüche nicht beachtet.

Im Zusammenhang mit § 76 Abs. 2 SGB X bestehen allerdings noch weitere Probleme, die einer datenschutzgerechten Lösung bedürfen. So weigern sich inzwischen einige Sozialleistungsträger – mit Unterstützung des BMA – unter Berufung auf den Wortlaut der neugefaßten Regelung über die Hinweispflicht, den Betroffenen vor der Übermittlung an einen bestimmten Empfänger, über diesen und den konkreten Zweck aufzuklären. Dies erscheint mir indessen im Hinblick auf das Grundrecht auf informationelle Selbstbestimmung und den Grundsatz der Verhältnismäßigkeit in Fällen geboten, in denen die medizinischen Daten des Betroffenen an ärztliche Gutachter übermittelt werden sollen. Zumindest muß dem Betroffenen in angemessener Weise ermöglicht werden, die Übermittlung seiner Daten an ärztliche Gutachter zu verhindern, die er aus wichtigem Grund im Sinne des § 65 Abs. 1 Nr. 2 SGB I ablehnen würde.

Ohne konkrete Information über den Zweck der Übermittlung und ggf. die Person des vorgesehenen Gutachters bleibt dem Betroffenen, wenn er die Beauftragung eines ihm nicht genehmen Gutachters unter allen Umständen ausschließen will, nur die Möglichkeit eines pauschalen Widerspruchs. Dies würde stets zu einer Verfahrensverzögerung führen, und zwar auch in den Fällen, in denen der Betroffene keine Einwände gegen den vorgesehenen ärztlichen Gutachter hätte. Dem Versicherten würde damit das Risiko einer ihm nachteiligen Verfahrensverzögerung auferlegt, ohne Kenntnis der Person des in Aussicht genommenen Gutachters Widerspruch einlegen zu müssen, um seine Rechte zu wahren, obwohl er bei Kenntnis des vorgesehenen Gutachters gar keinen Widerspruch erhoben hätte. Dies erscheint unzumutbar und mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Hinzu kommt, daß Versicherte, wie ich festgestellt habe, von ihrem pauschalen Widerspruchsrecht zu Beginn des Verfahrens offenbar aufgrund der Befürchtung kaum oder gar nicht Gebrauch machen, sie könnten damit ihren gesetzlichen Leistungsanspruch gefährden. Denn der Hinweis auf das Widerspruchsrecht wird regelmäßig mit dem weiteren Hinweis darauf verbunden, daß „bei einem Widerspruch aber die Leistung ganz oder teilweise versagt oder entzogen werden kann, nachdem auf diese Folge schriftlich hingewiesen und eine gesetzte Frist verstrichen ist (§ 66 SGB I)". Eine datenschutzrechtlich vorbildliche Lösung dieses Problems hat – meines Wissens als bisher einziger Sozialleistungsträger – die BfA gefunden (vgl. Nr. 10.12.5).

10.8.1 Berufsgenossenschaft der chemischen Industrie beachtet § 76 Abs. 2 SGB X nicht

Eine Versicherte beantragte bei der Berufsgenossenschaft die Anerkennung einer Berufskrankheit. Nach erfolglosem Verwaltungsverfahren ist die Angelegenheit mittlerweile in zweiter Instanz beim Landessozialgericht Hessen anhängig.

Ein gerichtsseitig bestellter Gutachter bejahte eine beruflich bedingte 30%ige Erwerbsminderung. Das Gutachten erhielt die Berufsgenossenschaft vom Gericht zur Stellungnahme. Zu diesem Zweck leitete sie das Gutachten und zusätzliche medizinische Informationen aus ihrer Verwaltungsakte an einen externen Gutachter weiter.

Die Versicherte wurde allerdings zu Beginn des Verwaltungsverfahrens nicht auf ihr Widerspruchsrecht nach § 76 Abs. 2 Nr. 1 SGB X bezüglich solcher medizinischer Daten hingewiesen, die der Berufsgenossenschaft in diesem Verfahren von einem Arzt zugänglich gemacht wurden. Darüber hinaus wurde sie nicht vorab über die konkret anstehende Übermittlung informiert.

Soweit es um die Übermittlung von medizinischen Daten aus dem Gerichtsgutachten geht, ist ein rechtskräftiges Urteil des Landessozialgericht Nordrhein-Westfalen von Bedeutung, auf das sich die BG beruft. Das Landessozialgericht vertritt die Auffassung, daß § 76 Abs. 2 Nr. 1 SGB X bei einer Übermittlung eines gerichtsseitig zur Verfügung gestellten medizinischen Gutachtens nicht einschlägig sei, weil das Gutachten nicht von einem Arzt, sondern vom Gericht an einen Unfallversicherungsträger zur Verfügung gestellt wurde. Mich überzeugt dieses Urteil nicht, weil es Sinn und Zweck des § 76 Abs. 2 Nr. 1 SGB X nicht Rechnung trägt, wenn ein Zugänglichmachen durch einen Arzt nur deshalb verneint wird, weil aufgrund prozeßrechtlicher Vorgaben die unmittelbare Zurverfügungstellung durch das Gericht erfolgt und nur deshalb bei einer anschließenden Weiterleitung durch eine BG an Dritte kein Widerspruchsrecht bestehen soll.

Die Übermittlung von medizinischen Informationen aus der Verwaltungsakte an einen externen Gutachter habe ich sowohl angesichts des nichterfolgten Hinweises auf das Widerspruchsrecht in allgemeiner Form zu Beginn des Verwaltungsverfahrens als auch bezüglich der Nichtinformation über die konkrete Übermittlung, deren Adressaten und ihren Inhalt als Verstoß gegen die Hinweispflicht auf das Widerspruchsrecht nach § 76 Abs. 2 Nr. 1 SGB X beanstandet.

Meine Empfehlung, den Versicherten ggf. über den Zweck eines bevorstehenden Begutachtungsauftrags und die Person des ärztlichen Gutachters zu informieren oder die von der BfA praktizierte Lösung zu übernehmen, hat die BG-Chemie unter Hinweis auf den Wortlaut des § 76 Abs. 2 Nr. 1 SGB X bedauerlicherweise abgelehnt. Ich werde mich weiter für eine datenschutzgerechte Lösung dieser Problematik einsetzen.

10.8.2 Bundesausführungsbehörde für Unfallversicherung – BAfU – übersendet Akte mit medizinischen Informationen an Gutachter trotz Widerspruchs nach § 76 Abs. 2 SGB X

Im Rahmen eines Verwaltungsverfahrens über die Anerkennung einer Berufskrankheit übersandte die BAfU die über eine Petentin geführte Verwaltungsakte, die auch medizinische Informationen im Sinne des § 76 Abs. 2 SGB X enthielt, dem zuständigen staatlichen Gewerbearzt zur Stellungnahme. Dieser beauftragte mit Einverständnis der BAfU einen Arbeitsmediziner mit der Untersuchung und Begutachtung der Petentin. Die Petentin hatte indessen bereits vor Versendung der Akte an den Gewerbearzt die BAfU darum gebeten, daß eine Weitergabe von Unterlagen an eine Stelle außerhalb der BAfU vorher mit ihr abzustimmen sei.

Als die Petentin von der Einschaltung des weiteren Gutachters erfuhr, teilte sie der BAfU unter Bezug auf ihren Widerspruch mit, daß sie von diesem Gutachter nicht begutachtet werden wolle. Er habe sie bereits früher im gleichen Zusammenhang untersucht und begutachtet. Aufgrund der hierbei angewandten Untersuchungsmethoden habe sich ihr Gesundheitszustand dauerhaft erheblich verschlechtert. Daher sei sie auch mit einer Weitergabe der Unterlagen an diesen Gutachter nicht einverstanden.

Die BAfU teilte der Petentin daraufhin mit, es verbleibe gleichwohl bei der Entscheidung, daß der betroffene Arzt ein Gutachten nach Aktenlage erstellen solle und beließ die Unterlagen der Petentin beim Gutachter. Auf deren Grundlage erstellte dieser Arzt ein für die Petentin negatives Gutachten nach Aktenlage, dem der staatliche Gewerbearzt beitrat.

Bereits die Versendung der Unterlagen an den staatlichen Gewerbearzt und deren Weitergabe durch diesen an den ärztlichen Gutachter verstieß gegen das Sozialgeheimnis im Sinne des § 35 Abs. 1 SGB I i.V. m. §§ 69 Abs. 1, 76 Abs. 2 SGB X. Soweit es um ärztliche Untersuchungsdaten im Sinne des § 76 Abs. 2 SGB X geht, war die Bitte der Petentin als Widerspruch gem. § 76 Abs. 2 Nr. 1 SGB X zu werten.

Mit der Erhebung des Gutachtens hat die BAfU gegen die Vorschriften der bis 30. Juni 1994 geltenden § 79 Abs. 1 SGB X i.V. m. § 13 BDSG verstoßen. Das Gutachten war infolge des Widerspruchs der Petentin gegen die Übermittlung ihrer Unterlagen und aufgrund ihrer Ablehnung des Gutachters aus wichtigem Grund gem. § 65 Abs. 1 Nr. 2 SGB I ungültig und damit als gegenstandslos zu betrachten.

Erst nachdem ich aufgrund der Eingabe der Petentin gegenüber der BAfU Stellung genommen hatte, hat diese auf meine dringende Empfehlung hin alle Exemplare des Gutachtens zunächst gesperrt, da nicht auszuschließen war, daß durch eine sofortige Vernichtung schutzwürdige Interessen der Petentin im Sinne des § 84 SGB X verletzt werden könnten. Sie hat weiterhin veranlaßt, daß ein anderer, mit Billigung der Versicherten eingeschalteter Gutachter dieses Gutachten nicht zur Kenntnis erhielt und zugesichert, daß das Gutachten für die noch ausstehende Verwaltungsentscheidung nicht berücksichtigt werde.

Da die Petentin inzwischen ein Exemplar des Gutachtens erhalten hat, sind sämtliche bei der BAfU vorhandenen Reststücke gem. § 84 Abs. 2 SGB X zu vernichten, weil dessen Speicherung wegen Verstoßes gegen § 76 Abs. 2 SGB X unzulässig war.

Mit Rücksicht darauf, daß die BAfU sowohl im vorliegenden Eingabefall, als auch im Zusammenhang mit der daraufhin durchgeführten Kontrolle (vgl. 14.2) meinen Empfehlungen ganz bzw. weitgehend entsprochen hat, habe ich auf eine förmliche Beanstandung gem. § 25 Abs. 2 BDSG verzichtet.

10.8.3 BfA und BA zeigen beispielhafte Lösungswege auf

Für die datenschutzrechtlichen Probleme, die dann entstehen, wenn der Versicherte nur zu Beginn des Verwaltungsverfahrens allgemein auf sein Widerspruchsrecht hingewiesen wird, hat die BfA folgende vorbildliche Lösungen gefunden und bereits weitgehend umgesetzt:

Im Reha-Verfahren wird der Versicherte bereits auf dem Vordruck des Reha-Antrags über seine Widerspruchsrechte nach Maßgabe des § 76 Abs. 2 Nr. 1 SGB X hingewiesen. Probleme in diesem Zusammenhang umgeht die BfA damit, daß sie es jedem Versicherten überläßt, sich einen Arzt seiner Wahl aus entsprechenden Arztlisten der jeweiligen Fachrichtung selbst auszusuchen, die bei den Rentenversicherungsträgern und Krankenkassen vorgehalten werden.

In Rentenfällen weist die BfA auf dem Antragsvordruck ebenfalls auf das Widerspruchsrecht gemäß § 76 Abs. 2 Nr. 1 SGB X hin. Darüber hinaus wird jedem Versicherten ein Merkblatt mit Erläuterungen zum Antrag ausgehändigt. Dieses Merkblatt wird anläßlich der nächsten Auflage um den Hinweis ergänzt werden, daß der Versicherte Namen und Anschriften derjenigen Ärzte benennen kann, von denen er nicht untersucht werden will bzw. denen keine medizinischen Unterlagen übermittelt werden sollen. Die BfA wird diese Angaben der Versicherten

als Widerspruch im Sinne von § 76 Abs. 2 SGB X – bezogen auf den benannten Arzt – behandeln.

Beide Lösungen begrüße ich ausdrücklich.

Ein weiteres Problem hat die BfA im Zusammenhang mit der Anwendung des § 76 Abs. 2 Nr. 1 SGB X in datenschutzrechtlich vorbildlicher Weise gelöst, das auch im Verwaltungsverfahren aller übrigen Sozialleistungsträger entstehen kann: So weist sie in den Antragsvordrucken ihre Versicherten darauf hin, daß ihre Krankenkasse der BfA die Arbeitsunfähigkeitszeiten und die dazugehörigen Diagnosen einschließlich der Angaben zu Krankenhaus- bzw. Rehabilitationsaufenthalten der letzten drei Jahre übermittelt, die Versicherten dieser Übermittlung jedoch gegenüber ihrer Krankenkasse widersprechen können (siehe hierzu Nr. 13.3.7, Hinweis aus dem Reha-Antrag).

Die BfA begründet diese Praxis zu Recht damit, daß bei den Krankenkassen durch das Übermittlungsersuchen der BfA gegenüber deren Versicherten kein Verwaltungsverfahren und damit auch keine Hinweispflicht nach § 76 Abs. 2 Nr. 1 SGB X ausgelöst werde. Daher sehe sich die BfA nach dieser Vorschrift als verpflichtet an, die Versicherten auf ihr Widerspruchsrecht gegenüber ihrer Krankenkasse hinzuweisen. Erst dann, wenn aufgrund dieses Hinweises ein Widerspruch des Versicherten nicht erfolge, dürfe die Krankenkasse die von der BfA erbetene Übermittlung zulässigerweise vornehmen. Dasselbe gilt entsprechend für die Erhebung dieser Daten durch die BfA: Erst wenn der auf sein Widerspruchsrecht gegenüber der Krankenkasse hingewiesene Versicherte von diesem keinen Gebrauch gemacht hat, kann die erhebende Stelle davon ausgehen, daß der Erhebung überwiegende schutzwürdige Interessen des Versicherten im Sinne des § 67 a Abs. 2 Satz 2 Nr. 1 SGB X nicht entgegenstehen und diese damit im Regelfall zulässig ist.

Auch die BA praktiziert ein entsprechendes Verfahren: Sie übermittelt auf Anforderung eines anderen Leistungsträgers medizinische Daten im Sinne des § 76 SGB X nur, wenn der anfordernde Leistungsträger darlegt, daß er den Versicherten auf sein Widerspruchsrecht gegenüber der BA hingewiesen oder – darüber hinaus – der Versicherte die BA von der ärztlichen Schweigepflicht befreit hat. Im letzteren Fall besteht die BA auf der Vorlage der schriftlichen Befreiungserklärung.

Ich empfehle allen Sozialleistungsträgern nachdrücklich, die vorbildliche Praxis der BfA und der BA zu übernehmen.

10.9 Sozialdatenschutz im gerichtlichen Verfahren

Im Berichtszeitraum war ich mehrmals mit der Frage befaßt, in welchem Umfang personenbezogene Daten von den Sozialversicherungsträgern an Gerichte weitergegeben werden dürfen. Dabei ging es um die Datenweitergabe an Sozialgerichte und an Familiengerichte.

10.9.1 Datenweitergabe an Sozialgerichte

Bereits in meinem 14. Tätigkeitsbericht habe ich unter Nr. 10.4.2 dargelegt, daß ich aus datenschutzrechtlicher Sicht im Falle einer Aktenanforderung durch ein Gericht eine Rückfrage bei dem Gericht für die Fälle empfehle, in denen aus der Anforderung erkennbar wird, daß es dem Gericht nur auf bestimmte konkrete Teilfragen ankommt, die durch Vorlage von Teilen der Akte beantwortet werden können.

Die BfA hat daraufhin betont, daß die Gerichte dann nur Aktenteile (z. B. Versicherungsverläufe, Rentenbescheide oder Versicherungsnachweise) erhalten, wenn nur solche Aktenteile von ihnen verlangt werden. Es ist mir bewußt, daß ein solcher Fall in der Praxis aber kaum vorkommen wird. Aktenanforderungen der Sozialgerichte ergehen vielmehr regelmäßig ohne jegliche Einschränkungen oder Hinweise, die erkennen ließen, daß die Vorlagen von Teilen der Akte für die Entscheidung des Streitfalles ausreichend sein könnten. Dies sei – so die BfA – im Hinblick auf den Amtsermittlungsgrundsatz des sozialgerichtlichen Verfahrens auch verständlich, denn eine mangelhafte Sachaufklärung bzw. eine Verletzung des § 103 SGG durch die Gerichte wäre ein wesentlicher Verfahrensmangel.

Die BfA hat des weiteren erklärt, daß „selbständige" Akten, z. B. Akten der Abteilung für Rehabilitation, die einem streitbefangenen Rentenvorgang beiliegen, dem Gericht nicht mit übersandt werden, da sie erkennbar mit dem Rentenverfahren nicht im Zusammenhang stehen.

Ich kann die geschilderte Praxis der BfA akzeptieren.

10.9.2 Datenweitergabe an Familiengerichte

Im Rahmen eines Versorgungsausgleichsverfahrens hatte die BfA dem Familiengericht eine Ablichtung eines Rentenbescheides mit einem Begleitschreiben übersandt. In diesem Begleitschreiben wurde ausgehend von dem Rentenbescheid die Berechnung des Ehezeitanteils der Altersrente dargestellt.

Gegen diese Vorgehensweise wandte sich ein Petent an mich, da er der BfA ausdrücklich untersagt hatte, jegliche Daten außerhalb der Ehezeit dritten Stellen bekanntzugeben. Diese Einschränkung hatte die BfA nicht beachtet, indem sie dem Familiengericht auch personenbezogene Daten, die nicht die Ehezeit betrafen, weitergegeben hatte.

Die Vorgehensweise der BfA verstößt nicht gegen das Sozialgeheimnis.

Das Familiengericht hat bei der BfA um Erteilung einer Auskunft über die nach § 1587 a BGB auszugleichende Versorgung gebeten. Nach dieser Vorschrift ist der Ehegatte mit den werthöheren Rentenanwartschaften oder Aussichten auf eine auszugleichende Versorgung dem anderen Ehegatten gegenüber ausgleichspflichtig.

Die BfA hat nach § 53 b Abs. 2 FGG gegenüber dem Familiengericht sowohl Auskunft über Grund wie auch über die Höhe der Versorgungsanwartschaft der einzelnen Ehegatten zu geben. Es handelt sich dabei um ein Beweismittel, das der Richter auf seine

Richtigkeit zu überprüfen hat. § 74 Nr. 1b SGB X normiert für diesen Fall eine gesetzliche Offenbarungsbefugnis für Sozialdaten.

Es reicht nicht aus, dem Familiengericht nur die ehezeitbezogenen Daten zur Verfügung zu stellen, sondern es ist auch die Übermittlung der darüber hinausgehenden erforderlich. Eine Berechnung der auf die Ehezeit entfallenden Rentenanwartschaften allein aus der während der Ehe zurückgelegten Zeiten ist nicht möglich; beispielsweise nicht bei der Bestimmung der Werteinheiten für beitragslose Zeiten oder bei der Berücksichtigung von sogenannten Anrechnungszeiten.

Darüber hinaus wandte sich der Petent dagegen, daß die BfA den gesamten Rentenbescheid dem Familiengericht überlassen hatte.

Es gibt mehrere Gründe, die dies rechtfertigen. Ich möchte hier nur beispielhaft auf § 1587c BGB hinweisen. Nach dieser Vorschrift findet ein Versorgungsausgleich in bestimmten Fällen nicht statt, beispielsweise soweit die Inanspruchnahme des Ausgleichsverpflichteten unter Berücksichtigung der beiderseitigen Vermögensverhältnisse der Ehegatten grob unbillig wäre. Darüber hinaus sind die Vorschriften des Versorgungsausgleichshärteregelungsgesetzes zu beachten, wonach ein unverfallbares, dem schuldrechtlichen Versorgungsausgleich unterliegendes Anrecht – z. B. durch vor der Ehe erworbene Rentenanwartschaften – ausgeglichen werden kann.

Allerdings hätte die BfA dem Petenten eine ordnungsgemäße Erklärung für ihre Verfahrensweise geben sollen, insbesondere da er einer Weitergabe ausdrücklich widersprochen hatte (§§ 13, 14 SGB I). Dieses Versäumnis wurde seitens der BfA auch eingeräumt und bedauert.

11 Arbeitsverwaltung

11.1 Kontrollen von Arbeitsämtern

Im Laufe des Berichtszeitraumes habe ich, teilweise aufgrund von Bürgereingaben, datenschutzrechtliche Kontrollen gem. § 24 BDSG bei fünf Arbeitsämtern durchgeführt.

In zwei Fällen führten die Kontrollen zu einer förmlichen Beanstandung gem. § 25 Abs. 1 BDSG. Bei den beiden betroffenen Arbeitsämtern habe ich gegenüber dem Vorstand der BA Verstöße gegen die in § 24 Abs. 4 BDSG normierte Mitwirkungs- und Unterstützungspflicht des BfD beanstandet.

In einem dieser Fälle war mit einem Petenten ein sog. „Teamgespräch", in das er eingewilligt hatte, in Anwesenheit des Arbeitsamtspsychologen geführt worden. Der Petent hatte mehrfach, u. a. auch in Schreiben an das Landesarbeitsamt und das Arbeitsamt vergeblich vollständige Einsicht in die Unterlagen des Arbeitsamtes über dieses Gespräch und seine Auswertung beantragt und sich dann an mich gewandt.

Zu der Vermutung des Petenten, daß es aufgrund dieses Gespräches und der hierbei erfolgten Datenerhebung zu einem vom Psychologen verfaßten Bericht gekommen sei, hat mir die BA in ihren schriftlichen Stellungnahmen, die anschließend Grundlage meiner datenschutzrechtlichen Bewertung gegenüber dem Petenten waren, mitgeteilt, ein solches Protokoll sei tatsächlich vom Psychologischen Dienst nicht erstellt worden. Dem Petenten sei in alle zu dem Gespräch vorhandenen Aufzeichnungen Einsicht gewährt worden.

Nicht zuletzt aufgrund der beharrlichen Nachforschungen des Petenten habe ich dann den Sachverhalt im Rahmen einer datenschutzrechtlichen Kontrolle vor Ort geprüft.

In dem von mir mit dem zuständigen Arbeitsamtspsychologen geführten Gespräch stellte sich – entgegen der Aussage der BA – heraus, daß sich der Psychologe während des Gesprächs sehr wohl Aufzeichnungen hierüber auf dem amtlichen Vordruck „Befundbogen", der im übrigen weitere personenbezogene Vermerke über den Petenten enthält, gemacht hat. Die Existenz dieser Aufzeichnung des Psychologen auf dem „Befundbogen" wurde bis zu meiner Datenschutzkontrolle – trotz meiner mehrfachen Anfrage – von der BA sowohl gegenüber dem Petenten als auch gegenüber mir bestritten.

Aufgrund der während der Kontrolle getroffenen Feststellungen war deshalb auch die Aussage der BA, dem Petenten sei in alle zu dem in Rede stehenden Gespräch vorhandenen Aufzeichnungen Einsicht gewährt worden, falsch.

Ich habe gegenüber dem Vorstand der BA zum Ausdruck gebracht, daß die Tatsache, daß die BA in ihren Stellungnahmen die Existenz einer Niederschrift oder eines Protokolls verneint bzw. in ihren Stellungnahmen mir gegenüber keinerlei Angaben darüber gemacht hat, daß handschriftliche Aufzeichnungen des Psychologen auf dem „Befundbogen" existieren, eine Verletzung der durch § 24 Abs. 4 Nr. 1 BDSG begründeten Pflicht, mir Auskunft zu meinen Fragen zu gewähren, darstellt. Dies trifft ebenfalls auf die Aussage der BA zur erfolgten Akteneinsicht zu.

Da die nicht korrekten Aussagen der BA mir gegenüber, trotz des erneuten Vorbringens des Petenten, wiederholt wurden und die schriftlichen Stellungnahmen der BA zu meiner nicht sachgerechten datenschutzrechtlichen Bewertung gegenüber dem Petenten geführt hatten, habe ich dies gem. § 25 Abs. 1 BDSG als Verstoß gegen § 24 Abs. 4 Nr. 1 BDSG förmlich beanstandet.

Ich habe den Vorstand darüber hinaus gebeten, in geeigneter Weise darauf hinzuwirken, mir in künftigen Fällen die notwendigen Auskünfte vollständig zu geben.

Ferner habe ich gebeten, den Petenten über die Existenz der Aufzeichnungen zu dem Teamgespräch zu unterrichten und ihm vollständige Akteneinsicht zu gewähren.

In seiner Stellungnahme hat der Vorstand der BA meine Beanstandung anerkannt und – für mich nach-

vollziehbar – betont, daß die Nichtbenennung der Unterlagen auf ein Mißverständnis zurückzuführen sei. Die Beanstandung sei darüber hinaus Anlaß gewesen, den Sachverhalt im Rahmen einer Dienstbesprechung mit den Leitenden Psychologen zu erörtern und diese in Form einer Weisung zu erinnern, daß in den Befundbogen immer Einsicht zu geben ist, unabhängig davon, welchen Status die Aufzeichnungen auf dem Befundbogen, bezogen auf die Fallbearbeitung, haben (zur Thematik „Akteneinsicht" vgl. auch Nr. 10.3).

11.2 Beratungsvermerke in der computerunterstützten Arbeitsvermittlung
Arbeitsamt löscht unzulässige Eintragungen während meiner Kontrolle in „vorauseilendem Gehorsam"

In mehreren Fällen war die Speicherung von Beratungsvermerken im von der Bundesanstalt für Arbeit (BA) genutzten Verfahren der computerunterstützten Arbeitsvermittlung – coArb – Gegenstand von Bürgereingaben. Hierbei ging es insbesondere um konkrete, teilweise für die Aufgabenerfüllung nicht erforderliche Eintragungen oder um Eintragungen mit negativen oder subjektiven Inhalten.

In meinem 13. TB (S. 63ff.) sowie 14. TB (S. 85f.) hatte ich dargelegt, daß die Erhebung und Speicherung personenbezogener Daten für die Arbeitsvermittlung und -beratung in einem bundesweit geltenden Runderlaß der BA grundsätzlich datenschutzgerecht geregelt sind. Danach dürfen Arbeit- und Ratsuchende weder negativ gekennzeichnet noch subjektive Eindrücke und Bewertungen in den Beratungsvermerken aufgenommen werden.

Meine Prüfung der Eintragungen führte insgesamt gesehen zu einem positiven Ergebnis. Daher halte ich die Weisungslage zu Form und Inhalt individueller Beratungsvermerke für ausreichend. In Einzelfällen traten allerdings Probleme bei der Umsetzung dieser Regelungen auf:

- Im Vordergrund meiner Kontrolle stand u. a. die Beschwerde eines Petenten über coArb-Eintragungen, die er als diskriminierend empfand. Entgegen der für den Petenten bestehenden Vermittlungszuständigkeit einer Nebenstelle des Arbeitsamts ergab sich, daß der Petent im Fachvermittlungsdienst für besonders qualifizierte Bewerber in der Hauptstelle geführt wurde. In der Nebenstelle waren im coArb geführten Bewerberangebot des Petenten folgende Eintragungen enthalten:
  - „ . . . (wirkte lt. Frau M., schon sehr schwierig – da er stets alles am liebsten schriftlich hätte . . .)"
  - „220493: wirkt leicht „hochmütig" – u. wolle schon w.g. U-Antr. lt. Frau M. nicht kommen . . ."
  - „Herrn . . . entspr. informiert u. gebeten, 1 Wo vorher pers. U-Antrag zu stellen (wird er nunmehr – schweren Herzens trotz Zeitaufw. tun)"

  Daraufhin wurde eine Kontrolle der im Fachvermittlungsdienst der Hauptstelle über den Petenten geführten coArb-Vermerke für den übernächsten Tag angekündigt. Bei dieser Kontrolle ergab sich, daß die zitierten Bemerkungen in coArb mit Ausnahme der letztgenannten nicht mehr vorhanden waren. Das Bewerberangebot des Petenten war inzwischen kurz nach der angekündigten Kontrolle bereinigt worden, um den rechtmäßigen Zustand wiederherzustellen. Weiterhin wurde erklärt, auf Veranlassung des Vorgesetzten sei darüber hinaus das gesamte von dem für den Petenten zuständigen Vermittler bearbeitete Bewerberangebot auf eventuelle Verstöße gegen den einschlägigen Runderlaß der Bundesanstalt überprüft und, soweit erforderlich, bereinigt worden.

  Von einer förmlichen Beanstandung der übereinstimmend als nicht erforderlich und damit unzulässig bewerteten coArb-Vermerke hätte ich möglicherweise absehen können, wenn das Arbeitsamt diese Bemerkung unmittelbar nach Durchführung der Kontrolle gelöscht hätte. Die – in „vorauseilendem Gehorsam" durchgeführte – Löschungsaktion hat es mir dagegen unmöglich gemacht, die Kontrolle wie vorgesehen und angekündigt durchzuführen und auf weitere Stichproben im Bewerberangebot des Fachvermittlungsdienstes auszudehnen.

  Ich habe das dargestellte Verhalten des Arbeitsamtes als gravierenden Verstoß gegen die in § 24 Abs. 4 BDSG normierte Mitwirkungs- und Unterstützungspflicht bewertet. Danach ist mir und meinen Beauftragten bei der Durchführung von Kontrollen insbesondere Einsicht in die gespeicherten Daten und in die Datenverarbeitungsprogramme zu gewähren. Ich habe diesen Verstoß gemäß § 25 Abs. 1 BDSG beanstandet.

- Ein schwerbehinderter Arbeitsloser beschwerte sich über folgende coArb-Eintragungen:
  - „Hirndauerschädigung durch Anfallsleiden"
  - „Äußeres angesprochen (sehr ungepflegt, ihm ist bekannt, daß gerade im grafischen Bereich „KL-Typen" rumlaufen! Meint selbst, daß Äußeres Probleme bereiten könnte, dafür sei er aber grundehrlich!"
  - „Ersch. 12.40 Uhr, hatte 1. E. zu 9.00 Uhr, mußte Kinder betreuen, da Ehefrau zur Bank mußte"
  - „Aufgrund des Verhaltens erhebliche Probleme, Praktikumsplatz für ihn zu finden"
  - „Weitere Teilnahme im o. a. Rahmen möglich, da für ihn aufgrund seines Äußeren und des Auftretens keine anderen Verm.-mögl. bestehen".

  Ich habe diese Eintragungen auch unter dem Gesichtspunkt problematisiert, daß Schwerbehinderte – inzwischen aufgrund ausdrücklicher Verfassungsbestimmung – im besonderem Maße vor Diskriminierung geschützt werden müssen. Es erscheint mir zwar nachvollziehbar, daß sowohl das äußere Erscheinungsbild, als auch Gesichtspunkte der Körperpflege für die Tätigkeit in dem vom Petenten selbst angestrebten Berufsfeld grundsätzlich vermittlungsrelevant sind und dies auch für schwerbehinderte Arbeitsuchende gilt. Entsprechende Vermittlungsvermerke, die Defizite hin-

sichtlich dieser Vermittlungskriterien kennzeichnen, können daher auch im Falle des schwerbehinderten Petenten zulässig sein, falls sie deren vermittlungsrelevanten Kern in objektivierter Formulierung wiedergeben. Dies war jedoch bei den vorgenannten Eintragungen nicht der Fall.

Die Bundesanstalt für Arbeit wies daher das Arbeitsamt an, die vorstehenden Vermittlungsvermerke zu löschen bzw. neu zu formulieren.

- Über eine Arbeitslose war vermerkt:

  „Ist nervlich sehr stark angespannt, fängt leicht an zu weinen. Dies sollte bei künftigen Gesprächen beachtet werden."

  Vom Arbeitsamt wurde bestätigt, daß dieser Vermerk nicht vermittlungsrelevant, sondern vielmehr als Hinweis für zukünftige Beratungen und Gespräche gedacht sei, um die Angaben dort berücksichtigen zu können. Da nicht auszuschließen war, daß die im Vermerk getroffenen Aussagen über den „Gemütszustand" der Arbeitslosen von anderen Mitarbeitern der Arbeitsverwaltung unzulässigerweise im Rahmen von Vermittlungsbemühungen berücksichtigt werden könnten, habe ich dessen Löschung gefordert. Hierbei war auch von Bedeutung, daß die nicht (ggf. durch ein psychologisches Gutachten) belegte Aussage „nervlich sehr angespannt" wenig präzise ist und damit unterschiedlich ausgelegt werden könnte.

  Die BA teilte meine Beurteilung des Vermerkes und veranlaßte dessen Löschung.

- Ein Petent hatte sich u. a. wegen folgenden Vermerks an mich gewandt:

  „In sehr überheblicher und unangenehmer Weise machte er deutlich, daß er weder an einer Beratung noch an einer Vermittlung des Arbeitsamtes interessiert sei . . ."

  Ich habe diese Eintragung als unzulässig bewertet, weil ihr Inhalt für die Vermittlung des Betroffenen nicht erforderlich war. Im Rahmen einer unangekündigten Kontrolle im Arbeitsamt konnte ich mich dann davon überzeugen, daß der Vermerk – wie von der BA zugesagt – im System gelöscht worden war.

  Des weiteren hatte der Petent mir gegenüber vorgetragen, daß zunächst in seinen Vermittlungsunterlagen vorhandene, aus seiner Sicht für ihn günstige Daten seitens des Arbeitsamtes gelöscht worden seien. Nach Aussagen der BA wurde die Löschung seinerzeit vorgenommen, weil man die Daten als für die Vermittlung nicht erforderlich angesehen habe. Die in Frage stehenden Daten wurden vom Arbeitsamt – auch hiervon habe ich mich vor Ort überzeugen können – wieder in das coArb-System aufgenommen.

- In einem anderen Arbeitsamt war folgender Beratungsvermerk gespeichert:

  „. . ., beschwert sich über Alles und Jeden."

  Das Beschwerderecht ist ein grundsätzliches Bürgerrecht. Darüber hinaus sollten – insbesondere bei Langzeitarbeitslosen stets – die möglichen Auswirkungen der Arbeitslosigkeit auf deren psychische Situation berücksichtigt werden. Ich habe insofern die Löschung des Eintrags gefordert.

  Die BA hat den Vermerk gelöscht und eingeräumt, daß das Beschwerdeverhalten eines Arbeitslosen grundsätzlich nicht vermittlungsrelevant und daher nicht in coArb aufzunehmen ist. Sie wird hierauf in ihren Arbeitsanweisungen ausdrücklich hinweisen.

11.3 Ärztlicher Dienst der Bundesanstalt für Arbeit

In meinem 14. Tätigkeitsbericht (Seite 87 f.) hatte ich berichtet, daß der Umgang mit Gutachten, die vom Ärztlichen Dienst der BA oder in dessen Auftrag erstellt werden, datenschutzgerechter gestaltet wurde.

Darüber hinaus hat die BA inzwischen das Verfahren der Begutachtung von **Beschäftigten** in einem bundesweiten Runderlaß datenschutzgerecht geregelt. Dem lagen meine Empfehlungen im Hinblick auf einen Einzelfall zugrunde (s. 14. TB S. 73 f.). Der neue Runderlaß gibt Hinweise, u. a. zur Einholung von Auskünften und ärztlichen Unterlagen bei behandelnden Ärzten, zur Nachprüfung bescheinigter Arbeitsunfähigkeit von Beschäftigten, zur Unterrichtung des Beschäftigen über Gutachten nach Aktenlage sowie zum Verhalten bei Sperrvermerken von BA-externen Ärzten in ärztlichen Unterlagen.

Mit Vertretern der BA habe ich die Thematik „Datenschutz im Ärztlichen Dienst" erörtert. Dem Sachstandsbericht der BA habe ich entnommen, daß im Rahmen der regelmäßigen Fortbildungsveranstaltungen und Dienstbesprechungen des ärztlichen und nicht-ärztlichen Personals der BA Fragen des Datenschutzes behandelt werden.

Um den Unsicherheiten in der Umsetzung von Weisungen bei der Zahl von rd. 1 200 Vertragsärzten entgegenzuwirken, gibt die BA den Vertragsärzten schriftliche Informationen auch im Hinblick auf datenschutzrechtliche Themen; etwa zur Formulierung arbeitsamtsärztlicher Gutachten, Entbindung von der ärztlichen Schweigepflicht, Offenbarungsbefugnis durch den Ärztlichen Dienst, Verwertung von Vertragsarztgutachten oder zum Gutachten nach Aktenlage.

Die BA hat eingeräumt, daß trotz aller Bemühungen Fehler in der Begutachtung und den damit verbundenen Verwaltungsfragen – hierzu gehört auch der Datenschutz – auftreten können. Sie hat mir mitgeteilt, aus diesem Grunde würden derzeit Grundlagen für eine Qualitätssicherung in der Begutachtung (und m.E. damit verbunden auch im Hinblick auf die datenschutzrechtlichen Fragen) unter Berücksichtigung der vorhandenen Möglichkeiten erarbeitet werden.

Ich bin grundsätzlich der Auffassung, daß das System des Ärztlichen Dienstes der Bundesanstalt für Arbeit sowie die diesbezüglichen Regelungen der BA insgesamt datenschutzrechtlichen Anforderungen genügen. In Einzelpunkten, insbesondere im Bereich der Inanspruchnahme von Vertragsärzten durch die BA, sind aber dennoch datenschutzrechtliche Verbesserungen notwendig.

11.4 Datenschutz und Maßnahmeträger

Im 14. Tätigkeitsbericht (S. 88) hatte ich über datenschutzrechtliche Probleme im Zusammenhang mit den von der BA bei der Umschulung und Fortbildung von Arbeitslosen eingeschalteten freien oder gemeinnützigen Einrichtungen berichtet (sog. Maßnahmeträger). Ich hatte als notwendig unterstrichen, die Einhaltung bestehender datenschutzrechtlicher Bestimmungen durch Maßnahmeträger generell besser sicherzustellen.

Leider wurden meine entsprechenden Empfehlungen im 2. Änderungsgesetz zum Sozialgesetzbuch nicht verwirklicht.

Die im Rahmen von Kontrollen im Berichtszeitraum hierzu getroffenen Feststellungen sowie die zahlreichen Eingaben zu dieser Thematik verdeutlichen die Notwendigkeit datenschutzrechtlicher Verbesserungen in diesem Bereich.

In Gesprächen mit Vertretern der BA habe ich den „Datenschutz im Bereich der beruflichen Rehabilitation und der beruflichen Fortbildung und Umschulung" ausführlich diskutiert. Ich habe auch dort vorgetragen, daß ich weiterhin Bedenken im Hinblick auf die Einhaltung des Datenschutzes bei den Maßnahmeträgern habe.

Ich habe darüber hinaus gefordert, daß die BA Datenschutzverstöße eines Maßnahmeträgers an die zuständige Aufsichtsbehörde weiterleitet und unter Berücksichtigung der Umstände im Einzelfall, insbesondere des Verhältnismäßigkeitsgrundsatzes, prüft, ob eine weitere Zusammenarbeit mit den Maßnahmeträgern möglich ist.

Bedauerlicherweise ist die BA bisher mit der von mir als erforderlich angesehenen Weiterleitung von Verstößen an die zuständige Aufsichtsbehörde nicht einverstanden. Sie hat sich jedoch bereit erklärt, Maßnahmeteilnehmer an die jeweils zuständige Aufsichtsbehörde zu verweisen, wenn von diesen Anzeigen wegen Datenschutzverletzungen geltend gemacht werden. Darüber hinaus will die BA noch weitergehende Möglichkeiten prüfen. So strebt sie insbesondere noch eine konkretere Formulierung der Datenschutzklausel in den Verträgen mit den Maßnahmeträgern an. Darin sollen Sanktionen, vor allem wirtschaftlicher Art, bei Verstößen gegen Datenschutzbestimmungen angekündigt werden. Die BA will jedoch künftig die weitere Zusammenarbeit mit Maßnahmeträgern überprüfen, wenn Datenschutzverstöße vorliegen und bei entsprechenden Anzeigen von Maßnahmeteilnehmern diese an die jeweils zuständige Aufsichtsbehörde verweisen.

11.4.1 Unzulässig gespeicherte Daten weitergegeben

In meinem 14. Tätigkeitsbericht (S. 88) hatte ich über von Maßnahmeträgern über die einzelnen Teilnehmer erstellte Abschlußberichte mit diskriminierenden Ausführungen berichtet. Die Aufbewahrung dieser Unterlagen in den Maßnahmeakten des zuständigen Arbeitsamtes hatte ich als unzulässige Datenspeicherung beanstandet.

Die BA hat mir hierzu mitgeteilt, die Abschlußberichte über Teilnehmer/innen an den in Rede stehenden Maßnahmen seien im Arbeitsamt sowie im Landesarbeitsamt vor Ablauf des Jahres 1992 ausnahmslos vernichtet worden. Dennoch haben sich auch im Berichtszeitraum weitere Teilnehmer dieser Maßnahmen mit datenschutzrechtlichen Eingaben an mich gewandt. So hat mir ein Petent Bewerbungsunterlagen überlassen, wie sie vom Arbeitsamt 1994 an einen Arbeitgeber und von diesem versehentlich an den Petenten (statt an das Arbeitsamt) zurückgesandt worden seien.

In diesen Unterlagen befand sich auch ein Abschlußbericht (mit umstrittenen psychologischen Wertungen über den Petenten) des Maßnahmeträgers, über den ich bereits in meinem 14. Tätigkeitsbericht berichtet hatte. Die BA hat nach meiner Einschaltung unmittelbar eine Prüfung des Arbeitsamtes durch das fachaufsichtlich zuständige Landesarbeitsamt eingeleitet. Nach dessen Prüfung befinden sich in den in der Abteilung Arbeitsvermittlung und Arbeitsberatung geführten Maßnahmeakten und Bewerbungsunterlagen keine psychologischen Begutachtungen oder ähnliche datenschutzrechtlich bedenkliche Dossiers von Bildungsträgern über Maßnahmeteilnehmer. Es wurde mir in diesem Zusammenhang nochmals bestätigt, daß im Jahre 1992 noch vorhandene Abschlußberichte der betroffenen Maßnahmeträger vernichtet worden seien.

Die BA hat eingeräumt, daß ein Arbeitsvermittler dem Arbeitgeber Bewerbungsunterlagen des Petenten ausgehändigt habe, die das in Frage stehende „Gutachten" enthielten. Warum zu einem späteren Zeitpunkt, d. h. nach der Vernichtung, ein weiteres „Gutachten" über den Petenten Verwendung finden konnte, ist auch dem prüfenden Landesarbeitsamt – so die BA – nicht mehr nachvollziehbar. Der Arbeitsvermittler habe offensichtlich die von dem Petenten selbst zusammengestellten Bewerbungsunterlagen nicht auf deren Vollständigkeit und Erforderlichkeit hin durchgesehen.

Wegen weiterer Eingaben in diesem Zusammenhang ist mir eine abschließende Bewertung dieser Angelegenheit noch nicht möglich.

11.4.2 Nachweis der Qualifikation der Mitarbeiter von Maßnahmeträgern

Im Berichtszeitraum haben sich mehrmals Mitarbeiter von Maßnahmeträgern, die Umschulungs- und Fortbildungsmaßnahmen für die BA und in deren Auftrag durchführen, an mich gewandt. Sie haben sich besorgt darüber geäußert, daß ihre Arbeitgeber in großem Umfange personenbezogene Daten von ihnen an die BA übermitteln.

Um Informationen über die einzelnen Lehrkräfte bei den Maßnahmeträgern zu erhalten, verwendet die BA einen sog. Erhebungsbogen über berufliche Bildungsmaßnahmen. Dieser Bogen verstößt nicht gegen Datenschutzrecht. Die BA ist – nicht zuletzt im Interesse der Effizienz der Maßnahmen und der Beachtung des Grundsatzes der wirtschaftlichen Verwendung von Haushaltsmitteln – darauf angewiesen, bestimmte Informationen über die Qualifikation der

Lehrkräfte und damit ihre Eignung für die einzelnen Maßnahmen zu erhalten.

Die BA hat zwischenzeitlich in einem neuen Runderlaß über die individuelle Förderung der beruflichen Fortbildung und Umschulung auch diesen Erhebungsbogen überarbeitet. Meine Empfehlungen hierzu wurden berücksichtigt.

Neben diesem Erhebungsbogen habe ich bei der Kontrolle in einigen Maßnahmeträgerakten ausführliche Lebensläufe der einzelnen Lehrkräfte gefunden. Teilweise wurde so verfahren, daß in den Erhebungsbögen bei den einzelnen Fragen nur „siehe Lebenslauf" stand und jeweils auf diesen verwiesen wurde. Des weiteren fanden sich in den Maßnahmeträgerakten teilweise Kopien von Zeugnissen der Lehrkräfte.

Hinsichtlich der Lebensläufe waren die Daten des Erhebungsbogens für die Aufgabenerfüllung der BA ausreichend und die Lebensläufe damit entbehrlich. Die Kopien der Zeugnisse in den Maßnahmeträgerakten sind für die dargestellten Ziele der BA nicht erforderlich. Ich habe vorgeschlagen – sofern in Einzelfällen die Vorlage eines Zeugnisses zum Nachweis der Qualifikation der Lehrkraft notwendig ist – nach Vorlage derselben einen entsprechenden Vermerk in die Akte aufzunehmen, darin jedoch auf die inhaltliche Wiedergabe des Zeugnisses zu verzichten.

Die BA hat bestätigt, daß die vorgefundenen Lebensläufe oder Kopien von Zeugnissen der Lehrkräfte mit dem geltenden Runderlaß nicht im Einklang standen. In diesem hat die BA, einer früheren Anregung von mir folgend, den Dienststellen bereits entsprechende datenschutzgerechte Weisungen erteilt. Sie hat die Vernichtung der in Einzelfällen vorgefundenen Unterlagen veranlaßt und die zuständigen Mitarbeiter erneut über die Weisungslage informiert und um künftige Beachtung gebeten.

11.5 Führung und Nutzung einer Historikdatei bei der Bundesanstalt für Arbeit

Ein Beispiel für das Spannungsfeld zwischen möglichst unbegrenzten Forschungsmöglichkeiten einerseits und datenschutzrechtlichen Belangen Betroffener andererseits stellt die bei der BA geführte Historikdatei als Forschungsdatei des Institutes für Arbeitsmarkt- und Berufsforschung (IAB) dar. Hiermit war ich während des Berichtszeitraumes mehrfach befaßt.

Diese Datei enthält für die Zeit ab 1974 (vollständig ab 1976) pro Kalenderjahr und sozialversicherungspflichtigem Arbeitnehmer der alten Bundesländer einen Datensatz mit personenbezogenen Daten über Versicherungsnummer, Geburtsdatum, Schul-/Berufsausbildung, Stellung im Beruf, Berufskennziffer des ausgeübten Berufs, Beginn und Ende der Beschäftigung, Staatsangehörigkeit, sozialversicherungspflichtiges Einkommen, Geschlecht, Familienstand sowie die Betriebsnummer des Beschäftigungsbetriebes.

Die Historikdatei umfaßt mittlerweile ca. 800 Mio. Datensätze, die auf Magnetband bei der BA abgelegt sind. Zu ihrem Aufbau verwendet die BA die bei ihr geführte Versichertendatei, welche aus einer „laufenden Datei" und einer „Archivdatei" besteht. Aus der „laufenden Datei" wird zu den jeweiligen Stichtagen der Bestand an sozialversicherungspflichtigen Beschäftigten ermittelt. Bei den Versicherungsfällen, bei denen nach frühestens 2 Jahren weitere Meldungen vorliegen, werden die vorangegangenen Meldungen und sonstigen Altfälle chronologisch innerhalb eines Meldejahrgangs nach Geburtstagsendziffern sortiert – in der „Archivdatei" abgelegt. Aus diesen beiden Dateien wiederum wird nun die Historikdatei gebildet, in der sämtliche Datensätze einer bestimmten Person nacheinander unter derselben Versicherungsnummer gespeichert sind. Damit stellt die Historikdatei einen äußerst umfangreichen und damit datenschutzrechtlich problematischen Informationsgehalt bereit.

Sicherlich ist – insbesondere im Bereich der Wirtschafts- und Sozialforschung – gerade in Zeiten wachsender Arbeitslosigkeit die statistische Untersuchung des Arbeitsmarktes vonnöten. Dennoch müssen auch solche Untersuchungen im Einklang mit den datenschutzrechtlichen Bestimmungen stehen.

Wie läßt sich diese Problematik entschärfen?

Hierzu muß zunächst bemerkt werden, daß eine Anonymisierung oder Teillöschung der Daten aus Sicht der Forschungstreibenden die Qualität der Daten stark einschränkt. Die in diesem Bereich betriebenen Forschungsvorhaben stellen auf eine langfristige vergleichende Auswertung verschiedener Parameter ab. Nach Auskunft des BMA sei daher beispielsweise eine Löschung der Versicherungsnummer nicht möglich, da man hierdurch gerade die Möglichkeiten vergeben würde, die vorhandenen Daten jeweils um die Daten des laufenden Jahrgangs zu ergänzen. Aber auch eine vollständige Verschlüsselung der Versicherungsnummer als Merkmalsträger sei nach Ansicht des BMA nicht praktikabel. Aufgrund des Umfanges der Historikdatei sei eine hierfür notwendige gesonderte Speicherung der personenbezogenen Merkmale, die mit den Einzelangaben zu Forschungszwecken zusammengeführt werden müßten, nicht möglich, da diese Zusammenführung – bedingt durch Hardwarezugriffe – der Arbeitsleistung eines Großrechners für mehrere Monate entspräche. Als Alternative wurde vom BMA/BA ein Verschlüsselungsprogramm vorgeschlagen, welches die Versicherungsnummer bei der Überführung in die Historikdatei etwas verfremdet. Diese Lösung sei um den Faktor 1000 schneller als die vollständige Verschlüsselung und somit anwendbar. Auch wenn das Verfahren datenschutzrechtlich als eher schwach zu bewerten ist, habe ich ihm aufgrund der Notwendigkeit, für die Ergänzung der Historikdatei die Datensatzreihenfolge beizubehalten, zugestimmt.

Auch das Verfahren der Datenbereitstellung ist durch den enormen Aufwand, bedingt durch den Umfang der Historikdatei, geprägt. So wird einmal jährlich ein Durchlauf gestartet, bei dem einerseits die notwendigen Datenergänzungen durchgeführt, andererseits die von Forschergruppen angeforderten Daten zusammen- und bereitgestellt werden.

Aufgrund der datenschutzrechtlichen Brisanz der Datei habe ich mich in Zusammenarbeit mit dem BMA und der BA um weitere Lösungsvorschläge bemüht. Hierbei bin ich zu der Überzeugung gelangt, daß die Historikdatei aufgrund ihrer Bedeutung für die Arbeitsmarkt- und Berufsforschung aufrecht erhalten werden sollte. Gerade wegen ihrer herausragenden Stellung sehe ich jedoch Handlungsbedarf zur Schaffung einer diese Datei betreffenden gesetzlichen Regelung. Die vorläufige interne Regelung der BA in bezug auf die Handhabung der Historikdatei gestaltet sich in der Weise, daß die Versicherungsnummer ehemaliger Arbeitnehmer mit Vollendung des 75. Lebensjahres endgültig aus der Historikdatei entfernt wird.

Die Magnetbänder, auf denen die Historikdatei gespeichert ist, sind im Zentralamt der BA abgelegt. Die BA hat insgesamt ausreichende technische und organisatorische Maßnahmen zur Gewährleistung der Datensicherheit ergriffen.

Insbesondere wegen der erheblichen Größe dieser Datei (derzeit ca. 800 Mio. Datensätze) sowie der umfassenden und vielfältigen Auswertungsmöglichkeiten (z. B. Erforschung von Erwerbsbiographien und betriebsbezogene Forschung), ist für das Führen und Arbeiten mit ihr eine normenklare Rechtsgrundlage notwendig. Das BMA hat inzwischen die Vorlage eines Entwurfes für eine entsprechende Ergänzung des Arbeitsförderungsgesetzes noch in diesem Jahr angekündigt.

11.6 Bankauskünfte an die Arbeitsverwaltung – Entbindung von der Schweigepflicht

Der Anspruch auf Arbeitslosenhilfe steht nach § 134 Abs. 1 Satz 1 Nr. 3 Arbeitsförderungsgesetz (AFG) nur dem bedürftigen Arbeitslosen zu, der seine laufenden Verpflichtungen also nicht aus eigener finanzieller Kraft oder der Unterstützung Unterhaltspflichtiger bestreiten kann. Bei der Bewertung der Bedürftigkeit sind die Vermögensverhältnisse des Antragstellers zu berücksichtigen. Hierbei stellte sich die Frage, inwiefern es für die Stellen der Arbeitsverwaltung über die Angaben des Antragstellers hinaus erforderlich ist, Daten über die Vermögenssituation des Arbeitslosen von Banken, Sparkassen, Versicherungen etc. direkt zu erheben. Hierbei soll die Überprüfung der Richtigkeit dieser Angaben erfolgen.

Ein Petent, der Arbeitslosenhilfe bezog, hatte eine nicht auf Gewinn orientierte private Hilfsorganisation gegründet. Er wurde vom zuständigen Arbeitsamt, dem die Gründung der Hilforganisation bekannt wurde, aufgefordert, seine Vermögensverhältnisse dezidiert aufzuschlüsseln. Dazu wurde dem Petenten ein Vordruck ausgehändigt, auf dem u. a. eine Aufforderung zur Entbindung der Bank, Sparkasse, Versicherung etc. von der Schweigepflicht aufgeführt war, um dort Datenerhebungen durchführen zu können, die „zur Durchführung des Arbeitsförderungsgesetzes erforderlich sind". Die Nichterteilung dieser Einwilligung hätte nach dem verwendeten Vordruck ggf. die Nichtgewährung der Arbeitslosenhilfe zur Folge gehabt.

Der Petent wandte sich mit der Bitte an mich, die datenschutzrechtliche Zulässigkeit eines derartigen Verfahrens zu überprüfen. Dabei stellte sich heraus, daß der beanstandete Vordruck lediglich von dem zuständigen Arbeitsamt entwickelt und verwendet wurde. Die Hauptstelle der Bundesanstalt für Arbeit wies dieses Arbeitsamt umgehend an, den Vordruck nicht mehr einzusetzen.

Im Einzelfall hat der Arbeitslosenhilfeempfänger nach § 60 Abs. 1 Nr. 1 SGB I auf Verlangen des zuständigen Leistungsträgers der Erteilung der **erforderlichen Auskünfte** durch Dritte jedoch zuzustimmen. Die BA hat mir mitgeteilt, daß im Regelfall bei der Prüfung der Vermögensverhältnisse des Arbeitslosenhilfeantragstellers die bei ihm erhobenen Angaben ausreichend seien. Hierfür werde bundeseinheitlich ein „Zusatzblatt" zum Arbeitslosenhilfeantrag verwendet, in dem eigene Angaben zum Vermögen erhoben werden. Eine **generelle Einholung von Bankauskünften** ist für die Aufgabenerfüllung der Arbeitsverwaltung nicht erforderlich und daher **datenschutzrechtlich unzulässig.**

Lediglich in Einzelfällen, in denen ein begründeter Verdacht auf unrichtige Angaben des Antragstellers besteht (beispielsweise bei abweichenden Angaben auf zeitlich nacheinanderfolgenden Anträgen), würden weitergehende Ermittlungen – ggf. auch bei Banken nach der Entbindung von der Schweigepflicht – angestellt.

11.7 Unzulässige Datenoffenbarungen bei „monatlichen Meldekontrollen" beanstandet

Mit mehreren Eingaben hatten sich Arbeitslose wegen der Offenbarung von Sozialdaten bei der Durchführung von Gruppenmaßnahmen bei monatlichen Meldekontrollen nach § 132 AFG an mich gewandt. Danach hat sich der Arbeitslose auf Aufforderung bei seinem Arbeitsamt zu melden.

Die BA hat mir hierzu mitgeteilt, Hintergrund sei die für die Dauer eines halben Jahres befristete Aktion „monatliche Meldekontrollen" arbeitsloser Leistungsempfänger gewesen, die am 30. September 1993 beendet worden sei. Hierbei sei in Einzelfällen die Anwesenheitskontrolle in einigen Arbeitsämtern durch Namensaufruf erfolgt, wobei auch die Namen Nichterschienener bekanntgegeben und damit unnötig offenbart worden seien. Sie teilt meine Auffassung, daß diese Form der Durchführung der Anwesenheitskontrolle zu nicht erforderlichen und damit unzulässigen Offenbarungen von Sozialdaten geführt hat.

Ich habe gegenüber dem Vorstand der BA die Offenbarung von Sozialdaten durch Namensaufruf oder namentliche Nennung im Zuge der o.a. Maßnahmen als unzulässig bewertet, da sie gegen das in § 35 Abs. 1 SGB I normierte Sozialgeheimnis verstößt.

Da es sich nicht um einen Verstoß in einem Einzelfall gehandelt hat, vielmehr eine unbestimmt hohe Zahl von Arbeitslosen hiervon betroffen war, habe ich diesen Verstoß gem. § 25 Abs. 1 BDSG förmlich beanstandet.

Der Vorstand der BA hat mir daraufhin mitgeteilt, daß die zwischenzeitlich eingeführten Folgeregelungen zur Aktion „monatliche Meldekontrollen" eine Namensnennung der Beteiligten bei entsprechenden Verfahren verhindern.

11.8 Private Arbeitsvermittler erhalten Daten Arbeitsloser

Mit dem Beschäftigungsförderungsgesetzes 1994 wurde das Alleinvermittlungsrecht der Bundesanstalt für Arbeit für Arbeitnehmer aufgehoben und die Arbeitsvermittlung durch Private zugelassen. Aus datenschutzrechtlicher Sicht ergeben sich dadurch eine Reihe von Problemen. Die privaten Arbeitsvermittler erheben und verarbeiten Daten von Arbeitslosen. Sie sind aber keine Stellen im Sinne des § 35 Abs. 1 SGB I, was zur Folge hat, daß die Informationen über die Arbeitslosen auch nicht dem Sozialgeheimnis unterliegen.

Im Beschäftigungsförderungsgesetz mußte daher eine Regelung geschaffen werden, die die datenschutzrechtlichen Anliegen der Arbeitslosen auch bei privaten Arbeitsvermittlern sicherstellt. In engem Kontakt mit dem BMA wurde eine aus datenschutzrechtlicher Sicht akzeptable Lösung (§ 23c AFG) erreicht. Danach gilt für private Arbeitsvermittler insbesondere folgendes:

- Daten über zu besetzende Stellen und über Stellensuchende dürfen nur erhoben, verarbeitet oder genutzt werden, soweit dies zur Arbeitsvermittlung erforderlich ist. Bei personenbezogenen Daten oder Geschäfts- oder Betriebsgeheimnissen ist dies darüber hinaus nur zulässig, soweit der Betroffene im Einzelfall nach Maßgabe des § 4 BDSG eingewilligt hat.
- Werden die Daten im Rahmen der Vermittlungstätigkeit einem Dritten übermittelt, darf dieser sie nur zu dem Zweck verarbeiten oder nutzen, zu dem sie ihm befugt übermittelt worden sind. Damit wird eine Zweckbindung erreicht, wie sie gemäß § 78 SGB X auch gelten würde, wenn die Daten von der Bundesanstalt für Arbeit an den Dritten übermittelt worden wären.
- Nach Abschluß der Vermittlungstätigkeit sind die zur Verfügung gestellten Unterlagen dem Betroffenen zurückzugeben. Personenbezogene Daten sind dann zu löschen, soweit nicht gesetzliche Aufbewahrungspflichten oder ein berechtigtes Interesse des privaten Arbeitsvermittlers entgegenstehen. Der Betroffene kann allerdings nach Abschluß der Vermittlungstätigkeit schriftlich etwas anderes zulassen.

11.9 Offenbarung von personenbezogenen Daten bei ABM

Im Rahmen einer datenschutzrechtlichen Eingabe wurden Bedenken gegen die Offenbarung personenbezogener Daten im Rahmen von Tagesnachweisen bei „Allgemeinen Maßnahmen zur Arbeitsbeschaffung (ABM)" gegenüber der Arbeitsverwaltung – insbesondere durch Soziale Dienste – geltend gemacht. Hier würden vor allem die Namen der Patienten, die Einsatzzeiten und die verrichteten Tätigkeiten mitgeteilt.

Nach ihrer Stellungnahme kann die BA im Rahmen von ABM nach den gesetzlichen und anordnungsrechtlichen Bestimmungen Arbeiten fördern, die zusätzlich sind, im öffentlichen Interesse liegen und deren Durchführung aus arbeitsmarktlicher Sicht zweckmäßig erscheint. Der **Zusätzlichkeit** der im Rahmen von ABM zu verrichtenden Arbeiten komme als Förderungsvoraussetzung besondere Bedeutung zu. Es seien nur solche Arbeiten förderungsfähig, die sonst nicht oder erst zu einem späteren Zeitpunkt durchgeführt würden.

Zur zweckentsprechenden Verwendung der ABM-Mittel komme der Überwachung der laufenden AB-Maßnahmen besondere Bedeutung zu. Neben der Auswertung der vom ABM-Träger vorgelegten Unterlagen (z. B. Nachweise über Lohnzahlung, Anzeigen über die Umsetzung von ABM-Arbeitnehmern, Angaben über den Stand der Arbeiten) würden hierzu regelmäßig Maßnahmeprüfungen vor Ort durch die ABM-Prüfgruppen der Arbeitsämter und Landesarbeitsämter durchgeführt.

Die Tagesnachweise seien nicht nur reine Arbeitszeitbelege, sondern hätten primär die Funktion, den maßnahmegerechten Einsatz der ABM-Kräfte sicherzustellen und damit verbunden, das Vorliegen des ABM-Förderungskriteriums der „Zusätzlichkeit" überprüfen zu können. Für diese Zwecke – so die BA – reichten im Regelfall die Angaben im Tagesnachweis zur Art der verrichteten Tätigkeit aus. Gerade im Bereich der sozialen Dienste, speziell der häuslichen Pflege, sei das Risiko einer Vermengung von krankenkassenfinanzierten und ABM-geförderten Arbeiten jedoch groß.

In Fällen, in denen Umfang und Art der über ABM verrichteten Tätigkeit nicht eindeutig aus den Tagesnachweisen ersichtlich seien oder wenn ein konkreter Mißbrauchsvorwurf gegenüber dem Arbeitsamt geäußert werde, sei es erforderlich, mit der über ABM betreuten Person Kontakt aufzunehmen, um die Art und den Umfang der tatsächlich verrichteten Tätigkeiten abzuklären. Die Information, wo bzw. bei wem über ABM geförderte Arbeiten verrichtet werden, sei daher unentbehrlich.

Ich habe der BA vorgeschlagen, wie im Bereich des Zivildienstes ein Verschlüsselungsverfahren einzuführen. Ein solches Verfahren wäre aus meiner Sicht geeignet, einerseits die Persönlichkeitsrechte der Betroffenen zu wahren und andererseits den maßnahmegerechten Einsatz der ABM-geförderten Arbeiten sicherzustellen und überprüfen zu können.

Hierzu hat mir die BA mitgeteilt, die Möglichkeit einer Verschlüsselung der Angaben in den Tagesnachweisen, also welche Arbeiten wann bei wem über ABM verrichtet wurden, sei unterschiedlich zu bewerten.

Als wichtigste Angabe aus dem Tagesnachweis sei die **Art der ausgeübten Tätigkeit** anzusehen. Eine Verschlüsselung sei hier nicht zweckmäßig, da die anfallenden Tätigkeiten von vornherein nicht abschließend codiert werden könnten. Auch eine Zu-

sammenfassung sei nicht sachgerecht, da es hierdurch zu einer Vermengung von förderungsfähigen und nicht förderungsfähigen Arbeiten kommen könne. Darüber hinaus seien die Angaben zu den über ABM zu fördernden zusätzlichen Arbeiten (z. B. Besuchsdienst, Besorgungen erledigen, Reinigungsarbeiten, sonstige allgemeine Hilfen) auch kaum zum Kern der vertraulichen Patientendaten zu rechnen.

Hinsichtlich des **Zeitpunktes und der Dauer** der über ABM verrichteten Tätigkeit erübrige sich eine Verschlüsselung, da hier keine vertraulichen Patientendaten offenbart werden würden.

Die BA hat jedoch eingeräumt, daß einer Verschlüsselung **des Namens** der betreuten Person unter bestimmten Voraussetzungen zuzustimmen sei. Hierfür müsse jedoch die Codierung seitens der Träger vorgenommen werden. Dabei müsse die Verschlüsselung so gestaltet sein, daß eine eindeutige Zuordnung zu der betreuten Person möglich sei. Im Zweifelsfall, also dann, wenn anhand des Tagesnachweises nicht eindeutig geklärt werden könne, ob ggf. auch maßnahmefremde Arbeiten verrichtet worden seien, müsse der Träger bereit und in der Lage sein, die Chiffre zu entschlüsseln und damit dem Prüfer die Möglichkeit geben, direkt mit der betreuten Person Kontakt aufzunehmen.

Die BA hat die Durchführungsanweisungen zur ABM-Anordnung überarbeitet und die Dienststellen angewiesen, bei den Tages-/Tätigkeitsnachweisen im Bereich der sozialen Dienste eine Verschlüsselung des Namens der betreuten Person durch den Träger zuzulassen, sofern dadurch die Überprüfbarkeit der Arbeiten gewährleistet ist.

Das gefundene Ergebnis begegnet keinen Bedenken aus datenschutzrechtlicher Sicht. Es gewährleistet einerseits die schutzwürdigen Persönlichkeitsrechte der betroffenen Patienten, läßt aber andererseits durch geeignete Prüfverfahren die Sicherstellung der zweckentsprechenden Verwendung der ABM-Mittel zu. Ich werde darauf drängen, daß von den vorgesehenen Namensverschlüsselungen so weit wie möglich Gebrauch gemacht wird.

12 Krankenversicherung

12.1 „Krankenkassen spüren dem Intimleben von HIV-Infizierten nach"

Mit dieser Schlagzeile machte eine Tageszeitung am 28. Juli 1994 auf ein datenschutzrechtlich problematisches Verfahren bei der Barmer Ersatzkasse (BEK) aufmerksam. Danach interessierten sich Mitarbeiter einer Bezirksstelle für das Sexualleben von HIV-Positiven. Die Patienten wurden – teilweise telefonisch – nach Details der Infektion befragt; sogar in der Aids-Ambulanz einer Universitätsklinik wurde versucht, Informationen über die Infizierten zu erhalten.

Die Bezirksstelle der BEK berief sich auf § 116 SGB X, wonach Schadensersatzansprüche, die z. B. ein HIV-Infizierter gegen einen Dritten wegen der Infektion – hat, kraft Gesetzes auf die Krankenversicherung übergehen.

Ich hatte schon vor der Zeitungsmeldung von dem Verfahren gehört und die Barmer Ersatzkasse um Stellungnahme gebeten, weil ich dieses Verfahren insbesondere deshalb für unzulässig halte, weil es keine ausdrückliche Rechtsgrundlage für eine solche Datenerhebung gibt. Die BEK teilte mir mit, daß sie keine Nachforschungen über das private Verhalten, insbesondere über Sexualkontakte, anstelle. Bei dem beschriebenen Vorgang handele es sich um einen Einzelfall; die örtlich zuständige Geschäftsstelle sei entgegen eindeutigenr Anweisungen der Hauptverwaltung der BEK verfahren. Die BEK hat diesen Vorgang ausdrücklich bedauert und versichert, daß sie sich gegenüber den Beteiligten für dieses Fehlverhalten entschuldigen wird.

Die BEK hat in der maßgeblichen Dienstanweisung zur Prüfung von Ersatz- und Erstattungsansprüchen bei HIV-Infektionen folgendes geregelt:

Sobald in Leistungsfällen (z. B. Arbeitsunfähigkeit, Krankengeldbezug, Krankenhausbehandlung, Rehabilitationsmaßnahmen oder sonstigen Behandlungen) erkennbar wird, daß die Erkrankung auf einer HIV-Infektion beruht, ist zunächst über den behandelnden Arzt zu klären – möglichst durch ein vertrauliches Gespräch – ob der/die Versicherte über die Aids-Erkrankung informiert ist. Hierbei sei davon auszugehen, daß der Arzt den Patienten von seiner HIV-Infektion in der Regel schon deshalb unterrichtet, damit weitere Ansteckungen vermieden werden. Verneint der behandelnde Arzt jedoch diese Frage – was nach Meinung der BEK wohl nur in Ausnahmefällen wahrscheinlich ist – sieht die Kasse bis zur Unterrichtung des Versicherten durch den behandelnden Arzt von weiteren Prüfungsmaßnahmen ab. Ist nach den Angaben des Arztes die HIV-Infektion dem Versicherten bekannt, wendet sich die Kasse an ihn, um mögliche Ersatz- und Erstattungsansprüche zu klären.

Die BEK hat des weiteren erklärt, daß die Fragen an den HIV-Infizierten ausdrücklich auf die Sachverhalte einer Infektion durch Bluttransfusion, Blutpräparate oder einer beruflich bedingten Infektion begrenzt werden. Keinesfalls würden Nachforschungen im Bereich des privaten Verhaltens, insbesondere des Sexuallebens, vorgenommen.Die Geschäftsstellen der BEK wurden angewiesen, die Befragung des Versicherten oder des behandelnden Arztes unverzüglich abzubrechen, wenn die Bereitschaft zur Beantwortung verneint wird. Die BEK anerkennt damit, daß die Angaben freiwillig gemacht werden. Ist ein Versicherter nicht bereit, die Fragen der Kasse zur möglichen Ursache einer Infektion zu beantworten, akzeptiert die BEK dies und verbindet damit auch keine Nachteile.

Dieses Verfahren halte ich – zumindest in einer Übergangsphase – für vertretbar:

- Die Krankenversicherung hat ein legitimes Interesse, Schadensersatzansprüche gegen potentielle Schädiger ihrer Versicherten geltend zu machen.

- Es ist sichergestellt, daß im Rahmen dieses Ersatz- und Erstattungsanspruchsverfahrens der Betroffene nicht zum ersten Mal von seiner Infizierung Kenntnis erhält.
- Die Fragen sind auf den Bereich von Bluttransfusionen, Blutpräparaten und beruflich bedingten Infektionen begrenzt.
- Ihre Beantwortung ist freiwillig.
- Der Versicherte hat keine Nachteile zu erwarten, wenn er die Fragen nicht beantwortet.

Da es sich bei den Daten in diesem Verfahren um besonders schützenswerte handelt, halte ich bereichsspezifische gesetzliche Grundlagen für erforderlich. In ersten Gesprächen hat das Bundesministerium für Gesundheit zugesagt, einen entsprechenden Gesetzentwurf zu erarbeiten.

12.2 Kontrolle der Betriebskrankenkasse der Preussag AG

Bei einer Kontrolle der Hauptgeschäftsstelle der Preussag Betriebskrankenkasse in Salzgitter habe ich in der Leistungsabteilung die „Betreuung von arbeitsunfähig Erkrankten", die nicht im Krankengeldbezug stehen, überprüft. Für jeden Einzelfall der Arbeitsunfähigkeit wird ein gesonderter Vorgang angelegt, der zunächst lediglich die Arbeitsunfähigkeitsbescheinigung – bei Arbeitsunfällen auch den Bericht des Durchgangsarztes – enthält. Je nach Erkrankung erfolgt nach ca. 3 bis 4 Wochen eine Anfrage an den Arzt, der die Arbeitsunfähigkeit bescheinigt, mit dem Ziel, ob und wann die Arbeitsfähigkeit des Betroffenen wiederhergestellt werden kann. Ist mit einer baldigen Arbeitsfähigkeit nicht zu rechnen, werden eventuell anrechenbare Vorerkrankungen überprüft. Sollte innerhalb des letzten halben Jahres die gleiche Erkrankung bereits einmal vorgelegen haben, wird diese Vorerkrankungszeit der aktuellen Erkrankungszeit hinzugerechnet. Das beschriebene Verfahren wird automatisiert unterstützt.

Soweit im Einzelfall der Verdacht auf eine mögliche Berufskrankheit besteht, wird unmittelbar mit dem Versicherten Kontakt gesucht, um mit ihm persönlich ggf. weitere Schritte (Beratung, Begutachtung durch den Medizinischen Dienst der Krankenkasse, ggf. Kontakte zum werksärztlichen Dienst) abzustimmen.

Die stichprobenweise durchgesehenen Unterlagen über Erholungs- und Heilkuren enthielten häufig Entlassungsberichte – und zwar ausschließlich von Kureinrichtungen, die nicht meiner datenschutzrechtlichen Zuständigkeit unterliegen – mit detaillierten Anamnese-, Befund- und Diagnosedaten über die Versicherten. Es handelt sich dabei um Kopien von Arztberichten, die von den Kliniken an den jeweiligen Hausarzt des Betroffenen gesandt wurden. Der in diesen Fällen festgestellte Inhalt ging bei weitem über den Katalog der in § 301 Abs. 4 SGB V aufgeführten, zulässigen Angaben hinaus. Von Seiten der Betriebskrankenkasse wurde mir zugesagt, künftig gegenüber den Kurkliniken unter Hinweis auf § 203 StGB darauf hinzuwirken, daß die Berichte nur noch die in § 301 Abs. 4 SGB V genannten Angaben enthalten.

12.3 Unzulässige Werbemaßnahmen der Ersatzkassen

Im Berichtszeitraum habe ich mich erneut mit den datenschutzrechtlichen Aspekten der Mitgliederwerbung von Ersatzkassen auseinandergesetzt.

Die Krankenkassen beschaffen sich Namen und Adressen zum Zwecke der anschließenden Werbung von Nichtmitgliedern auf vielfältige Weise, z. B. bei Schulen, bei Mitschülern, im privaten Umfeld ihrer Mitarbeiter und bei Arbeitgebern im Rahmen von sog. Betriebsprüfungen durch Außendienstmitarbeiter von Krankenkassen. Gerade die letztgenannte Vorgehensweise kann dabei zu Interessenkollisionen beim Betriebsprüfer im Hinblick auf seine eigentliche Aufgabe führen (so auch der Bundesrechnungshof in seiner jüngst erfolgten Unterrichtung des Bundesrates – BR-Drs. 865/94 unter 14.3.4 Seiten 47/48 –).

Allen dargestellten Sachverhalten gemeinsam ist der Umstand, daß es an einer Datenerhebungsbefugnis für die Krankenkassen im abschließenden Datenerhebungskatalog des § 284 Abs. 1 SGB V fehlt. Entsprechende Datenerhebungen habe ich daher vor dem Hintergrund beanstandet, daß die betroffenen Kassen trotz der fehlenden Datenerhebungsbefugnis an ihrer diesbezüglichen Praxis festhalten wollen.

Meine Rechtsauffassung wird vom Bundesversicherungsamt geteilt. Es hat gegen eine Ersatzkasse einen entsprechenden Verpflichtungsbescheid erlassen. Dieser war Gegenstand eines Rechtsstreits, der mittlerweile durch einen Ruhensbeschluß des SG Hamburg beendet wurde. Das SG Hamburg hat den Ruhensbeschluß damit begründet, daß im Zuge der größeren Kassenwahlfreiheit für Versicherte ab 1. Januar 1996 eine neue Sachlage eintrete.

Vor diesem Hintergrund teilt der Verband der Angestellten Krankenkassen (VdAK) meine Auffassung, daß zur Lösung des Problems eine Datenerhebungsbefugnis in § 284 Abs. 1 SGB V geschaffen werden muß. Hierzu werde ich an das zuständige Bundesministerium für Gesundheit (BMG) herantreten. Der VdAK hat zugesagt, ebenfalls entsprechend aktiv zu werden.

12.4 Der maschinenlesbare Krankenschein: Die Krankenversichertenkarte

Seit Ende vergangenen Jahres haben die gesetzlichen Krankenkassen den bisher nur für ein Quartal geltenden Krankenschein aus Papier durch eine mehrere Jahre lang gültige Chipkarte ersetzt. In der Krankenversichertenkarte sind folgende Daten gespeichert: Bezeichnung der ausstellenden Krankenkasse, Familienname und Vorname des Versicherten, Geburtsdatum, Anschrift, Krankenversichertennummer, Versichertenstatus, Tag des Beginns des Versicherungsschutzes, bei befristeter Gültigkeit der Karte das Datum des Fristablaufs. Andere Daten, insbesondere medizinische Daten, dürfen nach dem Sozialgesetzbuch (§ 291 Abs. 2 SGB V) nicht auf der

Karte gespeichert werden. Ausführlich habe ich mich zur Krankenversichertenkarte bereits im 14. Tätigkeitsbericht (S. 92 f. und S. 148) geäußert. Zur Funktion der Krankenversichertenkarte siehe die Abbildung 2 „Weitergabe von Abrechnungsdaten im Bereich der gesetzlichen Krankenkasse".

Von wesentlicher Bedeutung ist nach wie vor die Frage, mit welchen technischen Vorkehrungen gewährleistet wird, daß insbesondere unbefugte Eintragungen von nicht in gesetzlichen Datenkatalogen enthaltenen Daten durch in Arztpraxen eingesetzte Lesegeräte erkannt werden können. Hersteller solcher Geräte sind auf der Basis der technischen Spezifikation der Kassenärztlichen Bundesvereinigung an das Bundesamt für Sicherheit in der Informationstechnik – BSI – herangetreten, um dort ihre Lesegeräte zertifizieren zu lassen. Erste Zertifikate für stationäre Lesegeräte sind bereits erteilt.

In letzter Zeit wurde ich auf ein weiteres Problem aufmerksam. Ärzte setzen bei Hausbesuchen vermehrt portable Lesegeräte ein. Das bedeutet, daß der Arzt beim Hausbesuch die erforderlichen Daten in das Gerät einliest, also auch die Daten aus der Krankenversichertenkarte. Anschließend werden diese Daten in den Praxis-Computer übertragen. Ungelöst ist für mich z. Z. die Frage, wie diese temporär gespeicherten Daten gegen unbefugten Zugriff bei Verlust oder Diebstahl des Gerätes gesichert werden. Auch hier halte ich eine Zertifizierung der portablen Lesegeräte für erforderlich.

Der Kassenärztlichen Bundesvereinigung und dem BSI habe ich mitgeteilt, welche Aspekte bei der Zertifizierung portabler Lesegeräte zu berücksichtigen sind, um diesen Anliegen Rechnung zu tragen. Solche Anforderungen müssen z. B. sein der Schutz der gespeicherten Daten vor unbefugten Zugriffen über entsprechende Authentisierungs- und Identifikationsmechanismen, die Löschung der Daten nach erfolgreicher Übertragung in den Praxis-Computer sowie der Ausschluß einer Schreibfunktion auf die Krankenversichertenkarte im Gerät.

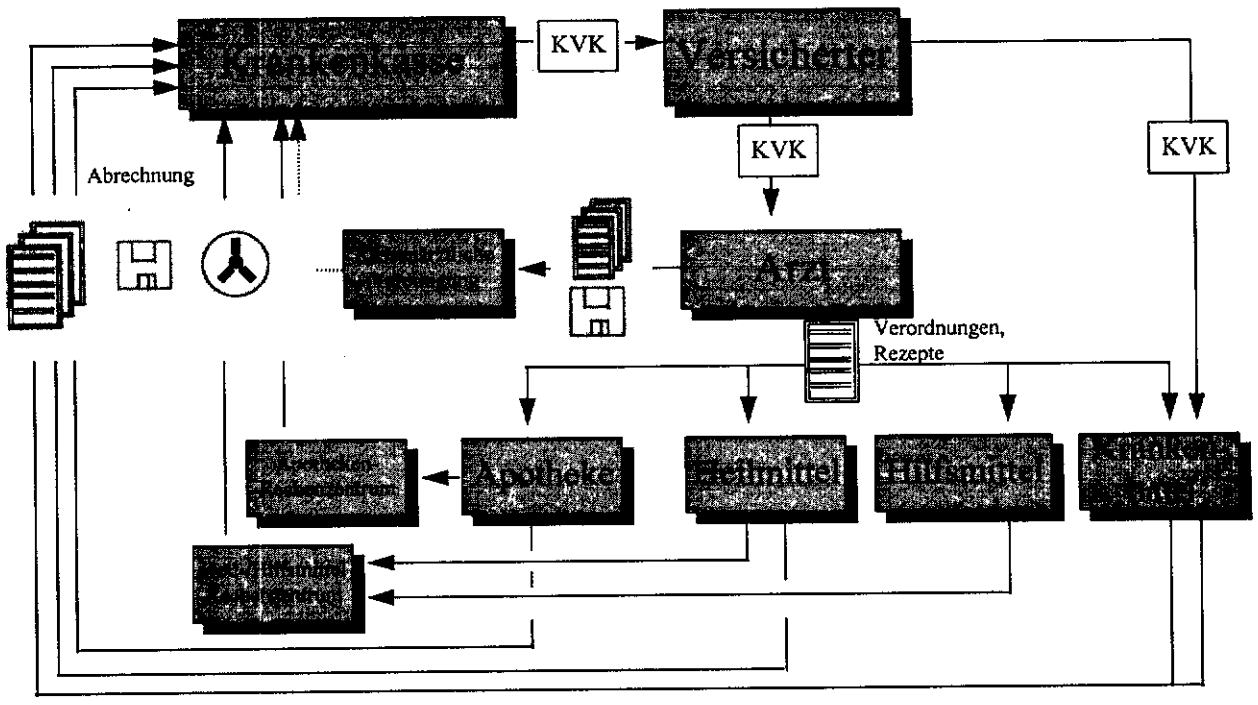
Zu Chipkarten mit Gesundheitsdaten und zu allgemeinen Anforderungen an die Sicherheit von Chipkarten, wie z. B. Kreditkarten, siehe Nr. 17.3 und Nr. 30.1.

12.5 Unzulässige Übermittlung von Vorerkrankungen der Versicherten an Berufsgenossenschaften auf Anforderung

Bei dem unter Nr. 12.2 erwähnten Besuch bei der BKK Preussag stieß ich erneut auf die Praxis von Berufsgenossenschaften, zur Beurteilung der für die Frage der Leistungsgewährung bedeutsamen Frage des ursächlichen Zusammenhanges zwischen schädigendem Ereignis und Erkrankung komplette Vorerkrankungsverzeichnisse bei Krankenkassen anzufordern.

Abbildung 2

„Weitergabe von Abrechnungsdaten im Bereich der gesetzlichen Krankenversicherung"



KVK = Krankenversichertenkarte
= Papier
= maschinell verwertbare Datenträger
= versichertenbezogen
= nicht versichertenbezogen

Diese Praxis berücksichtigt nicht den Erforderlichkeitsgrundsatz, wonach lediglich die für die Beurteilung der o. a. Fragen erforderlichen Informationen über Erkrankungen von Berufsgenossenschaften erhoben und damit von den Krankenkassen übermittelt werden dürfen.

Ich werde mich für eine datenschutzgerechte Gestaltung des Verfahrens im Rahmen des anstehenden Gesetzgebungsvorhabens zum SGB VII (vgl. auch Nr. 14.1.1 und Nr. 14.1.3) einsetzen.

12.6 Anforderungen von Einkommensteuerbescheiden durch Krankenkassen

Die Höhe der vom Versicherten zu zahlenden Beiträge zur gesetzlichen Krankenversicherung orientiert sich an seiner Einkommenshöhe. Um beim Versicherten den erforderlichen Nachweis seines beitragsrelevanten Einkommens zu erhalten, fordern Krankenkassen bei ihm eine Kopie seines letzten Einkommensteuerbescheides an. Dieser Bescheid enthält in der Regel auch Informationen, deren Erhebung für die Feststellung des beitragsrelevanten Einkommens in der gesetzlichen Krankenversicherung nicht von Bedeutung und damit nicht erforderlich ist.

Folgende datenschutzgerechte Lösungen haben daher die Spitzenverbände der gesetzlichen Krankenkassen und ich den Krankenkassen empfohlen:

- Vorlage einer Kopie eines Einkommensteuerbescheides, in dem nach vorherigen entsprechendem Hinweis durch die Krankenkasse nur die für die Beitragsberechnung erforderlichen Angaben lesbar bleiben, die übrigen Angaben jedoch geschwärzt werden können;
- vom Finanzamt bestätigte persönliche Erklärung des Versicherten über das beitragsrelevante Einkommen;
- vom Finanzamt bestätigte Erklärung/Bescheinigung eines Steuerberaters über dieses Einkommen.

13 Rentenversicherung

13.1 Neue Postrentendienst-Verordnung

Eine neue Postrentendienst-Verordnung ist am 1. September 1994 in Kraft getreten. Sie hat das Ziel, die Rechtsbeziehungen zwischen den Trägern der Renten- und Unfallversicherung und dem Postrentendienst der Deutschen Bundespost zu regeln, soweit dieser kraft Gesetzes die Geldleistungen der Renten- und Unfallversicherung auszahlt und anpaßt. Bei diesem Verfahren werden eine Menge personenbezogener Daten zwischen den beteiligten Stellen übermittelt. Ich wurde vom Bundesministerium für Arbeit und Sozialordnung bei der Formulierung der Verordnung beteiligt und konnte meine Anliegen im Text weitgehend realisieren. Aus datenschutzrechtlicher Sicht ist bei der neuen Postrentendienst-Verordnung (PostRDV) insbesondere folgendes erwähnenswert:

- Nach § 20 der VO übernimmt der Postrentendienst im Bereich der Krankenversicherung der Rentner für die Träger der Rentenversicherung bestimmte Aufgaben. Das Nähere wird durch Vereinbarung zwischen dem Verband Deutscher Rentenversicherungsträger und dem Postrentendienst geregelt.

  Ich habe dem BMA mitgeteilt, daß aus Gründen des Datenschutzes diese Regelung eine Begrenzung der Übermittlung an die Spitzenverbände der gesetzlichen Krankenversicherung für den Risikostrukturausgleich auf die in § 267 Abs. 6 Satz 1 SGB V genannten Daten enthalten sollte. Damit wird die Übermittlungsbefugnis auf die hier erforderlichen Daten begrenzt. Dies sind das Kennzeichen nach § 293 Abs. 1 SGB V, welches die Krankenkassen im Schriftverkehr und für Abrechnungszwecke mit anderen Trägern der Sozialversicherung verwenden, und die Rentenversicherungsnummer nach § 147 SGB VI.
- Es wird abschließend festgelegt, welche personenbezogenen Daten der Rentnerausweis enthalten darf (§ 21 Abs. 2 der VO). Dies sind neben dem Familien- und Vornamen einschließlich des Geburtsnamens das Geburtsdatum und die Versicherungsnummer.

  Gegen die Aufnahme der Versicherungsnummer habe ich ursprüngliche datenschutzrechtliche Bedenken zurückgestellt, da das BMA nachvollziehbar dargelegt hat, daß die Aufnahme im Interesse der Rentner unverzichtbar ist. Damit wird ein umfassendes und zügiges Auskunftsverfahren für die Betroffenen sichergestellt.

  Im Verordnungstext wird ausdrücklich sichergestellt, daß der Rentnerausweis nicht zum Abruf personenbezogener Daten in einem automatisierten Abrufverfahren verwendet werden darf. Außerdem ist sichergestellt, daß er keine Daten über Rentenzahlbeträge enthalten darf.
- Nach dem sogenannten Rentenauskunftsverfahren erteilt der Postrentendienst für die Träger der Rentenversicherung Auskünfte über die Höhe der ausgezahlten Geldleistungen und andere ihm zur Verfügung stehende Sozialdaten (§ 22 der VO).

  Ausdrücklich festgeschrieben in der Verordnung ist hierbei, daß entsprechende Auskünfte durch den Postrentendienst nur zulässig sind, wenn die Voraussetzungen des § 151 Abs. 1 SGB VI vorliegen. Danach kommt eine Auskunft nur in Betracht, wenn es sich um Sozialdaten handelt, die dem Postrentendienst im Zusammenhang mit der Zahlung, Anpassung, Überwachung, Einstellung oder Abrechnung von Renten oder anderen Geldleistungen nach dem Sozialgesetzbuch bekannt geworden sind. Des weiteren ist die Übermittlung beschränkt auf die in § 151 Abs. 1 SGB VI abschließend genannten Daten (Datenkatalog). Die Auskunft über andere Sozialdaten ist unzulässig.
- Die Träger der Rentenversicherung können verlangen, daß der Postrentendienst für sie im Rahmen der datenschutzrechtlichen Vorschriften Auskünfte von anderen öffentlichen Stellen einholt (§ 23 der Verordnung). Hierfür wird in dieser Vorschrift ausdrücklich eine Erhebungsbefugnis normiert, soweit dies für die Durchführung der Anpassung von

Geldleistungen durch den Postrentendienst erforderlich ist.

Ich möchte ausdrücklich darauf hinweisen, daß durch § 23 der VO keine Erweiterung im Hinblick auf die Datenerhebungsbefugnis der Rentenversicherungsträger geschaffen wird. Insbesondere wird durch diese Vorschrift keine Ausnahme vom Ersterhebungsgrundsatz normiert. Die Vorschrift setzt für eine zulässige Einholung von Auskünften vielmehr voraus, daß für den Rentenversicherungsträger eine Rechtsgrundlage für die Datenerhebung – und damit auch für den Postrentendienst – gegeben ist. Des weiteren ist Voraussetzung, daß eine Rechtsgrundlage für die Übermittlung der durch den Postrentendienst erhobenen Daten an den Rentenversicherungsträger besteht. Dies wurde seitens des BMA auch nochmals in der Verordnungsbegründung klargestellt.

- In § 119 SGB VI sind die Aufgaben festgeschrieben, die die Deutsche Bundespost für die Träger der Rentenversicherung der Arbeiter und der Angestellten wahrnimmt. Nach Meinung des Bundesministeriums der Justiz könne aus dieser Aufgabenzuweisung nicht abgeleitet werden, daß damit dem Postrentendienst alle für die Aufgabenwahrnehmung notwendigen Erhebungs- und Verarbeitungsbefugnisse eingeräumt werden. Die Einräumung dieser Befugnisse bedürfe vielmehr einer ausdrücklichen gesetzlichen Regelung. Deshalb solle bei nächster Gelegenheit in das Sechste Buch des Sozialgesetzbuches eine entsprechende gesetzliche Regelung aufgenommen werden.

Ich habe dieses Anliegen dem Bundesministerium für Arbeit und Sozialordnung übermittelt. Eine Stellungnahme von dort steht noch aus.

13.2 Rentenversicherungsträger wenden sich bei der Rückforderung überzahlter Rentenleistungen bei Todesfällen oft gegen das Bankgeheimnis

Renten werden durch die Rentenrechnungsstelle der Deutschen Bundespost ausgezahlt. Der Rentenbezug endet mit dem Ablauf des Todesmonats des Berechtigten. Damit die Rentenrechnungsstelle vom Todesfall frühzeitig erfährt, sind in den einschlägigen Meldevorschriften Regelungen getroffen worden, nach denen die Meldebehörden dem Rentendienst Sterbefälle mitteilen. Diese Mitteilungen gehen jedoch oft erst dann ein, wenn bereits eine Rente oder mehr zuviel überwiesen wurden. Der Rentendienst fordert dann die überzahlten Beträge nach § 118 Abs. 3 SGB VI zurück und teilt dies dem Rentenversicherungsträger mit. § 118 Abs. 3 Satz 2 SGB VI sieht vor, daß in solchen Fällen grundsätzlich das Kreditinstitut die überzahlten Beträge an die Rentenversicherung zurücküberweist. Die Rückzahlungsverpflichtung des Kreditinstituts entfällt jedoch, wenn über die überzahlten Beträge zwischenzeitlich bereits anderweitig verfügt wurde. In diesen Fällen ist der Rentenversicherungsträger verpflichtet, die Überzahlung vom Berechtigten oder dessen Erben zurückzufordern (§§ 76 Abs. 1 SGB IV, 50 Abs. 2 SGB X). Gegen ggf. andere Empfänger der Überzahlung besteht ein bürgerlich-rechtlicher Rückerstattungsanspruch.

Ich hatte vor einiger Zeit mit der BfA ein datenschutzrechtlich akzeptables Verfahren zur Ermittlung der Rechtsnachfolger des verstorbenen Rentenberechtigten entwickelt. Danach sind Ermittlungen vorrangig bei den Nachlaßgerichten, Gemeindeverwaltungen und als letzte Möglichkeit bei den Krankenkassen als datenschutzrechtlich zulässiger Weg vorgesehen. Dieses Verfahren führt jedoch nicht in allen Fällen zum Erfolg und ist im übrigen – nach Darstellung der Sozialversicherungsträger – mit einem nicht unerheblichen Verwaltungsaufwand verbunden.

Seitens der Rentenversicherungsträger wird daher eine gesetzliche Regelung angeregt, wonach Banken den Namen des Verfügungsberechtigten bekanntgeben müssen, wenn ihre Rückzahlungspflicht für nach dem Tod des Berechtigten erbrachte Geldleistungen wegen § 118 Abs. 3 Satz 3 SGB VI geendet hat. Zur Realisierung dieses Vorhabens wird eine Ergänzung des § 118 Abs. 3 SGB VI vorgeschlagen. Danach soll das Kreditinstitut der überweisenden Stelle oder dem Träger der Rentenversicherung – sofern nach Satz 3 eine Rücküberweisung nicht erfolgen kann – mitteilen, wer über die zu Unrecht erbrachten Geldleistungen verfügt hat und wer über das Konto verfügungsberechtigt ist.

Ich werde mich mit dem Bundesministerium für Arbeit und Sozialordnung um eine entsprechende, datenschutzgerechte Gesetzesänderung bemühen.

13.3 Bundesversicherungsanstalt für Angestellte – BfA –

Der Datenschutz im Bereich der BfA hat einen hohen Stellenwert, die Zusammenarbeit mit ihr ist vorbildlich. Bei den vielen Eingaben, welche die BfA betrafen, konnten im Ergebnis in aller Regel datenschutzgerechte Lösungen gefunden werden. Im Hinblick auf einzelne Kernprobleme hat die BfA Lösungen entwickelt, die für alle Sozialleistungsträger mustergültig sind.

13.3.1 Die BfA überprüft die Mitarbeiter von Kliniken

Mehrere Einrichtungen, die im Auftrag der BfA Rehabilitationsmaßnahmen für Versicherte durchführen, haben sich an mich gewandt. Sie haben Bedenken dagegen erhoben, daß sie personenbezogene Informationen über ihre Mitarbeiter an die BfA liefern sollen. Die BfA begründet dies mit der Sicherstellung einer ordnungsgemäßen Durchführung der Rehabilitationsmaßnahmen.

Ich habe gegen eine solche Datenerhebung grundsätzlich keine Bedenken. Die Erforderlichkeit ergibt sich aus der Verpflichtung zur wirtschaftlichen und sparsamen Verwendung der Gelder der Versichertengemeinschaft sowie aus dem Auftrag, eine optimale Betreuung der Versicherten in den Einrichtungen sicherzustellen. Dabei ist zu berücksichtigen, daß den größten Teil des Pflegesatzes die Personalkosten einnehmen. Diese müssen für die BfA transparent sein. Sie muß überprüfen können, für welches Personal mit welcher Qualifikation welche Gehälter

gezahlt werden. Dies ist nur aufgrund entsprechender Nachweise möglich. In diesem Zusammenhang habe ich insbesondere drei Themenbereiche mit der BfA erörtert:

- Die BfA verlangt von den Maßnahmeträgern bei bestimmten Mitarbeitern die **Vorlage von Qualifikationsurkunden.** Dies ist bei Chefärzten, Oberärzten, Psychologen und teilweise bei sonstigem therapeutischen Personal der Fall. Es wird damit begründet, daß bei diesen herausgehobenen Positionen anderenfalls eine notwendige Überprüfung der Qualifikation der Stelleninhaber nicht möglich sei. Die BfA weist ausdrücklich darauf hin, daß die Überprüfung der vorgelegten Unterlagen ausschließlich durch die damit befaßten Mitarbeiter vorgenommen werde, die insbesondere darauf achteten, daß die Qualifikationen tatsächlich vorliegen, damit die Patienten optimal betreut werden.

  Aus den vorgetragenen Gründen halte ich eine entsprechende Datenerhebung für zulässig. Die BfA will künftig die vorgelegten Unterlagen der Mitarbeiter nach deren Prüfung an die Einrichtungen zurückzusenden. In den Vorgängen der BfA werden nur noch Nachweise über die Approbation und die Facharztqualifikation aufbewahrt. Hinzu können noch Unterlagen kommen, die besondere Befähigungen ausweisen, die in Beziehung zur Rehabilitation stehen (z. B. Absolvierung sozialmedizinischer Kurse).

- Ein weiteres Thema ist, ob die **Einsichtnahme in Personalakten** der Klinikangestellten durch Mitarbeiter der BfA erforderlich und zulässig ist.

Das Bundesversicherungsamt vertritt die Auffassung, daß im Hinblick auf die spezifischen Erfordernisse des Abrechnungsverfahrens (z. B. Überprüfung des Vorliegens bzw. des Wegfalls von zahlungsbegründenden Umständen) auf die Einsichtnahme in Personalakten bei Vertragshäusern nicht generell verzichtet werden könne. Hinzu komme, daß ihre Mitarbeiter, in den Vertragshäusern bisher keine derartige Einsichtnahme gefordert oder vorgenommen hätten.

Ich habe im Hinblick auf den Vertraulichkeitsgrundsatz bei Personalakten erhebliche Bedenken. Das Problem ist noch nicht abschließend gelöst.

- Des weiteren haben sich einige Vertragshäuser der BfA an mich gewandt, weil sie gegen die **Erhebung der Urlaubs- und Krankheitszeiten** ihrer Mitarbeiter Bedenken haben. Auch dies wird seitens der BfA damit begründet, daß mit diesen Angaben die im Rahmen der Vertragsverhandlungen mit den Kliniken getroffenen personellen Vereinbarungen überwacht werden sollen. Ähnlich wie die Angaben über Name und Vorname sowie Arbeitszeit würden diese Angaben zur Überprüfung benötigt, in welcher Anzahl das medizinische Personal in der Klinik tatsächlich tätig ist. Es sollen dadurch Ausfälle deutlich gemacht werden.

Aus Anlaß einer Eingabe hat die BfA jedoch nochmals den Umfang dieser Datenerhebungen geprüft. Sie ist dabei zu dem Ergebnis gekommen, daß nur Daten über Fehlzeiten erhoben werden müssen, die über das normale Maß hinausgehen. Zur Verdeutlichung und auch zum besseren Verständnis für die Klinikleitungen hat sie veranlaßt, daß künftig in den der Personalstandsmeldungen Daten über Krankheit und Urlaub nur dann anzugeben sind, wenn die krankheits- oder urlaubsbedingte Abwesenheit mehr als zwei Monate beträgt.

13.3.2 Keine Offenbarung von Kureinrichtungen gegenüber Arbeitgebern

Den exakten Beginn einer Kur und den Entlassungstag teilt der Arbeitnehmer seinem Arbeitgeber unter Vorlage des Einberufungsschreibens bzw. der Entlassungsmitteilung der Behandlungsstätte mit. Zu diesem Verfahren ist er faktisch gezwungen. Hiergegen habe ich Bedenken, da erfahrene Personalsachbearbeiter anhand der Behandlungsstätte und teilweise sogar allein aufgrund des Behandlungsortes auf die Art der zu behandelnden Erkrankung schließen können.

Der Verband Deutscher Rentenversicherungsträger (VDR) hat sich mit der Thematik auseinandergesetzt. Im Ergebnis hat er seinen Verbandsmitgliedern empfohlen, die Rehabilitationseinrichtungen darüber zu unterrichten, daß Versicherte auf ihren Wunsch auch Bescheinigungen über Beginn und Ende der stationären Heilbehandlung erhalten können, ohne daß die Art der Behandlungseinrichtung durch Briefkopf oder Stempel ersichtlich ist. Auf die Tatsache, daß nach den organisatorischen Gegebenheiten bei den einzelnen Verbandsmitgliedern das nunmehr empfohlene Verfahren nicht überall sofort angewandt werden kann, sondern z. T. eine Umstellungsphase erforderlich ist, hat der VDR hingewiesen.

Die BfA hatte zunächst Bedenken gegen ein derartiges Verfahren, da sie die Gefahr sah, daß die notwendigen Informationsflüsse nicht so rechtzeitig abgewickelt werden können, damit die Betroffenen ihre Pflichten gegenüber ihren Arbeitgebern erfüllen können. Sie hat sich mittlerweile bereit erklärt, ein Verfahren zu entwickeln, das es ermöglicht, den Versicherten auf Wunsch eine derartige neutrale Bescheinigung zur Verfügung zu stellen.

13.3.3 Sozialversicherungswahlen

Bei der BfA habe ich die Durchführung der im ersten Halbjahr des Jahres 1993 stattgefundenen Sozialversicherungswahlen kontrolliert. Die Kontrolle fand nach dem Wahltag statt. Die Wahlunterlagen waren bereits von den Wahlberechtigten wieder zurückgesandt und wurden entsprechend ausgewertet. Mit vielen mit den Sozialversicherungswahlen zusammenhängenden Arbeiten war ein Privatunternehmen beauftragt worden.

Anlaß für diese Kontrolle waren mehrere an mich gerichtete Eingaben von Versicherten, die datenschutzrechtliche Bedenken im Hinblick auf die Durchführung der Sozialversicherungswahlen geäußert hatten; insbesondere in Zweifel gezogen wurde, ob die BfA das Wahlgeheimnis wahrt.

Rechtsgrundlage für die Durchführung der Sozialversicherungswahlen sind §§ 45 ff. SGB IV i. V. m. der

Wahlordnung über die Sozialversicherung (SVWO). Aus datenschutzrechtlicher Sicht ist § 37 a SVWO von zentraler Bedeutung. Die wichtigsten Aussagen dieser Vorschrift sind:

- Werden personenbezogene Kennzeichnungen als Wahlausweise verwendet, dürfen diese nur auf die Wahlbriefumschläge aufgedruckt werden.
- Bei der Verwendung personenbezogener Kennzeichnungen als Wahlausweise kann auf Stimmzettelumschläge verzichtet werden, wenn die personenbezogenen Kennzeichnungen verschlüsselt und im Wahlverfahren nur die verschlüsselten Kennzeichnungen verwendet werden.
- Das Verfahren zur Ver- und Entschlüsselung darf nur den mit der Verschlüsselung vertrauten Personen bekannt sein.
- Eine Entschlüsselung der personenbezogenen Kennzeichnungen ist nur zulässig, soweit das im Rahmen eines Wahlanfechtungs- oder Strafverfahrens notwendig ist.

Das Ergebnis meiner Kontrolle war, daß bei der BfA die einschlägigen datenschutzrechtlichen Bestimmungen bei der Durchführung der Sozialversicherungswahlen, insbesondere § 37 a SVWO, beachtet wurden.

13.3.4 Informationen an den Arbeitgeber durch die BfA ohne Kenntnis der Betroffenen

Eine Mitarbeiterin teilte ihrem Arbeitgeber mit, daß ein von ihr gestellter Antrag auf Erwerbsunfähigkeitsrente abgelehnt worden sei und sie deshalb Klage beim Sozialgericht eingereicht habe. Der Arbeitgeber wandte sich daraufhin mit der Bitte an die BfA, bevor er ein amtsärztliches Gutachten anfordere, möge ihm die BfA die Angaben der Petentin bestätigen. Zugleich fragte er, wann mit einer Entscheidung über den Rentenantrag zu rechnen sei. Die BfA antwortete, der Antrag sei aus medizinischen Gründen abgelehnt, ein Widerspruch sei zurückgewiesen worden. Weiterhin wurde mitgeteilt, das Klageverfahren sei noch nicht abgeschlossen; wann mit einer abschließenden Entscheidung zu rechnen sei, könne noch nicht gesagt werden.

Die Petentin hat sich zu Recht gegen das Verhalten der BfA gewandt. Die Weitergabe der Informationen durch die BfA ist mit dem Sozialgeheimnis nicht vereinbar (§ 35 Abs. 1 Satz 1 SGB I). Dem Arbeitgeber durften ohne Einwilligung der Betroffenen keine Informationen darüber gegeben werden, wie über einen gestellten Rentenantrag entschieden wurde und in welchem Verfahrensstadium sich der Entscheidungsprozeß befand.

Die BfA hat den Verstoß gegen datenschutzrechtliche Bestimmungen eingeräumt und den Fall zum Anlaß genommen, den zuständigen Fachbereich eindringlich zu belehren und das Thema in einem Informationsblatt für die Mitarbeiter aufzugreifen. Dennoch habe ich hier eine förmliche Beanstandung ausgesprochen, da ich vergleichbare Datenschutzverstöße in mehreren Einzelfällen nicht beanstandet hatte, bei denen die BfA ebenfalls zugesagt hatte, durch interne Maßnahmen eine datenschutzgerechte Verfahrenspraxis für die Zukunft sicherzustellen (§ 25 Abs. 2 BDSG).

Der Petentin kam es natürlich auch darauf an, daß ihr Arbeitgeber die erhaltenen Informationen nicht weiter verwertete. Die BfA wandte sich daher an den Arbeitgeber und wies auf die Unzulässigkeit der Datenübermittlung hin. Er wurde aus diesem Grunde gebeten, die an ihn gerichteten BfA-Schreiben zurückzusenden und keine Kopien für die dortigen Vorgänge zu fertigen.

Der Arbeitgeber hat zwischenzeitlich alle Originalschriftstücke zurückgegeben und ein sogenanntes Verwertungsverbot der erhaltenen Informationen bestätigt, indem er mitteilte, daß der Vorgang über seine Mitarbeiterin so geführt werde, als hätte er die Informationen der BfA niemals erhalten.

Dem Anliegen der Petentin konnte damit in vollem Umfang Rechnung getragen werden.

13.3.5 Rentenansprüche wurden an Partnerschaftsvermittlung abgetreten.

Ein Unternehmen zur Partnerschaftsvermittlung verwandte in seinen Vertragsformularen Klauseln, wonach die Kunden u. a. Rentenansprüche soweit gesetzlich zulässig – an sie abtreten. In einem mir vorgelegten Fall fragte die Partnervermittlung bei der BfA, ob die abgetretene Forderung bestehe und ob diese einredefrei sei; gegebenenfalls solle die BfA die pfändbaren Beträge an die Partnervermittlung überweisen.

Die BfA teilte daraufhin den maßgeblichen monatlichen Zahlbetrag sowie den davon pfändbaren und damit abtretbaren Teil mit. Eine Kopie dieses Schreibens an das Vermittlungsbüro ging auch an die Petentin. Diese wandte sich insbesondere deshalb gegen eine entsprechende Datenoffenbarung, weil sie hierzu ihre Einwilligung nicht gegeben habe und weil keine Forderung der Partnervermittlung gegen sie bestehe.

Die Vorgehensweise der BfA verstößt nicht gegen das Sozialgeheimnis. § 69 Abs. 1 Nr. 1 SGB X enthält eine gesetzliche Offenbarungsbefugnis. Danach ist hier eine Datenübermittlung an das Vermittlungsbüro zulässig, weil die Abwicklung einer Forderungsabtretung nach § 53 SGB I zu den gesetzlichen Aufgaben der BfA gehört. Wird eine Abtretungsvereinbarung nach § 398 BGB vorgelegt, muß die BfA die Rente, sofern pfändbare Beträge zur Verfügung stehen, entsprechend aufteilen.

Der neue Gläubiger, hier das Vermittlungsbüro, hat rechtlich die Möglichkeit, die Aufteilung zu überprüfen. Er muß daher über die Aufteilungsmodalitäten in Kenntnis gesetzt werden. Zu diesen Informationen gehört auch die monatliche Rentenhöhe als maßgeblicher Ausgangswert für die Berechnung des Pfändungsbetrages.

Darüber hinaus ist es weder Aufgabe der BfA noch kann sie prüfen, ob eine Abtretungsvereinbarung wirksam oder unwirksam ist. Dies muß im Zweifel zwischen den an der Abtretung beteiligten Parteien geklärt werden. Die BfA ist als sog. Drittschuldner an

der Abtretungsvereinbarung nicht beteiligt gewesen. An eine Ausnahme wäre allenfalls dann zu denken, wenn die Abtretung ganz offensichtlich rechtsfehlerhaft und damit für jeden erkennbar unwirksam ist. Hierfür ergaben sich im vorliegenden Fall jedoch keine Anhaltspunkte.

13.3.6 BfA fordert Krankenhausentlassungsberichte an

Nach Beendigung einer Behandlung werden oftmals die entsprechenden Entlassungsberichte von der BfA von dem Krankenhaus angefordert. Zur Begründung gibt die BfA an, daß sie sich z. B. bei einem Antrag auf Leistungen zur Rehabilitation ein genaues Bild darüber verschaffen muß, inwieweit die Erwerbsfähigkeit eines Versicherten erheblich gefährdet oder gemindert ist und ob diese durch Maßnahmen zur Rehabilitation wesentlich gebessert oder wiederhergestellt werden kann. Entsprechendes gelte für das Rentenverfahren. Hierzu bedient sich die BfA regelmäßig der Mithilfe externer ärztlicher Gutachter. Wurden aber in Einzelfällen zeitnah medizinische Untersuchungen von Dritten vorgenommen, fordert die BfA die Ergebnisse von diesen Stellen oder Ärzten an, auch um den Betroffenen unnötige Untersuchungen zu ersparen.

Über einen Landesdatenschutzbeauftragten hat sich ein Krankenhaus gegen diese Praxis der BfA gewandt. Bereits in meinem 8. Tätigkeitsbericht (s. Nr. 10.6.1) habe ich zur Frage ärztlicher Entlassungsberichte an die BfA grundsätzlich Stellung genommen und die Zulässigkeit der Übermittlung bejaht. Zweifelhaft erscheint allenfalls die Notwendigkeit bestimmter, üblicherweise in dem Bericht enthaltener Angaben z. B. über Laborbefunde, Vorerkrankungen, Familienanamnese. Der ärztliche Entlassungsbericht sollte insoweit auf den notwendigen Umfang hin überprüft und gegebenenfalls reduziert werden.

Nach der Schaffung eines Medizinischen Dienstes für die Krankenkassen stellt sich nach Meinung des gen. Krankenhauses die Problematik jedoch aus einem anderen Blickwinkel dar. Es sei nichts dagegen einzuwenden, die Entlassungsberichte dem beratungsärztlichen Dienst der BfA zu überlassen, nicht aber der Behörde selbst. Mit dem Medizinischen Dienst der Krankenkassen (MDK) habe man ein entsprechendes Verfahren gefunden, wonach nur dem jeweils zuständigen Arzt des MDK der Bericht übersandt und von diesem vertraulich behandelt wird. Damit ist sichergestellt, daß der zuständigen Krankenkasse nur die für die Leistungsbeurteilung unbedingt erforderlichen Informationen aus dem Entlassungsbericht übermittelt werden.

Die Überlegungen der Krankenhausleitung zeugen von einem hohen Datenschutzbewußtsein. Im Ergebnis ist jedoch festzustellen, daß auch die dargestellte Praxis der BfA aus datenschutzrechtlicher Sicht nicht zu beanstanden ist.

Rechtsgrundlage für die Weitergabe von Entlassungsberichten durch die Krankenhäuser ist § 100 Abs. 1 Sätze 1 bis 3 SGB X. Voraussetzungen für die dort normierte Auskunftspflicht der Krankenhäuser sind

- der Bedarf des Leistungsträgers an Auskünften über den Versicherten, soweit diese für die Entscheidung über die beantragte Leistung erheblich sind,
- ein Auskunftsersuchen des Leistungsträgers und
- das Einverständnis des Betroffenen.

Das zur Auskunft verpflichtete Krankenhaus kann die Übersendung eines Entlassungsberichtes nicht davon abhängig machen, ob die Organisation des auskunftsberechtigten Leistungsträgers Strukturen aufweist, die eine strikte Trennung von Verwaltungs- und ärztlichem Bereich vorsehen. Hier ist zu berücksichtigen, daß die Auskunftspflicht nach § 100 Abs. 1 SGB X gegenüber dem Leistungsträger, nicht aber gegenüber einem bestimmten Funktionsträger besteht.

Der Leistungsträger ist im übrigen verpflichtet, für den Arbeitsablauf sicherzustellen, daß Mitarbeiter mit Sozialdaten nur insoweit in Berührung kommen, als es das Aufgabengebiet verlangt. Nach § 35 Abs. 1 Satz 2 SGB I umfaßt die Wahrung des Sozialgeheimnisses die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, daß die Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden. Ich habe keine Anhaltspunkte dafür, daß im Bereich der BfA die entsprechend notwendigen organisatorischen Maßnahmen nicht getroffen wurden.

Die im Bereich der Krankenversicherung vorhandenen Organisationsstrukturen können m. E. nicht ohne weiteres auf die Rentenversicherung übertragen werden. Dem Medizinischen Dienst der Krankenversicherung, dessen sich die Krankenkassen zur Erfüllung bestimmter Aufgaben zu bedienen haben (z. B. Begutachtung in den gesetzlich bestimmten Fällen, medizinische Beratung), ist eine organisatorisch eigenständige Rolle in der Zusammenarbeit mit den Krankenkassen zugewiesen worden (vgl. §§ 275 bis 293 SGB V). Vergleichbare Regelungen existieren nicht für den medizinischen Dienst der Rentenversicherung.

13.3.7 Zeiten der Arbeitsunfähigkeit und Diagnosen werden von den Krankenkassen an die BfA gemeldet

Die Spitzenverbände der Krankenkassen und die BfA haben sich darauf geeinigt, daß ab 1. Oktober 1993 das sog. **AUD-Verfahren** praktiziert wird. Danach übermitteln die Krankenkassen bundesweit im Falle eines Antrages auf stationäre medizinische Rehabilitation die Arbeitsunfähigkeitszeiten und -diagnosen der letzten 3 Jahre dieser Antragsteller routinemäßig an die BfA. Dies wird mit der Durchführung erfolgversprechender Rehabilitationsmaßnahmen begründet.

Mit Schreiben vom April 1994 an seine Mitglieder hat der AOK-Bundesverband gegen dieses Verfahren datenschutzrechtliche Bedenken erhoben. Es sei nicht erkennbar, aus welchen Gründen sämtliche Da-

ten und Diagnosen der letzten 3 Jahre der BfA übermittelt werden müssen, auch solche, die offensichtlich in keinem Zusammenhang mit dem Rehabilitationsleiden stehen.

Bei der datenschutzrechtlichen Bewertung dieses Verfahrens ist eingangs zu berücksichtigen, daß hier in vielen Fällen viele sensible personenbezogene Daten offenbart werden. Dennoch bin ich im Ergebnis der Meinung, daß das Verfahren mit datenschutzrechtlichen Bestimmungen vereinbar ist.

Die Kenntnis der übermittelten Daten ist für die Aufgabenerfüllung der BfA erforderlich und ihre Übermittlung damit gem. § 69 Abs. 1 Nr. 1 SGB X zulässig.

Mit dem Überblick über die Arbeitsunfähigkeitszeiten der letzten 3 Jahre kann der Antragsteller eine seinem gesamten Krankheitsbild entsprechende ganzheitliche Behandlung erhalten. Dazu gehören auch bei Eilbedürftigkeit notwendige Rehabilitationsleistungen. Darüber hinaus wird sich durch eine gezielte Einweisung in Kureinrichtungen unter Berücksichtigung vorangegangener Arbeitsunfähigkeitszeiten und einer darauf ausgerichteten Therapie die Leistungsfähigkeit günstig beeinflussen und eine bestehende Arbeitsunfähigkeit möglicherweise beseitigen lassen.

Ich habe mich daher der Meinung der BfA angeschlossen, wonach eine Bewertung der Arbeitsunfähigkeitsdaten im Hinblick auf ihre sozialmedizinische Relevanz nicht von der Sachbearbeitung der Krankenversicherung geleistet werden kann. Zur Beurteilung der erheblichen Gefährdung oder Minderung der Leistungsfähigkeit im Erwerbsleben und der erforderlichen Reha-Maßnahmen muß vielmehr der Beratungsärztliche Dienst der BfA die gesamte gesundheitliche Situation eines Versicherten umfassend aufklären. Es gibt somit keine Beschränkung auf ein bestimmtes sog. „Rehaleiden". Diese Aufgabe kann deshalb auch nicht in den Verantwortungsbereich des medizinischen Dienstes der Krankenversicherung gelegt werden. Denn in die Bewertung müssen alle medizinischen Daten einschließlich der von der BfA veranlaßten Gutachten einbezogen werden.

Da es sich hier um medizinische Daten handelt, ist zusätzlich zu § 69 Abs. 1 Nr. 1 SGB X noch § 76 Abs. 2 Nr. 1 SGB X zu berücksichtigen. Danach ist der Betroffene von der speichernden Stelle zu Beginn des Verwaltungsverfahrens in allgemeiner Form schriftlich auf sein **Widerspruchsrecht** hinzuweisen. Um dieser Vorschrift Rechnung zu tragen, enthalten die **Reha-Antragsformulare der BfA** folgenden Hinweis:

„Ich nehme ferner zur Kenntnis, daß

- *meine Krankenkasse der BfA die Arbeitsunfähigkeitszeiten und die dazugehörigen Diagnosen einschließlich der Angaben zu Krankenhaus- bzw. Rehabilitationsaufenthalten der letzten 3 Jahre übermittelt,*
- *ich dem jedoch gegenüber meiner Krankenkasse widersprechen kann."*

Dieser Hinweis weist den einzelnen Betroffenen nochmals ausdrücklich auf sein Widerspruchsrecht gegen eine entsprechende Datenübermittlung hin. Er wird in datenschutzrechtlich vorbildlicher Weise von der BfA gegeben, obwohl sie nicht selbst übermittelnde Stelle ist. Dies ist jedoch deshalb notwendig, weil bei den Krankenkassen in der Regel kein Verwaltungsverfahren anhängig ist und deshalb die Hinweispflicht der Krankenkasse nicht ausgelöst wird.

Bedenken aus datenschutzrechtlicher Sicht habe ich gegenüber der BfA im Hinblick auf die **weitere Verwendung** der von den Krankenkassen erhaltenen Informationen geäußert. Eine zweckändernde Speicherung, Veränderung und Nutzung wäre grundsätzlich unter den Voraussetzungen des § 67 c Abs. 2 SGB X möglich, der u. a. die Einwilligung des Betroffenen vorsieht.

Hierzu hat mir die BfA ausdrücklich versichert, daß die im Rahmen des AUD-Verfahrens übermittelten Daten der Krankenkassen von den ärztlichen Gutachtern und dem beratungsärztlichen Dienst der BfA ausschließlich für das Reha-Verfahren, und zwar für die Antragsbearbeitung, verwendet werden.

13.4 Verstoß gegen das Sozialgeheimnis durch das Sozialamt der Deutschen Bundespost

Ein Sanitätshaus hatte im Zusammenhang mit einer ärztlichen Verordnung für ein Hilfsmittel einen Kostenvoranschlag erstellt. Die Übernahme der darin enthaltenen Kosten wurden vom Sozialamt der Deutschen Bundespost abgelehnt, wobei als Begründung dem Sanitätshaus ein fachärztliches Gutachten über den Petenten übermittelt wurde.

Die Offenbarung des Gutachteninhaltes war für die Aufgabenerfüllung des Sozialamtes nicht erforderlich, da es ausgereicht hätte, dem Sanitätshaus mitzuteilen, daß eine Kostenübernahme nicht erfolgt. Das Vorgehen des Sozialamts der Deutschen Bundespost stellt daher einen Verstoß gegen das Sozialgeheimnis dar. Es hat mir zugesichert, daß derartige Datenübermittlungen in Zukunft unterbleiben werden.

14 Unfallversicherung

14.1 Datenschutzrechtliche Grundsatzprobleme der gesetzlichen Unfallversicherung

Die langjährige öffentliche Diskussion über Kostensteigerungen im Gesundheitswesen und über die Sicherheit der Renten führten zur vollständigen Neuregelung des Rechts der gesetzlichen Kranken- und Rentenversicherung im Fünften und Sechsten Buch des Sozialgesetzbuches.

In beiden Büchern wurden auf der Grundlage des Volkszählungsurteils des Bundesverfassungsgerichts auch bereichsspezifische Regelungen über die Erhebung, Nutzung und Verarbeitung von personenbezogenen Daten der jeweiligen Versicherten und Dritter

geschaffen und in einem eigenen Kapitel Datenschutz zusammengefaßt.

Die gesetzliche Unfallversicherung ist demgegenüber allenfalls mit Einzelthemen wie z. B. dem Problem der Interessengebundenheit der berufsgenossenschaftlichen ärztlichen Gutachter Gegenstand der publizistischen Erörterung. Trotz zahlreicher grundlegender Probleme auch in diesem Bereich ist es bislang noch zu keiner Novellierung des Rechts der gesetzlichen Unfallversicherung gekommen. Dies ist vor allem auch aus datenschutzrechtlicher Sicht zu bedauern. Die vom Bundesverfassungsgericht geforderte Gewährleistung des Grundrechts auf informationelle Selbstbestimmung durch bereichsspezifische Datenschutzregelungen steht in diesem Bereich der gesetzlichen Sozialversicherung damit noch immer aus.

Nach wie vor finden sich die Rechtsgrundlagen der gesetzlichen Unfallversicherung in der Reichsversicherungsordnung (RVO). Auch der Umgang mit personenbezogenen Daten von Versicherten, Mitgliedern und Dritten ist Gegenstand zahlreicher RVO-Vorschriften. Auf diese sowie die allgemeinen Verfahrensregelungen der §§ 3 ff. SGB X stützen sich im wesentlichen bis heute die Verwaltungsvorschriften, das Selbstverständnis und die Praxis der Unfallversicherungsträger hinsichtlich der Erhebung, Nutzung und Verarbeitung personenbezogener Daten. Die auch für die gesetzliche Unfallversicherung einschlägigen Datenschutzvorschriften der §§ 67 ff. SGB X spielen demgegenüber allzu häufig eine nachrangige Rolle.

Der Versicherungsschutz tritt unabhängig von anderweitigen Umständen allein durch die Erfüllung der gesetzlichen Voraussetzungen ein. Daraus ergibt sich für den zuständigen Unfallversicherungsträger die Verpflichtung, das Vorliegen oder Nichtvorliegen der Voraussetzungen seiner Haftung rechtsfehlerfrei und – im Interesse des Betroffenen – zeitnah von Amts wegen zu ermitteln. Da der Unfallversicherte nach geltendem Recht für den Zusammenhang zwischen Berufstätigkeit und Gesundheitsschaden i. S. der sogenannten haftungsbegründenden und haftungsausfüllenden Kausalität beweispflichtig ist, ermitteln die Unfallversicherungsträger auch sämtliche Umstände, die ihre Leistungspflicht ausschließen könnten. Dabei kommt es regelmäßig zu einem Austausch unterschiedlichster personenbezogener medizinischer und nicht-medizinischer Daten der Versicherten zwischen Arbeitgebern, Krankenkassen, behandelnden und früher behandelnden Ärzten einerseits und den Unfallversicherungsträgern andererseits sowie insbesondere mit den von ihnen beauftragten ärztlichen Gutachtern.

Das bisher nach Maßgabe der Amtsermittlungsgrundsätze (§§ 20, 21 SGB X) praktizierte Ermittlungsverfahren der Unfallversicherungsträger ist nach meinen Feststellungen in vielfacher, wenn auch unterschiedlicher Weise mit den Vorschriften und Grundsätzen des Sozialdatenschutzes unvereinbar. Dies ist im wesentlichen darauf zurückzuführen, daß die Unfallversicherungsträger den **grundsätzlichen Vorrang der** Vorschriften über den Sozialdatenschutz in den §§ 67 ff. SGB X und über die Mitwirkungsobliegenheiten und -ablehnungsrechte des betroffenen Versicherten in §§ 60 ff. SGB I, unter dem ihre von Amts wegen durchzuführende Ermittlungstätigkeit gemäß § 37 SGB I steht, nicht oder nur unzureichend beachten. Daraus ergeben sich insbesondere folgende datenschutzrechtlich nicht hinnehmbare Verfahrensschritte:

- Entgegen dem Grundsatz der Ersterhebung von Sozialdaten beim Betroffenen (§ 67 a Abs. 2 Satz 1 SGB X) werden medizinische und nicht-medizinische Daten ohne hinreichende Rechtsgrundlage und ohne Kenntnis oder Zustimmung des Betroffenen unmittelbar bei Ärzten und Krankenkassen erhoben. Dabei kann der durch § 203 StGB normierte Schutz der Patientendaten verletzt werden.
- Entgegen dem Grundsatz der Erforderlichkeit werden Sozialdaten für denselben Zweck bei verschiedenen Adressaten mehrfach erhoben, unabhängig davon, ob die zunächst erhobenen Daten unvollständig, widersprüchlich oder unrichtig sind und
- entgegen dem grundsätzlichen Verbot der Datenspeicherung auf Vorrat gespeichert und zur Information über mögliche Leistungsausschließungsgründe genutzt.
- Entgegen dem Erfordernis einer nach Adressat, Datenart und -umfang und jeweils verfolgtem Zweck hinreichend konkret formulierten Einwilligungs- oder Zustimmungserklärung werden insbesondere ärztliche Daten – wenn überhaupt – regelmäßig auf der Grundlage zu unbestimmter und daher unwirksamer Pauschalerklärungen der Betroffenen auf entsprechenden Vordrucken erhoben und übermittelt.
- Entgegen dem Transparenzgebot vergeben die Unfallversicherungsträger regelmäßig ärztliche Gutachtenaufträge unter Übermittlung der ihnen vorliegenden medizinischen Daten des Versicherten, ohne diesen über die Person des Gutachters aufzuklären (siehe oben 10.8.1).
- Entgegen dem grundsätzlich unbegrenzten Anspruch des Versicherten auf Auskunft aus und Einsicht in die über ihn beim Unfallversicherungsträger vorliegenden Sozialdaten (§§ 83, 25 SGB X), verweigern Unfallversicherungsträger
  - die Erteilung von Kopien der in ihrem Auftrag erstatteten ärztlichen Gutachten unter Berufung auf angebliche Urheberrechte der Verfasser,
  - die Einsichtnahme in den im Zusammenhang mit einem Arbeitsunfall des Versicherten erstellten Untersuchungsbericht des Technischen Aufsichtsdienstes der Berufsgenossenschaften unter Berufung auf Betriebs- und Geschäftsgeheimnisse des betroffenen Unternehmens.
- Entgegen den ausdrücklichen umfassenden gesetzlichen Hinweis –, Aufklärungs- und Beratungspflichten nach §§ 67 a Abs. 3, Abs. 4, 67 b und c Abs. 2, 76 Abs. 2 Nr. 1 SGB X und §§ 14, 66 Abs. 3 SGB I geben die Unfallversicherungsträger diese Hinweise und Erläuterungen zumeist unvollständig, häufig irreführend, jedenfalls aber in einer Weise, die es dem Versicherten nicht ermöglicht,

die tatsächlichen und rechtlichen Zusammenhänge so konkret wie möglich zu erfassen, um seine schutzwürdigen Interessen durch bewußte und gezielte Wahrnehmung seiner Verfahrensrechte gegenüber dem Unfallversicherungsträger wirksam verfolgen zu können.

Im Ergebnis führt dies dazu, daß der von den Unfallversicherungsträgern praktizierte Austausch von Sozialdaten der Versicherten ohne konkrete Kenntnis der tatsächlichen und rechtlichen Zusammenhänge erfolgt. Damit wird das Grundrecht auf informationelle Selbstbestimmung der in der gesetzlichen Unfallversicherung Versicherten in seinen beiden wesentlichen Ausprägungen ausgehöhlt:

Zum einen weiß der Versicherte nicht zu jedem Zeitpunkt des Verfahrens, wer was wann und zu welchem Zweck über ihn weiß oder erfahren soll, zum anderen kann er zu keinem Zeitpunkt des Verfahrens grundsätzlich selbst wirksam darüber entscheiden, ob und ggf. zum Austausch welcher seiner Sozialdaten es im Rahmen des Verwaltungsverfahrens kommt.

Hinzu kommt, daß das Verfahren zu Lasten der Betroffenen in Fällen unzumutbar ausgeweitet und verlängert wird, in denen die Unfallversicherungsträger medizinische Gutachter beauftragt haben, die von den Betrofffenen möglicherweise abgelehnt worden wären, wenn ihnen die Namen zum Zeitpunkt der Auftragsvergabe bekannt gewesen wären. Diese, die ursächlichen Voraussetzungen einer Rentenleistungspflicht der Unfallversicherungsträger zumeist verneinenden Gutachten führen sodann zu kosten- und zeitaufwendigen Rechtsstreitigkeiten – wenn die betroffenen Versicherten dazu finanziell in der Lage sind.

Diese datenschutzrechtlichen Mängel wirken sich für die Betroffenen deswegen vergleichsweise gravierend aus und erscheinen um so dringender revisionsbedürftig, als die materiellen und verfahrensrechtlichen Hürden bis zur Anerkennung von Berufsunfällen und Berufskrankheiten ohnehin außerordentlich hoch sind.

14.1.1 Unzulässige regelmäßige Mehrfacherhebung sämtlicher Vorerkrankungen von Unfallversicherten durch die Unfallversicherungsträger bei Ärzten, Krankenhäusern, Krankenkassen und Arbeitgebern

– Nach meinen Feststellungen fordern zahlreiche Unfallversicherungsträger in einem weitgehend übereinstimmenden Verfahren zeitgleich oder zeitnah, ggf. unabhängig vom Ergebnis entsprechender Befragungen des Versicherten selbst und der einzelnen weiteren Anfragen, behandelnde und früher behandelnde Ärzte oder Krankenhäuser, Krankenkassen und Arbeitgeber der Unfallversicherten zur Angabe sämtlicher Vorerkrankungen oder zur Übersendung vollständiger Patientenunterlagen auf; entsprechendes gilt für die Erhebung nicht-medizinischer Daten wie z. B. zu Zeitpunkt und Hergang von Unfällen.

Die Unfallversicherungsträger und der Hauptverband der Gewerblichen Berufsgenossenschaften (HVBG) berufen sich dabei auf ihre Verpflichtung, den Zusammenhang zwischen der beruflichen Tätigkeit und dem Gesundheitsschaden zeitnah zu klären. Da für die Zusammenhangsfrage auch Vorerkrankungen des Verletzten oder Kranken – positiv oder negativ – von Bedeutung sein könnten, seien diese Daten ohne Beteiligung des Versicherten unmittelbar bei behandelnden und früher behandelnden Ärzten oder Krankenhäusern, Krankenkassen und beim Arbeitgeber zu erheben. Während die Ärzte gemäß § 100 SGB X i. V. m. § 1543 d RVO insoweit angabepflichtig seien, ergebe sich dies für die Krankenkassen aus § 69 Abs. 1 SGB X i. V. m. § 1502 RVO und für den Arbeitgeber aus § 1543 c RVO.

Die dargestellte Praxis und Rechtsauffassung der Unfallversicherungsträger ist in mehrfacher Hinsicht mit datenschutzrechtlichen Vorschriften und Grundsätzen unvereinbar.

Das Verwaltungshandeln der Unfallversicherungsträger wird durch die datenschutzrechtlichen Regelungen der §§ 67 ff. SGB X begrenzt. Insbesondere das Amtsermittlungsprinzip steht unter dem Generalvorbehalt des Grundsatzes, daß Sozialdaten zunächst beim betroffenen Versicherten zu erheben sind (§ 37 SGB I i. V. m. § 67 a Abs. 2 Satz 1 SGB X); dieser ist verpflichtet, die erforderlichen Angaben zu machen oder der Erhebung bei Dritten zuzustimmen (§§ 60 Abs. 1, 66 Abs. 1 SGB I), wenn er nicht riskieren will, eine Leistung nicht zu erhalten oder sie zu verlieren (Mitwirkungsobliegenheit).

Zwar dürfen die Daten unter gewissen Voraussetzungen auch unmittelbar bei Dritten erhoben werden (§ 67 a Abs. 2 Satz 2 SGB X). Dies setzt jedoch voraus, daß „eine Rechtsvorschrift die Erhebung bei anderen Personen oder Stellen zuläßt oder die Übermittlung an die erhebende Stelle ausdrücklich vorschreibt".

Die von den Unfallversicherungsträgern praktizierte weite Auslegung der hier anzuwendenden Vorschriften der Reichsversicherungsordnung begründet beispielsweise die von mir kontrollierte Südwestliche Bau-Berufsgenossenschaft mit dem Satz: *„In der Sache ist diese weite Auslegung des § 1543 d RVO vernünftig und erleichtert und beschleunigt das Verwaltungsverfahren, was nicht zuletzt auch im Interesse des Verletzten liegt."* Bisher in manchen Fällen noch verwendete, von mir als unzureichend formuliert bewertete, vorgedruckte Einwilligungserklärungen für die Versicherten werde sie, *„... im Hinblick auf die von uns praktizierte weite Auslegung des § 1543 d RVO zukünftig nicht mehr anfordern, um den Versicherten nicht zu verunsichern."*

Eine derart weite Auslegung der genannten Vorschriften im Sinne der Unfallversicherungsträger verbietet sich schon aus verfassungsrechtlichen Gründen im Hinblick auf das Recht auf informationelle Selbstbestimmung. Hinzu kommt, daß Sinn und Zweck der genannten Vorschriften der RVO

zunächst nicht in erster Linie auf die Klärung der Leistungsvoraussetzungen im Rahmen des unfallversicherungsrechtlichen Feststellungsverfahrens zielen, sondern vorrangig die schnelle und sachgemäße Heilung des Unfallverletzten oder Erkrankten sicherstellen sollen. Hierzu sind die Unfallversicherungsträger gemäß § 556 Abs. 1 und § 557 Abs. 2 RVO verpflichtet. Dies bestätigt auch das zwischen den Unfallversicherungsträgern und ihren Verbänden mit der Kassenärztlichen Bundesvereinigung geschlossene sogenannte Ärzteabkommen. Dort heißt es in den „Grundsätzen" (Erster Teil) u. a.:

„(1) Die Träger der gesetzlichen Unfallversicherung sind nach den gesetzlichen Vorschriften verpflichtet, alle Maßnahmen zu treffen, durch die eine möglichst bald nach dem Arbeitsunfall einsetzende schnelle und sachgemäße Heilbehandlung ... gewährleistet wird ..."

Die dargestellte Erhebungspraxis der Unfallversicherungsträger ist daher mit § 67a Abs. 2 Satz 2 Nr. 2 SGB X i. V. m. § 1543 d RVO aus den dargelegten Gründen insoweit unvereinbar und rechtswidrig, als sie

- Informationen über sämtliche Vorerkrankungen und nicht-medizinische Informationen umfaßt und diese
- bei früher behandelnden Ärzten oder Krankenhäusern eingeholt werden.

Während sich die Unzulässigkeit der Erhebung bei früher behandelnden Ärzten eindeutig aus dem Wortlaut des § 1543 d RVO ergibt, gilt für die Erhebung von Vorerkrankungen im Rahmen der Information über den „Zustand des Verletzten" folgendes: Der behandelnde Arzt hat dem Unfallversicherungsträger den körperlichen und ggf. seelischen Status des Patienten aus seiner Sicht einschließlich Befunden und Diagnosen zu Beginn/Aufnahme und bei Entlassung aus dessen Behandlung mitzuteilen. Hierzu gehören ggf. medizinische Angaben über Vorerkrankungen, die sich auf die Zeit vor dem Unfall oder vor dem Beginn der Behandlung durch den behandelnden Arzt beziehen, wenn ihre Erwähnung erforderlich ist, um den aktuellen Status medizinisch vollständig zu beschreiben. Danach dürfen beispielsweise Vorerkrankungen nicht übermittelt werden, die mit dem aktuellen Status in keinem inneren und unmittelbaren Zusammenhang stehen oder aus Sicht des Arztes keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben. Derartige Informationen bedürfen – soweit erforderlich – der ausdrücklichen Zustimmung des Versicherten bzw. der Entbindung von der ärztlichen Schweigepflicht in einem gesonderten Verfahren.

Das Bundesversicherungsamt hat sich im Sinne meiner Bewertung geäußert und insbesondere festgestellt, daß medizinische Unterlagen oder Auskünfte, die sich auf die Zeit vor dem Unfall beziehen, von der Vorschrift des § 1543 d RVO nicht erfaßt werden.

- Da die Erhebung der für die Klärung der Haftungspflicht ggf. darüber hinaus erforderlichen Angaben über Vorerkrankungen bei Ärzten und Krankenhäusern gemäß § 67 a Abs. 2 Satz 1 i. V. m. § 60 Abs. 1 SGB I nur mit Einwilligung des Betroffenen (Befreiung von der ärztlichen Schweigepflicht), bei Krankenkassen nur zulässig ist, wenn die Versicherten vom Unfallversicherungsträger auf ihr Widerspruchsrecht gemäß § 76 Abs. 2 Nr. 1 SGB X hingewiesen wurden und von diesem keinen Gebrauch gemacht haben (vgl. hierzu Nr. 10.8), dies im Regelverfahren der Unfallversicherungsträger bisher aber nicht erfolgt ist, sind die dargestellten, seit Jahren praktizierten Erhebungen datenschutzrechtlich äußerst problematisch.

  Hinzu kommt, daß die Unfallversicherungsträger gegenüber den befragten Ärzten regelmäßig auch den nach § 67 a Abs. 4 SGB X verbindlich vorgesehenen Hinweis auf die Freiwilligkeit ihrer Angaben oder auf die Rechtsvorschrift, die zur Auskunft verpflichtet, unterlassen.

- Schließlich ist, unabhängig von den vorstehend dargelegten Rechtsmängeln, die zeitgleiche bzw. zeitnahe Mehrfacherhebung von Angaben zu sämtlichen Vorerkrankungen und zu Zeitpunkt und Hergang von Unfällen für sich genommen datenschutzrechtlich problematisch. Denn gemäß § 67 a Abs. 1 SGB X dürfen Sozialdaten von Unfallversicherungsträgern nur erhoben werden, wenn ihre Kenntnis zur Erfüllung einer Aufgabe der erhebenden Stelle erforderlich ist. Mehrfache Erhebungen zu demselben Sachverhalt bei unterschiedlichen Adressaten sind indessen nur dann erforderlich, falls bei der ersten Erhebung gar keine Angaben gemacht wurden, die Angaben unvollständig oder widersprüchlich waren oder sich Zweifel an der Richtigkeit ergeben. Der HVBG rechtfertigt die hiervon abweichende Praxis damit, daß bei Beginn eines Feststellungsverfahrens häufig noch nicht übersehen werden könne, welche Diagnosedaten zur Bearbeitung des konkreten Falles tatsächlich benötigt würden; bei vielen Erkrankungen spielten auch Medikamenteneinnahme und sonstiges Verhalten bei der Ursachenprüfung eine wesentliche Rolle. Damit räumt er ein, daß nach der gegenwärtigen Praxis der Unfallversicherungsträger zum Zeitpunkt der Erhebung noch nicht benötigte Daten erhoben werden. Dies ist mit § 67a Abs. 1 SGB X unvereinbar. Es handelt sich um eine unzulässige Datenerhebung auf Vorrat; die Praxis der Unfallversicherungsträger erhält damit den Charakter einer Ausforschung möglicher geeigneter Anhaltspunkte zur Ablehnung eines Leistungsanspruchs des Versicherten.

14.1.2 Unzulässige Zentraldatelen beim Hauptverband der gewerblichen Berufsgenossenschaften beanstandet

Im Berichtszeitraum habe ich den Hauptverband der gewerblichen Berufsgenossenschaften, die Spitzenorganisation der gewerblichen Berufsgenossenschaften, kontrolliert:

- Der HVBG verarbeitet u. a. die Sozialdaten, die er von seinen Mitgliedsberufsgenossenschaften erhält, in verschiedenen Zentraldateien. Hinsichtlich sämtlicher Zentraldateien gehe ich – im Gegensatz zum HVBG, aber mit dem BMA – davon aus, daß es sich um Dateien mit personenbeziehbaren Daten handelt; die Datensätze der übermittelnden Berufsgenossenschaften enthalten Namen und Adressen der Versicherten nicht. Die Personenbeziehbarkeit ergibt sich aber daraus, daß der HVBG mit Hilfe des ihm als Ordnungsbegriff übermittelten, berufsgenossenschaftlichen Aktenzeichens jederzeit ohne großen Aufwand bei der meldenden Berufsgenossenschaft den Namen des Versicherten abfordern kann.

  Eine gesetzliche Aufgabenzuweisung für den HVBG zur Führung solcher Zentraldateien gibt es nicht. Nach § 96 Abs. 3 Satz 2 SGB X sind hierzu – bei Vorliegen der übrigen Voraussetzungen – lediglich einzelne Träger der Unfallversicherung befugt, nicht jedoch deren Verbände. Ein rechtswirksames Vertragsverhältnis zur Führung dieser Dateien im Auftrage der Mitgliedsberufsgenossenschaften besteht ebenfalls nicht.

  Ich habe die Erhebung der Daten und deren anschließende Verarbeitung durch den HVBG mangels entsprechender Rechtsgrundlagen beanstandet. Hinsichtlich der sich hieraus ergebenden Folgerungen dauert die Disskussion mit dem HVBG und dem BMA derzeit noch an. Das BMA beabsichtigt, in dem Entwurf des SGB VII entsprechende Rechtsgrundlagen für die Führung bestimmter Zentraldateien durch die Verbände der Unfallversicherungsträger zu schaffen.

- Nach den Erfahrungen aus meinen Kontrollen empfehle ich nachdrücklich, auch die Verbände der Unfallversicherungsträger im Rahmen des für die neue Legislaturperiode vorgesehenen SGB VII einer Fach- und Rechtsaufsicht zu unterstellen. Eine solche Rechts- und Fachaufsicht, die sich an entsprechenden Modellen im Bereich der gesetzlichen Krankenversicherung orientieren könnte (Rechts- und Fachaufsicht des Bundesministeriums für Arbeit und Sozialordnung oder des Bundesversicherungsamtes), ist bisher gesetzlich nicht bestimmt (s. auch Nr. 14.1.3).

- Seit mehreren Jahren habe ich mit dem HVBG Gespräche über einen gemeinsamen Musterentwurf über Form und Inhalt von Einwilligungserklärungen der Versicherten und gesetzlich vorgesehene Hinweise an Versicherte und Dritte geführt, die im Rahmen eines unfallversicherungsrechtlichen Verwaltungsverfahrens erforderlich werden. Dabei wurde zwar über verschiedene allgemeine Grundsätze Übereinstimmung erzielt, in zwei entscheidenden Punkten bestehen aber Meinungsunterschiede:

  Hinsichtlich des Widerspruchsrechts des Versicherten gegen die Offenbarung von medizinischen Daten im Sinne des § 76 Abs. 2 Nr. 1 SGB X im Zusammenhang mit der Vergabe medizinischer Gutachtenaufträge will es der Hauptverband auch in Fällen mehrjähriger Verfahren beim gesetzlich vorgeschriebenen allgemeinen Hinweis zu Beginn des Verwaltungsverfahrens belassen. Ich halte es wegen der verbreiteten Interessengebundenheit vieler bisher in unfallversicherungsrechtlichen Verfahren eingesetzten medizinischen Gutachter gerade in diesem Bereich der Sozialversicherung für dringend geboten, daß dem Versicherten die Namen der in Betracht gezogenen oder des vorgesehenen Gutachters vor der Auftragsvergabe genannt werden; denn anders kann er von seinem Recht, Gutachter aus wichtigem Grunde, z. B. wegen Befangenheit, abzulehnen (§ 65 SGB I) und der Übersendung seiner beim Unfallversicherungsträger vorhandenen medizinischen Unterlagen zu widersprechen, kaum Gebrauch machen. Ohne eine derartige Vorinformation bliebe dem Unfallversicherten nur die Möglichkeit, seine Rechte durch einen pauschalen Widerspruch „ins Blaue hinein" zu wahren. Dies könnte zum einen zu Verfahrensverzögerungen führen. Zum anderen werden die meisten Versicherten diesen Weg deswegen scheuen, weil sie in den entsprechenden Erläuterungsvordrucken auf ihre Mitwirkungspflicht und darauf hingewiesen werden, daß ihnen die Leistung bei fehlender oder verweigerter Mitwirkung entzogen werden kann. Hinweise auf die Grenzen der Mitwirkungspflicht nach Maßgabe des § 65 SGB I erhalten sie jedenfalls in diesem Zusammenhang teilweise nicht.

  Ich werde das Gespräch mit dem HVBG weiterhin fortsetzen, mich aber zugleich auch insoweit um eine datenschutzgerechte, bereichsspezifische Regelung im SGB VII bemühen. Bis dahin kann den Unfallversicherten nur empfohlen werden, den Namen des vorgesehenen Gutachters zu erfragen. Denn die von mir bisher darauf angesprochenen Unfallversicherungsträger haben es abgelehnt, wenigstens dem Beispiel der Bundesversicherungsanstalt für Angestellte zu folgen, die den Versicherten im Reha-Verfahren die Auswahl des ärztlichen Gutachters aus einer Liste selbst überläßt oder im Rentenverfahren schriftlich darauf hinweist, Namen von Ärzten benennen zu können, von denen sie nicht untersucht werden wollen.

14.1.3 Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum SGB VII

Das Bundesministerium für Arbeit und Sozialordnung hat inzwischen den Referentenentwurf eines Unfallversicherungsneuregelungsgesetzes (SGB VII) vorgelegt. Bereits ein erstes Gespräch über den Vorentwurf hat gezeigt, daß dieser den datenschutzrechtlichen Anforderungen nicht gerecht wurde. Es erscheint insbesondere geboten, das gesamte unfallversicherungsrechtliche Verwaltungsverfahren einschließlich seiner rechtlichen Grundlagen einer eingehenden datenschutzrechtlichen Prüfung zu unterziehen. Wegen der besonderen Bedeutung des SGB VII hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hierzu am 9. März 1995 eine Entschließung gefaßt, die ich der Aktualität halber und abweichend vom Redaktionsschluß als Anlage 23 wiedergebe.

14.2 Kontrolle der Bundesausführungsbehörde für Unfallversicherung

Im Mittelpunkt der Kontrolle standen die problematischen Mehrfacherhebungen medizinischer und nichtmedizinicher Versichertendaten bei verschiedenen Adressaten und der dabei verwendeten Vordrucke. Diese sind in vielen Punkten verbesserungsbedürftig.

Ebenso wie die meisten gewerblichen Berufsgenossenschaften erhebt die BAfU mit entsprechenden Vordrucken Angaben zu Vorerkrankungen bei behandelnden und früher behandelnden Ärzten sowie Krankenkassen und Arbeitgebern der Versicherten und stützt dies auf §§ 1502, 1543 c und d RVO. Dies habe ich ebenso problematisiert wie das regelmäßige Fehlen oder die Unvollständigkeit der Hinweise an die Versicherten oder Dritte gemäß § 67a Abs. 3 und 4 SGB X sowie nach § 76 Abs. 2 Nr. 1 SGB X auf das Widerspruchsrecht gegenüber der angefragten Krankenkasse (Nr. 14.1.1)

Die BAfU hat mir zugesagt, ihr Verfahren entsprechend meinen Empfehlungen zu ändern und die Vordrucke an die gesetzlichen Anforderungen anzupassen. Sie wird medizinische Informationen auf der Grundlage des § 1543 d RVO nur noch bei behandelnden Ärzten und nur in dem danach zulässigen Umfang erheben, bei früher behandelnden Ärzten nur noch mit Schweigepflichtentbindungserklärung des Versicherten und unter Hinweis auf die Freiwilligkeit ihrer Angaben.

Auch den bei der Erhebung medizinischer Informationen bei den Krankenkassen der Versicherten verwendeten Vordruck wird die BAfU umformulieren. Auf die Anforderung kompletter Vorerkrankungsverzeichnisse soll verzichtet und mitgeteilt werden, daß der Versicherte auf sein Widerspruchsrecht gemäß § 76 Abs. 2 Nr. 1 SGB X hingewiesen worden ist.

Die BAfU stimmt mit mir darin überein, daß in den Fällen, bei denen sich der genaue Unfallhergang weder aus der Unfallanzeige noch dem Durchgangsarztbericht erschließt, eine Mehrfacherhebung medizinischer und nicht-medizinischer Informationen oder sogar ergänzende Rückfragen beim Versicherten unumgänglich sein können, wenn keine oder unvollständige oder widersprüchliche oder anscheinend unrichtige Antworten gegeben werden. Darüber hinaus hält sie aber ihr bisheriges Verfahren der Mehrfacherhebung unabhängig hiervon für sachgerecht. Sie stellt dabei darauf ab, daß der Unternehmer in der Unfallanzeige eigene Angaben über den Unfallhergang mache, wodurch sich die Unfallanzeige wesentlich von dem Durchgangsarztbericht unterscheide, in dem lediglich Auskünfte des Versicherten wiedergegeben werden. Hinzu komme, daß die Unfallanzeige Grundlage für statistische Erhebungen sei, mit deren Hilfe die Ursachen von Unfällen erkannt und in der Folgezeit wirksame Unfallverhütungsmaßnahmen getroffen werden sollten. Nach dem zur Zeit geltenden Recht der RVO seien die Unternehmer zur Erstattung der Unfallanzeige verpflichtet; solange dieses Recht gelte, sei sie gehalten, die Unfallanzeige auch weiterhin zu ihren Akten zu nehmen.

Die Ausführungen der BAfU zur formalen Rechtsverbindlichkeit der unfallversicherungsrechtlichen Vorschriften über die Unfallanzeige des Unternehmers sind zutreffend. Die darüber hinausgehenden Ausführungen zur Erforderlichkeit der Mehrfacherhebung von Informationen zum Unfallzeitpunkt und -hergang überzeugen dagegen nicht. Denn in die Unfallanzeige des Unternehmers fließen auch die Angaben des unfallverletzten Versicherten ein. Da diese Angaben, soweit sie vom Unternehmer in der Unfallanzeige übernommen und ggf. ergänzt und vom Personal- bzw. Betriebsrat mitgetragen werden, der die Anzeige mit unterzeichnen muß, werden sie in ihrer inhaltlichen Aussage so entscheidend objektiviert, daß weitere Erhebungen beim Versicherten nur in Ausnahmefällen unvollständiger oder widersprüchlicher Angaben erforderlich werden können.

14.3 Berufsgenossenschaft der chemischen Industrie

In einem Berufskrankheitenfeststellungsverfahren hatte ein bei der BG Chemie versicherter Petent seinen bei einer anderen BG beschäftigten Schwager mit der Durchführung einer Akteneinsicht beauftragt und entsprechend bevollmächtigt.

Der Bevollmächtigte bat die BG Chemie schriftlich, ihm die Verwaltungsakten zu übersenden. Die Übersendung erbat er an die Adresse seines Arbeitgebers, aber mit dem ausdrücklichen Zusatz „persönlich".

Die BG Chemie hat das Schreiben des Bevollmächtigten per Telefax dessen Arbeitgeber übersandt. Dies hat sie damit begründet, sie habe klären wollen, ob die beantragte Akteneinsicht durch den Arbeitgeber des Petenten durchgeführt werden sollte. Aus der Bitte des Bevollmächtigten, ihm die Akten persönlich zu übersenden war aber zu folgern, daß er die Einschaltung seines Arbeitgebers zum Zwecke der Durchführung der Akteneinsicht nicht wünschte.

Durch die Übermittlung des Schreibens des Bevollmächtigten an seinen Arbeitgeber wurde dieser darüber informiert, daß einer seiner Mitarbeiter als Bevollmächtigter in einem Verwaltungsverfahren gegenüber einer anderen Berufsgenossenschaft fungiert.

Die BG Chemie hat sowohl mir als auch gegenüber dem vom Petenten in die Angelegenheit ebenfalls eingeschalteten Bundesversicherungsamt, das meine datenschutzrechtliche Bewertung teilt, deutlich gemacht, bei künftigen, gleichgelagerten Sachverhalten in gleicher Weise vorgehen zu wollen. Insbesondere im Hinblick auf die sich hieraus ergebende Wiederholungsgefahr habe ich die Vorgehensweise der BG Chemie als Verstoß gegen das Sozialgeheimnis (§ 35 SGB I) beanstandet.

14.4 BergbauBG: Vorbildliches Verfahren bei der Ersterhebung erreicht

Aufgrund einer Eingabe, die Vorgänge im Jahre 1985 betraf, habe ich festgestellt, daß die BergbauBG ohne Mitwirkung des Betroffenen bei seiner Krankenkasse, der Bundesknappschaft, im Rahmen des

Berufskrankheiten-Feststellungsverfahrens Beschäftigungsnachweise, eine über den Petenten geführte komplette Akte und Ablichtungen des Vorerkrankungsverzeichnisses übermittelt bekommen hatte. Dies verstieß schon damals gegen den Grundsatz der Ersterhebung beim Betroffenen.

Die BergbauBG hat mir abschließend mitgeteilt, daß sie künftig – dem Ersterhebungsgrundsatz entsprechend – die z. B. für ein Berufskrankheiten-Feststellungsverfahren erforderlichen Daten zunächst allein beim Versicherten erheben werde. Nur in den Fällen, in denen die BG vom Versicherten innerhalb einer ihm gesetzten angemessenen Frist keine hinreichenden Auskünfte erhalte, werde sie im dann noch erforderlichen Umfang gezielte Anfragen an die Bundesknappschaft richten.

Die Bundesknappschaft, deren jeweilige Offenbarungen wegen Verstoßes gegen den Ersterhebungsgrundsatz seitens der Bergbau-BG nicht erforderlich und daher nach § 69 Abs. 1 Nr. 1 SGB X ebenfalls unzulässig waren, hat mir das von der BergbauBG dargestellte neue Verfahren im einzelnen bestätigt. Hinsichtlich der künftigen Übermittlung von Informationen über Vorerkrankungen hat sie hervorgehoben, daß die BergbauBG der Bundesknappschaft künftig genau mitteilen müsse, welche Vorerkrankungen oder Diagnosen im Rahmen des jeweiligen Feststellungsverfahrens von ihr benötigt werden. Nur diese Daten werde die Bundesknappschaft dann auch übermitteln. Komplette Auszüge aus den Leistungsunterlagen werde die Bundesknappschaft aus den von mir dargelegten datenschutzrechtlichen Gründen in Zukunft auf Anfrage anderer Stellen grundsätzlich nicht mehr zur Verfügung stellen.

Die BergbauBG hat damit als bisher einzige gewerbliche Berufsgenossenschaft ihr Verwaltungsverfahren entsprechend meinen und den Empfehlungen des Bundesversicherungsamts in datenschutzgerechter Weise umgestellt. Ich habe dieses beispielhafte Ergebnis daraufhin zum Anlaß eines Rundschreibens an alle gewerblichen Berufsgenossenschaften genommen und um künftige Beachtung gebeten.

Leider vertritt der HVBG die Auffassung, daß das zwischen mir und der BergbauBG vereinbarte künftige Vorgehen allenfalls als spezielle Verfahrensweise zu betrachten sei, die sich durch die Besonderheiten der Beziehungen der BergbauBG zur Bundesknappschaft ergebe. Die datenschutzrechtlichen Verfahrensvorgaben würden jedoch den Notwendigkeiten des Berufskrankheiten-Feststellungsverfahrens bei den gewerblichen Berufsgenossenschaften insgesamt nicht gerecht (vgl. im einzelnen Nr. 14.1.1). Ich bedauere dies um so mehr, als der Bundesminister für Arbeit und Sozialordnung die Auffassung des HVBG im wesentlichen stützt. Der BMA hält insbesondere den Ersterhebungsgrundsatz bei der Erhebung von Vorerkrankungen im Berufskrankheiten-Feststellungsverfahren für ungeeignet, er hat mir hierzu jedoch Gespräche angeboten.

Das Problem wird im Rahmen des Gesetzgebungsverfahrens zum SGB VII ausführlich erörtert und einer datenschutzgerechten Lösung zugeführt werden müssen.

14.5 Daten über Rauchgewohnheiten von Arbeitnehmern in der ehemaligen DDR dürfen von den Unfallversicherungsträgern nicht zum Ausschluß von Leistungsansprüchen herangezogen werden

Das Bundesversicherungsamt hat gemäß §§ 7 und 5 des Gesetzes zur Regelung von Vermögensfragen der Sozialversicherung im Beitrittsgebiet (SVVermG) den gewerblichen Berufsgenossenschaften Akten, Dateien und Archive aus dem Vermögen des Gesundheitswesens Wismut zugewiesen. Darin sind insbesondere Gesundheitsdaten der ehemaligen und noch beschäftigten Arbeitnehmer der Wismut enthalten. In einem Erweiterungsbescheid vom Juli 1994 hat sie diesen Berufsgenossenschaften weitere Akten, Dateien und Archive zugewiesen, die sich auf alle anderen Berufskrankheiten beziehen.

Da die in den vorgenannten Unterlagen enthaltenen sog. Confounder-Daten (Rauchgewohnheiten u. ä.) bei der Entscheidung über eine unfallversicherungsrechtliche Leistungspflicht in der ehemaligen DDR nicht berücksichtigt wurden, habe ich mich dafür eingesetzt, daß derartige Daten – insbesondere über Rauchgewohnheiten – entweder von der Übermittlung an die Berufsgenossenschaften ausgenommen werden oder ihre künftige Nutzung für die gesetzlichen Aufgaben der Berufsgenossenschaften entsprechend eingeschränkt wird. Das Bundesversicherungsamt hat daraufhin – auch in Übereinstimmung mit dem HVBG – die künftige Verwertung der Confounder-Daten, insbesondere der erfaßten Angaben zu Rauchergewohnheiten, auf Forschungs- und Vorsorgezwecke beschränkt.

15 Verteidigung

15.1 Gerichtsbeschluß schränkt Gebot zur Löschung unzulässiger Daten auf den Wehrstammkarten der ehemaligen NVA ein

Das Bundesministerium der Verteidigung beabsichtigte, entsprechend der Empfehlung des Deutschen Bundestages die Datenfelder auf den **Wehrstammkarten** der ehemaligen NVA, die für die Durchführung der Aufgaben der Bundeswehr nicht erforderlich sind, immer dann zu löschen, wenn eine Wehrstammkarte im Zusammenhang mit der Bearbeitung eines Vorgangs vorgelegt wird (s. BT-Drs. 12/4094 S. 3 Nr. 3 und 14. TB S. 27 f.).

Die Löschungen unterblieben jedoch, weil das Amtsgericht Berlin-Tiergarten wenig später die Beschlagnahme der „in der Wehrbereichsverwaltung VII ... befindlichen Personalunterlagen (sogenannte „Kaderakten") von Angehörigen des ehemaligen Ministeriums für Nationale Verteidigung der früheren DDR" anordnete. Damit sollte Beweismaterial gegen Personen gesichert werden, die im Verdacht stehen, an der Errichtung und Erhaltung des sog. „Grenzregimes" mitgewirkt zu haben und somit strafrechtlich für die Gewalttaten an der innerdeutschen Grenze und der Berliner Mauer verantwortlich zu sein. Der Beschluß des Amtsgerichts untersagte u. a. ausdrücklich, daß Teile der Daten in den beschlagnahm-

ten Unterlagen unleserlich gemacht werden. Das BMVg sah sich dadurch gehindert, der Aufforderung des Deutschen Bundestages nachzukommen.

Daraufhin hatte ich gegenüber dem BMVg Bedenken geäußert und um Klärung gebeten, ob der Beschluß des Amtsgerichts Berlin-Tiergarten die Personalunterlagen **aller** früheren Soldaten der ehemaligen NVA umfaßt, also auch die solcher Personengruppen, die niemals Dienst in den Einheiten der ehemaligen Grenztruppen geleistet hatten (z. B. Bausoldaten) und die deshalb mit Sicherheit nicht im Zusammenhang mit Vorfällen an der innerdeutschen Grenze und an der Berliner Mauer gebracht werden können. Nach entsprechender Initiative des BMVg hat die zuständige Staatsanwaltschaft beim Kammergericht den vom Beschlagnahmebeschluß betroffenen Personenkreis insoweit eingeschränkt, daß künftig die unzulässigen Daten auf den Wehrstammkarten folgender konkret benannter Personengruppen entsprechend dem Beschluß des Deutschen Bundestages geschwärzt werden können:

- Bausoldaten,
- ungediente Wehrpflichtige, soweit sie nicht Zivilbeschäftigte des Ministerium für Nationale Verteidigung waren,
- Angehörige der Zivilverteidigung, der Transportpolizei und der Bereitschaftspolizei,
- Mannschaftsdienstgrade der NVA, bei denen zweifelsfrei feststeht, daß sie zu keiner Zeit in den Grenztruppen/der Grenzpolizei, der 6. Grenzbrigade Küste oder im Ministerium für Nationale Verteidigung Dienst getan haben,
- Dienende und Reservisten, die nach dem 3. Oktober 1990 zum Wehrdienst einberufen wurden.

Das BMVg hat mir mitgeteilt, daß die Dienststellen der Wehrbereichsverwaltung VII angewiesen sind, entsprechend der Entscheidung der Staatsanwaltschaft beim Kammergericht zu verfahren. Bei den im Bundesamt für den Zivildienst vorhandenen Wehrstammkarten (vgl. 14. TB S. 28 Nr. 2.8.2) werden die in Frage stehenden Datenfelder in gleicher Weise geschwärzt.

15.2 Tonbandkassetten mit Diktataufzeichnungen aus einem Kreiswehrersatzamt an private Dritte gelangt

Ein Journalist machte mich auf einen besonders schwerwiegenden Verstoß gegen das Persönlichkeitsrecht von Bürgern aufmerksam. Er übergab mir drei **Tonbandkassetten** mit Diktataufzeichnungen aus Verfahren vor einem **Ausschuß für Kriegsdienstverweigerung** mit zum Teil sensiblen Daten aus der Privat- und Intimsphäre der Betroffenen.

Wie meine Nachforschungen ergaben, waren die Tonbandkassetten im Zusammenhang mit der Veräußerung eines ausgesonderten Diktiergerätes durch eine Verwertungsgesellschaft an einen Händler und von dort an den Informanten des Journalisten gelangt. Der Händler hatte das Gerät mit der von der Verwertungsgesellschaft ausgestellten Abholvollmacht bei einer **Standortverwaltung der Bundeswehr** abgeholt und dort zusätzlich als „Beigabe" die drei Tonbandkassetten erhalten. Im Laufe meiner Untersuchung übersandte mir das Bundesamt für den Zivildienst, das mich ebenso wie das Bundesministerium der Verteidigung bei meinen Recherchen unterstützte, zwei weitere Tonbandkassetten aus dem Bestand desselben Händlers. Diese Tonbandkassetten enthielten Diktataufzeichnungen über Berufsförderungsangelegenheiten von Zeitsoldaten. Die Datenträger hatten sich in zwei weiteren Diktiergeräten im Besitz des Händlers befunden.

Alle fünf Datenträger stammten aus demselben Kreiswehrersatzamt, das die Geräte zur Aussonderung und Verwertung an die zuständige Standortverwaltung gegeben hatte. Nicht erst die Standortverwaltung, sondern bereits das Kreiswehrersatzamt als speichernde Stelle, war verpflichtet gewesen, die auf den Tonbandkassetten aufgezeichneten Daten zu löschen, sobald sie abgeschrieben waren. Die Speicherung der Daten war mit Wegfall dieser Zweckbestimmung unzulässig geworden. Ebenso unzulässig war die Weitergabe der auszusondernden Datenträger mit den personenbezogenen Daten. Sie widersprach insbesondere dem Einführungserlaß des Bundesministeriums der Verteidigung zum Bundesdatenschutzgesetz, der die Vernichtung von Datenträgern anordnet, die – wie hier – nicht an das Bundesarchiv abzugeben sind.

Ich habe die Nichtbeachtung der Löschungsverpflichtung und die unzulässige Datenübermittlung wegen Verstoßes gegen die §§ 4 Abs. 1, 12 Abs. 4 und 35 Abs. 2 Satz 2 Nrn. 1 und 3 BDSG beanstandet.

Das Bundesministerium der Verteidigung hat meine Bewertung des Vorgangs geteilt. Es hat mich unterrichtet, die nachgeordneten Dienststellen ausdrücklich angewiesen zu haben, Tonbänder und Kassetten zu löschen, sobald die endgültige Niederschrift der Aufnahme vorliegt. Ebenso hat es die Vernichtung der Datenträger angeordnet, wenn sie ausgesondert werden.

Der Fall macht deutlich, daß es trotz klarer datenschutzrechtlicher Regelungen immer wieder zu Verletzungen der Persönlichkeitsrechte der Bürger kommen kann, wenn durch Verwaltungsroutine die erforderliche Aufmerksamkeit beim Umgang mit personenbezogenen Daten nachläßt. Die Erfahrungen aus Beratungs- und Kontrollbesuchen meiner Mitarbeiter haben gezeigt, daß dieses Risiko durch regelmäßige Schulungen der Mitarbeiter und wiederholte Hinweise auf die einschlägigen Vorschriften erheblich verringert wird.

16 Zivildienst

16.1 Die Prüfkompetenz des BfD erstreckt sich auch auf Einrichtungen der Kirchen, soweit sie Aufgaben des Zivildienstes wahrnehmen

Die den Zivildienst tragenden Wohlfahrtsverbände haben – ähnlich den Wehrersatzverwaltungen der Bundeswehr – Verwaltungsstellen gemäß § 5a Zivildienstgesetz (ZDG) eingerichtet. Diese Stellen führen

auf der Grundlage öffentlich-rechtlicher Verträge Verwaltungsaufgaben durch, wie z. B. Fürsorge und Betreuung der Zivildienstleistenden oder auch Beratung der Stellen, die Zivildienstleistende beschäftigen. Die Durchführung dieser Aufgaben erfolgt nach Richtlinien des Bundesministeriums für Familie, Senioren, Frauen und Jugend und des Bundesamts für den Zivildienst (BAZ).

Im Vorfeld eines Kontroll- und Beratungsbesuchs bei einer **Verwaltungsstelle Zivildienst** des Diakonischen Werks Württemberg e.V. ergaben sich zwischen dem Beauftragten für Datenschutz der Evangelischen Landeskirche in Württemberg und mir unterschiedliche Rechtsansichten über mein Kontrollrecht gegenüber einer kirchlichen Einrichtung, die Zivildienstaufgaben des Bundes wahrnimmt.

Bei den auf der Grundlage des § 5 a ZDG eingerichteten Verwaltungsstellen Zivildienst im Bereich der Kirchen und Verbände der Freien Wohlfahrtspflege handelt es sich nach meiner Auffassung um sogenannte beliehene Unternehmer. Der diesen Stellen vertraglich zugewiesene Tätigkeitsrahmen umfaßt **ausschließlich** staatliche Aufgaben aus dem Zuständigkeitsbereich des BAZ. Als beliehene Unternehmer sind die Verwaltungsstellen Zivildienst öffentliche Stellen des Bundes nach § 2 Abs. 4 Satz 2 BDSG und unterliegen somit meiner Kontrolle nach § 24 Abs. 1 BDSG.

Der Beauftragte für Datenschutz der Evangelischen Landeskirche in Württemberg hält dagegen das Bundesdatenschutzgesetz hier nicht für anwendbar; Kirchen und ihre Verbände seien keine öffentlichen Stellen im Sinne des § 2 Abs. 4 Satz 2 BDSG. Er begründet seine Rechtsauffassung mit Artikel 140 des Grundgesetzes in Verbindung mit den dort genannten Artikeln der Deutschen Verfassung vom 11. August 1919 (Weimarer Reichsverfassung), insbesondere Artikel 137 Abs. 3, der das kirchliche Selbstverwaltungsrecht garantiert.

Diese Bewertung hat mich nicht überzeugt. Ich habe jedoch – einen pragmatischen Vorschlag des Beauftragten für Datenschutz der Evangelischen Landeskirche in Württemberg aufgreifend – das (frühere) BMFJ gebeten, in den Vertrag mit dem Diakonischen Werk der Evangelischen Kirche Württemberg zur Klarstellung eine Regelung über meine Kontrollzuständigkeit aufzunehmen. Das BMFJ hat die Bundesarbeitsgemeinschaft der Freien Wohlfahrtspflege wegen einer entsprechenden Ergänzung des Vertrags angeschrieben.

Das Ergebnis dieser Bemühungen steht noch aus.

16.2 Verbesserte Unterrichtung der Kriegsdienstverweigerer über Datenspeicherung

Durch eine Eingabe wurde ich darauf aufmerksam gemacht, daß Wehrpflichtige, die einen Antrag auf Anerkennung als Kriegsdienstverweigerer beim Kreiswehrersatzamt gestellt hatten, über die Speicherung ihrer personenbezogenen Daten beim Bundesamt für den Zivildienst (BAZ) erst mit zwei- bis dreimonatiger Verzögerung informiert wurden.

Wehrpflichtige, die als Kriegsdienstverweigerer anerkannt werden wollen, müssen nach § 2 Abs. 2 Kriegsdienstverweigerungsgesetz (KDVG) einen Antrag beim Kreiswehrersatzamt stellen. Sobald sie gemustert sind und der Musterungsbescheid unanfechtbar geworden oder über ihn rechtskräftig entschieden ist, leitet das Kreiswehrersatzamt den Antrag mit den Personalunterlagen des Wehrpflichtigen an das BAZ weiter. Gleichzeitig werden im Wege des Datenträgeraustauschs die über den Wehrpflichtigen elektronisch gespeicherten Daten an das BAZ übermittelt. Dieses entscheidet anschließend über den Antrag; mit der Übersendung des Bescheides tritt es zum ersten Mal mit dem Betroffenen in Kontakt. Erst zu diesem Zeitpunkt erfuhr der Betroffene bisher durch ein dem Bescheid beigefügtes Merkblatt von der Speicherung seiner Daten beim BAZ.

Meine Bedenken gegen dieses bis dahin praktizierte Verfahren hat das BAZ zum Anlaß genommen, in Absprache mit der Bundeswehrverwaltung für eine pragmatische Lösung des Problems zu sorgen. Seither fügen bereits die Kreiswehrersatzämter ihren Abgabenachrichten an den Wehrpflichtigen ein Merkblatt bei, das ausführlich über die im BAZ erfolgende Verarbeitung seiner personenbezogenen Daten informiert.

17 Gesundheitswesen

17.1 Was lange währt – das Krebsregistergesetz ist in Kraft getreten

Das Krebsregistergesetz ist am 1. Januar 1995 in Kraft getreten. Für das zugleich außer Kraft getretene Gesetz zur Sicherung und vorläufigen Fortführung der Datensammlung des „Nationalen Krebsregisters" der ehemaligen Deutschen Demokratischen Republik – Krebsregistersicherungsgesetz – (s. Nr. 17.2) wurde damit die Folgeregelung getroffen, die eine sinnvolle Fortsetzung und Nutzung der geleisteten Arbeit ermöglicht. Das Gesetz sieht die Einführung von bevölkerungsbezogenen Krebsregistern vor, die aus selbständigen, räumlich, organisatorisch und personell voneinander getrennten Vertrauensstellen und Registern bestehen (ausführlich hierzu s. 14. TB S. 103).

Nachdem der Bundesrat den Vermittlungsausschuß angerufen hatte, war lange Zeit unklar, ob das Krebsregistergesetz zustande kommen würde. Schließlich wurde ein Kompromiß gefunden, der auch aus datenschutzrechtlicher Sicht tragbar ist. Insgesamt sieht das Gesetz allerdings vor, daß die Länder sehr weitgehende Möglichkeiten haben, durch eigene Gesetze abweichende Regelungen zu treffen. Dies gilt auch für die im 14. TB beschriebenen Vorschriften für die Gewährleistung der Persönlichkeitsrechte des Patienten. So können die Länder die Voraussetzungen der Meldung zum Krebsregister und das Meldeverfahren abweichend vom Krebsregistergesetz des Bundes regeln. Dies bedeutet, daß statt der vorgesehenen Meldeberechtigung auch eine Pflicht zur Meldung von Krebserkrankungen für Ärzte und Zahnärzte eingeführt werden oder daß das Recht des Pa-

tienten, der Meldung seiner Daten zu widersprechen, eingeschränkt werden kann. Unter der Maßgabe, daß eine regelmäßige Abgleichung der gemeldeten Daten mit den Daten der Krebsregister der anderen Länder erfolgen kann und daß die Daten für Maßnahmen des Gesundheitsschutzes und der epidemiologischen Forschung genutzt werden können, haben die Länder die Möglichkeit, die Erhebung und Verarbeitung der Daten anders zu regeln, als im Krebsregistergesetz vorgesehen ist.

17.2 Das Gemeinsame Krebsregister

Das Gesetz zur Sicherung und vorläufigen Fortführung der Datensammlung des „Nationalen Krebsregisters" der ehemaligen Deutschen Demokratischen Republik – Krebsregistersicherungsgesetz – (14. TB S. 29) wurde durch das Krebsregistergesetz des Bundes (s. o. Nr. 17.1) abgelöst. Damit wurde eine sinnvolle Fortsetzung und Nutzung der geleisteten Arbeit ermöglicht.

Anläßlich einer datenschutzrechtlichen Kontrolle beim Robert-Koch-Institut habe ich mich über den Umgang mit den personenbezogenen Daten bei der Aufarbeitung des „Nationalen Krebsregisters" und der Fortführung dieser Datensammlung als Gemeinsames Krebsregister der neuen Bundesländer informiert. Die im Gesetz vorgesehenen Arbeiten wie Trennung der Registerangaben von den identifizierenden Daten und Übernahme von nur auf Karteikarten vorliegenden Angaben in automatisierte Verfahren waren im wesentlichen abgeschlossen. Datenschutzmängel habe ich nicht festgestellt.

17.3 Gesundheitsdaten auf der Chipkarte – viele Fragen noch ungelöst

Die Diskussionen über die zukünftige Struktur der Verarbeitung von Gesundheitsdaten und den Schutz der Patienten vor der mit jedem Zugriff auf diese Daten verbundenen Offenlegung sind seit Einführung der Krankenversichertenkarte sprunghaft angestiegen. Dabei hat sich gezeigt, daß es durchaus sachgerecht war, die Datenspeicherung auf der Krankenversichertenkarte und ihre Nutzung gesetzlich eng zu begrenzen und diese Begrenzung durch besondere Maßnahmen zu gewährleisten (s. auch Nr. 12.4). Bis jetzt sind zu viele Fragen offen, als daß man den Einsatz von Chipkarten als Träger von Gesundheitsinformationen über seinen Inhaber generell empfehlen könnte. Und auch die Alternative, über die Chipkarte des Patienten den Zugang zu diesen Informationen über ein Computernetz zu eröffnen, ist nicht hinreichend ausdiskutiert. Bei der Lösung dieser Fragen ist Eile geboten. Denn die Technik dazu ist nicht nur im Prinzip verfügbar, sondern mit vielen Millionen von Karten und Tausenden von Lesegeräten in den Praxen bereits eingeführt. Zugleich werden von interessierten Verbänden, Gruppen und Unternehmen Versuche mit Gesundheitsdatenkarten geplant oder schon durchgeführt.

Zu den jetzt erkennbaren offenen Problemen gehören insbesondere:

- Die Gesundheitsdaten, die auf einer Karte im Besitz des Betroffenen gespeichert sind, unterliegen dort nicht der ärztlichen Schweigepflicht. Das Recht des Patienten an diesen Daten wäre nicht nur durch Diebstahl gefährdet, sondern auch durch eine zulässige Beschlagnahme nach der Strafprozeßordnung. Und nach dem Wortlaut der entsprechenden zivilrechtlichen Vorschriften unterläge die Karte sogar dem Vermieterpfandrecht.

- Die besondere Pflicht, die zum persönlichen Lebensbereich der Betroffenen gehörenden Geheimnisse zu wahren (§ 203 Abs. 1 StGB), gilt derzeit nicht für den Betreiber eines Computernetzes, über das Gesundheitsdaten bei Bedarf zur Verfügung gestellt werden sollen, und auch nicht für seine Mitarbeiter.

- Die Daten müssen gegen unberechtigten Zugang besonders gesichert sein, damit die Strafvorschrift gegen das Ausspähen von Daten (§ 202 a StGB) wirkt. Andererseits müssen die Daten auch gerade dann zugänglich sein, wenn der Betroffene selbst nicht handlungsfähig ist und weder seine Helfer über besondere Gesundheitsprobleme informieren noch den Zugriff auf die Daten – z. B. durch Eingabe eines Codes – eröffnen kann.

- Auch wenn die systematische Erfassung der Gesundheitsdaten auf einer Chipkarte sinnvoll sein kann, ist es aber nicht jedermanns Sache, z. B. bei jedem Arztbesuch, den Zugang zu allen diesen Daten auf seiner Karte zu gestatten. Deshalb ist ein für die Patienten praktikabler Weg zu finden, bestimmte Daten auch einmal nicht offenzulegen.

- Neben den technischen Verfahren zur Datensicherung ist auch zu klären, ob und wie der Betroffene selbst auf seine Daten in seiner Karte zugreifen kann, z. B. um sich Gewißheit über deren Inhalt zu verschaffen, ohne daß die Sicherheit dadurch empfindlich gemindert wird.

Einige Probleme lassen sich allein durch technische Vorkehrungen (s. auch Nr. 30.1) und durch die organisatorische Gestaltung des Gesamtsystems lösen, für andere muß der Gesetzgeber die richtigen Rahmenbedingungen vorgeben. Es ist zu erwarten, daß aus den von seiten der Ärzte, der Apotheker und der Krankenkassen angestoßenen und mit Interesse verfolgten Feldversuchen mit allgemeinen Gesundheitsdaten, aus den Arbeiten zu Notfallkarten und speziellen Karten z. B. für Diabetiker und aus den intensiven Diskussionen über diese Projekte und die damit zusammenhängenden technischen, wirtschaftlichen und ethischen Fragen weitere Erkenntnisse über die notwendigen Regelungen und Maßnahmen gewonnen werden. Wie auch die Landesbeauftragten für den Datenschutz habe ich mich an der Entwicklung durch Beratung verschiedener Interessenten und durch Beiträge zu den fachlichen Diskussionen beteiligt (s. auch Anlage 4, Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu Chipkarten im Gesundheitswesen) und werde das fortsetzen.

17.4 Programm „Humanitäre Soforthilfe" – ein datenschutzrechtlich vorbildliches Verfahren der Deutschen Ausgleichsbank

Die Bundesregierung hat für Bürger, die durch Blut oder Blutprodukte mit dem HI-Virus (HIV) infiziert wurden, in einem besonderen Programm finanzielle Mittel bereitgestellt und die Deutsche Ausgleichsbank (DtA) mit der Durchführung des Programms beauftragt. Ein Rechtsanspruch auf Leistungen aus diesem Programm besteht jedoch nicht.

Die Leistungsgewährung richtet sich nach der „Richtlinie für die Gewährung von Leistungen an durch Blut oder Blutprodukte HIV-Infizierte oder infolge davon an AIDS erkrankte Personen durch das Programm ‚Humanitäre Soforthilfe'", an deren Fassung das BMG mich frühzeitig beteiligt hat. Aufgrund des Programms erhalten diese HIV-Infizierten einen monatlichen Betrag in Höhe von 1 000 DM und die zusätzlich an AIDS erkrankten Personen einen monatlichen Betrag in Höhe von 2 000 DM.

Bei der DtA habe ich mich von der datenschutzrechtlich vorbildlichen Durchführung des Programms überzeugen können. Die Anträge auf Zahlung der Leistungen aus dem Programm werden nur von den unmittelbar mit der Durchführung des Programms beschäftigten Personen eingesehen. Die ein- und ausgehende Post wird entsprechend direkt geleitet. Soweit die Betroffenen Interesse an einer Antragstellung per Telefax zeigen und um die Angabe der Telefax-Nummer der DtA bitten, wird ihnen eine spezielle Telefax-Nummer genannt. Die Bank begegnet in ihrem Bereich wirkungsvoll den Gefahren, die mit der Nutzung von Telefaxgeräten verbunden sind (s. dazu 13. TB S. 85 und 115).

Auch bei den Auszahlungen wird auf seiten der DtA alles mögliche getan, um die Anonymität der Antragsteller zu wahren. So überweist die Bank auf Wunsch von Antragstellern die Leistung auch auf Konten von Dritten, z. B. von Freunden und Verwandten, oder auf für diesen Zweck besonders eingerichtete Konten, soweit dies banktechnisch möglich ist. Damit kann jeder Antragsteller weitgehend selbst festlegen, mit welchen, seiner Situation angepaßten Maßnahmen die mit dem Schriftverkehr und den Überweisungen verbundenen Risiken der Preisgabe der Infektion am besten gemindert werden. Viele der Betroffenen verzichten jedoch auch auf entsprechende Vorkehrungen.

17.5 Transplantationsgesetz – ein Beispiel für gute, weil frühzeitige Beteiligung

An den Beratungen zum Vorentwurf eines Transplantationsgesetzes hat mich das BMG frühzeitig beteiligt. Der Entwurf macht deutlich, daß das BMG die Achtung des Persönlichkeitsrechts – insbesondere des Rechts auf einen humanen Tod und die Achtung vor dem menschlichen Körper, aber auch des Rechts auf informationelle Selbstbestimmung – bei dem heiklen Thema Transplantationsmedizin ernst nimmt. Klare und verständliche Regelungen sind hier besonders wichtig, weil die Daten über Organspender und Organempfänger in deren Intimsphäre eingreifen, und weil jede Unklarheit darüber, was mit den Daten geschieht, die Spendenbereitschaft herabsetzen würde. Die jetzt entworfenen Vorschriften erfüllen diesen Anspruch. Deshalb habe ich auch keine Bedenken gegen die vorgesehenen Übermittlungen von Daten an die Stiftung Eurotransplant nach Leiden in den Niederlanden, die unter der datenschutzrechtlichen Aufsicht der niederländischen Registratiekamer steht. Auch die anderen Vorschriften für die Übermittlung der für eine Transplantation von menschlichen Organen notwendigen personenbezogenen Daten von Organspendern und Organempfängern sind Beispiele für eine gelungene Zusammenarbeit zwischen den beteiligten Bundesressorts und meiner Dienststelle.

18 Verkehrswesen

18.1 Automatische Gebührenerhebung auf Autobahnen – „Spion im Auto"?

„Spion im Auto", „Abkassiert und kontrolliert", „Satellitenauge verfolgt die Autobahnfahrt" waren nur einige Schlagzeilen in der Presse, durch die auf Datenschutzprobleme bei der Erhebung von Autobahngebühren mit Computern hingewiesen wurde. Durch automatisiert erzeugte Bewegungsbilder, die nachweisen, wer wann auf welchen Straßen wohin unterwegs war und wie lange er dort gewesen ist, würde die freie – und das heißt auch: die von Beobachtung freie – Bewegung der Bürger massiv beeinträchtigt. Die Unvereinbarkeit eines solchen Eingriffs mit unserer freiheitlich demokratischen Grundordnung war so offensichtlich, daß sehr bald alle maßgeblich beteiligten Stellen derartige Lösungen einmütig ablehnten.

Wenn für Autobahnfahrten besondere Gebühren entrichtet werden sollen, dann muß dies ohne Speicherung der Daten über alle Fahrten erfolgen. Die Gebühren müssen statt dessen anonym erhoben werden, ähnlich, wie beim Telefonieren mit einer im voraus bezahlten Telefonkarte. Damit dafür nicht extra angehalten werden muß, sollen sowohl die Aufforderung zum Bezahlen als auch die Zahlung und gegebenenfalls die Kontrolle, ob richtig bezahlt wurde, über Funk erfolgen. Mit elektronischer Datenverarbeitung, Chipkarten und kryptographisch gesicherten Verfahren ist das im Prinzip möglich. Ob solche Systeme auch in der Praxis bei unterschiedlichen Wetterlagen und beliebigen Verkehrssituationen zuverlässig arbeiten, wird derzeit im Auftrag des Bundesministeriums für Verkehr in einem Feldversuch auf der A 555 zwischen Bonn und Köln erprobt. Die Landesbeauftragten für den Datenschutz und ich haben sich hierüber auch vor Ort unterrichten lassen.

Untersucht wird im wesentlichen die Kommunikation von Geräten in den Fahrzeugen mit außerhalb, z. B. über der Fahrbahn oder am Straßenrand installierten Sende- und Empfangsanlagen, aber auch mit den Satelliten des Globalen-Positionsbestimmungs-Systems (GPS). Diese Satelliten überwachen nicht den Verkehr, sondern senden Daten, aus denen der Empfänger seine eigene Position bestimmen kann. Ein Gerät im Fahrzeug soll dann durch Vergleich mit den be-

kannten Positionen der Mautstellen die Zahlungspflicht erkennen.

Die Versuche werden im Frühjahr 1995 abgeschlossen. Erst dann können zuverlässige Aussagen über die einsetzbaren Techniken und die dabei zu verarbeitenden Daten getroffen werden. Nach den Besprechungen im Rahmen des Versuchs und den z. T. recht intensiven Diskussionen, die ich auf Wunsch beteiligter Firmen geführt habe, zeichnen sich einige Datenschutzforderungen jedoch schon jetzt ab:

- Die Technik muß so verläßlich sein, daß nicht noch zur Sicherheit für alle Fälle Aufzeichnungen über jede Fahrt im System zu speichern sind.
- Die Kontrolle darf nicht so organisiert werden, daß jeder Fahrer oder Halter eines Fahrzeugs sich genötigt sieht, vorsichtshalber selbst lückenlose Aufzeichnungen über Fahrten zu führen, um noch nach Tagen oder Wochen erhobenen Vorwürfen begegnen zu können, er habe fällige Maut nicht entrichtet.
- Die Technik zur Erhebung von Beweisen über Schwarzfahrten darf nicht schon vorsorglich so gestaltet werden, daß ohne große Mühe auf die Vollerfassung aller Fahrten umgeschaltet werden kann.

Obwohl in anderen Staaten schon länger Mautstellen eingerichtet sind, ist das Interesse insbesondere aus den Mitgliedstaaten der EU an dem Versuch auf der A 555 und den zugrundeliegenden Lösungsansätzen groß. Denn die Vorteile der automatisierten Gebührenerhebung ohne Anhalten sind offensichtlich. Gleichzeitig kann man mit den dazu notwendigen Kommunikationseinrichtungen – sei es durch reine Information, sei es durch Preisdifferenzierung – die zukünftig wachsenden Verkehrsströme marktkonform beeinflussen. Damit durch unterschiedliche Verfahren in den einzelnen Ländern nicht neue Grenzen in Europa geschaffen werden, muß deshalb eine europäisch abgestimmte Lösung gefunden werden, damit die freie Fahrt über die Grenzen nicht gestoppt wird, bevor sie richtig begonnen hat.

Die zu erwartende breite Einführung eines Verfahrens zur Gebührenerhebung legt es nahe, schon von vornherein eine datenschutzgerechte Lösung zu finden.

18.2 Kraftfahrt-Bundesamt – KBA –

18.2.1 Kontrolle beim KBA

Die kooperative Zusammenarbeit zwischen meiner Dienststelle und dem KBA schließt Kontrollbesuche in regelmäßigen Zeitabständen ein, um dort Einzelprobleme mit den verantwortlichen Bearbeitern im Detail zu erörtern und mich über die Beseitigung von früher festgestellten Mängeln zu informieren.

Zum Teil liegt es an technischen und organisatorischen Problemen, daß Mängel länger bestehen bleiben. So stellten meine Mitarbeiter beim letzten Besuch im Kraftfahrt-Bundesamt fest, daß die bereits früher bekannt gewordenen Mängel bei der Datensicherung, wie

- Vergabe jeweils nur einer Benutzerkennung für KBA-interne Dateizugriffe an mehrere Personen, so daß bei Bedarf nicht feststellbar gewesen wäre, wer bestimmte Zugriffe getätigt hat,
- fehlende Verschlüsselung von Benutzerkennungen in den entsprechenden Datenbanken, so daß die geheimzuhaltenden Kennungen von Unbefugten dort hätten ausgelesen werden können,

noch nicht behoben waren, obwohl diese Probleme nach dem Stand der Technik seit längerer Zeit lösbar sind.

Nach Auffassung des KBA dienen die Gruppenkennungen u. a. dazu, einzelne Dateien durch mehrere Mitarbeiter pflegen zu lassen. Ein Mißbrauch sei bei ordnungsgemäßer Nutzung der Dateiattribute im Zusammenhang mit Paßwörtern ausgeschlossen. Zusätzlich sei der Zugriff mit einer solchen Kennung auf bestimmte Bereiche und Programme beschränkt. Im übrigen würde die Änderung der Gruppenkennungen in Einzelkennungen einen erheblichen Speichermehrbedarf erfordern, der Hardware-Kosten von ca. 100 000 DM verursachen würde. Es sei daher fraglich, ob eine Abschaffung der bisherigen Gruppenkennungen eine angemessene Maßnahme nach § 9 BDSG (technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes) sei.

Ich bin der Auffassung, daß es im Interesse eines DV-Großanwenders liegen müßte, die Nutzung seiner Systeme lückenlos durch anwenderbezogene Zugriffsberechtigungen zu sichern und zu dokumentieren. Ich habe Zweifel, ob dieses bei der Verwendung von Gruppenkennungen möglich ist, und halte dafür eine Schwachstellenanalyse durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) für notwendig.

Die Verschlüsselung von Benutzerkennungen wäre nach Auffassung des KBA nur sinnvoll, wenn die Kennung schon bei der Eingabe verschlüsselt würde. Hierzu sei jedoch eine Anpassung aller Anwendungen nötig, die im Rahmen der Anmeldung auf den Kennungsdatenbestand zugreifen. Hierfür sei ein erheblicher Programmieraufwand erforderlich, der nicht kurzfristig zu realisieren sei. Deshalb sei auch geplant, die Anwendungen im Rahmen notwendiger grundsätzlicher Programmänderungen bzw. Neuprogrammierungen um ein Verschlüsselungsmodul zu ergänzen. Auch dafür wäre eine durch das BSI durchzuführende Schwachstellenanalyse hilfreich.

Bisher erörterte das KBA mit dem BSI nur Einzelprobleme der DV-Sicherheit. Ich habe angeregt, vom BSI eine Schwachstellenanlyse zur Sicherheit der DV-Systeme insgesamt durchführen zu lassen. Dadurch könnten allgemeine Probleme der Datensicherheit bei DV-Großanwendern untersucht und für den Bundesbereich Standards erarbeitet werden. Das BSI soll nunmehr gebeten werden, im Rahmen seiner Aufgaben eine Schwachstellenanalyse der DV-Sicherheit beim KBA durchzuführen.

18.2.2 Verkehrszentralregister

Im 12. Tätigkeitsbericht hatte ich auf die Notwendigkeit hingewiesen, die gesetzlichen Regelungen für

die Verarbeitung personenbezogener Daten im Verkehrszentralregister dem tatsächlichen Bedarf anzupassen (12. TB S. 50).

Der vom BMV im Jahre 1992 erarbeitete Referentenentwurf eines Gesetzes zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze sah entsprechende Regelungen vor. Einige der darin vorgesehenen Datenspeicherungen sind jedoch nicht, andere nicht in allen Fällen erforderlich. Das Bundesministerium für Verkehr sollte m. E. noch einmal prüfen, ob

- das Zurückziehen und jede Ablehnung von Anträgen auf Erteilung einer Fahrerlaubnis oder einer Fahrlehrerlaubnis,
- die Verfahrenseinstellungen nach §§ 153a und 153b StPO und
- jeder Verzicht auf die Fahrerlaubnis

im Verkehrszentralregister eingetragen werden müssen.

Desgleichen bedarf einer Prüfung, inwieweit eine weitergehende Differenzierung, als bisher praktiziert (12. TB S. 50), für eine zweckorientierte Auskunftserteilung (Teilauskunft) im Behördenverkehr möglich ist. Hier bestehen Zweifel, ob z. B. zur Wahrnehmung luftverkehrsrechtlicher Aufgaben alle Eintragungen übermittelt werden müssen.

Das automatisierte System zur Erschließung und Verwaltung der VZR-Eintragungen unterstützt nicht die gesetzlich vorgeschriebene Tilgung von Einzeleintragungen (Blattilgung), wenn mehrere Eintragungen vorhanden sind, die zu unterschiedlichen Zeitpunkten getilgt werden müßten.

Seit Jahren dränge ich darauf, hier Abhilfe zu schaffen. Das KBA hält eine Änderung im bestehenden System für unzweckmäßig, weil an einem grundlegend neuen automatisierten Verfahren gearbeitet werde und dessen Fertigstellung durch einzelne Nachbesserungen am bestehenden System unzumutbar verzögert würde.

Die nach der Rechtslage unzulässigen Datenspeicherungen konnte ich bisher hinnehmen, da

- die Außenwirkung (Auskunftserteilung) die gleiche war wie bei zeitgerechter Blattilgung (keine Auskunft über die der Tilgung unterliegenden Eintragungen) und
- die vorgesehene Einführung der automatisierten Blattilgung mittelfristig in Aussicht gestellt worden war.

Über die kürzliche Mitteilung des KBA, daß die automatisierte Blattilgung aus finanziellen Gründen vorerst zurückgestellt worden sei, bin ich daher überrascht und befremdet. Ich bin der Auffassung, daß die Praxis der Tilgung im VZR nunmehr umgehend an die Rechtslage angepaßt werden muß.

18.2.3 Statistiken des KBA

Eine Kontrolle der Verfahren, mit denen das KBA Statistiken aus dem Verkehrszentralregister (VZR) und dem Fahrzeugregister erstellt, hat keine wesentlichen Mängel gezeigt. Nach der Art der Auswertungen und ihrer breiten Verwendbarkeit handelt es sich um Bundesstatistiken. Deshalb sollten die Übermittlungsregelungen des Straßenverkehrsgesetzes bald um Vorschriften über die statistischen Nutzung dieser Register, die nicht zur Übermittlung personenbezogener Daten führen, ergänzt werden.

Zu der Frage, unter welchen Umständen statistische Tabellen keine personenbezogene Daten enthalten, konnte anhand eines kleinen Beispieles gezeigt werden, wie leicht unter günstigen Umständen die Deanonymisierung schon mit Hilfe eines Telefonbuches ist, wenn in den Tabellenfeldern eine „1" auftaucht. Das KBA hat mir erklärt, sich künftig bei der Veröffentlichung von Tabellen an den vom Statistischen Bundesamt entwickelten Grundsätzen für die statistische Geheimhaltung zu orientieren.

18.3 Bedenkliche Tendenzen bei Regelungsentwürfen für den Verkehrsbereich

Im Verkehrsbereich ist die Tendenz erkennbar, vermeintliche Lücken bei der Verarbeitung personenbezogener Daten durch Rechtsänderungen so zu schließen, daß dabei datenschutzrechtliche Grundsätze außer acht gelassen werden. Nicht bedacht wird dabei, daß Eingriffe in die Rechte der Bürger nur zu vertreten sind, wenn sie im überwiegenden Allgemeininteresse auch erforderlich sind. Spezialgesetzliche Einzelregelungen dürfen deshalb die Prinzipien des Datenschutzes nicht unterlaufen, sie sollen vielmehr die bereichsspezifisch gebotenen Sonderregelungen treffen.

18.3.1 Keine kostenfreie Eigenauskunft aus dem Verkehrszentralregister

In meinem 14. Tätigkeitsbericht (S. 109) hatte ich darauf hingewiesen, daß das Kraftfahrt-Bundesamt entgegen der Regelung des § 19 Abs. 7 BDSG für Auskünfte aus dem Verkehrszentralregister (VZR) weiterhin 10,00 DM erhebt. Die Angelegenheit ist nach wie vor streitig.

Um künftig alle Zweifel an der Rechtmäßigkeit dieser Gebührenerhebung auszuräumen, wurde der inzwischen zurückgezogene Gesetzentwurf der Bundesregierung zur Änderung des Fahrlehrergesetzes und anderer Gesetze um eine Berechtigung zur Erhebung von Gebühren für Registerauskünfte ergänzt. Es mag verfassungsrechtlich zulässig sein, wegen der Art der gespeicherten Daten und dem besonderen Interesse an der Eigenauskunft diese von der Zahlung einer Gebühr abhängig zu machen. Eine mit fiskalischen Zwängen begründete Regelung würde jedoch den vom Gesetzgeber im BDSG aufgestellten Grundsatz mißachten, daß der Bürger ein Recht auf unentgeltliche Auskunft über die zu seiner Person gespeicherten Daten hat.

Keine Bedenken habe ich für das Verlangen einer Gebühr in den Fällen, in denen die Behörde eine **Bescheinigung** zur Vorlage bei Dritten ausstellen soll. Zu einer solchen Differenzierung ist das Bundesministerium für Verkehr bisher jedoch nicht bereit.

18.3.2 Zweckfremde Nutzung der ZEVIS-Protokollierung

Ein von der Bundesregierung in der abgelaufenen Legislaturperiode nicht mehr eingebrachter Entwurf eines Gesetzes zur Änderung des Fahrlehrergesetzes und anderer Gesetze sah vor, die zweckfremde Nutzung von Protokolldaten des Zentralen Verkehrsinformationssystems (ZEVIS) beim Kraftfahrt-Bundesamt zu erlauben. Die Aufzeichnungspflicht bei ZEVIS wurde seinerzeit als Ausgleichsmaßnahme für die Gefährdungen des informationellen Selbstbestimmungsrechts geschaffen, die von großen Online-Systemen ausgehen können. Die Daten sollten ausschließlich der Kontrolle der Zulässigkeit der Abrufe dienen. Nach dem o.a. Gesetzentwurf soll ihre Verwendung jedoch auch dann zulässig sein, wenn Anhaltspunkte dafür vorliegen, daß sie zur Verfolgung oder Verhinderung einer schwerwiegenden Straftat gegen Leib, Leben oder Freiheit einer Person führen kann und die Aufklärung oder Verhütung ohne die Maßnahme aussichtslos oder wesentlich erschwert wäre.

Für diskussionswürdig halte ich, ob und für welche Delikte und unter welchen sonstigen Bedingungen eine Öffnung der Zweckbindung von Protokolldaten im **Einzelfall** entgegen dem Rechtsgedanken von § 14 Abs. 4 BDSG für Fahndungszwecke verfügbar gemacht werden können. Denn es gibt Beispiele dafür, daß unter besonderen Umständen die Suche nach Anfragen zu einem bestimmten Fahrzeug sachdienlich und in diesen Fällen die Zweckentfremdung auch angemessen sein kann.

Eine Nutzung des gesamten Protokolldatenbestandes sämtlicher ZEVIS-Abrufe für Datenabgleiche wäre dagegen unverhältnismäßig und würde darüber hinaus Rasterfahndungen auf Bewegungsdaten ermöglichen. Eine derartige Umwidmung einer zunächst zur Datenschutzkontrolle bestimmten Datensammlung würde auch die in der Diskussion um die automatisierte Erhebung von Straßenbenutzungsgebühren vorgebrachten Befürchtungen nähren, daß gesetzliche Datenschutzgarantien, die zur Einführung neuer Verfahren gegeben werden, nach der Einführung leicht wieder zurückgenommen werden könnten.

18.3.3 Zentrales Fahrerlaubnisregister

Das Bundesministerium für Verkehr beabsichtigte, durch Änderung des Straßenverkehrsgesetzes ein Zentrales Fahrerlaubnisregister beim Kraftfahrt-Bundesamt in Flensburg zu errichten, in dem die personenbezogenen Daten aller Inhaber von Fahrerlaubnissen zentral gespeichert werden sollten. Die Daten hierzu sollten die örtlichen Führerscheinstellen liefern, nachdem deren Daten beim geplanten obligatorischen Umtausch der Führerscheine in EG-Führerscheine, der weder in der Richtlinie vorgesehen noch von den übrigen EU-Mitgliedern entsprechend durchgeführt wird, aktualisiert wären.

Begründet wurde diese zentrale Speicherung von ca. 50 Mio. Fahrerlaubnisinhabern mit dem in der 2. EG-Führerscheinrichtlinie vereinbarten effektiven Informationsaustausch, der aufgrund der neuen Rahmenbedingungen in der EU erforderlich sei. Die bei anderen Projekten zu einer strengen Prüfung der Erforderlichkeit zwingenden Kosten bildeten hier kein entscheidendes Hindernis, weil sie im Rahmen der ohnehin von den Fahrerlaubnisinhabern zu zahlenden Umtauschgebühr mit erhoben werden sollten.

Ich habe mich gegen eine zentrale Speicherung der Daten aller Fahrerlaubnisinhaber ausgesprochen, da die Veränderung der Verhältnisse in der EU nichts daran ändert, daß der Führerschein der Mitführungspflicht unterliegt. Aus dem vorzulegenden Dokument sind sowohl die ausstellende Behörde als auch diejenigen Angaben leicht zu erkennen, mit denen eventuell bestehende Fragen bei der zuständigen (örtlichen) Fahrerlaubnisbehörde leicht geklärt werden können, insbesondere, weil ohnehin die Verarbeitung dieser Daten auch dort bald automatisiert sein wird. In den Fällen, in denen ein Bürger die erforderliche Fahrerlaubnis nicht vorlegen kann, liegt es in seinem Interesse, die notwendigen Angaben zur Klärung des Sachverhalts beizubringen. Für die wenigen Fälle, in denen der Führer eines Fahrzeuges das nicht leisten kann, halte ich die Registrierung von ca. 50 Mio. Fahrerlaubnisinhabern für unverhältnismäßig. Das Register ist auch kein angemessenes Mittel, um dem Erwerb mehrer Führerscheine in verschiedenen Ländern zu begegnen. Schon heute kann durch eine Anfrage beim Verkehrszentralregister festgestellt werden, ob einem deutschen Bewerber für einen ausländischen Führerschein die Fahrerlaubnis entzogen wurde oder ob sein Führerschein schon „durch Punkte belastet" ist. Es besteht im übrigen wenig Anreiz, ohne solche Gründe zusätzlich die Kosten und Mühen für einen solchen „Zweitführerschein" zu tragen. Denn der Entzug einer erforderlichen Fahrerlaubnis gilt unabhängig davon, ob und welchen Führerschein ein Fahrer noch im Besitz hat.

Ich halte es für bedenklich, durch den Aufbau großer Dateien Online-Zugriffe auf personenbezogene Daten zu ermöglichen, ohne vorher besonders kritisch zu prüfen, ob diese Einschränkung des informationellen Selbstbestimmungsrechts auch wirklich im überwiegenden Allgemeininteresse erforderlich ist. Wenn darüber hinaus – wie im Entwurf des BMV vorgesehen war – Abgleiche mit dem Verkehrszentralregister und mit dem zentralen Fahrzeugregister ermöglicht werden sollen, stellt sich die Frage, ob als nächster Schritt ein allgemeiner Informationsverbund Kraftfahrzeugwesen entstehen wird, mit dessen Hilfe der „gläserne Autofahrer" Wirklichkeit werden kann.

18.3.4 Verspätete Beteiligung – nutzlose Arbeit

Datenschutzrechtliche Aspekte lassen sich in Rechtsvorschriften des Bundes umso leichter berücksichtigen, je früher ich schon im Entwurfsprozeß beteiligt werde. Wenig erfreulich ist es, wenn ich erst aus dem Bereich der Länder gelegentlich nach meiner Sicht zu datenschutzrechtlichen Aspekten in Entwürfen des Bundesministeriums für Verkehr gefragt werde, die ich noch nicht kenne.

Einen traurigen Rekord der verspäteten Beteiligung erzielte das BMV bei der 20. Verordnung zur Änderung verkehrsrechtlicher Vorschriften:

- Als Anlage zu seinem Schreiben vom 17. Oktober 1994 übersandte mir das BMV einen Referentenentwurf dieser Verordnung „mit der Bitte um Kenntnis und gegebenenfalls Stellungnahme".
- In meiner Stellungnahme vom 21. November 1994 machte ich dazu einen gut begründeten Ergänzungsvorschlag.
- In seinem Schreiben vom 4. Januar 1995 bedauerte das BMV, daß mein Ergänzungsvorschlag leider nicht berücksichtigt werden konnte, „da der Referentenentwurf bereits im November 1994 dem Bundesrat zur Zustimmung vorlag".

Das kann zumindest für das BMV nicht überraschend gewesen sein, denn bereits im Oktober, und zwar vier Tage bevor ich über den Entwurf informiert wurde, hatte der Chef des Bundeskanzleramtes den auf Regierungsebene abgestimmten Verordnungsentwurf mit der Bitte um Zustimmung durch den Bundesrat an dessen Präsidenten übersandt. Der Beschluß des Bundesrates hierzu erfolgte am 25. November 1994.

Eine derartige „Zusammenarbeit" – wie im vorliegenden Fall – verdient nicht den Namen, sie führt lediglich zu nutzloser Arbeit.

18.4 Deutsche Bahn AG

Die seit 1. Januar 1994 bestehende Deutsche Bahn AG unterfällt nicht mehr meiner Zuständigkeit. Die Kontrolle wird seitdem durch die Senatsverwaltung für Inneres in Berlin als Aufsichtsbehörde gemäß § 38 BDSG wahrgenommen. Die beiden nachfolgenden Abschnitte beziehen sich daher auf Ereignisse aus dem Jahr 1993.

18.4.1 Reisende mit falsch ausgestellten Fahrkarten als Schwarzfahrer

Bahnkunden hatten sich an mich gewandt, nachdem sie mit von einem Reisebüro falsch ausgestellten Karten bei einer Kontrolle als „Reisende ohne gültige Fahrausweise" zum Nachlösen des fehlenden Zuschlages und Zahlen eines erhöhten Fahrpreises von je 60,– DM aufgefordert worden waren. Weil sie dies abgelehnt hatten, wurden ihre Personalien erfaßt und ihnen gleichzeitig Nachlösezettel für die spätere Bezahlung ausgehändigt. Letztlich – die Reisenden weigerten sich standhaft – kam das verursachende Reisebüro für die Bezahlung auf. Die Reisenden befürchteten nun, daß ihre Daten in einer Schwarzfahrerdatei (s. 10. TB S. 49) stehen.

Wie mir die Bundesbahn mitteilte, werde für alle Fahrgeldnachforderungen und Nachlösefälle eine Schuldnerkartei geführt. Die Löschung in dieser Kartei erfolge bei Zahlungseingang; die Akten mit dem Schriftverkehr würden maximal drei Jahre aufbewahrt und dann vernichtet. Eine Übermittlung an Dritte erfolge nicht.

Ich habe keine Bedenken gegen dieses Verfahren, wenngleich auch unklar blieb, weshalb in diesem Fall, in dem die Fahrkarten zwar falsch ausgestellt, aber teurer als erforderlich waren, das Verfahren überhaupt durchgeführt werden mußte. Für die Reisenden, die sich an mich wandten, kam es jedoch darauf an, daß ihre Daten deswegen nicht auch noch in einer Schwarzfahrerdatei geführt werden.

18.4.2 Namensnennung in Planfeststellungsbeschlüssen

In meinem 14. Tätigkeitsbericht (S. 105) hatte ich über die unzulässige Aufnahme personenbezogener Daten in den Entwurf eines Gesetzes über den Bau der „Südumfahrung Stendal" berichtet. Leider wurden nun bei der Planung der neuen Eisenbahnstrecken Hannover–Berlin in einem Planfeststellungsbeschluß erneut personenbezogene Daten wie vollständige Einwenderlisten, Schreiben von Einwendern mit Einzelheiten u. a. über gesundheitliche Beschwerden und über Wertminderungen bestimmter Grundstücke veröffentlicht. An der Unzulässigkeit dieser Veröffentlichung personenbezogener Daten konnte auch hier kein Zweifel bestehen. Nachdem ich den Vorstand der Deutschen Bundesbahn hierauf hingewiesen habe, hat die Hauptverwaltung der DB/DR angeordnet, die Namen der natürlichen Personen, die Eigentümer oder Einwender sind, durch Schlüsselnummern zu ersetzen. Ich begrüße, daß die Deutsche Bundesbahn inzwischen klare Vorgaben formuliert hat, um ähnliche Vorkommnisse zukünftig zu verhindern.

18.5 Schiffahrt

18.5.1 Unklarheiten bei der Seeschiffsbestandsdatei

Der gemeinsame Datenbestand des Bundesamtes für Seeschiffahrt und Hydrographie (BSH), des Germanischen Lloyd und des Bundesamtes für Post und Telekommunikation (BAPT) bildet die Grundlage des Schiffsinformationssystems des Germanischen Lloyd. Dieses enthält praktisch die Daten aller See- und Binnenschiffe unter deutscher Flagge. Ein Personenbezug besteht dann, wenn die Halter natürliche Personen sind.

Mindestens zwei öffentliche und eine private Stelle erheben, verarbeiten und nutzen diese Daten. Das BAPT, das die funktechnischen Genehmigungsdateien in die Schiffsbestandsdatei übermittelt, hat nur Zugriff auf einen Teil des gesamten Datenbestandes. Auch das BSH greift nur auf einen Teil der Seeschiffsbestandsdatei zu. Die Daten werden insbesondere genutzt für das Erstellen unterschiedlicher Statistiken nach dem Seeschiffahrtsstatistikgesetz, für Flaggenregisterauskünfte, zur Schiffssicherheitsprüfung und für Verwaltungsverfahren der Seeämter. Jede der beteiligten Stellen liefert aus ihrem Aufgabengebiet die Daten zum gemeinsamen Bestand, die sie selbst oder eine der anderen benötigt, und nutzt den Bestand für ihre Zwecke.

Die bestehenden vertraglichen Regelungen zwischen dem BSH und dem Germanischen Lloyd lassen nicht in jedem Fall erkennen, wer für welche Daten verantwortlich bzw. nutzungsberechtigt und wer speichernde Stelle i. S. von § 3 Abs. 8 BDSG ist.

Ich habe das BSH zur Problematik der Seeschiffsbestandsdatei mehrfach beraten und angeregt, anhand der informationellen Beziehungen die einzelnen Zu-

ständigkeiten und Zugriffsberechtigungen zu klären und nach diesen Ergebnissen die vertraglichen Grundlagen zu gestalten.

Inzwischen wurde eine Übersicht darüber erarbeitet, wer welche Daten erhebt und wer welche Daten zu welchen Zwecken verarbeitet und nutzt. Auf dieser Grundlage sollen die Zugriffe auf die Daten der Seeschiffsbestandsdatei so geregelt werden, daß sie den Zugriffsberechtigungen entsprechen.

18.5.2 Kennzeichnung für kleine Wasserfahrzeuge

Sehr intensiv hat mich das Bundesministerium für Verkehr in die Vorbereitung einer neuen Kennzeichenverordnung für kleine Wasserfahrzeuge eingebunden. Dabei wurden für die Vergabe der Kennzeichen durch Behörden und für die Anerkennung der von Vereinen ausgegebenen Kennzeichen sowie für die entsprechenden Verzeichnisse und Register gute Datenschutzregelungen erreicht. Die Prüfung durch das Justizministerium bestätigte aber meine Besorgnis, daß die gesetzliche Grundlage für das Schaffen der registerrechtlichen Vorschriften nicht ausreicht. Diese Teile sind in der jetzt erlassenen Verordnung daher auch nicht enthalten.

18.5.3 Sportbootführerscheine

Mit der Erteilung von amtlichen Sportbootführerscheinen sind vom BMV der Deutsche Motoryachtverband und der Deutsche Segler-Verband (DSV) beliehen. Für den Führerschein-Binnen erfolgte die Beleihung an jeden Verband einzeln, für den Führerschein-See tragen beide Verbände in einem Koordinierungsausschuß gemeinsam die Verantwortung. Gleiches gilt für die ab Anfang 1994 erteilten amtlichen Schifferscheine-See und -Hochsee, für deren Bearbeitung eine Zentrale Verarbeitungsstelle eingerichtet wurde.

Aufgrund von Eingaben hatte ich mich dafür eingesetzt, das für die Prüfungsanmeldung geforderte ärztliche Zeugnis nicht länger in den Schulen einzusammeln und dann offen mit den Prüfungsunterlagen zu versenden. Das BMV hat nunmehr in der Sportbootführerscheinverordnung-See vorgeschrieben, das Zeugnis vom untersuchenden Arzt unmittelbar dem Vorsitzenden des zuständigen Prüfungsausschusses in verschlossenem Umschlag zuzuleiten. Der Antragsteller selbst erhält zugleich eine Kopie.

Seit Mitte 1994 führen die Verbände eine Datei der jeweiligen Führerscheine auf einem neuen Rechnersystem des DSV. Bei meinen im Berichtszeitraum erfolgten Kontrollen und Beratungen stellte ich fest, daß die Verteilung der Verantwortlichkeiten zwischen den beiden Verbänden, dem Koordinierungsausschuß und der Zentralen Verarbeitungsstelle nicht so eindeutig geregelt ist, wie es § 11 BDSG erfordert. Eine mir noch vor Inbetriebnahme zugesagte Vereinbarung steht z. Zt. noch aus.

Die Aufbewahrungsfristen aller Unterlagen betragen für die Führerscheine-Binnen zwei Jahre. Diese Frist halte ich für angemessen. Dagegen betrug die Frist für alle anderen amtlichen Scheine sechs Jahre. In der Diskussion darüber stellten die Verbände fest, daß diese Unterlagen nach Abschluß der Prüfung zur Klärung von Zweifelsfragen ebenfalls längstens zwei Jahre benötigt werden. Das BMV hat inzwischen für alle Sportbootführerscheine eine einheitliche Aufbewahrungsfrist von zwei Jahren festgelegt.

18.5.4 Internationaler Seefahrt-Daten-„Pranger"

Zu einem Verfahren, mit dem Verstöße gegen Regeln der internationalen Seefahrt durch Veröffentlichung des Sachverhalts an den „Pranger" gestellt werden sollen, hat mich das BMV um Beratung gebeten. Es hatte auf internationaler Ebene – im Rahmen des Memorandum of Understanding über Hafenstaatkontrolle – die personenbezogene Übermittlung zum Zwecke der Veröffentlichung in den Niederlanden zugesagt, wenn bei der Kontrolle von Seeschiffen durch die Hafenbehörden Mängel festgestellt werden, andererseits aber die Schaffung einer innerstaatlichen Rechtsgrundlage für eine Veröffentlichung dieser Daten fehlt. Auch wenn diese Anprangerung im überwiegenden Allgemeininteresse liegt, konnte ich nur dazu raten, die Übermittlung solange einzustellen, bis eine entsprechende Rechtsgrundlage geschaffen ist.

18.5.5 Prüfung einer Wasser- und Schiffahrtsdirektion

Das BMV hatte mich um Beratung bei Problemen im Umgang mit personenbezogenen Daten im Bereich der Bundeswasserstraßenverwaltung gebeten. Dazu habe ich bei einer Wasser- und Schiffahrtsdirektion die Erhebung, Speicherung und Weitergabe von Daten u. a. im Ordnungswidrigkeitenverfahren und bei der Auswertung von Seeunfällen geprüft. Das Ministerium hat mir mitgeteilt, daß auf meine Empfehlung hin inzwischen eine namentliche Meldung von Ordnungswidrigkeiten an das Ministerium unterbleibt. Wegen der nach wie vor erfolgenden listenmäßigen Übermittlung von personenbeziehbaren Daten im Ordnungswidrigkeiten-Verfahren an das Ministerium steht eine Klärung noch aus. Die personenbeziehbare Darstellung von Unfallgeschehen im Anhang der statistischen Mitteilungen der WSD'en hat das Ministerium eingestellt. Die Erörterung der personenbeziehbaren Veröffentlichung von Verwaltungsakten – sog. „Sprüchen" – des Bundesoberseeamtes in dessen amtlichen Sammlungen ist noch nicht abgeschlossen.

18.6 Luftverkehrsrechtliche Defizite

Die vor mehr als zehn Jahren festgestellten rechtlichen Defizite für die Erhebung und Speicherung personenbezogener Daten bei der Vorbereitung und Abwicklung des Flugverkehrs bestehen weiterhin fort. Das Bundesministerium für Verkehr hat diese Defizite anerkannt, dagegen aber nichts unternommen. Ich selbst habe das Ministerium wiederholt an die Schaffung normenklarer gesetzlicher Regelungen erinnert (s. auch 14. TB S. 111). Die vom Bundesministerium für Verkehr genannten personellen Engpässe und Hinweise auf andere vordringlichere Arbeiten erlauben allenfalls für eine begrenzte Zeit, Verstöße

gegen elementare Datenschutzgrundsätze zu tolerieren. Inzwischen ist es aber untragbar, keine ernsthaften Bemühungen zur Beseitigung dieser erheblichen rechtlichen Defizite zu unternehmen.

Auch die vom Bundesministerium für Verkehr bisher vorgelegten Entwürfe eines Elften Gesetzes zur Änderung des Luftverkehrsgesetzes sowie einer Verordnung zur Änderung der Luftverkehrsordnung sind nicht geeignet, den Mangel zu beheben. Durch die Änderung des Luftverkehrsgesetzes soll dem Bundesministerium für Verkehr lediglich die Ermächtigung zur „Erfassung von Daten" in verschiedenen Registern zu bestimmten Zwecken erteilt werden. Anders als Artikel 80 GG vorsieht, bliebe damit die Festlegung des wesentlichen Inhalts der Datenverarbeitung dem Verordnungsgeber überlassen.

Geboten ist statt dessen eine grundlegende gesetzliche Regelung der Verarbeitung personenbezogener Daten für die durch Gesetz festzulegenden Zwecke und Stellen. In diesem Zusammenhang wäre auch das Verhältnis zwischen Luftsicherheit, Luftaufsicht und Flugplatzhalter zu klären. Dabei ist zu regeln, welche personenbezogenen Daten von wem erhoben, durch welche Stellen sie genutzt und unter welchen Umständen sie veröffentlicht werden dürfen. Im wesentlichen handelt es sich um Daten

- der Luftverkehrszulassung,
- über die Erteilung von Flugscheinen und Genehmigungen,
- des Flugmedizinischen Dienstes,
- aus den Meldepflichten der Piloten,
- des Flugfunk- und Telefonverkehrs und
- über Verstöße gegen luftfahrtrechtliche Regelungen.

Auch die schon vor Jahren vorgelegten ersten Ansätze für eine dringend gebotene gesetzliche Regelung über die Erhebung, Verarbeitung und Übermittlung der besonders sensiblen Daten, die bei **Flugunfalluntersuchungen** entstehen, müssen endlich weiterverfolgt werden (s. 14. TB S. 111). Jedes – mittlerweile kaum noch verständliche – Zögern erhöht das Risiko, daß Gerichte selbst im überwiegenden Allgemeininteresse liegende Datenerhebungen und -verarbeitungen für unzulässig erklären werden, weil die erforderliche gesetzliche Grundlage trotz des seit vielen Jahren erkannten Fehlens nicht geschaffen wurde.

19 Umweltschutz

19.1 Inkrafttreten des Umweltinformationsgesetzes, ein kleiner Schritt zur „gläsernen" Verwaltung

Das Umweltinformationsgesetz, über dessen Vorbereitung ich berichtet habe (14. TB S. 113 f.), ist gegen Ende der Legislaturperiode in Kraft getreten. Mit diesem Gesetz wird das Recht eines jeden geregelt, freien Zugang zu Informationen über die Umwelt zu erhalten, die bei einer Behörde oder bei natürlichen oder juristischen Personen des privaten Rechts geführt werden, die im Bereich des Umweltschutzes öffentlich-rechtliche Aufgaben wahrnehmen und insoweit der Aufsicht von Behörden unterstellt sind. Der Anspruch auf freien Zugang zu Umweltinformationen besteht allerdings u. a. dann nicht, wenn durch das Bekanntwerden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden.

Diese Regelung im Umweltinformationsgesetz begrüße ich. Detailliertere Vorgaben könnten die Lösung des Konflikts zwischen Datenzugangsrecht (für interessierte Bürger) und Datenschutz (für betroffene Bürger) erleichtern. Dieses Gesetz, das nur einen allgemeinen Rahmen für die Umsetzung der Richtlinie des Rates der Europäischen Gemeinschaften über den freien Zugang zu Informationen über die Umwelt (90/313/EWG EG-Umweltinformationsrichtlinie) bildet, konnte Lösungen, die sowohl die Datenarten als auch die unterschiedlichen behördlichen Verfahren berücksichtigen, aber offensichtlich nicht enthalten.

Es bleibt abzuwarten, wie nach dem Inkrafttreten des Umweltinformationsgesetzes des Bundes und der Landesumweltinformationsgesetze die erwarteten Konflikte zwischen Datenschutz und Informationsanspruch gelöst werden. Die dabei zu gewinnenden Erfahrungen werden nicht nur zu Präzisierungen im Umweltinformationsrecht führen, sondern auch die Diskussionen über ein allgemeines Recht der Bürger auf Zugang zu behördlichen Informationen beeinflussen.

19.2 Kontrolle des Strahlenschutzregisters

Aufgabe des Strahlenschutzregisters ist es, die Einhaltung der Dosisgrenzwerte bei Personen zu überwachen, die beruflich in verschiedenen Einrichtungen mit ionisierenden Strahlen in Verbindung kommen. Dies sind hauptsächlich Personen aus dem medizinischen Bereich, etwa aus der Röntgendiagnostik oder aus der Nuklearmedizin, aber auch aus nichtmedizinischen Bereichen, wie etwa Mitarbeiter aus Kernkraftwerken. Um den Betroffenen vor gesundheitlichen Gefahren, die durch die Strahlenexposition drohen, zu schützen, werden eine Reihe von Meß- und sonstigen Daten personenbezogen im Strahlenschutzregister gespeichert.

Anläßlich einer Sitzung der Expertenkommission „Strahlenschutzregister" habe ich beim Institut für Strahlenhygiene des Bundesamtes für Strahlenschutz den Umgang mit personenbezogenen Daten kontrolliert. Meine datenschutzrechtliche Kontrolle hat keine Mängel ergeben.

20 Post und Telekommunikation

20.1 Postreform II

Zum 1. Januar 1995 wurden die drei Postunternehmen (Postdienst, Telekom und Postbank) in Aktiengesellschaften umgewandelt. Durch die Privatisierung der Bundespost im Rahmen der Postreform II wurde eine Reihe von Fragen aufgeworfen, die das Post- und Fernmeldegeheimnis sowie das Persönlich-

keitsrecht der Bürger betreffen. Erst recht spät – Ende November 1993 – wurde ich bei dem Reformvorhaben beteiligt. Im weiteren Verlauf der parlamentarischen Behandlung des Gesetzentwurfes hatte ich Gelegenheit, zu datenschutzrelevanten Aspekten Stellung zu nehmen und an Formulierungsvorschlägen mitzuwirken. Für die Privatisierung der Deutschen Bundespost mußten zunächst die verfassungsrechtlichen Voraussetzungen geschaffen werden. Hierzu war eine Änderung des Grundgesetzes erforderlich, die durch Einfügung der neuen Artikel 87 f und 143 b sowie durch entsprechende Anpassungen der Artikel 73 und 87 erfolgte. Damit waren die rechtlichen Voraussetzungen für die Regelungen des Gesetzes zur Neuordnung des Postwesens und der Telekommunikation (PTNeuOG) gegeben, das am 1. Januar 1995 in Kraft getreten ist (BGBl. I S. 2325 ff.).

Aus datenschutzrechtlicher Sicht galt es sicherzustellen, daß sich die Position des Bürgers im Hinblick auf sein Persönlichkeitsrecht durch die Privatisierung der Post nicht verschlechtert. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat mich dabei in meinen Forderungen unterstützt (vgl. Anlage 6). Insbesondere zwei Punkte waren von herausragender Bedeutung: Zum einen die Sicherstellung des grundrechtlich verbrieften Post- und Fernmeldegeheimnisses und zum anderen die Gewährleistung einer effektiven und unabhängigen Datenschutzkontrolle. Durch die Überführung der Deutschen Bundespost in privatrechtliche Unternehmen entfällt ein historisch gewachsener, wesentlicher Adressat des grundrechtlich geschützten Post- und Fernmeldegeheimnisses, denn auf Private finden die Grundrechte keine unmittelbare Anwendung. Daher muß das Post- und Fernmeldegeheimnis zumindest auf einfach gesetzlicher Ebene abgesichert werden, damit die Bürger im Ergebnis keine erhebliche Schwächung ihrer Rechte erfahren. Ein von mir geforderter verfassungsrechtlicher Ausgleich konnte nicht erreicht werden. Ich habe dem Deutschen Bundestag meine Besorgnisse vorgetragen und eine entsprechende Grundgesetzänderung vorgeschlagen. Die Bundesregierung hat im weiteren parlamentarischen Verfahren erklärt, daß die Grundrechte selbstverständlich auch in die Privatwirtschaft ausstrahlen und eine verfassungsrechtliche Regelung somit nicht erforderlich ist. Damit ist es ausreichend, daß das Post- und Fernmeldegeheimnis zumindest auf einfachgesetzlicher Ebene abgesichert wird, damit die Bürger im Ergebnis keine erhebliche Schwächung ihrer Rechte erfahren. Insoweit muß es nunmehr zunächst dem Gesetzgeber überlassen werden, im einfachen Recht den Schutz des Post- und Fernmeldegeheimnisses auch weiterhin in dem jetzigen Umfang zu gewährleisten.

Die Datenschutzkontrolle bei der Deutschen Bundespost wurde vor der Postreform II einheitlich vom Bundesbeauftragten für den Datenschutz als unabhängige Kontrollbehörde bundesweit und auch vorbeugend durchgeführt. Nach der jetzigen gesetzlichen Regelung des § 2 Abs. 1 Satz 2 BDSG soll der Bundesbeauftragte für den Datenschutz bis zum Ende der Postmonopole (voraussichtlich Ende 1997) auch weiterhin für die Datenschutzkontrolle in den „aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangenen Unternehmen" zuständig sein. Ausgenommen ist damit bereits jetzt die Postbank, die über keine Monopolstellung verfügt und daher wie andere Banken und Kreditinstitute zu behandeln ist. Nicht durchsetzen konnte ich mich mit meiner Forderung, auch bereits vor der Postreform entstandene Tochterunternehmen der DBP Postdienst und der Telekom, soweit sie vom Bund beherrscht sind und eine öffentliche Aufgabe (i. S. des Infrastrukturauftrages) wahrnehmen, der Kontrolle des Bundesbeauftragten für den Datenschutz zu unterwerfen. Ich hatte auch dargelegt, daß es keine Rolle spielen dürfe, ob die Gründung einer solchen Tochtergesellschaft „durch Gesetz" oder durch Rechtsgeschäft erfolgt (ist). Nach der jetzigen Regelung (vgl. § 2 Abs. 1 S. 2 BDSG; s. u. 20.2.3) wäre es denkbar, daß sich die Deutsche Bundespost Telekom durch Gründung von Tochtergesellschaften bereits vor dem Ende der Monopole in allen Bereichen der Kontrolle des Bundesbeauftragten für den Datenschutz entziehen könnte. Die Liste der schon jetzt gegründeten Tochtergesellschaften ist lang und umfaßt u. a. die Deutsche Telekom Medien GmbH (Herausgeber der Telefonverzeichnisse) und die Deutsche Telekom Mobilfunk GmbH (Betreiber der Funktelefonnetze C und D1). Nach Wegfall der Monopole werden die Aufsichtsbehörden der Länder für die Kontrollen zuständig sein. Nach dem Bundesdatenschutzgesetz können die Aufsichtsbehörden jedoch nicht so problemlos kontrollieren, wie ich es kann; sie brauchen einen konkreten Anlaß für Ihre Kontrolle. Dieser Mangel wird möglicherweise durch die noch ausstehende EG-Richtlinie zum Datenschutz geheilt werden. Bis es soweit ist, werden jedoch noch wenigstens drei bis vier Jahre vergehen. Hinzu kommt auch noch, daß anders als bisher sich das Wissen um die Telekommunikation nicht bei einer Stelle sammelt, sondern auf viele Stellen verteilt ist. Die Zuständigkeit der Aufsichtsbehörde richtet sich nach dem Sitz des Unternehmens. Da es das politische Ziel der Bundesregierung ist, staatliche Eingriffe in den freien Markt so gering wie möglich zu halten – und hierzu wird auch die Kontrolle gerechnet – hatten Überlegungen, im Interesse des Bürgers per Gesetz festzulegen, daß die Kontrolle bei mir bleibt, keine Chance. Ich bin jedoch nicht bereit hinzunehmen, daß die Erfüllung eines wichtigen Bürgeranliegens davon abhängen soll, wo der Sitz des datenverarbeitenden Unternehmens ist und wie gut informiert und ausgestattet die Aufsichtsbehörde ist. Ich habe daher gefordert, für die Datenschutzkontrolle in der Telekommunikation eine unabhängige, bundesweit tätige Institution zu schaffen, die auch initiativ tätig werden kann. Diese Forderung wird vom Postausschuß des Deutschen Bundestages weitestgehend mitgetragen.

In § 2 Abs. 2 Nr. 6 des Gesetzes zur Regulierung der Telekommunikation und des Postwesens (PTRegG) wurde auf meine Anregung hin auch die Gewährleistung eines wirksamen Datenschutzes als Regelungsziel aufgenommen. Hiermit hat sich der Gesetzgeber die besondere Verpflichtung auferlegt, im Wege der Regulierung die Belange des Persönlichkeitsrechtes sicherzustellen.

Bei der Novellierung des Fernmeldeanlagengesetzes (FAG) wurde der von mir wiederholt dargelegte Änderungsbedarf beim § 12 FAG nicht berücksichtigt: Hier sollten die Voraussetzungen für die Auskunft über den Fernmeldeverkehr dahin gehend geregelt werden, daß eine Beschränkung des Fernmeldegeheimnisses nicht bei minderschweren Straftaten erfolgt. An dieser Stelle ist auch an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. September 1991 (Bundesrats-Drucksache 416/91) zu erinnern.

20.2 Telekom

20.2.1 Privatisierung der Telekom

Zum 1. Januar 1995 ist das Gesetzpaket zur Postreform II und damit auch die Ermächtigungsgrundlage zum Erlaß von Datenschutzverordnungen gem. § 10 PTRegG in Kraft getreten. Die Telekom-Datenschutzverordnung (TDSV) und die Teledienstunternehmen-Datenschutzverordnung (UDSV) werden durch diese zu schaffende Verordnung ersetzt werden. Bei der Erarbeitung der neuen Verordnung werde ich beteiligt sein. Der Erlaß dieser Datenschutzverordnung verlangt nunmehr gem. § 10 Abs. 1 Satz 1 PTRegG die Zustimmung durch den Bundesrat.

Nach Artikel 13 § 1 Nr. 3 PTNeuOG tritt das Postverfassungsgesetz – die Ermächtigungsgrundlage der TDSV – außer Kraft und gem. Artikel 5 Nr. 14 PTNeuOG wird § 14 Abs. 2 Fernmeldeanlagengesetz (FAG) – die Ermächtigungsgrundlage der UDSV – aufgehoben. Damit stellt sich die Frage, nach welchen Rechtsvorschriften in der Übergangszeit – d. h. bis zum Erlaß von neuen Datenschutzverordnungen für den Bereich der Telekommunikation – zu verfahren ist. In diesem Zusammenhang gehe ich mit der wohl herrschenden Meinung davon aus, daß eine Rechtsverordnung – wie in dem vorliegenden Fall – auch dann rechtsverbindlich bleibt, wenn die sie tragende Ermächtigungsgrundlage entfällt. Damit bleiben die Regelungen der TDSV/UDSV – unter Berücksichtigung der Fangschaltungsentscheidung des Bundesverfassungsgerichtes – bis zur Schaffung der neuen Datenschutzverordnung auch nach dem 1. Januar 1995 anwendbar.

20.2.2 Neue Ermächtigungsgrundlage für Datenschutzverordnungen

Durch die Fangschaltungsentscheidung des Bundesverfassungsgerichts vom 25. März 1992 (1BvR1430/88) war der Gesetzgeber aufgefordert worden, eine tragfähige Ermächtigungsgrundlage für Eingriffe in das Post- und Fernmeldegeheimnis zu schaffen, die z. Z. in der Telekom-Datenschutzverordnung (TDSV) geregelt sind. Die Vorschrift des Postverfassungsgesetzes, auf die der Erlaß der TDSV gestützt wurde, (§ 30 Abs. 2) war nicht als ausreichende gesetzliche Ermächtigungsgrundlage zum Erlaß von Vorschriften über die Erhebung von personenbezogenen Daten, die dem Fernmeldegeheimnis unterliegen, angesehen worden. Das Bundesverfassungsgericht hatte allerdings auch ausgeführt, daß ein Gesetz „bei angemessenem Ausgleich der betroffenen Grundrechte, hinreichenden verfassungsrechtlichen Vorkehrungen und wirksamer Mißbrauchssicherung verfassungsrechtlich zulässig" wäre. Diesen Vorgaben ist der Gesetzgeber nun mit der Regelung des § 10 PTRegG nachgekommen. Aus datenschutzrechtlicher Sicht konnten hier im Verlauf der parlamentarischen Beratungen gegenüber dem Ausgangsentwurf erhebliche Verbesserungen erreicht werden. Die aus Datenschutzgesichtspunkten entstandenen Besorgnisse bezogen sich hauptsächlich darauf, daß die Art der Daten, die erhoben und verarbeitet werden dürfen, nicht ausreichend konkretisiert waren. So sah der Ausgangsentwurf einen nicht abschließenden Fallkatalog vor, der Eingriffe in das Post- und Fernmeldegeheimnis rechtfertigte. Durch die Streichung der Formulierung „insbesondere" ist nunmehr eine abschließende Aufzählung derjenigen Tatbestände normiert worden, in denen derartige Eingriffe zulässig sind. Hinsichtlich der Speicherung von personenbezogenen Daten hat der Gesetzgeber Höchstfristen festzulegen.

Besondere Bedeutung kam dabei auch dem Schutz der Nachrichteninhalte zu. Hier wurde eine Lösung gefunden, die aus meiner Sicht datenschutzrechtlichen Belangen in vertretbarer Weise Rechnung trägt. Demnach dürfen Nachrichteninhalte nur in zwei Fällen erhoben, verarbeitet und genutzt werden. Der eine Fall betrifft die Regelung des § 14 a FAG, der bestimmt, daß „Nachrichteninhalte nur aufgezeichnet, Dritten zugänglich gemacht oder sonst verarbeitet werden (dürfen), soweit dies Gegenstand oder aus verarbeitungstechnischen Gründen Bestandteil der Dienstleistung ist". Darüber hinaus ist eine derartige Verarbeitung von Nachrichteninhalten nur bei den in § 10 Abs. 2 Satz 1 Nr. 1 e PTRegG genannten Handlungen zulässig, soweit dies im Einzelfall unerläßlich ist. Die Vorschrift von Satz 1 Nr. 1 e betrifft die rechtswidrige Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie der Telekommunikations- und Informationsdienstleistungen. Als „vertrauensbildende Maßnahme" ist für diesen Fall weiterhin vorgesehen, daß jeweils der Bundesminister für Post und Telekommunikation und die zuständige Datenschutzkontrollbehörde über die Durchführung einer Maßnahme unter Mitteilung des zugrunde liegenden Sachverhalts unverzüglich in Kenntnis zu setzen sind. Darüber hinaus ist der Betroffene anschließend zu unterrichten, damit er gegebenenfalls eine Zulässigkeitsüberprüfung veranlassen kann.

Mit den hier beschriebenen Änderungen des Regierungsentwurfs des § 10 PRegG ist es gelungen, für den Datenschutz befriedigende Regelungen zu erreichen. Dies ist auch auf die Aufgeschlossenheit und das Interesse – trotz des großen Zeitdrucks – der parlamentarischen Gremien, insbesondere Innenausschuß und Postausschuß, zurückzuführen.

In den kommenden Monaten werden nunmehr die entsprechenden Datenschutzverordnungen zu erarbeiten sein. Auf der Grundlage der getroffenen Ermächtigungsnorm werden sich auch die zu schaffenden Rechtsverordnungen an den jetzigen Regelungen der TDSV/UDSV orientieren. Die gesetzliche

Vorgabe bietet insgesamt eine hinreichende Ausgangsposition, die datenschutzrechtlichen Belange der Betroffenen sicherzustellen.

20.2.3 Einheitliche Datenschutzkontrolle im Telekommunikationsbereich unerläßlich

Im Rahmen der Postreform II wurden auch Änderungen des Bundesdatenschutzgesetzes (BDSG) vorgenommen. Nunmehr wurde dem § 2 Abs. 1 BDSG folgender Satz angefügt: „Als öffentliche Stellen gelten die aus dem Sondervermögen Deutsche Bundespost durch Gesetz hervorgegangen Unternehmen, solange ihnen ein ausschließliches Recht nach dem Postgesetz oder dem Gesetz über Fernmeldeanlagen zusteht." Damit steht fest, daß sich bis zum Ende der Monopole (voraussichtlich Ende 1997) meine Kontrollzuständigkeit hinsichtlich der Einhaltung von datenschutzrechtlichen Vorschriften weiterhin auf die Deutsche Bundespost Telekom erstreckt. Zum Ende der Monopole würde sie hingegen entfallen und auf die Aufsichtsbehörden für den nicht-öffentlichen Bereich übergehen. Aus datenschutzrechtlicher Sicht wäre dies – vor dem Hintergrund der Sensibilität der im Telekommunikationsbereich anfallenden Daten und ihres besonderen grundrechtlichen Schutzes (Artikel 10 GG) – von großem Nachteil für den Bürger.

Zum einen würde es für ihn eine erhebliche Schlechterstellung bedeuten, weil eine vorbeugende Kontrolle nicht mehr möglich wäre. Zum anderen würde die Kontrolle nicht durch eine in gleicher Weise unabhängige Stelle erfolgen. Auch eine regionale Zersplitterung der Datenschutzaufsicht sollte vermieden werden, denn dadurch bestünde die Gefahr, daß die im Telekommunikationsbereich tätigen Wirtschaftsunternehmen ganz unterschiedlichen datenschutzrechtlichen Standards unterworfen werden; eine einheitliche Kontrolle wäre nicht mehr gesichert. Die notwendige Transparenz für den Bürger und insbesondere die – vom Bundesverfassungsgericht in seiner Volkszählungentscheidung aufgestellte – Forderung nach einer vorbeugenden Kontrolle wäre nicht mehr gewährleistet.

Diese Bedenken wurden im parlamentarischen Verfahren vom Postausschuß geteilt. So bestand Einigkeit darüber, „daß für die Zeit, wenn die Deutsche Bundespost Telekom und Deutsche Bundespost Postdienst über keine Monopole mehr verfügen und daher § 2 Abs. 1 Bundesdatenschutzgesetz für die Zuständigkeit des Bundesbeauftragten für den Datenschutz bei den Unternehmen seine Wirkung verlieren wird, in Absprache mit den Bundesländern eine zentrale Kontrollstelle für den Datenschutz bestimmt werden soll" (vgl. Beschlußempfehlung und Bericht des Ausschusses für Post und Telekommunikation zu § 10 PTRegG, Bundestags-Drucksache 12/8060, Seite 200.)

Hinsichtlich einer zentralen Kontrollstelle sind die verschiedensten Modelle vorstellbar. Eine Möglichkeit wäre z. B. die Schaffung einer völlig neuen Datenschutzinstitution für den Telekommunikationsbereich insgesamt, für deren Konstruktion mehrere Optionen möglich sind. Denkbar wäre allerdings auch ein Rückgriff auf bereits vorhandene Kontrollbehörden. Unerläßlich wäre dann allerdings eine zentrale koordinierende Stelle, die – z. B. in Zusammenarbeit mit den jeweils zuständigen Aufsichtsbehörden – in einem genau festgelegten Verfahren die einheitliche Auslegung der datenschutzrechtlichen Vorschriften bei Beratungen und Kontrollen sicherstellt. Selbstverständlich stünde auch meine Dienststelle für derartige Aufgaben zur Verfügung. Von besonderer Bedeutung ist jedenfalls, daß die **Funktionsfähigkeit** dieser auch vorbeugend tätigen, unabhängigen Kontrollstelle zum Zeitpunkt des Entfalls der Monopole sichergestellt ist: Bis dahin müßte nicht nur ein Konzept erarbeitet und ein eventuelles Regelungsdefizit behoben werden, auch der organisatorische Aufbau müßte abgeschlossen sein. Ich habe das Bundesministerium für Post und Telekommunikation auf das Problem aufmerksam gemacht und meine Beratung angeboten.

20.2.4 Telefonrechnungen nun leichter überprüfbar

Seit dem 1. April 1994 bietet die Deutsche Bundespost Telekom ihren Telefonkunden einen Einzelverbindungsnachweis (EVN) an. Ein solcher Einzelverbindungsnachweis ist in technischer Hinsicht allerdings grundsätzlich nur für solche Telefonanschlüsse möglich, die mit digitalen Vermittlungsstellen verbunden sind; meines Wissens betrifft dies derzeit fast 50 % aller deutschen Telefonanschlüsse. Aus verfassungsrechtlichen, also nicht aus datenschutzrechtlichen Gründen – es fehlt bisher an einer erforderlichen Rechtsgrundlage – („Fangschaltungsbeschluß", vgl. 14. TB S. 117) ist ein vollständiger EVN gegenwärtig nicht zulässig, vielmehr werden beim angebotenen EVN für alle Verbindungen die letzten drei Stellen der angewählten Rufnummer durch „xxx" ersetzt. Damit ist allerdings auch einerseits eine Überprüfbarkeit der Telefonrechnung gewährleistet, andererseits sind auch Anrufe bei der Mehrzahl der Beratungsstellen – wie von § 6 Abs. 9 Satz 5 TDSV gefordert – nicht erkennbar. Bei einzelnen Beratungsstellen, wie z. B. der Telefonseelsorge, reicht die Verkürzung der Rufnummer jedoch nicht aus, um die Anonymität der Beratung zu gewährleisten. Dies ist auf die besondere Rufnummer (1 11 01–1 11 03) der Telefonseelsorge zurückzuführen. Daher werden Anrufe bei der Telefonseelsorge und solchen privilegierten Beratungsstellen, die durch die besondere Gestaltung ihrer Rufnummer auch bei der Verkürzung um drei Stellen weiterhin erkennbar wären, gemeinsam mit solchen bei Auskunfts- und Ansagediensten der Telekom (Wetter, Telefonauskunft usw.) in einer Zeile unter der Rubrik „Sonstige Verbindungen" ausgewiesen, in der nur die Summe der Tarifeinheiten angegeben wird. Die Gestaltung des augenblicklichen Einzelentgeltnachweises muß folgenden Voraussetzungen genügen:

- Der Schutz der Mitbenutzer eines Telefons, die Beratungsstellen mit Sondernummern aus der Regional- und Weitzone anrufen, muß dadurch hinreichend gewährleistet werden, daß in die Summenzeile („Sonstige Verbindungen") auch Verbindungen zu einer ausreichenden Anzahl von Ansagediensten aufgenommen werden, die in kürzeren

Zeittakten tarifiert sind (z. B. die jetzigen Wetteransagen).

- Bei auftretenden praktischen Problemen in bezug auf die Arbeit der Beratungsstellen, wie z. B. Rückgang der Anrufe aus Angst vor Entdeckung, und den Schutz der anonymen Hilfesuchenden sollte die Deutsche Bundespost Telekom unmittelbar Gespräche mit den Trägern mit dem Ziel aufnehmen, die betreffenden Verfahrensregelungen in diesem Fall einvernehmlich nachzubessern.
- Die Deutsche Bundespost muß gewährleisten, daß die Anzahl der Rufnummern, die in der Summenzeile „Sonstige Verbindungen" zusammengefaßt sind, nicht derartig reduziert wird, daß kein hinreichender Rest zur „Verschleierung" der Anrufe zu Beratungsstellen übrig bleibt. Weiterhin muß – insbesondere in den neuen Bundesländern – durch Ausbau der Vermittlungstechnik die zeittaktfreie Erreichbarkeit der Telefonseelsorge erweitert werden.
- Die Deutsche Bundespost Telekom sollte im Zusammenhang mit der anstehenden Neukonzeption der IT-Verfahren zur Rechnungserstellung verbesserte Verfahren zur Wahrung des Schutzes der Anrufer (§ 10 Abs. 2 Nr. 3a PTRegG) vorsehen. Hierzu habe ich bereits mehrfach andere Rechnungskonzepte vorgeschlagen (vgl. zuletzt 14. TB S. 119). Zusätzlich zu den bereits dort dargestellten Modellen würde sich die sog. „niederländische Lösung" anbieten. Hiernach hat jeder Telefonkunde grundsätzlich das Recht darüber zu entscheiden, ob seine Rufnummer im Einzelverbindungsnachweis aufgenommen wird. Meines Wissens haben von diesem Wahlrecht ca. 20 % der dortigen Kunden Gebrauch gemacht.

Wie ich wiederholt betont habe, ist es auch ein Anliegen des Datenschutzes, daß die Verarbeitung personenbezogener Daten für den Betroffenen nachvollziehbar und richtig erfolgt. Daher ist es für den Telefonkunden u. U. von Nutzen, wenn er seine Rechnung detailliert aufgelistet erhält, so daß er die Korrektheit der Rechnung überprüfen und ggf. auch den Verursacher teurer Gespräche ermitteln kann. Soweit allerdings die erhöhte Telefonrechnung auf einen technischen Fehler bei der Telekom zurückzuführen ist, ist die Hilfestellung des Einzelverbindungsnachweises für den Bürger begrenzt: Die Telefonrechnung wird nämlich in der Regel gerade die Telefongespräche auflisten, die zu den hohen Kosten geführt haben. Mittels dieses Einzelverbindungsnachweises wird es dem Bürger aber nicht immer gelingen, die Telekom davon zu überzeugen, daß er oder seine Angehörigen das aufgelistete Gespräch nicht geführt haben, wenn wie im Falle der jüngsten Presseveröffentlichungen sich Hacker illegal auf Telefonanschlüsse Dritter aufgeschaltet hatten.

20.2.5 Kontrolle der Verbindungsdatenspeicherung im ISDN

Seit Ende 1993 stellt die Telekom ISDN-Anschlüsse bundesweit flächendeckend zur Verfügung. Wegen der mit dieser Technik verbundenen datenschutzrechtlichen Probleme (vgl. 12. TB S. 39 f. sowie 13. TB S. 49 f.) und nachdem mich die Telekom über die technische Realisierung der Wahlmöglichkeiten der Speicherung der Verbindungsdaten informiert hatte, hielt ich es für geboten, die Umsetzung der entsprechenden Regelungen der Telekom Datenschutzverordnung (TDSV) zu kontrollieren. Dabei konzentrierte ich mich nicht nur auf die sog. „Universalanschlüsse" (ISDN-Anschlüsse), sondern berücksichtigte auch jene „normalen" analogen Anschlüsse, die mit digitalisierten Vermittlungsstellen verbunden sind („ANIS-Anschlüsse") und damit auch Zugang zu Leistungsmerkmalen eines ISDN-Anschlusses haben; letzteres betrifft nach meinem Kenntnisstand etwa ein Drittel aller analogen Anschlüsse.

In den digitalen Vermittlungsstellen werden die Daten jeder abgehenden Verbindung

- bei ANIS-Anschlüssen grundsätzlich in Form von Entgeltdatensätzen,
- bei Universalanschlüssen in Form von Kommunikationsdatensätzen

registriert. In zwei Ausnahmefällen liegen auch bei ANIS-Anschlüssen individuelle Verbindungsdaten vor, und zwar bei der Nutzung der ISDN-Leistungsmerkmale „Anrufweiterschaltung" und „Dreierkonferenz".

Die Entgeltdatensätze – die keine Verbindungsdaten enthalten – werden in der Ortsvermittlungsstelle summiert und monatlich auf Magnetbändern dem für Erstellung und Versand der Telefonrechnung des Kunden zuständigen Rechenzentrum zugesandt.

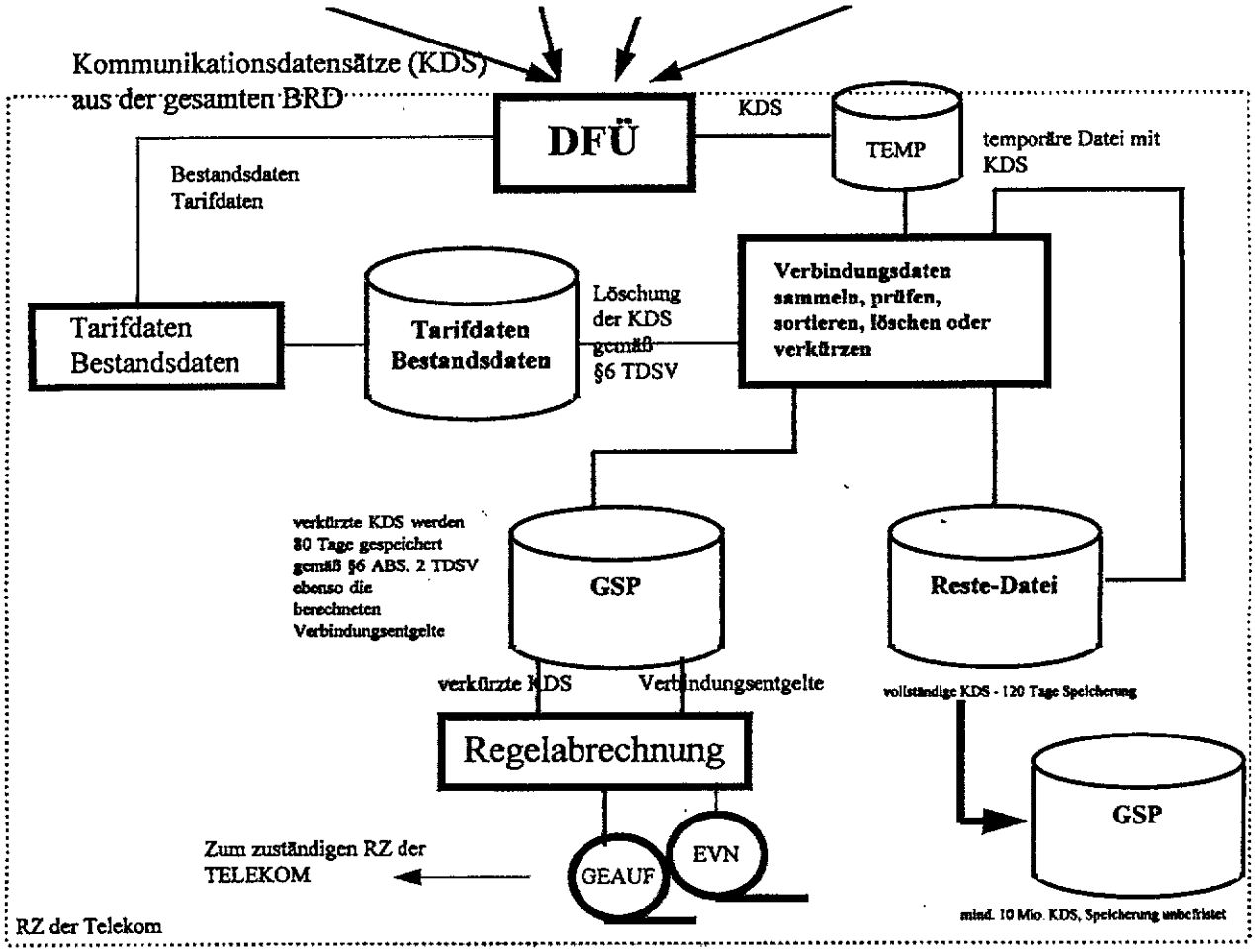
Die Kommunikationsdatensätze (KDS) enthalten für jede Verbindung im wesentlichen folgende Angaben: Fernmeldekontonummer (d. h., die Telefonnummer in besonderer Schreibweise), Zielrufnummer, Endedatum, Endeuhrzeit, Dauer des Gesprächs sowie ein Kennzeichen für den in Anspruch genommenen Dienst.

Die KDS der Universalanschlüsse – bei Inanspruchnahme der genannten besonderen Leitungsmerkmale auch die der betreffenden ANIS-Anschlüsse – werden täglich mittels Datenfernübertragung (DFÜ) an ein spezielles Rechenzentrum (RZ) der Telekom übersandt; in der Vermittlungsstelle sind sie somit maximal 24 Stunden gespeichert.

Aus den verarbeitungsfähigen KDS werden im RZ täglich die Verbindungsentgelte errechnet und – geordnet nach Fernmeldekontonummer (FKTO) und genutzten Diensten – in einem kumulierten Gebührenspeicher (GSP) abgelegt. Einmal monatlich werden mit dem Inhalt des GSP Magnetbänder (GEAUF) beschrieben, die den für Erstellung und Versand der Telefonrechnung zuständigen Rechenzentren zugeschickt werden, z. B. dem RZ Köln für die Bonner ISDN-Anschlüsse. Nach der Berechnung der Entgelte werden die KDS – je nach Kundenwunsch (TDSV § 6 Abs. 2 Ziffer 1) – gelöscht oder um die letzten drei Stellen der angerufenen Nummer gekürzt und für weitere 80 Tage gespeichert. Nicht verarbeitungsfähige KDS werden in der „Reste-Datei" (ERR/Rest) gespeichert und einem erneuten Verarbeitungszyklus zugeführt (siehe hierzu Abbildung 3).

Abbildung 3

Datenfluß von Verbindungsdaten am Beispiel Telekom



Bei der Kontrolle konnte ich hinsichtlich der technischen Umsetzung der Regelungen der TDSV folgendes feststellen:

1. In dem genannten Verfahren ermittelt das Rechenzentrum der Telekom aus den Verbindungsdaten nicht – wie dies Abs. 2 Satz 1 TDSV fordert – „unverzüglich die für die Berechnung des Entgelts erforderlichen Daten", sondern unmittelbar die Entgelte selbst; im übrigen verfährt es entsprechend der Verordnung. Als Begründung hierzu führt die Telekom an: „Die vollständige Speicherung und weitere Bearbeitung der Verbindungsdatensätze einschließlich der kompletten Zielrufnummer – ist für die Berechnung der Verbindungsentgelte erforderlich, weil die Entgeltpflicht bei bestimmten Zielrufnummern erst aus den letzten Ziffern dieser Rufnummer erkennbar ist, z. B. bei Auskunfts- und Ansagediensten. Für die Entgeltberechnung werden somit alle in den Kommunikationsdatensätzen (KDS) enthaltenen Daten benötigt".

   Demgegenüber steht zweifelsfrei fest, daß die Begründung allenfalls für eine Minderzahl der Verbindungen zutrifft; in nahezu allen Fällen ist lediglich die Ortsnetzkennziffer (ONKZ) entgeltrelevant, die Zielrufnummer für den genannten Zweck überflüssig. Die Forderung jedenfalls des Wortlautes des § 6 Abs. 2 Satz 1 TDSV wird also für die Mehrzahl der Verbindungen nicht erfüllt. Um dem Wortlaut der Vorschrift Folge zu leisten, müßte nicht nur ein zusätzlicher Verfahrensschritt eingerichtet, sondern auch eine zusätzliche Datei (KDS ohne Zielrufnummer) gespeichert werden für die weder Verarbeitung noch Nutzung oder Löschung in der TDSV geregelt sind. Der einzige Schutzzuwachs wäre für die Kunden, die die sofortige Löschung der KDS gewählt haben, eine frühere Löschung der nicht entgeltrelevanten Daten, insbesondere der Zielrufnummern, etwa um einen Tag. Dieser würde „erkauft" durch eine zusätzliche Datei personenbezogener Daten – mit zusätzlichem Schutzbedarf – und nicht unerheblichen Verarbeitungsaufwand.

   Eine Gesamtbewertung läßt es deshalb als vertretbar erscheinen, auf eine dem Wortlaut folgende Erfüllung der Vorschrift des § 6 Abs. 3 Satz 1 TDSV zu verzichten, zumal die geschilderte Verfahrensregelung dem Schutzzweck der TDSV besonders Rechnung trägt. Ich werde allerdings im Rahmen der Erarbeitung von Datenschutzverord-

nungen gemäß § 30 PTRegG (s. o. Nr. 20.2.2) darauf drängen, daß klarstellende Regelungen vorgesehen werden.

2. Die Kommunikationsdatensätze, die aufgrund falscher oder fehlender Bestandsdaten nicht verarbeitungsfähig waren, werden, wie bereits oben beschrieben, in einer Restedatei gespeichert. Diese wird nach Ergänzung oder Korrektur der Bestandsdaten 120 Tage lang erneut Verarbeitungsversuchen zugeführt, um damit das Entgelt einem gültigen Fernmeldekonto zuordnen zu können. Datensätze, die auch nach dieser Zeit noch nicht verarbeitet sind, werden in eine andere Datei („Reste-Restedatei") umgespeichert. Die „Reste-Restedatei" umfaßte zum Zeitpunkt der Kontrolle ca. 10 Millionen Kommunikationsdatensätze mit einem täglichen Zuwachs von einer nicht unbeträchtlichen Anzahl. Dies entspricht nichtgeltendgemachten Forderungen der Telekom zum Zeitpunkt der Kontrolle von einigen Millionen DM. Derzeit wird die Datei in keiner Weise genutzt, auch nicht, um diese Forderung gegenüber den Kunden geltend zu machen. Das Betreiben einer nicht genutzten und damit nicht erforderlichen Datei ist datenschutzrechtlich gemäß § 5 Abs. 1 und Abs. 2 TDSV unzulässig und gemäß § 25 Abs. 1 BDSG somit grundsätzlich Gegenstand einer Beanstandung. Ich habe der Telekom am 16. Juni 1993 mitgeteilt, daß es mir nur dann möglich ist, von einer Beanstandung abzusehen, wenn sie

   - die „Altbestände" der Datenverarbeitung so schnell wie möglich mit dem Ziel der Realisierung der Forderung verarbeitet und anschließend unverzüglich löscht und
   - das Verfahren der Restedatei datenschutzgerecht umgestaltet, insbesondere unter Verkürzung der 120-Tage-Frist auf einen sachgerechten, erforderlichen Zeitraum.

In ihrer jetzt eingegangenen Stellungnahme hat die Telekom mitgeteilt, daß die sog. Reste-Reste-Datei gelöscht wird. Eine Verkürzung der 120-Tage-Frist wurde jedoch mit Hinweis auf „manuelle betriebliche Verfahren" abgelehnt. Ich habe der Telekom dringend empfohlen, zeitgemäße automatisierte Verfahren einzuführen, die eine schnelle Bearbeitung ermöglichen.

20.2.6 Btx-Teilnehmer wurden fälschlich zu Schuldnern

Im Jahre 1984 startete die Deutsche Bundespost auf der Stuttgarter Messe Telematica ihren „Bildschirmtext"-Dienst, kurz Btx genannt. Btx gehört zu den sog. Datenmehrwertdiensten, die international als Videotext-Dienste bezeichnet werden, in Frankreich z. B. mit dem Namen Télétel. Der häusliche Fernseher oder PC, – durch Zusatzgerät verbunden mit dem Telefonanschluß, – ermöglicht es nicht nur, einfache Informationen – Fahrpläne, Börsenkurse usw. – abzurufen, sondern auch Telex- oder Telefaxmitteilungen abzusenden und schafft den Zugang zu kommerziellen Datenbanken, die Auskunft etwa über aktuelle Gesetzgebungsverfahren geben. Einige Informationsangebote sind kostenlos; für die kostenpflichtigen nimmt die Telekom das Inkasso der Entgelte vor, indem sie diese über die Telekomrechnung einzieht und sie an die Informationsanbieter weiterleitet.

Nachdem Btx jahrelang kränkelte – erst für 1995 werden schwarze Zahlen erwartet –, scheint 1993 mit einer technischen und Marketing-Umstellung die Trendwende erreicht worden zu sein: Btx wurde umbenannt in „Datex–J", mit mehr Komfort und zusätzlichen Leistungsmerkmalen versehen und erreichte 1994 eine Teilnehmerzahl von fast 700 000.

Bei der Gestaltung der rechtlichen Rahmenbedingungen für Btx wurde der „Unbeobachtetheit" des Nutzers stets besondere Bedeutung beigemessen: Auch elektronische Informationsmedien sollen vom Bürger genutzt werden können, ohne daß dies registriert und Dritten zur Kenntnis gegeben wird. Nach der Telekom-Datenschutzverordnung (TDSV) darf die Telekom einen Informationsanbieter überhaupt nur darüber informieren, daß und wann ein bestimmter Btx-Teilnehmer sein Angebot in Anspruch genommen hat, wenn dieser das vom Anbieter verlangte Entgelt auch nach Mahnung nicht bezahlen will. Anfang 1992 erreichten mich gehäuft Beschwerden, die Telekom verstoße gegen diese Vorschrift: Die Petenten hatten zwar entgeltpflichtige Informationsdienste in Anspruch genommen, die von der Telekom – als Inkassostelle für die Anbieter – in Rechnung gestellten Entgelte jedoch bezahlt, was zweifelsfrei geklärt werden konnte. Dennoch wurden die betreffenden Informationsanbieter – fälschlich – informiert, der Btx-Teilnehmer verweigere die Bezahlung von Entgelten, wobei auch mitgeteilt wurde, welche Informationsdienste wann in Anspruch genommen wurden und wie hoch das Entgelt war. Bis heute ist ungeklärt, ob die Telekom vor dieser – falschen – Information wie dies ihre Pflicht gewesen wäre – die Btx-Teilnehmer gemahnt hat, und ihnen somit Gelegenheit gegeben hätte, den fälschlichen Vorwurf zurückzuweisen. Fest steht lediglich, daß die fristgerecht eingegangenen Zahlungen viel zu spät verbucht wurden, wodurch aus ordentlichen Zahlern „Schuldner" wurden.

Das Vorgehen der Telekom in diesem Falle ist nicht nur ein Verstoß gegen formale Rechtspflichten: Wenn der Bürger die Besorgnis haben muß, Tatsache und Einzelheiten der Nutzung bestimmter Medien würden registriert und ausgewertet, so beeinträchtigt dies nicht nur sein Recht auf informationelle Selbstbestimmung, sondern auch auf Meinungsfreiheit aus Artikel 5 Abs. 1 Grundgesetz. An die sichere Gestaltung der Verfahren, die eine „versehentliche" oder fälschliche Datenübermittlung an die Informationsanbieter verhindern müssen, sind daher hohe Anforderungen zu stellen.

Die Telekom hat dargelegt, das beschriebene Problem resultiere aus der seinerzeit besonderen Arbeitsüberlastung der betroffenen Dienststellen und sei noch im Zusammenhang mit der Wiedervereinigung zu sehen; die bestehende Organisation sei grundsätzlich geeignet, einen ordnungsgemäßen Betriebsablauf sicherzustellen. Ich werde dies aufmerksam beobachten.

20.2.7 Telefon-„Geheimnummer" im Sichtfenster der Telefonrechnung

Auch im Berichtszeitraum beschwerten sich Bürger wieder darüber, daß ihre Telefonnummern im Sichtfenster der Telekom-Rechnung und auf Telefonbuch-Abholkarten ausgedruckt wurden und somit die Möglichkeit einer unbefugten Kenntnisnahme gegeben war, obwohl sie Ihre Telefonnummern gemäß § 10 Abs. 3 der Telekom-Datenschutzverordnung (TDSV) nicht im Telefonbuch hatten eintragen lassen. Nach den bestehenden Regelungen hätte es in diesem Fall unterbleiben müssen.

Die Telekom erklärte anfänglich, daß es sich hier um einzelne Arbeitsfehler gehandelt habe, die in einem „Massengeschäft" wie der Rechnungslegung für Telefonkunden hin und wieder vorkommen.

Diese Erklärung kann nur dann gelten, wenn es sich tatsächlich um seltene Ausnahmefälle handelt: Der Verordnungsgeber hat das Recht des Bürgers, nicht gegen seinen Willen in ein Telefonverzeichnis eingetragen zu werden, auch auf Drängen aus parlamentarischen Kreisen in die TDSV aufgenommen. Die steigende Anzahl der „Nichteintragungswünsche" belegt ein Bedürfnis vieler Bürger, ihre Telefonnummer nur gezielt, im Einzelfall, weiterzugeben. Wird durch einen „Arbeitsfehler" die Telefonnummer an falscher Stelle auf Telekom-Rechnungen und Abholkarten ausgedruckt, erfahren von ihr – entgegen dem erklärten Wunsch und ohne daß es erforderlich wäre – Dritte sowohl im Bereich der Deutschen Post AG als auch beim Empfänger der Fernmelderechnung.

Sicherlich sind insbesondere bei „Massenverfahren" Arbeitsfehler nie auszuschließen. Die Häufung von Eingaben der genannten Art legten jedoch den Eindruck nahe, die eingesetzten Verfahren und/oder einschlägigen Regelungen begünstigten oder förderten die Arbeitsfehler, die hier zugrunde lagen. Ich bat die Telekom deshalb, die betreffenden Verfahren und Regelungen eingehend zu überprüfen und nötige Ergänzungen oder Änderungen vorzunehmen.

Nach einer zehnmonatigen „Denkpause" informierte mich die Telekom im August 1994 darüber, daß sie wegen der aufgetretenen Arbeitsfehler die Ablauforganisation bei der Erstellung der Telekom-Rechnungen dergestalt geändert habe. Der Kundenwunsch des Nichteintrags in das Telefonbuch erreicht den Fernmelderechnungsdienst jetzt auf direktem Wege. Damit sollte das Problem eigentlich gelöst sein.

Gleichzeitig wurde ich jedoch auf ein grundsätzliches Problem hingewiesen, das mit der Rechnungsschreibung der Telekom zusammenhängt. Aus Gründen der Wirtschaftlichkeit sowie zur gleichmäßigen Auslastung des Personals der Telekom und der Rechenzentren schreibt und versendet die Telekom an jedem der zwanzig Arbeitstage, die normalerweise im Monat zur Verfügung stehen, ein Zwanzigstel der rund 40 Millionen Telekom-Rechnungen. Infolgedessen ist der Telefonanschluß jedes Kunden einer bestimmten Absendegruppe zugeordnet, so daß die Rechnungen jeden Monat ungefähr am gleichen Tag geschrieben und versandt werden. Eingabeschluß für Veränderungsdaten ist jeweils vier Tage vor Absendung der Telekom-Rechnung. Wenn nun ein Kunde z. B. den Wunsch für einen Nichteintrag im Telefonbuch der Telekom mitteilt, kann unter Berücksichtigung der Bearbeitungszeiten bei der Telekom der Eingabeschluß für Veränderungsdaten im Fernmelderechnungsdienst gerade vorbei sein. Der Kunde erhält dann – leider – noch einmal eine Rechnung mit der Fernmeldekontonummer im Sichtfenster, weil der Kundenwunsch erst zur nächsten Rechnungsschreibung berücksichtigt werden kann. Dies muß man allerdings auch im Lichte der Tatsache sehen, daß eine Revision des Telefonbuches erst möglich ist, wenn es neu gedruckt wird.

Ich wünschte mir jedoch, die Telekom würde auch den Telekom-Kunden über die Hintergründe und Zusammenhänge des Problems – z. B. beim Vorbringen seines Wunsches auf Nichteintrag in das Telefonbuch – informieren.

20.2.8 Rufnummernanzeige überraschte Telefonanrufer

Mit großem Nachdruck betreibt die Deutsche Bundespost Telekom die Modernisierung ihres Telefonnetzes, nämlich die Digitalisierung der Vermittlungsstellen: Gesteuert durch die am Telefon gewählte Rufnummer werden in den Vermittlungsstellen der Telekom Leitungsabschnitte „hintereinander geschaltet", so daß nach Ende der Wahl eine durchgehende Leitung etwa von Bonn bis zum gewünschten Teilnehmer in Berlin durchgeschaltet ist. Dieser Vorgang erfolgt derzeit immer noch zu einem erheblichen Teil mit Hilfe der sog. Wählertechnik; hierbei werden die Verbindungen durch mechanische Schalter hergestellt, die von Motoren gesteuert werden. Diese veraltete Technik wurde in den sog. Fernvermittlungsstellen, die die Ballungsräume miteinander verbinden, inzwischen vollständig durch moderne digitale Vermittlungsstellen ersetzt. Im Ortsbereich sieht dies jedoch anders aus; hier sind erst etwa ein Drittel aller Telefone an digitale Vermittlungsstellen angeschlossen. Besonders aber hier ist die Einführung der modernen Technik für den Kunden von erheblicher Bedeutung. Sie ermöglicht eine Reihe von Leistungsmerkmalen, die zum Teil völlig neu sind, zum Teil einfacher und komfortabler realisiert werden können. Dies gilt z. B. für die Anrufumleitung, mit der zu Hause ankommende Anrufe etwa zu Bekannten umgeleitet werden können, bei dem der Anschlußinhaber zu Besuch ist. Auch kann die Telekom dem Kunden eine detaillierte Telefonrechnung („Einzelverbindungsnachweis") erstellen, auf der er für jede Verbindung u. a. Zeitpunkt, Dauer und Entgelt erkennen kann (siehe Nr. 20.2.4; vgl. auch 14. TB S. 118 f.).

Aufregung und zum Teil Empörung entsteht bei vielen Telefonkunden jedoch häufig wegen eines „unerwünschten Leistungsmerkmals": Typisch ist der Fall eines Bürgers, der bei der Einkommenssteuerstelle seines Finanzamtes eine bestimmte Auskunft erbitten wollte. Bevor er seine Frage formulieren konnte, unterbrach ihn der Sachbearbeiter: „Wie ich aus Ihrer Telefonnummer sehen kann, wohnen Sie ja im Stadtteil X; dafür ist das Finanzamt Außenstadt zuständig." Ein anderer Bürger war bei einem Anruf

bei einem großen Versandhaus sofort mit seinem Namen angesprochen worden, noch bevor er sich gemeldet hatte.

In beiden Fällen hatten die Bürger von einem „normalen" Telefon aus angerufen, das allerdings – als sogenannter ANIS-Anschluß – an einer digitalen Vermittlungsstelle angeschlossen war. Demgegenüber verfügten die Angerufenen – Finanzamt bzw. Versandhaus – über Telefonanlagen, die an das ISDN (Integrated Services Digital Network) – Netz der Telekom angeschaltet sind, das Versandhaus zudem über einen Computer, der an der Telefonnummer sofort den Kunden erkannte. Bei Verbindungen zwischen solchen Anlagen oder zu einem ISDN-Einzelanschluß, den sich jeder Bürger anstelle des normalen Telefonanschlusses mieten kann, wird die Rufnummer des Anrufers zum Angerufenen übertragen und bei diesem auf dem Display seines Telefons angezeigt. Gerade dieses Leistungsmerkmal war seinerzeit bei Einführung des ISDN Gegenstand heftiger Diskussionen sowohl in der Öffentlichkeit als auch im parlamentarischen Bereich. Es bestand Konsens, daß der Anrufer die Möglichkeit haben muß, die Rufnummernanzeige generell oder im Einzelfall zu unterdrücken. Dahingehende und weitere Regelungen bezüglich des ISDN fanden Eingang in die Telekom-Datenschutzverordnung (13. TB S. 48 f.).

Völlig unvereinbar mit dem Recht auf informationelle Selbstbestimmung ist es, daß ein Anrufer – wie in den beschriebenen Fällen – „geoutet" wird, ohne daß er auch nur über die diesbezüglichen technischen Möglichkeiten informiert ist, geschweige denn über sie ebenfalls verfügt. Die Deutsche Bundespost Telekom hat daher auch gegenüber dem Ausschuß für Post und Telekommunikation des Deutschen Bundestages die Zusage gegeben, daß eine solche „heimliche" Übermittlung der Rufnummern von normalen Telefonanschlüssen an ISDN-Anschlüsse jedenfalls nicht ohne Einwilligung des Kunden erfolgen darf. Die Generaldirektion der Telekom hat in allen von mir kritisierten Fällen mitgeteilt, es habe sich um Fehler in der Software neu in Betrieb genommener Vermittlungsstellen gehandelt, die eine regelwidrige Rufnummernübermittlung zur Folge gehabt habe. Da diese Fälle jedoch immer wieder auftreten, sind Zweifel angebracht, ob die vorgesehenen technischen und organisatorischen Maßnahmen und Regelungen ausreichen, eine Wiederholung wirksam zu verhindern. Ich habe die Generaldirektion der Deutschen Bundespost Telekom um eine Stellungnahme gebeten; sie lag mir bei Redaktionsschluß noch nicht vor.

20.2.9 „Lauschangriff" für jedermann

Die Verkaufszahlen beweisen es: Der technische Fortschritt hält besonders auf dem Telekommunikationsmarkt Einzug in den häuslichen Bereich. Wenn man den Zahlen glauben darf, so wurden in den vergangenen Jahren weit mehr als eine Million Anrufbeantworter verkauft. Anlaß zur Sorge gibt die Tatsache, daß die meisten der heute angebotenen Anrufbeantworter die Möglichkeit der Fernabfrage, zum Teil sogar der Fernbedienung aller Gerätefunktionen aufweisen. Denn durch die unzureichenden Sicherheitsmechanismen dieser Geräte besteht die Möglichkeit des Mithörens von Gesprächen im Raum und Abhörens gespeicherter vertraulicher Mitteilungen.

Bei der **Fernabfrage** – von einem beliebigen Telefonanschluß aus – wird dem Anrufbeantworter mittels des (Tonwahl-)Telefons selbst oder eines Bediengerätes („Code-Sender") – dieser ist in einschlägigen Elektronikgeschäften für 5,– Mark zu beziehen – ein aus mehreren Tönen bestehendes Signal zugesandt, mit dem der Fernabfragende sich identifiziert und die Bedienvorgänge einleitet. Üblicherweise besteht das Signal aus nur zwei oder drei unterschiedlichen Tönen (Schutzcode), die somit leicht auszuspähen oder durch Ausprobieren zu erraten sind. Telekommunikationsteilnehmer, die über ein entsprechendes Wissen und einen PC verfügen, können mit Hilfe eines Zusatzgerätes (Modem) in Sekundenschnelle durch ein Programm die Codierung ermitteln, ohne daß dies mit erheblichen Kosten verbunden wäre. Ist der Schutzcode erst einmal bekannt, können – wie dargelegt – die im Anrufbeantworter gespeicherten Mitteilungen abgehört werden.

Durch Aktivieren der Raumüberwachungsfunktion ist sogar ein Mithören der Gespräche in den Räumlichkeiten, in dem das Gerät aufgestellt ist, möglich (siehe Abbildung 4 „Lauschangriff" für jedermann).

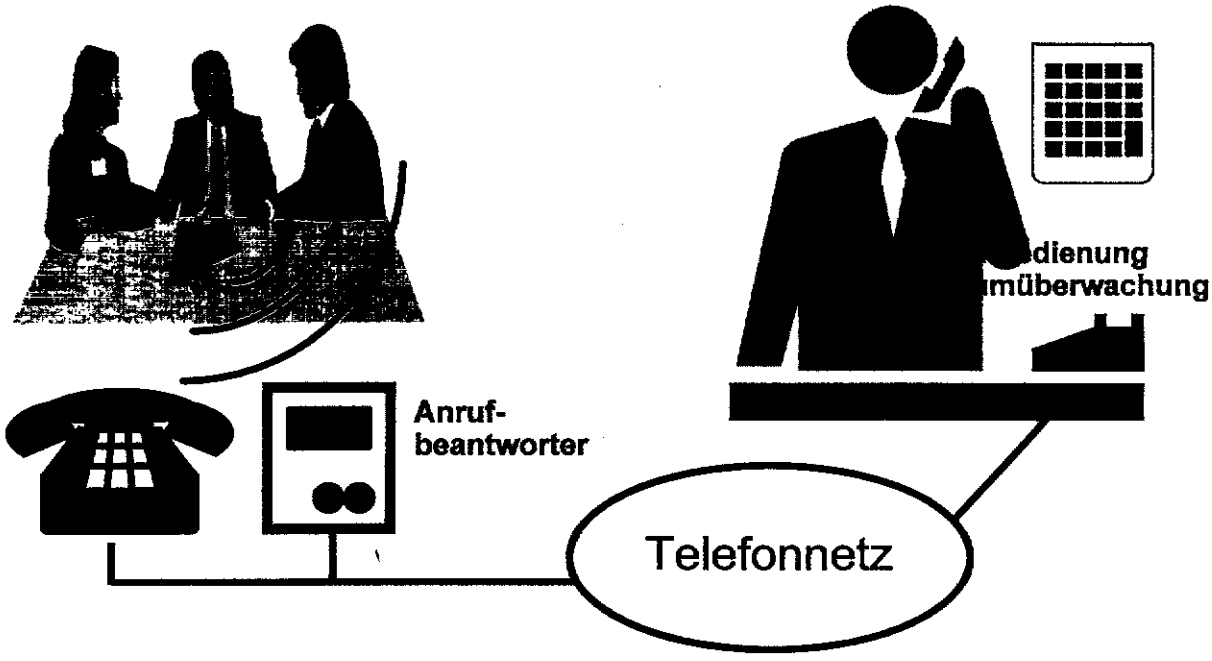
Wie mir berichtet wurde, verfügt ein Teil der Geräte auch über eine sogenannte „Notfallsicherung" für den Fall, daß der berechtigte Fernabfragende die richtige Codierung vergessen hat oder sie nach einem Stromausfall gelöscht worden ist. Für diesen Fall braucht er angeblich lediglich die Codierung „000" am Fernabfragegerät einstellen und hat somit Zugang zu dem Gerät; der ohnehin geringe Schutz gegen unerlaubtes Mithören wird damit völlig aufgehoben: Der „Lauschangriff" für jedermann ist somit realisierbar. Ich habe mich deshalb an das Bundesministerium für Post und Telekommunikation gewandt, damit bei der Zulassung der Geräte auf bessere Schutzmechanismen geachtet wird. Dies erscheint aber wegen geltender EU-Vorschriften nicht möglich.

In diesem Zusammenhang stellt sich auch die Frage, inwieweit Personen, die auf diese Weise Kenntnis von Daten erhalten, mit Strafverfolgung rechnen müssen. Nach den Darlegungen des zuständigen Bundesministeriums der Justiz ist die unbefugte Fernabfrage von Anrufbeantwortern nur dann ein Vergehen im Sinne des § 202a des Strafgesetzbuch (Ausspähen von Daten), wenn der Besitzer eines solchen Gerätes auf geeignete Schutzmechanismen in dem Anrufbeantworter selbst achtet und diese auch individuell bestimmt hat. Sollten ungeeignete Schutzmechanismen, z. B. nur einstelliger Schutzcode oder eine Notfallsicherung mit der Ziffernfolge „000", eingesetzt werden, so scheidet eine Strafbarkeit nach § 202a Strafgesetzbuch aus.

Ich habe daher sowohl die Arbeitsgemeinschaft der Verbraucherverbände als auch weitere Institutionen des Verbraucherschutzes auf diese Sicherheitslücke hingewiesen und gebeten, die Verbraucher über diese Schwachstellen von Anrufbeantwortern zu informieren. Dies wurde mir zugesagt.

Abbildung 4

„Lauschangriff" für jedermann



Entscheidend ist auch, daß Hersteller und Vertreiber ihre (Mit-)Verantwortung wahrnehmen und auf sicherheitsgefährdende Leistungsmerkmale verzichten, jedenfalls die Anwender besser als bisher über Sicherheitsprobleme sowie deren Minderungsmöglichkeiten informieren. Dabei sollte auch nicht vergessen werden, daß besondere Schutzmechanismen für den Wettbewerb von Vorteil sein können.

In einem Rundschreiben an die obersten Bundesbehörden vom 28. März 1994 habe ich auf die Gefahren beim Einsatz von Anrufbeantwortern hingewiesen und Empfehlungen zur Begrenzung der Risiken gegeben (siehe Anlage 20).

20.2.10 Vorsicht vor „Mithörern" in Telefonanlagen

Der technische Fortschritt wird häufig zuerst am Arbeitsplatz bemerkt: Während zu Hause bei vielen Bürgern immer noch das vertraut-schlichte Telefon mit Wählscheibe steht, hat der Büroapparat inzwischen nicht nur eine Tastatur mit vielen Knöpfen, sondern oft auch ein Anzeigedisplay und einen Lautsprecher. Nach einiger Eingewöhnungszeit stehen dem Nutzer damit eine Reihe komfortabler Leistungsmerkmale zur Verfügung, die ihm die Arbeit wesentlich erleichtern können. Die moderne Technik bringt jedoch mit sich, daß Telefonate – anders als früher – „Datenspuren" erzeugen, die (auch mißbräuchlich) ausgewertet werden können; ich habe hierüber beispielhaft im 14. TB (S. 123 f.) berichtet.

Während die genannte Problematik inzwischen weitgehend bekannt und auch zunehmend in Dienst- und Betriebsvereinbarungen geregelt wurde, ist ein anderer Aspekt der modernen Telefonanlagen – heute zumeist „Telekommunikationsanlagen" (TK-Anlagen) genannt – bislang wenig beachtet worden:

Große Bedeutung kommt aus verfassungsrechtlicher Sicht der Vertraulichkeit des nichtöffentlich gesprochenen Wortes zu. Der Bürger muß im Regelfall davon ausgehen können, daß ein Gespräch, das er mit einem anderen führt, nicht heimlich belauscht oder aufgezeichnet wird. Angesichts der großen Bedeutung von Telefongesprächen gerade im beruflichen Bereich muß dies grundsätzlich auch hierfür gelten. Die Technik der modernen TK-Anlagen schafft hier jedoch Gefährdungen, die erkannt und begrenzt werden müssen. Bereits der heute bei vielen Telefonen vorhandene Lautsprecher ist nicht unproblematisch, wenn er ohne Wissen des entfernten Partners heimlich eingeschaltet wird. Häufig ist daher gefordert worden, daß dies dem Partner zumindest – z. B. durch einen Hinweiston – signalisiert werden müßte; leider hat weder der Bundesminister für Post und Telekommunikation als Verordnungsgeber dem Rechnung getragen noch ist dies von der Industrie bisher realisiert worden.

Sehr viel kritischer ist das fast immer vorhandene Leistungsmerkmal „Aufschalten" zu sehen. Hierbei kann sich ein Dritter – etwa die Telefonistin oder

auch der Chef – auf bestehende Verbindungen aufschalten und dann mithören oder -sprechen. Zwar wird jedenfalls bei den Anlagen der großen deutschen Hersteller dieser Vorgang durch einen besonderen Hinweiston signalisiert, ein Mißbrauch ist aber schon dann gegeben, wenn dessen Lautstärke verändert werden kann und das Aufschalten somit unbemerkt bleibt.

Erhebliche Probleme gibt es auch bei Telefonapparaten mit Freisprechmöglichkeit, in die ein Mikrofon eingebaut ist und mit denen somit telefoniert werden kann, ohne daß der Hörer abgenommen zu werden braucht. Ist in der TK-Anlage das Leistungsmerkmal „Direktansprechen" installiert, wird dieser Apparat durch einen Anruf eingeschaltet, ohne daß der Besitzer tätig werden muß: Überhört er das Anrufsignal oder erfolgt der Anruf, bevor er das Zimmer betritt, kann der Anrufer alles belauschen, was im Zimmer gesprochen wird.

Ähnliche Probleme ergeben sich auch bei der gern genutzten „Konferenzschaltung", mittels der mehrere Telefonteilnehmer gleichzeitig telefonieren können. Nicht alle TK-Anlagen machen deutlich, wenn ein Teilnehmer die „Telefonkonferenz" verläßt, so daß dieser es vielleicht nur vorgibt und somit heimlich mithören kann.

In einem Rundschreiben an die obersten Bundesbehörden vom 27. Dezember 1993 habe ich auf die Problematik der Mithörmöglichkeiten in modernen TK-Anlagen hingewiesen und um Bekanntgabe auch im nachgeordneten Bereich gebeten (siehe Anlage 21).

Auch das Bundesamt für Sicherheit in der Informationstechnik hat inzwischen eine Arbeitsgruppe gebildet, die sich vertieft sowohl mit diesen Problemen, als auch generell mit der Sicherheit solcher Anlagen gegen Manipulationen und anderen unbefugten Zugriffen befaßt: Da es sich bei modernen TK-Anlagen um Computer handelt, ist auch hier grundsätzlich eine Manipulation durch Veränderung der Software möglich. Dies schließt auch die Möglichkeit ein, daß ein Fachkundiger „von draußen", also außerhalb des Dienstgebäudes von einem weltweit beliebigen Telefonanschluß aus, Zugang zur Betriebssoftware der TK-Anlage erhält und dort heimlich und gezielt Telefonate abhört. Das BSI will die Sicherheit marktgängiger TK-Anlagen gegen diese und andere Bedrohungen untersuchen und darüber berichten. Ich habe dies ausdrücklich begrüßt und gehe davon aus, daß bei der Bewertung der Risiken von praxisnahen Annahmen ausgegangen wird.

20.2.11 Mailboxsysteme – chaotische Zustände

Fragen zu Datenschutz und Datensicherung beim Betrieb und bei der Nutzung von sog. Mailboxsystemen sind auch an mich herangetragen worden, mehr aber noch an die Aufsichtsbehörden für den nichtöffentlichen Bereich, mit denen ich im sog. Düsseldorfer Kreis im Informationsaustausch stehe.

Wie schon der Name zum Ausdruck bringt, handelt es sich bei Mailboxsystemen um computergestützte „Postfachanlagen": Jedem Teilnehmer („User") wird vom Systembetreiber („Sysop") ein elektronisches Postfach, eine „Mailbox", eingerichtet. Die „Anschrift" dieser Mailbox, die im Regelfall auch den Namen des Mailboxinhabers enthält, wird öffentlich zugänglich gemacht, insbesondere auch im Teilnehmerverzeichnis des betreffenden Mailboxsystems, das auch von „Nichtteilnehmern" eingesehen werden kann. Häufigste und wichtigste Anwendung von Mailboxsystemen ist die „Elektronische Post": Jeder, der über die nötige technische Ausstattung verfügt, kann einem User in dessen Mailbox elektronische Nachrichten hinterlegen; nur der User selbst – und (leider auch) der Sysop – kann die Mailbox öffnen und die hinterlegten Nachrichten lesen. Die Nachrichten können dabei sowohl aus Texten und Graphiken bestehen, können aber auch (vom Computer ausführbare) Programme darstellen oder enthalten. Außer persönlichen Mailboxen enthält jedes Mailboxsystem auch Informationen, die Jedermann zugänglich sind und sein sollen („Schwarzes Brett").

Eine zunehmende Bedeutung gewinnen solche Mailboxen, die nicht zur Aufnahme von Nachrichten für den Inhaber bestimmt sind, sondern den Zugang zu sog. Mehrwertdiensten öffnen. Wird eine solche Mailbox vom User angewählt, kann sie z. B. den Zugang zu großen Datenbanken, wie z. B. JURIS, eröffnen, ohne daß der User Mitglied der Nutzergemeinschaft der Datenbank sein muß. Eine andere Mailbox wiederum ermöglicht es, Texte per Telefax abzusenden, ohne daß der Absender ein Telefaxgerät besitzt: Er gibt einfach den für den Empfänger bestimmten Text und dessen Anschrift ein und der Rechner des Mailboxsystems übernimmt die Absendung.

Als User eines Mailboxsystemes benötigt man lediglich einen PC mit Kommunikationsmöglichkeit, ein sog. Modem, das über das öffentliche Telefonnetz die Verbindung zum Mailboxsystem herstellt. Die technische Ausgestaltung eines solchen Systems ist sehr unterschiedlich: Im einfachsten Fall besteht dieses ebenfalls lediglich aus einem PC mit Modem, kommerzielle Anbieter setzen hier mittlere bis größere Rechenanlagen ein. Zu letzteren gehört neben etwa einem Dutzend privater Anbieter auch die Deutsche Bundespost Telekom mit ihrem System Telebox 400. Die Anzahl der kommerziellen Systembetreiber ist gering und auch die – überschaubare – Anzahl ihrer User steigt nur langsam. Um ein Vielfaches größer ist jedoch die Zahl der nicht- oder halbkommerziellen Anbieter; in die Millionen geht allein die Anzahl der deutschen Nutzer, da sie, wie ausgeführt, lediglich ein PC mit Modem benötigen – wovon es in Deutschland sicher über eine Million gibt. Unüberschaubar ist nicht nur die Anzahl der Systembetreiber, sondern auch die Leistungsfähigkeit der Systeme sowie Zielsetzung und Ausgestaltung der Angebotsinhalte. Eine Fachzeitschrift hielt es daher letztlich für erforderlich, nach „Ordnung im wilden Mailbox-Westen" zu rufen und auf die Rechtspflichten hinzuweisen, die sich für den Betreiber eines Mailboxsystems ergeben. Weitgehend unbekannt ist z. B., daß nach den Vorschriften des Fernmeldeanlagengesetzes (FAG) Betreiber ihre Anlage nicht nur beim Bundesamt für Post und Telekommunikation anmelden müssen (§ 1 a Abs. 1 Satz 1 FAG), sondern daß sie grundsätzlich

auch zur Wahrung des Fernmeldegeheimnisses (§ 10 FAG) verpflichtet sind – und der entsprechenden Strafdrohung unterliegen.

Da in jedem Mailboxsystem neben den Inhaltsdaten auch andere personenbezogene Daten erhoben, verarbeitet und genutzt werden, nämlich sowohl der User als auch der Mitarbeiter des Betreibers, sind auch datenschutzrechtliche Vorschriften zu beachten. Hier ist insbesondere auf § 32 BDSG zu verweisen, nach dem eine Meldepflicht gegenüber der zuständigen Aufsichtsbehörde besteht. Als wichtige bereichsspezifische Vorschrift ist § 15 der TDSV/UDSV zu nennen, der die Datenverarbeitung bei „Nachrichtenübermittlungssystemen mit Zwischenspeicherung" regelt.

Ein besonderes Problem, das zunächst nicht datenschutzrechtlicher Art ist, ergibt sich aus der Möglichkeit, ein Mailboxsystem zur Sammlung und zur Verbreitung strafbarer Nachrichteninhalte zu benutzen. So wurde bereits in der Frühzeit des Btx-Dienstes (siehe Nr. 20.2.6) dieser zur Verbreitung pornographischer Inhalte und in der letzten Zeit auch von Angeboten zur Kinderprostitution benutzt. Auch wissen die Strafverfolgungsbehörden von Mailboxsystemen zu berichten, mittels derer rechtsradikale Organisationen sowohl Nachrichtenaustausch betreiben als auch ihre Mitteilungsorgane drucktechnisch erstellen und den Vertrieb dieser Druckschriften organisieren. Daraus ergibt sich zunächst die Frage, wie die einzelnen Phasen einer „Mailboxverbindung", insbesondere die in einer Mailbox gespeicherten Nachrichten, rechtlich zu qualifizieren sind, und auf welche Rechtsvorschriften z. B. eine polizeiliche „Durchsuchung" der Mailbox gestützt werden kann (siehe Nr. 4.3).

20.2.12 Immer noch keine europäische ISDN-Richtlinie

In vielen Stellungnahmen und Entschließungen der Europäischen Union wurde die Entwicklung der Telekommunikation als ein zentraler Punkt zur Verwirklichung des gemeinsamen Marktes angesehen. Inzwischen wurden zahlreiche Richtlinien für diesen Bereich erlassen, andere werden zur Zeit erarbeitet. Aus Sicht des Datenschutzes kommt es hierbei darauf an, daß jedenfalls gleichzeitig mit der Harmonisierung der Telekommunikationsnetze und -dienste die rechtlichen Rahmenbedingungen geschaffen werden, um ein hinreichendes Niveau zum Schutz personenbezogener Daten und der Privatsphäre von Unionsbürgern zu gewährleisten. Die Kommission der Europäischen Gemeinschaft hat am 13. Juni 1994 den geänderten Vorschlag für eine „Richtlinie des Europäischen Parlaments und des Rates zum Schutz personenbezogener Daten und der Privatsphäre in digitalen Telekommunikationsnetzen, insbesondere im diensteintegrierenden digitalem Telekommunikationsnetz (ISDN) und digitalen Mobilfunknetzen" (im folgenden: ISDN-Richtlinie) vorgelegt (EG-Amtsblatt C 200 vom 22. Juli 1994, S. 4 f.).

Die ISDN-Richtlinie war im Anschluß an den Europäischen Rat von Edinburgh auf eine Liste anhängiger Rechtsetzungsmaßnahmen gesetzt worden, die von der Kommission unter dem Gesichtspunkt der Subsidiarität erneut überprüft werden sollten. Erfreulich ist zunächst, daß die Kommission auch unter Subsidiaritätsgesichtspunkten an der Richtlinie festhält; insgesamt hat die Richtlinie jedoch zahlreiche Streichungen und Änderungen erfahren und das datenschutzrechtliche Niveau abgenommen. Insbesondere in folgenden zentralen Punkten scheint daher eine Nachbesserung dringend geboten:

- Die Regelungen der Richtlinie gelten gem. Artikel 3 Abs. 1 (Betroffene Dienste) in vollem Umfang nur für Telekommunikationsorganisationen. Bei Diensteanbietern – die selbst keine Netze betreiben, nur deren Nutzung vermarkten – sind nach Abs. 2 dieser Vorschrift nur die Artikel 4 bis 6, 11, 14 und 16 anwendbar. Aus datenschutzrechtlicher Sicht sollte die Anwendbarkeit auch der übrigen Artikel für Diensteanbieter festgelegt werden. Dies gilt insbesondere für Artikel 7 (Einzelgebührennachweis): Im Mobilfunkbereich wird regelmäßig der Einzelgebührennachweis durch den Diensteanbieter erstellt.
- Artikel 4 a. F. wurde gestrichen. In Abs. 1 dieser Regelung war bisher der sogenannte Zweckbindungsgrundsatz verankert; der Umgang mit personenbezogenen Daten sollte grundsätzlich nur für Telekommunikationszwecke zulässig sein. Nach der Neufassung wäre es möglich, daß diese Daten auch für andere Zwecke (z. B. Adressenhandel) genutzt werden. Die Regelungen der allgemeinen Datenschutzrichtlinie können diese Schutzlücke nicht auffangen. Nach Artikel 4 Abs. 2 a. F. war die Erstellung von Kommunikationsprofilenelektronischen Profilen ohne die Einwilligung der Betroffenen untersagt. Auch die Streichung dieser Vorschrift stellt einen deutlichen Rückschritt in datenschutzrechtlicher Hinsicht dar.
- Durch den jetzt gestrichenen Artikel 5 a. F. war bisher festgelegt, daß die Verwendung der personenbezogenen Daten des Teilnehmers nur erfolgen sollte, soweit dies erforderlich ist, und daß diese Daten nach Beendigung der Vertragsbeziehungen zu löschen sind. Auch diese Regelung stellt eine wesentliche Forderung des Datenschutzes dar und sollte wieder aufgenommen werden.
- Hinsichtlich des nunmehr gestrichenen Artikel 7 a. F., der die Vertraulichkeit bei der Datenverarbeitung sicherstellen sollte, hatte ich eine Formulierung gefordert, die – etwa in Anlehnung an die des deutschen Fernmeldeanlagengesetzes – die Einhaltung eines definierten Fernmeldegeheimnisses verlangt und auch eine Strafbewehrung vorsieht (vgl. 13. TB S. 55). Durch die Streichung der gesamten Vorschrift ist ein weiterer datenschutzrechtlicher Aspekt verloren gegangen.
- Artikel 5 Abs. 2 (Daten für die Gebührenabrechnung) läßt die Speicherung der Gebührendaten für die Dauer der Anfechtungsfrist zu. In den einzelnen Mitgliedstaaten bestehen höchst unterschiedliche Fristenregelungen. So ist es denkbar, daß riesige zentralisierte Datensammlungen mit vollständigen Kommunikationsprofilen über Jahre hinweg entstehen. Aus meiner Sicht sollte hier ein Lösungsmodell gewählt werden, das dem Kunden

eine Wahlmöglichkeit – ähnlich wie das in der TDSV vorgesehene – läßt. Ein solches Modell sollte jedoch eine Höchstdauer der Speicherungsfrist vorsehen. Wählt der Teilnehmer die sofortige Löschung, könnte das Telekommunikationsunternehmen von einer Vorlagepflicht der Gebührendaten zu Beweiszwecken befreit werden.

- Artikel 7 (Einzelgebührennachweis) sieht für die detaillierte Telefonrechnung nicht mehr die Verkürzung der Rufnummer vor. Dies ist aus meiner Sicht hinnehmbar, wenn der Schutz der Betroffenen durch eine andere Gestaltung (z. B. „niederländisches Modell", vgl. Nr. 20.3) sichergestellt wird. Bleibt es allerdings bei der jetzigen Formulierung, so muß klarstellend eine zusätzliche Bestimmung zum Schutz der privilegierten Stellen (z. B. Telefonseelsorge) i. S. von § 6 Abs. 9 S. 5 TDSV/USDV aufgenommen werden.
- Zu begrüßen ist in Artikel 11 (Teilnehmerverzeichnisse), daß über die zur Identifizierung erforderlichen Daten hinaus weitere nur dann eingetragen werden dürfen, wenn der Teilnehmer zugestimmt hat. Auch kann der Teilnehmer verlangen, überhaupt nicht in das Teilnehmerverzeichnis aufgenommen zu werden. An dieser Stelle fehlt es allerdings an einer ähnlichen Regelung für die Rufnummernauskunft. Auch die Gebührenfreiheit des Ausschlusses der Eintragung ist nicht realisiert worden.

Ich habe das Bundesministerium für Post und Telekommunikation gebeten, diese Forderungen in den entsprechenden Gremien der Europäischen Union einzubringen, um eine Nachbesserung zu erreichen. In meinen Forderungen bin ich von den Landesbeauftragten für den Datenschutz (s. Anlage 13) und von der Konferenz der Europäischen Datenschutzbeauftragten (siehe Anlage 14) unterstützt worden. Die Richtlinie darf weder rechtlich noch und faktisch zu einer Senkung des Datenschutzniveaus in den Staaten führen, die über ein hohes Niveau verfügen. Ohne eine europäische Regelung mit hohem und verbindlichem Schutzniveau bestünde die Gefahr, daß sich die Mitgliedsstaaten mit hoch entwickeltem Datenschutz durch den internationalen Wettbewerbsdruck veranlaßt sehen, ihr Schutzniveau zurückzunehmen. Daher kommt der Schaffung eines hinreichenden Datenschutzniveaus auf europäischer Ebene eine besondere Bedeutung zu. Anderenfalls könnten – in den einzelnen Mitgliedstaaten oft mühsam erreichte, dem Schutz des Persönlichkeitsrechts dienende – nationale datenschutzrechtliche Regelungen unter dem Gesichtspunkt der Vermeidung von Wettbewerbsverzerrungen unanwendbar werden.

20.3 Postdienst

20.3.1 Neue Postleitzahlen – Persönliches Adreßheft

Der Postdienst führte am 1. Juli 1993 die fünfstellige Postleitzahl (PLZ) in Deutschland ein. Diese Aktion wurde durch intensive Werbung unterstützt, und für die größeren Adressenbestände waren automatisierte Umstellverfahren verfügbar. Die Benutzung der neuen PLZ durch private Haushalte wurde von der Post durch die Werbeaktion „Mein persönliches Adreßheft" gefördert. Etwa 35 Millionen Haushalte erhielten das Angebot für die kostenlose Erstellung und Zusendung eines Adreßheftes mit der eigenen neuen PLZ-Anschrift und der Umstellung von bis zu neun weiteren Anschriften, die in einen beigefügten Erfassungsbeleg eingetragen werden sollten.

Die Aktion war kaum angelaufen, als sich Bürger bei mir über die „Adressensammelei" der Post als den Beginn eines umfangreichen Adreßhandels beklagten und mich um Prüfung der Aktion baten. Die Befürchtungen von Verbraucherverbänden und Journalisten wurden auch dadurch genährt, daß die Rücksendung nach Gütersloh erfolgte, das als Sitz eines bedeutenden Werbeunternehmens bekannt ist.

Die Sätze in der Ausfüllanleitung „Vertraulichkeit ist zugesichert. Die Belange des Datenschutzes werden korrekt eingehalten." vermochten die Bedenken nicht auszuräumen. Denn von einigen wurde die Freiwilligkeit nicht richtig erkannt, und es fehlte eine klare Zusicherung, daß die Adressen ausschließlich für die Herstellung und Zusendung des Adreßheftes verwendet und danach gelöscht würden. Auch war der Nutzen der Aktion für den Postdienst für viele so undeutlich, daß sie weitere Nutzungen befürchteten. Das war im einzelnen datenschutzrechtlich nicht unbedingt zu beanstanden, zum Teil aber ungeschickt dargestellt. Es wirkte insgesamt so verunsichernd auf viele Bürger, daß ich der Post diese Bedenken darlegte und mich mit der Vorbereitung und Durchführung der Werbeaktion näher befaßte.

Schon meine erste Nachfrage bei der Generaldirektion Postdienst ergab, daß die Aktion als datenschutzrechtlich unbedenklich angesehen wurde. Deshalb war die dort für den Datenschutz zuständige Stelle nicht beteiligt worden, was sich als nachteilig erwies. Denn deren Erfahrungen wären bei der Formulierung von Erläuterungen vermutlich hilfreich gewesen.

So war zwar im Anschriftenerfassungsbeleg vorgesehen, daß als erstes die eigene Anschrift eingetragen werden sollte, der Zweck dieser Vorgabe – **an diese Anschrift wurde das fertige Heft adressiert** – war aber nicht genannt. Aus unterschiedlichen Gründen, z. B. weil man sich selbst nicht gern zuerst nennt, trug eine Reihe von Bürgern dort eine andere Anschrift ein, z. B. die ihres wichtigsten Korrespondenzpartners. Besonders beunruhigt waren dann die Bürger, die unerwartet an ihre Anschrift ein Heft mit einigen Adressen ihnen bekannter Personen, aber auch von völlig Unbekannten zugesandt bekamen. Sie vermuteten, daß bei dieser Aktion alles drunter und drüber ginge und die Datensicherung mangelhaft sei. Viele dieser Fälle habe ich bis zu den Originalbelegen zurückverfolgt und stets festgestellt, daß tatsächlich als erste Adresse im Beleg die Anschrift des Petenten stand. Nur selten war auf dem Erfassungsbeleg die eigene Anschrift des Bestellers dann noch besonders gekennzeichnet, was beim maschinellen Verarbeiten nicht berücksichtigt wurde, mir aber bei der Beratung des Petenten half.

Die Teilnehmer waren auch nicht darauf vorbereitet, daß alle Anschriften automatisch geprüft und dabei

nicht nur viele Straßen-Umbenennungen in der ehemaligen DDR berücksichtigt, sondern auch falsche Schreibweisen von Straßennamen durch die richtige ersetzt wurden. In einigen dieser Fälle waren die Bürger dann besorgt, weil man sich doch intensiver als erwartet mit ihren Angaben beschäftigt hatte.

Weil bei vielen Millionen zu prüfender Anschriften eben zwingend, erfolgte die Korrektur automatisch durch den Vergleich der gelesenen Straßennamen mit der für jeden Ort angelegten Straßennamen-Sammlung. Jeweils der am ehesten zutreffende Name wurde dann als richtig eingesetzt. Für den Ort Lathen ergab sich z. B. dadurch ein Fehler, daß die tatsächlich vorhandene Straße „Kösterskamp" nicht in der Sammlung aufgeführt war. Diese Angabe wurde dann „verbessert" und zwar auf den vorhandenen Namen „Everskamp". Ein Bürger von Lathen, der selbst ein Adreßheft bestellt hatte, erhielt daraufhin mit der falschen Adressierung „Everskamp" ein Adreßheft mit einigen Anschriften, die er nicht angegeben hatte, und außerdem mit derselben falschen Anschrift auch Zuschriften von Firmen. Sein Vertrauen in die Post war sowohl hinsichtlich der Ausführung seines Auftrages als auch hinsichtlich der Geheimhaltung erschüttert. Dabei war die falsche Adressierung durch die Firmen, die vorher stets seine richtige Adresse verwendet hatten, leicht dadurch zu erklären, daß auch die Adressenbestände dieser Firmen mit derselben Datenbasis umgestellt worden waren. In diesem Fall habe ich die Korrektur der Daten angeregt und die Post in Lathen auf die zu erwartenden Adressierungsfehler hingewiesen.

Das Unterlassen der intensiven Beschäftigung mit den Datenschutzfragen hat auch dazu geführt, daß beim Abschluß des Vertrages mit dem Unternehmen, das für die Post wesentliche Arbeiten dieser Aktion übernahm, Datenschutzvorschriften nicht beachtet wurden. Von dem Unternehmen wurden nicht posttypische Arbeiten, wie Annahme der von den Interessenten nach Gütersloh geschickten Briefe, automatisiertes Lesen der in die Erfassungsbögen eingetragenen Adressen, Ersetzen der alten Postleitzahlen durch die neuen, Druck der Adreßhefte und Anliefern der Adreßhefte zum Postversand, übernommen. Dazu hatte das Unternehmen für einzelne Arbeitsschritte wie z. B. das Lesen der Erfassungsbögen Unteraufträge an andere Firmen vergeben. Anders als in § 11 BDSG gesetzlich vorgeschrieben, enthielt der von der Post mit dem Unternehmen geschlossene Vertrag aber keine Regelungen für die Vergabe solcher Unteraufträge.

Außerdem waren die ebenfalls schriftlich festzulegenden technischen und organisatorischen Maßnahmen nur unklar beschrieben. So war z. B. nur vereinbart, daß die Belegformulare „nach Erfassung vernichtet" werden, ohne daß über die Vernichtungstechnik oder die Sicherheitsstufe der Datenträgervernichtung entsprechend der dafür bestehenden Norm (DIN 32757) Angaben gemacht wurden. Diese Vereinbarung war auch hinsichtlich des Vernichtungszeitpunktes kaum durchdacht, denn bei näherer Betrachtung stellte sich heraus, daß für die Bearbeitung von Reklamationen die Belege noch mehrere Monate nach der Erfassung aufbewahrt werden mußten. Das war zwar datenschutzrechtlich zulässig, hätte nach § 11 BDSG aber im schriftlichen Vertrag eindeutig und richtig geregelt werden müssen.

Die Verstöße gegen die gesetzlichen Vorgaben für den Abschluß von Verträgen über Datenverarbeitung im Auftrag haben zwar nicht feststellbar zu unzulässigen Nutzungen der Daten geführt. Weil der Vertrag aber Millionen von Anschriften und Kommunikationsbeziehungen betraf, konnte ich die Verstöße nicht als unerheblich ansehen und habe sie deshalb förmlich beanstandet. Die Generaldirektion hielt die Beanstandung zwar für nicht gerechtfertigt, räumte die datenschutzrechtlichen Versäumnisse aber ein und erklärte, in ähnlichen Fällen künftig die Fachseite zu beteiligen.

20.3.2 Ergänzung des Nachsendeverfahrens

Im Nachsendeverfahren gab es ab Juli 1994 formale und inhaltliche Veränderungen, an denen ich beratend mitgewirkt habe. Das Formblatt enthält jetzt eine bessere Unterscheidung zwischen Nachsendung wegen vorübergehender Abwesenheit – in der Regel weniger als sechs Monate, wie z. B. bei Urlaub – und Nachsendung wegen Umzugs. Die Verwechslung der beiden Nachsendegründe führte bisher gelegentlich dazu, daß dem Absender irrtümlich eine vorübergehende Anschriftenänderung mitgeteilt wurde, die er dann für endgültig hielt (s. 14. TB S. 114).

Eine wesentliche Veränderung ist, daß mit Einwilligung des Postkunden bei Umzug die Änderung seiner Anschrift an Dritte zum Zwecke der Anschriftenkorrektur gegeben werden kann. Auch bisher konnten die Angaben der Nachsendeanträge zur Adressenkorrektur genutzt werden: Wenn eine Sendung mit dem Vermerk „Falls verzogen nicht nachsenden, sondern mit neuer Anschrift zurück" versehen war, und der Adressat bei seinem Nachsendeantrag dem nicht widersprochen hatte, notierte der Zusteller die neue Anschrift auf der Sendung und sandte sie an den Absender zurück. So soll auch zukünftig verfahren werden. Das neue, zusätzliche Korrekturverfahren ist für große Anschriftenbestände, z. B. von Versicherungen, Versandhäusern und Direktwerbeunternehmen, aber wesentlich einfacher und kostengünstiger, weil es vorab und automatisiert abläuft.

Diese Korrektur wird als Dienstleistung von der unter Mehrheitsbeteiligung der Post gemeinsam mit der Firma Reinhard Mohn GmbH Gütersloh gegründeten „Deutsche PostAdress GmbH" angeboten. Dabei werden die alten Adressenbestände mit den Daten der Nachsendeanträge abgeglichen und die gefundenen alten Adressen durch die neuen ersetzt. Das Hinzufügen neuer Adressen erfolgt nicht. Die Vereinbarungen zwischen der Post und der PostAdress GmbH tragen den datenschutzrechtlichen Belangen ausreichend Rechnung.

Das Verfahren dient auch dem umziehenden Postkunden, weil es zuverlässiger wirkt als das bisherige. Denn wenn eine Sendung an die alte Anschrift adressiert wurde, nachdem die Halbjahresfrist des Nachsendeantrages abgelaufen war, konnte die neue Anschrift oft nicht gefunden werden. Das neue Ver-

fahren wirkt aber genauso undifferenziert wie das alte, insbesondere wird der Strom unerwünschter Werbung durch den Umzug nicht verkleinert. Wer aber die Einwilligungserklärung streicht und auch der Anschriftenmitteilung widerspricht, muß selbst und auf eigene Kosten dafür sorgen, daß seine neue Anschrift an diejenigen gelangt, deren Zuschriften ihm erwünscht sind.

20.3.3 Alle Jahre wieder

Seit vielen Jahren ist es gute Übung bei der Post, Briefe, die „an den Weihnachtsmann" oder „das Christkind" geschrieben werden, nicht zu vernichten oder als unzustellbar zu behandeln, sondern dem Absender einen Weihnachtsgruß zu senden. In den Weihnachtspostämtern in Orten wie Engelskirchen, Himmelpfort, Himmelpforten oder Himmelsthür gehen von Jahr zu Jahr mehr solcher Weihnachtsbriefe ein, in denen sich Wunschzettel, Gedichte oder Grüße befinden oder in denen die Post nur schlicht um die Briefmarke mit dem weihnachtlichen Sonderstempel gebeten wird.

Gelegentlich berichten Kinder auch über ihre guten Vorsätze oder von ihren Sorgen. Und nicht nur Kinder schütten ihr Herz aus: Auch von manchen Erwachsenen lesen die Helfer in den Postämtern Lebensberichte und Sorgen, die früher vielleicht nur dem Pfarrer ausgebreitet worden wären. Man würde der Mühe, die sich viele Kinder mit ihren Briefen, Bildern und verzierten Wunschzetteln gemacht haben, sicher nicht gerecht, wenn man alles nach dem Absenden des Antwortbriefes vernichten würde. Aber auch wenn diese Postämter hier nicht in der Funktion des Zustellers, sondern als Empfänger dieser Briefe zu sehen sind, so müssen sie beim Umgang mit diesen Briefen, z. B. bei Ausstellungen und Berichten, gleichwohl die Geheimnisse der Absender wahren.

Die damit gesetzten Grenzen wurden sicher überschritten, als Tausende von Kinderbriefen aus einem Weihnachtspostamt an einen Autor übergeben wurden, der etwas darüber schreiben wollte, ohne daß zuvor wirklich gesichert war, daß dabei die Anonymität der Briefeschreiber gewahrt würde. Im Gegenteil, der Autor nutzte die Adressen der Kinder, um deren Eltern anzuschreiben, für sein im wesentlichen aus der systematisierten Wiedergabe der Kinderbriefe und Wunschzettel bestehendes Werk zu werben und ihnen anzubieten, auf dafür reserviertem Platz – gegen Aufpreis – den Brief ihres Kindes abzudrucken.

Zunächst war für mich nicht zu klären, wer für die Beantwortung und Verwahrung der Briefe verantwortlich war. Deshalb haben meine Mitarbeiter sich in diesem Postamt über die allgemein übliche Bearbeitung und die Umstände der Zweckentfremdung der Briefe informiert. Dabei hat sich ergeben, daß die Briefe in Räumen des Postamts beantwortet, die Antworten mit Mitteln der Post dort frankiert und anschließend die Briefe auch vom Postdienst vernichtet werden. Auch wenn in diesem Einzelfall eine Person die Briefe unvorsichtig herausgegeben hat, und in diesem Amt auch ehrenamtliche Helfer – aus Verbundenheit mit der Post, für ihre Stadt und um in der Weihnachtszeit anderen eine Freude zu machen – viel zum Erfolg beitragen, so liegt die Gesamtverantwortung bei der Post.

Die Post hat mir inzwischen mitgeteilt, daß sie ihrer Verantwortung entsprechend alle Beteiligten in den Weihnachtspostämtern auf die besondere Verantwortung in angemessener Form hinweisen wird, damit derartige Fehler in Zukunft vermieden werden und Erwachsene wie Kinder vertrauensvoll an den Weihnachtsmann schreiben können, alle Jahre wieder.

20.4 Postbank

20.4.1 Kontrolle der Postbank München

Schwerpunkte meiner Kontrolle und Beratung bei der Niederlassung der Postbank (früher: Postgiroamt) in München waren neben der Kontonummer im Anschriftenfeld (s. Nr. 20.4.2) das Kontoeröffnungs-Verfahren, die Sperrdatei und die Stellung des behördlichen Datenschutzbeauftragten.

Für die Eröffnung eines Privat-, Gemeinschafts- oder Geschäfts-Girokontos sind jeweils unterschiedliche Anträge auszufüllen. Mit diesen Formblättern werden neben den für die Kontoführung erforderlichen Daten noch zusätzlich „persönliche" und „freiwillige" Kundendaten erhoben, die gegenwärtig weder benötigt noch automatisiert gespeichert werden. Dazu zählen z. B. Geburtsort, Familienstand, Staatsangehörigkeit, Anzahl der Kinder, Nettoeinkommen, vorherige Anschrift und Arbeitgeber. Als Grund wurde genannt, daß diese Angaben möglicherweise für statistische Zwecke und Scoring-Verfahren in einer weiteren Ausbaustufe der gegenwärtig für die Kontoführung angewandten Softwarelösung genutzt werden würden. Nach § 3 der Postbank-Datenschutzverordnung (PB-DSV) dürfen aber Kundendaten nur erhoben werden, soweit es im Rahmen der Zweckbestimmung von Vertragsverhältnissen erforderlich ist. Die Generaldirektion der Postbank begründet die Erhebung dieser Daten als „unumgänglich" und mit dem Argument der banküblichen Sorgfalt, obwohl einige dieser Daten gegenwärtig noch nicht genutzt werden. Damit ist zu erwarten, daß die Daten im Zeitpunkt ihrer erstmaligen Nutzung schon veraltet sind.

Zur Weitergabe von Warnungen und zur Sperrdatei habe ich auch im Berichtszeitraum wieder Eingaben erhalten (s. auch 12. TB S. 46). Die Sperrdatei wird von der Postbank zentral geführt, und die Aktualisierung regelmäßig an alle Niederlassungen versandt. Eine Überschreitung der Löschungsfristen habe ich hier nicht festgestellt. Die seit dem 1. Juli 1991 gültigen Regelungen in den §§ 4 und 5 PB-DSV halte ich für sachgerecht. Die von der Postbank herausgegebenen Warnmitteilungen über Kunden, die ihr Postbank-Konto vertragswidrig mißbraucht haben, gehen der Niederlassung schriftlich zu, werden in die Sperrdatei übernommen und in Hand- und Ablageakten aufbewahrt. Eine gleiche Akte wird in der Betriebssicherung geführt. Hier stellte ich allerdings Überschreitungen der Löschungsfrist fest. Es waren noch Mitteilungen vorhanden, die nach der Rechtslage hätten gelöscht sein müssen. Weiterhin bestanden organisatorische Mängel, deren Ausmaß Zweifel an

der Wirksamkeit und an der Erforderlichkeit dieser Datenverarbeitung begründet. Ebenso war die Vorschriftenlage in der Niederlassung nicht klar. Die Generaldirektion hat mir mitgeteilt, die darauf beruhenden Mängel seien inzwischen abgestellt.

Die Postbank hat für die Durchführung des Datenschutzes nach § 18 Abs. 1 BDSG in jeder Niederlassung einen internen Datenschutzbeauftragten bestellt. Die effektive Wirkung war in der Niederlassung München allerdings eher gering, da sich in dieser Position 1994 drei Bedienstete abwechselten. Der zur Zeit der Kontrolle gerade mit dieser Aufgabe betraute Mitarbeiter hatte für den Datenschutz keine Zeit. Er war mit seinen Arbeitsaufgaben im Controlling voll ausgelastet, obwohl auch nach Einschätzung der Niederlassungsleitung für die Datenschutzaufgaben eine halbe Arbeitskraft erforderlich wäre. Ein Teil der während der Kontrolle festgestellten Defizite – auch beim Paßwort-Schutz von PC's und der Altpapier- und Magnetband-Vernichtung – ist sicher Folge dieses Kapazitätsmangels. Daraus resultierte auch ein erheblicher Nachholbedarf an Schulung für den Datenschutzbeauftragten und die Mitarbeiter. Diese Situation war insgesamt inakzeptabel. Die personelle Unterbesetzung wurde inzwischen behoben, und für die Datenschutzbeauftragten in den Niederlassungen sind jetzt besondere Schulungsmaßnahmen vorgesehen.

20.4.2 Kontonummer im Anschriftenfeld

Auch in diesem Berichtszeitraum war die im Anschriftenfeld der Kontoauszugsbriefe aufgedruckte Kontonummer Gegenstand vieler Beschwerden von Postbank-Kunden (s. auch 14. TB S. 117). In der Niederlassung München habe ich geprüft, ob und weshalb die Kontonummer von außen erkennbar sein muß.

Der überwiegende Teil der gedruckten Kontoauszüge wird ohne Zusortierung weiterer Belege maschinell kuvertiert, verschlossen und versandt. Die Angabe der Kontonummer im Anschriftenfeld ist hier nicht erforderlich.

Für die Kontoauszüge, zu denen noch zusätzliche Belege z. B. von anderen Banken oder von Postämtern zusortiert werden müssen, ist nach dem gegenwärtigen Verfahren die Kontonummer hilfreich. Diese Zusortierung wird manuell vorgenommen. Warum die Kontonummer nicht so auf den Auszug gedruckt werden kann, daß sie im Brieffenster nicht sichtbar, von der Sortierkraft beim manuellen Zusortieren aber dennoch leicht erkennbar ist, konnte nicht geklärt werden.

Für die als weiteres Argument genannte Zuführung von nicht zustellbaren Kontoauszugsbriefen zu den jeweiligen Kontounterlagen muß die Kontonummer auch nicht im Anschriftenfeld stehen. Diese Briefe wurden generell erst geöffnet und dann entsprechend zugeordnet. Auch für einen gerade laufenden Betriebsversuch zur Behandlung derartiger Rückläufer ist die Kontonummer im Anschriftenfeld nicht zwingend notwendig.

Zur Kontonummer auf den Anschriftenaufklebern wurde übereinstimmend mit der Postbank festgestellt, daß diese nicht erforderlich ist. Ein kurzfristiges Weglassen halte ich hier für möglich, da diese Aufkleber nach einem anderen Verfahren gedruckt werden.

Die Postbank wird durch eine Programmänderung die Kontonummer zukünftig so ausdrucken, daß sie durch das Fenster des Umschlags nicht sichtbar ist, für Kontoauszüge mit manuell zusortierten Belegen soll es bis auf weiteres bei dem derzeitigen Verfahren bleiben. Für die Kunden der ab 1. Januar 1995 privatisierten Postbank wäre der Wegfall dieser immer wieder Bedenken und Ärger hervorrufenden Kontonummer im Anschriftenfeld nur zu wünschen.

20.4.3 Geburtsdaten-Nacherhebung bei Altkunden

Die Postbank Niederlassungen haben ab Ende 1993 die Altkunden zur Nachmeldung des Geburtsdatums aufgefordert, soweit es nicht in den Stammdaten ihres Privat-Girokontos gespeichert war. Die Niederlassung Berlin gab für diese Datenerhebung keine Begründung, von anderen Niederlassungen wurde als Grund eine zweifelsfreie Zuordnung der Konten zu bestimmten Personen, die Sicherung des Kontos gegen unberechtigte Zugriffe und eine höhere persönliche Sicherheit genannt. Diese Begründungen schienen vielen der betroffenen Kunden so unklar, daß sie sich mit ihren Bedenken an mich wandten.

Die Rechtsgrundlage für die Frage nach dem Geburtsdatum ist die Abgabenordnung, die in § 154 Abs. 2 vom Kontoführer fordert, sich Gewißheit über die Person des Verfügungsberechtigten zu verschaffen und die Angaben in geeigneter Form festzuhalten. Auch die Postbank-Datenschutzverordnung läßt diese Erhebung ausdrücklich zu, und nach den Allgemeinen Geschäftsbedingungen der Postbank ist das Geburtsdatum neben Namen, Anschrift, Vertretungs- oder Verfügungsbefugnissen als wesentliche Tatsache der Geschäftsverbindung schriftlich mitzuteilen.

Ich habe dies den Postbankkunden näher erläutert.

Bedauerlich ist, daß es nicht schon von der Postbank für die betroffenen Altkunden nachvollziehbar erklärt werden konnte.

20.4.4 Telefonische Kontoauskünfte

Die Postbank führte im 2. Halbjahr 1992 einen neuen Kontoauszug ein und stellte ihre Kunden vor die Wahl, diesen Kontoauszug entgeltfrei nur noch einmal monatlich zu erhalten oder – gegen Entgelt – alle 14 Tage, wöchentlich oder wie bis dahin üblich nach jedem Buchungstag. Viele Kunden wählten lange Intervalle, und einige stellten bald fest, daß sie doch zwischendurch Informationen über bestimmte Buchungen oder den Kontostand benötigten. Für die deswegen häufigen telefonischen Erkundigungen wurde übergangsweise ein spezieller telefonischer Auskunftsdienst eingerichtet, weil die Einrichtung des geplanten computergestützten „Postbank Telefon-Service" noch nicht abgeschlossen war. Der Anrufende sollte dann Auskunft über seinen Kontostand

erhalten, wenn er bestimmte vorgegebene personenbezogene und kontospezifische Daten korrekt und zweifelsfrei angibt, um seine Berechtigung glaubhaft zu machen.

Leider haben sich einzelne Bankbedienstete nicht in jedem Fall daran gehalten. Wie mir einige Postbankkunden mitteilten, ist es im Einzelfall besonders überzeugend wirkenden Anrufern gelungen, unter Angabe von erheblich abweichenden Identifizierungsdaten entweder ihren eigenen Kontostand oder sogar den des Bekannten oder Kollegen zu erfragen. Das war ein klarer Verstoß gegen die Sorgfaltspflicht im Umgang mit Kontodaten, gegen die Vorschriften zur Datensicherheit gem. Ziffer 6 der Anlage zu § 9 BDSG sowie eine Verletzung des Postgirogeheimnisses nach § 6 Postgesetz. Ich habe mich sofort an die Generaldirektion der Postbank gewandt und auf die Mängel bei der Beachtung der Regelungen hingewiesen. Auch wenn die Mitarbeiter eines telefonischen Auskunftsdienstes sich zu Recht bemühen, einem Anrufer zu helfen, so darf diese Hilfe nicht die berechtigten Interessen der Kunden gefährden. Inzwischen ist diese Telefonauskunft durch den o. a. Telefonservice ersetzt worden, zu dessen Nutzung vom Kunden eine individuelle Geheimzahl einzugeben ist.

21 Wissenschaft und Forschung

21.1 Bundesarchiv-Militärarchiv/militärisches Zwischenarchiv Potsdam

Im Bundesarchiv-Militärarchiv/militärisches Zwischenarchiv (MA/MZA) in Potsdam befinden sich insbesondere Unterlagen der Nationalen Volksarmee der ehemaligen DDR (NVA) sowie die Unterlagen des militärischen Oberstaatsanwaltes der ehemaligen DDR (MOSTA). Eine Kontrolle im MA/MZA hat keine datenschutzrechtlichen Mängel ergeben.

Hinsichtlich der Nutzung der Unterlagen für die Forschung habe ich gegenüber dem Bundesarchiv darauf hingewiesen, daß für die in den Unterlagen vorhandenen personenbezogenen Daten die Schutzfristen aus dem Bundesarchivgesetz gelten. Weil nach diesem Gesetz die Schutzfristen für Personen der Zeitgeschichte und Amtsträger in Ausübung ihres Amtes die Schutzfristen verkürzt werden können, wenn die schutzwürdigen Belange der Betroffenen angemessen berücksichtigt werden, ist es möglich, viele der Unterlagen der wissenschaftlichen Forschung zur Verfügung zu stellen.

21.2 Bundesarchiv – ehemaliges Berlin-Document-Center

Nach dem „Abkommen zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Vereinigten Staaten von Amerika über die Übertragung der Berliner Dokumentenzentrale auf die Bundesrepublik Deutschland" vom 8. Oktober 1993 (BGBl. II S. 2033) wurde am 1. Juli 1994 das frühere Berlin-Document-Center in deutsche Verwaltung überführt. Es wird jetzt als Außenstelle Berlin-Zehlendorf vom Bundesarchiv verwaltet. Das Bundesarchiv hat damit die ca. 11 Millionen Karteikarten umfassende Mitgliederkartei der NSDAP, mehr als 360 000 Personalunterlagen der SS (davon ca. 62 000 von SS-Offizieren), Personalunterlagen von mehr als einer halben Million SA-Angehörigen sowie ca. 240 000 Dossiers des SS-Rasse- und Siedlungshauptamtes übernommen, die Aufnahmegesuche in die SS sowie Verlobungs- und Verheiratungsgesuche von SS-Angehörigen enthalten. Hinzu kommen noch Millionen von Akten und anderen Unterlagen von verschiedenen Gliederungen der NSDAP und verschiedener Reichsbehörden.

Bei einem Informationsbesuch konnte ich mich von der datenschutzgerechten Verwahrung und Nutzung der Unterlagen überzeugen. Das Bundesarchiv gewährt den Zugang zu diesem für die zeitgeschichtliche Forschung wichtigen Archivbestand unter angemessenen Auflagen und Beschränkungen.

22 Statistik

22.1 Statistik in der Europäischen Union

22.1.1 Statistikverordnung der Europäischen Gemeinschaft

Einen Entwurf der Verordnung über das Gemeinschaftliche statistische System (GSS), über den ich berichtet hatte (14. TB S. 126), hat die Kommission der Europäischen Gemeinschaften unter dem Titel „Vorschlag einer Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik" vorgelegt. Die Vorlage dieser in ihrer Bedeutung dem Bundesstatistikgesetz entsprechenden allgemeinen Regelung für die Gemeinschaftsstatistik ist ein kleiner aber wichtiger Schritt, um auch für die Daten bei den Organen der EU Schutzregelungen einzuführen. Gegen einzelne Punkte des derzeitigen Entwurfes habe ich jedoch Bedenken (s. auch Anlage 8, Beschluß der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Statistik der Europäischen Union).

So habe ich gefordert, daß die in der EG-ÜbermittlungsVO Nr. 1588/90 (s. hierzu 13. TB S. 60) getroffene Regelung für die statistische Geheimhaltung beibehalten wird. Danach sind die von den statistischen Ämtern der Mitgliedstaaten gelieferten, geheimzuhaltenden Daten vom Statistischen Amt der Europäischen Gemeinschaften (EUROSTAT) so zu schützen, wie sie in den jeweils liefernden Mitgliedstaaten geschützt werden. Wenn die Kommission stattdessen eine EU-weit einheitliche Definition einführen möchte, dann darf dadurch der Schutz nicht hinter dem erreichten Standard zurückbleiben.

Besonders wichtig ist auch, ob EUROSTAT oder einer anderen Dienststelle der Kommission statistische Angelegenheiten zugewiesen werden. Denn nur für EUROSTAT können aufgrund der EG-ÜbermittlungsVO Nr. 1588/90 die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen für die statistische Geheimhaltung ge-

troffen werden, was zu einem großen Teil auch schon erfolgt ist. Der derzeit vorliegende Verordnungsvorschlag überläßt diese Aufgabenzuweisung einer jederzeit revidierbaren Organisationsentscheidung der Kommission. Damit bestünde die Gefahr, daß zur Erstellung von Statistiken erhobene Daten an unterschiedliche Stellen der Kommission übermittelt werden, wo sie dann weniger wirksam geschützt werden und u. a. auch zu Kontrollzwecken verwendet werden könnten. Deshalb habe ich gefordert, in der Verordnung selbst EUROSTAT als die für die Erstellung von Statistiken der Union zuständige Stelle zu bestimmen. Nach den mir vorliegenden Informationen soll ein neuer Verordnungsvorschlag dies vorsehen. Auch für die Arbeit von EUROSTAT gilt aber, daß es weiterhin an einer für die Organe der Europäischen Union zuständigen unabhängigen und effektiven Datenschutzkontrollinstanz fehlt (s. auch Nr. 33.6)

22.1.2 Umsetzung der EG-Unternehmensregisterverordnung

Die Verordnung über die innergemeinschaftliche Koordinierung des Aufbaus von Unternehmensregistern für statistische Verwendungszwecke (EG-UnternehmensregisterVO Nr. 2186/93), die die Möglichkeit des Zugriffs der statistischen Ämter der Mitgliedstaaten auf unternehmensbezogene administrative und gerichtliche Register zum Zwecke der statistischen Auswertung erlaubt und über die ich berichtet habe (14. TB S. 126f.), ist in Kraft getreten. Im Gegensatz zu den Vorentwürfen wurde vom Rat EUROSTAT als Empfänger der statistischen Daten bestimmt und außerdem auf die EG-ÜbermittlungsVO Nr. 1588/90 Bezug genommen, womit meine Bedenken berücksichtigt wurden.

Das Bundesministerium für Wirtschaft hat mittlerweile einen Gesetzentwurf zur Durchführung dieser Verordnung vorgelegt, der eine Änderung und Ergänzung der gesetzlichen Vorschriften für die zu nutzenden Register (insbesondere Handelsregister und die Register der Industrie- und Handelskammern und der Bundesanstalt für Arbeit) vorsieht.

22.2 Mikrozensusgesetz

Ende 1995 wird das Mikrozensusgesetz 1990 außer Kraft treten. Das BMI bereitet deshalb seit einiger Zeit eine Nachfolgeregelung vor. Es hat nunmehr einen Vorentwurf eines „Gesetzes zur Neuregelung der Repräsentativerhebung über die Bevölkerung und den Arbeitsmarkt sowie die Wohnsituation der Haushalte (Mikrozensusgesetz)" vorgelegt. Das künftige Mikrozensusgesetz soll danach – auch entsprechend einer Forderung des BMJ und mir – weiterhin ein Zeitgesetz bleiben. Gegen die nunmehr angestrebte Erhöhung der zeitlichen Geltungsdauer von fünf auf acht Jahre habe ich keine Bedenken, da dies ein Zeitraum ist, der dem Gesetzgeber die Möglichkeit gibt, danach vertieft auf die vom Bundesverfassungsgericht im Volkszählungsurteil geforderte Methodendiskussion einzugehen. Bei der Novellierung sollen jetzt u. a. Erfahrungen mit der im Mikrozensusgesetz 1990 für eine Reihe von Fragen eingeräumten Freiwilligkeit berücksichtigt und der Fragenkatalog den aktuellen Notwendigkeiten angepaßt werden.

22.2.1 Die Freiwilligkeit von Antworten

Im Mikrozensusgesetz 1990 wurde nach kontrovers geführter öffentlicher Diskussion über die bislang praktizierte weitgehende Auskunftspflicht für einige weitere Fragen die Freiwilligkeit der Beantwortung eingeführt (s. hierzu auch 12. TB S. 55). Gegen die Ausdehnung der Freiwilligkeit bei der Beantwortung von Fragen sprach damals u. a., daß in Testerhebungen nur Antwortquoten von 50 bis 60 % erreicht wurden und jeder Ausfall die Zuverlässigkeit der aus der Stichprobe hochgerechneten Schätzungen verringert. Das BMI, die Fachressorts und das Statistische Bundesamt gehen davon aus, daß die für die unterschiedlichen Verwendungszwecke des Mikrozensus erforderliche Zuverlässigkeit und Genauigkeit der Daten am besten durch die Anordnung der Auskunftspflicht der Bürger gewährleistet werden kann. Für die Freiwilligkeit sprach die Vermutung, daß unter Zwang gegebene Auskünfte eher falsch sein könnten als freiwillige Angaben und daß gewisse Einbußen an Genauigkeit als Preis für das Mehr an Selbstbestimmung hinnehmbar seien.

Erwartungsgemäß gab es bei den Fragen ohne Auskunftspflicht spürbare Ausfälle. Daß die Bürger, die von ihrem Recht Gebrauch machen, den Erhebungsbogen selbst auszufüllen und dann an das Statistische Landesamt zu senden, eher die Beantwortung der freiwillig beantwortbaren Fragen verweigern als diejenigen, deren Antworten von einem Interviewer in den Erhebungsbogen eingetragen werden, überrascht ebenfalls nicht. Überraschend war für mich allerdings das Ergebnis einer wissenschaftlichen Untersuchung zur Freiwilligkeit, nach der bei den freiwillig zu beantworteten Fragen die Ausfallquote nicht wie befürchtet bei 40 % lag, sondern bei den Ausländern betreffenden Fragen im Durchschnitt um 20 % und bei den übrigen untersuchten Fragen nur um 10 % (vgl. Emmerling/Riede, Wirtschaft und Statistik 1994, S. 435ff.). Teilweise, etwa bei den Fragen zur Pendlereigenschaft, lag die Ausfallquote unter 5 %. Allerdings machten bei den 15- bis 20jährigen Befragten bei der Frage nach ihrem letzten beruflichen Ausbildungsabschluß mehr als 45 % keine Angabe, was darauf zurückzuführen ist, daß sehr viele dieser Befragten davon überzeugt waren, ihren letzten beruflichen Ausbildungsabschluß noch nicht erreicht zu haben.

Aus statistisch-wissenschaftlicher Sicht sind diese Ausfälle störend, für die Nutzung der Ergebnisse im Rahmen praktischer politischer Entscheidungen dürften die damit in den Hochrechnungen erzeugten Fehler aber tolerierbar sein. Dies zeigt sich besonders in den Antworten zum höchsten allgemeinen Schulabschluß. Hier gab es eine durchschnittliche Ausfallquote in Höhe von 9,2 %. Erst bei den über 65jährigen lag die Ausfallquote bei über 10 %, bei den über 75jährigen Befragten bei fast 15 %. Solche Ausfälle lassen sich zwar nicht zuverlässig kompensieren, soweit aber die Ergebnisse Grundlage politischer Entscheidungen sein sollen, dürften die relativ hohen Ausfälle in den genannten Altersgruppen die

Brauchbarkeit der statistischen Ergebnisse kaum beeinträchtigen. Deshalb sehe ich die bisherigen Ergebnisse mit der Freiwilligkeit als Ermutigung an, auf diesem Wege weiterzugehen.

22.2.2 Fragehäufigkeit und Erhebungskatalog

Erfreulich aus der Sicht der von den Befragungen betroffenen Bürgern ist, daß die Periodizität der Erhebungsmerkmale zum Teil erhöht worden ist, d. h. einzelne Fragen aus dem Gesamtprogramm des Mikrozensus müssen vom Bürger nicht mehr jährlich, sondern nur noch alle zwei Jahre oder nur noch alle drei oder vier Jahre beantwortet werden. Auch der Auswahlsatz, daß heißt die Anzahl der Bürger, die befragt werden sollen, ist bei einzelnen Erhebungsmerkmalen verkleinert worden. So sollen bei einzelnen Erhebungsmerkmalen nicht mehr ein Prozent der Bevölkerung befragt werden, sondern etwa bei den Fragen nach der Nichterwerbstätigkeit nur noch 0,45%. Insoweit tritt eine Entlastung ein.

Meine Kritik richtet sich aber noch immer dagegen, daß – obwohl sich das BMI gegenüber den noch weitergehenden Wünschen der Fachressorts zum Teil erfolgreich durchgesetzt hat – das Erhebungsprogramm ausgeweitet werden soll. Die Begründung, die Erweiterung des Erhebungsprogrammes habe ihren Grund in Vorgaben der EU, trifft nur zu einem Teil zu und begründet auch nicht ohne weiteres die Einbeziehung in den Mikrozensus. Die Diskussion um die zusätzlichen Erhebungswünsche ist noch nicht abgeschlossen.

22.3 Bevölkerungsstatistik

Die Novellierung des Bevölkerungsstatistikgesetzes ist in der letzten Legislaturperiode vom Bundesministerium des Innern aufgrund des Föderalen Konsolidierungsprogramms, das auch Einsparungen im Bereich Statistik vorsah, nicht mehr weiter verfolgt worden. Begründet wurde dieser Schritt mit fehlenden Haushaltsmitteln für die Mehrkosten der geplanten Änderungen des Erhebungsverfahrens.

In der Begründung zu dem Entwurf (vgl. 14. TB S. 127, siehe auch 11. TB S. 47 und 12. TB S. 98) hatte das Bundesministerium des Innern selbst festgehalten, daß die Neufassung des Gesetzes auch den Anforderungen des Bundesverfassungsgerichts im Volkszählungsurteil vom 15. Dezember 1983 Rechnung tragen sollte. Das Bundesministerium räumt damit ein, daß das Bevölkerungsstatistikgesetz – das zwar mit dem Gesetz vom 14. März 1980 neu gefaßt wurde, in seinem Kern aber aus dem Jahr 1957 stammt – nicht in vollem Umfang im Einklang mit dem Grundgesetz steht. Deshalb habe ich angeregt, die Arbeiten an der Novellierung fortzusetzen, dabei aber das Statistikprogramm kostenneutral nicht über die derzeit erhobenen Merkmale hinaus zu erweitern.

Auf meinen Vorschlag aus dem Frühjahr 1993 steht trotz Erinnerung bis heute eine Antwort aus. Mittlerweile haben auch Landesbeauftragte für den Datenschutz gegenüber den zuständigen Landesministerien und den statistischen Landesämtern, die die Erhebungen durchführen, verfassungsrechtliche Bedenken gegen die Weiterführung der Bevölkerungsstatistiken auf einer verfassungsrechtlich bedenklichen Grundlage geltend gemacht.

22.4 Sozialhilfestatistik

Mit dem Gesetz zur Umsetzung des Föderalen Konsolidierungsprogramms wurden die Regelungen über die Sozialhilfestatistik novelliert und in das Bundessozialhilfegesetz (BSHG) integriert. Nach dem Willen des Gesetzgebers sollte die Sozialhilfestatistik wie bisher als sog. Sekundärstatistik durchgeführt werden, d. h. die Angaben für die Statistik sollten ausschließlich aus den Verwaltungsunterlagen der auskunftspflichtigen Behörden und sonstigen öffentlichen Stellen erstellt werden. Offensichtlich ging der Gesetzgeber bei der Schaffung der neuen gesetzlichen Regelungen davon aus, daß die Angaben, die in die Sozialhilfestatistik einfließen sollten, in den Unterlagen der Sozialämter und der anderen Träger der Sozialhilfe enthalten sind, oder – soweit sie für die Arbeit der Sozialhilfeträger im Einzelfall nicht erforderlich und deshalb nicht gespeichert sind – auch für die Statistik nicht benötigt werden.

Bei der praktischen Umsetzung der neuen Bestimmung ergab sich, daß die Verwaltungsunterlagen oft nicht alle Angaben enthielten, die für die Sozialhilfestatistik vorgesehen waren. Denn die Lebenslagen der Sozialhilfeantragsteller sind sehr unterschiedlich, und entsprechend unterschiedlich waren die von den Sozialhilfeträgern für ihre Entscheidung benötigten Daten. Weil nach dem Willen des Gesetzgebers eine Sekundärstatistik durchgeführt werden sollte, wäre es richtig gewesen, nur die vorliegenden Daten zu melden. Statt dessen erhoben einige Träger der Sozialhilfe die für die Statistik ihrer Meinung nach fehlenden Daten beim Sozialhilfebewerber bzw. -empfänger, zum Teil mit der Drohung, bereits zugesagte Sozialhilfe zurückzuhalten, bis der Fragebogen ausgefüllt sei. Diese gegen das Bundessozialhilfegesetz und die Regeln des Statistikrechts verstoßende Praxis einiger Träger der Sozialhilfe wurde durch mehrere Landesbeauftragte für den Datenschutz aufgegriffen und abgemahnt.

In diesem Zusammenhang bestand mit dem Bundesministerium für Familie und Senioren Einigkeit, daß die von den Sozialämtern durchgeführten Nacherhebungen nur für den Zweck, Angaben für die Sozialhilfestatistik zu erlangen, unzulässig waren. Sinn und Zweck der Ausgestaltung der Sozialhilfestatistik als Sekundärstatistik werden außerdem auch dann verfälscht, wenn anhand des Datenkatalogs der Statistik „erkannt" wird, daß Daten, die man bisher für eine Entscheidung nicht benötigte, nun sogar für bereits getroffene Entscheidungen nacherhoben werden müssen.

Dieses Beispiel wird für mich Anlaß sein, künftig bei der Anordnung von Sekundärstatistiken noch genauer nachzufragen, ob die für die Erreichung des Zweckes der Statistik erforderlichen Daten tatsächlich in dem erforderlichen Umfang in den Verwaltungsunterlagen vorhanden sind, und wie der beschriebene Fehler vermieden werden kann.

22.5 Wehrmedizinalstatistik

Das Institut für Wehrmedizinalstatistik und Berichtswesen in Remagen (siehe auch 6. TB S. 53 und 7. TB S. 58) habe ich im Berichtszeitraum erneut datenschutzrechtlich kontrolliert. Wesentliche datenschutzrechtliche Mängel beim Umgang mit den Daten haben sich nicht ergeben.

Dringend geboten ist jedoch, daß die im Laufe der Zeit erheblich angewachsene Wehrmedizinalstatistik bald eine gesetzliche Grundlage erhält. Die ca. 140 vom Institut veröffentlichten Tabellen dienen neben Bundeswehrzwecken auch der Beantwortung von Anfragen aus dem parlamentarischen Raum, aber auch privaten Zwecken, etwa für Anfragen der Automobil- und Bekleidungsindustrie. Rechtlich handelt es sich hierbei um Bundesstatistiken, für die nach dem Bundesstatistikgesetz eine gesetzliche Grundlage erforderlich ist. Ich habe dem Bundesministerium der Verteidigung einen Vorschlag für eine entsprechende Ergänzung des Soldatengesetzes gemacht und darauf hingewiesen, daß auch das Wehrpflichtgesetz entsprechend ergänzt werden müßte.

22.6 Wahlstatistik wurde ausgesetzt

Bislang erhob die amtliche Statistik bei den bisherigen Bundestagswahlen Angaben über das Wahlverhalten der Bürgerinnen und Bürger mit Hilfe von farblich gekennzeichneten Stimmzetteln, aufgeteilt nach Geschlecht und fünf Altersgruppen. Weil insbesondere in kleineren Wahlbezirken theoretisch das Risiko bestand, daß bei der öffentlichen Auszählung der Stimmen in extremen Fällen das Wahlgeheimnis verletzt werden könnte, hat der Deutsche Bundestag für die Bundestagswahl am 16. Oktober 1994 die Durchführung der Wahlstatistik ausgesetzt.

Zwar ist bisher kein Fall allgemein bekannt, in dem wegen der Durchführung der Wahlstatistik das Wahlgeheimnis tatsächlich verletzt wurde. Nach der Diskussion vor der letzten Bundestagswahl halte ich es aber für erforderlich, das Verfahren der Wahlstatistik so zu ändern, daß das Risiko für die Durchbrechung des Wahlgeheimnisses weiter verringert wird. Ich habe daher angeregt, die für die Statistik vorgesehenen Wahlzettel so zu kennzeichnen, daß Beobachter im Wahllokal künftig das Wahlverhalten einzelner Gruppen nicht mehr erkennen können. Auch sollten die Wahlbezirke, die in die Statistik einbezogen werden, in jeder Altersgruppe mit einer festzulegenden Mindestzahl von Wahlberechtigten besetzt sein.

23 Bundeskriminalamt

23.1 Gesetzgebungsstand – BKA-Gesetz steht noch aus

Alle Bemühungen in der 12. Legislaturperiode um ein neues Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten (BKA-Gesetz) waren leider vergebens. Das Bundeskriminalamt arbeitet auch elf Jahre nach Erlaß des Volkszählungsurteils noch immer auf unzureichender rechtlicher Grundlage. Dies ist um so bedauerlicher, weil dem Bundeskriminalamt im Rahmen der polizeilichen Zusammenarbeit in Europa neue Aufgaben zuwachsen werden. Es wird sowohl nach dem Schengener Durchführungsübereinkommen (vgl. Nr. 23.2.1) wie auch bei der Europäischen Drogeneinheit EDE/EUROPOL (vgl. Nr. 23.2.3.1) als eine Art nationaler Anlaufstelle fungieren. Für dringend regelungsbedürftig halte ich ferner Regelungen zur Aufgabe des Bundeskriminalamtes als Zentralstelle beim Betrieb des gemeinsam mit den Ländern betriebenen polizeilichen Informationssystems INPOL.

Immerhin haben die Koalitionsfraktionen in ihrer Vereinbarung zur Bildung der neuen Bundesregierung die Novellierung des Bundeskriminalamtsgesetzes zu einem der wichtigsten Gesetzesvorhaben auf dem Gebiet der Inneren Sicherheit erklärt. Ich werde bei der Vorbereitung des Gesetzentwurfs darauf achten, daß bei gleichzeitigem Verständnis für polizeiliche Erfordernisse nicht über Gebühr in die Rechte unbeteiligter Personen, die also weder Beschuldigte noch Tatverdächtige sind, eingegriffen wird.

23.2 Verstärkte Zusammenarbeit bei der polizeilichen Datenverarbeitung in Europa

Die Bemühungen um mehr Zusammenarbeit der EU-Mitgliedstaaten bei den polizeilichen Aufgaben der Verbrechensbekämpfung und Gefahrenabwehr sowie bei der Zollfahndung sind erheblich intensiviert worden. Titel VI des Vertrages über die Europäische Union bietet nunmehr einen rechtlichen Rahmen für diese zwischenstaatlichen Aktivitäten. Hatte ich in den vorangegangenen Tätigkeitsberichten noch schwerpunktmäßig über die Vorbereitung des Schengener Durchführungsübereinkommens (vgl. 14. S 130 f.) berichtet, so war ich im Berichtszeitraum intensiv an der Ausarbeitung der Übereinkommen zu EUROPOL (s. u. Nr. 23.2.3), zum Europäischen Informationssystem EIS (s. u. Nr. 23.2.2) sowie beim Übereinkommen über den Einsatz von Informationstechnologie im Zollbereich (s. u. Nr. 25.2) beteiligt. Mein Ziel war es den im Schengener Durchführungsübereinkommen erreichten Datenschutz-Standard auch in diesem Übereinkommen zu sichern. Dabei galt es, diesen Standard mit den unterschiedlichen Aufgabenstellungen und Systemarchitekturen der Projekte in Einklang zu bringen. Als besonders wichtige Punkte seien hierbei erwähnt das Recht des Betroffenen auf Auskunft, ein angemessener Individualrechtsschutz sowie eine gemeinsame Datenschutz-Kontrollinstanz. Zu prüfen ist noch, ob und inwieweit die Datenschutz-Kontrolle aufgrund unterschiedlicher Übereinkommen in einer gemeinsamen Instanz koordiniert werden kann.

Auch der Europäische Rat hat sich auf seiner Tagung am 24. und 25. Juni 1994 auf Korfu mit datenschutzrechtlichen Fragen befaßt und einen Bericht zum Stand des Datenschutzes in den vorerwähnten Entwürfen angefordert. Der Europäische Rat hat diesen Bericht am 9./10. Dezember 1994 zur Kenntnis genommen.

23.2.1 Schengen

23.2.1.1 Schengener Durchführungsübereinkommen – SDÜ –

Das Schengener Durchführungsübereinkommen (vgl. 14. TB S. 130) ist am 1. Dezember 1993 vertragsrechtlich in Kraft getreten, nachdem die fünf Erstunterzeichnerstaaten, darunter die Bundesrepublik Deutschland, ihre Ratifikationsurkunde hinterlegt hatten (vgl. Vertragsgesetz vom 15. Juli 1993, BGBl. II S. 1010 ff.). Zwischenzeitlich sind auch Griechenland, Italien, Portugal und Spanien dem Übereinkommen beigetreten. Die beiden erstgenannten Staaten haben noch kein Datenschutzgesetz, was eigentlich Voraussetzung für die Teilnahme am Schengener Informationssystem ist. Insbesondere infolge technischer Schwierigkeiten hat der Exekutivausschuß, das höchste Entscheidungsgremium der Schengener Vertragsparteien, erst am 22. Dezember 1994 beschlossen, das Übereinkommen am 26. März 1995 mit der gleichzeitigen Inbetriebnahme des Schengener Informationssystems (SIS) in Kraft zu setzen. Ab diesem Zeitpunkt wird es an den Binnengrenzen der Vertragsparteien keine Personenkontrollen mehr geben.

Der Wegfall der Grenzkontrollen bedingt umfangreiche Ausgleichsmaßnahmen zum Schutz der öffentlichen Sicherheit. Kernstück dieser Maßnahmen ist das Schengener Informationssystem (SIS), ein gemeinsames, automatisiertes Fahndungssystem, in das die Vertragsstaaten ihre Fahndungsersuchen einstellen. Das Informationssystem besteht aus dem jeweiligen nationalen Teil (N.SIS) – für Deutschland beim BKA geführt – und einer technischen Unterstützungseinheit (C.SIS) in Straßburg. Durch Nutzung der technischen Unterstützungseinheit ist gewährleistet, daß der Bestand jedes nationalen Teils/N.SIS mit demjenigen der N.SIS der anderen Vertragsparteien inhaltlich identisch ist. Das N.SIS beim BKA ist ein vom INPOL-System logisch getrennter Datenbestand; beide Bestände können jedoch von den abfrageberechtigten Stellen mittels einer sog. Kombi-Anfrage gleichzeitig abgefragt werden.

Das Schengener Durchführungsübereinkommen enthält für den Informationsaustausch im SIS umfangreiche Datenschutzregelungen, die für alle Vertragsparteien gelten. Hierzu zählen insbesondere

- ein genau festgelegter Datenkatalog,
- die Zweckbindung übermittelter Daten,
- eine Haftungsregelung,
- der Auskunftsanspruch des Betroffenen,
- eine Rechtsweggarantie sowie
- die Errichtung von Datenschutzkontrollinstanzen für die N.SIS und das C.SIS.

Daneben enthält das Übereinkommen auch Datenschutzregelungen zum Informationsaustausch außerhalb des SIS, z. B. bei der sonstigen polizeilichen Zusammenarbeit. Dieser Datenschutzstandard (sog. Schengen-Acquis) zum Datenschutz ist mittlerweile zur Richtschnur zum Mindeststandard in anderen europäischen Informationssystemen (z. B. EIS, CIS, EUROPOL) geworden.

Neben dem automatisierten Informationssystem bedarf es ergänzend einer Organisation für das Funktionieren des Systems. Zu diesem Zweck richtet jeder Vertragsstaat ein sog. SIRENE-Büro ein (für Deutschland beim BKA), das dem Endbenutzer nach einer Befragung des SIS im Trefferfall ermöglicht, die für sein weiteres Einschreiten erforderlichen zusätzlichen Informationen zu übermitteln. Obwohl das SIRENE-Netz für das Funktionieren des SIS von Anfang an unabdingbar war, ist es im Schengener Durchführungsübereinkommen nicht ausdrücklich erwähnt.

Im Berichtszeitraum habe ich mich mit Stellungnahmen an den innerstaatlichen Vorbereitungen zur Durchführung des Übereinkommens beteiligt. Ich habe mich ferner beim Bundeskriminalamt als Zentrale für den nationalen Teil des Schengener Informationssystems darüber informiert, wie der Stand der Datensicherheit im N.SIS und wie weit der Aufbau des nationalen SIRENE-Büros sind. Trotz anerkennenswerter Bemühungen aller Beteiligten ist damit zu rechnen, daß die eigentlichen datenschutzrechtlichen Probleme erst nach Aufnahme des tatsächlichen Betriebes des Schengener Informationssystems auftreten werden. Dann wird sich zeigen, ob die datenschutzrechtlichen Regelungen im Schengener Durchführungsübereinkommen zum Schutz der Rechte des einzelnen ausreichen.

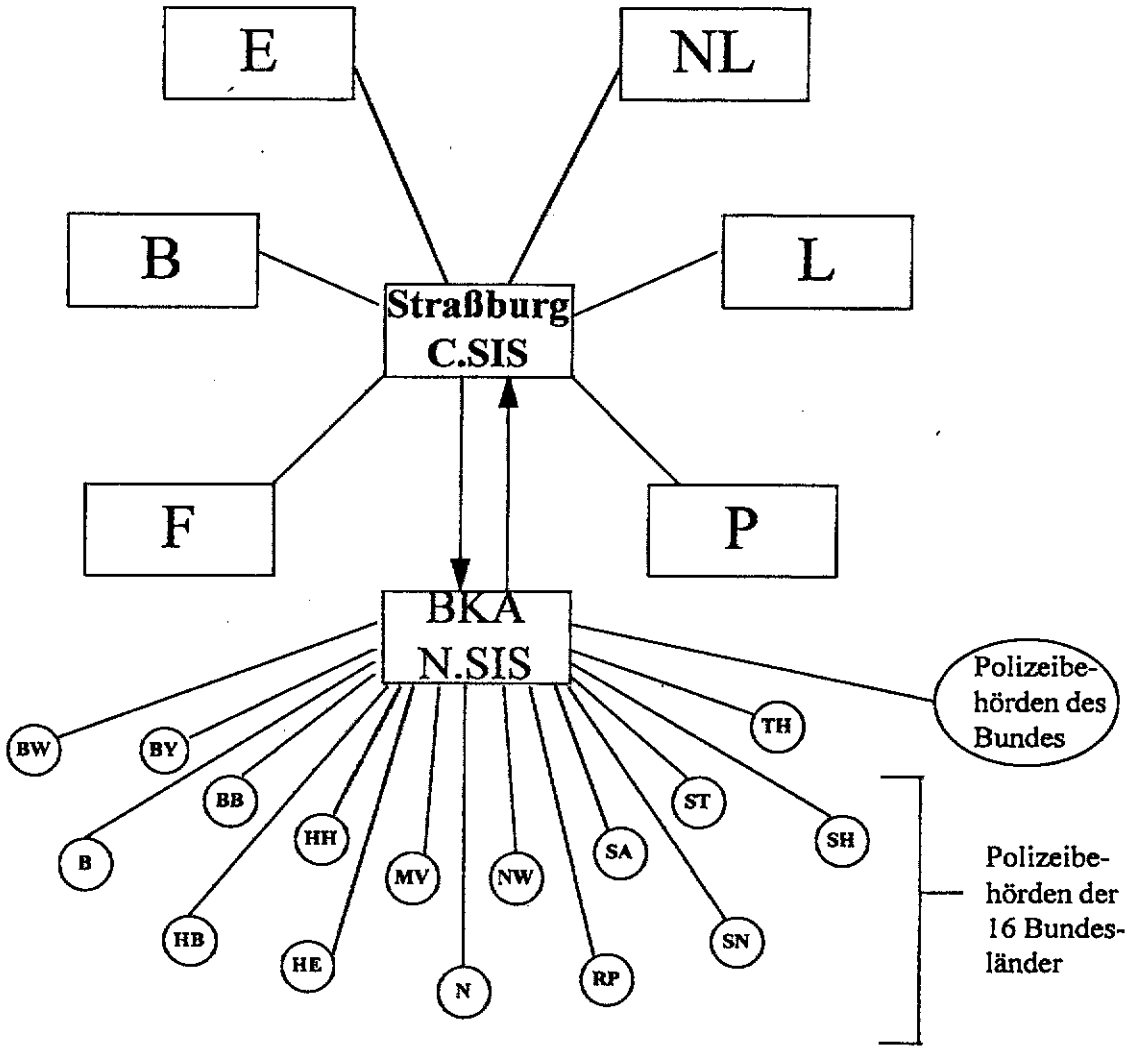
Im zwischenstaatlichen Bereich habe ich an mehreren Sitzungen der provisorischen gemeinsamen Datenschutzkontrollinstanz – GPK – teilgenommen. Ein Vertreter meiner Dienststelle führt in dieser Einrichtung den Vorsitz. Dieses Gremium hat, nachdem es sich auf eine vorläufige Geschäftsordnung verständigt hatte, zu verschiedenen datenschutzrechtlichen Fragen Stellung genommen oder Empfehlungen ausgesprochen. Dazu zählen u. a. die

- Feststellung, daß die Beitrittsländer Portugal und Spanien über eine Datenschutzgesetzgebung verfügen, die den Anforderungen des Schengener Durchführungsübereinkommens entspricht,
- Kenntnisnahme von der Liste der zur unmittelbaren Abfrage im Schengener Informationssystem berechtigten Stellen, wobei die GPK jedoch Wert auf eine genauere Auflistung dieser Stellen gelegt hat.

Im März 1994 hat die GPK die technische Unterstützungseinheit des SIS in Straßburg besucht. Diese Zentrale hat den Datenbestand zu führen, der der Online-Übermittlung der Informationen an die parallel geführten nationalen Bestände dient (s. auch Abbildung 5, folgende Seite). Damit wird die Identität der Datenbestände der N.SIS gewahrt. Zweck des Besuchs war es, den Stand der Datensicherung in der Schengen-Zentrale und im SIS insgesamt kennenzulernen; das System war damals noch in der Aufbauphase.

Abbildung 5

Schengener Informationssystem (SIS)



N.SIS = nationaler Teil des SIS
C.SIS = technische Unterstützungseinheit ("C" steht für central)

B = Belgien
E = Spanien
F = Frankreich
L = Luxemburg
NL = Niederlande
P = Portugal

Im Anschluß an den Besuch hat die GPK folgende Empfehlungen an die verantwortlichen Schengen-Gremien gerichtet:

- Räumliche Trennung zwischen den C.SIS-Anlagen und den DV-Anlagen der französischen Regierung in Straßburg,
- Aufbewahrung einer Sicherungskopie für den Katastrophenfall außerhalb der C.SIS-Räumlichkeiten,
- Maßnahmen zur Erhöhung der Betriebssicherheit der Kommunikationsverbindungen zwischen dem C.SIS und den N.SIS zur Minimierung des Ausfallrisikos.

Die Zentrale Gruppe der Schengen-Vertragsparteien hat die Empfehlungen der GPK zwar nicht aufgegriffen, die Kontrollinstitution sah sich aber insbesondere bezüglich der dritten Empfehlung zur Sicherheit der Kommunikationswege durch interne Papiere bestätigt, die ebenfalls auf diesen Schwachpunkt hinwiesen und hat insoweit ihren Standpunkt gegenüber dem zuständigen Schengen-Gremium nochmals bekräftigt.

Schließlich hat sich die GPK mit der Auswertung eines gemeinsamen Fragebogens über die Datenschutzgesetzgebung und insbesondere die datenschutzrechtliche Kontrolle des jeweiligen N.SIS in den einzelnen Vertragsstaaten befaßt. Sie hat damit eine gute Grundlage für die künftige Arbeit der gemeinsamen Kontrollinstanz nach Artikel 115 des Schengener Durchführungsübereinkommens gelegt.

23.2.1.2 Konsultationsverfahren nach Artikel 17 Abs. 2 Schengener Durchführungsübereinkommen

Das Schengener Durchführungsübereinkommen (SDÜ) sieht den Abbau der Personenkontrollen an den Binnengrenzen der Vertragsstaaten vor. Für Drittausländer wird deshalb ein einheitlicher Sichtvermerk (Schengen-Visum) für Aufenthalte bis zu drei Monaten eingeführt, der für das Hoheitsgebiet aller Vertragsparteien gültig sein soll.

Nach dem Übereinkommen darf ein Schengener Gemeinschaftsvisum von den Auslandsvertretungen nur nach vorhergehender Abfrage des Schengener Informationssystems (SIS) ausgestellt werden. Dieser Zugriff erfolgt zusätzlich zu der Abfrage des Ausländerzentralregisters (AZR) beim Bundesverwaltungsamt in Köln, um festzustellen, ob der Drittausländer zur Einreiseverweigerung nach Artikel 96 SDÜ ausgeschrieben ist.

In den Fällen des Artikel 17 Abs. 2 SDÜ, die der Exekutivausschuß festlegt, hängt die Erteilung eines Sichtvermerks zusätzlich von der Konsultation der zentralen Behörde der betroffenen Vertragspartei (für die Bundesrepublik Deutschland das Auswärtige Amt) und gegebenenfalls von der Konsultation der zentralen Behörden der anderen Vertragsparteien ab. Es handelt sich dabei um Sichtvermerksanträge von Staatsangehörigen bestimmter „Problemstaaten", bei denen pauschal ein erhöhtes Risiko für die nationale Sicherheit unterstellt wird. Daher ist bei diesem Konsultationsverfahren auch die Einschaltung der Sicherheitsbehörden (BKA, BfV, BND und ZKA) vorgesehen.

Auf nationaler Ebene besteht bereits ein derartiges Verfahren zur Beteiligung der Sicherheitsbehörden bei Sichtvermerksanträgen aus bestimmten Problemstaaten, von dem ich erstmals bei der Diskussion um die Durchführung des Artikel 17 Abs. 2 SDÜ erfahren habe. Dabei habe ich gegenüber dem BMI die Auffassung vertreten, daß für den gegenseitigen Informationsaustausch zwischen dem AA und den Sicherheitsbehörden keine Rechtsgrundlage besteht. Aus meiner Sicht enthalten weder das BDSG noch die Gesetze über die Nachrichtendienste eine ausreichende Rechtsgrundlage für diese Art des Austauschs personenbezogener Daten. Im Rahmen des neuen Konsultationsverfahrens nach Artikel 17 Abs. 2 SDÜ wird die Kommunikation zwischen dem AA und den Sicherheitsbehörden anders strukturiert sein. Von der Notwendigkeit des neuen Verfahrens habe ich mich durch einen Informationsbesuch vor Ort überzeugt und meine Bedenken bis zur Schaffung einer gesetzlichen Grundlage zurückgestellt. Inwieweit aufgrund des alten Verfahrens eine Datenbereinigung vorgenommen werden muß, ist von mir noch zu prüfen.

Schwierigkeiten bei der Durchführung des Schengener Konsultationsverfahrens bereitete auch die Frage, worauf sich die Übermittlung personenbezogener Daten durch das AA an die zentrale Behörde eines anderen Vertragsstaates stützt. Im SDÜ ist hierfür keine bereichsspezifische Übermittlungsregelung vorgesehen. Artikel 17 Abs. 2 enthält lediglich eine Kompetenzuweisung an den Exekutivausschuß zur Festlegung der Fälle, in denen ein Konsultationsverfahren notwendig ist. Ich halte es daher für erforderlich, die Beschlüsse des Exekutivausschusses zum Konsultationsverfahren durch Schaffung eines entsprechenden Vertragsgesetzes in innerstaatliches Recht umzusetzen (Artikel 59 Abs. 2 GG), womit das Konsultationsverfahren zwischen den zentralen Behörden der Schengener Vertragsparteien abschließend geregelt würde. Damit wäre ein Rückgriff auf die allgemeinen Regelungen des BDSG nicht mehr erforderlich. Bis zur Schaffung eines entsprechenden Vertragsgesetzes halte ich die Einwilligung des Betroffenen in die Übermittlung seiner Daten für ausreichend.

Ein weiteres Problem im Rahmen dieses Konsultationsverfahrens betrifft die Verschlüsselung der per Telex von den deutschen Auslandsvertretungen übermittelten Daten (vgl. hierzu 14. TB S. 44). Auch hier habe ich einstweilen meine Bedenken zurückgestellt, um die Umsetzung des geplanten Verfahrens der Konsultationen zentraler Behörden nicht zu gefährden. Eine Verschlüsselung der übermittelten Daten ist aber sobald wie möglich aus Gründen der Datensicherung erforderlich.

23.2.2 Europäisches Informationssystem – EIS –

Neben dem Schengener Informationssystem (SIS) ist der Aufbau eines Europäischen Informationssystems (EIS) geplant, dem auch die Nicht-Schengen-Mitglieder Dänemark, Irland sowie das Vereinigte Königreich angehören sollen (vgl. 14. TB S. 130). Die Aus-

arbeitung des Vorhabens erfolgt nun im Rahmen der Zusammenarbeit Justiz und Inneres nach Titel VI des EU-Vertrags.

Zunächst war das EIS lediglich als EDV-System für die Daten der zur Einreiseverweigerung ausgeschriebenen Drittausländer nach Artikel 10 und 13 des ebenfalls geplanten Außengrenzen-Übereinkommens vorgesehen. Nunmehr soll es zu einem umfassenden Fahndungssystem wie das Schengener Informationssystem ausgestaltet und mit diesem zusammengeführt werden. Das geplante Übereinkommen sieht deshalb Regelungen vor, die weitgehend mit den Vorschriften der Artikel 92ff. des Schengener Durchführungsübereinkommens (SDÜ) zur Einrichtung des SIS identisch sind. Weitere Regelungen im SDÜ, z. B. zur polizeilichen und justitiellen Zusammenarbeit (Artikel 39ff. und Artikel 48ff.), sollen nicht übernommen werden. Insoweit wird es nur die Zusammenarbeit der neun Schengenpartner geben. Ziel der Bemühungen ist, in Europa ein einziges gemeinsames Fahndungssystem zu schaffen.

Der wesentliche Unterschied zwischen dem SDÜ und dem EIS-Übereinkommen besteht jedoch darin, daß das SIS ausdrücklich als Ausgleichsmaßnahme für den Wegfall der Binnengrenzkontrollen (Artikel 2 SDÜ) konzipiert wurde. Eine derartige rechtliche Voraussetzung fehlt beim EIS. M.E. kommt es noch sehr auf eine Einigung der EU-Mitgliedsstaaten – insbesondere der Nicht-Schengen-Staaten – darüber an, daß Artikel 7a des EU-Vertrags auch den Wegfall der Grenzkontrollen umfaßt, um damit die Erforderlichkeit des EIS begründen zu können. Ich hielte es jedenfalls für bedenklich, wenn ein umfassendes Fahndungssystem eingeführt würde, ohne daß die eigentliche Geschäftsgrundlage, nämlich der Wegfall der Binnengrenzkontrollen, realisiert würde.

Bei den Beratungen zum EIS bleiben aus meiner Sicht folgende Punkte wichtig: Die Regelungen zur konventionellen Datenübermittlung (vgl. Artikel 26 und 27 des Entwurfs) müssen beibehalten werden; danach finden auch auf diese Übermittlungen die bei der automatisierten Verarbeitung geltenden Vorschriften sinngemäß Anwendung. Die konventionelle Datenübermittlung darf nicht vom Datenschutz ausgenommen werden.

Begrüßt habe ich, daß in Artikel 30 des Übereinkommens eine Regelung über die Einrichtung von SIRENE-Stellen (Supplementary Information Request for National Entry) vorgesehen ist. Die SIRENE-Stellen übermitteln ergänzende Informationen, die zur Identifizierung der ausgeschriebenen Personen oder Sachen erforderlich sind, sowie die sonstigen Unterlagen, die für die zu ergreifenden Maßnahmen bei einer Ausschreibung notwendig sind (die sog. Begleitpapiere). SIRENE-Stellen gibt es auch im Bereich des SDÜ, ohne dort ausdrücklich geregelt zu sein.

Vom BMI wird die Einrichtung eines automatisierten Abrufverfahrens beim EIS zugunsten des Europäischen Polizeiamtes (EUROPOL) angestrebt. Dagegen habe ich noch datenschutzrechtliche Bedenken, da von seiten des BMI die Erforderlichkeit eines solchen Direktzugriffs für EUROPOL bisher nicht ausreichend dargelegt wurde. Die Besprechungen hierzu sind jedoch noch nicht abgeschlossen.

23.2.3 EUROPOL

23.2.3.1 Die Europäische Drogeneinheit – EDE/EUROPOL – hat im Berichtszeitraum ihre Tätigkeit aufgenommen

Um schon im Vorfeld einer EUROPOL-Konvention die Zusammenarbeit beim Kampf gegen den internationalen Drogenhandel und damit zusammenhängende organisierte Kriminalität zu intensivieren, einigten sich die EU-Mitgliedstaaten auf ein Modell, das die Entsendung von Verbindungsbeamten aus den zwölf Vertragsstaaten zum Zweck des bilateralen Informationsaustausches vorsieht (vgl. 14. TB S. 130f.).

Rechtliche Grundlage hierfür ist die „Ministervereinbarung über die Einrichtung der EUROPOL-Drogeneinheit" vom 2. Juni 1993. Nachdem sich am 29. Oktober 1993 die Staats- und Regierungschefs der EU-Mitgliedstaaten auf Den Haag als Sitz von EDE/EUROPOL verständigt hatten, konnte die Ministervereinbarung in Kraft treten, deren Wirksamwerden bis zur Klärung der Sitzfrage aufgeschoben war. Ein internationaler Aufbaustab aus Vertretern der zwölf EU-Staaten, der seit Dezember 1992 in Straßburg tätig gewesen war, zog Ende Dezember 1993/Anfang Januar 1994 nach Den Haag, um dort seine Tätigkeit als Keimzelle von EDE aufzunehmen.

Nach der Ministervereinbarung bearbeiten die Verbindungsbeamten eingehende Ersuchen und Informationen auf der Grundlage ihrer nationalen Gesetze und Regelungen. Personenbezogene Informationen dürfen nur nach Maßgabe der nationalen Datenschutzgesetze sowie einschlägiger Rechtsvorschriften und Ministerweisungen über die Verarbeitung personenbezogener Informationen und unter Einhaltung der vom liefernden Staat gestellten Bedingungen für die Nutzung solcher Informationen ausgetauscht werden. Für die bei EDE ebenfalls vorgesehene Analysetätigkeit dürfen nach der Ministervereinbarung nur nicht personenbezogene Daten verwendet werden. Anfänglich gab es hierzu Überlegungen, ob und wie man für operative Analysen auch personenbezogene Daten verwenden könnte. Die deutsche Delegation hat jedoch bei den Verhandlungen im Rat deutlich gemacht, dies widerspräche der Ministervereinbarung, so daß man davon Abstand nahm.

Im Mai 1994 habe ich mit der Arbeitsgruppe „Polizei" der Datenschutzbeauftragten aus den EU-Mitgliedstaaten einen Informationsbesuch bei EDE/EUROPOL in Den Haag durchgeführt. Im Anschluß daran habe ich mich bei den deutschen Verbindungsbeamten über deren Tätigkeit aufgrund der Ministervereinbarung informiert und dabei auftretende Probleme erörtert. Zum Zeitpunkt des Informationsbesuchs befanden sich drei Verbindungsbeamte des BKA und ein Verbindungsbeamter des ZKA bei EDE/EUROPOL. Inzwischen sind noch zwei zum BKA abgeordnete Ländervertreter (aus Niedersachsen und Berlin) hinzugekommen.

Der Verfahrensablauf bei einer Anfrage stellte sich während des Besuchs wie folgt dar:

Nach Eingang einer Anfrage durch die nationale Stelle leitet der jeweilige Verbindungsbeamte diese mit Hilfe eines Mail-Programms an alle anderen Verbindungsbeamten bei EDE weiter. Diese senden per Fax oder Telefon die Anfrage an ihre nationalen Stellen. Darin liegt der wesentliche Vorteil gegenüber Interpol, da die Informationen sofort an die Ansprechpartner weitergegeben werden können. Sofern die angefragten nationalen Stellen eine Antwort geben, wird diese wieder per Mail-Programm durch den jeweiligen Verbindungsbeamten an den anfragenden Verbindungsbeamten weitergeleitet. Die Antwort geht grundsätzlich nur an den anfragenden Verbindungsbeamten. Die Verbindungsbeamten der anderen Vertragsparteien bekommen sie jedoch, wenn sie zu deren Aufgabenerfüllung relevant erscheint.

Meine Frage, wie bei dem Mail-Programm sichergestellt wird, daß der Versand genau an eine oder an bestimmte einzelne Empfangsstellen erfolgt, ist noch nicht geklärt. Nach Mitteilung des BMI werden die Informationen verschlüsselt weitergegeben. Nach meinen Erkenntnissen über das Mail-Programm ist davon auszugehen, daß die Informationen, die unter Zuhilfenahme des Programms ausgetauscht werden, nur „komprimiert" und nicht in Form kryptographischer Verschlüsselung gespeichert werden. Die Komprimierung erfüllt aber auf keinen Fall den Anspruch der kryptographischen Verschlüsselung.

Der geplante online-Zugriff der Verbindungsbeamten auf die einschlägigen nationalen Datenbestände war zum Zeitpunkt des Informationsbesuchs noch nicht realisiert. Inzwischen besteht jedoch für die deutschen Verbindungsbeamten diese Möglichkeit. Das BMI hat mir allerdings mitgeteilt, daß eine Verschlüsselung dieses online-Zugriffs, wie von mir gefordert, derzeit noch nicht möglich sei.

Für besonders problematisch halte ich den umfassenden Zugriff der deutschen Verbindungsbeamten bei EDE/EUROPOL auf das polizeiliche Informationssystem INPOL beim BKA. Ich habe von Anfang an die Auffassung vertreten, daß nur ein Zugang zu den rauschgiftrelevanten Daten beim BKA zulässig ist, da die Aufgabe von EDE/EUROPOL nach der Ministervereinbarung die Bekämpfung der Rauschgiftkriminalität ist. Laut BMI besteht aber eine Zugriffsmöglichkeit z. B. auf die Dateien KAN, Haft, Personenfahndung und Erkennungsdienst, obwohl die Verbindungsbeamten keine eigenen Ermittlungen führen. Sie fungieren lediglich als Informationsmittler zu anderen Delegationen. Zu der Abrufmöglichkeit von Falldateien des BKA, wie z. B. für Scheck-, Tötungs- und Sexualdelikte, hat mir das BMI mitgeteilt, daß es sich ausschließlich um rauschgiftrelevante Dateien handele. Was die genannten Anwendungen jedoch damit zu tun haben, ist mir vom BMI bisher nicht plausibel dargelegt worden. Weiterhin teilte das BMI mit, daß der Verbindungsbeamte in jedem Fall die Gesamtübersicht aus allen vorgesehenen Dateien erhalten müsse, damit eine umfassende und zuverlässige Einschätzung der Täterpersönlichkeit möglich ist. Das BMI verkennt m. E., daß nach der Ministervereinbarung ein Informationsaustausch nur über den unerlaubten Verkehr mit Drogen, die darin verwickelten kriminellen Vereinigungen und die damit verbundenen Geldwäschehandlungen vorgesehen ist.

Weiterhin habe ich gegenüber dem BMI auf einer lückenlosen Protokollierung aller Datenübermittlungen aufgrund der Ministervereinbarung bestanden. Eine Speicherdauer von max. 1 Jahr halte ich für ausreichend (vgl. 14. TB Anlage 14). Auch dieser Punkt ist mit dem BMI noch zu klären.

23.2.3.2 Wann kommt die EUROPOL-Konvention?

Die Mitgliedstaaten der Europäischen Union haben im Vertrag über die Europäische Union u. a. den Aufbau eines unionsweiten Systems zum Austausch von Informationen im Rahmen eines europäischen Polizeiamts (EUROPOL) für den Bereich der polizeilichen Zusammenarbeit zur Verhütung und Bekämpfung des Terrorismus, des illegalen Drogenhandels und sonstiger schwerwiegender Formen der internationalen Kriminalität vorgesehen (Artikel K.1 Nr. 9 EU-Vertrag).

Da EUROPOL vor allem personenbezogene Informationen sammeln, analysieren, übermitteln und hierfür eine eigene Datenbank erhalten soll, ist als Rechtsgrundlage eine völkerrechtlich bindende Konvention mit umfassenden Datenschutzregelungen erforderlich. Auf seiner Tagung im Oktober 1993 hatte sich der Europäische Rat dafür ausgesprochen, die Verhandlungen über eine EUROPOL-Konvention bis Oktober 1994 abzuschließen. Ausgangspunkt der Beratungen war ein bereits Ende Juni 1993 unter britischer Präsidentschaft vorgelegter Rohentwurf einer Konvention, der als Arbeitsgrundlage bei den weiteren Beratungen in der Ratsgruppe EUROPOL diente. Wichtige Punkte wie die Systemarchitektur und datenschutzrechtliche Regelungen waren dort jedoch noch nicht geregelt. Erstmals im Juli 1994 wurde unter deutschem Vorsitz ein vollständiger Entwurf auf Grundlage des britischen Dokuments und unter Einbeziehung zwischenzeitlich erzielter Ergebnisse vorgelegt. Doch konnten die Arbeiten bis Oktober 1994 nicht abgeschlossen werden, da in wesentlichen Punkten, wie den Aufgaben und der Zielsetzung, dem Auskunftsrecht, der Rolle des Europäischen Parlaments und dem Rechtsweg, keine Einigung erzielt wurde.

Bei den Beratungen zur EUROPOL-Konvention war ich von Anfang an umfassend beteiligt. Mein Anliegen war, den bereits beim Schengener Durchführungsübereinkommen erreichten Datenschutzstandard mit entsprechenden Anpassungen an die Aufgaben und Organisation von EUROPOL zu erhalten. Das bedeutet vor allem klare Regelungen über Art, Umfang und Verwendung der bei EUROPOL zu speichernden Daten, weiterhin ein umfassendes Auskunftsrecht für den Betroffenen, eine gerichtliche und parlamentarische Kontrolle sowie eine unabhängige Kontrollinstanz.

Nach den deutschen Vorstellungen soll eine zentral bei EUROPOL geführte Sammlung von Informatio-

nen entstehen, die aus einem Informationssystem, den Analysedateien und einem Indexsystem besteht. Dabei soll das Informationssystem einem Aktennachweis entsprechen und nur „harte" Grunddaten wie z. B. Name, Geburtsdatum und Geschlecht beinhalten, die für den Zugriff auf die zugrundeliegende Akte erforderlich sind. Eingabe- und abrufberechtigt sollen in jedem Vertragsstaat eine nationale Stelle, die Verbindungsbeamten sowie EUROPOL selbst sein. Die Analysedateien sollen auch „weiche" Informationen, d. h. auch ungesicherte Erkenntnisse, beinhalten. Diese werden von den Mitgliedstaaten auf konventionellem Wege übermittelt. Damit derartige Informationen überhaupt angeliefert werden, ist vertraulicher Umgang mit solchen Daten eine wichtige Voraussetzung. Eingabe- und abrufberechtigt sollen daher nach dem „need to know" Prinzip nur die EUROPOL-Beamten sein, da sie die Daten für Analysen benötigen. Ein Zugriff der nationalen Stellen und der Verbindungsbeamten wird für nicht erforderlich gehalten. Andere Mitgliedstaaten wollen jedoch einen Zugriff auf den gesamten Datenbestand eröffnen. Im ursprünglichen Vorschlag der deutschen Delegation war den Verbindungsbeamten, die schon derzeit bei EDE (s. o. Nr. 23.2.3.1) tätig sind, kein Zugriff auf die Analysedateien eingeräumt, sondern nur den EUROPOL-Beamten. Auf Grund der Beratungen soll der Status der nationalen Verbindungsbeamten bei EUROPOL aufgewertet werden. Deshalb ist die Einführung eines Indexsystems vorgesehen, das ausschließlich Stichworte enthält. Damit kann ein Verbindungsbeamter feststellen, ob seine nationale Stelle von einer Analyse betroffen ist. Um die Informationen aus den Dateien zu erhalten, muß sich der Verbindungsbeamte mit EUROPOL in Verbindung setzen.

Ein wichtiger Beratungspunkt ist auch das Auskunftsrecht des Betroffenen. Nach dem deutschen Vorschlag soll es ein direktes Auskunftsrecht gegenüber der speichernden Stelle geben. Danach erhält der Betroffene, wenn keine Hinderungsgründe, wie z. B. Gefährdung der öffentlichen Sicherheit, entgegenstehen, Auskunft über die zu seiner Person gespeicherten Daten. Nach den Vorstellungen einiger anderer Delegationen soll der Betroffene nur ein indirektes Auskunftsrecht bekommen. Danach soll lediglich die Datenschutzbehörde kontrollieren, ob eine Speicherung vorliegt und wenn ja, ob diese rechtmäßig ist. Dies entspricht u. a. dem französischen Datenschutzrecht. Beim indirekten Auskunftsrecht wird m. E. verkannt, daß die Daten bei EUROPOL eine neue Qualität erhalten, da Informationen aus verschiedenen Ländern zusammengeführt werden und diese zentral bei einer internationalen Polizeibehörde gespeichert werden. Auch sieht z. B. das französische Datenschutzrecht umfassende Befugnisse für die Kontrollbehörde vor, wie z. B. die Einschaltung eines Ermittlungsrichters. Derartige Kontrollbefugnisse gibt es nicht auf europäischer Ebene für eine gemeinsame Kontrollinstanz, die in der EUROPOL-Konvention vorgesehen ist. Bei einer Datenspeicherung auf internationaler Ebene ist es besonders wichtig, daß der Schutz des Bürgers angemessen gewährleistet wird. Dies bedeutet auch, daß er ein umfassendes Auskunftsrecht erhalten muß, um sich gegen eventuell unrichtige Speicherungen wehren zu können.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat auf ihrer 48. Sitzung einen Beschluß über die wichtigsten datenschutzrechtlichen Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL) getroffen (vgl. Anlage 11). Im Oktober 1994 hat sich auch die Arbeitsgruppe „Polizei" der EU-Datenschutzbeauftragten, in der ich vertreten bin, mit der EUROPOL-Konvention beschäftigt und im November eine Resolution an den Vorsitzenden des Rates der Justiz- und Innenminister übersandt (vgl. Anlage 17).

Auf seiner Tagung im Dezember 1994 hat nun der Europäische Rat beschlossen, daß die Konvention zur Errichtung von EUROPOL spätestens bis zur Sitzung des Europäischen Rates – voraussichtlich im Juni 1995 – in Cannes abzuschließen ist.

23.3 Automatisiertes Fingerabdruck-Identifizierungssystem – AFIS –

In AFIS wurden nach seiner Einrichtung im Dezember 1992 zunächst die Fingerabdrucke von Asylbewerbern und von Personen gespeichert, die nach dem Ausländergesetz erkennungsdienstlich behandelt worden sind (vgl. 14. TB S. 132). Seit Dezember 1993 werden auch die Fingerabdrucke von mutmaßlichen Straftätern in AFIS erfaßt. Neben der Identifizierung von Personen soll das System die Zuordnung von am Tatort gefundenen Fingerabdruckspuren ermöglichen. Die Erfassung in AFIS wird arbeitsteilig von Bund und Ländern vorgenommen. Die Speicherung der Zehnfinger-Abdrucke erfolgt durch das BKA. Die Bundesländer erfassen und recherchieren Einzelfingerspuren. In AFIS waren zum Jahresende 1994 ca. 2,1 Mio. Fingerabdrucksätze gespeichert. Hiervon sind ca. 530 000 Datensätze mit der Kennung „Asylbewerber" versehen, außerdem sind ca. 30 000 Einzelfingerspuren zur Spurenrecherche erfaßt.

Vor der Erfassung der Fingerabdrucke erfolgt eine Abfrage der übermittelten Personalien des Betroffenen im Informationssystem der Polizei (INPOL), um festzustellen, ob personenbezogene Daten bereits erfaßt sind. Ist kein Datensatz vorhanden, werden bei mutmaßlichen Straftätern die Personalien sowie eine daktyloskopische Nummer, die eine Verknüpfung zu AFIS ermöglicht, im Aktennachweis des Bundeskriminalamts (BKA-AN) erfaßt. In INPOL werden zusätzlich ein Hinweis auf die erkennungsdienstlich behandelnde Dienststelle und der Grund der ed-Behandlung erfaßt. Bis zur Schaffung eines eigenen Vorgangsnachweises Amtshilfe (VNA) für die Speicherung der personenbezogenen Daten von Asylbewerbern, die die in § 16 Abs. 4 AsylVfG geforderte getrennte Aufbewahrung von anderen erkennungsdienstlichen Unterlagen sicherstellt, werden deren Daten vorläufig im Vorgangsnachweis Personen (VNP) des Bundeskriminalamtes gespeichert, der nur dem Bundeskriminalamt zugänglich ist. Das BMI hat mir mitgeteilt, daß mit der Einführung der Datei

VNA nicht vor Ende 1994 zu rechnen sei. Bis Redaktionsschluß lag mir darüber noch keine Bestätigung vor.

Bei Unterlagen von Personen, deren Personalien bereits mit erkennungsdienstlichen Unterlagen im INPOL erfaßt sind, wird ferner geprüft, ob die Fingerabdruckblätter identisch sind. Trifft dies zu, wird dies in den entsprechenden AFIS-Datensätzen ergänzt. Die Speicherung eines weiteren Datensatzes erfolgt also nicht. Über die Personenidentität und über die beim BKA vorhandenen Erkenntnisse werden die übermittelnden Dienststellen unterrichtet. Bei Asylbewerbern erfolgt eine automatisierte Unterrichtung des Bundesamtes für die Anerkennung ausländischer Flüchtlinge (BAFl) und dessen Außenstellen, daß die Personalien des Asylbewerbers als identisch festgestellt worden sind. Konventionell wird diesen Stellen dann mitgeteilt, wo bereits erkennungsdienstliche Behandlungen bei früher gestellten Asylanträgen durchgeführt worden sind. Andere Erkenntnisse werden nicht mitgeteilt. Hiermit bleibt § 16 Abs. 3 Satz 3 AsylVfG gewahrt, wonach das Bundeskriminalamt den Grund der Aufbewahrung **anderer** vorhandener ed-Unterlagen (z. B. von mutmaßlichen Straftätern) nicht mitteilen darf (vgl. auch Nr. 3.2.1).

Die Erfassung der Fingerabdrucke in AFIS erfolgt mittels spezieller Arbeitsplatzcomputer durch Daktyloskopen. Die auf dem Fingerabdruckblatt vorhandene Barcodierung wird mittels Lichtstift in das System eingegeben. Daneben legt der Daktyloskop für jeden Finger eine Grundmusterbestimmung fest. Durch Speicherung von Schlüsselwerten werden die Daten von Asylbewerbern, die Daten von nach dem Ausländergesetz behandelten Personen und die Daten von Straftätern gekennzeichnet. Dies führt zur Vergabe eines Merkers, wodurch eine logische Trennung der Daten von Asylbewerbern und von Personen, die aus anderen Gründen erkennungsdienstlich behandelt worden sind, sichergestellt ist. Die in § 16 Abs. 4 AsylVfG genannten Anforderungen, nämlich Aufbewahrung der Daten von Asylbewerbern getrennt von anderen erkennungsdienstlichen Unterlagen und deren gesonderte Kennzeichnung, sind nach meinen Feststellungen erfüllt. Vor der endgültigen Erfassung erfolgt zunächst eine Zwischenspeicherung im System. Die endgültige Speicherung des Fingerabdrucks in AFIS erfolgt erst, wenn bei einem **Bestandsabgleich** kein identischer Fingerabdruck festgestellt werden konnte. Nach der Zwischenspeicherung wird das Fingerabdruckblatt getrennt nach Daten von Asylbewerbern und sonstigen erkennungsdienstlichen Unterlagen beim BKA aufbewahrt.

Bei dem zuvor erwähnten **Bestandsabgleich** wird die Formel des einzugebenden Fingerabdrucks mit den in AFIS gespeicherten und vom System vergebenen Formeln abgeglichen. Sowohl bei den Daten von Asylbewerbern als auch von mutmaßlichen Straftätern wird der Bestandsabgleich im Gesamtbestand von AFIS durchgeführt. Dieses Verfahren ist mit § 16 Abs. 3 Satz 2 AsylVfG vereinbar, wonach das BKA hierbei zur Erfüllung seiner Aufgaben aufbewahrte ed-Unterlagen verwenden darf. Bei Treffern in AFIS werden der Fingerabdruck und vorhandene Vergleichsabdrucke auf dem Bildschirm angezeigt. Durch Daktyloskopen wird geprüft, ob diese Fingerabdrucke tatsächlich mit den einzugebenden Fingerabdrucken identisch sind. Ist dies der Fall, wird bei mutmaßlichen Straftätern die übermittelnde Dienststelle über die Personenidentität unterrichtet und gleichzeitig werden die beim BKA vorhandenen Erkenntnisse mitgeteilt. Bei Asylbewerbern erfolgt wieder eine automatisierte Mitteilung an das BAFl und dessen Außenstellen, daß die Person bereits unter anderen Personalien aufgetreten ist; hinzu kommt ein Hinweis auf bereits vorhandene erkennungsdienstliche Unterlagen. Diesen Stellen wird auch mitgeteilt, wenn die Person wegen weiterer Asylverfahren bereits erkennungsdienstlich behandelt worden ist. Liegen weitere kriminalpolizeiliche Erkenntnisse vor, wird nur mitgeteilt, daß aus sonstigen Anlässen erkennungsdienstliche Unterlagen vorhanden sind. Hiermit erfüllt das BKA § 16 Abs. 3 Satz 3 AsylVfG, wonach dem BAFl und seinen Außenstellen der Grund der Aufbewahrung anderer Unterlagen nicht mitgeteilt werden darf. Der Abgleich der Daten von Asylbewerbern gegen den Gesamtbestand von AFIS entspricht somit § 16 Abs. 3 Satz 2 AsylVfG; eine Vorschrift, die mit mir abgestimmt wurde.

Dagegen ist der von mir festgestellte Abgleich der Daten von mutmaßlichen Straftätern gegen den gesamten AFIS-Bestand und damit auch gegen den Datenbestand von Asylbewerbern mit § 16 Abs. 5 AsylVfG nicht vereinbar und somit nicht zulässig. Die einschränkenden Voraussetzungen des § 16 Abs. 5 AsylVfG für die zweckändernde Verarbeitung und Nutzung von Asylbewerberdaten beziehen sich auf beide dort genannten Maßnahmen „Feststellung der Identität" und „Zuordnung von Beweismitteln". In § 16 Abs. 5 AsylVfG ist geregelt, unter welchen Bedingungen eine zweckändernde Verarbeitung und Nutzung von Asylbewerberdaten im Einzelfall zulässig ist. Dies ist nur dann der Fall, wenn bestimmte Tatsachen die Annahme begründen, daß der Datenabgleich zur Aufklärung einer Straftat führen wird. Ich habe dem Bundesministerium des Innern mitgeteilt, daß ich von einer förmlichen Beanstandung gem. § 25 BDSG nur dann absehen werde, wenn durch technische und organisatorische Maßnahmen sichergestellt wird, daß ein Abgleich der Daten von mutmaßlichen Straftätern gegen den Datenbestand von Asylbewerbern nur unter diesen Voraussetzungen erfolgt.

Gegenüber dem Bundeskriminalamt habe ich darüber hinaus eine Reihe technischer und organisatorischer Maßnahmen in bezug auf AFIS angeregt, über die ich hier aber wegen der Komplexität dieser Sachverhalte nicht im einzelnen berichten kann.

23.4 Einreise in die USA mit Schwierigkeiten verbunden

Ein Petent schilderte mir folgenden Fall:

Anläßlich einer Urlaubsreise nach Florida wurden er und seine Ehefrau auf dem Flughafen Miami von der dortigen Einwanderungsbehörde für drei Stunden festgehalten. Der Grund wurde ihm nicht ausdrücklich genannt, sondern lediglich, daß irgend etwas im

Computer sei. Sein Reisegepäck wurde auf das Gründlichste durchsucht und er wurde gefragt, ob er nicht schon öfter Kontakt mit der Polizei gehabt hätte. Ich habe daraufhin eine Kontrolle beim Bundeskriminalamt und beim Bundesministerium der Finanzen für den Bereich des Zollfahndungsdienstes durchgeführt. Dort stellte sich heraus, daß personenbezogene Informationen über den Betroffenen nicht gespeichert waren. Jedoch habe ich festgestellt, daß eine Person mit nahezu identischen Personalien erfaßt war. Um zukünftige Verwechslungen auszuschließen, hat das Bundeskriminalamt veranlaßt, daß die Reisepaßnummer des Petenten in INPOL mit dem Hinweis erfaßt wird „Existente Person weist sich mit dem Reisepaß Nummer XYZ aus". Auch das Bundesministerium der Finanzen hat mir versichert, es habe alles veranlaßt, um Verzögerungen bei einer Personenüberprüfung künftig zu vermeiden.

Anläßlich einer Geschäftsreise in die USA zwei Jahre später wurde der Petent wieder von der Einwanderungsbehörde intensiv vernommen. Ihm wurde vorgehalten, daß gegen ihn der Verdacht bestehe, der Baader-Meinhof-Gruppe zugerechnet zu werden. Aufgrund dieses erneuten Vorfalls bei der amerikanischen Einwanderungsbehörde habe ich beim Bundesamt für Verfassungsschutz und beim Bundesnachrichtendienst kontrolliert und festgestellt, daß auch bei diesen Behörden keine personenbezogenen Daten über den Petenten registriert sind.

Leider konnte im vorliegenden Falle nicht aufgeklärt werden, ob und ggf. durch welche deutsche Behörde seinerzeit Informationen über den Petenten in die USA übermittelt wurden. Der Fall verdeutlicht jedoch, daß bei solchen Übermittlungen ein äußerst strenger Maßstab anzulegen und darauf zu achten ist, daß bei Datenübermittlungen ins Ausland, insbesondere in Staaten, in denen es keine dem hiesigen Standard entsprechenden Datenschutzregelungen gibt, Zweckbestimmungs- und Löschungsregelungen eingehalten werden müssen.

Das Bundeskriminalamt hat sich über das nationale Zentralbüro von INTERPOL in Wiesbaden an die Dienststelle von INTERPOL in Washington gewandt und versucht, den Sachverhalt aufzuklären, damit dem Petenten bei zukünftigen Einreisen in die Vereinigten Staaten die oben beschriebenen Unannehmlichkeiten und auch zu befürchtende Nachteile erspart bleiben. Nach fast einem Jahr teilte die US-amerikanische Polizeibehörde dem BKA lapidar mit, dem Petenten werde empfohlen, sich zur Lösung seines Problems an den Zollattaché bei der Botschaft der Vereinigten Staaten in Bonn zu wenden.

Aus meiner Sicht ist diese Auskunft nicht befriedigend. Im Rahmen meiner Zuständigkeit werde ich bei den deutschen Behörden darauf hinwirken, daß an ausländische Stellen nur solche Informationen übermittelt werden, die bezüglich der Erkenntnislage hinreichend gesichert sind, und daß darüber hinaus verfahrensrechtliche Vorkehrungen getroffenen werden, die einen größtmöglichen Schutz des Persönlichkeitsrechts gewährleisten.

23.5 INPOL-Neukonzeption – mehr als nur neue DV-Technik

INPOL ist das gemeinsame Informationssystem der Polizeibehörden des Bundes und der Länder, dessen wichtigste Anwendungsbereiche auf Bundesebene die Personen- und Sachfahndung, die Akten- und Personennachweissysteme, die PIOS-Anwendungen, die Falldateien und Spurendokumentationssysteme sind. INPOL wird seit über 20 Jahren betrieben; seine Konzeption entspricht im Grundsatz noch dem Stand der Datenverarbeitung zu Beginn der 70iger Jahre und läßt sich nur noch schwer fortentwickeln. Eine zentrale Schwachstelle des Systems ist die aufwendige Mehrfacherfassung von Daten für die verschiedenen INPOL-Anwendungen. Ferner wird bemängelt, das Informationssystem entspreche nicht mehr den eher arbeitsplatzorientierten Bedürfnissen der Anwender. Es besteht deshalb Einvernehmen zwischen den für die polizeiliche Informationsverarbeitung Verantwortlichen, das System durch eine Neukonzeption abzulösen. Bereits 1992 hatte der AK II „Innere Sicherheit" der Arbeitsgemeinschaft der Innenminister der Bundesländer in diesem Sinne votiert. Eine Arbeitsgruppe hat daraufhin ein „grobes Fachkonzept" zu INPOL-neu erstellt. Danach soll INPOL-neu einen gemeinsamen Datenpool umfassen, in dem alle personenbezogenen Daten unterschiedslos und ohne Differenzierung nach ihrer Verwendung gespeichert werden. Die näheren Eigenschaften der Daten (gleichgültig ob sie Beschuldigte, Opfer, Zeugen oder Hinweisgeber in einem Ermittlungsverfahren betreffen) ergeben sich nur aufgrund eines komplexen Beziehungsgeflechtes in der Datenbank. Nach dem Grobkonzept ist auch vorgesehen, bisher konventionell verarbeitete Daten (Meldedienste) ebenfalls in INPOL-neu zu speichern. Diese Informationen werden gemeinsam verwaltet und stehen somit grundsätzlich allen Anwendern zur freien Verfügung.

Die Neukonzeption wirft datenschutzrechtliche Fragen auf:

- Es müssen differenziertere Zugriffsverfahren geschaffen werden, weil der Datenpool allen Anwendern zugänglich ist.
- Ich sehe eine Gefährdung für das Recht auf informationelle Selbstbestimmung darin, daß Recherchen in diesem gemeinsamen Datenbestand möglich sind, in die auch Informationen mit einer besonderen Zweckbindung einbezogen werden.
- Das vorliegende Grobkonzept gibt keine Antwort auf die Frage, wie landesrechtliche Regelungen, die z. T. restriktivere Bestimmungen zur Datenverarbeitung enthalten, eingehalten werden können.
- Mit den vorgenannten exemplarisch genannten Modalitäten von INPOL-neu ist eine erhebliche Qualitätsverbesserung der polizeilichen Informationsverarbeitung gegenüber den bisherigen Anwendungen verbunden, die einen adäquaten datenschutzrechtlichen Standard erforderlich macht. Im einzelnen zählen hierzu folgende Anforderungen:

- Grundsatz der Verhältnismäßigkeit
  Unabhängig von der Frage der Zugriffsberechtigung ist zu klären, welche inhaltlichen Differenzierungen bei der Ausgestaltung dieses bundesweiten Systems erforderlich sind. Es muß sichergestellt sein, daß in dem neuen Verfahren lediglich solche Daten gespeichert werden, die die bisher geltenden Kriterien der überregionalen Bedeutung und Schwere einer Straftat erfüllen. Es darf bei der Neugestaltung von INPOL-neu nicht dazu kommen, daß eine vorgangsunabhängige Speicherung zu präventiven Zwekken erfolgt. Die Speicherung personenbezogener Daten von Opfern, Zeugen und Hinweisgebern, also von Personen, die weder Tatverdächtige noch Beschuldigte sind, kann weder zur polizeilichen Aufgabenerfüllung erforderlich noch verhältnismäßig sein. Im vorliegenden groben Fachkonzept wird bisher nicht nach Personen und nach ihrer Stellung im strafprozessualen Ermittlungsverfahren differenziert.
- Auswertungsmöglichkeiten
  Es muß sichergestellt sein, daß nur im unerläßlich notwendigen Umfang und im Rahmen der jeweiligen Aufgabenerfüllung des Anfragenden unter strikter Beachtung bestehender Zweckbindungsregelungen Recherchen durchgeführt werden.
- Verantwortlichkeit
  Es bedarf konkreter Festlegungen, welche Stelle für die gespeicherten personenbezogenen Daten und somit auch für die Pflege dieser Informationen im Datenbestand verantwortlich ist. So muß gewährleistet sein, daß diejenige Polizeidienststelle diese Aufgaben übernimmt, die auch materiell für die der Speicherung zugrunde liegende polizeiliche Aufgabe der Gefahrenabwehr oder Strafverfolgung zuständig ist.
- Zweckbindung
  Zweckbindungsregelungen für bestimmte Arten von Daten dürfen durch die Organisation der Daten und die vielfältigen Verarbeitungsmöglichkeiten nicht aufgehoben werden.
- Protokollierung
  Ein derartig komplexes Verfahren muß hinreichend kontrollierbar sein. Ich habe daher gefordert, eine den Anforderungen genügende Protokollierung vorzusehen, die eine Kontrolle durch die Datenschutzbeauftragten möglich macht. Darüber hinaus bedarf es klarer Regelungen für die Nutzung der entstehenden Protokolldatenbestände.
- Nutzungsmöglichkeiten des Systems
  Hinsichtlich der Abfragearten ist darauf zu achten, daß dem jeweiligen Anwender nur die Informationen zur Verfügung gestellt werden, die er im Rahmen der Erfüllung ihm übertragener polizeilicher Aufgaben benötigt. Das bisherige INPOL-Verfahren sieht getrennte Abfragemöglichkeiten innerhalb der bestehenden einzelnen Dateien vor. Auf diese Weise ist sichergestellt, daß ein technisch wirkungsvoll ausgestalteter Zugriffsschutz besteht. Das neue Verfahren ermöglicht durch die Schaffung einer Gesamtübersicht bei Abfragen eine erhebliche Erweiterung der bisherigen Nutzungsmöglichkeiten von INPOL.

  Im Rahmen von Recherchen kann das neue Verfahren dem Anwender Informationen zur Verfügung stellen, die im geltenden INPOL-System nur in temporären Dateien (Spurendokumentationssystemen) gespeichert werden. Dazu zählen Informationen über Zeugen und Hinweisgeber, für die landesrechtlich unterschiedliche Regelungen zur Datenverarbeitung bestehen. Auch hier ist es notwendig, durch eine wirkungsvolle differenzierte Zugriffsregelung notwendige Beschränkungen zu schaffen.
- Meldedienste
  Die kriminalpolizeilichen Meldedienste werden bisher konventionell, z. B. auf Papier, durchgeführt. Bei dem jeweils zuständigen Landeskriminalamt oder dem Bundeskriminalamt wird entschieden, welche der gemeldeten personenbezogenen Daten in INPOL oder in anderen Informationssystemen zu speichern sind. Diese bisher konventionelle Datenanlieferung soll bei INPOL-neu automatisiert werden. Bereits in einem sehr frühen Stadium der polizeilichen Arbeit sollen künftig Informationen in den gemeinsamen Datenpool eingegeben werden. Die Entscheidung darüber, welche personenbezogenen Daten nun im einzelnen gespeichert werden, würde dem eingebenden Sachbearbeiter der örtlich zuständigen Polizeidienststelle obliegen. Damit ist zu erwarten, daß vermehrt Daten eingespeist werden, ohne in einer weiteren Filterfunktion auf ihre Relevanz geprüft worden zu sein.
- Die polizeiliche Kriminalstatistik soll zukünftig ebenfalls über das neue System erstellt werden. Es muß sichergestellt bleiben, daß die Daten, die für diesen Zweck verarbeitet werden, auch weiterhin ausschließlich in anonymisierter Form gespeichert, ausgewertet und genutzt werden dürfen.
- Zugriff externer Stellen
  Nach dem vorliegenden fachlichen Grobkonzept ist ein direkter Zugriff externer Stellen, z. B. des Kraftfahrtbundesamtes, auf Teildatenbestände von INPOL-neu vorgesehen. Nach bisheriger Rechtslage sind derartige online-Abfragen nicht zulässig. Ein konkreter Bedarf hierfür ist bisher nicht dargelegt worden. Die Erforderlichkeit solcher Direktzugriffe Dritter auf polizeiliche Datenbestände wäre unter Anlegung eines besonders strengen Maßstabes zu prüfen.

  Zu meinen vorgenannten, mit den LfD's abgestimmten Anregungen und Bedenken vom Juni 1993 hat das Bundesministerium des Innern mir geantwortet, daß nach Auffassung der Projektgruppe im Bundeskriminalamt die aufgeführten Zielsetzungen wie „Herstellung von Einvernehmen mit den Datenschutzbeauftragten von Bund und Ländern", „Harmonisierung der Da-

tenschutz-Situation bei den INPOL-Teilnehmern" und „Regelung des Datenaustausches mit externen Behörden bzw. Stellen auf Basis einvernehmlicher Datenschutzregularien" in diesem Umfang nicht zu erfüllen seien. Für die Beschreibung des Teilprojekts „Datenschutz/Datensicherheit" sei die Beachtung der Bestimmungen des Bundesdatenschutzgesetzes ausreichend. Dies trifft nach meiner Auffassung nicht zu, denn im Bereich der polizeilichen Informationsverarbeitung gelten eine Reihe von bereichsspezifischen Regelungen, die das Bundesdatenschutzgesetz zurückdrängen.

Ich verschließe mich nicht gegenüber der Notwendigkeit, das INPOL-System neu zu konzipieren. Ich werde jedoch weiterhin darauf drängen, neben den rein anwenderorientierten Bedürfnissen die schutzwürdigen Interessen der Betroffenen nicht zu vernachlässigen.

23.6 IKPO-Interpol – Auskunftsrechte des Betroffenen

Im Oktober 1994 habe ich gemeinsam mit Vertretern der Datenschutzbeauftragten aus den EU-Mitgliedstaaten an einem Informationsbesuch bei der Interpol-Zentrale in Lyon teilgenommen. Ziel des Besuchs waren eine Präsentation der Informationsverarbeitung bei Interpol sowie ein Meinungsaustausch mit dem internen Datenschutz-Kontrollausschuß bei der Zentrale. Die zunehmende polizeiliche Zusammenarbeit in Europa, beispielsweise im Rahmen des Schengener Durchführungsübereinkommens (vgl. Nr. 23.2.1) sowie bei der Europäischen Drogeneinheit EDE/Europol (vgl. Nr. 23.2.3) haben auch bei Interpol zu Überlegungen zu einer engeren Kooperation mit diesen Institutionen geführt, zumal gewisse Überschneidungen bei der Erfüllung der jeweiligen Aufgaben in den EU-Mitgliedstaaten nicht zu verkennen sind. Der Besuch vermittelte den Eindruck, Interpol sehe sich durch diese europäischen Aktivitäten in eine gewisse Randlage gedrängt. Sollte zwischen den genannten Organisationen ein engerer Informationsverbund angestrebt werden, müßte dies bei Interpol zuvor zum Anlaß genommen werden, das dortige Datenschutzniveau dem Schengener Standard anzunähern. Die Schwierigkeit dieser Zielbestimmung zeigt sich allein daran, daß in ca. 130 von mehr als 170 Interpol-Mitgliedstaaten keine oder allenfalls rudimentäre Datenschutzregelungen bestehen.

Bei dem Meinungsaustausch mit dem Datenschutz-Kontrollausschuß ging es vor allem um das Auskunftsrecht der Betroffenen. Gegenüber Interpol verfügt ein Petent nur über ein indirektes Auskunftsrecht, d. h. seine Eingabe wird vom Datenschutz-Kontrollausschuß nach dessen Prüfung mit der Mitteilung erledigt, die Angelegenheit sei geprüft worden. Gegen diesen Bescheid gibt es keinerlei Rechtsschutz. Dies halte ich für sehr unbefriedigend. Die deutschen Vertreter in der Generalversammlung, dem höchsten Entscheidungsgremium bei Interpol, sollten sich daher für eine Änderung einsetzen. Ziel muß ein direktes Auskunftsrecht des Betroffenen gegenüber Interpol unter angemessener Berücksichtigung möglicherweise entgegenstehender Sicherheitsinteressen sein.

24 Bundesgrenzschutz

24.1 Gesetzgebungsstand – BGS-Neuregelungsgesetz in Kraft getreten

Zum 1. November 1994 ist das Bundesgrenzschutz-Neuregelungsgesetz – BGSNeuRegG – in Kraft getreten. Es tritt an die Stelle des BGS-Gesetzes von 1972. Einer der wesentlichen Gründe für die Novellierung des BGS-Gesetzes war die Umsetzung der datenschutzrechtlichen Anforderungen aus dem Volkszählungsurteil von 1983. Der BMI hatte im Frühjahr 1993 einen überarbeiteten Referentenentwurf vorgelegt, mit einem schon damals beachtlichen datenschutzrechtlichen Niveau. Ich habe mich schriftlich und mündlich zu diesem Entwurf geäußert, der bis zur Kabinettreife noch erheblich verbessert wurde.

Positiv zu erwähnen sind aus meiner Sicht:

- Klare und eindeutige Regelungen zu Aufgaben und Befugnissen des Bundesgrenzschutzes
- Die gesetzliche Grundlage für die funktechnische Unterstützung des BGS zugunsten des Bundesamtes für Verfassungsschutz und anderer Stellen (vgl. Nr. 24.2)
- Bei der Erhebung personenbezogener Daten ist der Betroffene in Anlehnung an § 13 BDSG zu belehren, soweit dies mit der Aufgabenerfüllung des BGS vereinbar ist
- Das Gesetz enthält keine Regelungen über den Einsatz Verdeckter Ermittler, da nach den Aufgaben des BGS hierfür kein zwingendes Bedürfnis besteht

In einigen Punkten wurden meine Vorstellungen nicht verwirklicht:

- Zur grenzpolizeilichen Beobachtung ist keine Unterrichtung des Betroffenen nach Abschluß der Maßnahme vorgesehen. Ich hatte dies unter Hinweis auf vergleichbare Regelungen in den meisten Polizeigesetzen der Länder angeregt. Das BMI verwies hingegen auf die Parallelregelung des § 163e StPO (OrgKG), die keine Benachrichtigung des Betroffenen vorsieht.
- Eine ausdrückliche Klarstellung, daß beim BGS die Erhebung personenbezogener Daten durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen (Lauschangriff) sowie durch den Einsatz verdeckter Ermittler unzulässig ist, wurde zu meinem Bedauern aus einem Vorentwurf des Gesetzes wieder gestrichen.

Insgesamt gesehen halte ich das BGS-NeuReg-Gesetz jedoch für eine gelungene Verwirklichung datenschutzrechtlicher Prinzipien. Es ist zu hoffen, daß die Vorgaben dieses Gesetzes sich vorteilhaft auf die Novellierung des BKA-Gesetzes (s. Nr. 23.1) auswirken werden.

24.2 Gruppe Fernmeldewesen – Nachrichtendienstliche Fernmeldeüberwachung

Bei der Novellierung des Bundesgrenzschutzgesetzes (s. Nr. 24.1) ist mit § 10 eine Regelung über die Verwendung des BGS zur Unterstützung des Bundesamtes für Verfassungsschutz (BfV) auf dem Gebiet der Funktechnik eingefügt worden. Aufgaben- und Befugnisrahmen dieser Auftragsdatenerhebung bestimmen sich nach dem Bundesverfassungsschutzgesetz. Auch Zweckbindungs- und Löschungsregelungen entsprechen den engen Befugnissen eines Auftragnehmers nach § 11 BDSG: Die erhobenen Daten dürfen nur im Rahmen der Unterstützungsaufgabe verwendet werden, insbesondere nur so lange gespeichert werden, wie es für diesen Zweck erforderlich ist. Das Verfassungsgebot, die Befugnisse von Nachrichtendiensten und Polizeibehörden getrennt zu halten, ist somit gewahrt. Der Regelungsbedarf für eine Spezialregelung bestand m. E. allenfalls im Hinblick auf die organisationsrechtliche Komponente des Trennungsgebotes. Die organisatorische Abgrenzung der Unterstützungstätigkeit von sonstigen Aufgabenbereichen des BGS ist folgerichtig in § 10 Abs. 3 BGSG vorgeschrieben, wobei das Nähere noch in einer Dienstanweisung festzulegen ist.

Ob es unter Erwägungen einer effizienten Verwaltungsorganisation nicht näher gelegen hätte, die eingesetzten Mittel gleich der Behörde zuzuordnen, deren Aufgaben tatsächlich wahrgenommen werden, ist keine Datenschutzfrage. Ich hätte es jedoch vorgezogen, wenn diejenigen Sachmittel des BGS, die ausschließlich für das BfV eingesetzt werden, durch Umwidmung dem BfV zugewiesen worden wären. Dadurch hätte sich diese Unterstützungstätigkeit im wesentlichen erledigt. Bei angemessenen Festlegungen zur organisatorischen und technischen Gestaltung der Praxis begegnet aber auch die nunmehr vom Gesetzgeber gewählte Lösung keinen durchgreifenden Datenschutzbedenken.

Bei meiner Beteiligung an dem Gesetzesentwurf bin ich erstmalig auf diese funktechnische Unterstützung des BGS für das BfV aufmerksam geworden. Ich habe daraufhin die Gruppe Fernmeldewesen (GrFMW), die diese Aufgabe wahrnimmt, kontrolliert. Es haben sich dabei keine Bedenken ergeben.

Allerdings – so habe ich festgestellt – wird die GrFMW – mit anderen Sachmitteln als für den Hauptbereich der BfV-Unterstützung – auch für eigene Aufgaben des BGS sowie für andere Polizeibehörden tätig. Soweit dies auf dem Gebiet der Strafverfolgung – beispielsweise für das BKA – erfolgt, habe ich keine wesentlichen Sachprobleme festgestellt. Den beteiligten Stellen war insoweit nicht hinreichend bewußt, daß ihre Zusammenarbeit als Auftragsverhältnis im Sinne des § 11 BDSG zu qualifizieren ist, mithin die datenschutzrechtliche Verantwortung beim Auftraggeber liegt, der im Auftrag klare Festlegungen u. a. zum zulässigen Datenumgang treffen muß. Ich habe angeregt, solche Regelungen im Benehmen der zuständigen fachaufsichtsführenden Ministerien zu treffen.

Für den präventivpolizeilichen Bereich lassen die jeweils anzuwendenden Befugnisregelungen (bei eigenen Aufgaben: BGSG/bei Organleihe für Länder: jeweiliges Landespolizeigesetz) die eingesetzten Erhebungsmittel und -methoden nicht zur bloßen Verdachtsermittlung zu, sondern nur zur Konkretisierung eines bestehenden Verdachts. Ich konnte noch nicht abschließend klären, ob die GrFMW für eigene Aufgaben des BGS tatsächlich nur zur Abwehr einer im Einzelfall bestehenden Gefahr – und nicht auch zur abstrakten Gefahrenvorsorge – eingesetzt wird. Eine ergänzende Kontrolle habe ich mir ausdrücklich vorbehalten.

24.3 Datenschutzrechtliche Kontrollen

24.3.1 Kontrolle beim Grenzschutzamt Frankfurt/Oder

Schwerpunkte meiner Prüfung waren die Datei Grenzaktennachweis (GAN), die Dienstanweisung Amtshilfe/Grenze (s. 14. TB Nr. 25.1) und Fragen der Datensicherheit.

1. Die Datei GAN dient dem Nachweis von personenbezogenen Akten, deren Führung bei der Grenzschutzdirektion und den Grenzschutzämtern zur Erfüllung der ihnen obliegenden Aufgaben bei der Verbrechensbekämpfung und der Gefahrenabwehr erforderlich ist.

   Um dem Zweck der Datei gerecht zu werden, müssen daher alle Daten im GAN zeitnah und lückenlos erfaßt werden. Bei der Kontrolle habe ich jedoch festgestellt, daß ca. 80 000 Aktenvorgänge beim Grenzschutzamt noch nicht im GAN erfaßt waren. In meinem Prüfbericht habe ich dem BMI mitgeteilt, daß ich es unter datenschutzrechtlichen Aspekten für dringend erforderlich halte, Regelungen über Aufbewahrung, Nutzung und Verarbeitung der noch nicht in der Datei GAN erfaßten Unterlagen zu treffen. Bei den noch nicht im GAN erfaßten Aktenvorgängen besteht insbesondere die Gefahr, daß die Aussonderungsprüffristen aufgrund der Errichtungsanordnung nicht eingehalten werden. Bei personenbezogenen Daten, die im GAN gespeichert sind, weist das System automatisch auf die Prüffristen hin. Weiterhin dürfen aus Unterlagen, die nicht fristgerecht vernichtet wurden, keine Auskünfte erteilt und die Vorgänge auch nicht anderweitig genutzt werden. Das BMI hat sich meiner Auffassung angeschlossen und zur beschleunigten Bearbeitung der Altvorgänge vorübergehend zusätzliche Bedienstete eingestellt. Eine weitere Aufstockung des Personals und der materiellen Ausstattung bleibt einer Organisationsprüfung beim Grenzschutzamt vorbehalten. Desweiteren hat das BMI mir die Erstellung einer Dienstanweisung zugesichert, in der

   - Aufbewahrung, Nutzung und Verarbeitung der noch nicht in der Datei GAN erfaßten Unterlagen und
   - die Bearbeitung und Speicherung sämtlicher aktuell anfallender Informationen in GAN geregelt werden sollen.

   Probleme habe ich auch bezüglich der Speicherfristen festgestellt. Das Grenzschutzamt hat bei der Dateneingabe regelmäßig die Maximalfrist von fünf Jahren vergeben. Nach der Errichtungsanord-

nung des GAN sind jedoch je nach Schwere des Falles Fristen zwischen einem und fünf Jahren vorgesehen. Eine Differenzierung hat nach meinen Feststellungen nicht stattgefunden. Dabei habe ich den Eindruck gewonnen, daß bei den Bediensteten über die Festlegung der Aussonderungsprüffristen große Unsicherheit bestand und vorsichtshalber daher die Maximalfrist vergeben wurde. Dies lag zum einen an der mangelnden Schulung, zum anderen auch an laufenden personellen Veränderungen. Daher habe ich trotz der festgestellten Mängel von einer Beanstandung abgesehen und empfohlen, eine Liste mit den unterschiedlichen Delikten und den entsprechenden Fristen zu erstellen, um bei Unklarheiten eine Entscheidungshilfe zu bieten. Gleichzeitig habe ich angeregt, daß die Fristen aufgrund der Sachnähe von den Bearbeitern festgelegt werden sollen. Weiterhin habe ich empfohlen, im Rahmen der Bearbeitung der bereits erfaßten Fälle die verfügten Aussonderungsprüffristen nochmals zu kontrollieren. Auch diese Anregungen hat das BMI aufgegriffen. Zusätzlich sollen die Fristen noch durch den Dienststellenleiter oder den Leiter des Ermittlungsdienstes überprüft werden.

2. Ich habe ferner die Durchführung der kürzlich erlassenen Dienstanweisung Amtshilfe/Grenze nach § 17 Abs. 2 BVerfSchG überprüft. Diese Dienstanweisung regelt die Zulässigkeit besonderer Ersuchen der Verfassungsschutzbehörden, des Militärischen Abschirmdienstes und des Bundesnachrichtendienstes und deren Erledigung durch die dafür zuständigen Stellen. Nach Auskunft des Grenzschutzamtes Frankfurt/Oder erfolgt diese Art von Amtshilfe nur in geringem Umfang und nur in Fällen der benannten Amtshilfe. Die Informationen werden per Telex auf dem Dienstweg an die Grenzschutzdirektion gemeldet. Dabei habe ich bemängelt, daß die Übermittlung über Telex nicht verschlüsselt erfolgt, da kein entsprechendes Verschlüsselungsgerät zur Verfügung steht. Das BMI hat mir inzwischen mitgeteilt, daß Maßnahmen eingeleitet wurden, die die Errichtung einer Krypto-Betriebsstelle (Comsec-Bereich) bis 1996 sicherstellen sollen.

3. Auch die Datensicherheit war zum Zeitpunkt der Prüfung mangelhaft. Nach meinem Eindruck entsprach bereits die Gebäudesicherung nicht den Anforderungen der Nr. 1 der Anlage zu § 9 Satz 1 BDSG. So können sich z. B. Unbefugte Zugang zu dem Gelände des Grenzschutzamtes verschaffen. Das BMI hat mir hierzu mitgeteilt, daß die Erneuerung der Umzäunung der Liegenschaft geplant sei. Dies soll voraussichtlich im Zuge der Herrichtung der Infrastruktur im Haushaltsjahr 1995 erfolgen.

   Nach meinen Feststellungen waren Personalakten von Bediensteten des Grenzschutzamtes in einem Raum auf Regalen offen aufbewahrt. Meiner Anregung, diese in verschließbaren Stahlschränken aufzubewahren, ist das BMI inzwischen nachgekommen.

   Schließlich habe ich das Problem der Verschlüsselung von Satellitenfunkstrecken angesprochen. Das Grenzschutzamt verfügt über zwei Terminals, über die auf das Informationssystem GAN und den geschützten Grenzfahndungsbestand beim BKA zugegriffen werden kann. Diese Geräte sind über Satellitenleitungen mit dem Zentralrechner verbunden. Leitungen, über die Daten in verschlüsselter Form übertragen werden können, waren jedoch nicht vorhanden. Auch dieser Mangel ist inzwischen vom BMI behoben worden.

24.3.2 Kontrolle beim Grenzschutz- und Bahnpolizeiamt Schwandorf

Schwerpunkt der Prüfung war die Falldatei Schleuser/Geschleuste (FDS), die seit 1. Februar 1993 probeweise betrieben wird. Als Erprobungsphase war zunächst ein Jahr vorgesehen. Sie wurde schließlich bis Herbst 1994 verlängert. Bei der FDS handelt es sich um eine Verbunddatei, die beim Bundeskriminalamt im automatisierten Verfahren geführt wird. Zweck der Datei ist die Aufklärung und Verhütung von illegalen Schleusertätigkeiten und der damit zusammenhängenden Straftaten. Aufnahme in die Falldatei finden Daten von Schleusern und von Geschleusten.

Dem BMI habe ich mitgeteilt, daß ich die Erfassung der Daten von Geschleusten aus nachfolgenden Gründen für datenschutzrechtlich bedenklich halte:

Die Personalien werden zunächst im Kriminalaktennachweis (KAN) erfaßt, um die Daten der Betroffenen in der Falldatei überhaupt erfassen zu können, was systembedingt erforderlich ist. Der KAN dient jedoch dem Nachweis von Kriminalakten, die beim Bund und den Ländern in Fällen schwerer oder überregional bedeutsamer Straftaten angelegt werden. Meines Erachtens trifft dies für die „unerlaubte Einreise", derer sich ein Geschleuster in der Regel strafbar macht, nicht zu. Zugriff auf den KAN haben das Bundeskriminalamt, die Grenzschutzämter, die Grenzschutzdirektion sowie alle Polizeidienststellen der Länder. Auch aus diesem Grund halte ich eine Speicherung der Daten der Geschleusten im KAN für bedenklich. Mir erscheint zweifelhaft, inwieweit für die Polizeidienststellen der Länder die Kenntnis dieser Daten erforderlich ist. Zudem führt ein und derselbe Sachverhalt zu unterschiedlichen Speicherfristen. Neben der Erfassung im KAN und in der FDS erfolgt die Speicherung im Grenzaktennachweis (GAN). Im GAN werden die Daten von geschleusten Personen regelmäßig mit einer Aussonderungsprüffrist von 5 Jahren, in der FDS jedoch mit einer Frist von 3 Jahren gespeichert.

Erhebliche Zweifel habe ich auch an der Erforderlichkeit der Speicherung der Daten von Geschleusten in der FDS selbst. Die Daten des Betroffenen werden bereits aufgrund der unerlaubten Einreise im GAN erfaßt. Bei einer Wiederholungshandlung reicht daher ein Rückgriff auf den Grenzaktennachweis aus. Wenn erkennbar sein soll, ob der Betroffene mit einem Schleuser illegal eingereist ist, reicht m. E. ein Vermerk „Geschleuster" im Datenfeld „Sondervermerk" aus. Auch besteht der Zweck einer Falldatei vor allem darin, Straftaten durch Speicherung und Vergleich des modus operandi unbekannten Tätern

zuzuordnen. Der Geschleuste kann allenfalls Informationen zur FDS beitragen, indem er Angaben zu der Person des Schleusers, der Anwerbung, der Anzahl der geschleusten Personen sowie dem Schleusungsweg etc. macht. Dafür ist es jedoch nicht erforderlich, die Personalien des Geschleusten in der Falldatei zu speichern. Unberücksichtigt ist, daß der Geschleuste das „Opfer" des Schleusers sein kann und auch aus diesem Grund eine zusätzliche Speicherung neben dem Grenzaktennachweis nicht gerechtfertigt erscheint. Das BMI hat mir mitgeteilt, daß eine Entscheidung darüber erst nach Ablauf des Erprobungsbetriebs erfolgen könne. Bis dahin sollen die Daten der geschleusten Personen weiterhin gespeichert werden.

25 Zoll- und Außenwirtschaftskontrolle

25.1 Gesetzgebungsstand – noch kein bereichsspezifischer Datenschutz für das Zollkriminalamt und für den Zollfahndungsdienst

Für die Verarbeitung personenbezogener Daten beim Zollkriminalamt stehen immer noch bereichsspezifische Regelungen aus (14. TB S. 140). Ich habe allerdings Verständnis für die Argumentation des BMF, die eingeleiteten Vorarbeiten erst dann fortzuführen, wenn wegen des engen Sachzusammenhangs über vergleichbare Regelungen im BKA-Gesetz/Strafverfahrensänderungsgesetz ein grundsätzliches Einvernehmen erzielt worden ist.

Das Gesetzesvorhaben sollte auch zum Anlaß genommen werden, bereichsspezifische Regelungen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch den Zollfahndungsdienst zu schaffen. Bisher ist diese Materie in § 208 Abgabenordnung geregelt, was ich für unzulänglich halte (vgl. 3. TB, S. 22), da die Regelung nur eine Aufgabenbeschreibung, aber keine Einzelbefugnisse enthält. Die Zollfahndungsstellen erheben, verarbeiten und nutzen personenbezogene Daten ebenso wie das Zollkriminalamt für Zwecke der Strafverfolgung, zur vorbeugenden Bekämpfung von Steuerdelikten sowie zum Zweck der Marktbeobachtung.

25.2 Gemeinsames Zollinformationssystem der EU-Mitgliedstaaten –ZIS – Konvention noch nicht unterzeichnet

Bereits in meinem 14. Tätigkeitsbericht (S. 140) hatte ich über ein geplantes Zollinformationssystem der EU-Mitgliedstaaten berichtet. Die Verhandlungen über einen Konventionsentwurf sind nach wie vor nicht abgeschlossen, da zwei Punkte – Stellung des Europäischen Gerichtshofs und Inbetriebnahme des Systems – noch offen sind.

Im Berichtszeitraum hat es Diskussionen über das in Artikel 14 vorgesehene Auskunftsrecht gegeben, das der Regelung des Artikel 109 des Schengener Durchführungsübereinkommens entspricht. Danach kann der Betroffene sein Recht auf Auskunft in jedem Mitgliedstaat ausüben. Frankreich wollte dem Betroffenen ein Auskunftsrecht nur gewähren, wenn der Staat, der die Daten eingegeben hat, zuvor zugestimmt hat. Schließlich hat man sich bei den Verhandlungen auf eine Lösung analog Schengen verständigt, d. h. die Auskunftserteilung bedarf nicht der Zustimmung der ausschreibenden Vertragspartei.

Strittig war ferner, auf welcher Rechtsgrundlage die Europäische Kommission befugt sein soll, den Mitgliedstaaten die Hard- und Software des ZIS zur Verfügung zu stellen und zu verwalten. Dies hatte die Kommission den Mitgliedstaaten bereits zu Anfang der Verhandlungen angeboten, da sie parallel ein eigenes Informationssystem zur Bekämpfung von Zuwiderhandlungen gegen Zoll- und Agrarregelungen der EG (EG-ZIS) plant. Rechtsgrundlage soll eine neue EG Amtshilfe-Verordnung (siehe Nr. 5.6) werden. Hier hat man sich schließlich auf eine Regelung im Entwurf dieser Verordnung geeinigt. Danach werden die Zollbehörden der Mitgliedstaaten die Hard- und Software des EG-ZIS nutzen. Meine Sorge von einer Vermengung beider Systeme, womit die Kommission Zugriff auf den Datenbestand der Mitgliedstaaten erhalten würde, konnten zum Teil ausgeräumt werden. Beide Datenbestände sollen logisch voneinander getrennt bleiben. Des weiteren soll sich die Kommission in einer Erklärung zum Übereinkommen der Mitgliedstaaten verpflichten, die erforderlichen Maßnahmen zu treffen, um den Datenschutz zu gewährleisten. Auch soll die gemeinsame Aufsichtsbehörde über das ZIS der EU-Mitgliedstaaten ein Zugangsrecht zu diesem Zollinformationssystem erhalten. Wünschenswert wäre jedoch eine Klarstellung gewesen, die die Trennung zwischen den beiden Zollinformationssystemen ausdrücklich festschreibt. Die deutsche Delegation hat diesen Punkt bei den Verhandlungen in Brüssel mehrfach vorgetragen, konnte sich aber damit nicht durchsetzen. Nun wird für beide Datensammlungen der Begriff Zollinformationssystem – ZIS – verwendet, obwohl es sich um zwei Systeme mit unterschiedlichen Rechtsgrundlagen, verschiedenen Zweckbestimmungen und Benutzern handelt. Ich hoffe sehr, daß den eingebenden Stellen der Unterschied zwischen beiden Systemen bekannt ist, und die Daten in die richtige Datei eingegeben bzw. von dort abgerufen werden. Als nationaler Vertreter in der Datenschutz-Kontrollinstanz für das ZIS der EU-Mitgliedstaaten werde ich hierauf besonders achten.

25.3 Datenverarbeitungssystem KOBRA

Im Berichtszeitraum habe ich mich über den Ausbaustand des Datenverarbeitungssystems **Kontrolle bei der Ausfuhr** – KOBRA – der Zollverwaltung informiert. Dieses war am 1. April 1991 in Betrieb genommen worden, um nach den Erfahrungen aus dem Golfkrieg künftig sicherzustellen, daß im Außenwirtschaftsverkehr keine Waren, deren Ausfuhr besonderen Beschränkungen unterliegt, in Krisengebiete verbracht werden. Derzeit sind an KOBRA das Zollkriminalamt und ca. 200 Ausfuhrzollstellen angeschlossen. Die Zollstellen erfassen Waren, die z. B. als Rüstungsgüter oder zur Errichtung kerntechnischer Einrichtungen oder zur Herstellung chemischer Waf-

fen verwendet werden können. Der Umfang der in KOBRA gespeicherten Daten richtet sich danach, ob die Ausfuhren nach dem Gefährdungspotential dieser Waren als hochsensibel bzw. sensibel eingestuft werden. Bei hochsensiblen Waren wird das Ausfuhrdokument vollständig in KOBRA abgebildet, während sensible Waren nur mit einem Kurzsatz erfaßt werden. Personenbezogene Daten des Exporteurs, des Versenders und des Empfängers der Waren werden ebenfalls gespeichert.

KOBRA, das aus verschiedenen, miteinander verknüpften Unterdateien besteht, liefert den Ausfuhrzollstellen Hinweise zu den abzufertigenden Waren und ermöglicht damit die Überwachung der Einhaltung der Vorschriften des Außenwirtschaftsrechts. Eine Warnhinweisdatei als Bestandteil von KOBRA, die vom Zollkriminalamt erstellt wird, gibt darüber hinaus Hinweise, ob zu den am Warenverkehr Beteiligten Erkenntnisse vorliegen, daß diese gegen Vorschriften des Außenwirtschaftsrechtes verstoßen könnten. Ferner wird angezeigt, wenn für bestimmte Länder aufgrund politischer Vorgaben Handelsbeschränkungen vorgesehen sind, deren Nichtbeachtung strafbar ist. Im Hinblick darauf, daß die Warnhinweisdatei vielfach Erkenntnisse enthält, die noch nicht vollständig gesichert sind, beträgt die Frist für die Speicherung grundsätzlich ein Jahr mit einer Verlängerungsmöglichkeit von einem weiteren Jahr. Die Datei unterliegt einer strikten Zweckbindung; sie ist nur den Stellen zugänglich, die mit der Überwachung des Außenwirtschaftsverkehrs betraut sind.

Das Zollkriminalamt benutzt KOBRA zur Überwachung des Außenwirtschaftsverkehrs und zur Verhütung und Verfolgung von Verstößen gegen das Außenwirtschaftsrecht mittels Recherche. Rechtsgrundlage hierfür ist § 12 Abs. 4 Satz 2 Nr. 1a Finanzverwaltungsgesetz (FVG). Solche Recherchen dürfen nur von einem Beamten des höheren Dienstes mit der Befähigung zum Richteramt angeordnet werden. Sie sind darüber hinaus zu dokumentieren, was mir jederzeit eine Kontrolle der Zulässigkeit der durchgeführten Recherche ermöglicht. Im Rahmen dieser Recherchen wird z. B. festgestellt, welche Waren, von welchem Exporteur und für welchen Empfänger in einem bestimmten Zeitraum in ein bestimmtes Land verbracht worden sind. Aufgrund dieses Rechercheergebnisses wird dann im Rahmen einer Außenwirtschaftsüberprüfung festgestellt, ob die gesetzlichen Vorschriften des Außenwirtschaftsrechtes eingehalten worden sind. Ggf. werden noch im Rahmen der laufenden Außenwirtschaftsüberprüfung von der dann einzuschaltenden Zollfahndungsdienststelle Ermittlungsverfahren eingeleitet und durchgeführt. Die personenbezogenen Daten des Beschuldigten werden dann auch im Informationssystem für den Zollfahndungsdienst – INZOLL – gespeichert.

Über die Einhaltung der Recherchekriterien habe ich mich anläßlich eines Besuches beim Zollkriminalamt informiert. Die von mir eingesehenen Recherchedokumentationen enthielten den Grund der durchgeführten Recherche, die Genehmigung des verantwortlichen Beamten, die Rechercheergebnisse und darauf folgende weitere außenwirtschaftliche Maßnahmen. Auch weitere Empfänger von personenbezogenen Daten waren lückenlos dokumentiert.

25.4 Zusammenarbeit Polizei/Zoll bei der Rauschgiftbekämpfung

Der nationale Rauschgiftbekämpfungsplan, von der Nationalen Drogenkonferenz am 13. Juni 1990 verabschiedet, sieht zur Intensivierung der Maßnahmen zur Bekämpfung der Rauschgiftkriminalität u. a. eine verbesserte Zusammenarbeit zwischen Polizei und Zoll vor. Hierzu sollen Gemeinsame Ermittlungsgruppen Verfahren bearbeiten, für die sowohl Zoll als auch Polizei zuständig sind. Dies setzt voraus, daß das Rauschgift in das Bundesgebiet geschmuggelt worden ist. Inzwischen wurden 25 gemeinsame Ermittlungsgruppen Polizei/Zollfahndung eingerichtet. Wie auch aus der Presse zu entnehmen war, hat die Einrichtung gemeinsamer Ermittlungsgruppen zu Fahndungserfolgen geführt. So sollen in mehreren Fällen Rauschgifthändlerringe gesprengt und Betäubungsmittel in erheblichen Mengen sichergestellt worden sein. Die früher aufgetretenen Mißverständnisse und Pannen, die jeweils dann entstanden, wenn Polizei und Zoll in einem Ermittlungsverfahren nebeneinander ermittelten, ohne davon zu wissen, sollen durch die Einrichtung dieser gemeinsamen Ermittlungsgruppen verhindert werden.

Gegen die Einrichtung gemeinsamer Ermittlungsgruppen Zoll/Polizei bestehen keine grundlegenden datenschutzrechtlichen Bedenken, weil sie nur in solchen Ermittlungsverfahren tätig werden, für die beide Exekutivzweige zuständig sind. Das Bundesministerium der Finanzen hat mir bestätigt, daß andere Deliktsbereiche, die jeweils in der alleinigen Zuständigkeit von Polizei oder Zollfahndung liegen, von einer gemeinsamen Ermittlungsgruppe nicht bearbeitet werden. In einer Vereinbarung zwischen der Finanzverwaltung und den Innenministerien der Länder wird ausdrücklich festgelegt, daß die Informationsverarbeitung durch die Zollfahndung und die Polizei räumlich getrennt erfolgt. Insoweit ist eine organisatorische Trennung der Informationsverarbeitung gegeben. In der gemeinsamen Ermittlungsgruppe benutzt die Zollfahndung das Informationssystem für den Zollfahndungsdienst (INZOLL), die Polizei hat auf die rauschgiftspezifischen Informationssysteme von INPOL (Falldatei Rauschgift, Arbeitsdatei PIOS-Rauschgift) Zugriff. Eigene Informationssysteme betreiben die gemeinsamen Ermittlungsgruppen nicht. Eine gegenseitige konventionelle Übermittlung von Erkenntnissen erfolgt nur dann, wenn dies unter Beachtung der Polizeigesetze der Länder oder der Vorschriften der Abgabenordnung zulässig ist.

Für den Bürger, der eine Verarbeitung seiner personenbezogenen Daten durch eine gemeinsame Ermittlungsgruppe in den Informationssystemen der Zollfahndung oder der Polizei vermutet, entstehen hinsichtlich seines Auskunftsrechts keine datenschutzrechtlichen Defizite. Der Betroffene kann sich an eine gemeinsame Ermittlungsgruppe wenden und diese um Auskunft über die zu seiner Person gespeicherten Daten ersuchen. Sind personenbezogene Da-

ten von ihm gespeichert, entscheidet die für die Eingabe in INZOLL oder INPOL verantwortliche Stelle, ob dem Betroffenen Auskunft über seine Daten erteilt werden kann. Darüber hinaus kann sich der Betroffene auch an das zuständige Zollfahndungsamt oder an das Landeskriminalamt wenden und auch dort einen Auskunftsantrag stellen. Mit den Landesbeauftragten für den Datenschutz bin ich der Auffassung, daß die datenschutzrechtliche Kontrolle durch die Landesbeauftragten für den Datenschutz erfolgt, soweit eine Datenverarbeitung durch die Polizei eines Bundeslandes vorliegt, während ich für die Kontrolle der Zollfahndung zuständig bin.

25.5 Grundstoffüberwachungsgesetz – GÜG –

Erst in einem späten Stadium der Beratungen wurde ich vom Bundesministerium für Gesundheit über den Entwurf eines Gesetzes zur Überwachung des Verkehrs mit Grundstoffen, die für die unerlaubte Herstellung von Betäubungsmitteln mißbraucht werden können (GÜG), unterrichtet. Das Gesetz dient der Umsetzung einer entsprechenden EG-Richtlinie vom 14. Dezember 1992. Eine frühzeitige Beteiligung wäre jedoch wünschenswert gewesen, damit datenschutzrechtliche Anliegen von vornherein und damit leichter hätten berücksichtigt werden können. Das zwischenzeitlich erlassene Gesetz tritt zum 1. April 1995 in Kraft.

Das Gesetz sieht umfassende Kontrollmaßnahmen vor, um die mißbräuchliche Abzweigung von bestimmten chemischen Erzeugnissen (Grundstoffen) zum Zwecke der unerlaubten Herstellung von Betäubungsmitteln zu verhindern bzw. zu verfolgen. Hierfür benötigen die zuständigen Behörden (Bundesinstitut für Arzneimittel und Medizinprodukte, Bundeskriminalamt, Landeskriminalämter sowie Zollkriminalamt) zur Wahrnehmung ihrer Aufgaben Informationen von den Wirtschaftsbeteiligten. Die Anzeigen der Wirtschaftsunternehmen wegen des Verdachts einer mißbräuchlichen Chemikalienabzweigung erfolgen gegenüber einer beim BKA einzurichtenden Gemeinsamen Stelle, die sich aus Mitarbeitern des BKA und des ZKA zusammensetzt. Eine entsprechende Form der Zusammenarbeit zwischen Zoll und Polizei gibt es bereits, z. B. bei der Rauschgiftbekämpfung (s. Nr. 25.4). Diese Mitteilungen leitet die Gemeinsame Stelle nach der jeweiligen Zuständigkeit an BKA, LKA, ZKA sowie an das Bundesinstitut für Arzneimittel und Medizinprodukte weiter. Meine Anregungen – eine genaue Aufgabenbeschreibung der Gemeinsamen Stelle, die Aufnahme einer Regelung, wem die personenbezogenen Daten übermittelt werden, und eine Zweckbindungsvorschrift – wurden erfreulicherweise übernommen. Die Einrichtung eines automatisierten Abrufverfahrens zwischen dem Zollkriminalamt und dem Bundesinstitut für Arzneimittel und Medizinprodukte ist nach Auffassung der Bundesregierung erforderlich, da das ZKA zur Erfüllung seiner Aufgaben die konkreten Angaben über die Ein- und Ausfuhren der Grundstoffe, die die Wirtschaftsbeteiligten an das Bundesinstitut für Arzneimittel und Medizinprodukte melden, benötigt. Hierbei wurden Vorkehrungen nach § 10 BDSG über die Einrichtung eines automatisierten Abrufverfahrens meinen Vorstellungen entsprechend berücksichtigt.

26 Verfassungsschutz

– Unbefriedigende Zusammenarbeit mit dem Bundesamt für Verfassungsschutz –

Mit der Novellierung des Bundesverfassungsschutzgesetzes (BVerfSchG) im Jahre 1990 galt es, die geänderte Rechtslage in die Praxis umzusetzen. So hatte das Bundesamt für Verfassungsschutz u. a. seine dienstinternen Vorschriften anzupassen (s. Nrn. 26.5 bis 26.7). Insbesondere die Arbeitspläne der einzelnen Abteilungen des Bundesamtes für Verfassungsschutz, die für die Bearbeiter konkretisierende Regelungen enthalten und somit den Charakter von Verwaltungsvorschriften haben, mußten überarbeitet werden. Der Deutsche Bundestag hatte hierzu in seiner Sitzung am 5. Februar 1993 (Bundestagsdrucksache 12/4094) beschlossen, daß sämtliche Arbeitspläne bis zum 30. Juni 1993 – der neuen Sach- und Rechtslage folgend – in angepaßter Form in Kraft zu setzen sind. Vom Bundesministerium des Innern erhielt ich daraufhin Entwürfe der Arbeitspläne für die einzelnen Abteilungen des BfV, die zunächst vorläufig in Kraft gesetzt wurden. In schriftlichen und mündlichen Erörterungen mit dem Bundesministerium des Innern und dem Bundesamt für Verfassungsschutz habe ich zwischenzeitlich Einigung über eine Reihe der von mir geäußerten Kritikpunkte erreichen können; abgestimmte Fassungen der Arbeitspläne lagen jedoch bei Redaktionsschluß noch nicht vor (s. Nr. 26.5).

Bei Dateianordnungen, die das Bundesamt für Verfassungsschutz nach § 14 Bundesverfassungsschutzgesetz für jede automatisierte Datei zu erstellen hat, bin ich anzuhören. Da die Beschreibung des von einer Datei betroffenen Personenkreises partiell deckungsgleich ist mit den Festlegungen in dem jeweiligen Arbeitsplan, kann derzeit zu einzelnen Arbeitsplänen noch keine endgültige Aussage aus datenschutzrechtlicher Sicht erfolgen.

Gegen Ende des Berichtszeitraums hat es gravierende Meinungsverschiedenheiten zu der Frage gegeben, ob es sich bei einigen DV-Anwendungen überhaupt um solche automatisierte Dateien handelt, für die Dateianordnungen zu erstellen sind. Darüber hinaus scheint es, daß nicht für sämtliche automatisiert betriebenen Dateien beim Bundesamt für Verfassungsschutz die gesetzlich vorgeschriebenen Dateianordnungen erstellt wurden. Anhand der mir vom Bundesamt für Verfassungsschutz auf Anforderung im Jahre 1992 zugeleiteten internen Dateienübersicht habe ich festgestellt, daß diese dringend überarbeitungsbedürftig ist. Sie enthielt einige Dateien, für die mir bis dato keine Dateianordnungen vorliegen. Andererseits waren jedoch Dateianordnungen für einige automatisiert betriebene Dateien beim Bundesamt für Verfassungsschutz erstellt worden, die aber nicht in der internen Übersicht aufgeführt waren. Das Bundesamt für Verfassungsschutz sagte mir seinerzeit zu, die interne Dateienübersicht zu aktualisieren und mir dann unaufgefordert ein

Exemplar zuzusenden. Nachdem fast ein Jahr verstrichen war und mir weder sämtliche Dateianordnungen noch die angekündigte Dateienübersicht vorlagen, habe ich das Bundesamt für Verfassungsschutz unter Fristsetzung bis zum 1. März 1994 aufgefordert, die erbetenen Unterlagen zu übersenden. Die überarbeitete interne Übersicht der beim Bundesamt für Verfassungsschutz geführten Dateien ging mir am 25. Mai 1994 zu. Sie enthielt wiederum Unstimmigkeiten. Beispielsweise sind in der neueren Übersicht einige Dateien nicht mehr aufgeführt, obwohl diese noch bestehen. Bei einer Datei wurde mir bereits 1990 der Entwurf einer Dateianordnung übersandt. Nachdem ich mich hierzu geäußert hatte, erhielt ich sodann im Jahre 1991 die endgültige Fassung der Dateianordnung. Da auch diese Datei nicht mehr in der vorerwähnten Übersicht aufgeführt war, wies ich das Bundesamt für Verfassungsschutz darauf hin, worauf es lapidar mitteilte, die Datei werde nicht vom BfV betrieben. Eine Aufnahme der Datei in die neue Dateienübersicht erübrige sich daher. Bei anderen Dateien erfuhr ich zufällig, daß sie aufgelöst und die vorhandenen Datenbestände in andere Dateien übernommen worden sind. Um zu gewährleisten, daß ich über den aktuellen Stand der Datenverarbeitung bei der Verfassungsschutzbehörde informiert bin, halte ich es für unerläßlich, auch über die Löschung von automatisiert betriebenen Dateien unterrichtet zu werden. Ich könnte mir in diesem Bereich durchaus eine fruchtbarere Zusammenarbeit mit dem Bundesamt für Verfassungsschutz vorstellen. Diese könnte darin bestehen, daß mir jeweils nach Ablauf eines Jahres die interne Dateienübersicht unaufgefordert zugesandt wird.

Im Berichtszeitraum wollte ich mich auch über die Praxis der Auskunftserteilung an betroffene Bürger beim Bundesamt für Verfassungsschutz aufgrund der neuen Rechtslage unterrichten. Die bei der Behörde eingehenden Auskunftsersuchen der Betroffenen und die dazugehörigen Aktenunterlagen des behördlichen Datenschutzbeauftragten werden nicht im nachrichtendienstlichen Informationssystem (NADIS-PZD) nachgewiesen, sondern in einer besonderen Datei (REGA), die vorrangig Registraturzwecken dient. Hierfür ist nach Auffassung des Bundesamtes für Verfassungsschutz keine Dateianordnung zu erstellen, da es sich um eine reine Verwaltungsdatei handele (s. u. Nr. 26.9). Das Bundesamt für Verfassungsschutz bestritt überhaupt meine Kontrollkompetenz für die in dieser Datei gespeicherten Daten. Nach einigen Gesprächen auf höherer Ebene wurde, ohne präjudizierende Wirkung für die Zukunft, eine Regelung dahin gehend getroffen, daß mir ca. sechs bis acht Vorgänge zur Einsichtnahme vorgelegt werden. Diese habe ich im einzelnen überprüft. Auf dieser sehr eingeschränkten Basis mußte ich eine Bewertung unter datenschutzrechtlichen Aspekten vornehmen (s. u. Nr. 26.11). Ein solches Verfahren kann unter Beachtung der geltenden Rechtslage künftig nicht akzeptiert werden.

26.1 Aufgaben des Verfassungsschutzes

Zunehmend werden Forderung laut, die Aufgaben des Bundesamtes für Verfassungsschutz auszudehnen (siehe Anlage 12). Hierbei steht die Beobachtung von Feldern organisierter Kriminalität im Vordergrund, insbesondere Drogenhandel und Geldwäsche.

Der Präsident des Bundesamtes für Verfassungsschutz hat in einem Fachaufsatz die Meinung geäußert, seine Behörde habe bereits nach gegenwärtiger Rechtslage die Aufgabe, solche Bereiche **profitorientierter Kriminalität** aufzuklären. Angesichts der ausdrücklichen Begriffsbestimmungen des Bundesverfassungsschutzgesetzes, die eine klare Beschränkung auf politisch bestimmte Verhaltensweisen enthalten, erscheint mir diese Auffassung nicht zutreffend.

Dabei wird als Vorzug hervorgehoben, daß staatsanwaltschaftliche Sachleitung und Richtervorbehalt beim Einsatz von V-Leuten entfielen. Besonders betont wird auch die Möglichkeit, Quellenschutz zu gewährleisten – aus Sicht des Betroffenen formuliert: den Anspruch auf rechtliches Gehör substantiell zu beschneiden. Die Befassung des Verfassungsschutzes soll danach zentrale Grundsätze des Strafverfahrensrechts außer Acht lassen, das insoweit allgemein – auch vom Bundesverfassungsgericht – als „angewandtes Verfassungsrecht" verstanden wird.

26.2 Asylverfahren im nachrichtendienstlichen Informationszugriff – übermäßig und intransparent

Die Probleme der Zusammenarbeit des Bundesamtes für die Anerkennung ausländischer Flüchtlinge mit Nachrichtendiensten (s. 14. TB S. 145) sind noch nicht vollständig bereinigt. Jedoch ist mir das BMI zwischenzeitlich mit einigen Verbesserungen entgegengekommen:

- Ausländische Nachrichtendienste sind nicht mehr in das Verfahren einbezogen.
- Die allgemeine Weitergabe von Angaben zu Asylbewerbern an Nachrichtendienste ist eingestellt worden. Es werden nur noch Daten solcher Asylbewerber übermittelt, die bestimmten, abstrakt bezeichneten Merkmalen entsprechen. Diesem Verfahren liegen sog. Kriterienkataloge zugrunde, die von den Nachrichtendiensten aufgestellt wurden.
- Die Räume des BfV, in denen Asylbewerber befragt werden, wurden entsprechend ausgeschildert.

Gleichwohl sind meine Bedenken in Kernpunkten nicht ausgeräumt worden:

- Die eindeutige **Bezeichnung der datenerhebenden Stellen bereits auf** der **Laufkarte** ist rechtlich geboten (s. auch 14. TB S. 42). Auf der Laufkarte werden dem Asylbewerber die Stationen benannt, die er während seiner Anwesenheit in der Aufnahmeeinrichtung aufsuchen soll, wie z. B. „Zi.Nr. 240 – Bl Zirndorf". Die Verwendung einer solchen „Tarnbezeichnung" ist ein nachrichtendienstliches Mit-

tel, dessen Voraussetzungen nach § 9 Abs. 1 BVerfSchG nicht vorliegen. Auch die nach § 8 Abs. 4 BVerfSchG erforderlichen Hinweise auf Erhebungszweck und insbesondere Freiwilligkeit der Angaben müssen bereits auf der Laufkarte erfolgen, um dem Betroffenen – wie vom Gesetz gewollt – die freie Mitwirkungsentscheidung zu überlassen. Den Hinweis des BMI, die Legende diene dem Schutz der Betroffenen vor Strafverfolgung durch den Heimatstaat wegen Zusammenarbeit mit deutschen Nachrichtendiensten, halte ich für verfehlt. Zum einen tritt das BfV bei der Befragung als solches auf. Zum anderen sollte der Betroffene gerade dann, wenn die Zusammenarbeit Risiken birgt, diese auch erkennen können. Der Schluß, wenn der Betroffene nicht wisse, welcher Stelle er Angaben macht, handele er nicht vorsätzlich und könne auch im Herkunftsland nicht strafrechtlich belangt werden, scheint mir an der Rechtswirklichkeit gerade solcher Staaten vorbeizugehen, an denen die Nachrichtendienste ein besonderes Aufklärungsinteresse haben. Durch einschlägige Verwaltungsrechtsprechung sehe ich mich in dieser Einschätzung bestärkt.

- Auch die **reduzierte Datenübermittlung** des BAFl an die Nachrichtendienste überschreitet die gesetzlichen Befugnisse. Der Gesetzgeber hat eine Informationsweitergabe von Verwaltungsbehörden an Nachrichtendienste unter Durchbrechung der Bindung an den Erhebungszweck nicht uneingeschränkt zugelassen. Im Verwaltungsvollzug begründete Pflichten und Obliegenheiten sollen nicht pauschal auch nachrichtendienstlichen Aufgaben dienen. Die Gesetze unterscheiden, ob die informationelle Zusammenarbeit auf Dauer angelegt ist oder sich auf einen konkreten Sachverhalt bezieht.

  Die Dauerzusammenarbeit des BAFl mit dem BfV ist auf erkennbare Fälle geheimdienstlicher Tätigkeit oder gewaltorientierter Bestrebungen beschränkt (§ 18 Abs. 1 BVerfSchG). Soweit das BfV weitergehende Informationen für seine Aufgaben benötigt, kann es zwar um deren Übermittlung ersuchen (§ 18 Abs. 3 BVerfSchG). Zur Wahrung der zweck- und stellenbezogenen Befugnisschranken in § 18 Abs. 1 und 2 BVerfSchG müssen solche Ersuchen aber auf den Einzelfall beschränkt sein. Sie erstrecken sich nur auf vorhandene Erkenntnisse (§ 17 Abs. 1 BVerfSchG). Die angesprochenen Kriterienkataloge können deshalb allenfalls als Hilfen für das BAFl zur Auslegung der Spontanübermittlungsregelung (§ 18 Abs. 1 BVerfSchG) verstanden werden, nicht als weitergehende Übermittlungsersuchen. Die in den Katalogen aufgeführten Kriterien, die eine Übermittlung veranlassen sollen, gehen jedoch in Teilen – entgegen § 18 Abs. 1 BVerfSchG – über erkennbare Fälle geheimdienstlicher Tätigkeit oder gewaltorientierter Bestrebungen hinaus.

Ich bin mit dem BMI in der Sache weiter im Gespräch. Dabei spielen auch andere Fragen von mindestens ebensolchem Gewicht eine Rolle, die ich aufgrund vorgebrachter Geheimschutzeinwände jedoch nicht offen darstellen kann.

26.3 Aussiedleraufnahme und Nachrichtendienste

Bei der Aussiedleraufnahme durch das Bundesverwaltungsamt erfolgt eine vergleichbare Beteiligung von Nachrichtendiensten wie im Asylverfahren (s. Nr. 26.2), was ähnliche Probleme aufwirft:

Das BfV hat in seinen Befragungsstellen vor Ort über Terminals Zugriff auf bestimmte, vom BVA automatisiert gespeicherte Daten sämtlicher Antragsteller. Ich habe darauf hingewiesen, daß die Einrichtung automatisierter Abrufverfahren zugunsten der Dienste hier unzulässig ist, weil die einschlägige Regelung des § 10 BDSG im BVerfSchG für nicht anwendbar erklärt wird. Das BMI hat mir entgegnet, die Datenherrschaft gehe nicht erst mit dem Abruf über, vielmehr gehe dem die Entscheidung des BVA voraus, den Empfängern den zugriffsfähigen jeweiligen Gesamtbestand insgesamt zur Verfügung zu stellen. Das BMI ist der Auffassung, das Persönlichkeitsrecht der Betroffenen würde nicht verletzt, weil das BVA sämtliche der jeweils zum Abruf bereitgehaltenen Daten an das BfV übermitteln darf.

Dies ist jedoch unzutreffend, weil die Voraussetzungen für Spontanübermittlungen nach § 18 Abs. 1 BVerfSchG – unstreitig – nicht vorliegen und die Befugnis zur Übermittlung auf Ersuchen nach § 18 Abs. 3 BVerfSchG – entgegen der Auffassung des BMI – keine Grundlage für eine über den Einzelfall hinausweisende, auf Dauer angelegte informationelle Zusammenarbeit enthält, die faktisch die Schranken der gesetzlichen Spontanübermittlungsregelung unterliefe. Im übrigen setzt die Informationssammlung des BfV voraus, daß tatsächliche Anhaltspunkte für extremistische oder sicherheitsgefährdende Bestrebungen oder Tätigkeiten vorliegen (§ 4 Abs. 1 Satz 3 BVerfSchG). Aussiedler können jedoch nicht pauschal als Extremisten oder Spione verdächtigt werden.

Soweit die Dienste noch vor Ort präsent sind, werden sie unverändert unter einer fremden Bezeichnung auf der **Laufkarte** genannt (14. TB S. 42). Ich halte dies aus den unter Nr. 26.2 dargelegten Gründen weiterhin für unzulässig.

Die Erörterung mit dem BMI ist noch nicht abgeschlossen. Dabei geht es ebenfalls (s. o. Nr. 26.2) auch um Fragen, deren Darstellung hier aus Geheimschutzgründen unterbleibt.

26.4 Regelanfrage zur Verfassungstreue

Eine **Regelanfrage** von Verwaltungsbehörden beim Bundesamt für Verfassungsschutz zur Prüfung der Verfassungstreue ist grundsätzlich problematisch. Die Hoheitsverwaltung erhält dadurch nachrichtendienstliche Vorfelderkenntnisse über sensible Sachverhalte, ohne daß dies zur Klärung vorhandener Anhaltspunkte veranlaßt wäre. Die Entscheidung hierüber kann nur der Gesetzgeber treffen. Er hat dies im Bundesverfassungsschutzgesetz nur für Sicherheitsüberprüfungen zugelassen.

Bei der Kontrolle der Zusammenarbeit des Bundesverwaltungsamtes mit den Sicherheitsbehörden habe ich festgestellt, daß das BVA in Einbürgerungsver-

fahren eine Regelanfrage an das BfV richtet, um die Verfassungstreue des Ausländers zu prüfen. Mangels Rechtsgrundlage ist diese Routinebeteiligung unzulässig.

Ein sachlicher Bedarf für die Ausweitung der Mitwirkungsaufgabe des BfV ist zudem nicht erkennbar:

- Meine Nachfrage bei den Landesbeauftragten für den Datenschutz hat nur zwei Länder mit Regelanfrage ergeben. Die Länder sind für die Einbürgerung von Ausländern mit Aufenthalt in Deutschland zuständig, dem BVA verbleiben Auslandsfälle. Bei Auslandsfällen ist es aber noch unwahrscheinlicher, daß Verfassungsschutzbehörden – als Inlandsnachrichtendienste – überhaupt Informationen zur Verfassungstreue des Ausländers besitzen.
- Das BVA konnte mir keinen Fall nennen, in dem die Regelanfrage des BVA zu einem „Treffer" geführt hätte. Es war sogar auszuschließen, daß jedenfalls in den vergangenen sieben Jahren ein solcher Fall aufgetreten ist. Demnach sprechen auch Gründe der Verwaltungsvereinfachung dafür, Gebote des Datenschutzes hier aufzugreifen und offensichtlich überflüssige Verwaltungsroutinen auf das wirklich erforderliche Maß „zurückzustutzen".

Das BMI hat mir mitgeteilt, daß Regelanfragen in Einbürgerungsangelegenheiten weiterhin für erforderlich gehalten werden und keine Kriterien zur Eingrenzung solcher Anfragen gefunden werden konnten.

Ich halte an meiner Rechtsauffassung fest, daß die routinemäßige Beteiligung von Verfassungsschutzbehörden in Verwaltungsverfahren eine gesetzliche Regelung voraussetzt.

26.5 Arbeitspläne der Abteilungen des BfV Neues Gesetz – alte Praxis

Die „Arbeitspläne" (früher: „Verkartungspläne") der einzelnen Abteilungen des BfV enthalten Bestimmungen über die Verwendung personenbezogener Daten. Insbesondere wird festgelegt, welche Personenkreise für die speziellen Aufgaben der jeweiligen Abteilung zu erfassen sind und nach welchen Fristen dies zu überprüfen ist. Diese Regelungen sind von besonderer Bedeutung für die Beachtung des Persönlichkeitsrechts Betroffener. Ich setze mich nachdrücklich für angemessene Lösungen ein.

Zwischenzeitlich sind grundlegende Änderungen in der Sach- und Rechtslage eingetreten, die in den Arbeitsplänen umgesetzt werden müssen. So mußte die Auflösung der Nachrichtendienste der ehemaligen DDR Konsequenzen für Speicherungen im Bereich der Spionageabwehr haben. Das BfV hat hierzu sachgerechte Regelungen im Arbeitsplan der Abteilung IV eingeführt. Die von der Abteilung IV gespeicherten Daten mit DDR-Bezug sind zu zwei Drittel gelöscht worden. Bei noch verbliebenen Speicherungen handelt es sich bei ca. 80 v. H. um eindeutig identifizierte offizielle und inoffizielle Mitarbeiter des ehemaligen MfS.

Auch Änderungen des neuen Bundesverfassungsschutzgesetzes (13. TB, S. 72) haben Auswirkungen auf die Arbeitspläne. Auf meine Anregung hat der Deutsche Bundestag sich dieser Frage angenommen, worauf das BMI die Überarbeitung der Arbeitspläne bis zum 30. Juni 1993 zugesagt hatte (14. TB, Anlage 1, Beschluß 1 a). Zu einem Verfahrensabschluß ist es im Berichtszeitraum jedoch nicht gekommen.

Das BMI hat mir für alle Abteilungen des BfV Entwürfe zur Neufassung der Arbeitspläne zugeleitet, zu denen ich Verbesserungen empfohlen habe. Im Rahmen von Kontrollen hatte ich mich schon intensiv mit den Regelungen zu den Bereichen Extremismus (Abteilungen II und III) und Sicherheitsüberprüfung (Abteilung IV) befaßt. Nunmehr habe ich mich mit dem Arbeitsplan der Abteilung V – sicherheitsgefährdende und extremistische Bestrebungen von Ausländern – beschäftigt. Zu diesem Arbeitsplan besteht besonderer Überarbeitungsbedarf, da er in wesentlichen Regelungen hinter dem ansonsten vom BfV selbst anerkannten Datenschutzniveau zurückbleibt, ohne daß dies durch spezielle Besonderheiten der Informationssammlung zu Ausländern gerechtfertigt ist.

Die Erörterung war dabei durch die Grundposition des BMI erschwert, das neue BVerfSchG weise eine so hohe Regelungsdichte auf, daß daneben kein Regelungsbedarf zu konkretisierenden Verwaltungsvorschriften mehr bestehe. Angesichts der weithin generalklauselhaften Befugnisregelungen des BVerfSchG bin ich diesem Ansatz entgegengetreten. Mit der Pflicht zu Dateianordnungen (§ 14 BVerfSchG) hat der Gesetzgeber die Notwendigkeit ergänzender Festlegungen eindeutig klargestellt. Die Dateianordnungen haben keinen Selbstzweck, sondern sollen die Verfahrenspraxis steuern. Tatsächlich liegen die Dateianordnungen den Sachbearbeitern des BfV aber nicht vor. Deren Arbeitsgrundlage sind vielmehr die – im Regelungsgegenstand sich mit Dateianordnungen überschneidenden – Arbeitspläne. Bei dieser Praxis entspricht es dem gesetzgeberischen Willen, mit den Arbeitsplänen die in § 14 BVerfSchG vorgeschriebene Regelungsklarheit zu schaffen. Ein Beispiel:

In ihrem Gesetzentwurf für ein BVerfSchG erläutert die Bundesregierung die Regelung zu den Prüffristen (jetzt: § 12 Abs.3 BVerfSchG) folgendermaßen: *„Die Fristen für die nach Absatz 3 vorzunehmenden Prüfungen sind in der Dateianordnung (§ 10 Abs. 1 Satz 1 Nr. 6* [Anm.: § 14 Abs. 1 Satz 1 Nr. 6 der in Kraft getretenen Fassung)] *differenziert nach Art der Dateien und der Daten festzulegen"* (Begründung zu § 9 des Entwurfs, BT-Drs. 11/4306, Seite 62). Zur Ermessensausübung bei der Bestimmung solcher Prüffristen habe ich konkrete Vorschläge unterbreitet, die jedoch mit dem Hinweis abgelehnt worden sind, es bestehe kein Regelungsbedarf. Diese Auffassung sehe ich mit der dargestellten Rechtslage nicht in Einklang.

Vor der Frage der Datenpflege kommt den Festlegungen über den betroffenen Personenkreis (vgl. § 14 Abs. 1 Satz 1 Nr. 3 BVerfSchG) grundlegende Bedeutung zu. Angemessene Bestimmungen gerade zu

Randbereichen des zulässigen Blickfeldes waren mir besonders wichtig. Entsprechend der gesetzlichen Differenzierung in § 4 Abs. 1 BVerfSchG zähle ich dazu Personen, die nicht in einem extremistischen Personenzusammenschluß handeln, sondern dessen Bestrebung nur von außen unterstützen (§ 4 Abs. 1 Satz 2 BVerfSchG) oder überhaupt nur als Einzelperson von Interesse sind (§ 4 Abs. 1 Satz 4 BVerfSchG).

Wann ein Personenzusammenschluß verfassungsschutzrelevant ist, definiert § 4 Abs. 1 Satz 1 BVerfSchG, der auf die Ziel- und Zweckrichtung abstellt. Organisationen, deren Ziele nicht gegen Schutzgüter des BVerfSchG gerichtet sind, sind deshalb nach meinem Verständnis auch dann keine extremistischen Personenzusammenschlüsse, wenn sie von Extremisten zur Diffamierung der Verfassungswirklichkeit instrumentalisiert werden. Im Unterschied zu extremistischen Kern- oder Nebenorganisationen sehe ich die in der Terminologie der Verfassungsschutzberichte als „beeinflußte Organisationen" bezeichneten Personenzusammenschlüsse grundsätzlich nicht als extremistische Organisationen i. S. des § 4 Abs. 1 Satz 1 BVerfSchG an. In beeinflußten Organisationen betätigen sich auch Personen, die den verfassungswidrigen Einfluß sogar zurückdrängen wollen. Eine Betätigung „in" der beeinflußten Organisation rechtfertigt keine gezielte Informationssammlung zum Betroffenen. Das gezielte Interesse des BfV darf nur den Personen gelten, die den extremistischen Einfluß – „für" die beeinflussende Organisation (§ 4 Abs. 1 Satz 2 BVerfSchG) – maßgeblich ausüben. Erst ein eigener extremistischer Hintergrund des Betroffenen rechtfertigt es also, einen gezielten Informationszugriff durch personenbezogenen Aktennachweis zu ermöglichen. Der Deutsche Bundestag hat das sogar bei besonders aktiven Mitgliedern beeinflußter Organisationen gefordert, nämlich bei Rednern auf überregionalen, linksextremistischen Veranstaltungen (BT-Drs. 12/1384, S. 3, Beschlußempfehlung Nr. 5).

Im übrigen dürfen Personen, die auch nach Auffassung des BMI nicht „in", sondern allenfalls „für" einen Personenzusammenschluß tätig werden, als Zielpersonen gem. § 4 Abs. 1 Satz 2 BVerfSchG nur bei einer „nachdrücklichen" Unterstützung der Bestrebung erfaßt werden. Kontakte, bei denen keine Anhaltspunkte für eine solche nachdrückliche Förderung bestehen, rechtfertigen deshalb m. E. ebenfalls keine Erfassung in NADIS-PZD.

Nach Redaktionsschluß dieses Tätigkeitsberichtes hat das BMI mir einen überarbeiteten Arbeitsplanentwurf zugeleitet, der im einzelnen noch genauer Analyse bedarf.

26.6 NADIS

Das Nachrichtendienstliche Informationssystem – NADIS – wird gemeinsam von den Verfassungsschutzbehörden des Bundes und der Länder betrieben. Die Regelungen für dieses Informationssystem, die für alle Anwender gelten, sind in den NADIS-Richtlinien zusammengefaßt. Im Juni 1993 erhielt ich Kenntnis, daß diese Richtlinien von den Verfassungsschutzbehörden überarbeitet werden. Hierzu habe ich in einer Stellungnahme gegenüber dem BMI meine Bedenken dargelegt. Das BMI ist auf diese Anregungen allerdings nicht eingegangen, was ich sehr bedauere.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mit diesem Entwurf befaßt und hierzu die in der Anlage 15 abgedruckte Entschließung verabschiedet. Die neuen NADIS-Richtlinien sind am 6. Mai 1994 in Kraft gesetzt worden.

Insbesondere habe ich bemängelt, daß in der NADIS-Personenzentraldatei mehr personenbezogene Daten gespeichert werden, als zum Auffinden der Akten erforderlich ist:

Rund zweieinhalb Jahre nach Inkrafttreten des novellierten Bundesverfassungsschutzgesetzes übersandte mir das Bundesministerium des Innern den Entwurf einer zwischen dem BfV und den Landesbehörden für Verfassungsschutz abgestimmten Dateianordnung für die „Personenzentraldatei" (PZD).

In NADIS-PZD sind Personengrunddaten, Aktenzeichen sowie einige Zusatzinformationen enthalten. Diese können von den Verfassungsschutzbehörden direkt abgerufen werden; gleichzeitig wird für die Verbundteilnehmer ersichtlich, ob und welche andere Verfassungsschutzbehörde noch über weitere Informationen zu einer bestimmten Person verfügt. Das Bundesverfassungsschutzgesetz schreibt den Umfang der in NADIS-PZD zu erfassenden Daten in § 6 Satz 2 ausdrücklich vor. Danach darf diese Datei nur die Daten enthalten, die zum Auffinden von Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Nach meiner Auffassung muß der bestehende Datenkatalog von NADIS-PZD auf das erforderliche Maß reduziert werden. Die bestehende Datei enthält nämlich personenbezogene Daten, die nicht zum Auffinden von Aktenunterlagen oder der hierzu erforderlichen notwendigen Identifizierung einer Person geeignet sind. Dies habe ich neben einigen weiteren Anmerkungen zu der Dateianordnung dem Bundesministerium des Innern mitgeteilt. Das Bundesministerium des Innern vertritt u. a. auch bei dieser Dateianordnung die Auffassung, weitere Änderungen seien nicht erforderlich. Auf meine nochmalige Stellungnahme vom Juni 1994, in der ich meinen Standpunkt verdeutlicht habe, teilte mir das Bundesministerium des Innern wiederum mit, daß sich die in NADIS-PZD erfaßten personenbezogenen Daten im Rahmen der Vorschrift des § 6 Satz 2 BVerfSchG bewegten und somit eine Änderung des Entwurfs der Dateianordnung nicht erforderlich erscheine. Dieser Auffassung werde ich auch weiterhin entschieden widersprechen.

Die Landesbeauftragten für den Datenschutz teilen meine Bedenken gegen den Umfang des Datenkatalogs bei NADIS-PZD.

26.7 Neufassung der Koordinierungsrichtlinie ohne meine Beteiligung

Neben den NADIS-Richtlinien (vgl. Nr. 26.6) gibt es eine Vielzahl von dienstinternen Vorschriften der

Verfassungsschutzbehörden. Etliche davon werden derzeit noch in Anpassung an die geänderte Gesetzeslage überarbeitet. Eine der zentralen Vorschriften ist die „Richtlinie für die Zusammenarbeit des Bundesamtes für Verfassungsschutz und der Landesbehörden für Verfassungsschutz" (Koordinierungsrichtlinie). Sie regelt Art und Verfahren der Zusammenarbeit der Verfassungsschutzbehörden bei der Erfüllung ihrer gesetzlichen Aufgaben. Das Bundesministerium des Innern hatte mir mit Schreiben vom 17. März 1994 auf meine Bitte um Übersendung der Neufassung der Koordinierungsrichtlinie mitgeteilt, daß ich nach Inkrafttreten der Neufassung einen Abdruck erhalten werde. Dies geschah mit Schreiben vom 4. Juli 1994. Aus dem Begleitschreiben geht hervor, daß die Koordinierungsrichtlinie von der Ständigen Konferenz der Innenminister und -senatoren der Länder bereits am 26. November 1993 beschlossen wurde. Das Bundesministerium des Innern hat die Richtlinie für seinen Geschäftsbereich mit Wirkung ab 23. Juni 1994 in Kraft gesetzt. Aufgrund der verspäteten Übersendung war mir jegliche Möglichkeit genommen, rechtzeitig auf datenschutzrechtlich notwendige Änderungen hinzuwirken. Unabhängig davon habe ich im Juli 1994 gegenüber dem Bundesministerium des Innern zu einigen Punkten Änderungen angeregt, die aus meiner Sicht rechtlich geboten sind. Aus Gründen des Geheimschutzes kann an dieser Stelle nicht über Einzelheiten berichtet werden. Jedenfalls sah sich das Bundesministerium des Innern laut Schreiben vom 5. August 1994 nicht veranlaßt, den einen oder anderen meiner Änderungsvorschläge aufzugreifen. Mir wurde lediglich mitgeteilt, die verabschiedete Fassung der Richtlinie sei das Ergebnis eines umfänglichen, schwierigen Abstimmungsprozesses mit den Ländern. Änderungen der Richtlinie würden erneute Gespräche erfordern, was aus Sicht des Ministeriums vermieden werden sollte.

Im Interesse eines Ausgleichs zwischen den Aufgaben des Verfassungsschutzes und der Rechte des einzelnen halte ich das o. b. Verfahren für unbefriedigend. Die Übersendung der Neufassung der Koordinierungsrichtlinie erfolgte erst auf meine ausdrückliche Bitte und zu einem Zeitpunkt, in dem die Richtlinie bereits verabschiedet war. Ich sehe durch diese Verfahrensweise meine gesetzlich festgelegte Beratungsfunktion nach § 26 Abs. 3 BDSG nur als sehr schwierig bis nicht erfüllbar an.

26.8 Textkommunikationssystem ELKOM

Das Textkommunikationssystem ELKOM ist ein elektronisches Übertragungssystem zur Weitergabe von Nachrichten zwischen den Verfassungsschutzbehörden des Bundes und der Länder; es ist nicht mit NADIS verbunden. ELKOM soll nach seiner Zielsetzung eine schnelle, sichere und wirtschaftliche Erstellung und Übermittlung von schriftlichen Kurznachrichten und Schreiben ermöglichen. Hierbei kann es sich um Berichte, Formblattmeldungen o. ä. handeln. ELKOM ist nach Auffassung des Bundesministeriums des Innern keine Datei im Sinne § 3 Abs. 2 Nr. 1 BDSG, da es lediglich der Kommunikation diene. Die dateibestimmenden Merkmale des § 3 Abs. 2 BDSG lägen nicht vor. Aus diesem Grunde seien weder eine Dateianordnung gemäß § 14 Abs. 1 BVerfSchG noch ein Dateistatut nach § 18 Abs. 2 Satz 2 BDSG erforderlich. Die zu übermittelnden Informationen befänden sich nur für den Zeitraum der Kommunikation im Netz; sowohl beim Versender als auch beim Empfänger würden sie für Rückfragen bzw. nicht besetzter Empfangsstellen wenige Tage in einem „elektronischen Postkorb" abgelegt und anschließend automatisch gelöscht.

Nach einem Informationsbesuch im Bundesamt für Verfassungsschutz bin ich in meiner Auffassung bestärkt worden, daß es sich bei diesem Verfahren um eine Datei im Sinne des § 3 Abs. 2 Nr. 1 BDSG handelt. Auf die vorhandenen „Postkörbe", in denen übermittelte Informationen beim Empfänger abgelegt werden, können die berechtigten Teilnehmer zugreifen. Diese „Postkörbe" sind personenbezogen, zumindestens aber personenbeziehbar, natürlichen Personen zugeordnet. Bezüglich der Auswertbarkeit der gesammelten Informationen habe ich festgestellt, daß der berechtigte Teilnehmer dieses Systems nach Belieben aus der Menge der vorhandenen Eingänge auf die Nachrichten zugreifen kann, von denen er Kenntnis nehmen möchte. Darüber hinaus haben bestimmte Personen, die im Bereich der Datenverarbeitung tätig sind, die Möglichkeit, Recherchen durchzuführen. Aufgrund dieser Gegebenheiten habe ich das Bundesministerium des Innern aufgefordert, mir eine Dateianordnung für ELKOM zu übersenden. Das BMI beharrt bisher auf seiner gegenteiligen Auffassung.

26.9 Registratur- und Schriftgutverwaltungssystem des Bundesamtes für Verfassungsschutz – REGA –

Die Datei REGA (siehe auch Nr. 26), wird von der Zentralabteilung des Bundesamtes für Verfassungsschutz automatisiert betrieben. In dieser Datei werden diejenigen personenbezogenen Daten gespeichert, die üblicherweise für das Auffinden von Aktenvorgängen durch Registraturen notwendig sind. Darüber hinaus bietet sie die Möglichkeit von Recherchen. Es entstand jedoch ein Meinungsstreit zwischen dem Bundesministerium des Innern bzw. dem Bundesamt für Verfassungsschutz und mir darüber, ob für diese Datei eine Dateianordnung nach § 14 BVerfSchG zu erstellen ist. Das Bundesamt für Verfassungsschutz vertrat die Auffassung, es handele sich bei REGA um eine reine Verwaltungsdatei, die nicht der Aufgabenerfüllung nach § 3 BVerfSchG dient. Somit bedürfe es keiner Dateianordnung. Hingegen vertrat ich die Meinung, daß für diese Datei eine Dateianordnung zu erstellen ist, da in ihr u. a. die Vorgänge über Auskunftsersuchen Betroffener nachgewiesen werden. Die Erteilung von Auskünften über gespeicherte personenbezogene Daten an Betroffene ist eine Aufgabe, die dem Bundesamt für Verfassungsschutz als speichernde Stelle nach § 15 Abs. 1 BVerfSchG zugewiesen ist. Sie beruht auch auf dem gesetzlichen Auftrag des BfV (§ 3 BVerfSchG). Würde die Auffassung des Bundesamtes für Verfassungsschutz zutreffen, wären die Vorschriften des Bundesdatenschutzgesetzes anzuwenden, und das Bundesamt für Verfassungsschutz wäre ver-

pflichtet, ein Dateistatut nach § 18 Abs. 2 Satz 2 BDSG zu erstellen. Nach weiterem Schriftwechsel hat mir das Bundesministerium des Innern nunmehr ein Dateistatut für das „Registratur- und Schriftgutverwaltungssystem des Bundesamtes für Verfassungsschutz" übersandt.

26.10 Auszüge aus dem Bundeszentralregister

Bei Anfragen an das Bundeszentralregister wird vom Bundesamt für Verfassungsschutz zwischen zwei Anfragezwecken unterschieden. Diese laufen entweder unter der Rubrik „Sicherheitsaufgaben nach § 3 Abs. 1 Bundesverfassungsschutzgesetz" oder „Sicherheitsüberprüfungen". Nach Auffassung des Bundesamtes für Verfassungsschutz genügt diese Unterscheidung, insbesondere im Hinblick auf die Regelung des Bundeszentralregistergesetzes über die Einholung und Verwendung von unbeschränkten Auskünften, um den Besonderheiten hinsichtlich der Verwendung der übermittelten Informationen Rechnung zu tragen. Eine weitere Eingrenzung auf die einzelnen Tätigkeitsbereiche des Bundesamtes für Verfassungsschutz, wie z. B. Rechtsextremismus, Linksextremismus etc. sei nicht veranlaßt. Nach § 41 Abs. 4 Satz 2 BZRG ist bei derartigen Angaben der Zweck anzugeben, für den die Auskunft benötigt wird; sie darf nur für diesen Zweck verwendet werden. Ich habe das Bundesamt für Verfassungsschutz auf die Bestimmungen der Zweiten Allgemeinen Verwaltungsvorschrift zur Durchführung des Bundeszentralregistergesetzes hingewiesen. Danach ist der Zweck der Auskunft möglichst genau anzugeben; allgemeine Angaben wie „Verwaltungsangelegenheit" genügen nicht. Das Bundesamt für Verfassungsschutz vertritt hierzu die Auffassung, daß die zuvor beschriebene Unterscheidung der Anfragezwecke angesichts der Besonderheiten des Sicherheitsüberprüfungsverfahrens ausreiche, bei denen die Verwendung der Daten besonderen Einschränkungen unterliegt. Die von mir vorgeschlagene weitere Differenzierung bei der Zweckangabe in Auskunftsersuchen sei weder rechtlich erforderlich noch sinnvoll.

Anläßlich der Erörterung der Arbeitspläne des BfV (vgl. Nr. 26.5) ist die Frage aufgetreten, inwieweit die Regelungen des Bundeszentralregistergesetzes über das Verwertungsverbot von Eintragungen (§§ 51, 52) auch vom BfV zu beachten sind. BMJ und BMI vertreten hierzu die Auffassung, daß bei Übermittlungen zwischen den Verfassungsschutzbehörden die Voraussetzungen des § 51 Abs. 1 BZRG in der Regel nicht vorliegen dürften.

Diese Auffassung steht m. E. nicht im Einklang mit der Intention des § 51 BZRG, der einen Anspruch des Betroffenen auf „Resozialisierung" zum Zweck hat. Deshalb ist bereits die Übermittlung und nicht erst die Verwendung von Informationen durch den Empfänger als Verwertung zum Nachteil des Betroffenen i. S. von § 51 Abs. 1 BZRG anzusehen. Dies trifft insbesondere auch bei Übermittlungen zwischen den Verfassungsschutzbehörden zu. Etwas anderes kann nur in den Fällen des § 52 Abs. 1 Nr. 1 BZRG gelten.

Das Bundesamt für Verfassungsschutz hat im übrigen meine Anregung aufgegriffen, BZR-Auskünfte zu vernichten, die für die Aufgabenerfüllung des Bundesamtes für Verfassungsschutz keine relevanten Eintragungen enthalten. Dies gilt auch für später eingeholte weitere Auskünfte.

26.11 Fortschritte in der Auskunftspraxis

Dank der Unterstützung des Deutschen Bundestages (s. 14. TB, S. 144 f. i.V. Anlage 1, S. 163 ff.) konnte die Auskunftspraxis des BfV bürgerfreundlicher gestaltet werden. Zwar sind nicht alle meine Anregungen übernommen worden, gleichwohl konnte das BfV in einigen wichtigen Punkten von einer datenschutzfreundlicheren Praxis überzeugt werden. Das BfV erteilt nunmehr Auskunft nach folgenden Maßgaben:

- Jede konkrete Sachverhaltsangabe erfüllt die Anspruchsvoraussetzung des § 15 Abs. 1 BVerfSchG. Entgegen früherer Praxis wird dem Antragsteller also keine Selbstbezichtigung verfassungsfeindlichen Handelns abverlangt. Die Angaben dürfen nur zur Antragsbearbeitung verwendet werden. Dazu werden auch organisatorische Vorkehrungen zur Sicherung dieser Zweckbindung getroffen.
- Jedes glaubhaft dargelegte Auskunftsinteresse, das in irgendeiner Weise über das allgemein bestehende Interesse an einer Auskunft hinausgeht, wird als „besonderes Interesse" (§ 15 Abs. 1 BVerfSchG) anerkannt.
- Auch wenn ein Anspruch auf Auskunft nicht besteht, weil die vorbezeichneten Voraussetzungen nicht erfüllt sind, kann Auskunft erteilt werden, soweit kein Auskunftsverbot nach § 15 Abs. 2 BVerfSchG besteht. Dies ist immer der Fall, wenn der vom Antragsteller – ohne besonderes Auskunftsinteresse – dargelegte Sachverhalt kein Tätigwerden des BfV auslösen konnte oder bei erkennbar irrationalen Verfolgungsängsten oder wenn wegen hohen Alters des Antragstellers Belange der Aufgabenerfüllung des BfV nicht berührt sind.

Ich begrüße diese Entwicklung und empfehle darüber hinaus:

- Es sollte in dem zuletzt genannten Bereich nicht vom Grundsatz der Auskunftsablehnung ausgegangen werden. Im Gegenteil: Im Hinblick auf das Persönlichkeitsrecht muß meines Erachtens die Auskunftserteilung der Grundsatz sein, der nur bei überwiegendem Allgemeininteresse zurücktritt. Ausnahmekategorien wären nicht zur Auskunftserteilung, sondern zur Auskunftsablehnung zu bilden. Als Ausnahmegründe kommen dabei nur Umstände in Betracht, die auf einen Tatbestand hindeuten, wonach die Auskunft verboten wäre.

  Es geht nicht an, die Auskunftserteilung gewissermaßen als rechtsfreien Gnadenakt zu verstehen. Meines Erachtens ist das BfV rechtlich gehalten, bei der Abwägung das Persönlichkeitsrecht des Betroffenen angemessen zu berücksichtigen; der Betroffene hat auf eine solche pflichtgemäße Ermessensausübung einen Anspruch.

Eine sachgerechte Ermessensausübung ist deshalb von besonderer Bedeutung, weil der Auskunftsanspruch sich nur auf den vom Antragsteller dargelegten Sachverhalt bezieht.

- Auch zur Auslegung der gesetzlichen Auskunftsverbote bestehen noch unterschiedliche Auffassungen:

  Bei unbeteiligten Personen, bei „bekennenden", nicht konspirativ tätigen Extremisten oder bei bereits bekannt gewordenem Tätigwerden des BfV wird durch eine Auskunftserteilung die Aufgabenerfüllung des BfV regelmäßig nicht gefährdet werden.

  Belange der Strafrechtspflege sind nicht vom BfV durch Auskunftsverweigerung zu wahren. Die Entscheidung kann hier nur die – im übrigen auch sachnähere – Staatsanwaltschaft durch Sperrerklärung treffen (entsprechend § 5 Abs. 2 StUG).

- Der Betroffene hat zwar keinen Anspruch, daß ihm Datenherkunft und Empfänger benannt werden, doch ist dies auch nicht unzulässig. Hier muß zur Wahrung der Rechte des Betroffenen pflichtgemäßes Ermessen ausgeübt werden.

- Zur Begründungspflicht bei Auskunftsablehnung ist eine richtungsweisende Entscheidung des Bundesverwaltungsgerichts ergangen, wonach für die Verweigerung einer Aktenvorlage an das Gericht ein pauschaler Hinweis etwa auf Quellenschutz oder sonstige Aufgabengefährdung grundsätzlich nicht genügt. Das oberste deutsche Verwaltungsgericht hat dabei erkennen lassen, daß dieser Maßstab auch bei Direktauskunft an den Betroffenen gilt. Das BfV will dies in seiner Verfahrenspraxis jedoch nicht berücksichtigen. Dies ist umso unverständlicher, weil dadurch Verwaltungsprozesse geradezu provoziert werden: von der Verweigerung der Aktenvorlage gegenüber dem Gericht erhält der Kläger nämlich eine Ablichtung, einschließlich der Begründung.

- Ein besonderes Problem besteht für Angaben von Landesverfassungsschutzbehörden im gemeinsamen „Nachrichtendienstlichen Informationssystem". Hier sieht § 6 Abs. 2 BDSG vor, daß das BfV einen Auskunftsantrag an das jeweilige Landesamt zur Beantwortung weiterleiten und darüber dem Betroffenen oder mir Abgabenachricht erteilen muß. Dazu ist das BfV bislang jedoch noch nicht bereit.

Ich hoffe, auch in den noch offenen Punkten zu Fortschritten zu kommen. Wichtig wäre dies zumal bei einem Interesse, die Rechtmäßigkeit der Speicherung zu klären:

- Stellt das BfV bei der Bearbeitung eines Auskunftsantrags fest, daß Daten zum Betroffenen unzulässig gespeichert sind, hält es sich für berechtigt, die Daten zu löschen und dem Betroffenen dann mitzuteilen, es seien keine Informationen vorhanden.

  Das BVerfSchG sieht jedoch ausdrücklich vor, daß die Löschung unterbleibt, wenn Grund zu der Annahme besteht, daß schutzwürdige Interessen des Betroffenen beeinträchtigt würden; die Daten sind dann zu sperren (§ 12 Abs. 2 Sätze 2 bis 4). M.E. sind diese Voraussetzungen bei anhängigem Auskunftsantrag regelmäßig gegeben. Der Betroffene will ja erst einmal erfahren, welche Informationen über ihn gesammelt worden sind. Diese Auskunft kann für seine Rehabilitierung – auch bei anderen Stellen – wichtig sein.

- In Fällen, in denen das BfV Daten wegen schutzwürdiger Interessen des Betroffenen nicht löscht, sondern nur sperrt, habe ich angeregt, den Betroffenen davon grundsätzlich zu unterrichten. Wenn es um seine Interessen geht, sollte er selbst entscheiden, ob die Daten nicht doch zu löschen sind. Eine Ausnahme halte ich nur für sachgerecht, soweit der Anhörung des Betroffenen ein Auskunftsverweigerungsgrund entgegensteht. Das BfV vertritt dementgegen die Auffassung, Auskunft sei nach § 15 BVerfSchG nur auf Antrag zu erteilen, der in diesen Fällen nicht vorliege. Das ändert jedoch nichts an der Pflicht des BfV, von Amts wegen zu ermitteln, ob der Sachverhalt eine Ausnahme von der Löschung rechtfertigt. Da hierfür die Belange des Betroffenen entscheidend sind, muß eine pflichtgemäße Prüfung ihm grundsätzlich Gelegenheit geben, sich dazu zu äußern. Das setzt eine Unterrichtung über den maßgeblichen Sachverhalt voraus. Im übrigen ist die Sperrungsregelung als Beweissicherungsinstrument auch Ausfluß der Rechtsschutzgarantie des Artikel 19 Abs. 4 GG. Wegen der grundsätzlichen Unzulässigkeit der Speicherung bedarf es hier angesichts der geheimen Informationssammlung einer Mitteilung an den Betroffenen, um seine Rechtschutzmöglichkeit effektiv zu gewährleisten.

Zur bisherigen Entwicklung folgende Zahlen:

Jahr	Anträge	Antragsgemäße Auskunft (zum angegebenen Sachverhalt)	Teilablehnung	Gesamtablehnung	
				wegen Auskunftsverbot	Ermessensbereich
1991	82	39	2	1	40
1992	147	83	5	1	58
1993	77	42	3	9	23
1994	72	53	2	5	12

26.12 Fernmeldegeheimnis sichern

Das Fernmeldegeheimnis in Artikel 10 GG, ein Grundrecht von hohem Rang, muß entsprechend seinem Schutzzweck und entgegen anderen Tendenzen wieder gestärkt werden. Die erst nach 1968 eingeführte strafprozessuale Telefonüberwachung ist seither mehrfach ausgedehnt worden: Der Straftatenkatalog, der das Abhören eröffnet, umfaßt mittlerweile an die 100 Strafvorschriften. Die gewissermaßen nachrichtendienstlichen Abhörbefugnisse des Zollkriminalamtes (14. TB S. 139), die anlaßbezogen und deshalb befristet eingeräumt worden waren, sind verlängert worden (s. Nr. 35 32.), ohne die Entschei-

dung des Bundesverfassungsgerichts im dazu anhängigen Verfahren abzuwarten. Auch haben die Nachrichtendienste immer mehr Befugnisse erhalten, zuletzt durch das Verbrechensbekämpfungsgesetz, das neben einer Erweiterung der BND-Befugnisse (Nr. 28.2) auch den Verfassungsschutzbehörden zusätzliche Rechte eingeräumt hat:

Die bisherige Regelung in § 2 des Gesetzes zu Artikel 10 GG (G 10) bezog sich u. a. auf terroristische Vereinigungen. Sie ist nun auf andere kriminelle Vereinigungen mit politischer Zielsetzung ausgeweitet worden. Ich hatte mich dagegen ausgesprochen, weil hier die Strafverfolgungsbehörden aufgrund der Deliktsstruktur des § 129 StGB Überwachungsbefugnisse bereits im Vorfeld der von der Organisation begangenen Straftaten besitzen. Eine nochmalige Absenkung der Eingriffsschwelle – gewissermaßen ins „Vorfeld des Vorfeldes" – halte ich wegen der breiten Einbeziehung von tatsächlich unbeteiligten Personen nur im besonders gefährlichen Terrorismusbereich für angemessen.

Bedenken habe ich auch dagegen, zur Unterstützung der Sicherheitsbehörden eine zentrale Erfassungsstelle für Teilnehmer am öffentlichen Fernmeldeverkehr einzurichten. Vorstellungen für einen solchen Rufnummernpool mit zentraler Speicherung sämtlicher Telefonteilnehmer sind im Entwurfsverfahren für ein Verbrechensbekämpfungsgesetz diskutiert, vom Bundestag meiner Empfehlung folgend jedoch nicht aufgegriffen worden. Innerhalb der Bundesregierung wird eine Zentralstelle aber weiterhin gefordert. Aus einer Reihe fachlicher Erwägungen rate ich davon ab, nicht zuletzt, weil die zentrale Erfassung – anerkanntermaßen – sehr leicht zu umgehen wäre und damit gerade im Hinblick auf Bereiche organisierter Kriminalität im wesentlichen nutzlos bliebe. Da für diese Forderung nach einer zentralen Erfassung aller Rufnummern keine Besonderheiten im Rahmen der Telefonüberwachung geltend gemacht wurden, würde ein fatales rechtspolitisches Signal gesetzt. Die vorgebrachten Gründe könnten beispielsweise ebenso für eine vorratsmäßige Zentralerfassung sämtlicher Girokonten herangeführt werden sowie für eine Vielzahl weiterer Zentralstellen. Meines Erachtens liegt hier eine grundlegende Fehlgewichtung in der Abwägung von Persönlichkeitsschutz und Sicherheitsinteressen vor.

Ich werde mich weiterhin mit Augenmaß für die Sicherung des Fernmeldegeheimnisses einsetzen. Hierzu gehört auch das Verständnis für berechtigte Anliegen der Sicherheitsbehörden. So habe ich im Rahmen der Poststrukturreform eine Klarstellung zur Zweckbindungsdurchbrechung bei Rufnummern- und Teilnehmerauskünften an Strafverfolgungsbehörden mitgetragen. Damit wird auch geregelt, daß die Auskunftspflichten gegenüber den Strafverfolgungsbehörden insoweit keinen besonderen Einschränkungen unterliegen. Das ist sachgerecht, weil insoweit keine Besonderheiten für Einschränkungen sprechen.

Umgekehrt bestehen aber auch keine Besonderheiten zur Ausweitung strafprozessualer Pflichten in bezug auf diese Daten. Es widerspräche wesentlichen Grundentscheidungen des Strafverfahrensrechts, hier etwa Zeugenpflichten nicht nur gegenüber Richter und Staatsanwalt, sondern auch gegenüber deren Hilfsbeamten oder sogar im Vorfeld des für ein rechtsstaatliches Strafverfahren konstitutiven Anfangsverdachts zu begründen.

Anders liegt es bei der nachrichtendienstlichen Telefonüberwachung. Im Unterschied zum Strafverfahren sind Private hier bislang nicht zur Telefon- oder Inhaberauskunft verpflichtet. Es begegnete keinen Bedenken, diese Lücke der Auskunftspflicht zu schließen, um zulässige Überwachungsmaßnahmen zu ermöglichen. Zwar können Nachrichtendienste nach dem verfassungsrechtlichen Trennungsgebot nicht selbst Privatpersonen hoheitlich – zur Auskunft – verpflichten. Die Anordnungsbefugnis im ohnehin durchzuführenden Verfahren nach dem G-10 könnte jedoch entsprechend erweitert werden.

Auch zu anderen anstehenden Fragen, wie der Standortüberwachung von Mobilfunkteilnehmern, sind ausgewogene Positionen zu beziehen. Bestehende datenschutzrechtliche Defizite, die bei etwaigen Befugnisausweitungen noch zusätzliches Gewicht erhielten, müssen endlich bereinigt werden. Dazu gehört insbesondere die Gewährleistung einer effektiven Kontrolle durch Öffentlichkeit und Datenschutzbeauftragte (siehe Nr. 28.2). Erwägenswert scheint auch das Modell, Überwachungsmaßnahmen durch Höchstquoten zu kontingentieren und damit einer ausufernden Praxis wirksam vorzubeugen.

26.13 Probleme in der Zusammenarbeit

Seit vielen Jahren ist es gute Übung, daß an mich gerichtete Petenteneingaben, die mögliche Speicherungen beim Bundesamt für Verfassungsschutz betreffen, im schriftlichen Verfahren erledigt werden. In der Praxis sieht das so aus, daß ich das Bundesamt für Verfassungsschutz unter Mitteilung des Sachvortrages des Bürgers um Prüfung ersuche, ob und gegebenenfalls welche Informationen über den Petenten dort gespeichert sind. Anhand der Stellungnahme des Bundesamtes für Verfassungsschutz, die mir über das Bundesministerium des Innern zugeht, konnte ich aufgrund meiner Erfahrungen aus Kontrollen die Zulässigkeit einer Datenverarbeitung beurteilen. Bei besonders schwierig gelagerten Einzelfällen habe ich außerdem beim Bundesamt für Verfassungsschutz vorhandene Akten eingesehen. Anläßlich der Eingabe eines Petenten mußte ich nun feststellen, daß das Bundesamt für Verfassungsschutz dem Betroffenen unmittelbar geantwortet hatte und mir lediglich eine Abschrift dieses Schreibens zukommen ließ. Dies geschah auch in anderen Fällen, ohne daß das Bundesministerium des Innern oder das Bundesamt für Verfassungsschutz mich von dieser, von der bisherigen Praxis abweichenden Übung unterrichtet hätten.

Dem Bundesamt für Verfassungsschutz habe ich daraufhin mitgeteilt, daß ich mit dieser neuen Verfahrensweise nicht einverstanden bin, da sich die Betroffenen gemäß § 21 des Bundesdatenschutzgesetzes an mich gewandt haben. Der Gesetzgeber habe mir die Verpflichtung auferlegt, für den Betroffenen eine

Kontrolle durchzuführen, wenn dieser der Ansicht ist, er sei bei der Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten durch öffentliche Stellen des Bundes in seinen Rechten verletzt worden. Der Betroffene habe somit auch einen Anspruch, von mir über das Ergebnis der datenschutzrechtlichen Kontrolle bei der speichernden Stelle unterrichtet zu werden. Meine Kontrollbefugnis bei Petenteneingaben könne im übrigen nicht durch eine unmittelbare Auskunftserteilung des Bundesamtes für Verfassungsschutz ersetzt werden. Der Betroffene würde sonst in seinem Verlangen nach Rechtsschutz beeinträchtigt. Im übrigen liege es in der freien Entscheidung des Bürgers, sich an die Stelle zu wenden, die er mit der Verfolgung seiner Interessen betrauen möchte. Diese Stelle sei auch im Falle ihrer Zuständigkeit verpflichtet, den Betroffenen zu bescheiden.

Nach etwa 5 Monaten erhielt ich eine Antwort des Bundesamtes für Verfassungsschutz auf mein Schreiben. Es teilte mir mit, daß ihm an einer peinlich genauen Beachtung der Rechte des Bürgers gelegen sei. Man müsse unterscheiden zwischen Auskunftsersuchen nach § 15 Abs. 1 BVerfSchG und solchen Eingaben, die der Betroffene nach § 21 BDSG an mich richtet. Das Bundesamt für Verfassungsschutz vertrat die Auffassung, daß es selbst für die Beantwortung von Auskunftsersuchen nach § 15 Abs. 1 BVerfSchG als speichernde Stelle zuständig sei. Der Gesetzgeber habe damit dem Betroffenen ausdrücklich die Möglichkeit eingeräumt, eine bloße Auskunft über möglicherweise gespeicherte personenbezogene Daten unmittelbar von der speichernden Stelle zu erhalten. Diese Auskunftserteilung könne und solle daher nicht meine Kontrollbefugnis nach § 24 Abs. 1 BDSG ersetzen. Andererseits bleibe aber auch die Zuständigkeit des Bundesamtes für die Erteilung von Auskünften nach § 15 Abs. 1 BVerfSchG von meinen Rechten und Pflichten aus §§ 21, 24 Bundesdatenschutzgesetz unberührt. Schließlich müsse das Bundesamt für Verfassungsschutz Inhalt und Umfang einer Auskunft in einem etwaigen Verwaltungsstreitverfahren vertreten. Nur das Bundesamt für Verfassungsschutz könne dem Betroffenen insofern einen rechtsmittelfähigen Bescheid erteilen. Im übrigen war das Bundesamt für Verfassungsschutz bereit, die zwischenzeitlich zurückgehaltenen Stellungnahmen zu Petenteneingaben nunmehr gemäß dem bisher gehandhabten Verfahren an mich weiterzuleiten.

Nach meiner Auffassung muß verfahrensmäßig sichergestellt sein, daß der Bürger entsprechend den Vorgaben des Bundesverfassungsgerichts und den gesetzlichen Bestimmungen eine möglichst umfassende Auskunft über gegebenenfalls zu seiner Person gespeicherte personenbezogene Daten erhält. Grundsätzlich teile ich die Meinung, daß zwischen Auskunftsersuchen nach § 15 Abs. 1 BVerfSchG und Eingaben nach § 21 des BDSG zu unterscheiden ist. Aus meiner Sicht bestehen keine Bedenken, den Petenten, sofern er sich lediglich mit einem Auskunftsersuchen an mich wendet, darauf hinzuweisen, daß für dessen Beantwortung zunächst das Bundesamt für Verfassungsschutz als speichernde Stelle zuständig ist. Dieser Mitteilung werde ich neben einer Aufklärung über die Rechtslage einen Hinweis anfügen, daß sich der Betroffene bei Schwierigkeiten mit der Durchsetzung seines Auskunftsanspruchs an mich wenden kann. Alle übrigen Eingaben sehe ich als solche nach § 21 Bundesdatenschutzgesetz an, wenn ein weitergehendes Interesse des Bürgers an der Überprüfung einer Datenspeicherung erkennbar ist.

Ich gehe nunmehr davon aus, daß auf dieser Basis eine zügige und umfassende Auskunftserteilung an die Betroffenen gewährleistet ist.

27 Militärischer Abschirmdienst – MAD –

Der MAD befindet sich in Umorganisation. In diesem Zusammenhang stehen die innerdienstlichen Vorschriften weitgehend zur Überarbeitung an. Ich werde darauf hinwirken, daß bei der Umsetzung der gesetzlichen Vorgaben des MAD-Gesetzes – MADG – (BGBl. 1990 I, S. 2977) den Belangen des Persönlichkeitsrechts angemessen Rechnung getragen wird (siehe auch unten Nr. 27.2). Vordringlich erscheint mir, daß der MAD nun endlich die ausstehenden Dateianordnungen erläßt. Die gesetzliche Pflicht dazu nach § 8 MADG gilt seit über 4 Jahren und ist in der Sache auch nicht neu, da bereits § 15 BDSG a. F. zum Erlaß von Dateistatuten verpflichtet hatte. Es ist unverständlich und nicht akzeptabel, daß gerade zur Personenzentraldatei des MAD noch keine Festlegungen durch Dateianordnung getroffen sind.

27.1 Auskunft

Für die Auskunft des MAD an Betroffene hat der Gesetzgeber mit § 9 MADG auf die Auskunftsregelung des Bundesverfassungsschutzgesetzes verwiesen. Die Darstellung unter Nr. 26.11 gilt daher entsprechend für den MAD. Zu den Zahlen:

Jahr	Anträge	Antragsgemäße Auskunft (zum angegebenen Sachverhalt)	Teilablehnung	Gesamtablehnung	
				wegen Auskunftsverbot	Ermessensbereich
1991	41	22	4	./.	15
1992	52	33	./.	2	17
1993	33	31	./.	./.	2
1994	31	29	1	./.	1

27.2 Dienstvorschrift zu nachrichtendienstlichen Mitteln

Bereits 1980 hatte ein Untersuchungsausschuß des Deutschen Bundestages zu „Abhöraktionen amtlicher Dienststellen des Bundes" (BT-Drs. 8/3835) gefordert, diese tief in Persönlichkeitsrechte eingreifenden Maßnahmen durch verantwortliche Vorgaben an angemessenen Grundsätzen auszurichten. Die Grundsatzweisung des MAD zu nachrichtendienstlichen Mitteln (§ 4 Abs. 1 Satz 3 MADG) läßt gleichwohl wesentliche Fragen offen. Über Einzelheiten dieser Dienstvorschrift kann ich hier aus Gründen

des Geheimschutzes nicht berichten. Ich halte jedoch insbesondere folgende Vorkehrungen für geboten:

Nach § 5 MADG i.V. m. § 9 Abs. 3 BVerfSchG sind von Erhebungen, „die in ihrer Art und Schwere einer Beschränkung des Brief-, Post- und Fernmeldegeheimnisses gleichkommen", die Parlamentarische Kontrollkommission und nachträglich der Betroffene zu unterrichten. Diese – den Ausschluß rechtlichen Gehörs ausgleichenden – Vorkehrungen sind im Gesetz keineswegs auf Maßnahmen beschränkt, die mit technischen Mitteln durchgeführt werden und verbale Äußerungen zum Gegenstand haben. Auch lang andauernde Observationen oder die heimliche Informationsbeschaffung unter Ausnutzung besonderer Vertrauensverhältnisse greifen intensiv in schutzwürdige Interessen des Betroffenen ein. Daneben sind für Maßnahmen, die die im Gesetz bezeichneten Voraussetzungen erfüllen, Ausnahmen von der nachträglichen Mitteilung an den Betroffenen nicht vorgesehen. Der Gesetzgeber hat erst jüngst durch das Verbrechensbekämpfungsgesetz mit der Streichung der Ausnahmebestimmung in der entsprechenden Mitteilungsvorschrift des G 10 (bisheriger § 5 Abs. 5 Satz 3) die Bedeutung der Mitteilung an den Betroffenen betont. Die Praxis darf darüber nicht hinweggehen.

28 Bundesnachrichtendienst – BND –

28.1 Aufgaben des BND

Im Berichtszeitraum wurde zum Teil heftig diskutiert, ob der BND mithelfen soll, den internationalen Drogenhandel und damit im Zusammenhang stehende Geldwäsche aufzuklären (s. auch Nr. 28.2). Hierbei hat es auch undifferenzierte Pauschalkritik gegeben.

Der BND hat die Aufgabe, Auslandsvorgänge aufzuklären, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind (§ 1 Abs. 2 BNDG). Seit jeher ist anerkannt, daß dies nicht innerstaatlichen Zwecken dient, sondern das Aufklärungsziel außenpolitischer Natur sein muß (Dienstanweisung für den BND, BT-Drs. 7/3246, S. 47 und 50). Der Bundesgesetzgeber hat das BNDG auf seine Kompetenz zur Regelung der auswärtigen Angelegenheit nach Artikel 73 Nr. 1 GG gestützt (BT-Drs. 11/4306, S. 70). Auch in den parlamentarischen Ausschußberatungen ist die Tätigkeit des BND auf die Interessen der auswärtigen Politik bezogen worden (BT-Drs. 11/7235, S. 110). Aufgabe des BND ist also nicht, der Verbrechensbekämpfung im Inland zu dienen, sondern der Bundesregierung zur Unterstützung ihrer **Außenpolitik** die erforderlichen Informationen zu verschaffen. Dabei kann es beispielsweise von Bedeutung für die Außenpolitik der Bundesregierung sein zu erfahren, ob und inwieweit Entwicklungen in einem Staat, zu dem Deutschland Beziehungen unterhält, durch organisierte Kriminalität beeinflußt sind.

Wesentliche Datenschutzprobleme ergeben sich m. E. erst, wenn die Vorgänge nicht nur außenpolitisch, sondern zugleich auch innenpolitisch für die Verbrechensbekämpfung bedeutsam sind (man denke beispielsweise an Verbindungen auswärtiger Drogenkartelle nach Deutschland). Ein Interesse daran, die vorhandenen Informationen nicht nur für den eigentlichen Zweck der Aufgaben des BND zu verwenden, sondern auch für andere staatliche Aufgaben zu nutzen, liegt auf der Hand. Andererseits wird auch die Gefahr deutlich, daß nachrichtendienstliche und polizeiliche Befugnisse im Wege der Zusammenarbeit dieser Stellen faktisch zusammengeführt werden. Dies widerspräche dem **Trennungsgebot** nach Artikel 87 Abs. 1 Satz 2 GG (Auffassung von Bundesregierung – vgl. BT-Drs. 1/924, S. 4 – und Bundesrat – vgl. Niederschrift der 684. Sitzung des Rechtsausschusses vom 30. Mai 1994, S. 11), das sicherstellen soll, daß die Koppelung geheimdienstlicher Informationsmacht und polizeilicher Exekutivbefugnisse verhindert wird, um die Freiheitssphäre rechtstreuer Bürger nicht unverhältnismäßig zu beeinträchtigen. Verdeckte Ermittlungen für polizeiliche Aufgaben von der Einsatzschwelle eines konkreten Anfangsverdachtes zu lösen und – nach nachrichtendienstlicher Art – schon im Vorfeld zur Verdachtsgewinnung durchzuführen, würde im Ergebnis die Gefahr unverhältnismäßig ausweiten, daß tatsächlich Unschuldige mit strafrechtlichen Ermittlungen überzogen werden.

Eine faktische Aushöhlung des – auch speziell im BNDG mit § 1 Abs. 1 Satz 2 und § 2 Abs. 3 aufgegriffenen – Trennungsgebots hat der Gesetzgeber in der Aufgabenbestimmung des § 1 Abs. 2 BNDG verhindert. Zur Aufklärung von Vorgängen, die nicht lediglich von außen-, sondern zugleich **von sicherheitspolitischer Bedeutung** sind, ist der BND nur dann zuständig, wenn der Vorgang sicherheitspolitische Bedeutung **für die Bundesrepublik Deutschland** hat, d. h. für ihre Sicherheit oder ihren Bestand **als Ganzes** eine ernsthafte Gefahr darstellen kann (so m. E. zutreffend die Bundesregierung: BT-Drs. 12/7520, S. 3 i.V. m. 12/6938 S. 23). Ob eine solche Gefahr anzunehmen ist, ist eine hochpolitische Frage, die der Beurteilung der Bundesregierung und der Kontrolle der Parlamentarischen Kontrollkommission und des G-10-Gremiums unterliegt. Die Bundesregierung ist der Auffassung, daß die internationale Drogenkriminalität und die damit zusammenhängende Geldwäsche eine solche Bedrohungsintensität für Deutschland erreicht hat.

In jedem Fall stehen dem BND seine **Erhebungs- und Auswertungsbefugnisse auch bei solcher Gemengelage nur zur Erfüllung seiner** – auf die Außenpolitik zielenden – **Aufgaben** zu. Polizeiliche Interessen dürfen diese Befugnisausübung nicht steuern. Insbesondere ist es nicht Aufgabe des BND, Sachverhalte unter strafrechtlichen Gesichtspunkten zu prüfen. Soweit ein Straftatverdacht auch ohne gesonderte Prüfung offenbar wird, sollte der nachrichtendienstlichen Qualität des Erhebungseingriffs im übrigen auch bei der zweckändernden Weitergabe Rechnung getragen werden. Ich sehe es dazu als geboten an, zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen einen Filter zu setzen, der die abgesenkte Erhebungsschwelle jedenfalls durch eine angehobene **Übermittlungsschwelle** kompensiert: Der BND sollte der Polizei personenbezogene Daten hier nur bei einer

angemessenen Verdachtsverdichtung übermitteln (s. auch Anlage 12).

Im Berichtszeitraum habe ich eine **Datei** des BND **kontrolliert**, die ich wegen der vorstehenden Problematik ausgewählt hatte. Die Erkenntnisse haben mich darin bestärkt, zu den angesprochenen Punkten der Nutzung und Übermittlung klare Festlegungen in der Dateianordnung zu fordern (zu Dateianordnungen sowie dem Anknüpfungszeitpunkt für Wiedervorlagefrist und Speicherungsdauer siehe Nr. 28.3). Auch weitere Fragen sind aus diesem Anlaß noch mit Bundeskanzleramt und BND zu erörtern. Ich habe jedoch nicht den Eindruck gewonnen, daß die insoweit zur Tätigkeit des BND verschiedentlich geübte Grundsatzkritik im gegenwärtigen Verfahrensstand berechtigt ist. Die Antwort auf meinen Kontrollbericht steht noch aus.

28.2 Fernmeldeaufklärung des BND – mit dem Kescher im Äther

Im Frühjahr 1993 erklärte der BND öffentlich, satellitengestützte Fernmeldeverkehre zur Aufklärung des internationalen Waffen- und Drogenhandels zu überwachen, indem die über Satelliten weitergeleiteten Informationen erfaßt und ausgewertet würden. Die Erfassung ist dabei nicht auf einzelne „verdächtige" Fernmeldeverkehre beschränkt, sondern erstreckt sich auf sämtliche, die über die betreffende Bodenstation zu empfangen sind. Die inhaltliche Kommunikationsauswertung erfolgt in mehreren Stufen. Als erste Stufe wird technisch ein Rasterabgleich mit einer „Wortbank" durchgeführt, in die „Suchworte" zu den Bereichen Proliferation/Rauschgift eingegeben sind. Die hierbei vorausgewählten Fernmeldeverkehre werden dann in einer zweiten Stufe von BND-Mitarbeitern auf ihre konkrete Relevanz überprüft.

Die Bundesregierung hat mitgeteilt (BT-Drs. 12/5759), die Maßnahmen zielten auf Fernmeldeverkehre mit beiden Endpunkten im Ausland, Vorkehrungen gegen die Erfassung von Verkehren mit Inlandsteilnehmern seien getroffen, allerdings würden vereinzelt auch solche Fernmeldeverkehre erfaßt. Sobald dies erkannt sei, würden die angefallenen Unterlagen vernichtet.

Ich bin der Angelegenheit in Gesprächen mit dem Bundeskanzleramt und dem BND nachgegangen und habe den BND anschließend kontrolliert. Diese Fernmeldeaufklärung ist im Hinblick auf den Schutz des Fernmeldegeheimnisses durch Art. 10 Grundgesetz, Art. 8 Europäische Menschenrechtskonvention und Art. 17 des Internationalen Pakts über bürgerliche und politische Rechte rechtlich bedenklich. Von einer abschließenden rechtlichen Würdigung habe ich abgesehen, weil mit dem Verbrechensbekämpfungsgesetz eine gesetzliche Grundlage für diese Fernmeldeaufklärung geschaffen wurde.

Mit dem **Verbrechensbekämpfungsgesetz** (BGBl. 1994 I, S. 3186) wurde das Gesetz zu Art. 10 GG (G 10) geändert und die Befugnis der Fernmeldeaufklärung des BND erweitert. Die getroffenen Regelungen habe ich unter verschiedenen Gesichtspunkten kritisiert, nicht jedoch grundsätzlich abgelehnt.

Die frühzeitige Einbringung datenschutzrechtlicher Erwägungen war dadurch erschwert, daß das Bundesministerium des Innern mich entgegen üblicher Praxis an den Entwurfsvorarbeiten der Bundesregierung nicht beteiligt, sondern mir erst den letzten Entwurf – als Verschlußsache – zugeleitet hatte. Um so nachdrücklicher habe ich dann freilich meine Beratungsaufgabe gegenüber dem Deutschen Bundestag wahrgenommen, insbesondere als Sachverständiger in der öffentlichen Anhörung durch Rechts- und Innenausschuß am 11. April 1994 (s. Anlage 16). Meine schriftliche Stellungnahme wurde im Protokoll Nr. 120 des Rechtsausschusses ab S. 83 abgedruckt.

So fragt es sich, ob die **Verhältnismäßigkeit** bei Freiheitseinbußen dieses Umfangs gewahrt bleibt angesichts des zweifelhaften Nutzens der Überwachungsmaßnahmen. Nachrichten im Fernmeldeverkehr lassen sich mit billigen, frei erwerblichen und leicht einzusetzenden Verfahren so effektiv verschlüsseln, daß auch der BND sie faktisch nicht dechiffrieren kann. Daß ausgerechnet kriminelle Organisationen – trotz ausgebildeter Kommunikationsstruktur und -logistik – auf solche naheliegenden Schutzmechanismen verzichten, halte ich für eher unwahrscheinlich. Wenn keine aussagekräftigen Lageanalysen zu Bereichen organisierter Kriminalität erstellt werden können, sind die Eingriffe in das Fernmeldegeheimnis ungeeignet, jedenfalls aber unverhältnismäßig. Die Erkenntnisse aus der Kontrolle einer einschlägigen Bereichsdatei (siehe Nr. 28.1) haben meine Vorbehalte bestärkt. Ich gehe davon aus, daß die Bundesregierung – wie angekündigt – im Laufe der Legislaturperiode die Regelungen des Verbrechensbekämpfungsgesetzes überprüft und sich dabei auch der Frage stellt, welche Erfolge die Fernmeldeaufklärung tatsächlich hat (siehe auch Anlage 9).

Unter dem Vorbehalt dieser allgemeinen Skepsis habe ich konkrete Verbesserungsvorschläge unterbreitet, insbesondere zur effektiven Trennung von Polizei und Nachrichtendienst und für eine wirksame Kontrolle durch Öffentlichkeit und Datenschutzbeauftragte.

Wichtig war mir, daß die zusätzlichen Befugnisse **nur im Rahmen der bestehenden Aufgaben** des BND ausgeübt werden dürfen, also nur für außenpolitische, nicht für polizeiliche Interessen. Dies ergibt sich aus der allgemeinen Bestimmung des § 1 Abs. 1 Satz 1 Nr. 2 G 10. Besser wäre es allerdings, wenn dies direkt in der Befugnisregelung des § 3 G 10 klargestellt wäre und ausdrücklich auch die Auswertung umfaßte. Die Auswertungsbestimmung des § 3 Abs. 4 G 10, die allein die Anordnungszwecke in Bezug nimmt, ist jedoch vor dem Hintergrund der Entstehungsgeschichte in diesem Sinne auszulegen, zumal Zustimmungsverweigerung des Bundesrates und Vermittlungsvorschlag mit ihrer Kritik am ursprünglich vorgesehenen § 3 a G 10 (Unterstützung anderer Bedarfsträger) zentral auf die Aufgabenbindung der Befugnisausübung zielten. Die Vorschrift zur Übermittlung von Erkenntnissen zu bestimmten Straftaten (§ 3 Abs. 5 G 10) setzt also voraus, daß der BND solche Tatbestände gelegentlich der Auswertung für eigene Aufgaben feststellt, und macht ihn nicht etwa zum verlängerten Arm anderer Sicher-

heitsbehörden. Eine gezielte Auswertung für Zwekke der Empfänger wird damit nicht zugelassen. Im übrigen steht die mißverständliche Regelung einer „vollständigen" Übermittlung der erhobenen Daten unter dem ausdrücklichen Vorbehalt der Erforderlichkeit und besagt damit lediglich, daß Zufallsfunde nicht wegen Interessen des BND zurückgehalten werden dürfen.

Ergänzend hatte ich empfohlen, eine angemessene **Übermittlungsschwelle** (siehe Nr. 28.1) im Gesetz ausdrücklich vorzusehen und durch den Entscheidungsvorbehalt einer unabhängigen Institution (Strafrichter oder G-10-Kommission) zu sichern. Diese Empfehlung ist leider nicht aufgegriffen worden. Aber auch ohne spezielle Gesetzesregelung ist die Übermittlungsschwelle jedenfalls dem rechtsstaatlichen **Trennungsgebot** zu entnehmen: Erkenntnisse aus Maßnahmen, die unter Beschränkung spezieller Freiheitsgrundrechte gewonnen werden, aber nicht an einen Verdacht anknüpfen, sondern vedächtige Anhaltspunkte überhaupt erst finden sollen, können danach Polizeibehörden nicht ohne Ausgleichsvorkehrungen zum Schutze Unbeteiligter zugeleitet werden.

Erfolgreich war allerdings meine Forderung nach einer **öffentlichen Berichtspflicht** (§ 3 Abs. 10 G 10 n. F.), wenn mir auch die Beschränkung auf Maßnahmen nach § 3 G 10 (also insbesondere nicht zu Überwachungsmaßnahmen der Verfassungsschutzbehörden) zu eng erscheint. Der Bericht sollte aussagekräftige Angaben zur Beurteilung der Eingriffsdimension und der hieraus resultierenden Erfolge enthalten, um Freiheitseinbußen gegen Gemeinnutzen abwägen und Entwicklungstendenzen erkennen zu können:

- Zur Eingriffsseite könnten z. B. Zahlenangaben erfolgen zu: Anordnungsanträgen und -entscheidungen, erfaßten Fernmeldeverkehren vor und nach der Wortbank, Übermittlungen personenbezogener Daten, unterbliebenen Mitteilungen.
- Zur Erfolgsseite könnten die außenpolitischen Entscheidungen der Bundesregierung aufgelistet werden, die auf diesen Erkenntnissen beruhen.

Eine effektive **Datenschutzkontrolle** sehe ich nicht gewährleistet, obwohl die Verfassungsrechtsprechung zum G 10 die grundlegende Bedeutung einer unabhängigen Kontrolle durch Datenschutzbeauftragte ausdrücklich betont (BVerfGE 67, 157/185). Das Bundesdatenschutzgesetz schließt meine Kontrolle für den Zuständigkeitsbereich der G-10-Kommission aus (§ 24 Abs. 2 Satz 4 Nr. 1 BDSG). Diese Bestimmung ist leider nicht gestrichen worden, wie ich es vorschlug. Ich hatte empfohlen, daß ich aktiv im Benehmen mit der G-10-Kommission in diesem empfindlichen Bereich kontrollieren kann. In § 3 Abs. 9 G 10 ist jetzt lediglich vorgesehen, daß die Kommission mich vor ihrer Entscheidung über die Zulässigkeit und Notwendigkeit einer Maßnahme anhören „kann". Das ist rein deklaratorisch, denn solche Unterstützungsersuchen „kann" die Kommission ohnehin für ihren gesamten Zuständigkeitsbereich schon nach § 24 Abs. 2 Satz 4 Nr. 1 BDSG an mich richten. Von dieser Möglichkeit hat sie freilich bislang noch kein einziges Mal Gebrauch gemacht; auch nicht in einem Fall, in dem der Betroffene sich mit der ausdrücklichen Bitte an sie gewandt hatte, mich einzuschalten. Es wäre daher sachgerecht und notwendig, zusätzlich zur Kommission eine unabhängige Datenschutzkontrolle vorzusehen. Denn auch sonst unterliegt Verwaltungshandeln richterlicher Kontrolle, ohne daß dies meine Zuständigkeit beseitigt. Und selbstverständlich ist unbestritten, daß die Existenz der Parlamentarischen Kontrollkommission mich nicht von der Kontrolle der Nachrichtendienste ausschließt. Ich setze daher auf eine vernünftige Revision der Kontrollbeschränkung und sehe mich darin – wie auch in den übrigen angesprochenen Fragen – von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt (Anlage 12).

28.3 Innerdienstliche Vorschriften – Handlungsbedarf beim Datenschutz

Innerdienstliche Durchführungsvorschriften zur Konkretisierung der allgemein gehaltenen Bestimmungen des BND-Gesetzes sind wichtig, um die Umsetzung der gesetzlichen Vorgaben in der Alltagspraxis zu gewährleisten. Sie geben den Bediensteten zu schwierigen Fragen zugleich Entscheidungshilfen.

Insbesondere zur **Datenübermittlung** hat der BND ausführliche Regelungen geschaffen. Diese sind im wesentlichen ausgewogen, wenn auch weitere Verbesserungen wünschenswert wären:

- Bei der internationalen Zusammenarbeit ist mir besonders wichtig, einen vom Gesetz nicht gedeckten Informationshandel mit Partnerdiensten eindeutig auszuschließen. Bei der Anwendung des § 9 Abs. 2 BNDG i.V. m. § 19 Abs. 3 BVerfSchG ist für die Frage, ob die Übermittlung zur Erfüllung von Aufgaben des BND erforderlich ist, auf die damit bezweckte Verwendung beim Empfänger abzustellen. Ein lediglich mittelbarer Aufgabenbezug genügt nicht. Dies gilt auch, wenn die Informationen zur Verwendung beim Empfänger für dessen Aufgaben übermittelt werden, um im Gegenzug vom Empfänger Informationen zu erhalten, die für eigene Aufgaben benötigt werden.
- Bei der innerstaatlichen Zusammenarbeit kommt der Übermittlung an Polizeibehörden insoweit besondere Bedeutung zu, als es nicht im eigentlichen Sinne um Zufallsfunde geht, wenn bereits der Beobachtungsauftrag des BND sich mit einem polizeilichen Informationsbedürfnis überschneidet (siehe Nr. 28.1).

Zu Vorschriften über **nachrichtendienstliche Mittel** gelten meine Ausführungen zum MAD (siehe Nr. 27.3) entsprechend. Speziell zum BND sind im übrigen Fragen zu den Grenzen seiner Amtshilfe für andere Stellen aufgetreten, die noch weiterer Erörterung bedürfen.

Zur **Speicherung** bestehen vor allem Meinungsunterschiede zum **Anknüpfungszeitpunkt für die Überprüfungsfristen und die Speicherungsdauer** (vgl. ergänzend auch Nr. 26.5). § 5 Abs. 1 BNDG verweist dazu auf § 12 Abs. 3 BVerfSchG. Der Gesetzgeber

hatte dabei die Praxis des Bundesamtes für Verfassungsschutz vor Augen, die bei Sicherheitsbehörden allgemein üblich ist (Nr. 5.5 der Richtlinie für die Führung kriminalpolizeilicher personenbezogener Sammlungen, GMBl. 1981, S. 120): Maßgeblich ist das Datum des letzten relevanten Ereignisses, nicht erst das Datum seines Bekanntwerdens oder seiner Speicherung. Je länger zu dem Vorgang keine neuen Ereignisse mehr auftreten, desto mehr spricht dafür, daß die Angelegenheit insgesamt nicht mehr von Belang ist. Hierzu vertrete ich im übrigen die Auffassung, daß auch § 12 Abs. 3 Satz 2 BVerfSchG mit der grundsätzlichen **Höchstspeicherdauer** von 10 Jahren (d. h.: Löschung, wenn in den vergangenen 10 Jahren sich nichts mehr ereignet hat und außergewöhnliche Umstände auch keine Ausnahme gebieten) durch die Bezugnahme in § 5 Abs. 1 BNDG für den BND entsprechend gilt. Nur soweit bereits § 12 Abs. 3 Satz 2 BVerfSchG keine Höchstspeicherdauer bestimmt, nämlich für staatliche Vorgänge, gilt sie auch nicht für den BND. Dagegen ist es beispielsweise zum Terrorismusbereich (§ 3 Abs. 1 Satz 2 Nr. 2 G 10 n. F.) nicht hinzunehmen, daß – trotz der klaren Bezugnahme des BNDG auf das BVerfSchG – die für das BfV geltende Höchstspeicherdauer nicht ebenso vom BND beachtet wird.

Bedauerlich ist schließlich, daß trotz der nunmehr über vierjährigen Geltung des Gesetzes entgegen § 6 BNDG immer noch keine einzige **Dateianordnung** ergangen ist (siehe auch Nr. 27). Lediglich Entwürfe liegen zu einzelnen Dateien vor. Das Bundeskanzleramt hat mein Drängen aufgegriffen und dem BND aufgegeben, die ausstehenden Entwürfe bis Mitte 1995 vorzulegen. Speziell im Hinblick auf Dateien, die überhaupt erst nach Inkrafttreten des BNDG errichtet worden sind, läuft eine Inbetriebnahme ohne wenigstens vorläufige Genehmigung eines vorgelegten Entwurfs eindeutig dem gesetzlichen Zustimmungsvorbehalt des Bundeskanzleramtes sowie der Pflicht zuwider, mich zuvor anzuhören. Ich halte eine solche Praxis, die vorbeugende Verfahrensvorkehrungen des Gesetzes glatt übergeht, für grundsätzlich unzulässig.

28.4 Auskunft

Für die Auskunft seitens des BND an Betroffene hat der Gesetzgeber mit § 7 BNDG auf die Auskunftsregelung des Bundesverfassungsschutzgesetzes verwiesen. Die Darstellung unter Nr. 26.11 gilt daher entsprechend für den BND. Zu den Zahlen:

Jahr	Anträge	Antragsgemäße Auskunft (zum angegebenen Sachverhalt)	Teilablehnung	Gesamtablehnung	
				wegen Auskunftsverbot	Ermessensbereich
1992	33	28	1	./.	4
1993	13	8	./.	./.	5
1994	13	5	./.	./.	8

29 Sicherheitsüberprüfung

Geheimschutz bei Verschlußsachen (Nr. 29.1) und Sabotageschutz bei sicherheitsempfindlichen Stellen von lebens- oder verteidigungswichtigen Einrichtungen (s. Nr. 29.2) erfolgt vornehmlich durch materielle Vorkehrungen, die gewährleisten, daß nur Berechtigte Zugang erhalten. Das verbleibende Risiko unsorgfältigen oder mißbräuchlichen Umgangs durch Zugangsberechtigte soll durch Zuverlässigkeitsüberprüfung der Betroffenen minimiert werden. Solche Verfahren werden als „Sicherheitsüberprüfung" bezeichnet (§ 3 Abs. 2 Satz 1 Nrn. 1 und 2 BVerfSchG). Wegen der staatsbezogenen Schutzrichtung ist für diese Personenüberprüfungen die anlaßunabhängige Regelbeteiligung von Polizei- und Verfassungsschutzbehörden kennzeichnend.

Der Sensibilität von Informationen dieser Stellen muß durch bereichsspezifische Regelungen zum Schutz der Betroffenen Rechnung getragen werden. Deren Belange sind besonders gewichtig, weil sie für diese verdachtsunabhängigen Maßnahmen der Gefahrenvorsorge keinen Anlaß geboten haben, in der Regel aber dienst- oder arbeitsrechtlich – also für Drittinteressen – zur Mitwirkung sogar verpflichtet sind.

29.1 Geheimschutz – Gegen oder mit Betroffenen?

In dem Sicherheitsüberprüfungsgesetz vom 20. April 1994 (BGBl. I, S. 867) – SÜG – ist ein im ganzen erfreulicher Datenschutzstandard erreicht worden.

Ich hatte bei den parlamentarischen Beratungen u. a. empfohlen, die den Ehegatten oder Lebenspartner betreffenden Angaben gesondert und direkt bei diesem zu erheben. Es ist m. E. für den Zweck der Sicherheitsüberprüfung nicht erforderlich, daß der Lebenspartner so sensible Angaben wie „nachrichtendienstliche Kontakte" oder „verfassungsfeindliche Beziehungen" im einheitlichen Erklärungsbogen und damit zugleich gegenüber seinem Partner offenbart. Der Gesetzgeber ist meiner Empfehlung zwar nicht gefolgt. Das Bundesministerium des Innern hat aber eine Erprobung der Praktikabilität zugesagt.

Verwaltungsvorschriften zur Ausführung des Sicherheitsüberprüfungsgesetzes hat allgemein das Bundesministerium des Innern (GMBl. 1994, S. 550), für den Geheimschutz in der Wirtschaft das Bundesministerium für Wirtschaft (GMBl. 1994, S. 624) und für seinen Geschäftsbereich das Bundesministerium der Verteidigung (Neufassung der ZDv 2/30) erlassen. An den Entwurfsverfahren war ich intensiv beteiligt. Meine Anregungen sind weitgehend aufgegriffen worden. Diese Ausführungsvorschriften sind im ganzen erfreulich datenschutzgerecht ausgefallen. In einigen verbleibenden Punkten werde ich Nachbesserungsbedarf im Auge behalten:

Bei den allgemeinen Vorschriften des BMI sollte beispielsweise bei der Einschränkung der Anhörung des Betroffenen besser zwischen dem Schutz nachrichtendienstlicher Quellen und den Interessen befragter Personen unterschieden werden. Letztere sind hier nicht schutzwürdiger als Zeugen in anderen

Verfahren der Zuverlässigkeitsüberprüfung. Der Betroffene muß Gelegenheit erhalten, sich zur Glaubwürdigkeit der befragten Personen zu äußern. Ihm muß dazu mitgeteilt werden, wer belastende Angaben gemacht hat. Die Regelung darf nicht zum Freibrief für üble Nachrede werden.

Auch beim Geheimschutz in der Wirtschaft legt § 25 Abs. 2 Satz 1 SÜG den Grundsatz der Trennung von Sicherheitsbevollmächtigtem und Personalverwaltung fest. Das ist für den betroffenen Arbeitnehmer besonders wichtig, weil dadurch das Verbot der Informationsnutzung zu arbeitsrechtlichen Maßnahmen (§ 21 SÜG) organisatorisch gesichert wird. Bei Kleinbetrieben läßt § 25 Abs. 2 Satz 2 SÜG allerdings Ausnahmen vom Trennungsgrundsatz zu. Da dieser Grundsatz jedoch den Schutz des Betroffenen bezweckt, fordere ich, daß ihn die zuständige öffentliche Stelle zumindest anhört, bevor sie seinem Arbeitgeber eine Ausnahme gestattet. Das Bundesministerium für Wirtschaft will nicht entsprechend verfahren.

Das Bundesministerium für Verteidigung sieht in den Regelungen für seinen Geschäftsbereich ausdrücklich einen Mittelweg zwischen Verschlußsachenermächtigung und Ermächtigungsablehnung vor, nämlich die Ermächtigung mit Einschränkungen oder Auflagen. Ich halte es für notwendig, daß dem Betroffenen auch vor einer solchen Entscheidung – ebenso wie vor einer Ablehnung – rechtliches Gehör zu gewähren ist. Bisher lehnt dies das Bundesministerium für Verteidigung ab.

Über die quantitative Entwicklung bei Sicherheitsüberprüfungen zum Geheimschutz gibt künftig der Verfassungsschutzbericht im Anhang zu den Strukturdaten Auskunft. Im Nachrichtendienstlichen Informationssystem der Verfassungsschutzbehörden von Bund und Ländern waren 1993 aufgrund von Sicherheitsüberprüfungen 515 530 Personen erfaßt, überwiegend (ca. 386 000) in der Zuständigkeit des Bundesamtes für Verfassungsschutz.

29.2 Vorbeugender personeller Sabotageschutz

29.2.1 Allgemeine Entwicklung

Die Innenminister von Bund und Ländern haben meine Empfehlungen aus dem 14. TB (auf S. 141 f.) hinsichtlich des Geheimschutzes aufgegriffen und sich mit der Frage auseinandergesetzt, was als „lebens- und verteidigungswichtige Einrichtung" i. S. des § 3 Abs. 2 Satz 1 Nr. 2 BVerfSchG zu verstehen sei. Für mich hat diese Frage – ergänzt um die Festlegung der „sicherheitsempfindlichen Stellen" – grundlegende Bedeutung, weil damit zugleich der von Sicherheitsüberprüfungen betroffene Personenkreis im wesentlichen festgelegt wird. Diese Festlegung darf zum Schutz des Persönlichkeitsrechts nicht außer Verhältnis zu bestehenden Sicherheitsrisiken stehen.

Mit der Bestimmung zum personellen Sabotageschutz wollte der Gesetzgeber Vorsorge treffen gegen Gefahren für die „Sicherheit der Bundesrepublik Deutschland oder das Wohl ihrer Bevölkerung", wie sie „im Verteidigungsfall oder bei schweren innen- und außenpolitischen Krisen" eintreten könnten (BT-Drs. 6/3533, S. 5). Damit wird eine besondere Zurückhaltung bei vorbeugenden Sicherheitsüberprüfungen auferlegt. Ein relevantes Risiko besteht etwa bei solchen Einrichtungen, bei denen – wie z. B. bei Atomkraftwerken (s. Nr. 29.2.2) – bereits der punktuelle Sabotageakt zugleich das Leben zahlreicher Menschen gefährdet.

Eine restriktive Auffassung hatte auch das Bundesministerium des Innern vertreten, sich damit bedauerlicherweise jedoch nicht gegenüber den Ländern durchgesetzt. Hiernach sollen nunmehr Sicherheitsüberprüfungen auch bei Einrichtungen durchgeführt werden, „die für das Funktionieren des Gemeinwesens unverzichtbar sind". Ich befürchte, daß mit dieser unbestimmten Formel ein Tor zu zusätzlichen Sicherheitsüberprüfungen für weite Bereiche der Wirtschaft und des öffentlichen Dienstes aufgestoßen wird.

Um so wichtiger wäre eine restriktive Auslegung des Begriffs der „sicherheitsempfindlichen Stellen" solcher Einrichtungen. Ich werde nachdrücklich darauf hinwirken, dies auf Schlüsselpositionen zu beschränken, von denen aus die Funktionstüchtigkeit der Einrichtung als solcher gefährdet werden kann.

Im übrigen werde ich auf folgende – auch früher bereits betonte (8. TB, Anlage 3) – Grundsätze besonderen Wert legen:

- Überprüfung erst nach präziser und angemessener Festlegung der sicherheitsempfindlichen Bereiche der jeweiligen Einrichtung,
- Zustimmung des Betroffenen als Verfahrensvoraussetzung,
- Beschränkung auf vorhandene Erkenntnisse, also keine Sicherheitsermittlungen,
- strenge Zweckbindung und angemessene organisatorische Vorkehrungen zu deren Gewährleistung (insbesondere darf die Personalverwaltung der Einrichtung nicht mit Aufgaben der Sicherheitsüberprüfung betraut werden),
- eigene Verfahrensrechte des Betroffenen, insbesondere rechtliches Gehör vor ablehnender Entscheidung,
- angemessener Auskunftsanspruch, einschließlich Akteneinsicht.

29.2.2 Überprüfung nach § 12b Atomgesetz

Die bereits 1989 im Atomgesetz getroffene Regelung zur Personenüberprüfung, die wesentliche datenschutzrechtliche Grundsätze aufgreift, hatte ich begrüßt (12. TB S. 77). Der Gesetzgeber hatte in § 12b Abs. 2 AtomG der Bundesregierung aufgegeben, die Einzelheiten durch Rechtsverordnung festzulegen. Darauf habe ich das Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit (BMU) hingewiesen. In den nunmehr über fünf Jahren ist jedoch nichts geschehen. Dies ist deshalb besonders bedauerlich, weil die weiterhin angewendeten Verwaltungsvorschriften bedeutende Strukturmängel aufweisen.

Diese Richtlinien (GMBl. 1987 S. 337 und 1988, S. 330) tragen Sachverhalten unterschiedlicher Risikointensität nicht in angemessen differenzierenden Regelungen Rechnung. Die personellen Schutzvorkehrungen zu Kernkraftwerken können nicht einfach auf Beförderung und Aufbewahrung von Kernbrennstoffen übertragen werden. Dort ist nämlich bereits durch materielle Schutzvorkehrungen dem Sabotagerisiko sehr weitgehend vorgebeugt. Im öffentlichen Bereich werden von Stellen des Bundes deshalb insoweit auch keine Personenüberprüfungen durchgeführt.

Der Vollzug des AtomG liegt überwiegend bei Stellen der Länder. Für bestimmte Bereiche, insbesondere die Genehmigung der Beförderung von Kernbrennstoffen, ist jedoch das Bundesamt für Strahlenschutz zuständig (§ 12 b Abs. 1 Satz 1 i.V.m. § 23 AtomG). Die Überprüfung der Zuverlässigkeit durch diese öffentliche Stelle des Bundes habe ich – mit einem insgesamt erfreulichen Ergebnis – kontrolliert. Dabei habe ich allerdings auch festgestellt, daß sich das Bundesamt für Strahlenschutz – wie übrigens in den geltenden Richtlinien ausdrücklich vorgesehen – Informationen über unbeschränkte Auskünfte aus dem Bundeszentralregister beschaffte. Weil nach dem Bundeszentralregistergesetz solche Auskünfte an das Bundesamt für Strahlenschutz nicht vorgesehen sind, wandte sich das Bundesamt für Strahlenschutz an ein Landesministerium, um das Auskunftsersuchen stellen zu lassen. Dieses Ministerium teilte dann mit, ob im Register Eintragungen enthalten sind. In diesem Falle veranlaßte das Bundesamt für Strahlenschutz das BMU, eine weitere unbeschränkte Auskunft einzuholen, sie zu bewerten und ihm mitzuteilen, ob Sicherheitsbedenken bestehen. Ich habe dringend empfohlen, diese Praxis abzustellen (s. auch Nr. 4.4.2) und konkrete Alternativvorschläge für einzelfallbezogene Ersuchen unterbreitet. Das Bundesamt für Strahlenschutz ist dem gefolgt und hat auch meine übrigen Verbesserungsvorschläge weitgehend und zügig aufgegriffen.

29.3 Ausländische Sicherheitsüberprüfungen

Für ausländische Sicherheitsüberprüfungen sieht § 33 SÜG (s. o. Nr. 29.1.) eine Mitwirkung des Bundesamtes für Verfassungsschutz (BfV) vor. Die Bestimmung gewährleistet für den nationalen Verantwortungsbereich das – im internationalen Vergleich hohe – Datenschutzniveau des SÜG und beschränkt die weitere Verwendung der übermittelten Daten bei der ausländischen Stelle auf Zwecke der Sicherheitsüberprüfung. Außerdem wird dem BfV eine Mitwirkung verboten, wenn überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Nach meinem Verständnis sind die hierbei zu beachtenden Interessen durch die Grundentscheidungen des SÜG vorgegeben:

- Zustimmung des Betroffenen als Verfahrensvoraussetzung,
- organisatorische Maßnahmen zur Gewährleistung der Zweckbindung (Trennung von der Personalverwaltung),
- Gewährung rechtlichen Gehörs (11. TB S. 68),
- angemessenes Auskunftsrecht des Betroffenen.

Ich bin weiter bestrebt, daß dies in Verwaltungsvorschriften festgeschrieben und ergänzend eine Liste derjenigen Staaten und Überprüfungsverfahren erstellt wird, die diesen Voraussetzungen genügen.

Der gute Grund für eine nationale Zentralstelle bei der Mitwirkung liegt in der Filterfunktion. Erkenntnisse werden nur übermittelt, wenn sie fachlich als sicherheitserheblich bewertet worden sind. Ich habe mich davon überzeugt, daß das BfV keineswegs pauschal Auskünfte aus dem Bundeszentralregister weitergibt. Das ist insbesondere dann für den Betroffenen von Vorteil, wenn der Partnerstaat rigidere Vorstellungen zur Sicherheitserheblichkeit hat. Leider ist diese Filterfunktion nicht konsequent eingehalten worden: Im Gesetz zum NATO-Truppenstatut ist ein Artikel 4 b eingefügt worden (BGBl. II 1994 S. 2594), wonach die Entsendestaaten der Stationierungsstreitkräfte für bestimmte Sicherheitsüberprüfungen auch Direktauskunft aus dem Bundeszentralregister erhalten.

Auch Sicherheitsüberprüfungen bei Organen der Europäischen Union haben mich im Berichtszeitraum beschäftigt. Bislang sind solche Überprüfungen nur zur Europäischen Atomgemeinschaft im Hinblick auf Euratom-Verschlußsachen durch Ratsverordnung vorgesehen. Die Kommission wollte 1992 entsprechende Regelungen insbesondere auch im Hinblick auf Tätigkeiten der EWG einführen. Der Verordnungsvorschlag (Ratsdok. 5084/92; BR-Drs. 190/92) sah eine Sicherheitsüberprüfung nach dem jeweiligen nationalen Recht vor, für deutsche Staatsangehörige also nach dem SÜG. Somit wären keine wesentlichen Probleme aufgetreten. Allerdings sollte für die Ermächtigung das Gemeinschaftsorgan zuständig sein, ohne daß klare Regelungen vorgesehen wurden zum Übermittlungsumfang sowie zur Verwendung und zu Verfahrenssicherungen (einschließlich einer unabhängigen Datenschutzkontrolle) beim Organ.

Die Kommission hat ihren Vorschlag 1993 unter Subsidiaritätserwägungen zurückgezogen. Das Europäische Parlament wünscht jedoch weiterhin eine Verordnung. Ich werde die Angelegenheit im Auge behalten.

Für den nicht vergemeinschafteten Bereich der Europäischen Zusammenarbeit (Außen- und Sicherheitspolitik/Innen- und Rechtspolitik) werden entsprechende Überlegungen verfolgt, die allerdings aufgrund unterschiedlicher Vorstellungen der Mitgliedstaaten – etwa zur erforderlichen Rechtsqualität der zu treffenden Regelungen – blockiert scheinen. Nach Redaktionsschluß wurde mir bekannt, daß sich Kommission und Rat über die deutschen Bedenken hinweggesetzt und Regelungen durch Beschluß, nicht durch Verordnung getroffen haben.

29.4 Grundsatz der Erforderlichkeit von Daten muß auch für das Sicherheitsüberprüfungsgesetz gelten

Ein Petent, der im Geschäftsbereich des Bundesministeriums der Verteidigung tätig ist, hatte sich mit

der Bitte an mich gewandt, daß Informationen über ein strafprozessuales Ermittlungsverfahren aus dem Jahre 1987 und ein sich daran anschließendes Disziplinarverfahren aus dem Jahre 1988 aus seiner Sicherheitsüberprüfungsakte entfernt werden. Er selbst hatte bereits beim Amt für den Militärischen Abschirmdienst die Vernichtung dieser Aktenteile beantragt. Dieser Antrag wurde jedoch abgelehnt. Der Betroffene sieht in der Tatsache, daß die Unterlagen bei der Staatsanwaltschaft und der Disziplinarbehörde bereits vernichtet wurden, aber beim Amt für den Militärischen Abschirmdienst als Informationen noch vorhanden sind, eine Verletzung seines Persönlichkeitsrechts.

Ich habe beim MAD-Amt die Sicherheitsüberprüfungsakte des Petenten eingesehen und darauf hingewiesen, daß für die Entfernung dieser Unterlagen aus der Sicherheitsüberprüfungsakte die einschlägigen spezialgesetzlichen Tilgungsregelungen zu beachten seien. Im übrigen habe ich die Auffassung vertreten, daß die Kenntnis dieser Informationen für zukünftige Sicherheitsüberprüfungen nicht mehr erforderlich sei, da sie im Zeitpunkt der letzten Sicherheitsüberprüfung bereits bekannt waren und ohne nachteilige Konsequenzen für den Betroffenen bewertet wurden. Auch nach den Bestimmungen des zwischenzeitlich in Kraft getretenen Sicherheitsüberprüfungsgesetzes ist die Aufbewahrung derartiger Unterlagen nur insoweit erforderlich, als es für eine sicherheitsmäßige Beurteilung erheblich sein kann. Mit dieser Begründung habe ich die Aufbewahrung dieser Informationen in der Sicherheitsüberprüfungsakte des Petenten gegenüber dem Bundesministerium der Verteidigung beanstandet. Das Bundesministerium der Verteidigung hat diese Beanstandung mit der Begründung zurückgewiesen, daß die Sicherheitsüberprüfungsakten als Ganzes aufbewahrt und als Ganzes vernichtet würden. Dies sei bereits deswegen sinnvoll, weil die in diesen Akten enthaltenen Kenntnisse nicht nur für die Sicherheitsüberprüfung selbst, sondern auch für die sonstigen gesetzlichen Aufgaben der mitwirkenden Behörde genutzt werden dürften. Diese Rechtsauffassung stütze sich auf die Regelungen der §§ 19, 22 Abs. 2 Nr. 2 Sicherheitsüberprüfungsgesetz.

Wenngleich der Standpunkt des Bundesministeriums der Verteidigung auch nach der neuen Rechtslage vertretbar erscheint, bin ich doch der Auffassung, daß in die Sicherheitsüberprüfungsakte des Betroffenen nur solche Unterlagen Aufnahme finden dürfen, die sicherheitserheblich sind. Diese Sicherheitserheblichkeit sehe ich auch im Falle einer ohne Bedenken gegen den Betroffenen abgeschlossenen Sicherheitsüberprüfung als nicht mehr gegeben an, was zur Folge haben müßte, daß die entsprechenden Unterlagen aus der Akte herauszunehmen und zu vernichten sind.

Wegen der im vorliegenden Fall deutlich gewordenen Problematik werde ich im Falle einer Änderung des Sicherheitsüberprüfungsgesetzes eine Regelung fordern, die eine teilweise Vernichtung von Vorgängen in Sicherheitsüberprüfungsakten zuläßt, soweit keine Sicherheitsbedenken entstehen.

30 Informationstechnik

30.1 Chipkarten – viel Komfort und viele Probleme

In der heutigen Gesellschaft herrscht ein Informationsfluß wie noch nie zuvor. Dies hat zur Folge, daß die elektronische Form der Information den Vorzug vor der bisher üblichen schriftlichen Form auf Papier bekommt. Auf schnelle Verfügbarkeit und Verarbeitbarkeit der Information kommt es an. Dazu müssen „Medienbrüche", d. h., die Transformation der Information von einem Medium, z. B. Papier, auf ein anderes Medium, z. B. Datenträger, vermieden werden. Dies führte schon in der Vergangenheit zur Einführung der Magnetstreifenkarte, die immerhin etwa 150 Zeichen aufnehmen kann. Sie wurde ein „Riesenerfolg"; jährlich werden derzeit weltweit einige Milliarden Stück hergestellt und ausgegeben, u. a. auch die Eurocheque-Karte (s. Abbildung „Zuwachs bei verschiedenen Chipkarten-Anwendungen"). Was darauf gespeichert ist, kann mit dem Auge schon nicht mehr gelesen werden; nur in einem passenden Kartenterminal ist dies möglich. Mit seiner Hilfe lassen sich die Daten zur Aktualisierung ändern, allerdings auch kopieren. Fälschungen und Manipulationen jeglicher Art sind also möglich. Als Sicherheit gegen Diebstahl und Mißbrauch wurde darum eine zusätzliche Geheimzahl (PIN = Personal Identification Number) eingeführt, die nicht auf der Karte gespeichert ist. Dieser Sicherheitsmechanismus funktioniert in der Praxis leider nicht zuverlässig, wie die großen Mengen an kopierten oder gefälschten Magnetstreifenkarten beweisen. 1991 entstanden den Banken dadurch weltweit rund ca. 400 Mio. DM Schaden. Außerdem ist die auf Magnetstreifenkarten gespeicherte Information vor Verlust nicht sicher geschützt, Hitze oder auch kleine mechanische und magnetische Beschädigungen der Magnetschicht machen die Karte unbrauchbar. Wo hohe Sicherheit gefragt ist, reichen deshalb Magnetstreifenkarten nicht aus. Auch der begrenzte Speicherplatz läßt in vieler Hinsicht Wünsche offen. Daher kam die Industrie zu Beginn der achtziger Jahre auf ein Patent aus dem Jahre 1967 zurück, das diese Nachteile – bei gleicher Speicher- und Verarbeitungsmöglichkeit – nicht aufwies: Die Mikroprozessorkarte oder auch Chipkarte.

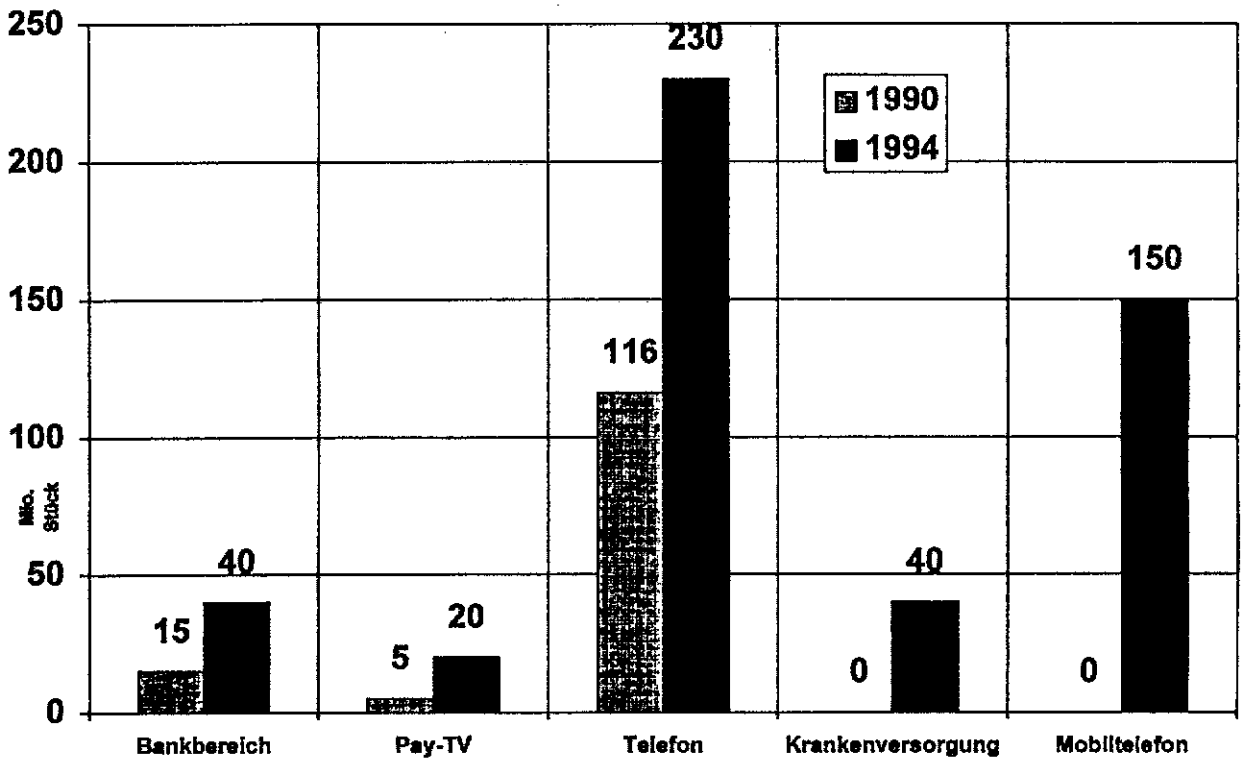
Die Chipkarte ist eine in Größe, physikalischen Eigenschaften und Lage des implantierten Chips international genormte Karte, im bekannten Magnetstreifenkartenformat. Nach der Struktur werden drei Typen von Chipkarten unterschieden:

- Speicherchip-Karten (Memory Cards)

  Dabei handelt es sich um Karten, die ähnlich der Magnetstreifenkarte im wesentlichen nur einen Datenspeicher enthalten und je nach eingesetzter Technik einmal oder mehrmals beschrieben und beliebig oft ausgelesen werden können. Als Anwendungsbeispiele seien hier die Telefonkarten und die Krankenversichertenkarte genannt. Das Datenspeichervolumen erreicht bei der Speicherchip-Karte ca. 5 000 Byte; dies entspricht einer vollständig beschriebenen DIN-A4-Seite. Da die Karte nur über einen Datenspeicher und keine vorge-

Abbildung 6

Zuwachs bei verschiedenen Chipkarten-Anwendungen



Quelle: SGS-Thomson

schaltete Logik verfügt, ergeben sich hinsichtlich ihrer Verarbeitungs- und Speichermöglichkeiten die gleichen Sicherheitsprobleme wie bei der Magnetstreifenkarte; Fälschung und Manipulation sind möglich.

- Intelligente Speicherkarte (Memory Card with logic)

  Diese Karten verfügen neben einem Datenspeicher über eine vorgeschaltete Sicherheitslogik, die den Zugriff auf den Speicher nur in Abhängigkeit von bestimmten Ereignissen, z. B. der PIN-Eingabe, erlaubt. Die Logik wird dabei schon beim Hardware-Design des Chips, der auf der Karte implantiert wird, berücksichtigt. Bezüglich des Speicherinhalts erreichen diese Karten die gleichen Größenordnungen wie die o. g. Speicherkarten. Hinsichtlich der Sicherheit bieten sie allerdings schon einige Vorteile. Durch die vorgeschaltete Logik kann zumindestens der Zugriff auf die Karte verhindert werden.

- Mikroprozessor-Karten (Micro-Controller-Cards, Smart-Cards)

  Bei dieser Art von Chipkarten steht neben Daten- und Programmspeicher auch ein eigener Mikroprozessor zur Verfügung, um aktiv auf der Karte Verarbeitungsoperationen durchführen zu können. Zur Verwaltung der Systemressourcen sowie zur Koordination der Abläufe wird dieser Chip mit einem eigenen Betriebssystem versehen. Mit der zur Verfügung stehenden „Intelligenz" auf der Karte lassen sich demzufolge auch hohe Sicherheitsanforderungen, wie z. B. dynamische Schlüsselverwaltungssysteme, Kontrolle von Speicherbereichen usw. realisieren.

Während bei den einfachen Speicherkarten keine Sicherheitsfunktionen auf den Karten selbst untergebracht werden und sie demzufolge nur durch entsprechende Maßnahmen in den Komponenten, die die Daten im weiteren verarbeiten, vorzusehen sind, verfügen intelligente Speicherkarten sowie Mikroprozessorkarten über Sicherheitsfunktionen. Im wesentlichen umfassen sie folgende Mechanismen:

- PIN-Prüfung

  Mit der PIN-Prüfung soll sichergestellt werden, daß nur ein Berechtigter, nämlich der Kartenbesitzer, die Karte benutzen kann. Als Minimallänge werden hier PIN's mit mindestens 4 Stellen vorgeschlagen, aber auch längere PIN's sind realisierbar.

- Authentisierung

  Bei der Authentisierung handelt es sich um eine Echtheitsprüfung aller beteiligten Systemkomponenten sowie des Kartennutzers. Damit soll bei der Verarbeitung der Daten auf dieser Karte sowohl die Authentizität des Kartennutzers als

auch der für die Verarbeitung berechtigten Systeme sichergestellt werden. Dies wird mit Hilfe von kryptografischen Verfahren und Schlüsseln erreicht.

- Autorisierung

  Bei der Autorisierung handelt es sich um die Prüfung, wer welche Anwendung auf der Karte auslösen darf. Die Autorisierung findet meist dort Anwendung, wo neben den Kartenbesitzern auch andere Personen Einträge auf der Karte vornehmen dürfen, z. B. bei einer „Patientennotfallkarte": Hier muß es dem Notarzt möglich sein, ohne Hilfe des Kartenbesitzers die Daten des Patienten von der Karte lesen zu können.

Diese Sicherheitsmechanismen werden zwar ständig erweitert und verbessert, der entscheidende Durchbruch ist allerdings ausgeblieben. Aus der Sicht des Datenschutzes sind einige Probleme trotz erheblicher Verbesserungen der Sicherheitsmechanismen noch nicht gelöst.

1. **Das „PIN-Problem"**

   Da die Anzahl der Karten in naher Zukunft sehr stark zunehmen wird, stellt sich die Frage: Wer kann sich die dann notwendigen vielen verschiedenen PIN's der vielen Karten für die verschiedenen Bereiche merken? Mit der Anzahl der Anwendungen auf Karten und der damit steigenden Anzahl von PIN's wird die theoretische Sicherheit, die sich mancher Hersteller wünscht, wohl nicht zu erreichen sein. Denn entweder werden zwar überall verschiedene PIN's verwendet und zur Sicherheit irgendwo – vielleicht sogar auf der Karte selbst – notiert oder es werden nur Trivialcodierungen benutzt, z. B. 4711; diese sind aber wiederum sehr leicht herauszufinden.

   Das Problem kann wohl nur durch die Verwendung biometrischer Merkmale (z. B. Fingerabdruck, Augenhintergrundabbildung) anstatt einer PIN befriedigend gelöst werden, wird dann aber noch datenschutzrechtlich vertieft zu diskutieren sein.

2. **Das „Daten-Sammel-Problem"**

   Sobald die Karte in das Kartenterminal gesteckt wird, verliert der Bürger alle Verfügungsmöglichkeiten über seine Daten. Sie „verschwinden" im Datenpool von Banken, Versicherungen, Krankenkassen oder sonstigen Anbietern von Dienstleistungen, um dann möglicherweise weltweit „online" zur Verfügung zu stehen. Bereits heute erweisen sich solche „privaten" Datenbestände als kaum kontrollierbar mit der eventuellen Folge, daß den Kartenbesitzer aufgrund falscher Daten Konsequenzen erwarten, ohne daß er Möglichkeiten zur wirkungsvollen Gegenwehr hat. Ich sehe deshalb beim datenschutzgerechten Einsatz verschiedener Chipkarten-Anwendungen einen erheblichen Bedarf zur Schaffung von rechtlichen Rahmenbedingungen sowie technischen und organisatorischen Maßnahmen, die beim Einsatz und der Verarbeitung der Daten dieser Karten beachtet werden müssen (s. auch Nr. 12.4 und Nr. 17.3). Wie aufwendig allein die Abläufe beim elektronischen Zahlungsverkehr mit Kredit- oder Scheckkarte sind, zeigt die nachfolgende Abbildung 7 hierzu.

3. **Das „Offenbarungs-Problem"**

   Besondere Akzeptanz erwarten Hersteller von Mikroprozessorkarten, auf denen mehrere Anwendungen realisiert sind, z. B. „Geldbörse", „Funktelefon" oder auch „Dialysepatient". Bei solchen „Multifunktionskarten" stellt sich das Problem: Wie findet ein Kartenterminal „seine" Anwendung auf der Karte? Der hierfür genormte Zugriffsmechanismus („Direct-File") sieht vor, daß das Kartenterminal zunächst alle Anwendungen (Applikationen) auf der Karte liest, um erst dann festzustellen, ob die benötigte Anwendung überhaupt vorhanden ist. Daraus folgt, daß sich der Kartenbesitzer gegenüber den Kartenterminals – und deren „Herren" – bezüglich seiner Anwendungen und deren Details offenbaren muß. Dies kann allerdings auch kopiert und gespeichert werden, ohne daß der Kartenbesitzer hiervon Kenntnis erhält. Auch kann an der Art der Anwendungen, die auf der Karte sind, auf die „Bonität" und die „Gesundheit" des Kartenbesitzers geschlossen werden; aus meiner Sicht ein bedenklicher Zustand. Ein besseres Zugriffsverfahren („Select-File") wurde durch die deutschen Vertreter im Internationalen Normungsausschuß zwar zur Normung vorgeschlagen, fand aber bisher keine Mehrheit in den zuständigen Gremien. Ich habe mich aus diesem Grunde an den zuständigen Normungsausschuß des Deutschen Instituts für Normung (DIN) in Berlin gewandt, um diese Initiative zu unterstützen; bislang wird über den deutschen Vorschlag noch beraten. Ich hoffe auf die Zustimmung und damit die Aufnahme in die internationale Norm. Auch unter dem Gesichtspunkt des zusammenwachsenden Europas und der Öffnung des Binnenmarktes wäre dieser Schritt sehr zu begrüßen.

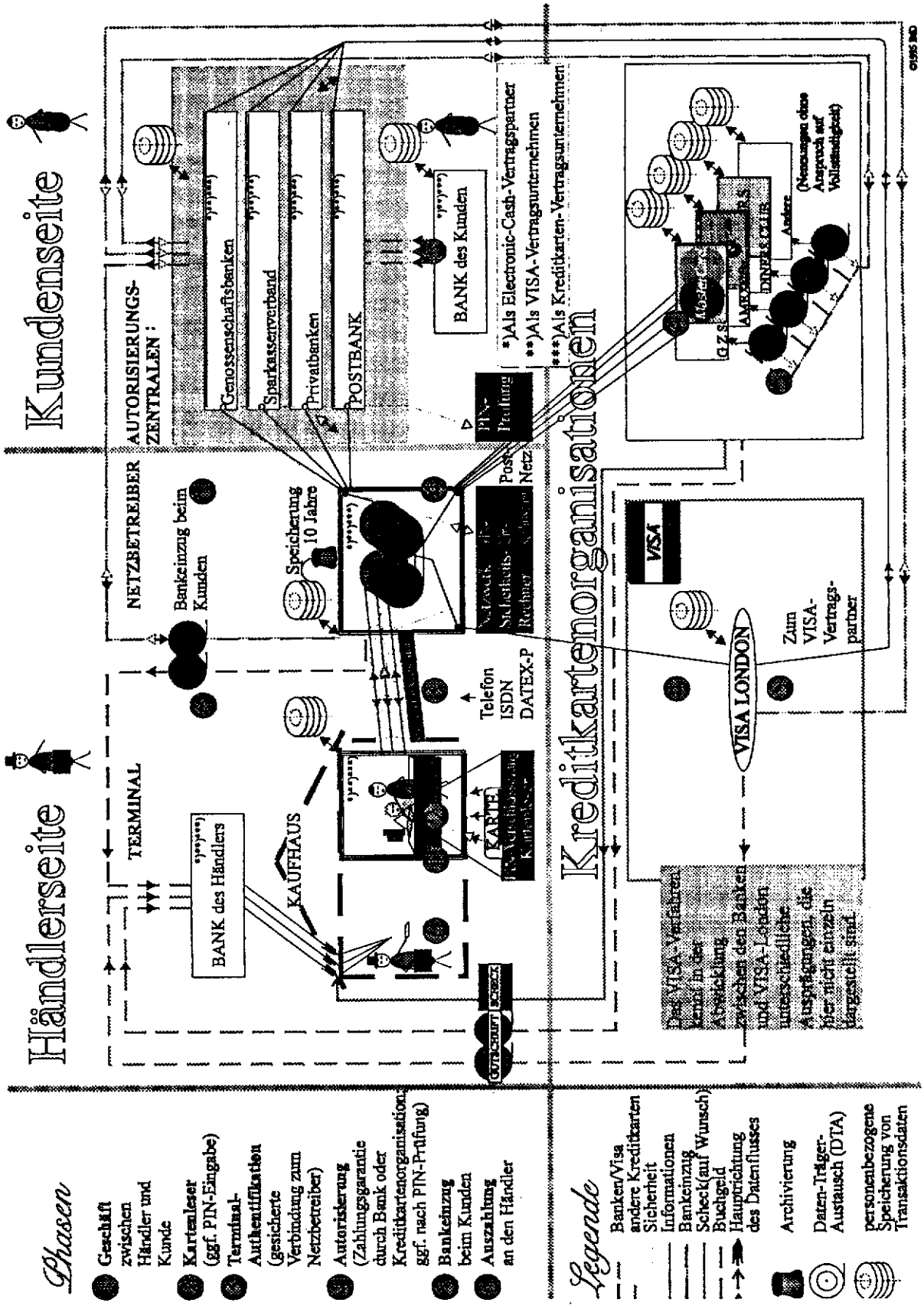
Die Chipkartennutzung wird in naher Zukunft weiterhin stark an Bedeutung gewinnen. Wenn es nicht gelingt, die Datenschutzprobleme zu lösen, die mit der Verbreitung dieser Karten verbunden sind, werden gravierende Probleme für das Persönlichkeitsrecht der Nutzer auftreten. Dem muß auch durch eine bereichsspezifische Gesetzgebung entgegengewirkt werden. Ich werde meine Beratungstätigkeit in Zukunft darauf ausrichten, daß sowohl die zur Sicherheit einer Karte notwendigen technischen und organisatorischen Maßnahmen umgesetzt, als auch die rechtlichen Rahmenbedingungen geschaffen werden. Ich begrüße es darum auch, daß sich das Bundesamt für die Sicherheit in der Informationstechnik dieser Thematik annehmen und in einen Arbeitskreis Vorschläge für Sicherheitsmechanismen bei Chipkarten erarbeiten will.

30.2 Tragbare PC immer noch ohne genügende Sicherheit

Die Bezeichnung „Laptop" für einen tragbaren Computer kann mit „Auf-dem-Schoß-Computer" frei übersetzt werden. Im Gegensatz dazu wird der heute

Abbildung 7

Elektronischer Zahlungsverkehr mit Kredit- oder Scheckkarte



vielerorts benutzte Personalcomputer oder Arbeitsplatzcomputer (APC) als „Desktop", als „Gerät auf dem Schreibtisch", bezeichnet. Der Laptop soll die baubedingten Nachteile seines „großen Bruders" – schwer, unflexibel, empfindlich gegen Stöße und Transporte, Stromnetzabhängigkeit – beheben und damit vor allen den Bedürfnissen von Beschäftigten im Außendienst nach kleinen, leichten, leistungsfähigen und robusten Geräten Rechnung tragen. Führten die Geräte der ersten Generation zunächst nur ein Schattendasein, da sie zwar flexibel und leicht gebaut, jedoch ein ungünstiges Preis-Leistungs-Verhältnis aufwiesen, so kam durch die technologische Entwicklung der letzten Jahre und dem damit verbundenen Preisverfall der Komponenten der Durchbruch dieser tragbaren APC. Die Miniaturisierung der Geräte schreitet weiter voran; neben dem Laptop gibt es heute folgende Geräteklassen: Notebook, Palmtop sowie die neueste Entwicklung „Personal Digital Assistant (PDA)".

Alle diese Geräte haben eines gemeinsam: Sie sind leicht, flexibel, robust, ebenso leistungsfähig wie ein stationäres Gerät und haben eine netzunabhängige Stromversorgung; leider sind sie noch unsicherer als alle bisherigen APC.

Während die Entwicklung der Prozessoren, Festplatten, Schnittstellen und peripheren Komponenten in den letzten Jahren ständig fortschreitet und ein Ende nicht absehbar erscheint, wurde die Sicherheit solcher Geräte geradezu sträflich vernachlässigt. Aus Datenschutzsicht gelten die „Kleinen" insbesondere deshalb als sehr problematisch, weil sie leicht entwendet und verloren werden können. Trotz dieses Risikos gibt es bei den tragbaren APC keine vernünftigen Sicherheitsmechanismen: Weder verfügen die Geräte über einen ausreichend sicheren Schutz gegen unberechtigte Kenntnisnahme der gespeicherten Daten noch gegen das unbefugte „Einspielen" von Programmen (Virenbefall!); fast stets fehlen auch Komponenten zur Verschlüsselung der Daten auf der Festplatte und der Diskette. Dies ist um so ärgerlicher, als mit dem Preisverfall der Geräte der Verbreitungsgrad in der Wirtschaft und auch in der Verwaltung rasant zunimmt. So sind z. B. bereits jetzt in der Finanzverwaltung, wie ich anläßlich einer Kontrolle feststellen konnte, weit über 1 000 solcher Geräte im Einsatz. Da auf tragbaren APC auch personenbezogene Daten höchster Sensibilität – wie z. B. Diagnosedaten von Patienten, Prüfberichte aus der Finanzverwaltung – gespeichert und verarbeitet werden, sind Maßnahmen zum Schutz dieser Daten dringend erforderlich. Die Einrichtung eines sog. „BIOS"-Paßwortes zum Schutz des Rechners und der Daten vor unbefugter Benutzung und unbefugten Zugriffen reicht aus der Sicht des Datenschutzes nicht aus: Dieser Paßwortschutz ist schon mit geringem Aufwand auszuhebeln und eröffnet damit einem Unbefugten Zugriff auf alle gespeicherten Daten – bei sensiblen Daten aus dem Bereich des Gesundheitswesens oder der Strafverfolgung ein höchst bedenkliches Verfahren.

Bei dem Betrieb besonders gefährdeter ADV-Verfahren und -systeme – zu denen ich aufgrund der derzeitigen Sicherheitsmechanismen grundsätzlich auch tragbare APC-Systeme zähle – sind auch besonders wirksame technische und organisatorische Maßnahmen im Sinne des § 9 BDSG, insbesondere zum Schutz gegen unbefugte Kenntnisnahme vorzusehen. Aus diesem Grunde halte ich bei der Verarbeitung personenbezogener Daten auf solchen Systemen folgende Sicherheitsmechanismen für geboten:

1. Einsatz einer Sicherheitssoftware zum Schutz gegen unberechtigte Kenntnisnahme der Daten und unbefugtes Einspielen von Programmen sowie zur Gewährleistung einer sicheren Menüführung,
2. die Verschlüsselung der Festplatte sowie eventuell benötigter Disketten, der Verschlüsselungsalgorithmus muß hinreichende Sicherheit bieten.

Beide Maßnahmen sind unerläßlich, um die beim Einsatz solcher Systeme vorhandenen Sicherheitsdefizite ausgleichen zu können.

30.3 Elektronischer Dokumentenaustausch – auf dem Weg zum „papierlosen Büro"

Für die Fortentwicklung der Bürokommunikation kommt der elektronischen Übertragung von Dokumenten, die bereits in elektronischer Form gespeichert sind, eine zentrale Bedeutung zu. Bislang wurde der Telefaxdienst in erheblichem Umfang für den schnellen und direkten Austausch von Dokumenten verwendet, obwohl dies den Nachteil hat, daß die empfangenen Nachrichten nicht direkt in elektronischer Form weiterverarbeitet werden können. Mit elektronischen Mitteilungssystemen soll dieser Nachteil behoben werden und gleichzeitig eine neue Qualität der Kommunikation auch zwischen öffentlichen Stellen erreicht werden.

Die Bedeutung von elektronischen Mitteilungssystemen zeigt sich auch im Beschluß der Konferenz der Innenminister und -senatoren der Länder vom 20. August 1993, der vorsieht, ab dem 1. Januar 1995 ein elektronisches Mitteilungssystem für den Dokumentenaustausch zwischen den Ländern zu verwenden und dafür bis zu diesem Zeitpunkt geeignete Maßnahmen zu treffen. Auch durch den Berlin-Beschluß des Bundestages wurde der Aufbau von neuen Kommunikationsinfrastrukturen dringend notwendig. Im Rahmen des „Informationsverbundes Berlin-Bonn (IVBB)" wird deshalb u. a. ein elektronisches Mitteilungssystem auf der Basis des X.400-Standards des Comité Consultatif International de Télégraphique et Téléphonique (CCITT) bzw. der International Organization for Standardization (ISO) eingeführt werden.

Beim elektronischen Dokumentenaustausch über private oder öffentliche Übertragungswege werden die bekannten Bedrohungen – der Verlust der Vertraulichkeit, Integrität, Verfügbarkeit und insbesondere der Verbindlichkeit – dadurch verschärft, daß eventuell Unbefugte Zugriff auf Daten und Programme erhalten und die Übertragungswege von dem Kommunikationspartner nicht sicher kontrolliert werden können. Da in Zukunft vermehrt damit zu rechnen ist, daß mit Hilfe elektronischer Mitteilungssysteme bedeutsame Informationen jeglichen Inhalts, insbe-

sondere vertrauliche personenbezogene Daten, über öffentliche Netze ausgetauscht werden, gilt es, beim Einsatz solcher Systeme das Risikobewußtsein bei den Verantwortlichen sowie den Anwendern zu schärfen. In jedem Fall gewinnt der Schutz der elektronisch gespeicherten, verarbeiteten und übertragenen Information gegen Risiken durch umfassende Sicherheitsmaßnahmen zunehmend an Bedeutung. Datenschutz und Datensicherheit können bei elektronischen Mitteilungssystemen nur durch ein Bündel von aufeinander abgestimmten Maßnahmen erreicht werden.

Die Vertrauenswürdigkeit wurde bisher durch handschriftliche Unterschrift, Dienstsiegel, Spezialpapier u. ä. gewährleistet und die Vertraulichkeit durch den verschlossenen oder gar versiegelten Briefumschlag. Zumindest die gleichwertige Sicherheit muß durch ein elektronisches Mitteilungssystemen erreicht werden. Dazu müssen vor allem Maßnahmen gegen folgende Risiken ergriffen werden:

1. Sicherstellung der Authentizität von Benutzern, Nachrichten und Systemmeldungen

   Für den Empfänger einer Nachricht muß jederzeit die Möglichkeit bestehen, anhand bestimmter Kriterien die Authentizität des Absenders der Nachricht sowie von an ihn gerichteten Meldungen des Systems (z. B. Empfangs- und Weiterleitungsbestätigung, Sendeanforderung, Teilnehmerkennungen, Teilnehmereinstufungen) zu überprüfen.

2. Sicherstellung der Vertraulichkeit der übertragenen Daten

   Für alle Arten von Daten im elektronischen Mitteilungssystem – Nachrichten sowie Verkehrs- und Verbindungsdaten – muß die Vertraulichkeit gewahrt werden. Hier sind aus der Sicht des Datenschutzes geeignete technische Maßnahmen, z. B. kryptografische Verfahren, unerläßlich; dies ist bei der Wahl des elektronischen Systems zu berücksichtigen.

3. Sicherstellung der Integrität von Nachrichten und Meldungen

   In Abhängigkeit von der Sensibilität der übertragenen Daten und der Sicherheit des eingesetzten Systems müssen Maßnahmen getroffen werden, die verhindern, daß bei Speicherung und Weiterleitung keine unbefugte, unerkannte Veränderung übermittelter Daten erfolgen kann.

4. Bereitstellen von fälschungssicheren Kommunikationsnachweisen

   Die für die Anerkennung einer elektronisch stattgefundenen Kommunikation erforderlichen Nachweise (Sende-, Empfangs- und Übertragungsnachweis) müssen dem Anwender auf Wunsch zur Verfügung stehen. Die unter 1. bis 3. genannten Forderungen gelten entsprechend, insbesondere ist sicherzustellen, daß die Nachweise im Nachhinein nicht gefälscht werden können und ausreichend lange zu Beweiszwecken vorgehalten werden.

5. Verhindern der Bildung von Kommunikationsprofilen

   Die Erstellung von Kommunikationsprofilen muß untersagt sein, wenn möglich, auch durch technische Maßnahmen verhindert werden. Soweit entsprechende Protokollierungsdaten gespeichert werden, dürfen diese nur für Datenschutz- und Datensicherungszwecken (§ 14 Abs. 4 BDSG, § 31 BDSG) genutzt werden.

Erst wenn ein elektronisches Mitteilungssystem gegen diese Risiken Sicherheitsmechanismen bereitstellt, können sowohl die Vertrauenswürdigkeit als auch die Vertraulichkeit von Daten, die innerhalb des Systems transportiert werden, als gesichert gelten. Aus diesem Grunde sollten – auch um die Akzeptanz solcher Systeme nicht zu gefährden – geeignete Maßnahmen zur Erfüllung dieser Sicherheitsbedürfnisse vorgesehen werden. Als geeignete Maßnahmen sehe ich Integritäts- und Authentisierungsmaßnahmen an.

Integritätsmechanismen dienen dem Schutz der Daten vor unbefugter Änderung bei der Übertragung. Die Identifizierung solcher Integritätsverletzungen kann nur durch geeignete kryptographische Maßnahmen erreicht werden. Authentisierungsmechanismen sollten ebenso wie Integritätsmechanismen auf kryptografischen Verfahren beruhen. Darüber hinaus sollten Nachrichteninhalte oder Angaben zum Ursprung der Nachricht durch Verwendung der „elektronischen Unterschrift" vor den bekannten Bedrohungen angemessen geschützt werden. Für alle Maßnahmen stehen Hard- und Softwareprodukte am Markt bereit und sollten eingesetzt werden. Diese Maßnahmen sind durch sichere Protokollierungen (sowohl auf Absender-, als auch auf Empfängerseite), Archivierung der gesendeten und empfangenen Nachrichten sowie durch organisatorische Maßnahmen zu unterstützen.

Als Grundsicherungsmaßnahmen empfehle ich, beim Einsatz von elektronischen Mitteilungssystemen folgendes zu beachten:

- Grundsätzlich sind nur solche Systeme einzusetzen, die die Vorgaben der X.400-Empfehlung aus dem Jahre 1988 erfüllen. Vorhandene Systeme – insbesondere solche, die noch auf Empfehlungen von 1984 basieren – sollten hinsichtlich ihrer Sicherheit durch geeignete Zusatzprodukte verbessert oder durch neuere Softwareversionen ersetzt werden.
- Nach Möglichkeit ist die Funktion des Systemverwalters von der Verwaltung des elektronischen Mitteilungssystems zu trennen; ich verweise hierzu auf meine Ausführungen in Nr. 29.7.
- Für das elektronische Mitteilungssystem ist grundsätzlich separate Hard- und Software – z. B. in Form eines Kommunikationsservers – vorzusehen und auch separat zu administrieren.
- Bei Verwendung von öffentlichen Übertragungswegen sind zur Abwehr des Angriffs durch Externe die vorhandenen Sicherheitsmechanismen dieser Netze – z. B. geschlossene Benutzergruppen, Rufnummernidentifikation usw. – zu nutzen.

- Zur Beweissicherung einer stattgefundenen Kommunikation muß die eingesetzte Software sowohl sichere Zustellungs-/Empfangsnachweise als auch Sendeübergabe/Empfangsübergabenachweise erzeugen.
- Bei der Übertragung von personenbezogenen Daten auf Übertragungswegen des öffentlichen Netzes ist zumindest eine Verbindungsverschlüsselung vorzusehen. Bei sensiblen personenbezogenen Daten ist eine Übertragung nur mit einer Ende-zu-Ende-Verschlüsselung vertretbar.
- Verschlüsselungsgeräte sind durch technische, bauliche und organisatorische Maßnahmen vor Zugriff Unbefugter zu schützen.
- Die Verschlüsselung der Daten muß mit einem hinreichend sicheren Verschlüsselungsverfahren erfolgen. Neben der Auswahl eines effektiven Verschlüsselungsalgorithmus (z. B. DES) muß dabei insbesondere eine ordnungsgemäße Schlüsselerzeugung, -verwaltung und -verteilung gewährleistet sein.
- Zur Absicherung der Integrität der Daten ist auf Verfahren der „elektronischen Unterschrift" zurückzugreifen.
- Für die Dauer der Speicherung der Kommunikationsnachweise sollte grundsätzlich ein fester Zeitraum vorgesehen werden; eine im Einzelfall erforderliche längere Speicherung sollte von dem Benutzer selbst festgelegt werden können.

Aufgrund des flächendeckenden Einsatzes von elektronischen Mitteilungssystemen sowohl in den Ländern als auch im Bund werde ich in der Konferenz der Datenschutzbeauftragten des Bundes und der Länder darauf hinwirken, daß eine Empfehlung für den Einsatz dieser Systeme erarbeitet wird und verabschiedet werden kann. Bei der Entwicklung und dem Betrieb des IVBB bin ich bisher beratend tätig geworden. So wird auch auf meine Anregung hin derzeit ein Verschlüsselungssystem getestet, das in Zukunft im Rahmen des IVBB eingesetzt werden soll. Ich werde die weitere Entwicklung des IVBB beratend begleiten.

30.4 Großrechner sind noch immer unentbehrlich

Auch im Zeitalter der Personalcomputer und deren zunehmender Vernetzung bleiben Großrechner unentbehrlich. Sie werden als Knoten in großen Rechnernetzen eingesetzt, aber auch dort, wo es besonders große Datenmengen, wie z. B. in der Gehaltszahlung, zu verarbeiten gilt. Großrechner sind in einer Zeit entstanden, als Speicherplatz knapp und teuer war. Während in Personalcomputern und in modernen Netzen eher großzügig mit Speicherplatz umgegangen wird und oft unnötiger Ballast – z. B. in Gestalt übertrieben aufwendiger graphischer Oberflächen – mitgeschleppt wird, geizen Großrechner bis heute mit Platz, obwohl er eigentlich in ausreichendem Maße zur Verfügung steht. Bei der Benutzung von Großrechnern muß man sich in vielen Fällen immer noch mit kryptischen Kürzeln zurecht finden, man bekommt dürftige, wenig aussagefähige Bildschirmmasken, und manche notwendige Arbeit wird zur Tortur. Das gilt auch für den „gewöhnlichen" Endbenutzer, mehr noch aber für den Systemadministrator. Aufgrund der Komplexität der Systeme, aber auch wegen der unzulänglichen Benutzeroberflächen geht in punkto Sicherheit oft die Übersicht verloren: Versetzt man sich in die Lage des Administrators eines großen Systems mit mehreren 10 000 Benutzern, so kann es angesichts der zur Verfügung stehenden Mittel nicht verwundern, daß erhebliche Sicherheitslücken bleiben. Will der Administrator z. B. sicherstellen, daß die Benutzer bestimmte Paßwörter – etwa Banalpaßwörter (Asterix, Obelix, Name der eigenen Firma) – nicht verwenden, so muß er dafür eigens ein Programm schreiben. Auch wenn er sich eine Übersicht darüber verschaffen will, welche Benutzer welche Rechte haben oder welche Benutzer wie lange nicht im System angemeldet waren, so ist dies recht aufwendig. Hinzu kommt, daß Systemparameter, die für die Sicherheit des System von Bedeutung sind, in aller Regel in einer Weise gesetzt sind, die weniger Sicherheit gewährleistet.

Bei der Bewertung der Sicherheit von Großrechnern ist die Sicherheit, die theoretisch erreicht werden könnte, ohne Bedeutung. Die tatsächlich erreichte Sicherheit liegt in der überwiegenden Anzahl aller Fälle weit unter diesem Niveau. Glücklicherweise gibt es inzwischen „Zusatzwerkzeuge" für den Administrator. Oft werden diese Softwareprodukte auf der Basis von Empfehlungen der Administratoren selbst oder von Revisoren von kleineren Firmen entwickelt. Diese Werkzeuge bieten ungleich mehr Möglichkeiten, Sicherheitslücken im System aufzuspüren und damit die Systemsicherheit zu erhöhen. Wegen der mit der Anschaffung verbundenen Kosten sind derartige Werkzeuge aber noch wenig verbreitet. Die Hersteller der Betriebssysteme für Großrechner sind daher aufgefordert, im Betriebsystem selbst Sicherheitswerkzeuge zu implementieren, die den Administrator in die Lage versetzen, das System auf komfortable Weise sicher zu verwalten und Lücken zu erkennen.

30.5 Kontrolle des Rechenzentrums Frankfurt der Deutschen Bahn AG

Im Berichtszeitraum habe ich das Rechenzentrum Frankfurt der Bundesbahndirektion Frankfurt sowie Teile der „Zentrale, Zentrale Datenverarbeitung (ZZD)", die Weisungsrechte gegenüber dem Rechenzentrum hat, kontrolliert. In dem Rechenzentrum werden die folgenden drei großen Datenverarbeitungsanlagen betrieben:

- IBM-Datenverarbeitungsanlage unter dem Betriebssystem MVS, das eingesetzt wird für kommerzielle Aufgaben, z. B. für die Abrechnung der Finanzmittel und die Frachtabrechnung;
- ein Tandemrechner unter dem Betriebssystem Guardian 90, das Aufgaben der Fahrkartenausgabe (Kurs 90, z. B. Platzbuchung) erledigt;
- eine Siemens-Datenverarbeitungsanlage unter dem Betriebssystem BS 2000, die für die Abwicklung des Güterverkehrs eingesetzt wird.

In allen drei Datenverarbeitungsanlagen werden personenbezogene Daten verarbeitet.

Im Laufe der Kontrolle wurde folgendes festgestellt:

- Organisation des Datenschutzes

  Der Datenschutz ist gemäß einer internen Bundesbahnvorschrift Aufgabe des Dienststellenleiters. Dienststellenleiter im vorliegenden Fall war der Präsident der Bundesbahndirektion Frankfurt. Im Verlauf der Kontrolle konnte aber nicht geklärt werden, wer in dem Rechenzentrum die Datenschutzaufgaben in der Praxis wahrnimmt. Es waren auch keinerlei datenschutzrechtliche Kontrollen durchgeführt worden. Auch die Schulung des Personals über die datenschutzrechtlichen Pflichten der speichernden Stelle war offenkundig unzureichend.

- Outsourcing

  Aus Dateien des Verfahrens „Kurs 90" wurden Daten sowohl an Stellen der Bundesbahn – zur Aufklärung von Kassenfehlbeträgen – übermittelt als auch – zur Beantwortung von Anfragen – an Polizei und andere Behörden. Die Recherchen für diese Anfragen wurden von einer privaten Firma durchgeführt, die von der Bundesbahn mit der Administration des Verfahrens beauftragt ist. In dieser Firma waren jedoch datenschutzrechtliche Regeln oder interne Dienstvorschriften für Datenübermittlungen nicht bekannt.

- Benutzerverwaltung und Beweissicherung bei den drei Rechenanlagen

  Die Benutzerverwaltung in der **IBM-Rechenanlage** wird mittels des Zugriff-Kontrollsystems „Resource Access Control Facility (RACF)" durchgeführt, mit dem grundsätzlich eine ausreichende Sicherheit erreicht werden kann. Der organisatorische Ablauf der Benutzerverwaltung nutzt die vorhandenen Möglichkeiten jedoch nur mangelhaft aus und macht das System daher angreifbar. Stichproben ergaben, daß bei der Einrichtung von 20 neuen Benutzern für die Hälfte nicht belegt werden konnte, aufgrund welcher Anträge sie im System zugelassen worden waren. Eine weitere Stichprobe ergab, daß von 20 Benutzern sich fünf länger als ein Jahr nicht im System angemeldet hatten, fünf weitere noch nie angemeldet waren. Die Gesamtzahl aller Benutzer betrug nahezu 20 000, davon waren ein Viertel länger als ein Jahr nicht mehr im System angemeldet. Ich habe deshalb eine Neuordnung der Benutzerverwaltung empfohlen.

  Die Protokollierung des RACF-Systems ist grundsätzlich geeignet, den Anforderungen der Anlage zu § 9 BDSG zu entsprechen. Eine Auswertung der Protokolldateien findet jedoch nicht statt. Eine Ursache dafür ist sicherlich, daß eine Auswertung der Protokolldateien mit dem RACF-Monitor bei der derzeitigen Vielzahl von Benutzern sehr aufwendig und damit zeitraubend ist. Für eine Verbesserung der Administration und eine Auswertung der Protokolle habe ich den Einsatz einer zusätzlichen Software empfohlen.

- Die Kontrolle der Benutzerverwaltung des **Tandemsystems** ergab, daß das Paßwort des Systemadministrators neun Mitarbeiter der Systemverwaltergruppe bekannt ist. Das Paßwort für die Anwendersystemgruppe ist mindestens neun Mitarbeitern einer beauftragten Privatfirma bekannt. Beides widerspricht dem Grundsatz, daß das Paßwort für einen Benutzer nur einer einzigen natürlichen Personen bekannt sein darf.

  Die Verwaltung der Normalbenutzer erfolgt dezentral in den Fahrkartenausgaben. Sie ist aktuell und ausreichend sicher. Die Konventionen für den Zugang zum System sind aber unter Sicherheitsaspekten unzureichend. So wird z. B. ein Benutzer, der die zulässige Zahl von Fehlversuchen bei der Paßworteingabe überschreitet, nur eine Minute gesperrt. Zur Verbesserung der Systemsicherheit habe ich den Einsatz einer speziellen Software empfohlen. Dann wäre auch eine Beweissicherung möglich, die gegenwärtig nicht durchgeführt werden kann.

- Die Kontrolle der Benutzerverwaltung der **Siemens-Rechenanlage** ergab, daß ein Teilnehmerbetrieb (Dialog) im Regelfall nicht stattfindet. Für die Aufgabe Systemadministration wird der Teilnehmerbetrieb von Fall zu Fall zugelassen. Eine Überprüfung der Teilnehmer ergab keine Mängel. Im Teilhaberbetrieb gibt es keine zugelassenen Benutzer, sondern zugelassene Geräte, die mit einem besonderen Befugnisprofil versehen sind. Da das System zum Zeitpunkt der Kontrolle nur noch etwa zwei Jahre in Betrieb sein sollte, konnte diese Art des Zugangs akzeptiert werden. Eine Protokollierung im Teilnehmerbetrieb erfolgt nicht; angesichts der hohen Befugnisse der Teilnehmer habe ich eine solche dringend empfohlen. Im Teilhaberbetrieb werden alle Transaktionen mit Angabe der Station zentral protokolliert. Diese Protokolle werden aber nur für die Störungssuche ausgewertet. Eine Auswertung zu Datenschutz- und Datensicherheitszwecken habe ich dringend empfohlen.

Durch die Bahnreform bin ich für die Datenverarbeitung bei der Deutschen Bahn AG nicht mehr zuständig. Eine förmliche Stellungnahme zu meinem Kontrollbericht war deshalb nicht mehr erforderlich. Weil eine Erhöhung der Datensicherheit aber im Eigeninteresse der Bahn AG liegt, hat sie meine Anregungen aufgegriffen, und meine Mitarbeiter haben auf Wunsch der Bahn AG noch einzelne Details der Feststellungen und Verbesserungsmöglichkeiten erläutert.

30.6 Datenschutz braucht Regelungen – auch bei modernen PC-Netzwerken

Bei der datenschutzrechtlichen Betrachtung vernetzter Informationssysteme – auch der immer häufiger in Wirtschaft und Verwaltung anzutreffenden PC-Netzwerke – sind zwei Problemfelder zu unterscheiden:

Zum einen gilt es die personenbezogenen Daten zu schützen, die den Gegenstand der Informationsverarbeitung bilden, also die Daten der **„Betroffenen"**. Zum anderen werden beim Betrieb der Systeme personenbezogene Daten verarbeitet, die sich auf die **Nutzer** des Netzes beziehen – Namen und Berechtigungen der Nutzer sowie Protokolldaten ihrer

Systemnutzung usw. – und ebenfalls schutzwürdig sind.

Moderne Netzwerkbetriebssysteme beinhalten zu diesem Zweck eine Vielzahl von Schutz- und Sicherheitsmechanismen, die in der einschlägigen Literatur bereits eingehend diskutiert und bewertet wurden.

Nach meinen Erfahrungen werden besonders viele Datenschutz-Problemfälle in Netzwerken durch Irrtum – z. B. Fehlinterpretation von Funktionalitäten – und Nachlässigkeit der Nutzer beim Umgang mit vorhandenen Sicherheitskomponenten verursacht. Deshalb sollten nicht nur leistungsfähige Sicherheitsmechanismen konsequent in die Hard- und Anwendungssoftware eingebunden und genutzt werden. Hohe Aufmerksamkeit muß vor allem dem organisatorischen Umfeld des Netzes und hier der Schaffung von **Verfahrensregelungen** gewidmet werden, die von den Nutzern **akzeptiert** und somit auch eingehalten werden können. Mit diesen Regelungen (Dienstvereinbarung, Dienstanweisung, usw.) sollte für jeden Nutzer einerseits eine hohe Transparenz des Netzbetriebes und andererseits die erforderliche Sensibilität für richtiges, insbesondere datenschutzgerechtes „Verhalten im Netz" erreicht werden.

Weil sich in einem solchen Regelwerk nicht jede in der Praxis auftretende Situation von Anfang an regeln läßt, sollte Wert darauf gelegt werden, es ergänzungs- und änderungsfreundlich zu gestalten. So lassen sich Veränderungen, die aus neuen oder modifizierten Anwendungen resultieren, ebenso ergänzend regeln wie die sich aus den in immer schnellerer Abfolge sowohl auf dem Hard- als auch Softwaresektor ergebenden neuen Möglichkeiten zur Netzgestaltung.

Schon in der Aufbauphase eines PC-Netzes ist es jedoch möglich, ausgehend von den in der Anlage zu § 9 BDSG dargestellten „10 Geboten", die wesentlichen – auf die konkrete Einsatzsituation bezogenen – Regeln für dessen Betrieb und Nutzung aufzustellen. Hier und bei der weiteren Ausgestaltung kommt es darauf an, den Blick der Adressaten auf ein für sie **überschaubares Handlungsumfeld** zu eröffnen und zu schärfen. Eine knappe, aber aussagekräftige und möglichst im Hinblick auf die einzelnen Adressatengruppen gegliederte Darstellung erleichtert es den betroffenen Mitarbeitern, sich in dieses Umfeld einzufügen und die dort geltenden Regeln bewußt einzuhalten. Nur diese Akzeptanz und die Durchschaubarkeit des Netzbetriebes für den einzelnen Nutzer führen – gemeinsam mit der konsequenten Nutzung technischer Möglichkeiten – zu einer Eindämmung der oben erwähnten Hauptursache für Sicherheitsprobleme: Irrtum und Nachlässigkeit.

Was sollte in einem solchen Regelwerk – unabhängig von der Form der Darstellung – enthalten sein?

In einer **„Präambel"** sollten neben Zweck und Anwendungsbereich die wesentlichen Aspekte von Datenschutz und Datensicherheit dargestellt werden:

- Nutzung des Netzes nach Regelungen, die allen Nutzern bekanntgegeben werden,
- Nutzung des Netzes nur im Rahmen der Aufgabenerfüllung,
- Hinweis auf die Mechanismen, die Verstöße gegen das Recht auf informationelle Selbstbestimmung verhindern sollen,
- Festlegung des Prinzips, daß bei der Nutzung und dem Betrieb des Netzes die Zweckbindung der gespeicherten Daten gewahrt bleibt.

Weitere Punkte der Präambel könnten sein:

- Hinweis auf die Rolle und die besonderen Möglichkeiten der Systemverwalter (vgl. Nr. 30.7),
- Hinweis auf die Befugnisse des behördlichen Datenschutzbeauftragten,
- Hinweise an die Nutzer auf die eigene Verantwortung bei der Arbeit im Netz und die möglichen Sanktionen bei Verstößen gegen geltende Festlegungen,
- Hinweise auf die Notwendigkeit der eigenen Netzdisziplin, um die anderen Netznutzer nicht in ihrer Arbeit zu behindern.

Für den Betrieb und die Nutzung jedes PC-Netzes lassen sich **„allgemeingültige Regelungen"** aufstellen, die für jeden Nutzer – unabhängig von seiner Zugehörigkeit zu einer Adressatengruppe – Bedeutung haben:

- Pflichten und Maßnahmen zur Aus- und Weiterbildung der Netznutzer,
- Regelungen zur technischen Zugangssicherung und zum Benutzer- und Paßwortmanagement,
- Regelungen zur Rechtevergabe und -verwaltung,
- Festlegungen zur Verarbeitung besonders sensibler personenbezogener Daten (vgl. 14 TB S. 149 f),
- Konventionen, z. B. zur Vergabe von Verzeichnis- und Dateinamen,
- Hinweise zur Erstellung dienstlichen Schriftgutes im Netz,
- Regelungen zur Nutzung, zum Einsatz und zum Umgang mit Hard- und Software und Verbrauchsmaterial bis hin zu Entsorgungsfragen,
- Festlegungen zur Nutzung von Netzdiensten (z. B. Fax, externe Datenbanken usw.),
- Hinweise auf Pflichten und Maßnahmen zur Aufrechterhaltung eines reibungslosen Netzbetriebes und zur effektiven Nutzung von Ressourcen (z. B. Auslagerung von selten genutzten Dateien, Speicherplatzbeschränkungen usw.),
- Verhalten bei Störungen des Netzbetriebes, Art und Weise der Störungsbeseitigung.

Nicht fehlen sollten auch Regelungen über die Pflichten, Rechte und Möglichkeiten des **Systemverwalters**:

- Pflichten und Maßnahmen zur Qualifizierung der Systemverwalter,
- Regelungen zur Benutzerverwaltung und -kontrolle,
- Umgang mit den vom Betriebssystem angebotenen Möglichkeiten zur Protokollierung von Aktivitäten im Netz,

- Verantwortlichkeiten der Systemverwaltung für die Sicherung von Hard- und Softwarekomponenten des Netzes und die Art ihrer Wahrnehmung,
- Notfallplanung,
- Datenträgerverwaltung und
- Störungsbeseitigung.

In Abhängigkeit von den gegebenen Verhältnissen könnten spezielle Regelungen für einzelne Nutzergruppen getroffen werden, so z. B. für

- die Sekretariate und den Schreibdienst,
- die Registratur,
- Organisationseinheiten mit besonders sensiblen Daten (z. B. Personalreferat) usw.

Nach dieser Vorgehensweise entsteht ein Werk, das jedem Netznutzer die von ihm einzuhaltenden Regelungen nahebringen kann.

Bei der Erarbeitung und Aktualisierung der Dienstanweisung für das IT-System meiner Dienststelle hat sich die Beteiligung aller Mitarbeiter als sehr hilfreich erwiesen. Um deren Kenntnisse, Erfahrungen, Vorstellungen und Wünsche in den Prozeß des Auf- und Ausbaus der IT-Anwendung einfließen zu lassen, habe ich einen IT-Koordinierungsausschuß (ITKA) eingesetzt, der sich aus Mitarbeitern jeder Organisationseinheit des Hauses zusammensetzt. Der ITKA, der wenigstens zweimal im Jahr zusammentritt, hat nicht nur bei der Konzeption und Ausgestaltung der Dienstanweisung mitgewirkt, sondern berät mich auch hinsichtlich der im IT-Rahmenkonzept (vgl. auch IT-Richtlinie des Bundes vom 18. August 1988, Nr. 8 Abs. 2) dargestellten Maßnahmen zur Nutzung und der Erweiterung der IT einschließlich der dazu in Dienstanweisungen oder Vereinbarungen zu treffenden Festlegungen.

30.7 Die „Allmacht" des Systemverwalters

Für den professionellen Betrieb moderner Systeme der Informationstechnik – namentlich von Computersystemen mit mehreren Benutzern und von APC-Netzwerken – ist die Funktion des Systemverwalters von großer Bedeutung: Er setzt Systemparameter, meldet neue Benutzer an, verändert Zugriffsrechte usw., wartet und implementiert neue Software und behebt Störungen.

Die Arbeit des Systemverwalters erfordert neben einer guten „IT-Grundausbildung" breite und vertiefte Kenntnisse der eingesetzten Hard- und Software sowie umfangreiche praktische Erfahrungen mit deren Einsatz: Der Systemverwalter ist in der Regel derjenige, der das eingesetzte IT-System am genauesten kennt, mit seinen Leistungsmöglichkeiten, aber auch mit seinen Schwächen. Der Systemverwalter hat uneingeschränkte Zugriffsmöglichkeiten auf alle Dateien und Programme des Systems; in der Tat ergeben sich in der Praxis immer wieder Situationen, in denen eine schnelle Störungbehebung nur möglich ist, wenn der Systemverwalter Zugriff auf alle Systemdateien und die Dateien der Benutzer hat. Der Systemverwalter kann somit alle im System gespeicherten Daten einsehen, verändern, löschen und auch kopieren, und zwar unabhängig davon, ob es hierzu einen Anlaß gibt oder nicht. Eine unberechtigte Nutzung – etwa Kopieren einer bestimmten Datei auf Diskette – ist somit nicht nur möglich, sondern wird im Regelfall unbemerkt bleiben, da in vielen Systemen die Aktivitäten der Benutzer nicht protokolliert werden. Dort wo sie protokolliert werden, kann der Systemverwalter das Protokoll editieren und die Spuren seines „schändlichen Tuns" verwischen.

Ein weiteres Problem ergibt sich aus dem Umstand, daß in großen Systemen z. B. mit mehreren tausend Benutzern – die Aufgabe der Systemverwaltung naturgemäß nicht von einer einzelnen Person geleistet werden kann, vielmehr hierfür eine entsprechende Arbeitseinheit eingerichtet ist. Zwar hat im – positiven – Regelfall jeder Mitarbeiter der Systemverwaltung eine eigene Benutzerkennung (User Identifikation) und auch ein eigenes Paßwort. Leider kommt es jedoch immer noch oft vor, daß alle Mitarbeiter der Arbeitseinheit unter einer einzigen Benutzerkennung und entsprechend auch nur einem Paßwort arbeiten. Dies führt dazu, daß – falls konkrete Hinweise den Verdacht eines Mißbrauchs begründen – die unerlaubte Handlung nicht einer einzelnen Person zugeordnet werden, diese somit auch nicht zur Verantwortung gezogen werden kann. Dies bedeutet allerdings auch, daß es den „unschuldigen" Mitarbeitern der Arbeitseinheit auch nicht möglich ist, ggf. den Unschuldsbeweis anzutreten.

Während alle „normalen" Benutzer in ihren Rechten begrenzt sind und durch Auswertung der Protokolldateien auch kontrollierbar sind, wird die „Allmacht" und die Unkontrollierbarkeit des Systemverwalters heute allgemein als selbstverständlich hingenommen; gegen unberechtigte Zugriffe des Systemverwalters sowie für die Möglichkeit seines Unschuldsbeweises hilft scheinbar nur das „Prinzip Vertrauen". Diese Situation ist für alle Beteiligten unbefriedigend, auch für den Systemverwalter selbst, denn bei jedem nicht oder nicht vollständig aufgeklärten Mißbrauchsfall wird er allein aufgrund seiner Möglichkeiten zwangsläufig in Verdacht geraten.

In aller Regel ist aber an dieser Situation derzeit nichts zu ändern, weil die eingesetzten Betriebssysteme hierzu keine Möglichkeiten bieten.

Beschränkung und Kontrolle des Systemverwalters sind dort in aller Regel nicht vorgesehen. Allerdings gibt es mittlerweile für bestimmte Rechner und APC-Netze Zusatzsoftware mit der Möglichkeit, die Befugnisse des Systemverwalters zu beschränken, sie auf mehrere Personen zu verteilen und Protokolle zu führen, die ihm nicht oder nur gemeinsam mit anderen zugänglich sind. Es gibt vereinzelt auch schon Betriebssysteme, die über solche Funktionen verfügen. Den Zugang zu dem dort entstehenden Protokoll hat nur ein besonderer Benutzer (Sonderuser, Revisor oder Datenschutzbeauftragter). Dieser wertet die Protokolle aus und kontrolliert somit den Systemverwalter. Meist hat er seinerseits keine anderen Rechte im System. Der Sonderuser muß natürlich gute Systemkenntnisse haben, um die Protokolle qualifiziert auswerten zu können. Leider werden derartige Betriebssysteme bisher nur in Ausnahmefällen

eingesetzt. Die Hersteller, die solche Systeme auf den Mark bringen, klagen über einen schlechten Absatz. Die speichernde Stelle ist bei der Verarbeitung personenbezogener Daten nach § 9 Bundesdatenschutzgesetz aber verpflichtet, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen des Gesetzes zu gewährleisten. Der Aufwand muß dabei in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen. Der für die Datenverarbeitung Verantwortliche hat also abzuwägen, ob das Verfahren so schutzwürdig ist, daß eventuell anfallende höhere Kosten gerechtfertigt sind. Nach meiner Einschätzung ist die unkontrollierte volle Zugriffsmöglichkeit des Systemverwalters sehr problematisch. Dies gilt insbesondere dann, wenn es sich um besonders schutzbedürftige personenbezogene Daten handelt, also etwa solche, die einem besonderen Amtsgeheimnis unterliegen, wie Personaldaten von Arbeitnehmern oder Sozialdaten.

30.8 Es muß nicht immer ein Safe sein – „Grundschutz" für die Informationstechnik

Das Bundesdatenschutzgesetz verlangt von jeder Stelle, die personenbezogene Daten verarbeitet, die erforderlichen technischen und organisatorischen Maßnahmen zu treffen, um die gesetzlichen Anforderungen zu gewährleisten (§ 9).

Die aus datenschutzrechtlicher Sicht von der verantwortlichen – der „speichernden" – Stelle zu fordernden Maßnahmen betreffen lediglich die Verarbeitung personenbezogener Daten, allerdings nicht nur in automatisierter, sondern auch in manueller Form. Lediglich die in der Anlage zu § 9 BDSG aufgeführten „10 Gebote der Datensicherung" gelten nur für automatisierte Verarbeitung.

Demgegenüber muß **jedes** – heute stets automatisiert betriebene – System der Informationstechnik Anforderungen im Hinblick auf Informationssicherheit erfüllen, die von der Art der verarbeiteten Daten, den bedrohenden Risiken und den Folgen des Eintrittes des Risikofalles abhängen. Die „Richtlinien für den Einsatz der Informationstechnik in der Bundesverwaltung (IT-Richtlinien)" des Bundeskabinetts vom 18. August 1988 fordern daher sowohl eine Risikoanalyse als auch – darauf aufbauend – Vorkehrungen zur Gewährleistung der Vollständigkeit, Richtigkeit und Aktualität der zu verarbeitenden Daten („Nr. 10: Sicherheit beim Einsatz der IT").

Das BSI hat 1992 im Auftrag der Bundesregierung ein „Handbuch für die sichere Anwendung der Informationstechnik (IT-Sicherheitshandbuch)" herausgegeben, das ein wertvolles Hilfsmittel zur Abschätzung der vorhandenen und zur Schaffung einer angemessenen Sicherheit darstellt. Die Anwendung des IT-Sicherheitshandbuches ist jedoch insbesondere zur Erstellung einer Risikoanalyse mit erheblichem Aufwand verbunden, der für Daten mit geringem und mittleren Schutzbedarf nicht immer angemessen ist. Zur Gewährleistung der IT-Sicherheit in Anwendungen, in denen Daten mit geringem und mittlerem Schutzbedarf verarbeitet werden, hat das BSI daher ein Konzept entwickelt, das Niederschlag im „IT-Grundschutzhandbuch" gefunden hat. Das im Juli 1994 vorgelegte IT-Grundschutzhandbuch ist als Loseblattwerk konzipiert und enthält zunächst nur Maßnahmen für die IT-Sicherheit von dezentralen IT-Systemen, insbesondere Stand-alone-PC und TK-Anlagen. Eine erste Bewertung des IT-Grundschutzhandbuches hat aus meiner Sicht bestätigt, daß das zugrundeliegende Konzept sowie die vorgeschlagenen Schutzmaßnahmen grundsätzlich gut geeignet sind, den verpflichteten Stellen wirksame Hilfen bei den zu treffenden Maßnahmen zu geben. Dabei gehe ich davon aus, daß für **jedes** IT-System, in dem personenbezogene Daten verarbeitet werden oder das hierfür geeignet ist, die für dieses System vom Grundschutzhandbuch empfohlenen Maßnahmen realisiert werden müssen. In Abhängigkeit vom Schutzbedarf der Daten einerseits, der technisch-organisatorischen Umgebung der Verarbeitung andererseits können über den Grundschutz hinausgehende Maßnahmen erforderlich sein („Grundschutz + x"); dies ist im Einzelfall zu prüfen. So wird z. B. bei der Verarbeitung besonders sensibler Daten häufig deren kryptografische Verschlüsselung geboten sein (vgl. 14. TB S. 149).

Das für die IT-Sicherheit zuständige Bundesministerium des Innern beabsichtigt, nach einer Erprobungsphase des IT-Grundschutzhandbuches bis Anfang 1995 im Einvernehmen mit dem Interministeriellen Koordinierungsausschuß für Informationstechnik in der Bundesverwaltung (IMKA) eine allgemeine Empfehlung zur verbindlichen Anwendung des Handbuches herauszugeben.

31 Entwicklung des allgemeinen Datenschutzrechts

31.1 Datenschutz im Grundgesetz

Um für die Bürger und Bürgerinnen deutlich zu machen, daß unsere Verfassung ihr Recht auf Datenschutz in gleicher Weise garantiert wie die traditionellen Grundrechte, habe ich zusammen mit den Landesbeauftragten empfohlen, das Recht auf informationelle Selbstbestimmung in den Grundrechtskatalog aufzunehmen (so zuletzt auf der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 10./11. März 1994). Zu meinem Bedauern ist es hierzu nicht gekommen.

Der verfassungsrechtliche Rang und die grundrechtliche Qualität des Rechts auf informationelle Selbstbestimmung sind zwar inzwischen unbestritten – nicht zuletzt dank der konsequenten Judikatur des Bundesverfassungsgerichts und der Rechtsprechung insgesamt. Das von den Gegnern einer Grundgesetzergänzung vorgebrachte Argument, ein ausdrückliches Datenschutzgrundrecht sei damit überflüssig, erscheint mir aber zu kurz gegriffen. Eine Verfassung hat nach allgemeiner Überzeugung nicht nur die rein juristische Aufgabe, offene Fragen zu regeln, sondern daneben die nicht minder wichtige politische Funktion, gemeinsamen Überzeugungen und Werten Ausdruck zu geben und dadurch den gesellschaftlichen Zusammenhang zu unterstützen. Angesichts der enormen und weiter zunehmenden Bedeu-

tung der Informationstechnik für Wirtschaft und Verwaltung und ihres breiten Einzugs auch in den privaten und familiären Bereich wäre die Aufnahme eines Datenschutzgrundrechts der adäquate Ausdruck des politischen Willens, den freiheitlichen Grundwerten auch gegenüber dieser so enorm durchsetzungskräftigen, aber auch prägbaren Technologie zur Geltung zu verhelfen.

Nachdem sich in der gemeinsamen Verfassungskommission des Bundestages und des Bundesrates zwar eine Mehrheit, aber keine Zwei-Drittel-Mehrheit für eine positive Beschlußempfehlung gefunden hatte (vgl. 14. TB Nr. 31.2), war auch die Entscheidung des Bundestages negativ.

Die Verfassungsgeber der neuen Bundesländer waren insoweit aufgeschlossener und haben, wenn auch mit unterschiedlichen Formulierungen und unterschiedlichem Regelungsumfang, die Problematik des Umgangs mit der modernen Informationstechnik unter dem Gesichtspunkt der Selbstbestimmung angesprochen. Sie sind damit den Verfassungen einer Reihe europäischer Staaten gefolgt. Für das Grundgesetz wurde eine gute Gelegenheit für eine zeitgemäße Erweiterung des Grundrechtskatalogs versäumt, was nicht nur aus der Sicht des Datenschutzes zu bedauern ist.

31.2 Grundprobleme bei der Anwendung des BDSG

31.2.1 Dienst- und Fachaufsicht begrenzen Vertraulichkeit der persönlichen Beratung

Aus verschiedenen Bundesbehörden wurde – teilweise vermittelt durch den behördlichen Datenschutzbeauftragten und die Personalvertretung – die Frage an mich herangetragen, ob und in welchem Umfang Informationen, die die Mitarbeiter einem behördlichen Sozialdienst anvertraut haben, im Rahmen der Dienst- und Fachaufsicht von den Angehörigen des Sozialdienstes deren Vorgesetzten bekanntgegeben werden müssen. Insbesondere war die Frage, ob Aufzeichnungen, aus denen die beratenen Mitarbeiter und die Themen der Beratung ersichtlich sind, zur Überprüfung der Qualität und Quantität der Arbeit der Berater vorzulegen sind. Gegen solche Forderungen hatten sich Angehörige der Sozialdienste gewandt und waren darin von ihrer Personalvertretung unterstützt worden.

Ein Sozialer Dienst besteht bei großen Bundesbehörden; mitunter ist der soziale Dienst für alle Behörden einer Region bei einer einzelnen Behörde konzentriert. Der Soziale Dienst kann mit dem Ärztlichen Dienst organisatorisch zusammengefaßt sein. Der Soziale Dienst unterstützt Bedienstete nicht nur im wirtschaftlichen und sozialen Notsituationen, sondern auch im persönlichen-psychologischen Bereich und umfaßt insofern auch therapeutische Elemente. Regelmäßig werden daher neben Sozialarbeitern auch Sozialpädagogen und Psychologen im Sozialen Dienst beschäftigt. Zu den typischen Gefährdungslagen, in denen der Soziale Dienst in Anspruch genommen werden kann, gehören Alkohol- und Medikamentenmißbrauch sowie Beziehungskonflikte im Verhältnis zu Kollegen, Vorgesetzten und Mitarbeitern.

Bei dieser Art der Tätigkeit liegt es auf der Hand, daß der Erfolg des Sozialen Dienstes wesentlich davon abhängt, daß der einzelne sich dem Mitarbeiter des Sozialen Dienstes in umfassender Weise anvertrauen kann, ohne befürchten zu müssen, daß seine persönlichen Angelegenheiten anderen Behördenangehörigen, insbesondere Vorgesetzten und Kollegen, bekannt werden. Wäre die Vertraulichkeit nicht gewährleistet, könnte der Soziale Dienst einen wesentlichen Teil seiner Aufgaben nicht erfüllen, weil seine Dienste von den hilfebedürftigen Mitarbeitern nicht in Anspruch genommen würden. Daher ist es sachgerecht, wenn dieses Vertrauensverhältnis mit dem einzelnen Berater besteht und nicht etwa mit der Gesamtheit der Mitarbeiter des Sozialen Dienstes.

Im geschriebenen Datenschutzrecht findet sich keine für diese Situation genau passende Regelung.

Das BDSG geht zwar vom Grundsatz der Zweckbindung aus (§ 14 Abs. 1); es betrachtet jedoch gerade die Verwendung personenbezogener Daten für die Wahrnehmung von Aufsichts- und Kontrollbefugnissen nicht als Zweckentfremdung (§ 14 Abs. 3). Auch die Übermittlungsvorschriften greifen nicht, da die Vorgesetzten im Verhältnis zu den Beratern keine Dritten sind. Eine strikte Zweckbindung verlangt das BDSG nur für personenbezogene Daten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden (§ 13 Abs. 4).

Auf der Ebene des bereichsspezifischen Datenschutzes ist das Berufsgeheimnis der „Berufspsychologen mit staatlich anerkannter wissenschaftlicher Schlußprüfung", der „staatlich anerkannten Sozialarbeiter" und „der staatlich anerkannten Sozialpädagogen" zu beachten, dessen Verletzung in gleicher Weise strafbewehrt ist, wie die des Arztgeheimnisses (§ 203 Abs. 1 Nrn. 2 und 5 StGB). Allerdings hat das Bundesministerium für Verteidigung geltend gemacht, wer sich wegen einer Beratung an den Sozialdienst wende, vertraue sich nicht dem individuellen Berater an, sondern nehme die Dienstleistung einer Behörde in Anspruch, die dann von den nach der Geschäftsverteilung „zuständigen" Behördenangehörigen im Namen der Behörde erbracht werde, wie es auch bei der Erfüllung anderer Behördenaufgaben der Fall sei. Andere Angehörige einschließlich des Leiters des Sozialen Dienstes könnten deshalb jedenfalls insoweit unterrichtet werden, als sie derselben beruflichen Schweigepflicht unterliegen. Die Dienst- und Fachaufsicht sei der Behördenorganisation immanent und berechtige zur uneingeschränkten Einsicht in alle bei der Aufgabenerfüllung anfallenden Unterlagen sowie zur Befragung der beaufsichtigten Mitarbeiter, so daß das Offenbaren der dem Berufsgeheimnis unterliegenden Angaben nicht „unbefugt" im Sinne des Strafgesetzbuchs erfolge.

Aus meiner Sicht ist das Vertrauensverhältnis zwischen dem einzelnen und dem Sozialen Dienst, soweit dieser in persönlichen Problemlagen in Anspruch genommen wird, schutzbedürftig und zwar

im Hinblick auf den besonders sensiblen Charakter der personenbezogenen Daten, die in diesem Rahmen notwendigerweise mitgeteilt werden, grundsätzlich mit Vorrang vor den Belangen der Dienst- und Fachaufsicht. Die Dienst- und Fachaufsicht kann m. E. durchaus in einer Weise gestaltet und wahrgenommen werden, daß sie mit dem Grundsatz der persönlichen Vertraulichkeit vereinbar ist.

Im einzelnen empfehle ich bei dem Betrieb des Sozialen Dienstes folgendes:

- Den Bediensteten sollte durch Rundschreiben oder in anderer geeigneter Form deutlich gemacht werden, daß sie die einzelnen mit der in Beratung betrauten Angehörigen des Sozialen Dienstes ganz persönlich und vertraulich in Anspruch nehmen können und daß die insoweit offengelegten Informationen aus dem persönlichen Lebensbereich von dem betreffenden Berater uneingeschränkt vertraulich behandelt werden.
- Die Berater sollten ausdrücklich angewiesen werden, die ihnen anvertrauten personenbezogenen Daten anderen Personen – gleich ob Angehörige des Sozialen Dienstes, der Anstellungsbehörde oder Dritte – nur auf ausdrücklichen Wunsch der beratenen Person bekanntzugeben.
- Die Dienst- und Fachaufsicht sollte so organisiert werden, daß dabei keine personenbezogenen Daten aus dem persönlichen Lebensbereich der Bediensteten, die den Sozialen Dienst in Anspruch genommen haben, offengelegt werden. Soweit dies für Zwecke der Aufsicht erforderlich ist, können die Berater angewiesen werden, Aufzeichnungen über ihre Tätigkeit in nicht personenbezogener Form zu erstellen. Auch soweit eine begleitende fachliche Kontrolle notwendig ist – wie z. B. eine Supervision durch einen Fachkollegen im Falle einer Beratung mit psychotherapeutischem Einschlag –, sollte dies in nicht personenbezogener Form erfolgen. Läßt es sich aus praktischen Gründen nicht vermeiden, daß die Identität der beratenden Person erkennbar wird, so ist die Zustimmung des Betroffenen erforderlich.

Hält eine Behörde daran fest, daß die Vertraulichkeit innerhalb des Sozialen Dienstes durch Dienst- und Fachaufsicht und durch Vertretungsregelungen eingeschränkt sein soll – wofür ich eine durchgreifende Begründung nicht erkennen kann –, so muß aus meiner Sicht diese Gestaltung den Mitarbeitern vor Beginn einer Beratung deutlich gemacht werden. Nachdem das Bundesministerium der Verteidigung auch dies abgelehnt hat, habe ich eine Beanstandung nach § 25 Abs. 1 BDSG ausgesprochen.

31.2.2 Behördlicher Datenschutzbeauftragter – Modellvorschlag

Die Bestellung eines Datenschutzbeauftragten ist eine der wichtigsten organisatorischen Maßnahme zur Sicherstellung des Datenschutzes auf der Ebene der datenverarbeitenden Stellen. Sie ist jedoch bis heute nicht flächendeckend gesetzlich vorgeschrieben. Während die Mehrzahl der neueren Landesdatenschutzgesetze wie auch das Sozialgesetzbuch jeweils für ihren gesamten Anwendungsbereich die Bestellung interner Datenschutzbeauftragter fordern, verlangt das Bundesdatenschutzgesetz dies nur im nicht-öffentlichen Bereich.

Dennoch haben die meisten Bundesbehörden einen internen Datenschutzbeauftragten bestellt. Da es aber an gesetzlichen Vorgaben fehlt, sind Stellung, Aufgaben und Befugnisse recht unterschiedlich, teils aber auch nur lückenhaft, festgelegt. Dadurch besteht eine verbreitete Unsicherheit, die sich nachteilig auf die praktische Arbeit auswirkt und mitunter zu Reibungsverlusten führt.

Ich habe deshalb Empfehlungen für die Behördenleitungen und die Datenschutzbeauftragten ausgesprochen und unter dem Titel „Der behördliche Datenschutzbeauftragte" als Nummer 4 der Schriftenreihe BfD-Info veröffentlicht. Die Resonanz ist sehr positiv.

Erfreulicherweise findet das Modell des Datenschutzbeauftragten, das in gesetzlicher Form bisher nur in Deutschland verankert ist, zunehmend auch auf internationaler Ebene Anerkennung. Bei den Beratungen zur EG-Datenschutzrichtlinie konnte die deutsche Seite die anderen Partner davon überzeugen, daß für die praktische Durchsetzung der Datenschutzvorschriften die Bestellung eines internen Datenschutzbeauftragten grundsätzlich ein ebenso geeignetes und wirksames Mittel darstellen kann wie die Anmeldung der Dateien bei einer Datenschutz-Aufsichtsbehörde. Der Richtlinienentwurf bietet nunmehr beide Möglichkeiten als grundsätzlich gleichwertige Alternativen an.

31.2.3 Elektronische Textverarbeitung: meldepflichtige Datei?

Die Anwendung des Bundesdatenschutzgesetzes auf die elektronische Textverarbeitung hat in der Praxis zu einigen Schwierigkeiten geführt. Viele öffentliche Stellen haben bei mir angefragt,

- ob die elektronische Textverarbeitung in den Anwendungsbereich des BDSG falle,
- ob jedes einzelne Dokument oder nur die Gesamtheit der im System verarbeiteten Dokumente und ob die vom System selbsttätig gespeicherten Daten jeweils eine Datei im Sinne des BDSG darstellen,
- ob und in welcher Form diese Dateien mir zur Aufnahme in das öffentliche Dateienregister zu melden seien.

Aus meiner Sicht kommt es darauf an, auf der einen Seite die Textverarbeitung wegen der mitunter erheblichen Sensibilität der dabei verarbeiteten personenbezogenen Daten nicht etwa aus dem Schutzbereich des Gesetzes auszuschließen, auf der anderen Seite aber in bezug auf die Registermeldungen keine überzogenen Anforderungen zu stellen. In diesem Sinne habe ich einige Grundsätze aufgestellt und durch Rundschreiben vom 23. 11. 1993 an die obersten Bundesbehörden bekanntgegeben (abgedruckt als Anlage 22). Die Grundsätze sind allgemein akzeptiert worden und werden in der Praxis berücksichtigt.

32 Nicht-öffentlicher Bereich

Den Meinungs- und Erfahrungsaustausch der obersten Datenschutz-Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich (Düsseldorfer Kreis) habe ich verfolgt und mich an der Diskussion über Einzelfragen, die auch meinen Bereich betrafen, beteiligt.

32.1 Umgehung des Datenschutzes: Vermieter verlangen Schufa-Selbstauskünfte von Mietinteressenten

Den Aufsichtsbehörden sind vermehrt Fälle bekannt geworden, in denen Vermieter von den Mietinteressenten wie auch von Bürgen die Vorlage einer Schufa-Selbstauskunft verlangten. Hiergegen haben die Aufsichtsbehörden ganz überwiegend erhebliche datenschutzrechtliche Bedenken.

Vertragspartner der Schufa – und damit Nutzer ihrer Daten – können nur Unternehmen sein, die gewerbsmäßig Geld- oder Warenkredite an Konsumenten geben. Diese Beschränkung ist der aus Datenschutzgründen notwendige Ausgleich dafür, daß die kreditgebende Wirtschaft ihre Privatkunden mittels der sog. Schufa-Klausel in einheitlicher und umfassender Weise der Verarbeitung ihrer Daten im Schufa-System unterwirft. Eine Einwilligung zur unbegrenzten Datennutzung könnten die Kreditgeber nicht verlangen. Diese Grundsätze werden mit der genannten Praxis umgangen. Zudem wird der Sinn des Auskunftsrechts (§ 34 BDSG), dem Betroffenen die Tätigkeit von Unternehmen wie der Schufa transparent zu machen und ihm dadurch die Möglichkeit zur Wahrnehmung seiner Rechte und Interessen zu geben, offensichtlich pervertiert.

Einen noch gravierenderen Fall gab es auch in meinem Kontrollbereich. Eine private Sicherheitsfirma hatte ihre Stellenbewerber aufgefordert, beim Bundeskriminalamt Anträge auf Auskunft über ihre dort gespeicherten Daten zu verlangen (§ 19 BDSG). Da die Firma den Bewerbern ein entsprechendes Formular zur Verfügung gestellt und einen Teil der Briefe mit dem firmeneigenen Freistempler frankiert hatte, konnte das BKA den Hintergrund erkennen. Im BKA, das mich erfreulicherweise sogleich unterrichtete, war zunächst erwogen worden, den Auskunftssuchenden lediglich eine Einsichtnahme in die Unterlagen anzubieten. Freilich hätte das die betroffenen Mitbewerber gegenüber ihren Konkurrenten, deren Auskunftsersuchen erfüllt wurden, benachteiligt und hätte die betreffenden Unternehmen anspornen können, generell „geschickter" vorzugehen. Mit meinem Einvernehmen hat das BMI daher das betreffende Sicherheitsunternehmen unter Hinweis auf die Rechtslage aufgefordert, von seiner Verfahrensweise Abstand zu nehmen. Weitere Fälle sind dann – soweit erkennbar – nicht mehr aufgetreten.

Einzelne Aufsichtsbehörden sind für den Bereich Schufa-Selbstauskünfte ähnlich vorgegangen. Andere sehen sich allerdings zu einer rechtsverbindlichen Aufforderung an die betroffenen Vermieter außerstande, da die Rechtswidrigkeit der Forderung, eine Schufa-Selbstauskunft vorzulegen, nach dem BDSG nicht zweifelsfrei sei. Zwar sei das Vermieterverlangen nicht durch die Schufa-Richtlinien gedeckt und unterlaufe denm gesetzlichen Sinn des Auskunftsrechts, so daß die Datenerhebung nicht nach Treu und Glauben und auf rechtmäßige Weise erfolge (§ 28 Abs. 1 Satz 2 BDSG). In den meisten Fällen nähmen die Vermieter die Schufa-Auskunft lediglich zur Kenntnis, ohne die erlangten Daten in einer Datei zu speichern; daher erfolge auch die Datenerhebung nicht „in oder aus einer Datei", wie es das BDSG im nicht-öffentlichen Bereich voraussetze (§§ 1 Abs. 2 Nr. 3, 27 Abs. 1). Diese Auffassung berücksichtigt m. E. allerdings zu wenig, daß eine dateimäßige Verarbeitung der Selbstauskunft aufgrund der objektiven Eignung regelmäßig nicht ausgeschlossen werden kann. Darüber hinaus wirkt sich die Auskunft regelmäßig auf die Entscheidung über den Vertragsabschluß aus und geht damit im Falle des Abschlusses als implizites Datum (etwa i. S. „Auskunft positiv") in die Datenspeicherung mit ein. Schließlich läßt sich die Anwendbarkeit des BDSG damit begründen, daß die Auskunftsdaten „offensichtlich aus einer Datei entnommen worden sind" (§ 27 Abs. 2 BDSG). Sollte sich diese Auffassung aber nicht durchsetzen lassen, wäre eine Gesetzeskorrektur – sei es durch Änderung des BDSG, sei es durch ein Kreditauskunfteigesetz – unumgänglich, wenn der Datenschutz nicht in einem entscheidenden Punkt unwirksam bleiben soll.

32.2 Datenweitergabe für Kundenwerbung im Rahmen von Allfinanzkonzepten nur mit Einwilligung

Die Arbeitsgruppen Versicherungswirtschaft und Kreditwirtschaft des Düsseldorfer Kreises haben sich weiterhin mit den sog. „Allfinanzkonzepten" befaßt (s. schon 14. TB Nr. 32.5). Um den Kunden die gesamte Palette von Finanz- und Versicherungsdienstleistungen rationell und kostengünstig anbieten zu können, arbeiten Versicherungsunternehmen mit Banken und Bausparkassen, aber auch mit Unternehmen zusammen, die sich ausschließlich auf die Vermittlung entsprechender Dienstleistungen spezialisiert haben. Die Werbung für weitere Dienstleistungen innerhalb eines Verbundes bzw. Konzernes macht die Weitergabe der Daten aus einer bestehenden Vertragsbeziehung erforderlich. Da eine derartige Übermittlung normalerweise nicht mehr im Rahmen dieses Vertragsverhältnisses liegt, ist eine ausdrückliche Einwilligung des Kunden erforderlich. In Zusammenarbeit mit der Arbeitsgruppe Versicherungswirtschaft hat der Gesamtverband der Deutschen Versicherungswirtschaft im Mai 1994 eine neue Einwilligungsklausel erstellt, die Datenschutzbelange in ausreichendem Maße berücksichtigt. Mit Blick hierauf sollen nun auch für die Banken und Bausparkassen im Verbund bzw. Konzern solche Klauseln erarbeitet werden. Aufgrund der teils unterschiedlichen Sachverhalte ist eine direkte Übertragung der mit der Versicherungswirtschaft erreichten Ergebnisse nicht möglich. Die Gespräche mit den Vertretern der Kreditwirtschaft dauern derzeit noch an. Der Düsseldorfer Kreis ist auch hier bestrebt, ausreichend den Datenschutz zu sichern. So sollen die Klauseln kenntlich machen, welche Unternehmen im

Verbund bzw. Konzern zusammengeschlossen sind und als Datenempfänger in Betracht kommen. Daneben soll konkret benannt werden, welche Daten übermittelt werden und aus welchem Anlaß dies geschieht. Desweiteren ist ein klarer Hinweis auf die jederzeitige Widerruflichkeit der Einwilligung erforderlich. Schließlich soll der Klausel ein ausführliches Merkblatt beigefügt werden, um den Kunden die Bedeutung und Tragweite ihrer Einwilligung zu verdeutlichen.

32.3 Mehr Transparenz beim Direktmarketing/Adreßhandel

Daß nach wie vor Probleme beim Vollzug der Vorschriften des BDSG bestehen, zeigt die Erfahrung mit dem Direktmarketing, insbesondere dem Adreßhandel. Bei dieser Art der Werbung entspricht eine kundenscharfe Selektierung zwar den wirtschaftlichen Bedürfnissen der Branche, die daher auf möglichst ausdifferenzierte Werbelisten potentieller Kunden angewiesen ist. Der Adreßhandel erfüllt dieses Bedürfnis, indem er nach mehreren Selektionsdaten ausgewählte Adressenstämme (etwa von der Art „kaufkräftige Frührentner mit Englischkenntnissen in Süddeutschland") für Werbezwecke anbietet oder für die jeweiligen Unternehmen im Rahmen einer Geschäftsbesorgung selbst nutzt oder vom Datenbesitzer nutzen läßt. Der Gesetzeswortlaut läßt aber eine beliebig tiefe Differenzierung von Kundendaten grundsätzlich nicht zu. In § 29 Abs. 2 Nr. 1 b i.V. m. § 28 Abs. 2 Nr. 1 b BDSG sind die einzelnen Daten benannt, die über die Angehörigkeit zu einer Personengruppe hinaus als Auswahlkriterium bei der Übermittlung oder Nutzung berechtigterweise verwendet werden dürfen. Wenn es gleichwohl nicht übermäßig viele spezifizierte Beschwerden gibt, so wohl vor allem deswegen, weil für den Betroffenen meist nicht erkennbar ist, von welcher Stelle die verwendeten Daten stammen, und er daher auch nicht weiß, wo er sein Widerspruchsrecht ausüben soll. Längst nicht alle Adreßhandelsunternehmen sind der sog. Robinson-Liste angeschlossen, bei welcher man seinen Widerspruch zentral einlegen kann.

Die Kontrolle durch die Aufsichtsbehörden gestaltet sich in der Praxis schwierig, weil die Sachverhalte nachträglich nur schwer rekonstruiert werden können und regelmäßig mehrere Unternehmen – oft aus unterschiedlichen Bundesländern – beteiligt sind. Dennoch erscheint es mir wichtig, weiter abzuklären, ob hier ein breites Datenschutzdefizit besteht, um ggf. auf Korrektur zu drängen. Auch wird die Frage gestellt werden können, ob die mit § 28 Abs. 2 getroffene Lösung die beiderseitigen Interessen sachgerecht miteinander in Einklang gebracht hat. Die EG-Richtlinie könnte hier ohnehin Anlaß zu einer Prüfung geben.

32.4 Bereichsspezifische Regelungen für den Arbeitnehmerdatenschutz dringend erforderlich

Nach wie vor bereitet den Aufsichtsbehörden die Thematik des Arbeitnehmerdatenschutzes beträchtliche Schwierigkeiten. Die Vorschriften des BDSG sind oftmals nicht genügend präzise und differenziert. Selbst unkompliziert erscheinende Einzelfragen, wie etwa die firmeninterne Bekanntgabe von Krankheitszeiten, Ausbildungsergebnissen und „Rennlisten" oder die Auskunft des bisherigen an den künftigen Arbeitgeber oder die Übermittlung von Arbeitnehmerdaten werfen erhebliche Auslegungsprobleme auf oder provozieren Versuche, die Angelegenheit durch – mitunter routinemäßig eingeholte – Einwilligungen zu lösen. Da die Freiwilligkeit der Einwilligung wegen der in Arbeitsverhältnissen häufig bestehenden Abhängigkeit zweifelhaft ist, ist dieser Weg juristisch aber keineswegs tragfähig – ganz abgesehen von seiner datenschutzmäßigen Kontraproduktivität.

Die Vorschriften der §§ 90 f. BBG, § 56 f. BRRG (eingefügt durch das Neunte Dienstrechtsänderungsgesetz, in Kraft getreten am 1. Januar 1993) haben für Beamte einen bereichsspezifischen Datenschutz geschaffen. Niemand wird freilich behaupten wollen, für die Angestellten und Arbeiter des öffentlichen Dienstes oder gar für die Arbeitnehmer in der Privatwirtschaft sei der Ausbau des Datenschutzes weniger dringlich. Die Bundesregierung hat einen entsprechenden Gesetzentwurf für die neue Legislaturperiode angekündigt (Antwort auf Kleine Anfrage der SPD-Fraktion, Drucksache 12/2948 vom 26. Juni 1992); der Deutsche Bundestag hatte die Bundesregierung schon im Februar 1992 dazu entsprechend aufgefordert (Beschlußempfehlung des Innenausschusses vom 21. Dezember 1993, Drucksache 12/4094 im Anschluß an ein entsprechendes Votum des Ausschusses für Arbeit und Sozialordnung vom 13. November 1991, vom Plenum beschlossen am 5. Februar 1993, Plenarprotokoll 12/138). Es ist dringend zu wünschen, daß das Vorhaben nunmehr die notwendige politische Priorität erhält.

32.5 Örtliche Beschränkung des bankinternen Zugriffs auf Kontoinformationen auf Kundenwunsch

Banken sind zur Wahrung des Bankgeheimnisses verpflichtet. Sie haben hinsichtlich aller kundenbezogenen Daten, die sie verarbeiten und nutzen, Verschwiegenheit zu wahren, auch innerhalb des jeweiligen Unternehmens. Die Berechtigung der Mitarbeiter von Kreditinstituten zum Zugriff auf Kontodaten der Kunden wird in der Praxis meist nur aufgabenbezogen definiert, nicht jedoch auf die einzelne Filiale oder Geschäftsstelle begrenzt, der Mitarbeiter angehören.

Dagegen haben sich mehrere Sparkassenkunden mit Eingaben an den LfD Rheinland-Pfalz gewandt. Wegen der örtlichen Nähe oder der persönlichen Bekanntschaft mit Mitarbeitern der Sparkasse ist manchen Kunden daran gelegen, daß nicht alle Informationen über ihre finanziellen Verhältnisse von allen Filialen aus zugänglich sind. Der LfD Rheinland-Pfalz hat daher vorgeschlagen, den Kunden eine Wahlmöglichkeit derart zu eröffnen, daß der Zugriff auf ihre Kontoinformationen auf Wunsch auf eine bestimmte Zweigstelle beschränkt wird; zentrale Aufgaben wie Rechnungswesen oder Revision können davon unberührt bleiben.

Während manche Kreditinstitute sich bereiterklärt haben, ihren Kunden eine solche Option einzuräumen, verweisen andere darauf, daß die durch ihr Filialnetz garantierte überregionale oder bundesweite Servicebereitschaft ein zentrales Element ihres Qualitätsprofils sei und deshalb nicht zur Disposition stehen könne. Dies trifft etwa auf die Postbank und auf die großen Geschäftsbanken zu. Soweit man insofern davon ausgehen kann, daß die Freizügigkeit im gesamten Filialnetz die Geschäftsbeziehung zum einzelnen Kunden von vornherein prägt, wird man dies auch bei der Anwendung von § 9 BDSG i.V. m. Nr. 10 der Anlage (Organisationskontrolle) beachten müssen.

Die Thematik wird von den Aufsichtsbehörden sowohl mit einzelnen Instituten wie auch mit den Verbänden weiter erörtert. Wenn – wie ich hoffe – ein wesentlicher Teil der Kreditinstitute sich bereitfinden wird, die erwähnte Option anzubieten, dürfte sich ein datenschutzrechtliches Einschreiten erübrigen.

33 Ausland und Internationales

33.1 EG-Datenschutzrichtlinie

33.1.1 Ratsgruppenvorsitz durch Bundesbeauftragten für den Datenschutz während der deutschen EU-Präsidentschaft

Die ursprüngliche Absicht der Europäischen Kommission, die Datenschutzrichtlinie (zu deren Inhalt und allgemeinen Problemen s. 13. TB S. 87 ff. sowie 14. TB S. 159 f.) noch vor Beginn des Europäischen Binnenmarktes, also zum Ende des Jahres 1992, in kraft zu setzen, konnte bekanntlich nicht verwirklicht werden. Auch während des gesamten Jahres 1993 wurden die Beratungen nicht abgeschlossen. Immerhin fanden die erste und eine darauffolgende zweite Durchsicht unter belgischer Präsidentschaft statt und konnten von meinem griechischen Kollegen im Vorsitz während der 1. Jahreshälfte 1994 zum Abschluß gebracht werden. Als ich am 1. Juli 1994 im Zuge der deutschen EU-Präsidentschaft auf Bitte des Bundesministeriums des Innern den Vorsitz in der Ratsgruppe „Wirtschaftsfragen/Datenschutz" übernahm, war allerdings noch kein einziger Artikel des Richtlinienvorhabens konsentiert, d. h. jede einzelne Vorschrift des Entwurfes stieß auf den Vorbehalt zumindest eines Mitgliedstaates. So mußte mein griechischer Vorgänger im Ratsgruppenvorsitz anläßlich der Amtsübergabe in Brüssel resignierend feststellen: „We agree to disagree". Umso erfreulicher war es daher, daß der „Gemeinsame Standpunkt des Rates" (Art. 189 b Abs. 2 Unterabs. 2 Satz 1 EG-Vertrag), der den entscheidenden Meilenstein im Beratungsverfahren der Richtlinie bildet, unter deutscher Präsidentschaft in greifbare Nähe gerückt war. Nachdem unter Ausschöpfung aller Kompromißmöglichkeiten – auch Dank des fortwährend hohen Einsatzes der Kommission – ein Konsens auf breiter Basis gefunden worden war, konnte nach nunmehr vierjähriger Beratungszeit der Gemeinsame Standpunkt formuliert und lediglich aus technischen Gründen nicht mehr im Jahre 1994 verabschiedet werden. Dies wurde am 20. Februar 1995 im Ministerrat – nunmehr unter französischer Präsidentschaft – nachgeholt.

In allen Phasen der Beratungen und Verhandlungen stand ich dabei mit der Bundesregierung, vertreten von dem die deutsche Delegation anführenden Bundesministerium des Innern, in engem Kontakt.

33.1.2 Problematische rechtliche Ausgangslage und angestrebte Lösungswege für den „Gemeinsamen Standpunkt des Rates"

Die rechtlichen Rahmenbedingungen für eine europaweite Harmonisierung des Datenschutzrechts waren nicht einfach. Dem Richtlinienentwurf lag, methodisch gesehen, ein Prinzip zugrunde, das Vorzug und Nachteil gleichermaßen in sich bergen mußte: Während er eine eigene Konzeption des Datenschutzes nicht versuchte, war er in seinen wesentlichen Teilen von europäischen Vorbildern geprägt, und zwar von der Europaratskonvention aus dem Jahre 1981 einerseits sowie einer Zusammenschau wesentlicher Grundgedanken bereits bestehender mitgliedstaatlicher Regelungen andererseits.

Es ist offensichtlich, daß eine derartige Kombination aus Teilen unterschiedlicher Konzepte des Datenschutzes Gefahren für die systematische Geschlossenheit des neu entstehenden Regelungswerkes nach sich ziehen konnte. Die bei den Beratungen aufgetretenen, bisweilen nahezu unüberbrückbar erschienenen Divergenzen wurden – wie bei vielen anderen Rechtssetzungsvorhaben der Gemeinschaft – nicht zuletzt dadurch angereichert, daß die damalige Zwölfergemeinschaft und nunmehr um drei weitere Mitglieder erweiterte Union aus Angehörigen des romanischen, des angelsächsischen, des nordischen und des deutschen Rechtskreises besteht, die unterschiedliche rechtliche Traditionen aufweisen. Damit wurde die Erreichung eines Kompromisses auch immer wieder dadurch erschwert, daß jeder Mitgliedstaat sich mit seinen rechtlichen Auffassungen möglichst umfassend in der Richtlinie „wiederfinden" wollte. Bezogen auf das Projekt der Datenschutzrichtlinie konnte allerdings eine bloße Kumulation der mitgliedstaatlichen Rechtspositionen schon aus Gründen der Redundanz und der darauf gegründeten Schwerfälligkeit nicht beabsichtigt sein.

Der Lösungsansatz ist im EG-Vertrag selbst zu suchen, nach dem eine Richtlinie für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Zieles verbindlich ist, jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel überläßt (Art. 189 Abs. 3).

Unter dieser Prämisse hat die Ratsgruppe neben einigen harmonisierungsbedingten Rechtsangleichungen zu verschiedenen Punkten zahlreiche alternative Lösungen erarbeitet, weil dies die meisten Erfolgsaussichten versprach. So wird es beispielsweise möglich sein, im Hinblick auf Unterschiede bei Organisation und Verfahren der Aufsichtsbehörden auch nach Inkraftsetzung der Datenschutzrichtlinie in Frankreich nach dem dort bewährten Muster und in Deutschland nach den hier gewachsenen Strukturen zu verfahren. Von der gleichen Intention war die Suche nach akzeptablen Regelungen zur Zulässigkeit

der Datenverarbeitung und den Rechten der Betroffenen getragen. Das wichtigste Ziel der Brüsseler Verhandlungen bestand darin, Rechtssicherheit für Bürger und Unternehmen zu schaffen und grenzüberschreitende Datenübermittlungen akzeptabel zu machen, weil in allen Mitgliedstaaten gemeinsame Regeln eingehalten werden.

Wenn bisweilen darauf verwiesen wird, daß der unterschiedlichen Integrationswilligkeit und Integrationsfähigkeit der Partnerländer durch flexiblere Strukturen Rechnung getragen werden müsse, so ist genau dies mit der Datenschutzrichtlinie in der vorliegenden Fassung des Gemeinsamen Standpunktes erreicht worden.

33.1.3 Erzielte Kompromisse und Folgerungen für das deutsche Datenschutzrecht im Überblick

Im Ergebnis kann man feststellen, daß das gemeinsame Ziel der Harmonisierung des europäischen Datenschutzes auf hohem Niveau erreicht wurde. So sind insbesondere die manuellen Dateien sowie Bild- und Tonaufzeichnungen in den Schutzbereich der Richtlinie einbezogen, und die Informations- und Auskunftsrechte der betroffenen Bürger sind umfassend gewährleistet. Ebenso ist der Ausgleich zwischen den Datenschutzinteressen und denen der Forschung gelungen; die Richtlinie sieht vor, daß die Mitgliedstaaten forschungsfreundliche Regelungen treffen dürfen – nicht in jedem Falle müssen –, wenn die Daten ausschließlich zur wissenschaftlichen Forschung oder für Statistiken genutzt werden und der Persönlichkeitsbereich der Betroffenen nicht beeinträchtigt wird. Die Richtlinie wird auch die künftige Weiterentwicklung des Datenschutzes nicht versperren, was insbesondere wegen der rasanten technischen Entwicklungen z. B. im Chipkartenbereich von großer Bedeutung ist.

Im Hinblick auf mögliche Änderungserfordernisse aufgrund der notwendigen Umsetzung der Richtlinie stehen wir sowohl beim BDSG als auch auf bereichsspezifischem Gebiet noch am Anfang der Überlegungen. Allerdings kündigt sich dank des schon vor Verabschiedung der Richtlinie anerkannt hohen Datenschutzniveaus in Deutschland kein grundlegender Wandel an. So bleibt die Einrichtung betrieblicher Datenschutzbeauftragter erhalten und bildet – auch für andere Mitgliedstaaten – eine Alternative zu umfangreichen Meldepflichten. Bezogen auf das Ausland wird das Ausweichen auf datenschutzfreie Zonen in Zukunft erschwert. Auch wird es zum Schutz des Persönlichkeitsrechts künftig gewisse Grenzen bei der Automatisierung von Entscheidungen geben.

33.1.4 Kernaussagen der Richtlinie zu den Grundfragen eines europäischen Datenschutzrechts

Die allgemeinen Grundgedanken finden sich in den Bestimmungen der Richtlinie wie folgt wieder:

1. Erhebung als Verarbeitungsform (Artikel 2 Buchstabe b)

   Die Richtlinie zählt im Rahmen der Begriffsbestimmungen – anders als das Bundesdatenschutzgesetz – auch das Erheben zur „Verarbeitung personenbezogener Daten".

   Gleichwohl bringt die Einbeziehung der Erhebung in den Begriff der Verarbeitung, die sich auch im privaten Sektor auswirkt, m. E. keine einschneidenden Änderungen mit sich. Denn im öffentlichen Bereich sind Zulässigkeit und Einzelheiten des Verfahrens der Erhebung ausdrücklich geregelt (§ 13 BDSG), und auch für den privaten Bereich ist schon jetzt vorgesehen, daß personenbezogene Daten „nach Treu und Glauben und auf rechtmäßige Weise" erhoben werden müssen (§ 28 Abs. 1 BDSG).

2. Begriff der Datei (Artikel 2 Buchst. c)

   Im BDSG 1977 war der Begriff der Akte nicht erwähnt, weil Akten und Aktensammlungen regelmäßig nicht dem Dateibegriff zugeordnet wurden. Nachdem das Erfordernis erkannt worden war, den Begriff der Akten näher festzulegen, enthält nunmehr § 3 Abs. 3 BDSG eine – weit gefaßte – Legaldefinition zum Aktenbegriff.

   Die Richtlinie regelt hingegen mit der Begriffsbestimmung des Artikels 2 Buchst. c lediglich den Begriff der Datei („Datei mit personenbezogenen Daten"). Akten fallen grundsätzlich nicht unter die Richtlinie. Auch der Inhalt von Akten, deren Deckblätter eine manuelle Datei bilden können, fällt definitiv nicht unter den Anwendungsbereich der Richtlinie. Die Mitgliedstaaten können jedoch in ihren Rechtsvorschriften präzisieren, unter welchen Gesichtspunkten manuelle Dateien zu einer strukturierten Sammlung gehören bzw. aufgrund welcher Kriterien eine solche Sammlung zugänglich sein muß.

3. Anwendbares einzelstaatliches Recht (Artikel 4)

   Bei der jetzigen Regelung, die vom Sitzprinzip ausgeht, sind umfangreiche Ausnahmen vorgesehen, so daß auch von einem abgeschwächten Territorialitätsprinzip gesprochen werden kann.

   Im Grundsatz sieht die Richtlinie vor, daß für die Datenverarbeitung, die ein Unternehmer mit Sitz in einem anderen Mitgliedstaat vornimmt, die Datenschutzgesetzgebung seines Landes gilt. Diesem reinen Sitzprinzip standen aber eine Reihe von Bedenken gegenüber. Eine Konsequenz läge nämlich darin, daß im Bereich des Datenschutzes fremdes Recht gelten würde, dagegen im Arbeitsrecht, Gewerberecht, Baurecht usw. aber das des Verarbeitungsortes. Die Kontrollstellen müßten europaweit fünfzehn verschiedene Datenschutzgesetzgebungen kennen und anwenden. Der Betroffene unterläge somit, je nach Sitz des Verantwortlichen, unterschiedlichen Datenschutzvorschriften.

   Das nunmehr vorliegende Mischmodell sieht deshalb vor, daß das Recht des Sitzlandes nicht gilt, wenn ein Unternehmen in einem anderen Mitgliedstaat eine auf Dauer eingerichtete, feste Niederlassung gründet. Das heißt, wenn dort nur eine Agentur oder Zweigstelle – auch ohne eigene Rechtspersönlichkeit – besteht, gilt das Recht des Verarbeitungsortes. Damit ist die große Mehrzahl der problematischen Fallgestaltungen, insbesondere im Arbeitsrecht, abgedeckt. Für die

Anwendung (orts-)fremden Rechts bleiben nur wenige Fälle, wie z. B. die Tätigkeit von Versicherungsvertretern ohne eigenes Büro, deren Unternehmenssitz in einem anderen Mitgliedstaat liegt.

4. Bewahrung eines höheren nationalen Schutzniveaus (Artikel 5)

   Zu den zentralen Punkten bei den Beratungen in der Ratsgruppe zählte die Frage nach der Bewahrung eines höheren nationalen Schutzniveaus. Hierbei ging es um die Forderung, daß Mitgliedstaaten mit besonders strengen Schutzvorschriften diese beibehalten und daß derartige Vorschriften neu geschaffen werden dürfen, wobei dieser strenge Standard auch bei Übermittlungen in andere Mitgliedstaaten zur Geltung gebracht werden darf. Es sollte, mit anderen Worten, sichergestellt werden, daß die Richtlinie einen hoch entwickelten nationalen Datenschutzstandard unberührt läßt. Diese von der deutschen Delegation vertretene Forderung der Bundesregierung habe ich als Vorsitzender nachdrücklich unterstützt.

   Dieses Anliegen mußte aus meiner Sicht seinen Niederschlag in einer unangreifbaren Formulierung des Richtlinientextes finden. Denn es ist nie ganz auszuschließen, daß es künftig einmal zu Meinungsverschiedenheiten über die Auslegung eines zur Zeit der Beratungen im Kompromißwege gefundenen Artikels kommt.

   Auch auf deutscher Seite bestanden Befürchtungen, die Formulierung in Artikel 5 (*„Die Mitgliedstaaten bestimmen ... die Voraussetzungen näher, unter denen die Verarbeitung personenbezogener Daten rechtmäßig ist."*) erlaube es den Mitgliedstaaten nicht klar genug, ein höheres Schutzniveau beizubehalten oder noch zu schaffen. Hier spielte besonders die Sorge mit, daß möglicherweise der Arbeitnehmer- und Sozialdatenschutz bedroht sein könnte. Ähnliche Besorgnisse bestanden in bezug auf Datenschutzregelungen der Tarifpartner und Regelungen auf Betriebsebene.

   Als Ergebnis langer und intensiver Beratungen enthält die Richtlinie nun auf deutschen Vorschlag hin in einem sog. Erwägungsgrund eine zufriedenstellende Lösung. Danach besitzen die Mitgliedstaaten einen Spielraum, der im Rahmen der Durchführung der Richtlinie auch von den Betriebs- und Sozialpartnern genutzt werden kann. Entsprechend dem Erwägungsgrund können die Mitgliedstaaten somit *„in ihrem einzelstaatlichen Recht allgemeine Bedingungen für die Rechtmäßigkeit der Verarbeitung festlegen, wobei sie eine Verbesserung des gegenwärtig durch ihre Rechtsvorschriften gewährten Schutzes anstreben."*

5. Verarbeitung sensibler Daten – Arbeitnehmer- und Sozialdatenschutz (Artikel 8)

   Da Daten aus dem Arbeitsverhältnis sowie Sozial- und Gesundheitsdaten schon aufgrund ihrer Art geeignet sind, in Grundfreiheiten einzugreifen oder die Privatsphäre zu beeinträchtigten, dürfen sie grundsätzlich nicht ohne ausdrückliche Einwilligung der betroffenen Person verarbeitet werden. Ausnahmen von diesem Verbot dürfen nur Hand in Hand mit geeigneten besonderen Garantien zum Schutz der Grundrechte und der Privatsphäre erfolgen. Das sind nach unserem Rechtsverständnis bereichsspezifische Datenschutzgesetze sowie – darauf beruhend oder auf Standesrecht gegründet – die Berufsgeheimnisse oder entsprechende Geheimhaltungspflichten.

   Artikel 8 Abs. 1 untersagt den Mitgliedstaaten die Verarbeitung personenbezogener Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von Gesundheitsdaten oder solchen, die das Sexualleben betreffen.

   Die Ausnahmen, die Art. 8 Abs. 2 und 3 für das Arbeits- und Sozialrecht (hier: die Gesundheitsdaten) zuläßt, sind mit den Grundsätzen des informationellen Selbstbestimmungsrechts vereinbar. Während die Verarbeitung arbeitsrechtlicher Daten ohne Einwilligung des Betroffenen nur zulässig ist, wenn das nationale Recht angemessene Garantien vorsieht, ist die Verarbeitung von Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten nur erlaubt, wenn sie durch ärztliches Personal erfolgt, das dem Berufsgeheimnis oder entsprechenden Geheimhaltungspflichten unterliegt.

6. Auskunfts- und Mitwirkungsrecht bei automatisierten Einzelentscheidungen (Artikel 15)

   Für weiteren, nicht unerheblichen Beratungsstoff sorgte das Problem der automatisierten Einzelentscheidungen. Im Hinblick auf die insbesondere für Frankreich wesentliche Vorschrift des Artikel 15, deren Anwendungsbereich in der Praxis aber wohl gering sein wird, wurde in einer Reihe von Sitzungen um Klarstellung gerungen. So ist der frühere Begriff *„Persönlichkeitsprofil"* dahingehend präzisiert worden, daß es um die *„Wertung einzelner Aspekte einer Person"* gehen muß *„wie beispielsweise ihre berufliche Leistungsfähigkeit, ihre Kreditwürdigkeit, ihre Zuverlässigkeit oder ihr Verhalten"*.

   Zu beachten ist, daß die Vorschrift dann greift, wenn eine Entscheidung vorliegt, die rechtliche Folgen für den Betroffenen nach sich zieht, und wenn diese Entscheidung ausschließlich aufgrund einer automatisierten Verarbeitung ergeht, die für bestimmte Zwecke erfolgt, ohne daß einer natürlichen Person die letzte Entscheidung vorbehalten wird.

   Wenn die automatisierte Einzelentscheidung nicht auf Ersuchen der betroffenen Person ergangen ist, kann sie ihre berechtigten Interessen z. B. dadurch wahren, daß sie ihren – u. U. gegenteiligen – Standpunkt zur Geltung bringt (Ar-

tikel 15 Abs. 2). In jedem Fall kann sie vom Verantwortlichen der Verarbeitung Auskunft über den logischen Aufbau der automatisierten Verarbeitung der sie betreffenden Daten erhalten. Dieses Recht kann sie frei und ungehindert, in angemessenen Abständen, ohne unzumutbare Verzögerung oder übermäßige Kosten geltend machen (Artikel 12 Nr. 1).

7. Meldepflicht (Artikel 18, 19)

Beim Thema Meldepflicht strebten der Vorsitz wie auch die deutsche Delegation von vornherein an, unverhältnismäßig umfangreiche Meldepflichten bei den Kontrollbehörden zu verhindern.

Die im Entwurf ursprünglich vorgesehene Kombination aus Prüfung der Rechtmäßigkeit einer personenbezogenen Datenverarbeitung und gleichzeitiger umfassender Pflicht zur Meldung aller Dateien entsprach in ersterem dem deutschen Recht und im letzterem der französischen und englischen Rechtslage.

Eine schlichte Kumulation beider Prinzipien konnte nicht in Frage kommen, da sie zu erheblichem Mehraufwand geführt hätte, ohne daß damit – zumindest in Deutschland – eine erkennbare Verbesserung des Datenschutzes für die Betroffenen verbunden gewesen wäre.

In schwierigen Verhandlungen konnte auch hierzu ein Kompromiß gefunden werden. Danach können die Mitgliedstaaten von umfassenden Meldepflichten absehen, wenn sie statt dessen zur wirksamen Vorabkontrolle die Einrichtung eines Datenschutzbeauftragten (im wesentlichen nach deutschem Vorbild) gewährleisten.

Auch hinsichtlich des Meldeverfahrens konnte ein Kompromiß erzielt werden, der auch den deutschen Belangen Rechnung trägt. Danach ist eine Befreiung von der Meldepflicht u. a. auch dann vorgesehen, wenn bei dem Verantwortlichen der Verarbeitung ein interner Datenschutzbeauftragter eine wirksame Selbstkontrolle der speichernden Stelle garantiert.

8. Haftung (Artikel 23)

Den als Haftungsfolge wegen einer rechtswidrigen Verarbeitung zu leistenden Schadensersatz regelt Artikel 23.

Da die Mitgliedstaaten bei Umsetzung dieser Vorschrift sowohl eine reine Gefährdungshaftung als auch eine verschuldensabhängige Haftung mit Beweislastumkehr einführen können, besteht aus deutscher Sicht kein Umsetzungsbedarf (vgl. Artikel 7 und 8 BDSG).

9. Übermittlung personenbezogener Daten in Drittländer (Artikel 25, 26)

Zentrale Punkte bei der Weitergabe personenbezogener Daten in Drittländer sind die Fragen des angemessenen Schutzniveaus im Drittland und die Möglichkeit von Ausnahmeregelungen bei dessen Nichtvorliegen.

Artikel 25 enthält hierzu die grundsätzlichen Bestimmungen, denen der Ausnahmenkatalog des Artikels 26 gegenübersteht.

Die Angemessenheit des Schutzniveaus beurteilt sich nach Artikel 25 Abs. 2 „unter Berücksichtigung aller Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen". Insbesondere werden neben der Art der Daten auch die Zweckbestimmung sowie die Dauer der geplanten Verarbeitung und ferner das Endbestimmungsland, die in dem Herkunftsland und dem betreffenden Drittland geltenden allgemeinen oder sektoriellen Rechtsnormen sowie die dort beachteten Standesregeln und Sicherheitsmaßnahmen berücksichtigt.

Von dieser Grundsatzposition ausgehend mußte sich die Ratsgruppe dem Problem der tatsächlichen Gegebenheiten und Umstände millionenfacher Datentransfers stellen. Die auf einen deutschen Vorschlag zurückgehende und von den Delegationen im wesentlichen gebilligte Formulierung des Artikel 26 sieht einen stark erweiterten Ausnahmenkatalog vor, der eine Übermittlung in Drittländer unabhängig von dem dort gesetzlich garantierten Schutzniveau in den meisten für die Praxis relevanten Fallgruppen ermöglicht. So kann abweichend von Artikel 25 ein Transfer personenbezogener Daten in ein Drittland ohne angemessenes Schutzniveau unter bestimmten Voraussetzungen vorgenommen werden und zwar bei

- zweifelsfreier Einwilligung der betroffenen Person,
- Vertragserfüllung oder Durchführung vorvertraglicher Maßnahmen,
- Abschluß oder Erfüllung eines Vertrages im Interesse der betroffenen Person,
- wichtigem öffentlichen Interesse,
- lebenswichtigen Interessen der betroffenen Person sowie
- unter bestimmten Voraussetzungen – bei Übermittlungen aus öffentlichen Registern.

Für den Fall, daß ein Datentransfer trotzdem noch Probleme aufwirft, kann ein Mitgliedstaat nach der Regelung des Artikel 26 Abs. 2 eine Übermittlung oder Kategorien von Übermittlungen genehmigen, wenn der Verantwortliche der Verarbeitung ausreichende Garantien hinsichtlich des Schutzes der betroffenen Personen erbringt.

Ingesamt läßt sich zur Weitergabe personenbezogener Daten in Drittländer festhalten, daß versucht wurde, Praxisnähe walten zu lassen, andererseits aber keinen Datenfransfer in Drittländer zuzulassen, der innerhalb der EU nicht gestattet wäre. Letztlich strebt die Richtlinie im Hinblick auf die Staaten außerhalb der EU eine internationale Harmonisierung an, so daß auch hier von einer „Festung Europa" nicht die Rede sein kann.

10. Status und Befugnisse der Kontrollbehörden (Artikel 28)

Die Einrichtung der Kontrollstelle und ihre Befugnisse regelt Artikel 28.

Nach dem ursprünglichen Richtlinienentwurf waren für die Kontrollbehörden, also für die Aufsichtsbehörden, die Landesbeauftragten oder für den Bundesbeauftragten für den Datenschutz nach deutschem Recht, sowohl ein unabhängiger Status als auch die Verleihung hoheitlicher Befugnisse vorgesehen. Eine derartige Verknüpfung mußte nach deutschem Verfassungsverständnis jedoch auf Bedenken stoßen. Denn den Kotrollbehörden mit unabhängigem Status (BfD und LfDs) stehen nach deutschem Recht nur ein Beanstandungsrecht zu sowie das Recht, sich jederzeit an das Parlament zu wenden. Hingegen stehen den Aufsichtsbehörden der Länder Eingriffsbefugnisse zu, mit denen sich ein unabhängiger Status aufgrund ihres hoheitlichen Wirkens wegen des Grundsatzes der parlamentarischen Verantwortung der Regierung verbietet.

Zur erzielten Problemlösung hat sich eine Formulierung durchgesetzt, die den deutschen Forderungen Rechnung trägt.

33.1.5 Zusammenfassende Bewertung und Ausblick

Als Resümee ist festzustellen, daß die Richtlinie den Herausforderungen der Gegenwart in einem europäischen Raum ohne Binnengrenzen in notwendiger und geeigneter Weise entspricht. Denn europäischer Datenschutz in harmonisierter, rechtsangeglichener Form ist dringender denn je und die Richtlinie in ihrer derzeitigen Gestalt des Gemeinsamen Standpunktes trägt in entscheidender Weise hierzu bei.

Im nationalen, innerstaatlichen deutschen Recht wird es zwar auch nach Inkrafttreten der Richtlinie keinen grundlegenden Wandel geben, und den Anwendern wird eine flächendeckende und kostenintensive Umstellung erspart bleiben. Insoweit kommt uns das anerkannt hohe Datenschutzniveau in Deutschland zugute.

Auf der anderen Seite werden wir aber mit den Regelungen über die Kontrollierbarkeit automatisierter Entscheidungen und über die Grenzziehung zwischen automatisierten und dem Menschen vorbehaltenen Entscheidungen neue Elemente aufnehmen, die gegenwärtig nur geringe Praxisrelevanz haben, jedoch die Prinzipien aussprechen, an denen sich unser Datenschutzdenken in der Zukunft wesentlich wird orientieren müssen.

Insgesamt bin ich sehr zuversichtlich, daß das Europäische Parlament jetzt – im zweiten Durchgang – der Richtlinie zustimmen kann. Denn wir haben uns auch aus eigener Überzeugung bemüht, seinen Forderungen und der Vielzahl von Änderungswünschen aus dem ersten Durchgang (s. 14. TB, S. 159) durch einen abgewogenen, aber aus Datenschutzsicht hochwertigen Gemeinsamen Standpunkt zu entsprechen.

33.2 Europäische Informationssysteme

Die derzeitig als „Gemeinsamer Standpunkt des Rates" vorliegende europäische Datenschutz-Richtlinie (Nr. 33.1) bezieht sich allein auf den europäischen Binnenmarkt. Sie gehört damit in den Bereich des dem EG-Vertrag unterliegenden „klassischen" Europarechts, das – im Gefolge des in Maastricht beschlossenen Vertrages über die Europäische Union – als „erste Säule" bezeichnet wird.

Hierunter fällt auch die europäische Zollunion, in deren Rahmen in Brüssel die Verhandlungen über eine zentrale Datenbank zur Bekämpfung von Zuwiderhandlungen gegen die EG-Zoll- und Agrarregelungen (EG-Zollinformationssystem – EG-ZIS) geführt werden. Die Beratungen über eine neue EG-Amtshilfe-Verordnung für den Zollbereich, die dem EG-ZIS als Rechtsgrundlage dienen soll, wurden inzwischen mit einem gemeinsamen Text abgeschlossen, der dem Europäischen Parlament (EP) vorliegt (s. Nr. 5.6).

Das in dem Vertrag über die Europäische Union verankerte „Drei-Säulen-Konzept" sieht neben der wirtschaftlichen Integration im Rahmen der Europäischen Gemeinschaft die Gemeinsame Außen- und Sicherheitspolitik – GASP – sowie die Zusammenarbeit in den Bereichen Inneres und Justiz als sog. zweite und dritte Säulen vor. Im Zusammenhang mit dem letztgenannten Bereich Inneres und Justiz ist unter Datenschutzgesichtspunkten auf die geplante Einrichtung von gemeinschaftsweiten Informationssystemen hinzuweisen, die unterschiedlichen Zielsetzungen dienen und, entsprechend der Verschiedenartigkeit ihrer Aufgabenstellungen, voneinander abweichende Systemarchitekturen besitzen. Diese Informationssysteme werden auf zwischenstaatlicher Ebene – mühsam – unter den jeweils beteiligten Staaten ausgehandelt. Auf europäischer Ebene habe ich mitgewirkt bei Überlegungen

- zur Errichtung eines Zentralen Europäischen Kriminalpolizeiamtes – EUROPOL – zur Bekämpfung des internationalen Drogenhandels (Nr. 23.2.3),
- zum Aufbau eines Europäischen Informationssystems – EIS – als Fortentwicklung des Schengener Informationssystems (Nr. 23.2.2),
- zum Einsatz eines Zollinformatiossystems der EU-Mitgliedstaaten ZIS – (Nr. 25.2) und
- für ein Integriertes Verwaltungs- und Kontrollsystem für gemeinschaftliche Beihilferegelungen im Bereich der Landwirtschaft – InVeKoS (Nr. 8.1).

33.3 Entwicklung des Datenschutzes im Ausland

Auch in den zurückliegenden zwei Jahren hat sich nichts daran geändert, daß Italien und Griechenland als die letzten weißen Flecken auf der EU-Datenschutzlandkarte auszumachen sind. In beiden Mitgliedstaaten der Union wartet man ganz offensichtlich die Verabschiedung der europäischen Datenschutzrichtlinie (Nr. 33.1) ab, um die notwendigen gesetzgeberischen Schritte an den harmonisierten Rahmenvorgaben zu orientieren. Österreich, das seit 1. Januar 1995 der EU als neuer Mitgliedstaat ange-

hört und dessen Datenschutzgesetz in das Jahr 1980 zurückreicht, hat 1994 auf bereichsspezifischer Ebene gesetzliche Regelungen erlassen: Das Telekommunikationsgesetz mit Sondervorschriften zum Datenschutz und das Gentechnikgesetz, das strenge Maßstäbe für den Umgang mit personenbezogenen Daten enthält.

Gesetzgeberische Bestrebungen sind aus Polen und der Türkei zu berichten. In beiden Ländern werden Entwürfe zu Datenschutzgesetzen auf Kabinetts- bzw. Parlamentsebene beraten.

Unter den Mitgliedstaaten des Europarats hat der Datenschutz weiter an Boden gewonnen. Das Europaratsübereinkommen aus dem Jahre 1981 zum Schutz des Menschen bei der automatisierten Verarbeitung personenbezogener Daten („Datenschutzkonvention des Europarats") wurde zuletzt von Belgien, den Niederlanden, Portugal und Slowenien und damit insgesamt von sechzehn Staaten ratifiziert und in Kraft gesetzt. Weitere fünf Staaten – zuletzt Ungarn – haben das Übereinkommen gezeichnet.

Im überseeischen Raum ist besonders auf die Entwicklungen in Kanada und Hongkong hinzuweisen. In Kanada gibt es seit 1983 ein Datenschutzgesetz für den Bundesbereich, und auch die meisten Provinzen besitzen Datenschutzgesetze. Während diese gesetzlichen Regelungen jedoch ausnahmslos für den öffentlichen Bereich gelten, findet das neue Datenschutzgesetz der Provinz Quebec aus dem Jahre 1993 erstmals auch für den nicht-öffentlichen Bereich Anwendung. Bemerkenswert ist ferner, daß es – wie das Bundesdatenschutzgesetz im öffentlichen Bereich – für jegliche personenbezogene Informationen gilt. Ein ausgereiftes Datenschutzmodell enthält auch der in Hongkong eingehend beratene Gesetzentwurf, mit dessen Verabschiedung für das nächste Jahr gerechnet wird. Der Entwurf gilt für automatisierte wie für manuelle Dateien und zwar im öffentlichen wie im nicht-öffentlichen Bereich. Er sieht die Einrichtung eines Datenschutzbeauftragten vor und erkennt ausdrücklich die Notwendigkeit für die Schaffung weiterer bereichsspezifischer Regelungen an.

33.4 Internationale Zusammenarbeit der Datenschutzkontrollinstanzen

Die 15. Internationale Konferenz der Datenschutzbeauftragten fand unter dem Motto „All about people" im September 1993 in Manchester auf Einladung des britischen Data Protection Registrar statt. Thematische Schwerpunkte waren Identifizierungs- und Registrierungssysteme, Überwachung am Arbeitsplatz, Medien und internationale Entwicklungen. Die deutsche Delegation berichtete zu den Themen Marketing und Reality TV.

Zur 16. Konferenz hatte die niederländische Registratiekammer im September 1994 nach Den Haag eingeladen. Erörtert wurden erneut die internationale Entwicklung, vor allem internationale Informationssysteme in Europa, neuere technologische Entwicklungen, wie Bild- und Tonverarbeitung, Chipkarten und „Super-Highway", sowie der Finanz- und der Gesundheitssektor. Die geplante EG-Richtlinie wurde – auch aus der Sicht der außereuropäischen bzw. nicht der Europäischen Union angehörenden Staaten – diskutiert, wobei vor allem auf die für die Entwicklung des Datenschutzes in Drittstaaten sehr positiven Effekte hingewiesen wurde. Eine Sitzung galt der Besinnung auf die dem Datenschutz zugrunde liegenden Grundwerte, wobei Vertreter der Philosophie, der Sozialwissenschaft und des Verfassungsrechts zu Wort kamen.

Entsprechend einer in Manchester getroffenen Absprache haben die Datenschutzbeauftragten ihre Zusammenarbeit intensiviert. Der letzte und der nächste geplante Gastgeber der Konferenz bilden ein semi-permanentes Sekretariat, das vor allem die Aufgabe übernimmt, themen- oder projektbezogene Interessen zusammenzuführen. Dazu wird eine Datenbank mit entsprechenden Interessenprofilen aufgebaut – natürlich mit Einwilligung der Betroffenen.

Die im Rahmen des sog. dritten Pfeilers des Maastricht-Vertrages (Titel VI des Vertrages über die Europäische Union) erheblich intensivierten Bemühungen um mehr Zusammenarbeit der Mitgliedstaaten der EU bei den polizeilichen Aufgaben der Verbrechensbekämpfung und Gefahrenabwehr sowie bei der Zollfahndung hatten intensive Beratungen zur Errichtung europäischer Informationssysteme zur Folge (Nr. 33.2). Bei den drei noch nicht verabschiedeten Konventionen, an deren Ausarbeitung ich beteiligt bin, handelt es sich um die geplanten Übereinkommen

- zur Errichtung eines Zentralen Europäischen Kriminalpolizeiamtes zur Bekämpfung des internationalen Drogenhandels – EUROPOL – (Nr. 23.2.3),
- zum Aufbau eines Europäischen Informationssystems als Fortentwicklung des Schengener Informationssystems – EIS – (Nr. 23.2.2) sowie
- über ein Zollinformationssystem der EU-Mitgliedstaaten – ZIS – (Nr. 25.2).

Bei der Ausarbeitung dieser verschiedenen Rechtsakte mit ihren unterschiedlichen Aufgabenstellungen und Systemarchitekturen – alle drei Konventionsentwürfe enthalten abschließende bereichsspezifische Regelungen für das jeweilige Informationssystem – setze ich mich vor allem für das Recht der Betroffenen auf Auskunft und Zugang zu dem System, für einen angemessenen Individualrechtschutz und für die Einrichtung einer gemeinsamen Aufsichtsstelle ein.

Zwar können die datenschutzrechtlichen Regelungen schon wegen der unterschiedlichen Systemarchitekturen nicht völlig identisch sein. Auch ist für die Kontrolltätigkeit zu beachten, daß sich die Kontrolle bei EUROPOL auf den Datenbestand in Den Haag, beim EIS auf die in Straßburg vorgehaltenen Daten und beim ZIS auf den zentralen Bestand in Brüssel bezieht. Gleichwohl sehen alle drei Übereinkommensentwürfe – im wesentlichen textgleich – für zentral gehaltene Datenbestände jeweils eine gemeinsame Datenschutzkontrollinstanz vor. Diese setzt sich aus zwei Vertretern (EIS und ZIS) bzw. aus bis zu zwei Vertretern (EUROPOL) der Vertragsstaa-

ten zusammen. Der Entwurf des EUROPOL-Übereinkommens sieht inzwischen die Einrichtung eines Sekretariats vor, dem auch die Befugnis zur Durchführung der Kontrollen übertragen werden kann, während die Einrichtung einer gemeinsamen Kontrollinstanz für alle drei Systeme bislang nicht beabsichtigt ist. Die Voraussetzungen für die praktische Arbeit einer gemeinsamen Datenschutzkontrollinstanz sind daher in den zuständigen Gremien noch gründlich zu prüfen. Entsprechende Beschlüsse können erst nach Anhörung der Datenschutzkontrollinstanzen der Mitgliedstaaten gefaßt werden.

33.5 Europarat

Im Europarat hat die Projektgruppe Datenschutz die Beratung von zwei weiteren fachspezifischen Empfehlungen abgeschlossen, die sich mit der Telekommunikation und der Medizin befassen. Nach Beratung im Lenkungsausschuß im Dezember 1994 wird eine Verabschiedung durch den Ministerrat im ersten Halbjahr 1995 erwartet.

Mit der Vorbereitung weiterer Empfehlungen zu den Bereichen Statistik und Versicherungsrecht sind zwei Arbeitsgruppen befaßt.

Die Frage eines Beitritts der Europäischen Gemeinschaft bzw. Union zur Datenschutzkonvention des Europarats wird auf seiten des Europarats grundsätzlich positiv gesehen; eine endgültige Abklärung der Modalitäten wird wohl erst erfolgen, wenn ein Beitrittsantrag gestellt worden ist. Hierzu dürfte es aber nicht vor der Verabschiedung der EG-Richtlinie kommen.

33.6 Datenschutz bei den Organen der Europäischen Union

In der Diskussion blieben auch weiterhin die Datenverarbeitung bei den Organen der Europäischen Union und die erforderlichen, nach wie vor nicht vorhandenen Datenschutzregelungen. Auf das Fehlen der insoweit notwendigen verfassungskonformen Rechtsgrundlagen habe ich bereits in früheren Tätigkeitsberichten hingewiesen (12. TB S. 49, 13. TB S. 57 f.).

Daß der Datenschutz immer noch aus dem Wirken der Gemeinschafts- und Unionsorgane ausgeklammert bleibt, ist umso bedauerlicher, als die Europäische Kommission bereits vor Jahren für sich selbst eine vielversprechende Vorreiterrolle in Anspruch genommen hatte. Als sie mit der Vorlage eines „Vorschlags für eine Richtlinie des Rates zum Schutz von Personen bei der Verarbeitung personenbezogener Daten" (SYN 287) im Jahre 1990 auf dem Gebiet des Datenschutzes endlich die Initiative ergriff, schlug sie in einem ganzen Paket zugleich weitere Maßnahmen vor mit dem Ziel, eine datenschutzrechtliche Gesamtkonzeption innerhalb der EG zu verwirklichen. Dabei betraf ein Teil dieses Pakets 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 war vorgesehen, daß die Kommission die erforderlichen Maßnahmen treffen oder vorschlagen würde, um diese Grundsätze auch für die eigenen Organe und Einrichtungen der Gemeinschaft verbindlich zu machen. Bereits mit der Vorlage des Pakets verpflichtete sich die Kommission, in der Zwischenzeit die Bestimmungen der geplanten Richtlinie auf ihre eigenen Dateien anzuwenden.

Ich bescheinigte der Kommission damals, sich damit in eindrucksvoller Weise an die Spitze der Entwicklung gestellt zu haben und sagte ihr im kollegialen Rahmen der Datenschutzbeauftragten der EG-Mitgliedstaaten Unterstützung in ihren Bemühungen zu (s. 13. TB S. 58).

Nachdem das Europäische Parlament eine Vielzahl von Änderungswünschen beschlossen hatte, legte die Kommission im Jahre 1992 einen geänderten Vorschlag (KOM(92) 422 endg. – SYN 287) vor, auf dessen Grundlage seitdem in Brüssel der Entwurf einer europäischen Datenschutzrichtlinie beraten wird (s. hierzu Nr. 33.1). Das Vorhaben „betreffend die Anwendung der Grundsätze der Datenschutzrichtlinie auf die Organe und Einrichtungen der Europäischen Gemeinschaften" wird seit dieser Zeit jedoch nicht mehr vorangebracht. Im Rahmen der Brüsseler Beratungen über die Datenschutzrichtlinie wurde immer wieder angemahnt, daß die Gemeinschaft auch selbst institutionell nicht länger untätig bleiben darf und eigene Vorsorge für den Datenschutz treffen muß. Insbesondere wurde in diesem Zusammenhang hervorgehoben, daß die Organe der Gemeinschaft, ihre Verwaltungseinrichtungen und Mitarbeiter dringend einen europäischen Datenschutzbeauftragten benötigen. Die vielfältigen und umfangreichen Aktivitäten der Gemeinschaft und insbesondere der Kommission, beispielsweise auf den Gebieten der Informationstechnik, der Subventionen, des Wettbewerbsrechts und hier vor allem der Fusionskontrolle bedürfen der rechtzeitigen und systematischen Prüfung der datenschutzrechtlichen Auswirkungen. Bereits vor Jahren habe ich davor gewarnt, daß die Gemeinschaft ohne eine besondere Institution, die den notwendigen Sachverstand bündelt und den Datenschutz durch Beratung und Kontrolle praktisch voranbringt, zwangsläufig noch weiter hinter das europäische Datenschutzniveau zurückfallen wird (12. TB S. 49).

Daran ändert wenig – zumindest im gegenwärtigen Zeitpunkt – der Minimalkonsens, zu dem sich die Kommission im Zuge der Verhandlungen über die Datenschutzrichtlinie in Brüssel durchringen konnte: Anläßlich der Verabschiedung der Datenschutzrichtlinie wollen sich die Organe der Europäischen Union in einer „Erklärung zu Protokoll des Rates" verpflichten, den Bestimmungen der Richtlinie entsprechende, eigene Regelungen zu schaffen. Denn mehr als eine Absichtserklärung beinhaltet diese Formulierung zunächst nicht. Ich appelliere daher zum wiederholten Male an die Bundesregierung und an die Verantwortlichen in den Organen der Union, die entscheidenden Schritte zu unternehmen, um den Datenschutz in der Europäischen Union Wirklichkeit werden zu lassen. Unterstützung finde ich hierin beim Bundesrat, der in seinem Beschluß zur geplan-

ten Datenschutz-Richtlinie vom 23. September 1994 (BR-Drucksache 672/94) auf den Mißstand hinweist und die Forderung nach einer unabhängigen und effektiven europäischen Datenschutzkontrollinstanz erhebt, an die sich jeder Betroffene wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der EU in seinen Rechten verletzt zu sein.

Wie wenig sensibel manche europäische Einrichtung mit personenbezogenen Daten umgeht, zeigte jüngst der Europäische Gerichtshof (EuGH). Er veröffentlichte mit seiner Entscheidung zum Nachtarbeitsverbot für Schwangere und zur hierauf gegründeten Anfechtung eines Arbeitsvertrages nicht nur den vollen Namen der Klägerin, sondern gab darüber hinaus auch noch das genaue Datum des Beginns der Schwangeschaft preis (abgedruckt in einer Fachzeitschrift für Arbeitsrecht).

34 Aus meiner Dienststelle

34.1 Informationen für die Bürger und auch für die Verwaltung

Im Berichtszeitraum habe ich 3 neue Broschüren erstellt.

Nach der BfD-Info 1 „Bundesdatenschutzgesetz – Text und Erläuterung –", die erstmals im Dezember 1992 erschienen ist, sind dies:

- BfD-Info 2 „Der Bürger und seine Daten"
- BfD-Info 3 „Schutz der Sozialdaten"
- BfD-Info 4 „Der behördliche Datenschutzbeauftragte"

Die genannten Broschüren werden kostenlos abgegeben. Überwiegend von Bürgern werden rund 100000 Exemplare jährlich angefordert. Auch daran zeigt sich das große Interesse der Bürgerinnen und Bürger an datenschutzrechtlichen Fragen.

34.2 Einsatz von Informationstechnik in meiner Dienststelle

Wegen der fortschreitenden Entwicklung der Informationstechnik in der Bundesverwaltung und des damit verbundenen Aufgabenzuwachses bei meiner Kontroll- und Beratungsfunktion war es notwendig, die Informationstechnik in meiner Dienststelle weiter auszubauen. Hierzu trugen auch bei:

- Die Informationstechnik in der Bundesverwaltung wird in immer breiterem Ausmaß und in größerer Komplexität eingesetzt, sie erfordert eine neue Dimension an datenverarbeitungstechnischer Fortbildung und Kompetenz bei meinen Mitarbeitern. Diese kann nur bei tatsächlicher Verfügbarkeit moderner Technik und täglichem Umgang mit ihr erlangt werden.
- Ich habe Bürger und öffentliche Stellen des Bundes bei Fragen des Datenschutzes und der Datensicherheit zu beraten. Sehr oft stehen diese Fragen in Zusammenhang mit der Anwendung von Informationstechnik.
- Infolge des Personalzuwachses meiner Dienststelle von früher 30 auf derzeit 52 Mitarbeiter mußte die Schriftguterstellung effektiviert werden.

1993 wurden daher das Dienstgebäude mit einer kompletten Netzverkabelung versehen sowie Hard- und Software beschafft, um die erste Ausbaustufe eines PC-Netzes (Local Area Network – LAN) zu installieren. 1994 wurde dies fortgesetzt.

In diesem Netz arbeiten seit Ende 1994 zwei Server und sechsundzwanzig Workstations. Aus Gründen der Datensicherheit und des Datenschutzes verfügen nur sechs Workstations über Platten- und Diskettenlaufwerke. Die Tastaturen sind mit einem Magnetstreifen-Kartenleser ausgestattet und können nur mit Hilfe einer personengebundenen Magnetstreifenkarte entsperrt werden.

Schwerpunkte der künftigen IT-Anwendung sind eine wirksame Unterstützung des Schreibdienstes durch den Zugang zur Textverarbeitung für weitere Mitarbeiter, die Führung und Nutzung von Datenbanken zur Unterstützung der Schriftgutverwaltung und als Wissensspeicher sowie die Schaffung von Möglichkeiten für die Fortbildung der Bediensteten im Arbeitsprozeß.

1994 standen jeder Organisationseinheit meines Hauses zumindest zwei APC zur Verfügung, der Schreibdienst wurde komplett ausgestattet.

Ab 1995 ist die Teilnahme meiner Dienststelle am Informationstechnischen Verbund Berlin-Bonn (IVBB) vorgesehen.

Für den Betrieb und die Nutzung der Informationstechnik werde ich unter Mitwirkung des Personalrats des BMI eine Dienstanweisung erlassen.

35 Am Schluß noch einiges Wichtige aus zurückliegenden Tätigkeitsberichten

1. Im 14. Tätigkeitsbericht S. 36 hatte ich bereits berichtet, daß die notwendigen **Verwaltungsvorschriften zum Ausländergesetz** (AuslG) weiterhin fehlen, die u. a. die Datenschutzbestimmungen des § 75 ff. AuslG präzisieren. Der Innenausschuß des Deutschen Bundestages unterstützt meine Empfehlungen und hat die Bundesregierung aufgefordert, möglichst bald die Verwaltungsvorschriften in Kraft zu setzen (100. Sitzung des Innenausschusses vom 15. Juni 1994 TOP 16 nebst Anlage 18 unter Nr. 2).
2. Schon seit langem ist es mein Anliegen (vgl. zuletzt 14. TB S. 50), im Strafverfahren der routinemäßigen öffentlichen Erörterung so sensibler personenbezogener Informationen wie der Einkommens- und Vermögensverhältnisse des Beschuldigten – und damit oft auch seines Ehe- oder Lebenspartners – zumindest in den Fällen entgegenzuwirken, in denen diese Datenerhebung mit dem eigentlichen Gegenstand des Strafverfahrens nichts zu tun hat. Das sog.

Selbstleseverfahren, d. h. die **schriftliche Darstellung der Einkommens- und Vermögensverhältnisse** unter Verzicht auf die Verlesung eines solchen Schriftstückes in der Verhandlung, bietet hier nach meiner Auffassung in einer Vielzahl von Fällen das geeignete Instrument für einen wirksamen Schutz des Persönlichkeitsrechtes der Betroffenen. Leider hat der Gesetzgeber im Verbrechensbekämpfungsgesetz zwar den Anwendungsbereich dieses Selbstleseverfahrens erneut erweitert; ausweislich der Begründung ist dies jedoch nach wie vor nur zulässig zur Beschleunigung des Verfahrens und nicht – wie von mir vorgeschlagen – auch zur Gewährleistung des grundrechtlich verbürgten Persönlichkeitsschutzes.

3. Die datenschutzrechtlichen Probleme, die durch die Zusammenfassung mehrerer Entscheidungen (Scheidungsausspruch/Umgang mit ehelichen Kindern u. a.) in **Ehescheidungsverbundurteilen** entstehen, wenn solche Urteile Behörden vorgelegt oder dem Gerichtsvollzieher für Zwecke der Zwangsvollstreckung übergeben werden, habe ich zuletzt im 13. Tätigkeitsbericht (S. 90) angesprochen. In der Diskussion mit dem Bundesministerium der Justiz hat sich ergeben, daß zur Vorlage an Behörden in den meisten Fällen Auszüge aus dem Urteilstenor ausreichen und für die Zwangsvollstreckung regelmäßig vollstreckbare Teilausfertigungen ohne Tatbestand und Entscheidungsgründe genügen. Entscheidend ist daher nur, daß die Parteien des Zivilprozesses über die Möglichkeit unterrichtet werden, sich für die vorgenannten Zwecke Auszüge aus dem Tenor des Ehescheidungsverbundurteils fertigen zu lassen. Für eine solche Unterrichtung könnte dem Urteil ein Merkblatt oder ein Stempelaufdruck mit einem entsprechenden allgemeinen Hinweis beigefügt werden. Im Interesse einer koordinierten Prüfung dieses Vorschlags durch die hierfür zuständigen Landesjustizverwaltungen habe ich mich in Übereinstimmung mit den Landesbeauftragten für den Datenschutz an das BMJ mit der Bitte gewandt, diese Empfehlung an die Länder heranzutragen. Eine Antwort liegt mir noch nicht vor.

4. Entgegen meiner im 13. Tätigkeitsbericht (S. 90) ausgesprochenen Erwartung ist die **Steuerdaten-Abruf-Verordnung** noch immer nicht in Kraft getreten. Zunächst hatte sich eine eingehende Diskussion zur Rechtsgrundlage für den automatisierten Abruf von Steuerdaten durch Rechnungsprüfungsbehörden ergeben. Insoweit hat das Bundesministerium der Finanzen zugesagt, den gesetzgebenden Körperschaften bei der nächsten Änderung der Abgabenordnung (AO) eine Ergänzung des § 30 Abs. 6 AO vorzuschlagen, auf den sich die Verordnung stützt; die Rechnungsprüfungsbehörden sollen in dieser Vorschrift ausdrücklich genannt werden. Der Verordnungsentwurf hat danach zwar bereits dem Bundesrat vorgelegen. Im Hinblick auf Bedenken der kommunalen Spitzenverbände gegen Regelungen, die nach ihrer Ansicht die Bedürfnisse und technischen Möglichkeiten der Gemeinden nicht ausreichend berücksichtigen, hat der Bundesrat das BMF jedoch gebeten, die Verordnung mit diesen nochmals zu erörtern; bis zur erneuten Vorlage der Verordnung hat er die Beratung „vertagt". Zur Vorbereitung der Gespräche mit den kommunalen Spitzenverbänden hat das BMF sich zunächst an die obersten Finanzbehörden der Länder gewandt und diese zugleich ausdrücklich gebeten, ihre Stellungnahme mit „dem Datenschutz" des jeweiligen Landes abzustimmen. Ich werde die Arbeiten am Verordnungsentwurf weiterhin unterstützen.

5. Die bei Vorlage des 14. Tätigkeitsberichts erst als Regierungsentwurf vorhandene **Insolvenzordnung** – InsO – (14. TB S.54) ist inzwischen verkündet worden (BGBl. 1994 I S.2866) und wird gemeinsam mit dem Einführungsgesetz zur Insolvenzordnung (BGBl. 1994 I S. 2911) am 1. Januar 1999 in Kraft treten. Das umfangreiche Gesetz enthält verhältnismäßig wenig datenschutzrechtlich relevante Regelungen. Meine Änderungsvorschläge sind vom Bundesministerium der Justiz in die eingehenden Gespräche der Berichterstatter des Rechtsausschusses des Deutschen Bundestages über den Entwurf eingebracht und in das Gesetz übernommen worden. Erwähnen möchte ich eine Änderung in § 97 Abs. 1 Satz 3 InsO. Diese Vorschrift legt mit der umfassenden Formulierung „verwendet" fest, daß die vom Schuldner aufgrund gesetzlicher Verpflichtung zu erteilenden Auskünfte an das Gericht, an den Insolvenzverwalter und an die Organe der Gläubiger ohne seine Zustimmung auch nicht als Ansatz für strafrechtliche Ermittlungen gegen ihn oder einen Angehörigen herangezogen werden dürfen; es sei denn, er stimmt zu. Andere Änderungen betreffen z. B. die Eingrenzung der verschiedenen öffentlichen Bekanntmachungen auf den erforderlichen Umfang.

6. In meinem 14. Tätigkeitsbericht (S. 55 f.) hatte ich meine Zuversicht ausgedrückt, daß notwendige bereichsspezifische Datenschutzvorschriften möglichst bald in das **Zollverwaltungsgesetz** aufgenommen werden. Auf meine Nachfragen hin hatte das Bundesministerium der Finanzen mitgeteilt, es habe wegen anderer vordringlicher Arbeiten noch keinen entsprechenden Gesetzentwurf erarbeiten können. Kurz vor Fertigstellung dieses Berichts hat das BMF mir einen Entwurf für die Aufnahme einer Rechtsverordnungsermächtigung zum Erlaß bereichsspezifischer Vorschriften über die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch die Zollverwaltung in das Zollverwaltungsgesetz zusammen mit einem Entwurf für eine entsprechende Rechtsverordnung angekündigt.

7. Im 14. Tätigkeitsbericht (S. 57) habe ich auf meine – bisher leider nicht berücksichtigten – Empfehlungen zu einzelnen von der Bundesrepublik Deutschland mit einigen Nicht-EU-Staaten geschlossenen Verträgen über die **gegenseitige Unterstützung der Zollverwaltungen** hingewiesen. Die in diesen Verträgen (z. B. mit der Russischen Föderation) vereinbarten daten-

schutzrechtlichen Vorkehrungen sind im Vergleich zu dem erreichten oder noch angestrebten innergemeinschaftlichen Datenschutzstandard unzureichend. Das Bundesministerium der Finanzen hat mir angeboten, den von deutscher Seite bereits ratifizierten Vertrag mit der Russischen Föderation (BGBl. 1994 II Seite 1052) nach seiner Ratifizierung durch den Vertragspartner bei der Vereinbarung vertraglich vorgesehener Durchführungsbestimmungen um datenschutzrechtliche Vorschriften zu ergänzen. Ich begrüße die Bereitschaft des BMF, auf diesem Wege zu versuchen, eine datenschutzgerechte Praxis im Amtshilfeverkehr mit der Zollverwaltung der Russischen Föderation herbeizuführen. Das BMF rechnet damit, Verhandlungen über die Durchführungsbestimmungen im ersten Halbjahr 1995 aufnehmen zu können und hat mir zugesagt, mich rechtzeitig zu beteiligen. Ich hoffe, daß künftig schon bei der Vorbereitung derartiger Verträge ausreichende Datenschutzregelungen vorgesehen werden.

8. Das Recht des Wirtschaftsprüfers, im von der Wirtschaftsprüferkammer herausgegebenen Wirtschaftsprüferverzeichnis auf Wunsch nicht genannt zu sein (s. 14. TB S. 59), wurde durch die Änderung der **Wirtschaftsprüferordnung** im Berichtszeitraum nun auch gesetzlich festgeschrieben. Gleichzeitig traten bereichsspezifische Datenschutzbestimmungen in der Wirtschaftsprüferordnung in Kraft.

9. Das Bundesministerium der Verteidigung hat noch keine **Personalaktenverordnung** gem. **§ 29 Abs. 9 Soldatengesetz** erlassen (14. TB S. 100). Nach entsprechender Mitteilung ist die Ressortabstimmung noch nicht abgeschlossen.

10. Im Rahmen des Gesetzes zur Neuordnung des Erfassungs- und Musterungsverfahrens sind die ursprünglich mit dem Zweiten Gesetz zur Änderung des Wehrpflichtgesetzes vorgesehenen datenschutzrechtlich bedeutsamen Änderungen des Wehrpflichtgesetzes in Kraft getreten. Meine früheren Bedenken (14. TB S. 101), mit der Formulierung des § 20 a WPflG sei nicht ausreichend sichergestellt, daß ein Wehrpflichtiger, der einen Antrag auf Kriegsdienstverweigerung gestellt hat, neben der Musterung nicht auch noch der **Eignungsuntersuchung** unterzogen wird, habe ich nach Erläuterung des BMVg zum Wortlaut der Vorschrift im Zusammenhang mit § 3 Abs. 2 Satz 1 des Kriegsdienstverweigergungsgesetzes nicht mehr aufrechterhalten. Ebenso habe ich die zunächst von mir kritisierte Regelung, daß Akten über das Anerkennungsverfahren von Wehrpflichtigen, deren Antrag auf Anerkennung als Kriegsdienstverweigerer abgelehnt, zurückgenommen oder infolge Verzichts gegenstandslos geworden ist, längerfristig aufbewahrt werden, u. a. im Hinblick auf Ausführungen des Bundesverfassungsgerichts zu Zweitanträgen von Kriegsdienstverweigerern (NJW 1984, 1519ff., 1523f.) als sachlich begründet akzeptiert. Ich hoffe, daß ein erster Entwurf der nach § 27 WPflG zu erlassenden **Personalaktenverordnung für ungediente Wehrpflichtige** in absehbarer Zeit vorgelegt wird.

11. Das Bundesministerium für Familie, Senioren, Frauen und Jugend hat die Arbeiten an der nach **§ 36 Abs. 8 Zivildienstgesetz** zu erlassenden **Personalaktenverordnung** (14. TB S. 101 f.) noch nicht abgeschlossen. Im Interesse sachgerechter Durchführung der gesetzlichen Regelungen ist zu fordern, daß ein Entwurf bald vorgelegt wird.

12. Im 14. Tätigkeitsbericht (S. 102) hatte ich dargelegt, daß das Bundesamt für den Zivildienst (BAZ) die in § 23 Kriegsdienstverweigerungsgesetz (KDVG) festgelegte Frist für die **Vernichtung der Anerkennungsteile der Personalunterlagen von Kriegsdienstverweigerern,** die ihren Zivildienst bereits vor dem Inkrafttreten des § 2 Abs. 6 KDVG abgeleistet haben, nicht eingehalten hat. Auf meine dringende Empfehlung hat das BAZ diese Arbeit mit Zeitangestellten im Laufe des Jahres 1994 abgeschlossen.

13. Die in meinem 14. Tätigkeitsbericht (S. 28 f.) dargestellte Schwierigkeit, die **Personalunterlagen** der über 32jährigen gedienten **Bausoldaten** aus dem Bestand von ca. 2 Mio. Personalunterlagen der ehemaligen NVA an das BAZ zu überführen, besteht unverändert fort. Nach Mitteilung des Bundesministeriums der Verteidigung werden sie immer dann an das BAZ abgegeben, wenn sie aus einem aktuellen Bearbeitungsanlaß „zur Hand genommen werden". In Anbetracht des verhältnismäßig großen Verwaltungsaufwands für eine gesonderte Überprüfung von ca. 2 Mio. Akten sehe ich darin eine vertretbare Vorgehensweise.

14. Im 14. TB (S. 63) habe ich die Problematik der **Abschottung von Beihilfestelle und Personalverwaltung** am Beispiel der **Bundesknappschaft** verdeutlicht. Aufgrund einer bei einer Außenstelle der Knappschaft durchgeführten Kontrolle konnte ich erreichen, daß künftig über Beihilfeanträge nicht mehr von Mitarbeitern entschieden wird, die an Personalentscheidungen beteiligt sind. Dasselbe gilt für Leistungsanträge von Mitarbeitern, die bei der Bundesknappschaft selbst krankenversichert sind. Im übrigen wird künftig durch eine eindeutige Adressierung der Beihilfeanträge eine unzulässige Weitergabe im knappschaftsinternen Geschäftsgang ausgeschlossen.

    Desweiteren habe ich festgestellt, daß im Bereich der Bundesknappschaft ein **Antragsformular auf Anerkennung von Pflegebedürftigkeit** verwendet wird, dessen Inhalt über das für die Aufgabenerfüllung Erforderliche hinausgeht. Ich habe gegenüber der Bundesknappschaft empfohlen, den Inhalt dieses Fragebogens zu reduzieren; hier kommt beispielsweise der durch den Spitzenverband des Medizinischen Dienstes unter Beachtung der Rechtsprechung des Bundessozialgerichtes entwickelte Mustervordruck in Betracht.

15. Bereits früher habe ich mich zur **Weitergabe von Bewerbungsunterlagen** durch das Arbeitsamt an den Arbeitgeber geäußert (z. B. 10. TB S. 63). Mehrere Eingaben haben gezeigt, daß es bei der Anwendung der geltenden Regelungen in der Praxis erneut Rechtsunklarheiten gegeben hat.

    Die Bundesanstalt für Arbeit hat deshalb, auf meine Anregung hin, in einem neuen bundeseinheitlich geltenden Runderlaß auf die bestehende Rechts- und Weisungslage beim Verfahren der Überlassung und der Vorlage von Bewerbungsunterlagen durch das Arbeitsamt an Arbeitgeber hingewiesen. Darüber hinaus hat sie ergänzende Erläuterungen gegeben und zusätzliche datenschutzrechtliche Anmerkungen aufgenommen. Betont wird in diesen Weisungen u. a. die Freiwilligkeit der Herausgabe von Bewerbungsunterlagen durch Arbeitslose (oder nicht arbeitslose Arbeitsuchende), die Entscheidungsfreiheit der Betroffenen über eine Vorlage beim Arbeitgeber und die Unterrichtung des Bewerbers über diese Vorlage. Außerdem wird der Anspruch auf Rückgabe der Bewerbungsunterlagen ausdrücklich festgeschrieben.

16. Die Deutsche Arbeitsverwaltung ist seit 1980 an das **„Europäische System zur Übermittlung von Stellen- und Bewerberangeboten im internationalen Ausgleich"** (früher SEDOC – jetzt EURES) angeschlossen (14. TB S. 88). Sie hatte angekündigt, durch Umorganisation der Auslandsabteilung in der Zentralstelle für Arbeitsvermittlung – ZAV – die datenschutzrechtlichen Anforderungen an dieses System besser zu berücksichtigen. Hierzu liegt mir mittlerweile eine ergänzende Stellungnahme der Bundesanstalt vor.

    Die EURES-Stelle in der ZAV hat zwischenzeitlich die Partnerverwaltungen im Ausland gebeten, sie über für die Arbeitsvermittlung wichtige Bestimmungen des Datenschutzes im jeweiligen Land zu unterrichten. Die Partnerverwaltungen in Belgien, den Niederlanden, Irland und Dänemark haben dazu auf den Datenschutz bei der Arbeitsvermittlung in ihren Ländern hingewiesen. Von den weiteren EURES-Partnerverwaltungen kamen keine entsprechenden Auskünfte.

    Auf der Grundlage der nun vorliegenden Informationen unterrichtet die ZAV alle Bewerber über die datenschutzrechtlichen Gegebenheiten in den Partnerländern. Ein Merkblatt hierzu ist in Vorbereitung. In die Länder, die die Einhaltung datenschutzrechtlicher Bestimmungen nicht sicherstellen, werden personenbezogene Daten von der ZAV nur auf ausdrücklichen Wunsch der Bewerber übermittelt.

    Eine Übermittlung personenbezogener Daten unterbleibt in allen Fällen, in denen die Arbeitsverwaltung Grund zur Annahme hat, daß dadurch schutzwürdige Belange des Betroffenen beeinträchtigt werden.

17. Die Vorschrift des § 305 SGB V gewährt dem Versicherten einen **Auskunftsanspruch über die der Krankenkasse verfügbaren Angaben über** die von ihm **in den letzten zwei Geschäftsjahren** (ab dem 1. Januar 1996 im jeweils letzten Geschäftsjahr) **in Anspruch genommenen Leistungen** und deren Kosten (s. 14. TB S. 89).

    Informationsbesuche bei zwei Ersatzkassen haben gezeigt, daß die Kassen das Auskunftsverfahren ausreichend organisiert haben. Bei einem Auskunftsverlangen des Versicherten stellt die Kasse die verfügbaren Informationen zusammen und informiert ihn. Auf Wunsch erhält er entsprechende Kopien von Unterlagen. Dem steht nicht entgegen, daß ärztliche und zahnärztliche Abrechnungsdaten von den Krankenkassen nur noch fall- und nicht mehr versichertenbezogen erhoben und gespeichert werden dürfen (§ 295 Abs. 2 SGB V). Soweit sich ein Auskunftsersuchen des Versicherten auf solche Angaben richtet, werden diese gem. § 305 Satz 2 SGB V in der ab 1. Januar 1996 gültigen Fassung von der jeweiligen kassenärztlichen oder kassenzahnärztlichen Vereinigung den Krankenkassen gesondert in einer Form übermittelt, die eine Kenntnisnahme durch die Krankenkasse ausschließt. Dadurch ist sichergestellt, daß der Auskunftsanspruch des Versicherten nicht ins Leere läuft.

18. Im 14. Tätigkeitsbericht (S. 26) hatte ich darüber berichtet, daß ich mit dem Bundesministerium für Arbeit und Sozialordnung erörtert habe, unter welchen Voraussetzungen Daten aus der bei der **Bundesanstalt für Arbeitsmedizin** (BAfAM) geführten **„Datei über arbeitsmedizinische Vorsorgeuntersuchungen"** an gewerbliche Berufsgenossenschaften übermittelt werden dürfen. Es besteht mittlerweile Einigkeit mit dem BMA, daß eine solche Übermittlung (unter dem Vorbehalt der Erforderlichkeit für die Aufgabenerfüllung der Berufsgenossenschaft) generell der Einwilligung des Betroffenen bedarf.

19. Über die Erhaltung der Daten des **„Nationalen Krebsregisters" der ehemaligen DDR** und die Entwicklung der Diskussion um eine gesetzliche Regelung der Einrichtung von Krebsregistern habe ich mehrfach berichtet, (s. zuletzt 14. TB S. 29 und S. 103 f.). Durch das Krebsregistergesetz wird nunmehr bundesweit die Errichtung von Krebsregistern geregelt, siehe dazu Nr. 17.1 in diesem Bericht.

20. Die **Meldepflicht für Gefahrguttransporte,** über die ich berichtet hatte (14. TB S. 112), wurde bei der Änderung des § 12.01 der Rheinschiffahrtspolizeiverordnung durch die Zentralkommission für die Rheinschiffahrt in Straßburg berücksichtigt. Die Umsetzung in nationales Recht ist inzwischen erfolgt; datenschutzrechtlich ist das Problem damit zufriedenstellend gelöst.

21. Nach intensiven Gesprächen hat das BMV die **Aufbewahrungsfrist für Vorgänge über Ordnungswidrigkeiten für die Wasser- und Schiffahrtsdirektionen, das Bundesamt für Seeschiffahrt und Hydrographie sowie die See-Berufsgenossenschaft** (vgl. 14. TB S. 112) in einem Erlaß einheitlich für den Regelfall auf drei Jahre fest-

gelegt. In Ausnahmefällen, etwa bei Geldbußen von mehr als 1000,– DM, sind die Unterlagen in Ordnungswidrigkeitenverfahren fünf, und wenn das Verfahren im Zusammenhang mit Patententziehungs- oder Patentwiderrufsverfahren steht, zehn Jahre aufzubewahren. Gegen diese Fristen bestehen keine datenschutzrechtlichen Bedenken.

22. In seiner sog. **Fangschaltungsentscheidung** hatte das Bundesverfassungsgericht das Fehlen einer gesetzlichen Grundlage für diejenigen Vorschriften der TDSV festgestellt, die das grundrechtlich geschützte Fernmeldegeheimnis berühren (14. TB S. 117). Die Vorgabe des Gerichtes, eine gesetzliche Grundlage zu schaffen, wurde im Rahmen der Postreform II durch das Gesetz über die Regulierung der Telekommunikation und des Postwesens (PTRegG) geschaffen.

23. Zu kritisieren hatte ich auch das Verfahren der Telekom, bei **Einwendungen gegen die Telefonrechnung** die Verbindungsdaten der Telefonate des Beschwerdeführers zu registrieren, ohne diesem auch nur einen Hinweis darauf zu geben (14. TB S. 120). Die von mir geforderte Verfahrensänderung, die insbesondere Transparenz für den Betroffenen schaffen soll, ist inzwischen erfolgt, Erfahrungen liegen jedoch ebenfalls noch nicht vor.

24. In verschiedenen Fällen hatte die Telekom versucht, Angehörige – Schwiegereltern, Großeltern – von Telefonschuldnern zum **Begleichen der** betreffenden **Rechnungen** zu veranlassen und in diesem Zusammenhang das Bestehen von Telefonschulden sowie deren Höhe dem Familienangehörigen mitgeteilt (14. TB S. 122). Wegen der fehlenden Rechtsgrundlage hatte ich das Verfahren kritisiert; es wurde inzwischen eingestellt.

25. Bezüglich des Verfahrens der **Registrierung von Verbindungsdaten** in Fällen von (angeblichen) belästigenden Anrufen hatte ich gegenüber der Telekom kritisiert, daß hierfür ein nicht substantiierter Vorwurf ausreichte und der Betroffene über die Registrierung auch nicht informiert wurde (14. TB S. 125). Entsprechend meiner Forderung wurde zwischenzeitlich eine Verfahrensänderung vorgenommen; Erfahrungen liegen jedoch noch nicht vor.

26. Das **Umweltstatistikgesetz,** über das ich zuletzt in meinem 14. TB (S. 128) berichtet hatte, ist im Berichtszeitraum verabschiedet worden. Es enthält die erforderlichen klaren Regelungen über die Verknüpfung umweltrelevanter Daten aus verschiedenen Quellen für Zwecke der Umweltstatistik.

27. Auch im Berichtszeitraum hat das Bundesministerium der Justiz keinen neuen Entwurf eines **Strafverfolgungsstatistikgesetzes** (s. zuletzt 14. TB S. 129) vorgelegt. Mittlerweile führt in einigen Ländern dieses Versäumnis zu Problemen bei der Bereitstellung statistischer Angaben aus den Strafrechtspflegestatistiken für die wissenschaftliche Forschung.

28. Der Einsatz von **tragbaren Personalcomputern (Laptops) bei der Erhebung von amtlichen Statistiken** bedarf einer gesetzlichen Regelung (14. TB S. 129). Das BMI hat dagegen unter Berufung auf die amtliche Begründung zum Bundesstatistikgesetz darauf verwiesen, daß ein Unternehmen die für die amtliche Statistik notwendigen Antworten auch auf Magnetbändern liefern darf. Dies ist wenig überzeugend. Der Gesetzgeber hat sich in seiner Begründung zum Bundesstatistikgesetz erkennbar an Wirtschaftsstatistiken orientiert, bei denen Unternehmen aufgrund einer besonderen Vereinbarung (vgl. Satz 1 der amtl. Begründung zu § 11 BStatG) große Mengen von Daten an das Statistische Landesamt übermitteln. Die Situation bei Personenbefragungen, wie beim Mikrozensus, in denen der Bürger für die amtliche Statistik weitgehend spontan antworten muß, ist damit nicht annähernd vergleichbar.

29. Auf meine frühere Anregung, den **Gesamtbestand des Aktennachweissystems (BKA-AN) des Bundeskriminalamtes** von ca. 2 Mio Datensätzen wegen der festgestellten Mängel (vgl. 14. TB S. 134) zu bereinigen, hat das Bundesministerium des Innern ausgeführt, eine solche Bereinigung würde aufgrund des hohen Aufwandes zahlreiche Kräfte mehrere Jahre lang binden. Ich habe deshalb mit dem Bundesministerium des Innern vereinbart, daß die beim Bundeskriminalamt gespeicherten alten Datensätze im Rahmen der aktuellen Sachbearbeitung ausgesondert werden. Diese Datensätze unterliegen grundsätzlich einer Auskunftssperre und dürfen nur dann übermittelt werden, wenn sie für aktuelle Verfahren neue gravierende Erkenntnisse enthalten (z. B. seit mehr als 10 Jahren gespeicherte Informationen, die mit einem aktuellen Kapitalverbrechen im Zusammenhang stehen).

    Das Bundeskriminalamt hat mir weiterhin mitgeteilt, daß die Länder auf den erkennungsdienstlichen Unterlagen, die zur Speicherung eines Datensatzes im BKA-AN führten, kenntlich machen, ob es sich um ein Delikt von geringfügiger Bedeutung handelt. Das Bundeskriminalamt ist damit in der Lage, die zutreffenden Speicherfristen festzusetzen.

    Im Bundeskriminalamt wurde sichergestellt, daß die Datei VNP (Vorgangsnachweis Personen) grundsätzlich nur zu administrativen Zwecken genutzt wird. Eine Auskunftserteilung aus dieser Datei im Rahmen kriminalpolizeilicher Ermittlungstätigkeit darf allenfalls nach erfolgter Relevanzprüfung erfolgen.

30. Meine Kritik an der **Dienstanweisung Amtshilfe/Grenze** (14. TB S. 137) ist im Kreise der Parlamentarischen Kontrollkommission aufgegriffen worden. Es zeichnet sich eine deutliche Verbesserung ab. Das BMI hat zugesagt, die von mir hauptsächlich kritisierte Regelung (a. a. O. S. 138) zu streichen. Dabei geht es darum, daß die Nachrichtendienste den BGS nicht um die Übermittlung solcher personenbezogener Daten ersuchen

dürfen, die nicht bei der eigentlichen Wahrnehmung grenzpolizeilicher Aufgaben bekannt werden.

31. Im 14. Tätigkeitsbericht (S. 138) habe ich über die Eingabe eines Petenten berichtet, der seinen **Arbeitsplatz** durch eine zweifelhafte **Überprüfungspraxis** verloren hatte. Das Bundesministerium des Innern hatte mir ursprünglich zum Abschluß meiner Kontrolle mitgeteilt, daß in Zukunft in vergleichbaren Fällen unbeschränkte Auskünfte aus dem Bundeszentralregister nicht mehr eingeholt würden. Solche seien auch nicht erforderlich, weil ein Führungszeugnis, unter Umständen ergänzt durch eine polizeiliche Auskunft, für den verfolgten Zweck ausreiche. In der Stellungnahme der Bundesregierung zu meinem Tätigkeitsbericht wird demgegenüber ausgeführt, ein Führungszeugnis sei nicht geeignet, die unbeschränkte Auskunft aus dem Bundeszentralregister zu ersetzen. Es werde deshalb auch künftig aus allgemeinen Sicherheitserwägungen für erforderlich gehalten, im konkreten Einzelfall weiterhin unbeschränkte BZR-Auskünfte im Rahmen des vorbeugenden Personen- und Objektschutzes einzuholen. Hierzu wird auf die Ereignisse von Bad Kleinen verwiesen, womit eine zusätzliche Gefährdungssituation für den Bundesgrenzschutz entstanden sei. Das Bundesministerium des Innern hat dann mit Erlaß vom 22.4.1994 klargestellt, daß das Formular der BZR-Auskunft und die Ausfüllanleitung weiterhin Bestandteil der Geheimschutzanweisung bleiben. Im Einzelfall seien begründete Anlässe denkbar, die ein Auskunftsersuchen gem. § 41 Abs. 1 Nr. 2 BZRG erforderlich machen könnten. Ich halte jedoch an meiner Rechtsauffassung zu § 41 Abs. 1 Nr. 2 BZRG, die ich in meinem 14. Tätigkeitsbericht dargestellt habe, weiterhin fest. Das BZRG gestattet die Einholung einer unbeschränkten Auskunft nur den obersten Bundesbehörden für die Erfüllung ihrer Aufgaben. Diese Regelung darf nicht umgangen werden. Es wird bei späteren Kontrollen festzustellen sein, in welchen Einzelfällen derartige Auskunftsersuchen an das BZR gerichtet werden.

32. Die ursprünglich bis zum 31. Dezember 1994 befristete **Befugnis des ZKA zur Überwachung des Brief-, Post- und Fernmeldeverkehrs** gem. § 39 AWG (14. TB S. 139, siehe auch oben Nr. 26.1) ist bis zum 31. Dezember 1996 verlängert worden (Art. 1 Nr. 15 des 8. Gesetzes zur Änderung des Außenwirtschaftsgesetzes BGBl. I 1994 S. 2068/2069). Die im Gesetz vorgesehene Zweckbindung nur für Stellen des Bundes gilt bedauerlicherweise weiterhin nicht für andere Stellen, wie z. B. sämtliche Landesbehörden einschließlich Polizei und Staatsanwaltschaften

33. Im 14. Tätigkeitsbericht (S. 146) hatte ich das Verfahren der **Sperrung von Datensätzen in der Datei NADIS-PZD** dargestellt. Das Bundesministerium des Innern teilt nunmehr meine Auffassung, daß gesperrte Datensätze, wie es das Bundesverfassungsschutzgesetz in § 12 Abs. 2 Satz 4 vorschreibt, nur noch mit Einwilligung des Betroffenen übermittelt werden dürfen. Die weitere Verarbeitung oder Nutzung wird dadurch auf die Übermittlung beschränkt, in die der Betroffene einwilligen muß.

    Im übrigen besteht Einigung, daß gesperrte Datensätze nach am Einzelfall orientierten Wiedervorlagefristen auf die Zulässigkeit der weiteren Speicherung kontrolliert werden.

34. In meinem 14. Tätigkeitsbericht (S. 147) habe ich über die Eingabe einer Petentin berichtet, die ihre Zustimmung zur **Einbeziehung in die Sicherheitsüberprüfung ihres beim Bundesnachrichtendienst tätigen Ehemannes** verweigert hatte. Ihrem Ehemann seien hierdurch erhebliche berufliche Nachteile entstanden, da ihm der Sicherheitsbescheid aberkannt worden war. Nachdem die Fragen zur Prüfkompetenz anläßlich meines ersten Kontrollbesuchs ausgeräumt waren, konnte ich bei einem zweiten Besuch beim Bundesnachrichtendienst die Sicherheitsüberprüfungsakte des Betroffenen einsehen. Nach langen Erörterungen habe ich nunmehr erreicht, daß die über die Petentin gespeicherten personenbezogenen Daten in der Personenzentraldatei beim BND gelöscht werden. Der BND hatte dies mit Hinweis auf § 2 Abs. 1 Nr. 1 BND-Gesetz ursprünglich abgelehnt, weil er der Auffassung war, die Speicherung sei zum Zwecke der Eigensicherung erforderlich. Dabei komme es lediglich darauf an, ob ein Gefährdungspotential vorhanden ist. Ich halte es für nicht mehr hinnehmbar, den Ehegatten eines BND-Bediensteten von vornherein als mögliches Sicherheitsrisiko anzusehen. Ein mögliches Gefährdungspotential kann sich nach meiner Auffassung nur aus den Umständen des Einzelfalles ergeben. Dies setzt eine Prüfung mit entsprechenden Tatsachenhinweisen voraus. Da solche nicht ersichtlich waren, hat der Bundesnachrichtendienst – meiner Anregung folgend – die Löschung der Daten vorgenommen.

Anlage 1 (zu Nr. 1.14)

Übersicht über durchgeführte Kontrollen, Beratungen und Informationsbesuche

Deutscher Bundestag (Verwaltung sowie Parlament nach § 26 Abs. 2 BDSG)

Bundeskanzleramt

Auswärtiges Amt

Bundesministerium des Innern

Bundesministerium der Justiz

Bundesministerium der Finanzen

Bundesministerium für Wirtschaft

Bundesministerium für Ernährung, Landwirtschaft und Forsten

Bundesministerium der Verteidigung

Bundesministerium für Familie und Senioren

Bundesministerium für Frauen und Jugend

Bundesministerium für Gesundheit

Bundesministerium für Verkehr

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit

Bundesministerium für Post und Telekommunikation

Bundesministerium für Raumordnung, Bauwesen und Städtebau

Bundesministerium für Forschung und Technologie

Bundesministerium für Bildung und Wissenschaft

Bundesnachrichtendienst

eine Botschaft

Statistisches Bundesamt – Außenstelle Berlin

Bundesverwaltungsamt mit Außenstellen Gießen, Rastatt und Empfingen

Bundesarchiv: Militärarchiv

Bundesamt für die Anerkennung ausländischer Flüchtlinge – Zentrale Nürnberg, Außenstellen Chemnitz und Zirndorf

Bundesamt für Verfassungsschutz

Bundeskriminalamt

ein Warnamt

Grenzschutzamt

Gruppe Fernmeldewesen des Bundesgrenzschutzes

zwei Grenzschutzämter

eine Grenzschutzstelle

Bundesamt für Sicherheit in der Informationstechnik

Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR – Zentrale Berlin, Außenstellen Schwerin, Dresden und Frankfurt/Oder

EUROPOL/EDE

Stiftung Preußischer Kulturbesitz

Generalbundesanwalt – Dienststelle Bundeszentralregister –

Kriminologische Zentralstelle e. V.

Bundesamt für Finanzen einschließlich Außenstelle Saarlouis

Zollkriminalamt

vier Hauptzollämter

fünf Zollämter

fünf Oberfinanzdirektionen

Bundesvermögensamt – Außenstelle Berlin

Deutsche Ausgleichsbank

Treuhandanstalt

Bundesausfuhramt

Monopolkommission

Bundesausführungsbehörde für Unfallversicherung

Bundesanstalt für Arbeit

fünf Arbeitsämter

Bundesversicherungsanstalt für Angestellte

Bundesknappschaft – eine Außenstelle

Deutsche Angestellten-Krankenkasse: Hauptverwaltung und eine Außenstelle

Postbeamtenkrankenkasse – eine Außenstelle

eine Betriebskrankenkasse

Hauptverband der gewerblichen Berufsgenossenschaften (HVBG)

zwei Berufsgenossenschaften

Zentrale ADV-Prüfung der Bundesverbände der Krankenkassen (ZAP)

MAD-Amt

Streitkräfteamt

Institut für Wehrmedizinalstatistik und Berichtswesen

ein Kreiswehrersatzamt

Bundesamt für den Zivildienst

zwei Zivildienstschulen

zwei Verwaltungsstellen Zivildienst

zwei Zivildienstgruppen

Bundesgesundheitsamt

Robert-Koch-Institut

Kraftfahrt-Bundesamt

Bundesamt für Seeschiffahrt und Hydrographie

Bundesoberseeamt

eine Wasser- und Schiffahrtsdirektion

Hauptverwaltung der Deutschen Bundesbahn

Deutsche Reichsbahn

Bundesamt für Strahlenschutz

Deutsche Bundespost Telekom, Generaldirektion

Deutsche Bundespost Postdienst, Generaldirektion

Deutsche Bundespost Postbank, Generaldirektion und eine Niederlassung

Produktzentrum Telesec der Deutschen Bundespost Telekom

drei Fernmeldeämter

Bundesdruckerei

Rentenrechnungsstelle Hannover

Deutsches Institut für Normung (DIN)

Deutscher Motoryachtverband e. V.

Deutscher Segler-Verband e. V.

AZ Direkt Marketing Bertelsmann GmbH

Anlage 2 (zu Nr. 1.14)

Übersicht über Beanstandungen nach § 25 BDSG

Bundesministerium der Finanzen

Zwei Verstöße gegen §§ 4, 15 Abs. 1 i.V. m. § 14 Abs. 2 BDSG durch unzulässige Kontrollmitteilungen von Hauptzollämtern an Finanzämter (s. Nr. 5.2)

Bundesministerium der Verteidigung

- Verstoß gegen §§ 4, 12 Abs. 4 i.V. m. 35 Abs. 2 Nrn. 1 und 3 BDSG durch Herausgabe von nicht gelöschten Tonträgern mit sensiblen personenbezogenen Daten an privaten Käufer ausgesonderter Diktiergeräte (s. Nr. 15.2).
- Verstoß gegen § 9 BDSG wegen fehlender Paginierung (s. Nr. 9.1.2.3).
- Verstoß gegen § 13 Abs. 1 BDSG wegen unzulässiger Datenerhebung durch uneingeschränkte Einsichtnahme in Beratungsakten von Sozialarbeitern durch Vorgesetzte (s. Nr. 31.2.1).
- Verstoß gegen § 14 Abs. 1 BDSG i. V. m. §§ 16, 17 der Sicherheitsrichtlinien wegen unterlassener Vernichtung von Unterlagen in einer Sicherheitsüberprüfungsakte beim MAD (s. Nr. 29.4).

Bundesministerium für Verkehr

Verstoß gegen § 24 Abs. 4 BDSG wegen mangelnder Unterstützung (s. Nr. 9.7.6).

Bundesministerium für Post und Telekommunikation

Verstoß gegen §§ 13 Abs. 1, 12 Abs. 4 i.V. mit 28 Abs. 1 Satz 2 BDSG wegen unzulässiger Datenerhebung durch die Anforderung von Diagnoselisten durch die Bundesdruckerei (s. Nr. 9.3.2).

Vorstand der Deutschen Bundespost Postdienst

Verstoß gegen § 11 BDSG im Rahmen der Aktion „Mein persönliches Adreßheft" (s. Nr. 20.3.1).

Vorstand der Deutschen Bundespost Telekom

Unzulässige Übermittlung von Nutzungsdaten solcher Btx-Kunden, die fälschlicherweise als Nichtzahler ausgewiesen wurden, an Btx-Anbieter; Verstoß gegen § 12 Abs. 3 TDSV (s. Nr. 20.2.6).

Bundesanstalt für Arbeit

- Verstoß gegen § 35 Abs. 1 SGB I bei der Durchführung von Gruppenmaßnahmen nach § 132 AFG (s. Nr. 11.7).
- Verstoß gegen § 24 Abs. 4 BDSG durch ein Arbeitsamt; hier: mangelnde Unterstützung des BfD durch unrichtige Angaben seitens der BA (s. Nr. 11.1).
- Verstoß gegen § 24 Abs. 4 BDSG durch ein Arbeitsamt; hier: mangelnde Mitwirkung und Unterstützung während einer Kontrolle (s. Nr. 11.2).

Vorstand der Deutschen Bundesbahn

- Verstoß gegen das Arztgeheimnis wegen unzulässiger Datenweitergabe an den Dienstherrn (s. Nr. 9.4.3).
- Verstoß gegen das Personalaktengeheimnis § 90 BBG.

Bundesversicherungsanstalt für Angestellte

Mitteilung seitens der BfA an den Arbeitgeber eines Versicherten; Verstoß gegen § 35 SGB I i.V. m. § 69 SGB X (s. Nr. 13.3.4).

Hauptverband der gewerblichen Berufsgenossenschaften (HVBG)

Verstöße gegen §§ 35 Abs. 1 SGB I, 79 Abs. 1 SGB X, §§ 4 Abs. 1 i.V. m. 13 Abs. 1 und 14 Abs. 1 BDSG sowie § 67 i.V. m. § 96 Abs. 3 SGB X wegen unzulässig geführter Zentraldateien (s. Nr. 14.1.2)

Vorstand der Berufsgenossenschaft der chemischen Industrie

- Verstoß gegen § 76 Abs. 2 Nr. 1 SGB X durch die Weitergabe ärztlicher Unterlagen (s. Nr. 10.8.1).
- Verstoß gegen § 69 SGB X i.V. m. § 35 SGB I wegen unzulässiger Datenübermittlung an Arbeitgeber (s. Nr. 14.3).

Drei gesetzliche Krankenkassen

Verstoß gegen § 79 SGB X (alte Fassung) i.V. m. § 13 BDSG durch Erhebung personenbezogener Daten zu Zwecken der Mitgliederwerbung ohne entsprechende Rechtsgrundlage (s. Nr. 12.3).

Vorstand der Südwestlichen Bau-Berufsgenossenschaft

- Verstoß gegen § 24 Abs. 4 BDSG wegen fehlender Unterstützung des BfD (s. Nr. 9.15).
- Verstoß gegen §§ 67 a Abs. 2 Satz 1, Abs. 4 SGB X i.V. m. §§ 37, 60 Abs. 1, 66 Abs. 1 und 2 SGB I wegen unzulässiger Erhebung jedweder Vorerkrankungen bei behandelnden und früher behandelnden Ärzten.
- Verstoß gegen § 90 c Abs. 4 BBG wegen fortdauernder Verweigerung der Akteneinsicht gegenüber dem Petenten.

Anlage 3 (zu Nr. 8.1)

Entschließung der 46. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 1993 zum Integrierten Verwaltungs- und Kontrollsystem – InVeKoS – (Verordnungen der EWG Nrn. 3508/92 und 3887/92)

Die vom Ministerrat der EG 1992 beschlossene Reform der gemeinsamen Agrarpolitik sieht die Angleichung der gemeinschaftlichen Preise für bestimmte Kulturpflanzen an den Weltmarkt vor und gewährt auf Antrag als Ausgleich für die dadurch bedingten Einkommenseinbußen flächen- und tierbezogene Zuwendungen an die Erzeuger. Zur Verhinderung einer mißbräuchlichen Verwendung von Fördermitteln hat die EG die Mitgliedsstaaten dabei zur Einführung eines „Integrierten Verwaltungs- und Kontrollsystem (InVeKoS)" verpflichtet. Diese haben danach integrierte Datenbanken mit Angaben über Flurstücke, deren kulturartige Nutzung sowie den Tierbestand einzurichten und in einem Mindestumfang entsprechende Kontrollen durchzuführen.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder hat die EG mit dem „Integrierten Verwaltungs- und Kontrollsystem" den Landwirtschaftsverwaltungen der Länder ein überwachungssystem verordnet, das dem Grundsatz der Verhältnismäßigkeit, insbesondere dem übermaßverbot, widersprechen kann. Insbesondere legt das EG-Recht für die Kontrolldichte nur ein Mindestmaß an Kontrollen, jedoch keine Obergrenze fest.

Zur Vermeidung unverhältnismäßiger Einschränkungen des informationellen Selbstbestimmungsrechts der betroffenen Landwirte fordern daher die Datenschutzbeauftragten des Bundes und der Länder,

- ortsunabhängige überwachungsmöglichkeiten (Fernerkundung mittels Satellit oder Flugzeug) nicht für eine flächendeckende Totalüberwachung einzusetzen, sondern auf den von der EG geforderten Stichprobenumfang zu beschränken;

- bei der Nutzung des Kontrollsystems InVeKoS und der darin gespeicherten personenbezogenen Daten den Grundsatz der Verhältnismäßigkeit und insbesondere der Zweckbindung zu beachten;

- nur dezentrale Datenbanken in den einzelnen Bundesländern einzurichten (keine Euro- oder Zentraldatenbank über Landwirte!), und an zentrale Datenbanken keine personenbezogenen Daten zu übermitteln;

- zu beachten, daß die EG-Verordnungen zu InVeKoS keine Rechtsgrundlage für eine Erweiterung der Nutzungen enthalten (z. B. zu Kontrollzwecken bei anderen landwirtschaftlichen Förderungsmaßnahmen oder außerhalb des landwirtschaftlichen Bereichs, z. B. zur Besteuerung).

Anlage 4 (zu Nr. 17.3)

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zu Chipkarten im Gesundheitswesen

Die Datenschutzbeauftragten von Bund und Länder verfolgen die zunehmende Verwendung von Chipkarten im Gesundheits- und Sozialwesen mit kritischer Aufmerksamkeit.

Chipkarte als gesetzliche Krankenversicherungskarte

Die Krankenversicherungskarte, die bis Ende des Jahres in allen Bundesländern eingeführt sein wird, darf nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten. Die Datenschutzbeauftragten überprüfen, ob

- die Krankenkassen nur die gesetzlich zulässigen Daten auf den Chipkarten speichern und
- die Kassenärztlichen Vereinigungen dafür sorgen, daß nur vom Bundesamt für Sicherheit in der Informationstechnik zertifizierte Lesegeräte und vom Bundesverband der Kassenärztlichen Vereinigungen geprüfte Programme eingesetzt werden.

Chipkarte als freiwillige Gesundheitskarte

Sogenannte „Gesundheitskarten", etwa „Service-Karten" von Krankenversicherungen und privaten Anbietern, „Notfall-Karten", „Apo(theken)-Cards" und „Röntgen-Karten" werden neben der Krankenversicherungskarte als freiwillige Patienen-Chipkarte angeboten und empfohlen. Während die Krankenversicherungskarte nach dem Sozialgesetzbuch nur wenige Identifikationsdaten enthalten darf, kann mit diesen „Gesundheitskarten" über viele medizinische und andere persönliche Daten schnell und umfassend verfügt werden.

Gegenüber der konventionellen Ausweiskarte oder einer Karte mit einem Magnetstreifen ist die Chipkarten-Technik ungleich komplexer und vielfältig nutzbar. Damit steigen auch die Mißbrauchsgefahren bei Verlust, Diebstahl oder unbemerktem Ablesen der Daten durch Dritte. Anders als bei Ausweiskarten mit Klartext können Chipkarten nur mit technischen Hilfsmitteln gelesen werden, die der Betroffene in der Regel nicht besitzt. So kann er kaum kontrollieren, sondern muß weitgehend darauf vertrauen, daß der Aussteller der Karte und sein Arzt nur die mit ihm vereinbarten Daten im Chip speichern, das Lesegerät auch wirklich alle gespeicherten Daten anzeigt und der Chip keine oder nur eindeutig vereinbarte Verarbeitungsprogramme enthält.

Die Freiwilligkeit der Entscheidung für oder gegen die Gesundheitskarte mit Chipkarten-Technik ist in der Praxis bisweilen nicht gewährleistet. So wird ein faktischer Zwang auf die Entscheidungsfreiheit des Betroffenen ausgeübt, wenn der Aussteller – etwa ein Krankenversicherungsunternehmen oder eine Krankenkasse – mit der Einführung der Chipkarte das bisherige konventionelle Verfahren erheblich ändert, z. B. den Schriftwechsel erschwert oder den Zugang zu Leistungen Karten-Inhabern vorbehält bzw. erleichert.

So stellt beispielsweise eine Kasse ihren Mitgliedern Bonuspunkte in Aussicht, wenn sie auf sog. Aktionstagen der Kasse Werte wie Blutzucker, Sauerstoffdynamik, Cholesterol sowie weitere spezielle medizinische Daten ohne ärztliche Konsultation messen und auf der Karte speichern und aktualisieren lassen. In Abhängigkeit von der Veränderung dieser Werte wird von der Kasse gegebenenfalls ein Arztbesuch empfohlen. Die Vergabe solcher Bonuspunkte widerspricht dem Prinzip der Freiwilligkeit bei der Erhebung der Daten für die Patienten-Chipkarte. Der Effekt wird noch verstärkt, indem die Kasse die „Möglichkeit einer Beitragsrückerstattung" in Aussicht stellt. Die Datenschutzbeauftragten des Bundes und der Länder sehen in dieser Art der Anwendung der Chipkarten-Technik das Risiko eines Mißbrauchs, solange der Inhalt und die Nutzung der Daten nicht mit den zuständigen Fachleuten – wie den Medizinern – und den Krankenkassen abgestimmt ist.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hält für den Einsatz und die Nutzung freiwilliger Patienten-Chipkarten zumindest – vorbehaltlich weiterer Punkte – die Gewährleistung folgender Voraussetzungen für erforderlich:

- Die Zuteilung einer Gesundheitskarte und die damit verbundene Speicherung von Gesundheitsdaten bedarf der schriftlichen Einwilligung des Betroffenen. Er ist vor der Erteilung der Einwilligung umfassend über Zweck, Inhalt und Verwendung der angebotenen Gesundheitskarte zu informieren.
- Die freiwillige Gesundheitskarte darf nicht – etwa durch Integration auf einem Chip – die Krankenversichertenkarte nach dem Sozialgesetzbuch verdrängen oder ersetzen.
- Die Karte ist technisch so zu gestalten, daß für die einzelnen Nutzungsarten nur die jeweils erforderlichen Daten zur Verfügung gestellt werden.
- Der Betroffene muß von Fall zu Fall frei und ohne Benachteiligung – z. B. gegenüber dem Arzt, der Krankenkasse oder der Versicherung – entscheiden können, die Gesundheitskarte zum Lesen der Gesundheitsdaten vorzulegen und ggf. den Zugriff auf bestimmte Daten zu beschränken. Er muß ferner frei entscheiden können, wer welche Daten in seinen Datenbestand übernehmen darf. Der Um-

fang der Daten, die gelesen oder übernommen werden dürfen, ist außerdem durch die gesetzliche Aufgabenstellung bzw. den Vertragszweck der Nutzer beschränkt.

- Der Kartenaussteller muß sicherstellen, daß der Betroffene jederzeit vom Inhalt der Gesundheitskarte unentgeltlich Kenntnis nehmen kann.
- Der Betroffene muß jederzeit Änderungen und Löschungen der gespeicherten Daten veranlassen können.

Die Datenschutzbeauftragten des Bundes und der Länder sprechen sich dafür aus, daß der Gesetzgeber dies durch bereichsspezifische Rechtsgrundlagen sicherstellt.

Anlage 5 (zu Nr. 4.2.1)

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zur Informationsverarbeitung im Strafverfahren

Die Datenschutzbeauftragten des Bundes und der Länder erinnern an ihre Vorschläge zu gesetzlichen Regelungen der Informationsverarbeitung im Strafverfahren, die sie seit 1981 unterbreitet haben.

Während die Befugnisse von Polizei und Staatsanwaltschaft zur Datenerhebung bei Ermittlungen mittlerweile in weitreichender Form gesetzlich abgesichert wurden, fehlen weiterhin Regelungen in der Strafprozeßordnung, wie die erhobenen Daten in Akten und Dateien weiter verarbeitet werden dürfen.

Die Datenschutzbeauftragten des Bundes und der Länder halten die Beachtung folgender Grundsätze für notwendig, die in den Entwürfen des Bundes (Art. 4 §§ 474 ff. StPO des Entwurfs für ein Verbrechensbekämpfungsgesetz – BT-Drucksache 12/6853) und der Länder (Entwurf eines Strafverfahrensänderungsgesetzes 1994 des Strafrechtsausschusses der Justizministerkonferenz) nicht ausreichend berücksichtigt sind:

1. Strafrechtliche Ermittungsakten enthalten eine Vielzahl höchstsensibler Daten insbesondere auch über Opfer von Straftaten und Zeugen, die deshalb eines wirksamen Schutzes bedürfen. Es würde den Besonderheiten der im Strafverfahren – auch mit Zwangsmitteln – erhobenen Daten nicht entsprechen, wenn Strafakten als Informationsquelle für jegliche Zwecke anderer Behörden oder von nicht am Strafverfahren Beteiligten dienten. Die einzelnen Zwecke und die zugriffsberechtigten Stellen sind daher abschließend normenklar festzulegen.

1.1 Insgesamt ist sicherzustellen, daß der in anderen Zweigen der öffentlichen Verwaltung verbindlich geltende Standard des Datenschutzes für Übermittlungen keinesfalls unterschritten wird.

1.2 Soweit ein unabweisbarer Bedarf anderer Stellen an Informationen aus Strafverfahren besteht, ist er in erster Linie durch Erteilung von Auskünften zu befriedigen. Akteneinsichtnahmen oder Aktenübersendungen können erst dann zugelassen werden, wenn eine Auskunftserteilung nicht ausreicht. Nicht erforderliche Aktenteile müssen ausgesondert werden. An Privatpersonen dürfen Informationen aus strafrechtlichen Ermittlungen nur weitergegeben werden, wenn deren rechtliche Interessen davon abhängen.

2. Bei Regelungen zur dateimäßigen Speicherung ist zu unterscheiden zwischen Systemen zur Vorgangsverwaltung (wie z. B. zentrale Namensdateien) und Dateien, die der Unterstützung strafprozessualer Ermittlungen dienen (z. B. Spurendokumentations- und Recherchesysteme).

2.1 Der Datensatz zur Vorgangsverwaltung ist auf die Angaben zu beschränken, die zum Auffinden der Akten und zur Information über den Verfahrensstand erforderlich sind. Daten über Personen, die keine Beschuldigten sind, dürfen nur dann erfaßt werden, wenn dies zur Vorgangsverwaltung zwingend erforderlich ist. In diesen Fällen bedarf es besonderer Zugriffs- und Verwendungsbeschränkungen.

In jedem Fall sind die Daten entsprechend dem Verfahrensstand zu aktualisieren. Vom Gesetzgeber sind konkrete Löschungsfristen vorzusehen. Die Speicherung ist längstens auf den Zeitpunkt zu begrenzen, für den die Akte aufbewahrt wird. Vorgangsverwaltungssysteme können so auch für eine wirksame Kontrolle der Aufbewahrungsfristen genutzt werden.

2.2 Die Staatsanwaltschaft kann sich zur Verwaltung ihres konventionell gespeicherten Datenmaterials grundsätzlich eines behördeninternen, automatisierten Nachweissystems bedienen. Länderübergreifende automatisierte Informationssysteme dürfen in Beachtung des Erforderlichkeitsprinzips demgegenüber allenfalls für solche Vorgänge errichtet werden, bei denen bestimmte Tatsachen die Prognose begründen, daß auf die erfaßten Daten zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben (erneut) zugegegriffen werden muß.

Eine solche Prognose wird in der Regel dann nicht gerechtfertigt sein, wenn das zugrundeliegende Verfahren mit einer Einstellung nach § 170 Abs. 2 StPO oder einem rechtskräftigen Freispruch abgeschlossen worden ist, sofern nicht auch nach Abschluß des Verfahrens noch tatsächliche Anhaltspunkte dafür vorliegen, daß der Beschuldigte eine strafbare Handlung begangen hat. Eine Bereitstellung von Daten jedenfalls zu Zwecken der Strafverfolgung wird ferner grundsätzlich dann nicht in Betracht kommen, wenn die Ermittlungen konkrete Anhaltspunkte dafür bieten, daß der Beschuldigte nicht erneut strafbare Handlungen begehen wird. Dies kann z. B. bei Fahrlässigkeitstaten der Fall sein. Bei laufenden Verfahren kann die Zulässigkeit der Aufnahme von Daten im Hinblick auf die Möglichkeiten einer Verbindung von Verfahren, die Einstellung nach § 154 StPO oder die Gesamtstrafenbildung gegeben sein.

2.3 Für einen Informationsverbund zwischen verschiedenen speichernden Staatsanwaltschaften mit der Möglichkeit eines Direktzugriffs auf die Daten der jeweils anderen Behörden ergibt sich als Voraussetzung, daß die Weitergabe aller dem Zugriff unterliegenden Daten zumindest bei ab-

strakter Betrachtung zur Erfüllung durch Rechtsnorm zugewiesener Aufgaben der übermittelnden oder der zugriffsberechtigten Stellen geeignet und angemessen sein muß.

Für den Bereich der Strafverfolgung gilt ein umfassendes Aufklärungsgebot (§§ 152 Abs. 2, 160 StPO). Die Staatsanwaltschaft kann im Rahmen ihrer Ermittlungen grundsätzlich ohne Rücksicht auf das Gewicht des Tatvorwurfs von allen öffentlichen Behörden – also auch von anderen Staatsanwaltschaften – Auskunft verlangen (§ 161 Satz 1 StPO). Diese Auskunftspflicht besteht über das Ermittlungsverfahren hinaus bis zum Abschluß des Strafverfahrens. Daten, die im Falle einer entsprechenden Anfrage zu mit einem Strafverfahren zusammenhängenden Zwecken offenbart werden müßten, können damit – ungeachtet der besonderen Voraussetzungen für die Errichtung eines Direktabrufverfahrens – von jeder Staatsanwaltschaft für andere Staatsanwaltschaften grundsätzlich auch in einem Informationssystem mit Direktabrufmöglichkeit bereitgestellt werden, sofern nur bestimmte Tatsachen die Annahme rechtfertigen, daß die Daten in einem Verfahren einer anderen Behörde verwertet werden müssen. Eine solche Annahme wird regelmäßig wiederum in den unter 2.2 dargestellten Fällen nicht zu begründen sein. Eine Bereitstellung von Daten wird darüber hinaus auch dann nicht erfolgen können, wenn diese einem besonderen Amtsgeheimnis unterliegen und deshalb auch auf Anforderung nicht ohne weiteres übermittelt werden dürften. Auf § 78 SGB X ist in diesem Zusammenhang hinzuweisen. Ein Direktabruf durch andere Stellen als Staatsanwaltschaften ist schon nach der Zweckbestimmung des Systems ausgeschlossen.

2.4 In der Praxis dienen derzeit die bestehenden polizeilichen Informationssysteme auch den Zwecken der Strafverfolgung. Eine Abstimmung der polizeilichen und der staatsanwaltschaftlichen Informationssysteme ist geboten. Eine weitere Abstimmung wird im Hinblick auf das Bundeszentralregister zu erfolgen haben, das ebenfalls Daten zu Zwecken der Strafverfolgung, aber auch der Strafvollstreckung speichert.

Die Datenschutzbeauftragten halten daher eine grundlegende Überarbeitung dieser Entwürfe für notwendig und bieten hierfür ihre Unterstützung an (vgl. Beschlüsse der Datenschutzkonferenzen vom 28./29. September 1981 zu „Mindestanforderungen für den Datenschutz bei den Zentralen Namenskarteien der Staatsanwaltschaften", vom 24./25. November 1986 „Überlegungen zu Regelungen der Informationsverarbeitung im Strafverfahren" und vom 5./6. April 1989 zum Entwurf eines Gesetzes zur Änderung und Ergänzung des Strafverfahrensrechts vom 3. November 1988).

Bayern enthielt sich der Stimme.

Anlage 6 (zu Nr. 20.1)

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Gesetzentwurf der Bundesregierung zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz – PTNeuOG, BR-Drs. 115/94 = BT-Drs. 12/6718) und zu der dafür erforderlichen Änderung des Grundgesetzes (BR-Drs. 114/94 = BT-Drs. 12/6717)

I.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, daß mit der Umwandlung der Deutschen Bundespost POSTDIENST in die Deutsche Post AG und der Deutschen Bundespost TELEKOM in die Deutsche Telekom AG zwei staatliche Einrichtungen aufhören zu existieren, gegenüber denen sich der Bürger bisher unmittelbar auf das Post- und Fernmeldegeheimnis berufen kann. Sie treten deshalb dafür ein, in der Verfassung sicherzustellen, daß jeder, der Post- und Fernmeldedienstleistungen erbringt, das Post- und Fernmeldegeheimnis zu wahren hat.

II.

Im Gesetz zur Neuordnung des Postwesens und der Telekommunikation ist ein den Vorgaben des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 und in seinem Fangschaltungsbeschluß vom 25. März 1992 entsprechender Schutz von Individualrechten zu gewährleisten.

Die Datenschutzbeauftragten halten inbesondere folgende Änderungen des Gesetzentwurfs für erforderlich:

a) Der Umfang der zulässigen Verarbeitung personenbezogener Daten im Post- und Telekommunikationswesen ist im Gesetz selbst festzulegen; lediglich deren konkrete Ausgestaltung kann der Regelung durch Rechtsverordnungen überlassen bleiben.

b) Die Gewährleistung des Datenschutzes und des Post- und Fernmeldegeheimnisses muß in den Katalog der Ziele der Regulierung aufgenommen werden.

c) Das Post- und Telekommunikationswesen muß auf Dauer – auch nach dem Wegfall der Monopole – einer effektiven, unabhängigen datenschutzrechtlichen Kontrolle von Amts wegen nach bundesweit einheitlichen Kritierien unterworfen bleiben, auch soweit personenbezogene Daten nicht in Dateien verarbeitet werden.

d) Die Frist für die Speicherung von Verbindungsdaten zur Ermittlung und zum Nachweis der Entgelte ist präzise festzulegen.

e) Die vorgesehene Vorschrift zum Einzelentgeltachweis schränkt den Kreis der Einrichtungen, die Telefonberatung durchführen und die nicht auf Einzelentgeltnachweisen erscheinen sollen, in unakzeptabler Weise ein. Dem Schutz des informationellen Selbstbestimmungsrechtes und des Fernmeldegeheimnisses der Angerufenen würde es dagegen am ehesten entsprechen, wenn jeder inländische Anschlußinhaber selbst entscheiden kann, ob und gegebenenfalls wie seine Rufnummer auf Einzelentgeltnachweisen erscheinen soll. Damit wäre auch die Anonymität von Anrufen bei Beratungseinrichtungen unbürokratisch sicherzustellen. Ein entsprechendes Verfahren wird in den Niederlanden bereits praktiziert.

f) Es wäre völlig unangemessen, wenn in Zukunft erlaubt würde, daß die Telekommunikationsunternehmen Nachrichteninhalte über die Befugnisse des § 14 a Fernmeldeanlagengesetz hinaus auch für die Unterbindung von Leistungserschleichungen und sonstiger rechtswidriger Inanspruchnahme des Telekommunikationsnetzes und seiner Einrichtungen sowie von Telekommunikations- und Informationsdienstleistungen erheben, verarbeiten und nutzen dürften.

III.

Die Datenschutzbeauftragten betonen, daß angesichts der neuen technischen Möglichkeiten digitaler Kommunikations- und Informationsdienste und der mit ihrer Nutzung zwangsläufig verbundenen Datenverarbeitung eine grundlegende Überarbeitung des § 12 Fernmeldeanlagengesetz, der die Weitergabe vorhandener Telekommunikationsdaten in Strafverfahren erlaubt, überfällig ist. Sie erinnern an die Umsetzung der entsprechenden Entschließung des Bundesrates vom 27. August 1991 (BR-Drs. 416/91).

Anlage 7 (zu Nr. 3.1.1)

Entschließung der 47. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1994 zum Ausländerzentralregistergesetz

Das Ausländerzentralregister beim Bundesverwaltungsamt in Köln existiert seit 40 Jahren ohne gesetzliche Grundlage. Derzeit stehen den verschiedenen Benutzern des Registers Daten zu mindestens 8 Millionen Ausländern, die sich in der Bundesrepublik aufhalten oder aufgehalten haben, zur Verfügung. Gespeichert sind neben Daten zur Identifizierung und weiteren Beschreibung der Person insbesondere Angaben zum Meldestatus, Aufenthaltsrecht und Asylverfahren.

Die Datenschutzbeauftragten des Bundes und der Länder haben immer wieder darauf hingewiesen, daß die Führung eines derartigen Registers ohne gesetzliche Regelung mit dem vom Grundgesetz Deutschen wie Ausländern gleichermaßen garantierten Recht auf informationelle Selbstbestimmung unvereinbar ist. Sie begrüßen daher, daß mit dem am 2. März 1994 vom Bundeskabinett beschlossenen Entwurf für ein Ausländerzentralregistergesetz eine gesetzliche Grundlage geschaffen werden soll.

Zwar enthält dieser Gesetzentwurf gegenüber früheren Entwürfen eine Reihe datenschutzrechtlicher Verbesserungen, Bedenken bestehen jedoch weiterhin: Die Datenschutzbeauftragten wenden sich insbesondere dagegen, daß das Ausländerzentralregister nicht nur als Informations- und Kommunikationssystem für die mit der Durchführung ausländer- und asylrechtlicher Vorschriften betrauten Behörden dienen, sondern darüber hinaus als Informationsverbund für Aufgaben der Polizei, Strafverfolgungsorgane und Nachrichtendienste zur Verfügung stehen soll.

Die Funktionserweiterung wird deutlich durch die Speicherung von Erkenntnissen der Sicherheitsbehörden zu Ausländern in das Register. So soll der INPOL-Fahndungsbestand des BKA, soweit er Ausschreibungen zur Festnahme und zur Aufenthaltsermittlung von Ausländern enthält, in das Ausländerzentralregister übernommen werden. Gleiches gilt für die vorgesehene Speicherung von Angaben zu Personen, bei denen Anhaltspunkte für den Verdacht bestehten, daß sie im einzelnen bezeichnete Straftaten planen, begehen oder begangen haben. Diese Informationen dienen nicht einem Informationsbedarf zur Erfüllung ausländerbehördlicher Aufgaben, sondern – worauf die Entwurfsbegründung hinweist – der Kriminalitätsbekämpfung. Für diese Zwecke stehen den Sicherheitsbehörden aber eigene Informationssysteme zur Verfügung. Nach Auffassung der Datenschutzbeauftragten dürfen deshalb derartige Erkenntnisse nicht in das Register aufgenommen werden.

Die im Entwurf vorgesehenen Voraussetzungen unter denen u. a. für Polizeibehörden, Staatsanwaltschaften und Nachrichtendienste automatisierte Abrufverfahren eingerichtet werden können, stellen keine wirksamen Vorkehrungen für eine Begrenzung der Abrufe dar. Besonders problematisch ist der geplante automatisierte Zugriff durch die Nachrichtendienste auf einen – wenn auch reduzierten – Datensatz. Für die Dienste ist in den jeweiligen bereichsspezifischen Gesetzen der automatisierte Abruf aus anderen Datenbeständen ausgeschlossen. Die Erforderlichkeit derartiger Abrufe ist in keiner Weise belegt. Die Datenschutzbeauftragten sprechen sich deshalb dafür aus, zumindest auf den automatisierten Abruf durch Nachrichtendienste zu verzichten.

Bayern stimmte gegen diese Entschließung.

Anlage 8 (zu Nr. 22.1.1)

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zum Vorschlag der Kommission der Europäischen Union für eine Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik – EG-Statistikverordnung – *) (KOM(94) 78 endg.; Ratsdok. 5615/94 = BR-Drs. 283/94)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen, daß die Europäische Union eine allgemeine Regelung für die Gemeinschaftsstatistik trifft, weisen allerdings daraufhin, daß die datenschutzrechtliche Entwicklung bei der Europäischen Union mit dem Aufbau der europäischen Statistik keineswegs Schritt gehalten hat.

Sie stellen mit Besorgnis fest, daß der vorliegende Vorschlag einer EG-Statistikverordnung die nationalen datenschutzrechtlichen Grundsätze und wesentliche Standards des Statistikrechts weitgehend nicht berücksichtigt. Sie fordern daher zur Wahrung des Rechts der Betroffenen auf informationelle Selbstbestimmung mit Nachdruck, daß die Bundesregierung ihre Bedenken gegen diesen Vorschlag geltend macht und diese bei den Beratungen auf europäischer Ebene zum Tragen bringt.

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen ausdrücklich den Beschluß des Deutschen Bundesrates vom 8. Juli 1994 (BR-Drs. 283/94 – Beschluß –).

Gegen den vorgelegten Vorschlag einer **Verordnung (EG) des Rates über die Tätigkeit der Gemeinschaft im Bereich der Statistik** (EG-Statistikverordnung) erheben sie insbesondere die folgenden datenschutzrechtlichen Bedenken:

1. In Art. 1 sollte als die zuständige Gemeinschaftsdienststelle unmißverständlich das Statistische Amt der Europäischen Gemeinschaften (EUROSTAT) bestimmt werden, weil die erforderlichen rechtlichen, administrativen, technischen und organisatorischen Maßnahmen – insbesondere zur Sicherung der Zweckbindung der zu statistischen Zwecken erhobenen Daten sowie zur Wahrung der statistischen Geheimhaltung – bei dieser Stelle bereits aufgrund der EG-Übermittlungsverordnung 1588/90 vom 11. Juni 1990 getroffen werden können. Eine jederzeit revidierbare Organisationsentscheidung der Kommission darüber, welche Dienststelle der Europäischen Union für statistische Aufgaben zuständig ist, birgt dagegen die Gefahr, daß Daten an unterschiedliche Stellen der Kommission zu unterschiedlichen Zwecken übermittelt werden.

   Zugleich sollte EUROSTAT zumindestens einen der Selbständigkeit der Statistischen Ämter in der Bundesrepublik Deutschland vergleichbaren organisationsrechtlichen Status erhalten, der die unter dem Gesichtspunkt der Objektivität und Neutralität gebotenen Eigenständigkeit bei der Aufgabenerfüllung garantiert. Dies könnte anläßlich der für 1996 vorgesehenen Revision des Vertrages über die Europäische Union geschehen.

2. Das mehrjährige statistische Programm sollte nicht wie in Art. 3 vorgesehen von der Kommission beschlossen werden. Die grundlegenden Entscheidungen über die Bürger belastende Datenerhebungen sollten dem Rat mit Zustimmung des Europäischen Parlaments vorbehalten bleiben. Dabei sollte der Planungscharakter des Programms in den Vordergrund gestellt werden.

3. Art. 5 sollte festlegen, daß statistische Einzelmaßnahmen durch einen Rechtsakt gemäß dem Verfahren nach Art. 189 b EG-Vertrag angeordnet werden. Dies gilt auch für die statistische Auswertung von Daten, die bei den administrativen Stellen bereits vorliegen (sog. Sekundärstatistik). Die im Vorschlag vorgesehene generelle Befugnis der Kommission, statistische Einzelmaßnahmen zu regeln, ist viel zu weitgehend.

4. Die in Art. 12 vorgesehene Übertragung der Befugnis zur Organisation der Verbreitung der statistischen Daten auf die Kommission widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag, aus dem folgt, daß grundsätzlich die Mitgliedstaaten nach ihrem nationalen Recht zur Verbreitung der statistischen Daten zuständig sind. Ferner sollte in Art. 12 festgelegt werden, daß an Stellen außerhalb der statistischen Gemeinschaftsdienststelle nur nicht-vertrauliche statistische Daten übermittelt werden dürfen.

5. Der in Art. 13 gegenüber der Definition in der EG-Übermittlungsverordnung 1588/90 neu definierte Begriff „statistische Geheimhaltung" muß präzisiert werden. Dazu gehört insbesondere, daß festgelegt wird, unter welchen Voraussetzungen statistische Daten vertraulich sind und nicht nur als vertraulich gelten. Dies gilt um so mehr, als im Verordnungsvorschlag dieser Begriff nicht nur in Art. 13, sondern auch in Art. 9 Abs. 2 – allerdings mit einem anderen Begriffsinhalt – definiert wird. Der Begriff „statistische Geheimhaltung" sollte an einer Stelle in der Verordnung und so definiert werden, daß er Art. 2 Nr. 1 der EG-Übermittlungsverordnung 1588/90 und damit den derzeit geltenden nationalen Begriffsbestimmungen entspricht. Dies stände auch im Einklang mit dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag.

6. Gemäß dem Grundsatz der Subsidiarität sollte – ebenso wie die Befugnis zur Verbreitung statistischer Ergebnisse (Art. 11 Abs. 1) – auch die Fest-

*) Entschließung im schriftlichen Verfahren vom 25. August 1994

legung der Zuständigkeit für die Durchführung der statistischen Einzelmaßnahmen (Art. 7) den Mitgliedstaaten überlassen bleiben.

7. Auch die in Art. 16 vorgesehene generelle Zugangsregelung einzelstaatlicher Stellen und der Gemeinschaftsdienststelle zu Registern der Verwaltung widerspricht dem Grundsatz der Subsidiarität nach Art. 3 b EG-Vertrag. Dieser gebietet hier, daß – jedenfalls grundsätzlich – die Mitgliedstaaten zu bestimmen haben, in welcher Weise sich die für die Erstellung der Gemeinschaftsstatistiken zuständigen nationalen Stellen Daten beschaffen. Damit ist aber nicht zu vereinbaren, daß auch Stellen der Kommission unmittelbar Zugang zu nationalen Verwaltungsregistern haben sollen.

   Ferner bleibt unklar, ob die nach Art. 16 erhobenen Daten Erhebungs- oder Hilfsmerkmale sein sollen. Im übrigen darf über Art. 16 ein Zugang zu solchen personenbezogenen Daten, die nach nationalem Recht einer besonderen Geheimhaltung, z. B. dem Steuer- oder auch dem Sozialgeheimnis unterliegen, nicht eröffnet werden.

8. Die Regelung des Art. 17 ist mißglückt. Allem Anschein nach soll hier eine weitgehende Ausnahmeregelung von der statistischen Geheimhaltung zugunsten von Forschungsinstituten, einzelner Forscher und von für die Erstellung von Nicht-Gemeinschaftsstatistiken zuständigen Stellen vorgesehen werden, die die Möglichkeit eröffnet, die in diesem Bereich geltenden strengeren nationalen Regelungen zu umgehen. Außerdem würde von der für EUROSTAT geltenden EG-Übermittlungsverordnung 1588/90 abgewichen werden. Art. 17 sollte deshalb so gefaßt werden, daß die nationalen Zugangsregelungen für Einrichtungen mit der Aufgabe der unabhängigen wissenschaftlichen Forschung nicht umgangen werden können.

9. Der Vorschlag der Kommission sieht weder eine alsbaldige Trennung und Aufbewahrung von Erhebungs- und Hilfsmerkmalen noch eine alsbaldige Löschung personenbezogener Hilfsmerkmale vor. In der Bundesrepublik Deutschland dagegen gehören entsprechende Regelungen (vgl. § 12 BStatG) zum Kernbereich des Statistikrechts. Im Volkszählungsurteil hat das Bundesverfassungsgericht ihnen grundrechtssichernde Bedeutung beigemessen.

10. Schließlich fehlt es für die Organe der Europäischen Union noch immer an einer unabhängigen und effektiven Datenschutzkontrollinstanz, an die sich jeder wenden kann, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten durch Stellen der Europäischen Union in seinen Rechten verletzt zu sein.

Anlage 9 (zu Nr. 28.2)

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu: Vorschläge zur Überprüfung der Erforderlichkeit polizeilicher Befugnisse und deren Auswirkungen für die Rechte der Betroffenen

Angesichts der aktuellen Diskussion über die innere Sicherheit weisen die Datenschutzbeauftragten des Bundes und der Länder darauf hin, daß umfangreiche polizeiliche Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten, insbesondere im technischen Bereich, gesetzlich verankert worden sind.

Zum Kreis der Betroffenen zählen dabei nicht nur Personen, gegen die Verdachtsgründe vorliegen, sondern auch nichtverdächtige Kontakt- und Begleitpersonen und Unbeteiligte, deren Schutz nach Auffassung der Datenschutzbeauftragten besonders wichtig ist.

Vor diesem Hintergrund schlagen die Datenschutzbeauftragten vor, den derzeitigen Erkenntnisstand über die Erforderlichkeit polizeilicher Befugnisse zur Erhebung und Verarbeitung personenbezogener Daten sowie ihre Auswirkungen auf die Rechte der Betroffenen durch folgende Maßnahmen zu verbessern:

1. Die Datenschutzbeauftragten teilen die von einigen Innenministern vertretene Auffassung, daß bloße Angaben über Einsatzzahlen der besonderen Befugnisse zur Datenerhebung nur einen begrenzten Aussagewert haben. Aufschluß über die tatsächliche Praxis, ihre Erforderlichkeit und Verhältnismäßigkeit läßt sich nur durch Überprüfung und Auswertung der einzelnen Einsätze gewinnen. Hierzu müssen unter Beteiligung der Datenschutzbeauftragten und der Wissenschaft, insbesondere der Kriminologie und des Polizeirechts, objektive und nachprüfbare Auswertungskriterien entwickelt werden.

   Die Datenschutzbeauftragten begrüßen daher die Initiative für eine sog. Rechtstatsachensammlung, die Erhebungen zu polizeilichen Ermittlungsmethoden und Eingriffsbefugnissen durchführen soll. Sie schlagen vor, in diese Rechtstatsachensammlung insbesondere Angaben über den Anlaß einer Datenerhebung mit besonderen Mitteln, die Örtlichkeit und die Dauer der Maßnahme, den Umfang der überwachten Gespräche, den betroffenen Personenkreis sowie die Anzahl der ermittelten, verurteilten, aber auch der entlasteten Personen einzubeziehen. Derartige Aufstellungen wären nicht nur für elektronische Überwachungsmethoden, sondern auch für Observationen, den Einsatz verdeckter Ermittler und V-Personen sowie für Rasterfahndungen denkbar.

2. Einige Polizeigesetze verpflichten dazu, zu überprüfen, ob es notwendig ist, bestehende Dateien weiterzuführen oder zu ändern. Dabei soll nicht nur darauf eingegangen werden, ob die Anwendungen, d. h. die Dateien, weiterhin erforderlich sind, sondern auch auf ihren Nutzen sowie auf ihre Schwachstellen und Mängel. Ferner sind Vorschläge zu machen, wie festgestellte Defizite beseitigt oder minimiert werden können.

3. Die Datenschutzbeauftragten gehen davon aus, daß sie bei den Überlegungen zur Rechtstatsachensammlung rechtzeitig beteiligt und die jeweiligen Materialien und Zwischenergebnisse mit ihnen erörtert werden.

Anlage 10 (zu Nr. 4.2.1)

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu: Fehlende bereichsspezifische gesetzliche Regelungen bei der Justiz

Obwohl seit dem Volkszählungsurteil des Bundesverfassungsgerichts mehr als 10 Jahre vergangen sind, werden im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet. Stattdessen sind in den letzten Jahren in zunehmendem Maße automatisierte Verfahren neu eingesetzt worden. Die Eingriffe in das Recht auf informationelle Selbstbestimmung stützen die Justizverwaltungen auf die Rechtsprechung des Bundesverfassungsgerichts zum sog. Übergangsbonus.

Die Datenschutzbeauftragten des Bundes und der Länder weisen im Hinblick auf die kommende Legislaturperiode den Bundesgesetzgeber erneut darauf hin, daß gesetzliche Regelungen im Bereich der Justiz überfällig sind. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muß vorab unter datenschutzrechtlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und verarbeitung in welchem Umfang erforderlich ist. Der zur Zeit dem Bundesrat vorliegende Entwurf eines Strafverfahrensänderungsgesetzes beispielsweise wird datenschutzrechtlichen Anforderungen in keiner Weise gerecht.

Im Bereich der Justiz fehlen ausreichende gesetzliche Regelungen für die

- Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien,
- Datenerhebung, -verarbeitung und -nutzung im Strafvollzug,
- Übermittlung von Daten aus den bei Gerichten geführten Registern (z. B. Grundbuch) und deren Nutzung durch die Empfänger,
- Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentliche Stellen (Justizmitteilungsgesetz)
- Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien.

Eine Berufung auf den sog. Übergangsbonus auf unbegrenzte Zeit steht nicht in Übereinstimmung mit der Rechtsprechung des Bundesverfassungsgerichts. Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe in der neuen Legislaturperiode unverzüglich bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes des Bürgers entgegenwirken.

Anlage 11 (zu Nr. 23.2.3.2)

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu: Datenschutzrechtliche Anforderungen an ein Übereinkommen der Mitgliedstaaten der Europäischen Union über die Errichtung eines europäischen Polizeiamtes (EUROPOL)

Die Datenschutzbeauftragten der Länder gehen gemeinsam mit dem Bundesdatenschutzbeauftragten davon aus, daß bei den Verhandlungen mindestens folgende Punkte berücksichtigt werden:

- Das Übereinkommen muß der verfassungsrechtlichen Kompetenzverteilung in Bund und Ländern für die Polizei entsprechen. Die materielle Verantwortung für die Datenverarbeitung muß, soweit die Daten von Landesbehörden erhoben worden sind, weiterhin bei den Ländern liegen. Davon bleiben die Zuständigkeiten und die dazugehörigen Befugnisse des BKA als nationale Stelle für den Informationsverkehr mit EUROPOL unberührt.
- Die Regelungen zur Verarbeitung personenbezogener Daten müssen präzise sein und dem Grundsatz der Verhältnismäßigkeit entsprechen. Beispielsweise erfüllen die in den bisherigen Entwürfen vorgesehenen Befugnisse zur europaweiten Speicherung von Daten unbeteiligter Personen diese Voraussetzungen nicht.

Die Datenschutzbeauftragten erwarten, daß die deutsche Seite eine Klarstellung über die Verantwortung der Länder, zum Beispiel durch eine Protokollerklärung zum EUROPOL-Übereinkommen, trifft.

Anlage 12 (zu Nr. 26.1, 28.1 und 28.2)

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zu Art. 12 Verbrechensbekämpfungsgesetz, zur Trennung von Polizei und Nachrichtendiensten

Geheimdienstliche Informationsmacht und polizeiliche Exekutivbefugnisse müssen strikt getrennt bleiben. Die Datenschutzbeauftragten des Bundes und der Länder stellen mit Besorgnis Entwicklungen fest, die die klare Trennungslinie zwischen Nachrichtendiensten und Polizeibehörden weiter zu verwischen drohen. Dies betrifft vor allem den Einsatz des Bundesnachrichtendienstes nach dem Verbrechensbekämpfungsgesetz:

- Der BND erhält danach bei der Fernmeldeaufklärung auch Befugnisse, die auf eine gezielte Erhebung von Daten für polizeiliche Zwecke hinauslaufen können. Deshalb ist bei dem Vollzug des Gesetzes darauf zu achten, daß nicht gezielt Informationen gesammelt werden, die vom Auftrag des BND nicht umfaßt werden.
- Zwischen nachrichtendienstlichen Vorfelderkenntnissen und polizeilichen Zwangsmaßnahmen ist ein Filter erforderlich, der vor allem Unbeteiligte vor überzogenen Belastungen schützt.

Die Datenschutzbeauftragten fordern, für die Zusammenarbeit von Nachrichtendiensten und Polizei in der Durchführung und Gesetzgebung das Trennungsgebot strikt zu beachten. Dies gilt auch bei der Fernmeldeaufklärung des BND. Eine wirksame Kontrolle durch den Datenschutzbeauftragten in diesem sensiblen Bereich ist auch nach der Rechtsprechung des Bundesverfassungsgerichts sicherzustellen.

Anlage 13 (zu Nr. 20.2.12)

Entschließung der 48. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. September 1994 zur: Geänderter Vorschlag für eine Europäische Richtlinie zum Datenschutz im ISDN und in Mobilfunknetzen vom 13. Juni 1994 (KOM (94) 128 endg. – COD 288

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt es, daß die Europäische Kommission mit der Vorlage des geänderten Vorschlags für eine Richtlinie zum Datenschutz im ISDN ihre Absicht bekräftigt hat, unionsweit bereichsspezifische Regelungen für den Datenschutz in Telekommunikationsnetzen zu schaffen. Es kann kein Zweifel daran bestehen, daß die digitalen Telekommunikationsnetze in der Europäischen Union zunehmend zur wichtigsten Infrastruktur für die Verarbeitung personenbezogener Daten werden. Der Regelungsdruck wird erhöht durch die Tatsache, daß die Europäische Union die rechtlichen und technischen Voraussetzungen für die Liberalisierung der Telekommunikationsmärkte in weiten Bereichen bereits geschaffen hat und mehrere Mitgliedsstaaten, darunter Deutschland, derzeit ihr nationales Telekommunikationsrecht auf die Vorgaben der EU umstellen.

Aus diesem Grund sollte der geänderte Vorschlag für eine ISDN-Richtlinie so bald wie möglich vom Ministerrat und vom Europäischen Parlament abschließend beraten werden. Die Bundesregierung sollte die deutsche Ratspräsidentschaft dazu nutzen, den geänderten Vorschlag für eine ISDN-Richtlinie im Rat behandeln zu lassen.

Dabei sollte sich die Bundesregierung insbesondere für folgende Verbesserungen des Richtlinienvorschlags aus datenschutzrechtlicher Sicht einsetzen:

1. Für Telekommunikationsorganisationen und Diensteanbieter müssen die gleichen gemeinschaftsrechtlichen Regelungen zum Datenschutz gelten. Die Verarbeitung personenbezogener Daten durch Diensteanbieter darf nicht privilegiert werden.
2. Die Beschränkung der Datenverarbeitung auf Zwecke der Telekommunikation sollte wieder in die Richtlinie aufgenommen werden. Der allgemeine Zweckbindungsgrundsatz der Datenschutzrichtlinie läßt die Zweckentfremdung schon bei „berechtigten Interessen" der Verarbeiter zu. Das ist angesichts zunehmender Diversifizierung der Aktivitäten von Netzbetreibern und Diensteanbietern eine zu weitgehende Lockerung der Zweckbindung im Telekommunikationsbereich.
3. Das ursprünglich vorgesehene Verbot, personenbezogene Daten zur Erstellung von elektronischen Profilen der Teilnehmer zu nutzen, sollte wieder in die Richtlinie aufgenommen werden.
4. Die Speicherung von Inhaltsdaten nach Beendigung der Übertragung sollte – wie im ursprünglichen Richtlinienentwurf vorgesehen – untersagt werden.
5. Die Vertraulichkeit der Kommunikationsbeziehungen und -inhalte (Fernmeldegeheimnis) sollte – wie es der ursprüngliche Richtlinienvorschlag ebenfalls vorsah – auf Unionsebene garantiert werden.
6. Um eine Harmonisierung des Gemeinschaftsrechts beim Einzelgebührennachweis zu erreichen, sollten konkrete Vorgaben in die Richtlinie aufgenommen werden, z. B. indem den angerufenen Teilnehmern die Aufnahme ihrer Rufnummer in Einzelgebührennachweise freigestellt wird.
7. Im Fall der Anrufweiterschaltung sollte die automatische Information des anrufenden Teilnehmers darüber, daß sein Anruf (z. B. bei einem Arzt) an einen Dritten weitergeschaltet wird, gewährleistet sein.

Die Konferenz begrüßt die im geänderten Vorschlag vorgesehene Kostenfreiheit für die verschiedenen Optionen der Anzeige der Rufnummer des Anrufers und für die Nichtaufnahme von Daten in das Teilnehmerverzeichnis (Telefonbuch).

Diese Vorschläge berücksichtigen das Subsidiaritätsprinzip und beschränken sich auf Änderungen, die zur Gewährleistung der Vertraulichkeit der Kommunikation in der Europäischen Union realisiert werden müssen. Zudem wird die Europäische Union insoweit im Rahmen ihrer ausschließlichen Zuständigkeit tätig. Die Konferenz bittet auch die Entscheidungsträger auf Unionsebene sowie die Datenschutzbehörden der anderen Mitgliedsstaaten, diese Anregungen zu unterstützen.

Anlage 14 (zu Nr. 20.2.12)

Gemeinsame Erklärung der Europäischen Datenschutzkonferenz vom 25./26. Mai 1994 zu dem Verhältnis zwischen den Datenschutzrichtlinien des Europäischen Parlamentes und des Rates und Maßnahmen zur Entwicklung neuer Telekommunikationsnetze und -dienste

Seit der Veröffentlichung des Grünbuchs über die Entwicklung des gemeinsamen Marktes für Telekommunikationsdienstleistungen und Telekommunikationsgeräte (KOM (87) 290, 30.06.1987) hat die Europäische Kommission zahlreiche Vorschläge für Richtlinien und andere Maßnahmen zur schnellen Einführung neuer Telekommunikationsdienste und zum Aufbau transeuropäischer Telekommunikationsnetze gemacht. Einige dieser Vorschläge sind bereits angenommen worden oder werden bald angenommen.

Während keine dieser vorgeschlagenen oder beschlossenen Maßnahmen selbst ein hinreichendes Niveau zum Schutz personenbezogener Daten und der Privatsphäre von Unionsbürgern vorsieht, werden die wichtigen Vorschläge für eine Richtlinie betreffend den Schutz personenbezogener Daten und der Privatsphäre im Zusammenhang digitaler Telekommunikationsnetze (ISDN-Richtlinie SYN 288) und für eine Rahmenrichtlinie zum Schutz natürlicher Personen bei der Verarbeitung personenbezogene Daten und zum freien Datenverkehr (Rahmenrichtlinie SYN 287) nur zögerlich beraten.

Die Europäischen Datenschutzbeauftragten sehen die konkrete Gefahr, daß beide Datenschutzrichtlinien schon obsolet sein könnten, wenn sie schließlich in Kraft gesetzt werden, weil zahlreiche spezielle Maßnahmen der Union zur Einführung neuer Telekommunikationsdienste und -netze dann bereits umgesetzt sein werden. Die Datenschutzbeauftragten halten eine Synchronisierung und Harmonisierung zwischen den Datenschutzrichtlinien und Richtlinien sowie anderen Maßnahmen zur Entwicklung von neuen Telekommunikationsdiensten und -netzen für dringend erforderlich.

Es gibt zahlreiche Vorschläge und Dokumente auf europäischer Ebene im Bereich Telekommunikation, die in bisher unbekanntem Ausmaß zu einer Verarbeitung personenbezogener Daten führen werden, die aber Probleme des Persönlichkeitsschutzes und des Datenschutzes nicht einmal erwähnen. Ein aktuelles Beispiel ist die vorgeschlagene Verordnung des Rates über Gemeinschaftszuschüsse für transeuropäische Netze (KOM (94) 62 endg.).

Die Europäischen Datenschutzbeauftragten fordern deshalb die Organe der Europäischen Union auf, spezielle Datenschutzvorschriften in diejenigen Rechtsakte in diesem Bereich aufzunehmen, deren Verabschiedung vor der Abnahme der Rahmenrichtlinie und der Richtlinie zum Datenschutz im ISDN für notwendig gehalten wird.

Anlage 15 (zu Nr. 26.6)

Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom April 1994 zu dem Entwurf der NADIS-Richtlinien

Das von den Verfassungsschutzbehörden des Bundes und der Länder betriebene Verbundsystem NADIS-PZD (Nachrichtendienstliches Informationssystem/ Personenzentraldatei) ist nach den Vorgaben der in Überarbeitung befindlichen NADIS-Richtlinien und der nunmehr erstellten Dateianordnung als Aktenhinweissystem zu qualifizieren. Die NADIS-Richtlinien und die Dateianordnung haben sich hinsichtlich ihres Regelungsgehaltes an den Bestimmungen der Verfassungsschutzgesetze zu orientieren.

Die Datenschutzbeauftragten des Bundes und der Länder halten den Entwurf der NADIS-Richtlinien und der Dateianordnung für die Personenzentraldatei für zu weitgehend und fordern deshalb:

- Die in der Personenzentraldatei gespeicherten personenbezogenen Daten sind auf das unerläßlich notwendige Maß zu reduzieren. Eine solche automatisierte Datei darf nach den bindenden Vorgaben des Bundesverfassungsschutzgesetzes nur die Daten enthalten, die für das Auffinden der Akten und der dazu notwendigen Identifizierung von Personen erforderlich sind. Eine Erweiterung für andere Identifizierungszwecke scheidet somit aus. Die Dateianordnung enthält darüber hinaus Arten von Daten, die über den Zweck einer Aktenhinweisdatei hinausgehen.
- Alle Rechtsvorschriften, die für die an dem zu übermittelnden Datensatz beteiligten Verfassungsschutzbehörden maßgeblich sind, sind zu beachten. Die in dem Entwurf der NADIS-Richtlinien enthaltenen Regelungen für die Übermittlung personenbezogener Daten sehen hingegen vor, daß hierfür ausschließlich das Recht der übermittelnden Stelle gelten soll.
- Die Dauer der Speicherung von Protokolldatenbeständen ist einheitlich zu regeln. Eine Differenzierung, ob die ursprünglich in der Personenzentraldatei erfaßte Information infolge Fristablaufs oder aufgrund einer Einzelfallentscheidung gelöscht wurde, erscheint nicht sachgerecht. Außerdem muß sichergestellt sein, daß Protokolldaten, so wie es die Verfassungsschutzgesetze vorsehen, nur für Zwecke der Datenschutzkontrolle, der Datensicherung oder zur Sicherung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage verwendet werden.
- Die Datenschutzbeauftragten sind im Rahmen der Durchführung und Fortentwicklung des Nachrichtendienstlichen Informationssystems frühzeitig zu unterrichten und zu beteiligen. Dies muß insbesondere bei der Vorbereitung von datenschutzrechtlichen Regelungen gelten.

Anlage 16 (zu Nr. 28.2)

Auszug aus dem Vortrag des Bundesbeauftragten für den Datenschutz, Dr. Joachim Jacob, zum Verbrechensbekämpfungsgesetz in der öffentlichen Anhörung am 11. April 1994

„... Wegen besonderer datenschutzrechtlicher Besorgnisse konzentriere ich mich auf die im Verbrechensbekämpfungsgesetz Artikel 12 vorgesehene Ausweitung nachrichtendienstlicher Eingriffe in das Fernmeldegeheimnis. Im Zentrum steht dabei die Erweiterung der BND-Fernmeldeaufklärung.

Mir ist bislang die zentrale Frage zu kurz gekommen – was kostet das an Freiheitseinbußen, was bringt es dem Bürger an Sicherheitsgewinn? Wird damit noch die Verhältnismäßigkeit gewahrt?

Anders als alle anderen Telefonüberwachungen ist die BND-Fernmeldeaufklärung **nicht** verdachtsbezogen. Es werden nicht zielgerichtet Straftäter, Verdächtige oder deren Kontaktpersonen überwacht. Vielmehr wird bewußt dann **jedermann** einbezogen, wenn mit Fernsprechteilnehmern im Ausland kommuniziert wird. Nach Aussagen von Insidern muß damit gerechnet werden, daß **täglich** rund viertausend Gespräche, zur weiteren Bearbeitung ausgewertet werden. Das bedeutet, daß zunächst in einem vorangegangenen Schritt mehrere hunderttausend Gespräche betroffener Bürger täglich aufgezeichnet wurden. Über diese Dimension der Fernmeldeaufklärung bei Gesprächen, von deren Aufzeichnung die Betroffenen nichts ahnen können, muß man sich im klaren sein, wenn man die Befugnisse derart erweitert. Angesichts dieser neuen Qualität müssen ausreichende und angemessene Schutzvorkehrungen für die Freiheitsrechte getroffen werden.

Nach allem, was mir bekannt ist, bin ich besorgt, daß der Ertrag der Fernmeldeaufklärung bei weitem nicht das bringt, was man sich erwartet und was auch nach der öffentlichen Diskussion erhofft wird. Ich denke hier vor allem an verfügbare und leicht zu handhabende Verschlüsselungsverfahren, die so effektiv sind, daß sie von Niemanden, außer er ist im Besitz des Schlüssels, – auch nicht vom BND – bei vertretbarem Aufwand zu knacken sind. Gerade die organisierte Kriminalität dürfte über eine Kommunikationsstruktur und -logistik verfügen, bei der anzunehmen ist, daß solche naheliegenden Schutzmechanismen genutzt werden. Wenn der „Fang" also im wesentlichen nur in kleinen Fischen bestehen wird, ist es m. E. unangemessen, mit dem Kescher im Äther täglich in das Fernmeldegeheimnis hunderttausender Unbeteiligter einzugreifen.

Die im Gesetzentwurf im einzelnen genannten Befugnisausweitungen sollten demgemäß noch einmal hinterfragt werden.

In jedem Fall müßte der Gesetzentwurf aber noch nachgebessert werden, um den verfassungsrechtlich gebotenen Mindeststandard zu erfüllen. In meiner schriftlichen Äußerung habe ich die staats- und völkerrechtliche Situation dargestellt – wesentlich ist hiernach:

1. Primärnutzung – also Aufgaben des BND – und Sekundärinteressen, etwa der Strafverfolgung, sind strikt und konsequent zu **trennen.**

   Der BND erarbeitet Lagebilder, er betreibt keine Verbrechensbekämpfung – Strafverfahrenserkenntnisse müssen **zufälliges** Nebenprodukt bleiben. Die Sekundärinteressen dürfen keinerlei Einfluß auf die Fernmeldeüberwachung und die Erkenntnisauswertung des BND erlangen. Hierzu sind Klarstellungen in der Erhebungs- und in der Übermittlungsvorschrift nötig.

2. Um zu erreichen, daß Unschuldige durch die Maßnahmen der Fernmeldeaufklärung mit anschließenden Verfahren **nicht** belastet werden, müssen zwei Schwellen vorgesehen werden:

   Die erste Eingriffsschwelle muß sein, daß der BND personenbezogene Daten nur bei **erheblichem** Verdacht weitergeben darf.

   Weiterhin:

   Vor Weitergabe der Daten an die Sekundärnutzer muß von einer unabhängigen Institution – wie der G 10-Kommission oder einem Ermittlungsrichter – überprüft werden, ob die Daten den Verdacht rechtfertigen und ein Verfahren eingeleitet werden soll.

3. Da die erweiterten Befugnisse des BND zu erheblichen Eingriffen in das Persönlichkeitsrecht führen, muß als Ausgleich in diesem überaus empfindlichen Bereich eine effektive Kontrolle gewährleistet werden.

   Ich empfehle deshalb nachdrücklich eine aussagekräftige Unterrichtung des Parlaments und der Öffentlichkeit über die Arbeit des BND, und zwar, wie zuverlässig das Persönlichkeitsrecht der Betroffenen gewahrt wird und ob sich der Aufwand für die erweiterten Befugnisse rechtfertigt.

   Diese Unterrichtung halte ich für eine wichtige Maßnahme, um Fehlentwicklungen in der Verfahrenspraxis zu vermeiden.

   Weiterhin empfehle ich angesichts der Befugnisausweitung Verbesserungen hinsichtlich einer effektiven Datenschutzkontrolle. Dies ist auch verfassungsmäßig geboten.

   Wegen der gewaltigen Dimension und der Heimlichkeit der Maßnahme muß ein jederzeitiges Kontrollrecht geschaffen werden. Diese Kontrolle sollte in den Händen einer unabhängigen Institution liegen, die dies im Benehmen mit der G 10-Kommission wahrnimmt. Eine nur gelegentliche

Kontrolle halte ich in diesem Rahmen für keine angemessene Ausgleichsmaßnahme.

Diese Kontrolle kann deshalb nur von einer Institution mit entsprechender Infrastruktur und Ausstattung wahrgenommen werden. Ich erlaube mir insoweit meine Dienststelle ins Gespräch zu bringen, weil sie über die entsprechenden Kenntnisse für die Durchführung von Kontrollen verfügt.

Im übrigen verweise ich auf meine schriftliche Stellungnahme; . . .".

Anlage 17 (zu Nr. 23.2.3.2)

Übersetzung eines Schreibens der Arbeitsgruppe „Polizei" der EU-Datenschutzbeauftragten an den Vorsitzenden des Rates der Europäischen Union der Innen- und Justizminister vom 10. Novemer 1994

Betr.: EUROPOL

Anrede,

ich schreibe Ihnen im Namen der Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union und Österreichs, Finnlands, Norwegens und Schwedens, um auf die Bedeutung angemessener Datenschutzmaßnahmen in der zukünftigen EUROPOL-Konvention hinzuweisen.

Die EU-Datenschutzbeauftragten haben wiederholt ihre Meinungen über EUROPOL ausgetauscht. In einem Schreiben vom 7. Dezember 1993 an den Vorsitz des Ministerrats hat die EDPC-Arbeitsgruppe Polizei sich nachdrücklich dafür eingesetzt, Datenschutzklauseln in die EUROPOL-Konvention aufzunehmen, die denen des Schengener Übereinkommens gleichen, und dem Rat ihre Bereitschaft, in dieser Hinsicht behilflich zu sein, signalisiert.

Angesichts des Wunsches des Rates, die Arbeiten am Konventionsentwurf im Oktober d. J. zu beenden, trat die EDPC-Arbeitsgruppe Polizei am 26. Oktober 1994 in Rijswijk zusammen. Die Datenschutzbeauftragten Österreichs, Finnlands, Norwegens und Schwedens wurden als Beobachter eingeladen.

Auf dieser Sitzung informierte der Vorsitzende der Arbeitsgruppe EUROPOL die EDPC-Arbeitsgruppe über die jüngsten Entwicklungen bzgl. EUROPOL. Diese Informationen wurden sehr begrüßt.

Im Lichte der jüngsten Entwicklungen möchten die EU-Datenschutzbeauftragten und ihre Kollegen aus den neuen Mitgliedstaaten die Bedeutung eines kohärenten Systems von Datenschutzprinzipien in der EUROPOL-Konvention und einer sorgfältig abgestimmten Informationsarchitektur betonen. Beide sollten nicht nur die Merkmale der EUROPOL-Organisation und den besonderen Charakter der Polizeizusammenarbeit bei der Bekämpfung schwerer Formen des internationalen Verbrechens widerspiegeln, sondern auch dem grundsätzlichen Bedürfnis nach Datenschutz in diesem sensiblen Bereich Rechnung tragen.

Die EUROPOL-Konvention sollte im Einklang stehen mit der Europarats-Konvention vom 28. Januar 1981 über den Schutz des Einzelnen im Hinblick auf die automatische Verarbeitung personenbezogener Daten und der Empfehlung R (87) 15, die die Nutzung personenbezogener Daten im Polizeibereich regelt. Angemessene Sicherungen für den Betroffenen, einschließlich eines Rechts auf Auskunft, das nicht unangemessen kompliziert wahrgenommen werden kann, sollten ein integraler Bestandteil der internationalen Zusammenarbeit im Rahmen von EUROPOL sein.

Sowohl vor dem Hintergrund ihrer nationalen Aufgabe und ihrer Aufgabe im Hinblick auf die EDE/EUROPOL möchten die Datenschutzbeauftragten erneut ihre Bereitschaft bekräftigen, bei der Ausarbeitung der Datenschutzprinzipien in der EUROPOL-Konvention behilflich zu sein, und fordern den Rat und die nationalen Regierungen auf, sie regelmäßig über den Text des Konventionsentwurfs sowie sonstige neue Entwicklungen, die für ihre Aufgabe relevant sind, zu unterrichten.

Die Berücksichtigung unseres Anliegens würden wir sehr schätzen.

Schlußformel

(gez.) Peter J. Hustinx

Präsident des Registeramtes

Anlage 18 (zu Nr. 5.6)

Übersetzung

Az.: FGBA/TAM/KO160

The Data Protection
Registrar
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

Herrn Peter Wilmott
Generaldirektor
Generaldirektion XXI
Europäische Kommission
Rue de la Loi 200
1049 Brüssel
Belgien

11. November 1994

Entwurf einer EU-Verordnung über die gegenseitige Amtshilfe in Zollangelegenheiten

Sehr geehrter Herr Wilmott,

die Datenschutzbeauftragten der EU hatten kürzlich Gelegenheit, die Frage des Schutzstandards für personenbezogene Informationen zu erörtern, der im Vorschlag einer EU-Verordnung über die gegenseitige Amtshilfe in Zollangelegenheiten vorgesehen ist. Ich schreibe Ihnen auch im Namen meiner Kollegen, um Ihnen das Ergebnis unserer Überlegungen mitzuteilen.

Nach Ansicht der Datenschutzbeauftragten sind die personenbezogenen Informationen, die im Rahmen eines derartigen internationalen Verfahrens anfallen, sensibel und sie werden für sensible Zwecke verarbeitet. Daher sollten alle derartigen Informationen selbstverständlich in hohem Maße geschützt werden, damit anerkannten europäischen Standards Rechnung getragen wird.

Den Datenschutzbeauftragten ist bekannt, daß es schwierig war, eine geeignete Lösung für dieses Problem des Verordnungsentwurfs zu finden. Den Datenschutzbeauftragten ist auch bekannt, daß eine Lösung vorgeschlagen wurde, die sich auf Artikel 15 des Dubliner Asylübereinkommens stützt. Eine Prüfung dieses Artikels ergibt, daß darin systematisch die eingeschränkten Kategorien der auszutauschenden Informationen aufgeführt werden. Weiterhin werden die Zwecke dargelegt, für die die Informationen verwendet werden sollen, und die Zuständigkeit für andere, die Qualität der Daten betreffende Regeln. Außerdem wird das Auskunftsrecht des Betroffenen vorgesehen. Die Datenschutzbeauftragten stimmen darin überein, daß Artikel 15 ein hilfreiches Muster für die Lösung des ähnlich gelagerten Problems in der vorgeschlagenen Verordnung darstellt. Sie möchten der Kommission und dem Rat empfehlen, diese Lösungsmöglichkeit für den Schutz von Informationen im Rahmen der Verordnung zu prüfen.

Mit freundlichen Grüßen

(gez.)
Elizabeth France
Data Protection Registrar

Anlage 19 (zu Nr. 9.7 und 9.7.3)

Hinweise zum Einsatz von Datenbanksprachen bei der automatisierten Personaldatenverarbeitung *)

In der typischen ADV-Anwendungen wird der Anwender am Bildschirm vom Rechner mittels „Masken" durch ein „Menü" geführt. Diese erleichtern ihm die Benutzung des Programms durch vorformulierte „Fragebögen", in denen er seine Abfragen z. B. „ankreuzen" kann. Sie erlauben ihm aber nur solche Abfragen und Auswertungen, die vom Anwendungsprogramm vorgegeben – im Idealfall also hausintern unter Datenschutzaspekten geprüft und genehmigt – sind; andere Abfragen werden abgewiesen. Anders ist dies bei Datenbanksprachen („freien Abfragesprachen"): Sie ermöglichen dem Anwender, selbst Abfragen über den Datenbestand zu formulieren, ohne an die Restriktionen eines Anwendungsprogramms gebunden zu sein.

Die technische Weiterentwicklung von Datenbanksystemen und neue Überlegungen beim Einsatz von Datenbanksprachen haben mich veranlaßt, meine bisherige Position hinsichtlich der „freien Abfragesprachen" bei der automatisierten Personaldatenverarbeitung (vgl. 8. TB S. 16 ff., 12. TB S. 35) neu zu definieren.

Da die technische Entwicklung inzwischen Möglichkeiten bietet, die mit einer „freien Abfragesprache" verbundenen datenschutzrechtlichen Risiken abzubauen, halte ich in begründeten Einzelfällen den eingeschränkten Einsatz „freier Abfragesprachen" für vertretbar. Eine Beeinträchtigung des Persönlichkeitsrechts der Mitarbeiter muß aber ausgeschlossen sein. Auch die qualifizierte Mitbestimmung der Personalräte ist zu gewährleisten. Die Möglichkeit zum Einsatz der „freien Abfragesprache" ist, soweit erforderlich, zu beschränken.

Die wichtigsten Voraussetzungen hierfür sind:

Das System muß eine technische Begrenzung, ähnlich einem Filter aufweisen, die sicherstellt, daß die „freie Abfragesprache" nur in dem vereinbarten Umfang eingesetzt werden kann. Der Umfang kann beispielsweise durch eine Zugriffsbeschränkung auf bestimmte weniger sensitive Datenfelder festgelegt sein. Ein Umgehen des Filters ist insbesondere programmtechnisch zu verhindern.

Die Daten, auf die mit einer solchen Abfragesprache zugegriffen werden soll, und die zu eröffnenden Abfragearten müssen vorab – bei Personaldaten unter Beteiligung der Personalvertretung – geprüft werden. Kriterien sind hierbei insbesondere

- der Nachweis, daß eine anonymisierte Auswertung für den jeweils verfolgten Zweck nicht genügt,
- die Erforderlichkeit für die Aufgabenerfüllung,
- die Sensibilität, d. h. der Schutzbedarf, der einzelnen Daten in der vorgesehenen Verknüpfung und Systemumgebung sowie
- der jeweilige Zweck und Kontext der Datennutzung.

Ferner halte ich es für erforderlich, daß das vorgesehene Verfahren organisatorisch im Rahmen einer Dienstvereinbarung mit der Personalvertretung festgeschrieben wird. Die Einhaltung der Verfahrensregelungen ist in geeigneter Weise – beispielsweise durch eine Protokollierung – zu kontrollieren.

Keine datenschutzrechtlichen Bedenken habe ich gegen den Einsatz einer „freien Abfragesprache" auch dann, wenn die Auswertung nur zu anonymisierten Ergebnissen führt.

*) Mit Schreiben III – 450/1 vom 17. Mai 1993 an oberste Bundesbehörden

Anlage 20 (zu Nr. 20.2.9)

Unbefugte Fernbedienung von Anrufbeantwortern *)

Die meisten der heute angebotenen telefonischen Anrufbeantworter weisen die Möglichkeit der Fernabfrage der aufgezeichneten Telefonate, zum Teil auch der Fernbedienung aller Gerätefunktionen – insbesondere der Raumüberwachungsfunktion auf. Bei der Fernabfrage – über einen beliebigen Telefonanschluß – wird dem Anrufbeantworter mittels des (Tonwahl-) Telefons selbst oder eines Bediengerätes („Code-Sender") ein aus mehreren Tönen bestehendes Signal zugesandt, mit dem der Fernabfragende sich identifizieren und die Bedienvorgänge einleiten kann.

Problematisch ist, daß ein erheblicher Teil der verkauften Geräte über einen mangelhaften Schutz gegen unbefugte Abfrage verfügt: Oft besteht das Signal aus nur zwei oder drei unterschiedlichen Tönen, die somit leicht festzustellen sind. Auch ist es in der Regel möglich, einen Vielzahl aufeinanderfolgende Versuche zu unternehmen, um die Codierung „durch Probieren" in Erfahrung zu bringen. Technisch versierte Telekommunikationsteilnehmer verfügen zumeist über ein Zusatzgerät (Modem) mit dessen Hilfe sie in Sekundenschnelle durch ein Programm die Codierung ermitteln können. Mir wurde auch berichtet, daß einige der Geräte über eine „Notfallsicherung" für den Fall verfügen, daß der berechtigte Fernabfragende die richtige Codierung vergessen hat oder sie nach einem Stromausfall gelöscht ist. Für diesen Fall braucht er angeblich lediglich die Codierung „0 0 0" am Fernabfragegerät einstellen.

*) Mit Schreiben VI – 191/77 vom 22. März 1994 an oberste Bundesbehörden

Ich empfehle allen Behörden, bei denen **Anrufbeantworter mit Fernabfrage** in Einsatz sind, folgende Sicherheitshinweise zu beachten:

1. Ändern Sie **umgehend**, soweit noch nicht geschehen, die werksseitig eingestellte Codierung.
2. Stellen Sie den Anrufbeantworter – insbesondere, wenn er über eine Raumüberwachungsfunktion verfügt – nur in solchen Diensträumen auf, in denen keine schutzbedürftigen dienstlichen Gespräche stattfinden.
3. Ändern sie in regelmäßigen Abständen die Codierung.
4. Verzichten Sie auf Trivialcodierungen, wie z. B. 007, oder „Monatsschlüssel", z. B. 003.
5. Prüfen Sie, ob Ihr Gerät über die o. g. „Notfallsicherung" verfügt; sie stellt ein untragbares Sicherheitsrisiko dar!
6. Weisen Sie bitte im Ansagetext darauf hin, daß die gespeicherte Nachricht eventuell Unbefugten zugänglich ist.
7. Klären Sie ggf. Ihre Mitarbeiter über die Mithörmöglichkeiten der Raumüberwachungsfunktion auf.
8. Achten Sie beim Abhören der Nachrichten auf Unregelmäßigkeiten bzw. auf Signale, die auf einen unbefugten Abhörer hindeuten könnten.
9. Achten Sie bei Neubeschaffung darauf, daß das Gerät sowohl über eine mindestens dreistellige Codierung als auch über die Möglichkeit verfügt, nach max. 3 Fehlversuchen die Verbindung zu unterbrechen.

Anlage 21 (zu Nr. 20.2.10)

Hinweise zum Datenschutz bei Telekommunikationsanlagen (TK-Anlagen); Unbefugtes Mithören von Telefon- oder Raumgesprächen *)

Die Mehrzahl der heute eingesetzten Telekommunikationsanlagen (TK-Anlagen) verfügt über Leistungsmerkmale, die grundsätzlich das Mithören von Telefonaten Dritter oder von Gesprächen im Raum eines der Verbindungsteilnehmer ermöglichen.

Hierzu möchte ich die folgenden tatsächlichen und rechtlichen Anmerkungen machen, die jedenfalls für die marktführenden Anbieter von TK-Anlagen gelten. Ich habe mich im folgenden beispielhaft auf Anlagen der Fa. Siemens AG bezogen. Dies gilt insbesondere für die Bezeichnungen der Leistungsmerkmale; die Anbieter verwenden unterschiedliche.

1. Eintreten in bestehende Telefonverbindungen

   Das Leistungsmerkmal „Aufschalten" ermöglicht – typischerweise der Vermittlungskraft – das Eintreten in eine bestehende Verbindung, um z. B. auf ein bei der Zentrale angekommenes dringendes Auslandsgespräch aufmerksam zu machen. Die Möglichkeit des Aufschaltens kann allerdings auch für „normale" Anschlüsse eingerichtet werden. In jedem Fall wird während des Aufschaltens eine Aufmerksamkeitssignal („Aufschalteton") zwangsweise eingeblendet und damit den betroffenen Teilnehmern die Tatsache des Aufschaltens signalisiert. Ein Unterdrücken oder eine Lautstärkeverminderung zum Unhörbarmachen des Tones ist nicht möglich.

   Zusätzlich wird z. B. bei Siemens-TK-Systemen das Leistungsmerkmal „Verhindern des Aufschaltens" angeboten. Damit kann teilnehmerindividuell ein Schutz gegen das Aufschalten eingerichtet werden.

   Eine Nutzung des Leistungsmerkmals Aufschalten zum unbemerkten, mißbräuchlichen Mithören von Telefonaten ist somit nahezu unmöglich.

2. Lauthören

   Viele Endgeräte geben dem Benutzer die Möglichkeit, einen Lautsprecher zuzuschalten, so daß im Raum Anwesende das Gespräch mithören können („Lauthören"). Ich habe mich mit einer seinerzeit gegenüber dem Bundesministerium für Post und Telekommunikation (als Zulassungsbehörde) erhobenen Forderung, die Zuschaltung eines Lautsprechers zwangsweise zu signalisieren und somit dem Gesprächspartner zu verdeutlichen, nicht durchsetzen können. In meiner Dienststelle besteht jedoch die Anweisung, eine Lautsprecherzuschaltung stets von der Einwilligung des Telefonpartners anbhängig zu machen.

3. Zeugenzuschalten

   Manche TK-Anlagen verfügen auch über das Leistungsmerkmal „Zeugenzuschalten": Dabei wird ein anderer Teilnehmer oder ein Tonbandgerät unbemerkt in eine bestehende Verbindung eingeschaltet. Dieses Leistungsmerkmal ist m. W. in der Bundesrepublik nicht zugelassen – eine Tonbandaufnahme wäre gem. § 201 Abs. 1 Nr. 1 StGB strafbar – und wird daher jedenfalls von der Fa. Siemens AG nicht installiert.

4. Direktansprechen/Direktantworten

   Viele Endgeräte sind mit der Möglichkeit des Freisprechens ausgerüstet, d. h., zum Führen eines Telefonates braucht der Hörer nicht abgenommen zu werden; es braucht lediglich ein Knopf („Leitungstaste") gedrückt zu werden. Wird für solche Endgeräte das Leistungsmerkmal „Direktansprechen/Direktantworten" (Gegensprechanlage) eingerichtet, braucht auch die Leitungstaste nicht mehr betätigt zu werden: Ein ankommender Anruf schaltet das Endgerät automatisch ein – auch das eingebaute Mikrophon.

   Typischerweise wird dieses Leistungsmerkmal für die Kommunikation zwischen Chef und Sekretärin eingerichtet, häufig wird es aber in Teamfunktion gewünscht: Der Chef kann damit kurze Rückfragen an seine Mitarbeiter richten, ohne daß diese den Hörer abzunehmen brauchen oder den Besprechungstisch verlassen müssen. Grundsätzlich ist es nicht möglich, mittels des direkten Ansprechens in bestehende Verbindungen einzutreten.

   Um eine Beeinträchtigung der Persönlichkeitsrechte zu verhindern, wird jedenfalls bei TK-Anlagen der Firma Siemens AG beim Direktansprechen stets wohl ein optisches als auch akustisches Aufmerksamkeitssignal erzeugt. Zusätzlich kann für die Dauer der Verbindung ein periodisch wiederkehrendes akustisches Signal eingeblendet werden. Darüber hinaus wird das Leistungsmerkmal Direktes Ansprechen stets gemeinsam mit dem Leistungsmerkmal „Ansprechschutz" ausgeliefert. Wird letzteres (durch Knopfdruck) aktiviert, ist ein Direktansprechen dieses Anschlusses nicht möglich.

5. Konferenzschaltung

   Das Leistungsmerkmal „Konferenzschaltung" ermöglicht – durch Knopfdruck am Endgerät der TK-Anlage – einem der Teilnehmer der Verbindung, einen oder mehrere weitere Teilnehmer in die Verbindung einzubeziehen, um z. B. eine gemeinsame Terminklärung schnell und einfach herbeizuführen. Das Eintreten eines weiteren Teilnehmers in die Verbindung wird dabei stets durch

*) Mit Schreiben VI – 191/52 vom 27. Dezember 1993 an oberste Bundesbehörden.

ein Aufmerksamkeitssignal angekündigt und somit allen Teilnehmern bewußt gemacht. Ein Unterdrücken oder eine Lautstärkeverminderung zum Unhörbarmachen des Tones ist nicht möglich.

Das Verlassen einer solchen Konferenzschaltung durch einen der Teilnehmer wird demgegenüber war in den meisten, nicht jedoch in allen TK-Anlagen signalisiert, wodurch demjenigen ein „heimliches Lauschen" ermöglicht wird, der den Austritt aus einer Konferenzschaltung lediglich erklärt, nicht jedoch vollzieht. Dieser Umstand sollte allen Nutzern der TK-Anlage nachdrücklich verdeutlicht und im übrigen auch in eine diesbezügliche Dienstvereinbarung aufgenommen werden. Bei Neubeschaffung sollte in jedem Falle eine Anlage mit ausreichender Signalisierung gewählt werden.

Die Firma Siemens AG hat mir in diesem Zusammenhang mitgeteilt, daß die Software der von ihr in der Bundesrepublik Deutschland ausgelieferten Anlagen keine unzulässigen Leistungsmerkmale enthält, die etwa lediglich deaktiviert oder gesperrt sind. Das unbefugte Implementieren von Leistungsmerkmalen, die in Deutschland nicht zugelassen sind, oder das Verändern eines zulässigen Merkmales in unzulässiger Weise – etwa Unterdrückung eines Aufmerksamkeitssignales – ist in der Realität nahezu unmöglich, da dieses sehr gute anlagenbezogene Fachkenntnisse und Zugang zu spezifischen Informationen und Programmen erfordert.

Im übrigen ist die Kontrolle der Auflistung der installierten Leistungsmerkmale stets Bestandteil von mir durchgeführter diesbezüglicher Datenschutzkontrollen; ich empfehle dies auch den behördlichen Datenschutzbeauftragten der Bundesbehörden.

Sofern die dargelegten Sicherheitsmechanismen realisiert sind und von ihnen auch Gebraucht gemacht wird, habe ich gegen eine Nutzung der beschriebenen Leistungsmerkmale keine grundsätzlichen Bedenken. Hinzuweisen ist allerdings auf die Mitwirkungsrechte der Personalvertretung gemäß § 75 Abs. 3 BPersVG.

Anlage 22 (zu Nr. 31.2.3)

Textverarbeitung und Dateibegriff *)

Bei der datenschutzrechtlichen Beurteilung von Textverarbeitungssystemen bestehen in der Praxis nach wie vor erhebliche Unsicherheiten. Schwierigkeiten macht es vor allem, den Dateibegriff auf die Funktionen eines Textverarbeitungssystems so anzuwenden, daß einerseits dem unbezweifelbaren Schutzbedürfnis Rechnung getragen wird, andererseits aber auch die Verpflichtung, die Verarbeitung und Nutzung personenbezogener Daten dateibezogen durch Dateistatute zu regeln und die Dateien dem BfD zum öffentlichen Dateienregister mitzuteilen, in einer praktikablen und zweckorientierten Weise erfüllt wird. Der BfD hat hierzu die nachfolgenden Grundsätze entwickelt.

Es ist zu unterscheiden zwischen der Erfüllung des Dateibegriffs als Voraussetzung für die Anwendbarkeit des Gesetzes (A) und seiner Behandlung im Rahmen der organisatorischen Maßnahmen der speichernden Stellen (B und C).

Zur datenschutzrechtlichen Bewertung ist nicht lediglich auf Textverarbeitungssysteme im engeren Sinne, also auf entsprechende ADV-Programm(paket)e allein (z. B. WORD, Q-Office) abzustellen. Vielmehr sind die Möglichkeiten mitzuberücksichtigten, die die gesamte installierte Software (Betriebssystem, andere Anwendungsprogramme) bietet, soweit sie Zugriff auf die von Textverarbeitungssystemen benutzten Dateien hat. In diesem Sinne wird der Begriff „Textverarbeitungssystem" im folgenden benutzt:

A. Dateibegriff nach § 3 Abs. 2 Nr. 1 BDSG (als Voraussetzung der BDSG-Anwendung – 3. Abschnitt – bzw. der Anwendung der dateibezogenen materiellen Vorschriften – 2. Abschnitt –):

1. „Verwaltungsteil" des Textverarbeitungssystems

Ein Textverarbeitungssystem umfaßt neben Programmen zum Speichern, Bearbeiten und Löschen der Texte auch „Verwaltungs"-Funktionen, die es z. B. ermöglichen, festzustellen, welche Texte im System welchen Benutzern zuzuordnen sind. Enthalten die mittels solcher Verwaltungsfunktionen erstellten Datensammlungen personenbezogene Daten, wie dies nahezu stets der Fall ist, so wird der Dateibegriff unzweifelhaft erfüllt. Typisch wäre ein Verzeichnis der gespeicherten Texte mit personenbezogenen Angaben zum Inhalt (z. B. „Brief an Herrn X") zum Betreff (z. B. „Bewerbung Frau Y"), zum Autor oder zur Schreibkraft.

2. Dokumentensammlung und Einzeldokumente

Problematischer ist die Einordnung der Texte („Dokumente"), die vom Textverarbeitungssystem verwaltet werden, z. B. der mit ihm erstellten Briefe. Stellt der Verwaltungsteil eine Datei nach 1. dar, so ist die Gesamtheit der Dokumente als Bestandteil dieser Datei anzusehen, weil ihr personenbezogener Inhalt über den Verwaltungsteil ausgewertet werden kann (§ 3 Abs. 2 Satz 2 BDSG).

Für die Auswertbarkeit kommt es darauf an, ob das Textverarbeitungssystem Funktionen enthält, die es ermöglichen, die Dokumentensammlung oder das Dokument nach personenbezogenen Merkmalen zu erschließen (z. B. Abfrage danach, ob darin der Name „Meier" oder der Begriff „krank" vorkommt) oder ob es um solche ohne großen Aufwand erweitert werden kann.

Auf die direkte inhaltliche Auswertbarkeit der Dokumentensammlung als ganzer nach personenbezogenen Elementen ihres Inhalts kommt es (entgegen einer in der Literatur vertretenen Auffassung) nur an, wenn ein Verwaltungsteil, durch den der Dateibegriff erfüllt wird, fehlt. Praktisch dürften solche Systeme nicht vorkommen.

B. Interne Verzeichnisse nach § 18 Abs. 2 BDSG

1. Eine Textverarbeitungsanlage als technisches System ist eine Datenverarbeitungsanlage nach § 18 Abs. 2 Satz 1 BDSG; sie ist daher in das entsprechende Verzeichnis aufzunehmen.

2. In das nach § 18 Abs. 2 Satz 2 BDSG zu führende Dateistatut (Übersicht) sind aufzunehmen

   a) die bei der Textverarbeitung entstehende Datensammlung als ganzes; dabei ist eine Umschreibung unter Verdeutlichung der Sensibilität der Dokumente vorzunehmen, z. B.: „1. Schreiben des Pressereferates zur Übersendung von Druckschriften, 2. Schreiben und Gutachten des Ärztlichen Dienstes";

   b) im Textverarbeitungssystem geführte Datensammlungen, die schon kraft ihrer eine Auswertung erlaubenden Struktur den Dateibegriff erfüllen, wie z. B. Adressenbestände, Verteiler, Abonnentenlisten.

Die gesetzliche Ausnahme zugunsten von Dateien, die nur vorübergehend vorgehalten und innerhalb von drei Monaten nach ihrer Erstellung gelöscht werden (§ 18 Abs. 3), stellt auf die Existenz der Datei (nicht der in ihr gespeicherten Daten) ab. Maßgeblich ist daher nicht die Aufbewahrungsdauer des einzelnen Dokuments, sondern die Verwendungsdauer des Textverarbeitungssystems.

*) Anlage zu meinem Rundschreiben an die obersten Bundesbehörden vom 23. November 1993, I 101-1/9

C. Meldungen zum Dateienregister des BfD nach § 26 Abs. 5 BDSG

Angesichts der weiten und noch zunehmenden Verbreitung von Textverarbeitungssystemen ist eine genaue und aktuelle Kenntnis, welche Stellen über welche Systeme verfügen, weder für den BfD noch für die Öffentlichkeit, der das Dateienregister zugänglich ist, aufschlußreich oder für die Rechtswahrnehmung von praktischer Bedeutung. Zudem wäre der Aufwand für einen entsprechenden Melde- und Änderungsdienst unverhältnismäßig hoch. Eine Registermeldung ist deshalb nur in den vorstehend unter B 2 b genannten Fällen vorzunehmen.

Anlage 23 (zu Nr. 14.1.3)

Entschließung der 49. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 9./10. März 1995 zum Sozialgesetzbuch VII

Verfassungsgemäßer Datenschutz für Unfallversicherte erforderlich

Durch die Träger der gesetzlichen Unfallversicherung werden oft Daten der Versicherten hinter deren Rücken oder zumindest ohne deren konkrete Kenntnis erhoben und weitergegeben. Der vorliegende Referentenentwurf des Bundesministeriums für Arbeit und Sozialordnung zum Unfallversicherungs-Einordnungsgesetz – SGB-VII sieht dazu keine Änderungen vor.

Aus dem Recht auf informationelle Selbstbestimmung der Versicherten, insbesondere auf Transparenz der einzelnen Verfahrensschritte, ergeben sich mehrere grundlegende Forderungen, die bei einer Überarbeitung des Referentenentwurfs berücksichtigt werden müssen:

1. Auskunftspflicht behandelnder Ärzte gegenüber Unfallversicherungsträgern

Für behandelnde Ärzte sollte eine gesetzliche Auskunftspflicht gegenüber Unfallversicherungsträgern nur festgelegt werden, soweit dies erforderlich ist für eine sachgerechte und schnelle Heilung (§ 557 Abs. 2 RVO – § 34 Referentenentwurf SGB VII). Die gesetzliche Auskunftspflicht ist daher auf Angaben über die Behandlung und den Zustand des Verletzten zu beschränken. Danach dürfen Vorerkrankungen, die aus Sicht des Arztes mit dem aktuellen Status in keinem Zusammenhang stehen oder keine Bedeutung im Zusammenhang mit dem Arbeitsunfall oder der Berufskrankheit haben, nicht übermittelt werden (Beispiel: Handverletzung und Salmonellenvergiftung).

2. Datenerhebung, -verarbeitung und -nutzung durch Durchgangsärzte und Berufskrankheitenärzte

Soweit von den Unfallversicherungsträgern bestellte Durchgangsärzte personenbezogene Daten über den Unfallverletzten erheben und Unfallversicherungsträgern und anderen Stellen mitteilen, muß dies auf eine normenklare gesetzliche Grundlage gestellt werden; die bisherige Regelung in dem zwischen den Verbänden der Kassenärzte der Unfallversicherungsträger geschlossenen „Ärzteabkommen" reicht für die damit verbundenen Eingriffe in das informationelle Selbstbestimmungsrecht der Betroffenen nicht aus. Entsprechendes gilt für die geplante Einführung eines Berufskrankheitenarztes.

3. Mitteilung personenbezogener Patientendaten durch Unfallversicherungsträger an ärztliche Gutachter

Im Hinblick auf das Recht der Betroffenen, der Bestellung eines bestimmten Gutachters im Einzelfall aus wichtigem Grund – z. B. wegen möglicher Befangenheit – zu widersprechen, haben die Betroffenen ein besonderes berechtigtes Interesse an der Transparenz dieser Datenübermittlungen.

Gesetzlich festzulegen ist daher, daß dem Betroffenen vor Übermittlung seiner Daten an einen Gutachter der Zweck des Gutachtens und die Person des Gutachters unter Hinweis auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X mitzuteilen sind.

4. Eingriffe der Unfallversicherungsträger und ihrer Verbände in das Recht auf informationelle Selbstbestimmung

Aufgaben der Unfallversicherungsträger und ihrer Verbände und ihre Befugnisse zur Datenerhebung, -verarbeitung und -nutzung – einschließlich der Aufbewahrungsfristen – sind differenziert in der verfassungsrechtlich gebotenen Klarheit gesetzlich zu regeln. Der vorliegende Referentenentwurf erscheint in diesem Punkt weitgehend unzureichend. So werden undifferenziert Unfallversicherungsträger und ihre Verbände behandelt, die Fachaufgaben dieser Stellen nicht oder nicht hinreichend deutlich genannt und andererseits Selbstverständlichkeiten wie das Führen von Dateien über erforderliche Daten aufgeführt. Außerdem beschränkt sich die Regelung auf die Datenverarbeitung in Dateien und übergeht die gerade im Bereich der Berufsgenossenschaften mit Gutachten und ähnlichen Unterlagen stark ausgeprägte Datenverarbeitung in Akten.

Die Zuweisung von Aufgaben und Befugnissen an Verbände der gesetzlichen Unfallversicherung muß zudem wie bei allen anderen Verbänden von Leistungsträgern durch die Einrichtung einer staatlichen Aufsicht ergänzt werden.

Soweit Vorschriften der Unfallversicherungsträger und ihrer Verbände (z. B. Unfallverhütungsvorschriften) durch Regelungen über die Erhebung, Verarbeitung und Nutzung sensibler medizinischer Daten in das Recht auf informationelle Selbstbestimmung eingreifen, sind diese Eingriffe gesetzlich zu regeln.

5. Anzeige eines Berufsunfalls und einer Berufskrankheit

Bei Datenschutzkontrollen der bisherigen Anzeigen von Berufsunfällen und krankheiten hat sich gezeigt, daß der Umfang der an die verschiedenen Stellen übermittelten Daten zum Teil dem Grundsatz der Verhältnismäßigkeit, insbesondere der Erforderlichkeit nicht Rechnung trägt. Der Inhalt dieser Anzeigen muß an diesen Grundsätzen gemessen neu festgelegt werden.

6. Zentraldateien mehrerer Unfallversicherungsträger oder ihrer Verbände

Zweck und Inhalt zentral geführter Dateien sind in angemessenem Umfang gesetzlich präzise zu regeln. Dasselbe gilt für die Datenverarbeitung und nutzung sowie die Festlegung der jeweils speichernden Stelle.

Die rechtzeitige Beteiligung des jeweils zuständigen Bundes- oder Landesbeauftragten für den Datenschutz vor Einrichtung einer Zentraldatei ist vorzusehen.

7. Anforderung medizinischer Unterlagen bei anderen Sozialleistungsträgern

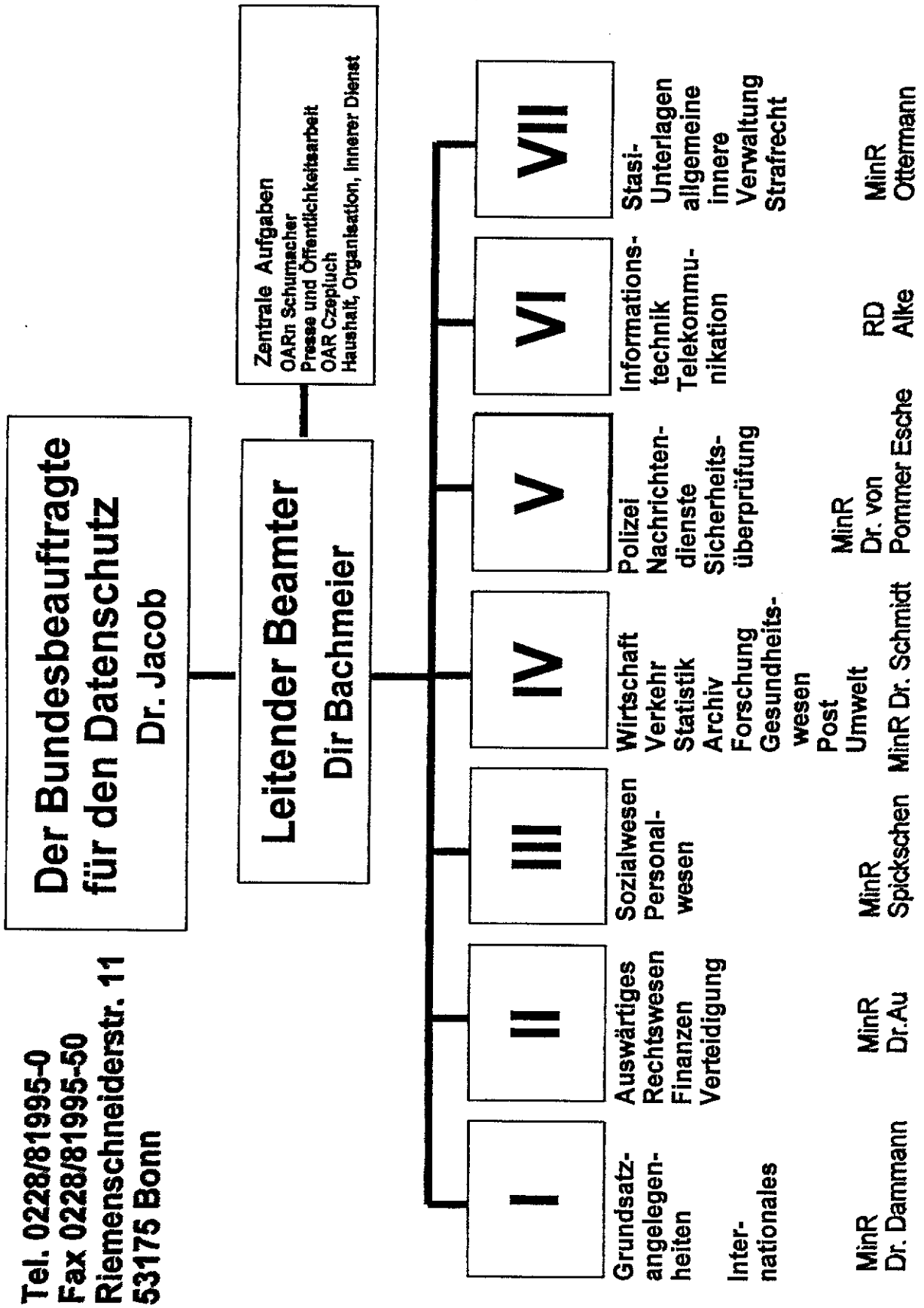
Der in § 76 Abs. 2 SGB X vorgesehene Hinweis auf das Widerspruchsrecht gegen die Übermittlung medizinischer Daten geht stets dann ins Leere, wenn bei der speichernden bzw. übermittelnden Stelle kein Verwaltungsverfahren läuft.

Es ist daher festzulegen, daß ein Unfallversicherungsträger vor der Anforderung von Sozialdaten im Sinne des § 76 SGB X bei anderen Sozialleistungsträgern den Versicherten auf dessen Widerspruchsrecht nach § 76 Abs. 2 SGB X gegenüber der übermittelnden Stelle hinzuweisen hat.

8. Akteneinsichtsrecht der Versicherten

Hinsichtlich des gesetzlichen Akteneinsichtsrechts nach § 25 SGB X treten in der Praxis seitens der Unfallversicherungsträger Unsicherheiten auf, ob zum Schutz von Betriebs- und Geschäftsgeheimnissen oder Urheberrechten das Einsichtsrecht beschränkt werden muß. Hierzu ist eine gesetzliche Klarstellung geboten, daß diese Rechte dem Akteneinsichtsrecht nicht entgegenstehen.

Anlage 24


Der Bundesbeauftragte für den Datenschutz
Dr. Jacob
Tel. 0228/81995-0
Fax 0228/81995-50
Riemenschneiderstr. 11
53175 Bonn
Leitender Beamter
Dir Bachmeier
Zentrale Aufgaben
OARn Schumacher
Presse und Öffentlichkeitsarbeit
OAR Czepluch
Haushalt, Organisation, innerer Dienst
I
Grundsatzangelegenheiten
Internationales
MinR Dr. Dammann
II
Auswärtiges
Rechtswesen
Finanzen
Verteidigung
MinR Dr.Au
III
Sozialwesen
Personalwesen
MinR Spickschen
IV
Wirtschaft
Verkehr
Statistik
Archiv
Forschung
Gesundheitswesen
Post
Umwelt
MinR Dr. Schmidt
V
Polizei
Nachrichtendienste
Sicherheitsüberprüfung
MinR Dr. von Pommer Esche
VI
Informationstechnik
Telekommunikation
RD Alke
VII
Stasi-Unterlagen
allgemeine innere Verwaltung
Strafrecht
MinR Ottermann

Sachregister

Abkürzungsverzeichnis

AA	Auswärtiges Amt
a. a. O.	am angegebenen Ort
ABM	Allgemeine Maßnahmen zur Arbeitsbeschaffung
ADV	Automatisierte Datenverarbeitung
a. F.	alte Fassung
AFG	Arbeitsförderungsgesetz
AG	Aktiengesellschaft
AFIS	Automatisiertes Fingerabdruck-Identifizierungssystem
AIDS	Acquired Immune Deficiency Syndrome
AK	Arbeitskreis
AO	Abgabenordnung
AOÄG	Gesetz zur Änderung der Abgabenordnung
AOK	Allgemeine Ortskrankenkasse
APC	Arbeitsplatzcomputer
ASYLON	Asyl-online
AsylVfG	Asylverfahrensgesetz
AtomG	Atomgesetz
AuslG	Ausländergesetz
AuD	Arbeitsunfähigkeitszeiten und Diagnosen
AWG	Außenwirtschaftsgesetz
AZR	Ausländerzentralregister
AZRG	Ausländerzentralregistergesetz
BA	Bundesanstalt für Arbeit
BAFA	Bundesausfuhramt
BAfAM	Bundesanstalt für Arbeitsmedizin
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BafU	Bundesausführungsbehörde für Unfallversicherung
BAG	Bundesarbeitsgericht; auch: Bundesamt für Güterverkehr
BAPT	Bundesamt für Post und Telekommunikation
BArchivG	Bundesarchivgesetz
BAT	Bundesangestelltentarifvertrag
BAT-O	Bundesangestelltentarifvertrag Ost
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
BDO	Bundesdisziplinarordnung
BDSG	Bundesdatenschutzgesetz
BEK	Barmer Ersatzkasse
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BG	Berufsgenossenschaft
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblatt
BGHZ	Entscheidungen des Bundesgerichtshofs in Zivilsachen
BGS	Bundesgrenzschutz
BGSG	Bundesgrenzschutzgesetz
BHO	Bundeshaushaltsordnung
BIOS	Basic Input Output System
BKA	Bundeskriminalamt
BKA-AN	BKA-Aktennachweisdatei
BKK	Betriebskrankenkasse
BMA	Bundesministerium für Arbeit und Sozialordnung
BMBau	Bundesministerium für Raumordnung, Bauwesen und Städtebau
BMF	Bundesministerium der Finanzen
BMFT	Bundesministerium für Forschung und Technologie
BMG	Bundesministerium für Gesundheit
BMI	Bundesministerium des Innern

BMJ	Bundesministerium der Justiz
BML	Bundesministerium für Ernährung, Landwirtschaft und Forsten
BMPT	Bundesministerium für Post und Telekommunikation
BMU	Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit
BMV	Bundesministerium für Verkehr
BMVg	Bundesministerium der Verteidigung
BMWi	Bundesministerium für Wirtschaft
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BPersVG	Bundespersonalvertretungsgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSH	Bundesamt für Seeschiffahrt und Hydrographie
BSHG	Bundessozialhilfegesetz
BStatG	Bundestatistikgesetz
BStU	Bundesbeauftragter für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BR-Drs.	Bundesrats-Drucksache
BRRG	Beamtenrechtsrahmengesetz
BS 2000	Betriebssystem der Firma Siemens
BT-Drs.	Bundestags-Drucksache
Btx	Bildschirmtext
BVA	Bundesverwaltungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Bundesverfassungsgerichtsentscheidung
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVerwGE	Bundesverwaltungsgerichtsentscheidung
BVFG	Bundesvertriebenengesetz
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
BZRÄndG	Änderungsgesetz zum Bundeszentralregistergesetz
CCITT	Comité Consultatif International Télégraphique et Téléphonique
CIS	Zollinformationssystem (Customs Information System)
coArb	computerunterstützte Arbeitsverwaltung
C.SIS	technische Unterstützungseinheit des Schengener Informationssystems
DAK	Deutsche Angestellte Krankenkasse
DAV	Dienstanschlußvorschriften
DB	Deutsche Bundesbahn
DR	Deutsche Reichsbahn
DDR	Deutsche Demokratische Republik
DES	Data Encryption Standard
DFÜ	Datenfernübertragung
DIN	Deutsches Institut für Normung
DNA	Desoxyribonoclein acid (acid = Säure)
DSB	Datenschutzbeauftragter
DSV	Deutscher Segler-Verband
DtA	Deutsche Ausgleichsbank
Dv/dv	Datenverarbeitung
DVZ	Datenverarbeitungszentrum
ed	erkennungsdienstlich
EDE	Europäische Drogeneinheit
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
EG-Vertrag	Vertrag zur Gründung der Europäischen Gemeinschaft
EG-AH-G	EG-Amtshilfe-Gesetz
EIS	Europäisches Informationssystem
ELKOM	Elektronisches Kommunikationssystem
EP	Europäisches Parlament
EStG	Einkommensteuergesetz
EuGH	Europäischer Gerichtshof
EU	Europäische Union
EUROPOL	Zentrales Europäisches Kriminalpolizeiamt
EURES	Europäisches System zur Übermittlung von Stellen- und Bewerberangeboten im internationalen Ausgleich

EPR	Elektronisches Personenregister
EUROSTAT	Statistisches Amt der Europäischen Gemeinschaft
EURODAC	Europäisches daktyloskopisches System
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft
ENeuOG	Eisenbahnneuordnungsgesetz
FAG	Fernmeldeanlagengesetz
FDS	Falldatei Schleuser/Geschleuste
FKTo	Fernmeldekontonummer
FGG	Gesetz über die Angelegenheiten der freiwilligen Gerichtsbarkeit
FTZ	Forschungs- und Technologiezentrum der Telekom
FVG	Finanzverwaltungsgesetz
GAN	Datei Grenzaktennachweis
GASP	Gemeinsame Außen- und Sicherheitspolitik
GBO	Grundbuchordnung
GBVerf	Grundbuchverfügung
GG	Grundgesetz
GEAUF	Magnetbänder mit Gebührendaten
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GMBl	Gemeinsames Ministerialblatt
GmbH	Gesellschaft mit beschränkter Haftung
GrFMW	Gruppe Fernmeldewesen des BGS
GPS	Globales Positionsbestimmungs-System
GSS	Gemeinschaftliches Statistisches System
GdED	Gewerkschaft der Eisenbahner Deutschlands
GPK	Gemeinsame Provisorische Kontrollinstanz
GSP	Gebührenspeicher
GÜG	Grunstoffüberwachungsgesetz
G10	Gesetz zu Artikel 10 GG
GVG	Gerichtsverfassungsgesetz
HBV	Gewerkschaft Handel, Banken und Versicherungen
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
IHK	Industrie- und Handelskammer
IKK	Innungskrankenkasse
IKPO	Internationale Kriminalpolizei-Organisation
IMKA	Interministerieller Koordinierungssausschuß für Informationstechnik in der Bundesverwaltung
INPOL	Informationssystem der Polizei
InsO	Insolvenzordnung
InVeKoS	Integriertes Verwaltungs- und Kontrollsystem
INZOLL	Informationssystem für den Zollfahndungsdienst
ISDN	Integrated Services Digital Network
ISO	International Standard Organisation
IT	Informationstechnik
ITKA	IT-Koordinierungssausschuß
IVBB	Informationsverbund Berlin–Bonn
JURIS	Juristisches Informationssystem
JZ	Juristenzeitung
KAN	Kriminalaktennachweisdatei
KBA	Kraftfahrt-Bundesamt
KBV	Kassenärztliche Bundesvereinigung
KDS	Kommunikationsdatensatz
KDVG	Kriegsdienstverweigerungsgesetz
KfbG	Kriegsfolgenbereinigungsgesetz
KKH	Kaufmännische Krankenkasse Hannover
KOBRA	Kontrolle bei der Ausfuhr
KOM	Kommission der EU
KVK	Krankenversichertenkarte
LAN	Local Area Network
LBA	Luftfahrt-Bundesamt
LfD	Landesbeauftragter für den Datenschutz
LuftVG	Luftverkehrsgesetz

LKA	Landeskriminalamt
LVA	Landesversicherungsanstalt
MA/MZA	Militärarchiv/Militär-Zwischenarchiv
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den MAD
MfS	Ministerium für Staatssicherheit/Amt für nationale Sicherheit (der ehemaligen DDR)
MOSTA	militärischer Oberstaatsanwalt (der ehemaligen DDR)
MRRG	Melderechtsrahmengesetz
MTB	Manteltarifvertrag Bund
MTArbO	Manteltarifvertrag Arbeiter Ost
MTA	Manteltarifvertrag für Angestellte
MV	Mitteilungsverordnung
MVS	Multiple Virtuell Storage System
NADIS	Nachrichtendienstliches Informationssystem
NADIS-PZD	Personenzentraldatei im NADIS
n. F.	neue Fassung
NJW	Neue Juristische Wochenzeitschrift
N.SIS	nationaler Bestand des Schengener Informationssystems
NVA	Nationale Volksarmee
NVwZ	Neue Zeitschrift für Verwaltungsrecht
NSDAP	Nationalsozialistische Deutsche Arbeiterpartei
NZA	Neue Zeitschrift für Arbeitsrecht
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
ONKZ	Ortsnetzkennzahl
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität
PB-DSV	Postbank-Datenschutzverordnung
PC	Personalcomputer
PDA	Personal Digital Assistant
PERSY	Personalbezogenes Dateiensystem des AA
PIOS	Auskunftssystem über Personen, Institutionen, Objekte und Sachen
PIN	persönliche Identifikationsnummer
PLZ	Postleitzahl
PTNeuOG	Gesetz zur Neuordnung des Postwesens und der Telekommunikation (Postneuordnungsgesetz)
PostG	Gesetz über das Postwesen
PostVerfG	Gesetz über die Unternehmensverfassung der Deutschen Bundespost (Postverfassungsgesetz)
PTB	Physikalisch-Technische Bundesanstalt
PtRegG	Gesetz über die Regulierung der Telekommunikation und des Postwesens
REGA	Registratur- und Schriftgutverwaltungssystem des BfV
RDV	Recht der Datenverarbeitung (Zeitschrift)
RegVBG	Registerverfahrensbeschleunigungsgesetz
RZ	Rechenzentrum
RVO	Reichsversicherungsordnung
RACF	Ressource access control facility
SA	Sturmabteilung
SAEG	Statistisches Amt der Europäischen Gemeinschaft
SAP	Sozialamt der Deutschen Bundespost
SchuVVO	Verordnung über das Schuldnerverzeichnis
SDÜ	Schengener Durchführungsübereinkommen
SED	Sozialistische Einheitspartei Deutschlands
SEDOC	Europäisches System zur Übermittlung von Stellen und Bewerberangeboten im internationalen Ausgleich
SIRENE	Supplementary Information Request for National Entry
SG	Soldatengesetz
SGB I	Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)
SGB IV	Sozialgesetzbuch Viertes Buch (Gemeinsame Vorschriften für die Sozialversicherung)
SGB V	Sozialgesetzbuch Fünftes Buch (Gesetzliche Krankenversicherung)
SGB VI	Sozialgesetzbuch Sechstes Buch (Gesetzliche Rentenversicherung)
SGB VII	Sozialgesetzbuch Siebentes Buch (Gesetzliche Unfallversicherung)
SGB VIII	Sozialgesetzbuch Achtes Buch (Kinder- und Jugendhilfe)

SGB IX	Sozialgesetzbuch Neuntes Buch (Rehabilitations- und Schwerbehindertenrecht)
SGB X	Sozialgesetzbuch Zehntes Buch (Verwaltungsverfahren)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
SGG	Sozialgerichtsgesetz
SIS	Schengener Informationssystem
SS	Schutzstaffel
Stasi	Staatssicherheitsdienst
StGB	Strafgesetzbuch
StMBG	Mißbrauchsbekämpfungs- und Steuerbereinigungsgesetz
StPO	Strafprozeßordnung
StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StUGÄndG	Änderungsgesetz zum Stasi-Unterlagen-Gesetz
StVG	Straßenverkehrsgesetz
StVÄG	Strafverfahrensänderungsgesetz
StVZO	Straßenverkehrs-Zulassungs-Ordnung
SÜG	Sicherheitsüberprüfungsgesetz
Sysop	System operator
TB	Tätigkeitsbericht*)
TDSV	Telekom-Datenschutzverordnung
TK-Anlagen	Telekommunikationsanlagen
TKK	Techniker-Krankenkasse
TOP	Tagesordnungspunkt
UDSV	Teledienst-Unternehmen-Datenschutzverordnung
UNHCR	United Nations the High Commissioner for Refugees (Vereinte Nationen Der Hohe Flüchtlingskommissar)
VdAK	Verband der Angestellten Krankenkassen
VDR	Verband Deutscher Rentenversicherungsträger
VMBl	Ministerialblatt des Bundesministeriums der Verteidigung
VNP	Vorgangsnachweis Personen
VNA	Vorgangsnachweis Amtshilfe
VSA	Verschlußsachenanweisung
VO	Verordnung
VwGO	Verwaltungsgerichtsordnung
VZR	Verkehrszentralregister
WPflG	Wehrpflichtgesetz
WSD	Wasser- und Schiffahrtsdirektion
WRV	Weimarer Reichsverfassung
WÜD	Wiener Übereinkommen über diplomatische Beziehungen
WÜK	Wiener Übereinkommen über Konsularische Beziehungen
ZAP	Zentrale ADV-Prüfung der Bundesverbände der AOK, BKK und IKK
ZAV	Zentralstelle für Arbeitsvermittlung
ZDG	Zivildienstgesetz
ZDr	Zentrale Dienstvorschrift
ZEVIS	Zentrales Verkehrsinformationssystem
ZIS	Zollinformationssystem
ZKA	Zollkriminalamt
ZPO	Zivilprozeßordnung
ZZD	Zentrale Zentralstelle Datenverarbeitung

*) zu den bisher erschienenen Tätigkeitsberichten siehe Rückseite.

Tätigkeits-bericht	Zeitraum	Bundestags-Drucksache
1.	1978	8/2460
2.	1979	8/3570
3.	1980	9/93
4.	1981	9/1243
5.	1982	9/2386
6.	1983	10/877
7.	1984	10/2777
8.	1985	10/4690
9.	1986	10/6816
10.	1987	11/1693
11.	1988	11/3932
12.	1989	11/6458
13.	1990	12/553
14.	1991–1992	12/4805

Druck: Bonner Universitäts-Buchdruckerei, 53113 Bonn
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon: 02 28/3 82 08 40, Telefax: 02 28/3 82 06 44
ISSN 0722-8333