Der Bundesbeauftragte
für den Datenschutz

Tätigkeitsbericht 2003–2004
– 20. Tätigkeitsbericht –

Tätigkeitsbericht 2003–2004

– 20. Tätigkeitsbericht –

Dieser Bericht wurde am 19. April 2005 dem Präsidenten des Deutschen Bundestages, Herrn Wolfgang Thierse, überreicht.

Der Bundesbeauftragte für den Datenschutz
Peter Schaar

Tätigkeitsbericht 2003 und 2004 des Bundesbeauftragten für den Datenschutz – 20. Tätigkeitsbericht –

Inhaltsverzeichnis

Seite

Abbildungsverzeichnis

Seite

Seite

Seite

1 Einführung – Überblick und Ausblick –

Die Suchmaschine Google liefert zum Stichwort „Datenschutz“ mehr als 30 Millionen Treffer, beim englischen „privacy“ sind es über 430 Millionen. Es ist also kaum zu bestreiten, dass sich der Schutz personenbezogener Daten inzwischen sowohl in Deutschland als auch international etabliert hat. Seit dem Volkszählungsurteil des Bundesverfassungsgerichts vor mittlerweile mehr als zwanzig Jahren ist auch klar, dass der Datenschutz als Recht auf informationelle Selbstbestimmung zu den Grundrechten gehört.

Trotzdem wird bisweilen der Eindruck vermittelt, Datenschutz sei eine lästige und bürokratische Pflichtübung, die sinnvolle Lösungen be- und verhindere. Immer wieder höre ich die Forderung, der Datenschutz müsse zugunsten vermeintlich bedeutsamerer Rechtsgüter – wie Sicherheit, Wissenschafts- und Forschungsfreiheit, Steuergerechtigkeit – eingeschränkt werden. In einzelnen Bereichen ist es auch tatsächlich zu erheblichen Gewichtsverschiebungen zu Lasten des Datenschutzes gekommen, vor allem für Zwecke der Kriminalitätsbekämpfung und im Finanz- und Sozialwesen.

Im Berichtszeitraum war es wiederum das Bundesverfassungsgericht, das in verschiedenen Entscheidungen das Grundrecht auf informationelle Selbstbestimmung gestärkt und damit einen wichtigen Kontrapunkt gesetzt hat. Dies gilt vor allem für die Entscheidung zur akustischen Wohnraumüberwachung („Großer Lauschangriff“) vom 3. März 2004, die betont, dass ein unantastbarer Kernbereich privater Lebensgestaltung vor jeglicher Überwachung geschützt bleiben muss, für den also auch Nützlichkeitserwägungen einen Eingriff nicht rechtfertigen können. Wie vor zwanzig Jahren beim Volkszählungsurteil ist in einigen Diskussionsbeiträgen das Bemühen erkennbar, das Urteil zum Lauschangriff kleinzureden. So wird davon gesprochen, die Entscheidung habe ausschließlich Konsequenzen für die akustische Wohnraumüberwachung, nicht jedoch für andere Befugnisse zur heimlichen Datenerhebung, etwa für die Telefonüberwachung. Dabei hat das BVerfG in einer anderen Entscheidung vom gleichen Tage festgestellt, dass die Grundsätze des Urteils zum Lauschangriff auch bei der Befugnis zur präventiven Telekommunikationsüberwachung durch das Zollkriminalamt zu beachten sind. Bei einem von mir veranstalteten wissenschaftlichen Kolloquium bestand zwischen den Experten Einigkeit, dass eine „kleine Lösung“ nicht ausreicht, also auch die übrigen Befugnisse zur verdeckten Datenerhebung auf den Prüfstand gehören. (Vgl. Nr. 7.1)

Auch die Befugnisse, die den Sicherheitsbehörden nach den terroristischen Anschlägen am 11. September 2001 eingeräumt wurden, müssen überprüft werden, wie dies bereits im Gesetzgebungsverfahren vorgesehen wurde. In diesem Zusammenhang begrüße ich es, wenn die dabei verwendeten Kriterien und die Ergebnisse der Öffentlichkeit zugänglich gemacht werden, damit die anstehende politische Debatte auf Basis einer gesicherten Faktenlage geführt werden kann. Dies ist deshalb besonders wichtig, weil über Grundrechtseingriffe zu entscheiden ist, die nur unter Wahrung des verfassungsrechtlichen Verhältnismäßigkeitsgrundsatzes eingeführt oder fortgesetzt werden dürfen. (Vgl. Nr. 5.5.4)

Technologische Innovationen, insbesondere bei der Ortungstechnik, der Datenübertragung und bei der Bilderkennung, sind im Berichtszeitraum so weit vorangeschritten, dass die durch sie ermöglichten neuen Dienste und Verfahren kurz vor ihrer Einführung bzw. Durchsetzung in großem Maßstab stehen: Mobilkommunikations- und Ortungstechniken erlauben Lokalisierungsdienste, die nicht nur zur Komfortsteigerung beitragen und neue Geschäftsmodelle ermöglichen, sondern auch die Verfolgung und Registrierung der Aufenthaltsorte und Bewegungen von Personen gestatten. Biometrische Verfahren können sowohl im privaten als auch im staatlichen Bereich eingesetzt werden, um die Identifikation von Personen zu erleichtern. Sie ermöglichen es jedoch auch, den Einzelnen heimlich zu überwachen. Leider hat die Entwicklung technologischer Instrumente, mit denen sich der Einzelne gegen Überwachung schützen kann, nicht mit den Überwachungstechnologien Schritt gehalten. Umso wichtiger ist es, bei neuen Systemen den Datenschutz bereits in der Entwicklungs- und Konzeptionsphase zu berücksichtigen, wie dies das Bundesdatenschutzgesetz bereits seit 2001 vorsieht. Offenbar hat diese Erkenntnis allerdings noch nicht alle Beteiligten erreicht. So musste ich feststellen, dass selbst bei einem Großprojekt wie der Umstellung der Arbeitslosen- und Sozialhilfe auf das Arbeitslosengeld II elementare Datenschutzanforderungen bei der Systemgestaltung nicht beachtet wurden. (Vgl. Nr. 16.1)

Von grundlegender Bedeutung sind auch die neuen Erkenntnisse bei der Erforschung des menschlichen Genoms und die daraus erwachsenen Anwendungsmöglichkeiten. Aus der DNA lassen sich sowohl die Identität und die Abstammung feststellen als auch Hinweise auf persönliche Eigenschaften und über die Veranlagung zu Krankheiten gewinnen. Die Kontroversen um die Nutzung der DNA als „Fingerabdruck des 21. Jahrhunderts“ und über die Zulässigkeit heimlicher Vaterschaftstests sind dabei nur ein erster Ausdruck für die Umwälzungen, die sich aus den neuen Erkenntnissen ergeben. Die hiermit verbundenen Fragen gehen weit über das kodifizierte Datenschutzrecht hinaus. Die kommenden Jahre werden entscheidende Weichenstellungen bringen, ob angesichts dieser qualitativ neuen Möglichkeiten das Persönlichkeitsrecht bewahrt werden kann. (Vgl. Nr. 7.3)

Bei der Datenschutzgesetzgebung wurden während der Berichtsperiode leider kaum sichtbare Fortschritte erzielt. Das für den Vollzug des BDSG 2001 erforderliche Datenschutzauditgesetz, das vom Bundestag seit langem geforderte Arbeitnehmerdatenschutzgesetz und das dringend notwendige Gendiagnostikgesetz lassen weiter auf sich warten, und bei der angekündigten grundlegenden Modernisierung des Datenschutzrechts herrscht Stillstand. Lediglich in einigen gesetzlichen Spezialregelungen konnten erfreuliche Ergebnisse erreicht werden – ich möchte hier beispielhaft auf die Bestimmungen zum Datenschutz bei der Gesundheitskarte hinweisen. Vor diesem Hintergrund begrüße ich Ankündigungen aus dem

Deutschen Bundestag, in wichtigen Datenschutzfragen parlamentarisch initiativ zu werden, wie dies bereits bei dem – mit dem Datenschutz eng verwandten – Informationsfreiheitsgesetz deutlich wurde. (Vgl. Nr. 2.7)

Die grenzüberschreitende Datenverarbeitung und vor allem die Datenübermittlungen zwischen den nunmehr 25 Mitgliedstaaten der EU nehmen deutlich zu. Zwar ist die europäische Datenschutzrichtlinie inzwischen durchgehend in nationales Recht umgesetzt; sie bezieht sich jedoch nicht auf die Verarbeitung personenbezogener Daten im Sicherheitsbereich. Wenn Polizei- und Strafverfolgungsbehörden intensiver zusammenarbeiten und dabei auch personenbezogene Daten ohne Rücksicht auf nationale Grenzen austauschen sollen, wie dies im Haager Programm beschlossen wurde, muss der Datenschutz auch auf diesem Gebiet europäisiert werden. Ausgangspunkt müssen dabei die Datenschutz-Grundrechte der Europäischen Grundrechtecharta sein, die unverändert in den Entwurf für eine Europäische Verfassung übernommen wurden. (Vgl. Nr. 3.3)

Die Berichtsperiode umfasst etwa zur Hälfte noch die Tätigkeiten unter der Verantwortung meines Amtsvorgängers Dr. Joachim Jacob, dem ich auch an dieser Stelle für seine hervorragende Arbeit danken möchte. Am 17. Dezember 2003 wurde ich zum Bundesbeauftragten für den Datenschutz ernannt. Für diesen Tätigkeitsbericht trage ich selbstverständlich die volle Verantwortung. Dabei möchte ich darauf hinweisen, dass die Tätigkeiten – auch wenn über sie in der „Ich-Form“ berichtet wird – größtenteils von meinen Mitarbeiterinnen und Mitarbeitern ausgeführt wurden. Auch ihnen möchte ich für ihr großes Engagement und ihre erfolgreiche Arbeit danken. Mein Dank gilt schließlich den Abgeordneten aller Fraktionen des Deutschen Bundestages, die sich nachhaltig für den Datenschutz interessiert und engagiert haben, und den Vertretern von öffentlichen und privaten Stellen, für die Datenschutz eine Bedingung erfolgreichen Handelns ist.

Peter Schaar

2 Datenschutzrechtlicher Rahmen

Wirkungsvoller Datenschutz setzt einen rechtlichen Rahmen voraus, der den Umfang und die Grenzen zulässiger Datenverarbeitung klar umreißt und die Rechte und Pflichten aller Beteiligter festlegt. Aufgrund der rasanten technischen Entwicklung und immer neuer Problemfelder muss dies als dynamischer Prozess begriffen werden, der sich in einem stetigen Wandel befindet und auch den Gesetzgeber immer wieder aufs neue fordert, um bestehende Normen neuen Entwicklungen und Erkenntnissen anzupassen und verbliebene oder sich neu eröffnende Regelungslücken zu schließen. Dabei geht es nicht um bürokratische Überregulierung, sondern im Gegenteil darum, durch eine umfassende Modernisierung des Datenschutzrechts zu effizienten und unbürokratischen Lösungen zu kommen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat zu Beginn der 15. Legislaturperiode des Deutschen Bundestages in einer Entschließung eine Reihe von Forderungen an Bundesgesetzgeber und Bundesregierung beschlossen (vgl. Kasten zu Nr. 2, Anlage 13), um den Reformbedarf beim Datenschutz aufzuzeigen und Anstöße für die gesetzgeberische Arbeit zu geben.

Kasten zu Nr. 2

Forderungen der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Weiterentwicklung des Datenschutzrechts im Überblick:

- Verankerung des Rechts auf informationelle Selbstbestimmung als eigenständiges Grundrecht im Grundgesetz
- Modernisierung des BDSG
  - Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes
  - gleichwertiges Schutzniveau in allen Bereichen
  - verbesserte Regelungen zur Einwilligung
- Realisierung des Datenschutzaudits
- Förderung von datenschutzgerechter Technik
- Anonyme Internetnutzung
- Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden
- Verbesserter Schutz von Gesundheitsdaten
- Datenschutz in der Gentechnik
- Datenschutz im Steuerrecht
- Arbeitnehmerdatenschutz
- Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

Der volle Wortlaut der Entschließung ist als Anlage 13 abgedruckt.

2.1 Weiterentwicklung des Datenschutzrechts

Die zweite Stufe der Datenschutzreform ist ins Stocken geraten.

Bereits während der Vorbereitung der BDSG-Novelle 2001 hatte die Bundesregierung eine zweite Stufe der Reform des Datenschutzrechts angekündigt, mit der wichtige Weichenstellungen für einen modernen und innovativen Datenschutz vorgenommen werden sollten. Ein hierzu in Auftrag gegebenes umfangreiches Gutachten enthielt eine Fülle von beachtlichen Vorschlägen und Anregungen (vgl. 19. TB Nr. 3.3). Obwohl sich der Deutsche Bundestag mehrfach und zum Teil mit eindrucksvollen Mehrheiten hinter dieses Reformvorhaben gestellt hat (Entschließung zum 18. TB, Bundestagsdrucksache 14/9490 Nr. 2; Beschluss „Umfassende Modernisie-

rung des Datenschutzrechts voranbringen“, Bundestagsdrucksache 14/9709; Entschließung zum 19. TB, Bundestagsdrucksache 15/4597 Nr. 1, Kasten zu Nr. 2.1), das auch Gegenstand der Koalitionsvereinbarung für die 15. Legislaturperiode ist, hat die Bundesregierung bislang keinen entsprechenden Gesetzentwurf vorgelegt. Umso wichtiger ist es, dass dieses Reformvorhaben nunmehr zügig in Angriff genommen wird.

Die Zusammenfassung der inzwischen fast unüberschaubaren Zahl von Spezialregelungen in einem leicht verständlichen und übersichtlichen neuen Datenschutzrecht, wie es auch das Gutachten vorschlägt, könnte ein erster wichtiger Schritt auf dem Weg zur Modernisierung des Datenschutzrechts sein. Auch die ständig wachsende Anzahl groß angelegter Datenbestände im nicht-öffentlichen Bereich und deren zunehmende Vernetzung sowie neue technologische Entwicklungen lassen das geltende Datenschutzrecht an seine Grenzen stoßen und ergeben neuen gesetzgeberischen Handlungsbedarf.

Deswegen bedauere ich die Verzögerung bei der Reform des Datenschutzrechts außerordentlich. Gerade in diesem Bereich ist eine kontinuierliche Weiterentwicklung und Anpassung an sich sehr rasch ändernde Verhältnisse unabdingbar und einmal eingetretene Fehlentwicklungen lassen sich nur schwer wieder rückgängig machen. Auch wird der gesetzgeberische Aufwand immer größer, je länger die Modernisierung des Datenschutzrechts auf sich warten lässt.

Kasten zu Nr. 2.1

Aus der Entschließung des Deutschen Bundestages zum 19. Tätigkeitsbericht vom 17. Februar 2005, Bundestagsdrucksache 15/4597:

„1. Der Deutsche Bundestag hält eine Modernisierung und Weiterentwicklung des Datenschutzrechts in der Bundesrepublik Deutschland unverändert für erforderlich und fordert die Bundesregierung auf, die entsprechenden Arbeiten zügig fortzuführen. Dabei sollte zunächst der Schwerpunkt auf einer kontinuierlichen Vereinfachung des Rechts und einer Konzentration der datenschutzrechtlichen Vorschriften im Bundesdatenschutzgesetz liegen. Spezialgesetzliche Sonderregelungen sollten auf das unabweisbar notwendige Maß zurückgeführt werden (19. TB Nr. 3.3.).

...“

2.2 Wann endlich kommt das Auditgesetz?

Die Regelung zum Datenschutzaudit in § 9a BDSG läuft mangels Umsetzung unverändert leer.

Das Datenschutzaudit, das im Grundsatz seit der Novellierung des Bundesdatenschutzgesetzes im Mai 2001 in § 9a geregelt ist (vgl. 19. TB Nr. 3.2.1), war als eine datenschutzrechtliche Innovation gedacht. Damit diese Regelung aber die beabsichtigten Wirkungen entfalten kann, bedarf es nach § 9a Satz 2 BDSG eines Durchführungsgesetzes, das die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter zum Gegenstand haben soll. Zu dessen Vorbereitung hatte das BMI die Verwaltungshochschule Speyer mit einer Gesetzesfolgenabschätzung beauftragt, deren Ergebnis für Herbst 2002 angekündigt worden war, aber jedenfalls mir bis heute nicht bekannt geworden ist.

Zu meinem großen Bedauern hat die Bundesregierung auch bislang keinen entsprechenden Gesetzentwurf vorgelegt. Obwohl der Deutsche Bundestag die Grundsatzentscheidung für ein Datenschutzaudit bereits getroffen hat und es nur noch um dessen nähere Ausgestaltung geht, wurden sogar erneut der Sinn einer solchen Regelung in Frage gestellt und Gesichtspunkte der Modernisierung der Verwaltung und der Entbürokratisierung dagegen vorgebracht.

Für diese Verzögerung habe ich kein Verständnis. Dabei wurde völlig übersehen, dass gerade das Datenschutzaudit ein wichtiger Reformschritt auf dem Weg zu einem modernen Datenschutz ist, weil es wegführt von Verbot, Kontrolle und Sanktion und statt dessen als Mittel des wirtschaftlichen Wettbewerbs begriffen wird, das von den Beteiligten gezielt zur Stärkung ihrer Marktposition eingesetzt werden kann. Aufgrund vielfältiger Überlegungen und Vorschläge, die an mich herangetragen worden sind, bin ich überzeugt davon, dass sich ein Verfahren finden lässt, das in Kooperation mit privaten Anbietern effizient und unbürokratisch ist und ohne zusätzliche Verwaltungsstrukturen auskommt. Erfahrungen auf Länderebene und zahlreiche Anfragen bei mir, wo ein Audit nach § 9a BDSG beantragt werden kann, zeugen von einem großen Interesse betroffener Wirtschaftskreise an einer solchen Regelung, deren weiteres Hinausschieben nachhaltig negative Folgen haben kann, wie ich bereits in meinem 19. TB (Nr. 3.2.1) ausgeführt habe.

Deswegen habe ich die Ankündigung aus dem parlamentarischen Raum, im Frühjahr 2005 mit den Arbeiten an einem Auditgesetz zu beginnen, mit großem Interesse zur Kenntnis genommen. Gerne bin ich bereit, im Rahmen meiner Möglichkeiten dabei aktiv mitzuwirken, damit dieses wichtige datenschutzrechtliche Reformvorhaben endlich verwirklicht werden kann.

2.3 Zusammenarbeit bei der Datenschutzkontrolle

Die Verteilung der Datenschutzaufsicht in Deutschland auf viele Schultern verlangt Zusammenarbeit und gegenseitige Abstimmung.

Wegen der föderalen Struktur und verfassungsrechtlicher Vorgaben ist die Datenschutzaufsicht in der Bundesrepublik Deutschland auf eine Vielzahl von Stellen verteilt. Neben dem Bundesbeauftragten und den Landesbeauftragten für Datenschutz gibt es die Aufsichtsbehörden der Länder für den nicht-öffentlichen Bereich sowie eigene unabhängige Datenschutzbeauftragte für öffentlich-rechtliche Rundfunkanstalten und für Kirchen.

Da die anzuwendenden Rechtsnormen vielfach die gleichen oder zumindest ähnlich sind und vergleichbare Problemstellungen möglichst überall in gleicher Weise gelöst werden sollten, ist es unerlässlich, dass sich die Kontrollinstanzen wechselseitig informieren und abstimmen, um trotz ihrer jeweiligen Unabhängigkeit zu möglichst einheitlichen Rechtsauffassungen zu kommen. § 26 Abs. 4 BDSG weist mir die Aufgabe zu, auf die Zusammenarbeit mit den öffentlichen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 BDSG hinzuwirken. Diesem gesetzlichen Auftrag komme ich u. a. dadurch nach, dass ich aktiv an entsprechenden Arbeitskreisen und Konferenzen teilnehme.

Für den Bereich der öffentlichen Verwaltung wird die Zusammenarbeit von der Konferenz der Datenschutzbeauftragten des Bundes und der Länder koordiniert, die zweimal im Jahr zusammentritt und in mehreren Arbeitskreisen auf Fachebene vorbereitet wird. Eine Reihe von einstimmig angenommenen Entschließungen zu wichtigen datenschutzrechtlichen Fragen, auf die ich in diesem Tätigkeitsbericht an inhaltlich entsprechender Stelle jeweils hinweise, sind nur ein Ergebnis dieses fruchtbaren und ergebnisorientierten Austausches.

Für den nicht-öffentlichen Bereich treffen sich die Vertreter der obersten Aufsichtsbehörden der Länder zweimal im Jahr im so genannten „Düsseldorfer Kreis“ (vgl. 17. TB Nr. 31.5) zum Erfahrungsaustausch, um eine möglichst einheitliche Rechtsanwendung sicherzustellen. Auch in diesem Gremium und seinen vorbereitenden Arbeitsgruppen bin ich vertreten. Obwohl es sich um kein Beschlussgremium handelt, das für alle verbindlich Entscheidungen treffen kann, sondern um ein Forum zum Austausch von Informationen und Rechtsauffassungen, ist es in der Vergangenheit immer wieder erfolgreich gelungen, gemeinsame Positionen der Aufsichtsbehörden zu entwickeln und durchzusetzen, was allerdings fortdauernde Meinungsunterschiede im Einzellfall (vgl. Nr. 21.3) nicht ausschließt.

Auch die Datenschutzbeauftragten der öffentlich-rechtlichen Rundfunkanstalten und der Kirchen haben ihre Abstimmungsgremien, an denen ich als Gast schon teilgenommen habe. Zur Information der Öffentlichkeit über datenschutzrechtliche Themen und Aktivitäten betreibe ich als Projektpartner zusammen mit anderen unabhängigen Datenschutzkontrollinstanzen das virtuelle Datenschutzbüro (http://www.datenschutz.de).

Meinem gesetzlichen Koordinierungsauftrag werde ich weiterhin mit dem Ziel nachkommen, dass trotz der Vielzahl der unterschiedlichen Kontrollinstanzen eine möglichst einheitliche Datenschutzpraxis in Deutschland erreicht wird. Bei der anstehenden Neufassung des Datenschutzrechts sollte erwogen werden, die Struktur des Datenschutzes an sich zu vereinfachen.

Kasten zu Nr. 2.2

§ 9a BDSG
Datenschutzaudit

Zur Verbesserung des Datenschutzes und der Datensicherheit können Anbieter von Datenverarbeitungssystemen und -programmen und datenverarbeitende Stellen ihr Datenschutzkonzept sowie ihre technischen Einrichtungen durch unabhängige und zugelassene Gutachter prüfen und bewerten lassen sowie das Ergebnis der Prüfung veröffentlichen. Die näheren Anforderungen an die Prüfung und Bewertung, das Verfahren sowie die Auswahl und Zulassung der Gutachter werden durch besonderes Gesetz geregelt.

2.4 Stärkung der behördlichen Datenschutzbeauftragten

Mangels ausreichender Freistellung können die behördlichen Datenschutzbeauftragten ihre gesetzlichen Aufgaben oft nicht optimal erfüllen.

Den behördlichen Datenschutzbeauftragten, die seit der BDSG-Novelle 2001 in allen Dienststellen des Bundes bestellt sein müssen (vgl. 19. TB Nr. 3.2.5), hat das Gesetz wichtige Aufgaben zur Gewährleistung umfassenden Datenschutzes im Interesse der Bürger und Beschäftigten übertragen. Ihre kontinuierliche Tätigkeit ist ein besonders wichtiger Beitrag zur Umsetzung der datenschutzrechtlichen Bestimmungen und Grundsätze. Deswegen habe ich im Berichtszeitraum diese Arbeit weiter gefördert. Als zentrales Problem hat sich dabei immer wieder herausgestellt, dass das BDSG, anders als etwa für Gleichstellungsbeauftragte oder Mitglieder von Personalvertretungen vorgesehen, keine konkreten Freistellungsregelungen für die Tätigkeit als Datenschutzbeauftragter vorsieht. Dies führt vielfach dazu, dass die Betroffenen ihre Aufgaben nach dem BDSG nur neben ihrer eigentlichen Tätigkeit ausüben können und deswegen schon aus rein zeitlichen Gründen nicht in der Lage sind, allen an dieses Amt gestellten Anforderungen in vollem Umfang gerecht werden zu können. Deswegen ist der Gesetzgeber aufgefordert, hier umgehend mit einer adäquaten gesetzlichen Freistellungsregelung Abhilfe zu schaffen. In einer Behörde mit mehreren hundert Mitarbeitern und umfangreicher elektronischer Datenverarbeitung sollte das Amt des Datenschutzbeauftragten entweder in Vollzeit wahrgenommen werden können oder mit entsprechendem Hilfspersonal nach § 4f Abs. 5 Satz 1 BDSG versehen sein. Obwohl eine solche gesetzliche Regelung bislang fehlt, habe ich dennoch in jüngster Zeit feststellen können, dass in einigen Ressorts Anstrengungen in diese Richtung unternommen werden. Weiter wäre es wünschenswert, wenn die Datenschutzbeauftragten bei den obersten Bundesbehörden für ihre Kollegen in den jeweils nachgeordneten Behörden eine gewisse Leit- und Koordinierungsfunktion übernehmen könnten. Auch hierfür gibt es bei einigen Ressorts positive Beispiele, die sich ohne eine entsprechende gesetzliche Regelung aber wohl nicht allgemein durchsetzen werden.

Den von mir initiierten Erfahrungsaustausch mit den Datenschutzbeauftragten der obersten Bundesbehörden habe ich auch im Berichtszeitraum fortgeführt. Bei zwei Veranstaltungen im März 2003 und Januar 2004 sowie einem Sondertreffen zum Mitarbeiterdatenschutz im Sommer 2004 (vgl. Nr. 10.5) konnten die Situation der behördlichen Datenschutzbeauftragten in ihren jeweiligen Dienststellen, datenschutzrechtliche Probleme und Entwicklungen von allgemeinem Interesse und konkrete Einzelfragen vertieft erörtert werden. Themenschwerpunkte waren die Vorstellung des Verfahrens „Datscha“ zur automatisierten Führung von Verfahrensverzeichnissen, Fragen der Aus- und Fortbildung, Sicherheitskonzepte und IT-Fragen, Entwicklung des Datenschutzrechts, private Internet- und E-Mail-Nutzung am Arbeitsplatz und Mitarbeiterdatenschutz.

Das unverändert große Interesse an diesem Erfahrungsaustausch ist für mich ein Ansporn, auch weiterhin ein Forum zur Erörterung gemeinsamer Probleme und Diskussion offener Rechtsfragen anzubieten und dadurch die verantwortungsvolle Tätigkeit der behördlichen Datenschutzbeauftragten nach Kräften zu unterstützen.

2.5 Arbeitnehmerdatenschutzgesetz

Gesetzgeberische Initiativen zur Schaffung eines Arbeitnehmerdatenschutzgesetzes waren auch in diesem Berichtszeitraum nicht zu verzeichnen.

Die Notwendigkeit eines Arbeitnehmerdatenschutzgesetzes hat die Fachwelt seit langem aufgezeigt und auch wiederholt angemahnt. In zurückliegenden Tätigkeitsberichten (vgl. u. a. 18. TB Nr. 1.8; 18.1; 19. TB Nr. 21.1) hatte ich zudem mehrfach an die Bundesregierung appelliert, einen entsprechenden Gesetzentwurf vorzulegen und die Grundsätze und Gesichtspunkte ausführlich dargestellt, die hierbei Berücksichtigung finden sollten.

Mehrfach hat auch der Deutsche Bundestag in seinen Entschließungen zu meinen Tätigkeitsberichten die Bedeutung gesetzlicher Regelungen zum Arbeitnehmerdatenschutz betont und die Bundesregierung aufgefordert, einen Gesetzentwurf in das parlamentarische Verfahren einzubringen (vgl. zuletzt Beschlussempfehlung zum 18. TB, Bundestagsdrucksache 14/9490).

Ausdrücklich begrüße ich, dass die Bundesregierung in ihrer Stellungnahme zu meinem 19. TB meine Auffassung teilt, dass die Schaffung eines Arbeitnehmerdatenschutzgesetzes erforderlich ist und erklärt, den Gesetzentwurf in dieser Legislaturperiode vorzulegen. Es ist zu hoffen, dass dieses überfällige Projekt nun endlich auf den Weg gebracht wird. Gesetzliche Regelungen zum Schutz der Daten von Arbeitnehmerinnen und Arbeitnehmern dürfen nicht zuletzt aufgrund einer immer schneller fortschreitenden technischen Entwicklung und den aktuellen Veränderungen in der Arbeitswelt von Behörden, Betrieben und Unternehmen nicht länger auf sich warten lassen (vgl. Nr. 10.1).

2.6 Wann kommt das Gendiagnostikgesetz?

Bereits seit einigen Jahren fordere ich die Schaffung von Regelungen im Bereich der Gendiagnosen.

Wie ich bereits berichtet habe (19. TB Nr. 28.5), verläuft die wissenschaftliche Entwicklung auf dem Gebiet der molekulargenetischen Forschung rapide. Neuere Forschungen haben zu der Entdeckung immer weiterer Sequenzen geführt, deren Auftreten ein Indiz für einen möglichen Ausbruch bestimmter Krankheiten ist. Es ist zu erwarten, dass in naher Zukunft weitere Erkenntnisse über den Zusammenhang zwischen besonderen Genomkonstellationen und Eigenschaften seines Trägers gewonnen werden. Diese werden erhebliche Folgen sowohl in der medizinischen Behandlung als auch in anderen Teilen unseres täglichen Lebens mit sich bringen.

Da für die flächendeckende Anwendung von Gendiagnosen die vorhandenen rechtlichen Rahmenbedingungen nicht ausreichend sind, fordere ich schon seit Jahren die Schaffung eines entsprechenden Gendiagnostikgesetzes. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits auf ihrer 62. Konferenz im Oktober 2001 eine Entschließung mit einer entsprechenden Aufforderung an den Gesetzgeber gefasst (vgl. 19. TB Anlage 19).

Durch Genanalysen können lange vor dem tatsächlichen Ausbruch einer Krankheit Vorhersagen über deren Eintrittswahrscheinlichkeit getroffen werden, selbst wenn dem Betroffenen seine Anfälligkeit für diese Krankheit nicht bekannt ist. Dies kann zu Begehrlichkeiten von potentiellen Arbeitgebern oder beim Abschluss von Versicherungsverträgen führen. Auch lassen Genanalysen Rückschlüsse auf die medizinische Konstellation von Blutsverwandten zu, ohne dass diese an der Untersuchung beteiligt sind; hier sind insbesondere heimliche Vaterschaftstests zu nennen. Daher sind besondere Regelungen zu schaffen, die der Sensibilität und Komplexität dieser Materie gerecht werden. Wichtig ist dabei die Schaffung eines gegen Jedermann gerichteten, ausdrücklichen und strafbewehrten Verbotes, die Genanalyse eines Anderen ohne Befugnis durchzuführen oder durchführen zu lassen oder Ergebnisse der Genanalyse eines Anderen zu verarbeiten oder zu nutzen.

Im politischen Raum werden zur Zeit erste Entwürfe erörtert, die insbesondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, zu Forschungszwecken sowie Fragen im Zusammenhang mit Arbeits- und Versicherungsverhältnissen enthalten. Ich bin guter Hoffnung, dass datenschutzgerechte Lösungen entwickelt werden und dass das Gendiagnostikgesetz noch in dieser Legislaturperiode verabschiedet wird (vgl. Kasten a und b zu Nr. 2.6).

Kasten a zu Nr. 2.6

Die wichtigsten datenschutzrechtlichen Forderungen zum Gendiagnostikgesetz

- Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;
- Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;
- Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;
- Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;
- Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;
- Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;
- Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;
- Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;
- Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;
- Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung individuell bedeutsame Untersuchungsergebnisse mitzuteilen;
- Absicherung der Regelungen durch die Einführung von Straftatbeständen.

2.7 Informationsfreiheitsgesetz

Das Informationsfreiheitsgesetz des Bundes wurde endlich auf den Weg gebracht.

Schon vor Jahren hatte die Bundesregierung angekündigt, dem Beispiel einer großen Zahl demokratisch verfasster Staaten und einiger Bundesländer folgen und ein Informationsfreiheitsgesetz vorlegen zu wollen, mit dem der freie und voraussetzungslose Zugang jeden Bürgers zu den bei der Verwaltung des Bundes vorhandenen Akten, Unterlagen und Informationen sichergestellt werden solle (vgl. 19. TB Nr. 3.4).

Inzwischen haben die Fraktionen von SPD und BÜNDNIS 90/DIE GRÜNEN den Entwurf eines Informationsfreiheitsgesetzes erarbeitet und am 14. Dezember 2004 in den Deutschen Bundestag eingebracht (Bundestagsdrucksache 15/4493).

Zum Spannungsverhältnis zwischen dem freien Zugang zu Unterlagen und Informationen der Verwaltung einerseits und dem Schutz der Persönlichkeitsrechte Betroffener andererseits enthält der Gesetzentwurf Ausnahmeregelungen und Verfahrensvorschriften, die ich aus datenschutzrechtlicher Sicht für ausreichend halte, um zu einem fairen Interessenausgleich zu kommen. Darüber hinaus ist vorgesehen, mir die Aufgabe eines Bundesbeauftragten für die Informationsfreiheit zu übertragen, die mit den gleichen Rechten und Pflichten versehen sein soll, die das BDSG für meine Tätigkeit als Bundesbeauftragter für den Datenschutz vorsieht. Danach soll sich jeder an mich wenden können, wenn er sein Recht auf Informationszugang nach den vorgesehenen gesetzlichen Vorschriften als verletzt ansieht.

In dieser beabsichtigten Doppelfunktion, die es in gleicher Weise auch in den Bundesländern gibt, die bereits ein Informationsfreiheitsgesetz erlassen haben, und die sich dort bewährt hat, sehe ich keine Interessenkollision, denn Informationsfreiheit und Datenschutz sind keine unüberbrückbaren Gegensätze, sondern eher die zwei Seiten der gleichen Medaille, geht es doch in beiden Fällen um Offenheit und Transparenz. Auf diese Weise wird es möglich, dass im Einzelfall erforderliche Abgrenzungen und der nötige Interessenausgleich von einer, beiden Seiten gesetzlich gleichermaßen verpflichteten Stelle vorgenommen und unnötige Frontstellungen vermieden werden, was weder dem Datenschutz noch der Informationsfreiheit dienen würde.

Den weiteren Gang des Gesetzgebungsverfahrens werde ich im Rahmen meiner Aufgaben und Zuständigkeiten begleiten und dabei insbesondere darauf achten, dass ein ausgewogenes Verhältnis zwischen dem Schutz von Persönlichkeitsrechten und Informationsfreiheit erhalten bleibt.

Kasten b zu Nr. 2.6

Aus der Entschließung des Deutschen Bundestages zum 19. Tätigkeitsbericht vom 17. Februar 2005, Bundestagsdrucksache 15/4597

„3. Der Deutsche Bundestag bekräftigt seine Forderung aus der Entschließung zum 18. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz, jetzt zügig ein Gendiagnostikgesetz vorzulegen. Die Entschlüsselung des menschlichen Genoms und die damit verbundenen Anwendungsmöglichkeiten erfordern eine umfassende gesetzliche Regelung genetischer Untersuchungen für medizinische Zwecke für die Lebensplanung, für die Erstellung von Abstammungsgutachten, im Versicherungsbereich, im Arbeitsleben sowie für Zwecke wissenschaftlicher Forschung. Zuwiderhandlungen gegen grundlegende Vorschriften der Regelung, insbesondere über die erforderliche Einwilligung der betroffenen Person, sind entsprechend der Schwere des Verstoßes durch Straf- oder Bußgeldbestimmungen zu sanktionieren (19. TB, Nr. 1.9, 28.5). Es sollte ein entsprechender Gesetzentwurf so rechtzeitig vorgelegt werden, dass er noch in dieser Legislaturperiode vom Deutschen Bundestag verabschiedet werden kann.

..."

3 Datenschutz in Europa

3.1 Die zunehmende Bedeutung europäischer Rechtsinstrumente und ihre Auswirkungen auf den Datenschutz

Die Ankündigung eines europäischen Raums der Freiheit, der Sicherheit und des Rechts macht die Schaffung eines harmonisierten Datenschutzes auch für den Bereich der Kriminalitätsbekämpfung dringlich.

Die Schaffung eines Raums der Freiheit, der Sicherheit und des Rechts ist in der Politik der Europäischen Union an die erste Stelle getreten. Eines der wichtigsten Ziele besteht darin, einen ungehinderten Datenaustausch im Bereich der Dritten Säule, also zwischen den Polizeibehörden und den Organen der Strafverfolgung der Mitgliedstaaten, zu gewährleisten. Ein harmonisierter europäischer Datenschutz auch für dieses Gebiet ist von der gleichen grundsätzlichen Bedeutung wie seinerzeit die EG-Datenschutzrichtlinie für den Bereich der Ersten Säule, also im wesentlichen den privaten Sektor. Dazu gehören einheitliche Rechtsgrundsätze, eine effektive Kontrolle der europäischen Informationssysteme und die Gewährleistung der Einbeziehung der unabhängigen Datenschutzbehörden in die Vorbereitung von Rechtsakten durch den europäischen Gesetzgeber.

Bereits mit der Harmonisierung des Datenschutzes im Bereich der Ersten Säule hat die europäische Dimension in der Praxis des Datenschutzes eine neue Qualität erhalten. Wesentliche Entscheidungen sind ohne Berücksichtigung der europäischen Dimension hier nicht mehr möglich. Die notwendige fortdauernde Anpassung des Datenschutzes an die sich dynamisch weiterentwickelnde Informationstechnik wird künftig im wesentlichen auch durch Entwicklungen auf der europäischen Ebene bestimmt.

Erfreulicherweise gelingt es zunehmend besser, mit der IT-Industrie bereits im Entwicklungsstadium in einen Dialog über neue technologische Produkte und Anwendungskonzepte einzutreten und so den Datenschutz von Anfang an zu integrieren. Ich setze mich dafür ein, dass sich dieser Trend fortsetzt. Da die IT-Industrie international aufgestellt ist, ist für einen wirksamen Datenschutz auch die Diskussion auf internationaler Ebene zu führen. Die Art. 29-Gruppe ist in diesem Zusammenhang für die Industrie der wichtigste europäische Ansprechpartner für Datenschutzfragen.

Vor diesem Hintergrund habe ich, wenige Wochen nach meinem Amtsantritt, gern den Vorsitz der Art. 29-Gruppe für zwei Jahre übernommen. Die Übernahme dieser Funktion ist mit großen Möglichkeiten, einer hohen Verantwortung, aber auch mit erheblichen Belastungen verbunden, sowohl für den Amtsträger, als auch für die Dienststelle. Als Vorsitzender muss ich nicht nur die z. T. unterschiedlichen Vorstellungen der jetzt 25 Mitgliedstaaten zusammenführen, sondern auch programmatisch-strategische Akzente setzen und den Europäischen Datenschutz innerhalb und außerhalb der Europäischen Union vertreten. Nach meinem ersten Amtsjahr ist festzustellen, dass sich der Anteil der Europäischen Angelegenheiten am Geschäft der Dienststelle sowohl qualitativ als auch quantitativ erheblich ausgeweitet hat.

3.2 Schwerpunkte der europäischen Datenschutzdiskussion

3.2.1 Die Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie

Die Harmonisierung des europäischen Datenschutzes soll durch eine europaweit abgestimmte Kontrollstrategie vorangetrieben werden.

Die Europäischen Datenschutzbeauftragten, die in Brüssel im Rahmen des Artikel 29 der EG-Datenschutzrichtlinie zusammenarbeiten, haben mich am 11. Februar 2004 einstimmig zu ihrem neuen Vorsitzenden gewählt. Zu meinem Vertreter bestimmte die Gruppe den Leiter der Spanischen Datenschutzbehörde, Prof. José Luis Piñar Manas. Neben den Datenschutzbeauftragten der Mitgliedstaaten der EU gehören der Europäische Datenschutzbeauftragte (vgl. Nr. 3.2.3) als Mitglied der Art. 29-Gruppe an sowie als nichtstimmberechtigtes Mitglied die Europäische Kommission.

Auch im Berichtszeitraum hat sich die Gruppe mit einer weitgespannten Palette von Themen auseinandergesetzt, 30 Stellungnahmen wurden verabschiedet (vgl. Anlage 12). Ein Schwerpunkt war die Übermittlung von Passagierdaten in die USA (vgl. Nr. 22.2), nach Kanada und nach Australien. Auch hat sich die Gruppe intensiv mit der Verarbeitung von biometrischen und genetischen Daten für Zwecke der inneren Sicherheit und Strafverfolgung auseinandergesetzt. Die Verarbeitung von Kommunikationsdaten, eGovernment und Videoüberwachung standen ebenso auf der Tagesordnung wie Spam (vgl. Nr. 13.8) und Online-Authentifizierungssysteme.

Eine wesentliche Aufgabe der Gruppe neben der Beratung der Kommission ist es, die Harmonisierung des Datenschutzes innerhalb der Europäischen Union voranzutreiben. So wurde zum Beispiel eine Stellungnahme zu den Informationspflichten der Datenverarbeiter verabschiedet, eine weitere gibt konkrete Hinweise, wie Fluggäste in die USA über ihre Rechte zu unterrichten sind.

Auch hat sich die Art. 29-Gruppe in einem Arbeitspapier darauf verständigt, zukünftig durch konzentrierte Kontrollen die Einhaltung datenschutzrechtlicher Bestimmungen in bestimmten Bereichen gezielt besser durchzusetzen. So sollen etwa Sektoren überprüft werden, wo besonders sensible personenbezogene Daten verarbeitet werden oder wo besonders häufig Beschwerden anfallen. Solche europaweit durchgeführten Untersuchungen haben auch das Ziel, die Kenntnisse der verantwortlichen Stellen über einzuhaltende Bestimmungen zu verbessern und die Betroffenen über ihre Rechte aufzuklären. Durch die Koordination der Kontrollen kann die Harmonisierung nicht nur bei der Anwendung des nationalen Rechts, sondern auch bei der Ahndung von Verstößen voraussichtlich deutlich verbessert werden.

Herausragendes Ereignis im Berichtszeitraum war die Aufnahme von zehn neuen Mitgliedstaaten zum 1. Mai 2004. Vor diesem Datum hatten die neuen Mitglieder bereits die Möglichkeit, als Beobachter an den Sitzungen der Art. 29-Gruppe teilzunehmen. Die Erweiterung war Anlass, das Selbstverständnis der Gruppe zu klären. In einem Strategiepapier wurden die künftigen Arbeitsschwerpunkte festgelegt und das Verhältnis der Gruppe zu den unterschiedlichen Ansprechpartnern in der Gesellschaft beschrieben. Ziel des Strategiepapiers ist es nicht zuletzt, die Arbeit der Gruppe transparenter zu machen und alle am Datenschutz interessierten Parteien zum Dialog einzuladen (Dok. 11648/04 vom 29. September 2004, WP 98; vgl. Anlage 12).

Die Gruppe trifft sich in der Regel fünf Mal pro Jahr in Brüssel zu zweitägigen Sitzungen und wird in ihrer Arbeit durch Untergruppen unterstützt. Im Berichtszeitraum waren Untergruppen zu den Themenbereichen Internet, Passagierdaten und verbindlichen Unternehmensrichtlinien aktiv.

Kasten zu Nr. 2.7

Aus dem Entwurf des Informationsfreiheitsgesetzes (Bundestagsdrucksache 15/4493)

§ 1 Grundsatz

(1) Jeder hat nach Maßgabe dieses Gesetzes gegenüber den Behörden des Bundes einen Anspruch auf Zugang zu amtlichen Informationen, ohne ein rechtliches Interesse darlegen zu müssen. Für sonstige Bundesorgane und -einrichtungen gilt dieses Gesetz, soweit sie öffentlich-rechtliche Verwaltungsaufgaben wahrnehmen. Einer Behörde im Sinne dieser Vorschrift steht eine natürliche Person oder juristische Person des Privatrechts gleich, soweit eine Behörde sich dieser Person zur Erfüllung ihrer öffentlich-rechtlichen Aufgaben bedient.

(2) Die Behörde kann Auskunft erteilen, Akteneinsicht gewähren oder Informationen in sonstiger Weise zur Verfügung stellen. Begehrt der Antragsteller eine bestimmte Art des Informationszugangs, so darf dieser nur aus wichtigem Grund auf andere Art gewährt werden. Als wichtiger Grund gilt insbesondere ein deutlich höherer Verwaltungsaufwand.

(3) Regelungen in anderen Rechtsvorschriften über den Zugang zu amtlichen Informationen gehen mit Ausnahme des § 29 des Verwaltungsverfahrensgesetzes und des § 25 des Zehnten Buches des Sozialgesetzbuchs vor.

§ 5 Schutz personenbezogener Daten

(1) Zugang zu personenbezogenen Daten darf nur gewährt werden, soweit das Informationsinteresse des Antragstellers das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs überwiegt oder der Dritte eingewilligt hat. Besondere Arten personenbezogener Daten im Sinne des § 3 Abs. 9 des Bundesdatenschutzgesetzes dürfen nur übermittelt werden, wenn der Dritte ausdrücklich eingewilligt hat.

(2) Das Informationsinteresse des Antragstellers überwiegt nicht bei Informationen aus Unterlagen, soweit sie mit dem Dienstverhältnis des Dritten in Zusammenhang stehen, insbesondere aus Personalakten, und bei Informationen, die einem Berufs- oder besonderen Amtsgeheimnis unterliegen.

(3) Das Informationsinteresse des Antragstellers überwiegt das schutzwürdige Interesse des Dritten am Ausschluss des Informationszugangs in der Regel dann, wenn sich die Angaben auf Name, Titel, akademischen Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und -telekommunikationsnummer beschränkt und der Dritte als Gutachter, Sachverständiger oder in vergleichbarer Weise eine Stellungnahme in einem Verfahren abgegeben hat.

(4) Name, Titel, akademischer Grad, Berufs- und Funktionsbezeichnung, Büroanschrift und -telekommunikationsnummer von Bearbeitern sind vom Informationszugang nicht ausgeschlossen, soweit sie Ausdruck und Folge der amtlichen Tätigkeit sind und kein Ausnahmetatbestand erfüllt ist.

3.2.2 Die Umsetzung der Datenschutzrichtlinie 95/46/EG in den Mitgliedstaaten der Europäischen Union

3.2.2.1 Bericht der Europäischen Kommission

Der Bericht der EU-Kommission zur Umsetzung der EG-Datenschutzrichtlinie gibt derzeit keinen Grund zur Änderung der Richtlinie.

Der dem Europäischen Parlament vorgelegte Kommissionsbericht vom 15. Mai 2003 über die Durchführung der Datenschutzrichtlinie (EG 95/46, KOM(2003) 265 endgültig) war längst überfällig, hätte er doch bereits drei Jahre nach Verabschiedung der Richtlinie erstellt werden müssen. Mitschuld an der Verspätung hatten einzelne Mitgliedstaaten, die die Richtlinie nur zögerlich und zum Teil erst im Jahre 2004 vollständig umsetzten.

Die Richtlinie verfolgt zwei Ziele, zum einen die Vollendung des Binnenmarktes und zum anderen die Gewährleistung des Schutzes von Grundrechten und Grundfreiheiten des Einzelnen in allen Mitgliedstaaten. Mit Befriedigung stellte die Kommission fest, dass es gelungen sei, in allen Mitgliedstaaten ein hohes Datenschutzniveau zu erreichen. Dem freien Verkehr von personenbezogenen Daten in der EU stünden keine Schranken mehr im Wege. Bei der Umsetzung der Richtlinie hätten die Mitgliedstaaten einen großen Freiraum gehabt, der es erlaubte, gewachsene Datenschutztraditionen zu berücksichtigen. Die daraus resultierenden Unterschiede bei der Umsetzung der Richtlinie hätten sich als beträchtlich erwiesen. Die Kommission stellte insbesondere fest, dass sich die Industrie über zu große Divergenzen innerhalb der EU beklagt; sie könne deshalb keine gesamteuropäische Datenschutzstrategie entwickeln.

Unterschiedliche Interpretationen der Richtlinie sind z. B. bei den Begriffsbestimmungen, bei der Interpretation so genannter sensibler Daten, bei der Information der Betroffenen und bei der Übermittlung von Daten in Drittländer festgestellt worden. Zwar stellen diese Abweichungen nicht notwendigerweise Verletzungen des Gemeinschaftsrechts dar; gleichwohl stören sie die Harmonisierung und erfordern daher Abhilfe.

Einige der festgestellten Mängel beruhen auf unzureichenden finanziellen und personellen Ressourcen für die Durchsetzung der Richtlinie, andere liegen in der lückenhaften Befolgung der Vorschriften durch die für die Verarbeitung Verantwortlichen; diese müssten vielfach kaum fürchten, für ihr Verhalten geahndet zu werden. Nicht zuletzt wurde auch ein sehr geringer Kenntnisstand bei den Betroffenen hinsichtlich ihrer Rechte festgestellt.

Die Bestimmungen der Richtlinie zum Auskunftsrecht der Betroffenen werden in den einzelnen Ländern unterschiedlich ausgelegt. Um dem abzuhelfen, hat die Art. 29-Gruppe eine Stellungnahme verabschiedet, die die offenen Fragen durch Muster-Informationstexte klärt (vgl. Anlage 12, WP 100).

Weitere Unterschiede bestehen in der Behandlung von Text-, Ton- und Bilddaten in den Mitgliedstaaten. Auch hier hat die Art. 29-Gruppe ein Grundsatzpapier verabschiedet, das diesem Mangel abhelfen soll (vgl. Anlage 12, WP 89).

Große Abweichungen in den einzelnen Staaten offenbarten sich nach dem Kommissionsbericht auch bei der Praxis des Datentransfers in Drittstaaten. So ist z. B. die in einigen Ländern praktizierte Regelung, alle Übermittlungen in Drittstaaten von der Genehmigung der zuständigen Aufsichtsbehörde abhängig zu machen, unvereinbar mit der Richtlinie. Zwar können die Behörden die Meldungen solcher Übermittlungen verlangen, diese aber nicht in De-Facto-Genehmigungen umwandeln. Vereinfachungen bei der Genehmigung von Drittstaatentransfers sind in der Tat dringend erforderlich. Wünschenswert wäre auch der verbreitete Gebrauch von Gruppengenehmigungen auf der Basis von konzerninternen verbindlichen Unternehmensregelungen, um so den Datentransfer in Länder zu erleichtern, die kein angemessenes Datenschutzniveau garantieren. Hier sieht die Kommission ein wichtiges Betätigungsfeld für die nationalen Datenschutzbehörden. Auch die Art. 29-Gruppe arbeitet daher an der Erleichterung der Verfahren zur Genehmigung solcher konzerninterner Regelungen.

Um den aufgezeigten Mängeln abzuhelfen, hat die Kommission ein weit gefächertes Aktionsprogramm beschlossen, das z. B. Erörterungen mit den einzelnen Mitgliedstaaten und bessere Informationen auf der Internetseite der Kommission vorsieht. Weiterhin setzt sie sich für die Förderung von Technologien zur Verbesserung des Datenschutzes, sog. Privacy Enhancing Technologies, ein (vgl. Anlage 12, WP 86; Anlage 9). Zudem fordert sie die Mitgliedstaaten auf, die Öffentlichkeit stärker für die Belange des Datenschutzes zu sensibilisieren. Insbesondere setzt die Kommission aber auf die Art. 29-Gruppe. Mit ihrer Hilfe soll die Harmonisierung auf der praktischen Ebene vorangetrieben werden. Die Erwartungen an die Datenschutzbehörden der Mitgliedstaaten sind dabei erheblich; vielfach sollen sie Einigkeit dort herstellen, wo dies dem europäischen Gesetzgeber bei der Abfassung der Richtlinie nicht oder nur in Form von Formelkompromissen gelungen ist. Das Festhalten an überlieferten nationalen Rechtsfiguren und gewachsenen Verwaltungspraktiken ist in vielen Mitgliedstaaten aber nach wie vor stark. Dennoch hat die Art. 29-Gruppe das Aktionsprogramm der Kommission als Zielvorstellung akzeptiert und arbeitet intensiv an seiner Umsetzung. Allen Beteiligten ist klar, dass ohne Harmonisierungsfortschritte auf der praktischen Ebene eine Änderung der Richtlinie nicht zu vermeiden wäre.

3.2.2.2 Bedeutende Entscheidungen des Europäischen Gerichtshofs

Der Gerichtshof der Europäischen Gemeinschaft (EuGH) hat festgestellt, dass die EG-Datenschutzrichtlinie auch auf Sachverhalte ohne Binnenmarktbezug anzuwenden ist.

Der EuGH hatte erstmals Gelegenheit, auf Fragen von nationalen Gerichten aus Österreich und Schweden zur Auslegung und zum Anwendungsbereich der Richtlinie Stellung zu nehmen. Im österreichischen Fall (Urteil „Österreichischer Rundfunk“ vom 20. Mai 2003 C-465/00) ging es um die Zulässigkeit der nach nationalem Recht vorgeschriebenen Weitergabe der Besoldungshöhe bestimmter, bei öffentlichen Stellen beschäftigter Personen an den Rechnungshof, der diese Daten personenbezogen in einem Bericht an das Parlament übermitteln wollte. Im schwedischen Fall (Urteil „Lindqvist“ vom 6. November 2003 C 101-01) spielte die Veröffentlichung von Namen und weiteren personenbezogenen Informationen aus der kirchlichen Gemeindearbeit im Internet durch eine Einzelperson eine Rolle.

Die Annahme einer sog. Mindestharmonisierung hält der EuGH für nicht mit der in der Richtlinie enthaltenen vollständigen Harmonisierung vereinbar. Deren Zielsetzung, die Unterschiede in den nationalen Regelungen und damit die vor der Harmonisierung bestehenden Hindernisse für den Binnenmarkt abzubauen, habe die zwingende Folge, dass die Mitgliedstaaten nach erfolgter Harmonisierung nicht mehr von dem gemeinsam beschlossenen Rahmen abweichen können. Der Gerichtshof macht deutlich, dass die Anwendung der Richtlinie die Regel ist, während ihre Nichtanwendung die Ausnahme bildet, die nach den allgemeinen Grundsätzen des Gemeinschaftsrechts eng auszulegen ist. Ausgenommen sind daher allein die ausdrücklich in Artikel 3 Abs. 2 der Richtlinie genannten Bereiche der Gemeinsamen Außen- und Sicherheitspolitik sowie der polizeilichen und justiziellen Zusammenarbeit in Strafsachen. Die verbreitete Auffassung, dass nur Sachverhalte mit Binnenmarktbezug unter die Richtlinie fallen, wies der EuGH zurück.

3.2.3 Bestellung des Europäischen Datenschutzbeauftragten erfolgt

Die Berufung eines Europäischen Datenschutzbeauftragten bringt den Datenschutz in der Europäischen Union voran.

Der Vorsitzende der Niederländischen Datenschutzkommission Peter J. Hustinx wurde am 22. Dezember 2003 vom Europäischen Parlament und dem Rat der Europäischen Union für eine Amtszeit von fünf Jahren zum ersten Europäischen Datenschutzbeauftragten gewählt und hat sein neues Amt im Januar 2004 angetreten. Zu seinem Stellvertreter ebenfalls mit einer Amtszeit von fünf Jahren wurde der Spanier Joaquín Bayo Delgado ernannt.

Der Europäische Datenschutzbeauftragte arbeitet als gleichberechtigtes Mitglied in der Art. 29-Gruppe mit. Er – wie auch sein Stellvertreter – übt sein Amt in völliger Unabhängigkeit aus und nimmt keine Weisungen entgegen. Sein Dienstsitz ist Brüssel. Er hat dem Europäischen Parlament, dem Rat und der Kommission jährlich einen Tätigkeitsbericht vorzulegen. Für die Bediensteten seiner Dienststelle gilt das Statut der Beamten und anderer Bedienstete der Europäischen Gemeinschaften. Er ist im Internet unter www.edps.eu.int. präsent.

Kasten zu Nr. 3.2.3

Zu den wichtigsten **Aufgaben des europäischen Datenschutzbeauftragten** gehört die Kontrolle der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft. Ferner berät er diese Organe und Einrichtungen in allen Fragen, die die Verarbeitung personenbezogener Daten betreffen. Er hat zudem relevante Entwicklungen, sofern sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere bei der Entwicklung- und Kommunikationstechnologie zu überwachen. Zudem ist er sowohl für Beschwerden von Angehörigen der EU-Institutionen als auch von Bürgern der Europäischen Union, die sich durch die Behandlung ihrer persönlichen Daten durch die Organe und Einrichtungen der EU in ihren Rechten beeinträchtigt fühlen, zuständig. Es bleibt jedoch den nationalen Aufsichtsbehörden vorbehalten, Beschwerden von Bürgern der EU über die Verarbeitung ihrer Daten in den Mitgliedstaaten nachzugehen.

Die genaue Tätigkeitsbeschreibung des Europäischen Datenschutzbeauftragten wurde im Amtsblatt der Europäischen Gemeinschaft (ABL C 224 A vom 20. September 2004) veröffentlicht.

3.2.4 Safe-Harbor-Review

Die Europäische Kommission stellte Mängel bei der Durchführung des Safe-Harbor-Arrangements fest. Eine Überprüfung der Auswirkungen der in der Folge der Ereignisse des 11. September 2001 in den USA erlassenen Gesetze auf Safe Harbor steht noch aus.

Die von den Vereinigten Staaten von Amerika (zu den USA vgl. Nr. 27.2) initiierte Sondervereinbarung mit der Europäischen Union zur Sicherstellung eines angemessenen Schutzniveaus für Datenübermittlungen aus der EU in die USA („Safe Harbor“) war nach der Entscheidung der Europäischen Kommission vom 26. Juli 2000 zum 1. November desselben Jahres in Kraft getreten (vgl. 18. TB Nr. 2.2.2, zur Funktionsweise von Safe Harbor vgl. Kasten zu Nr. 3.2.4). Zuvor hatte das Europäische Parlament (EP) mit seiner Entschließung vom 5. Juli 2000 die Mitgliedstaaten und die Kommission aufgefordert, eine zu treffende Entscheidung „im Lichte der Erfahrungen und möglicher künftiger rechtlicher Entwicklungen unverzüglich zu überprüfen“, weshalb in die Kommissionsentscheidung – zur Genugtuung der Art. 29-Gruppe (vgl. Nr. 3.2.1) – mit Artikel 4 Abs. 1 eine entsprechende Überprüfungsklausel eingefügt worden war. Eine erste bewertende Bestandsaufnahme des Safe-Harbor-Arrangements durch die Kommission Anfang 2002 hatte vor allem Resonanzprobleme innerhalb der amerikanischen Wirtschaft und verbreitete Defizite bei der Transparenz festgestellt (vgl. 19. TB Nr. 3.7).

Kasten zu Nr. 3.2.4

Funktionsweise von Safe Harbor

Durchführung in den USA

Online-Selbstzertifizierungsverfahren des US-Handelsministeriums für amerikanische Unternehmen/Organisationen

- Beitritt freiwillig, danach Grundsätze verbindlich
- Liste der beigetretenen Unternehmen/Organisationen http://www.export.gov/safeharbor

Gremien zur Streitbeilegung

- Nicht-staatliche unabhängige Schiedsstellen mit Sanktionsbefugnissen:

  BBBOnline

  TRUSTe

  Direct Marketing Association Safe Harbour Program

  Entertainment Software Rating Board Privacy Online EU Safe Harbour Programme

  Judicial Arbitration and Mediation Service (JAMS)

  American Arbitration Association

- Alternativ: Meldung an Federal Trade Commission, die Geldstrafen und Unterlassungsanordnungen aussprechen kann
- Alternativ: Zusammenarbeit mit dem Beschwerdepanel der EU-Datenschutzbehörden

Umsetzung in Europa

Veröffentlichung aller Dokumente in den Amtssprachen der Gemeinschaft http://www.europa.eu.int/comm/privacy

Einrichtung eines Beschwerdepanels

- Fragen und Antworten http://www.europa.eu.int/comm/internal_market/de/dataprot/news/datatransf.htm
- Beratung fernmündlich oder über die Mailbox der Generaldirektion Binnenmarkt (Markt-A4@cec.eu.int)

Um der Forderung des EP nachzukommen, spätestens drei Jahre nach Inkrafttreten der Safe-Harbor-Vereinbarung eine Überprüfung durchzuführen, erteilte die Kommission im Herbst 2003 einem internationalen Team von Fachleuten aus verschiedenen Ländern den Auftrag zu einer Studie mit dem Ziel, den Zeitraum zwischen dem 1. November 2000 und dem 1. November 2003 zur Vorbereitung einer „Safe-Harbor-Review“ zu begutachten. Am 19. April 2004 wurde der Kommission die umfangreiche, einschließlich Anhängen fast 300 Seiten starke Safe Harbor Decision Implementation Study vorgelegt, auf die die Kommission – neben ihren eigenen Erfahrungen und Recherchen – ihre Beurteilung stützt. Diese präsentierte sie zum 20. Oktober 2004 mit dem Commission Staff Working Document – The implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbour privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce (Dok. SEC (2004) 1323).

In ihrer Überprüfungsstudie gelangt die Kommission im wesentlichen zu folgenden Ergebnissen:

- Wenngleich die Teilnahme seitens der amerikanischen Unternehmen am Safe-Harbor-Programm insgesamt recht gering ist, ist dennoch ein stetiger Anstieg zu verzeichnen. Von knapp 300 Unternehmen in 2002 und 400 in 2003, waren es bei Redaktionsschluss über 600.
- Zahlreiche der durch Selbstregulierung dem Safe-Harbor-Programm beigetretenen Unternehmen besitzen entweder keine privacy policy, die den Voraussetzungen von Safe Harbor entspricht, oder es mangelt überhaupt an einer solchen. Dies veranlasst die Kommission zu einer Reihe von Vorschlägen an das amerikanische Wirtschaftsministerium und an die Federal Trade Commission (FTC). Da die interessierten Unternehmen sich ohne weitere Nachprüfung durch Selbstzertifizierung in das Programm eintragen können, werden Ministerium und FTC zu einer proaktiven Überprüfung aufgefordert, die die Teilnehmer mit einer mangelhaften privacy policy rechtzeitig erkennen und ausschließen kann.
- Zwar kann bis dato als positiv bewertet werden, dass noch keine Beschwerdefälle bekannt geworden sind, die nicht von den davon berührten Unternehmen zur Zufriedenheit der Betroffenen beigelegt wurden (vgl. schon 19. TB Nr. 3.7). Allerdings haben sich bisher weder Unternehmen noch Betroffene an das EU Panel gewandt.

Eine wichtige Aufgabe wird darin liegen, die Auswirkungen des US Patriot Act und anderer Gesetze, die die Vereinigten Staaten im Gefolge der Ereignisse des 11. September 2001 erlassen haben, auf das Funktionieren des Safe-Harbor-Arrangements zu untersuchen und zu überprüfen, ob sie die Angemessenheit des Datenschutzniveaus tangieren.

Die Safe Harbor Decision Implementation Study ist auf der Website der Kommission verfügbar unter http://europa.eu.int/comm/internal_market/privacy/index_en.htm.

3.2.5 Datenschutz im Europarat

Das Datenschutzübereinkommen des Europarats wurde inzwischen von 25 Staaten ratifiziert.

Mit der Aufnahme von Monaco und von Serbien/Montenegro ist die Zahl der Mitglieder des Europarates auf 46 angewachsen. Mittlerweile sind 25 Staaten dem „Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten“ – der Europaratskonvention 108 – aus dem Jahre 1981 beigetreten.

Ein Zusatzprotokoll zur Europaratskonvention verpflichtet die Vertragsparteien, die Anwendungsmöglichkeiten der in der Konvention enthaltenen Grundsätze durch zwei substantiell neue Mechanismen zu verbessern. Zum einen sind die Partnerstaaten des Übereinkommens gehalten, völlig unabhängige Kontrollstellen mit Untersuchungs- und Einwirkungsbefugnissen sowie Klagerecht beziehungsweise Anzeigebefugnis einzurichten. Zum anderen wurden nach dem Vorbild der EG-Datenschutzrichtlinie Regelungen über den grenzüberschreitenden Datenverkehr mit Nicht-Vertragsstaaten eingeführt. Nachdem die Ratifikationsgesetze in Deutschland (BGBl. II 2000 S. 1882) und fünf weiteren Staaten zeitgleich zum 1. Juli 2004 in Kraft traten und damit das Quorum von mindestens fünf Ratifizierungen erreicht worden war, ist auch das Zusatzprotokoll selbst seit diesem Datum in Kraft gesetzt.

Die Konvention und die dazu ergangenen Empfehlungen und Berichte sind – in Englisch und Französisch – abrufbar über http://www.coe.int/T/E/Legal_affairs/Legal_cooperation/Data_protection/.

3.2.6 Konferenz der Datenschutzbeauftragten der Europäischen Union

Die Europäische Datenschutzkonferenz befasste sich vor allem mit Überlegungen für eine vertiefte Zusammenarbeit der europäischen Datenschutzbehörden sowie mit Fragen des Datenexports in Drittländer.

Die Frühjahrskonferenz der europäischen Datenschutzbehörden vom 2. bis 4. April 2003 in Sevilla behandelte schwerpunktmäßig aktuelle Probleme des grenzüberschreitenden Datenverkehrs in Drittstaaten außerhalb der EU und setzte sich mit dem Selbstverständnis der Datenschutzbehörden – nicht zuletzt vor dem Hintergrund der Erfahrungen nach den Terroranschlägen in den USA vom 11. September 2001 – auseinander. Der Stand der Umsetzung der europäischen Datenschutzrichtlinie 95/46/EG (vgl. Nr. 3.2.2) beschäftigte die Teilnehmer ebenso wie die Umsetzung der Telekommunikationsrichtlinie 2002/58/EG, wozu ich gemeinsam mit meinem Berliner Kollegen die Erfahrungen aus deutscher Sicht (vgl. Nr. 13.1) vorgetragen habe. Wichtige Einblicke in den Stand der Rechtsentwicklung der inzwischen zum 1. Mai 2004 in die EU aufgenommenen neuen Mitgliedstaaten erfuhr die Konferenz von den Datenschutzbeauftragten mehrerer Beitrittsländer.

Auch die Frühjahrskonferenz vom 21. bis 23. April 2004 in Rotterdam befasste sich eingehend mit der Rolle der Datenschutzbehörden, wobei Fragen der inneren Organisation, der Optimierung der Verfahrensabläufe und einer allgemeinen Effektivitätssteigerung im Hinblick auf den Schutz der Datenschutzposition des Bürgers im Vordergrund standen. Daneben stand zur Diskussion, wie die europäische Zusammenarbeit – über das von der Datenschutzrichtlinie geschaffene Gremium der Art. 29-Gruppe (vgl. Nr. 3.2.1) und die von der Richtlinie vorgesehene europäische Amtshilfe nach Artikel 28 Abs. 6 hinaus – vertieft werden kann. Diese Überlegungen mündeten in eine – anlässlich der Internationalen Datenschutzkonferenz von Breslau am 14. September 2004 (vgl. Nr. 27.3) angenommene – von mir eingebrachte „Entschließung der Europäischen Datenschutzkonferenz zur Schaffung eines gemeinsamen Gremiums zur Beratung der Organe der Europäischen Union auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit (Datenschutz in der Dritten Säule)“ (vgl. Kasten zu Nr. 3.2.6).

Kasten zu Nr. 3.2.6

Europäische Datenschutzkonferenz, Breslau, 14. September 2004

Entschließung

eingereicht vom Bundesbeauftragten für den Datenschutz, Deutschland, und befürwortet von der Niederländischen Datenschutzbehörde

Entschließung der Europäischen Datenschutzkonferenz zur Schaffung eines gemeinsamen Gremiums zur Beratung der Organe der Europäischen Union auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit (Datenschutz der Dritten Säule)

Der Vertrag über die Europäische Union (EUV) in der Fassung vom 2. Oktober 1997 (Vertrag von Amsterdam) enthält in Titel VI umfassende Bestimmungen über die polizeiliche und justizielle Zusammenarbeit in Strafsachen. Nach dem Vertrag von Nizza soll zudem die Zusammenarbeit der Polizei- und Justizbehörden der EU-Mitgliedstaaten noch weiter intensiviert werden. Dies zählt zu den vordringlichen Aufgaben der Union.

Die Datenschutzbeauftragten der Mitgliedstaaten der Europäischen Union verkennen nicht die Notwendigkeit einer engeren Zusammenarbeit der Strafverfolgungsbehörden der Mitgliedstaaten mit dem Ziel, den Bürgern der Union ein hohes Maß an Sicherheit in einem Raum der Freiheit, der Sicherheit und des Rechts zu gewährleisten. Dennoch ist es erforderlich, einen Mittelweg zu finden zwischen diesem Bedürfnis und der Aufrechterhaltung bürgerlicher Freiheitsrechte, einschließlich durch die Charta der Grundrechte der Europäischen Union geschützten Datenschutzrechte.

Es gehört zu den wichtigsten Aufgaben der Datenschutzbeauftragten, die an der Gesetzgebung beteiligten Organe in allen Fragen des Datenschutzes zu beraten, dabei insbesondere auf Risiken für die oben erwähnten Freiheitsrechte hinzuweisen und bürgerfreundliche Lösungen vorzuschlagen. Diese Beratung wird von der Kommission, dem Rat und dem Europäischen Parlament mehr und mehr in Anspruch genommen.

Die Datenschutzbeauftragten kommen dieser Nachfrage selbstverständlich nach bestem Vermögen nach. Sie müssen allerdings darauf hinweisen, dass bisher die organisatorischen Voraussetzungen für die Erfüllung dieser wichtigen Aufgaben fehlen und deshalb eine zeitnahe und europäisch abgestimmte Beratung auf dem gebotenen hohen Qualitätsniveau nicht gesichert ist. Während nämlich die Datenschutzbeauftragten für den Bereich des Binnenmarktes (Erste Säule) mit der Arbeitsgruppe nach Artikel 29 der Richtlinie 95/46/EG einen geeigneten organisatorischen Rahmen besitzen, der ein (von der Kommission gestelltes) ständiges Sekretariat umfasst und regelmäßige Sitzungen in Brüssel – mit dem erforderlichen Sprachendienst – erlaubt, fehlen diese Voraussetzungen im Bereich der Dritten Säule vollständig. Die im Bereich der Dritten Säule bestehenden gemeinsamen Kontrollinstanzen (z. B. Europol, Schengen, Eurojust) sind hierfür wegen ihrer eng begrenzten und speziellen Aufgabenstellung nicht geeignet, da zur Sicherung eines einheitlichen Datenschutzstandards für den gesamten Bereich der polizeilichen und justiziellen Zusammenarbeit ein übergeordneter Ansatz erforderlich ist.

Zur Zeit sind die Teilnehmer der Konferenz dabei, ihre Zusammenarbeit in polizeilichen und justiziellen Angelegenheiten zu vertiefen. Deshalb wurde von der Konferenz der Europäischen Datenschutzbehörden eine Polizeiarbeitsgruppe eingesetzt, die Richtlinien für die Arbeit setzen soll. Sie untersucht Fälle, die außerhalb des Aufgabengebietes der existierenden Datenschutzbehörden auf EU-Ebene liegen. Außerdem wurde eine weitere Untergruppe der Konferenz gegründet. Dieser Planungsgruppe, die sich unter anderem aus den Vorsitzenden der gemeinsamen Aufsichtsbehörden zusammensetzt (von Europol, Schengen, Zoll und Eurojust), dem Vorsitzenden der Arbeitsgruppe nach Artikel 29 sowie dem Europäischen Datenschutzbeauftragten, obliegt die Entwicklung strategischer Ansätze bei neuen Initiativen. Diese sollen sowohl die Verwendung von persönlichen Daten in der Strafverfolgung als auch den europäischen Aspekt beinhalten.

Dennoch sind zusätzliche strukturelle Maßnahmen notwendig. Angesichts des forcierten Ausbaus der Europäischen Sicherheitsarchitektur in der Dritten Säule ist die institutionelle Sicherung einer geregelten Datenschutzberatung durch den Europarat von höchster Priorität. Die Konferenz der Europäischen Datenschutzbeauftragten fordert deshalb den Rat auf, die notwendigen personellen und organisatorischen Maßnahmen umgehend zu ergreifen, damit das Datenschutzgremium noch in diesem Jahr seine wichtige Arbeit im Interesse der Bürger aufnehmen kann. Der Europäische Datenschutzbeauftragte nach Art. 286 Abs. 2 des EG-Vertrages sollte in dem zu schaffenden Gremium mitwirken.

Die Konferenz fordert den Rat und die Kommission ebenfalls dazu auf, die rechtlichen Bedingungen für die Harmonisierung der Datenschutzkontrolle innerhalb der Dritten Säule zu schaffen, und zwar in enger Zusammenarbeit mit den zuständigen Organisationen.

Der Vorsitzende wird angewiesen, diese Entschließung dem Rat, der Kommission sowie dem Parlament zu übermitteln.

Breslau, den 14. September 2004

3.3 Intensivierung der polizeilichen Zusammenarbeit in Europa

3.3.1 Europol

3.3.1.1 Änderung des Europol-Übereinkommens

Die dänische Initiative zur Änderung des Europol-Übereinkommens ist noch nicht in Kraft getreten.

In meinem 19. TB (Nr. 16.1) berichtete ich über eine Initiative Dänemarks für einen Rechtsakt des Rates zur Erstellung eines Protokolls zur Änderung des Europol-Übereinkommens. Der Gemeinsamen Kontrollinstanz (GKI) liegen aus ihrer Beratungs- und Kontrolltätigkeit Erkenntnisse vor, wie wichtig eine solche Rechtsanpassung für die weiteren Aktivitäten von Europol wäre. Gleichwohl gibt es bisher nur eine politische Grundsatzentscheidung des Rates über die Annahme der dänischen Initiative, die jedoch wegen nationaler Parlamentsvorbehalte noch nicht in Kraft treten konnte. Auch das BMI hat bisher nur einen Entwurf für ein Vertragsgesetz ausgearbeitet.

3.3.1.2 Aktivitäten der Gemeinsamen Kontrollinstanz von Europol

Der erste Tätigkeitsbericht der GKI für den Zeitraum Oktober 1998 bis Oktober 2002 wurde inzwischen veröffentlicht.

War die Tätigkeit der GKI in der Anlaufphase seit 1999 eher von der Prüfung von Anwendungs- und Auslegungsfragen geprägt, so tritt inzwischen immer stärker die Kontrolltätigkeit in den Vordergrund. So hat die GKI mehrere Kontrollbesuche bei Europol durchgeführt, an denen auch Vertreter meiner Dienststelle beteiligt waren. Bei den ersten Kontrollbesuchen stand noch die Beratung und Unterstützung beim Aufbau der Informations- und Kommunikationsstruktur bei Europol im Vordergrund. Es geht hier um ein komplexes System, denn Europol soll neben der hauseigenen Analysetätigkeit (vgl. Artikel 10 der Konvention) für die Mitgliedsstaaten insbesondere ein Europäisches Informationssystem (EIS) gem. Artikel 8 der Konvention betreiben. Mit der Intensivierung der Fallanalyse bei Europol wird die Prüftätigkeit der GKI zunehmend auf diesen Bereich ausgeweitet. Als Ergebnis lässt sich festhalten, dass die Mitgliedstaaten zwar in wachsendem Maße Datenmaterial für Analysezwecke an Europol liefern, dies jedoch vielfach ohne die notwendige Vorabbewertung seitens der anliefernden nationalen Stellen erfolgt. Es gehört aber zum Wesen einer effizienten Analyse, dass die zu untersuchenden Informationen und deren Quellen vorab auf Authentizität, Verlässlichkeit usw. untersucht werden. Dadurch soll vermieden werden, dass Datenfriedhöfe ohne wesentlichen Nutzwert entstehen.

Mit dem Beitritt von zehn neuen EU-Mitgliedstaaten zum 1. Mai 2004 werden diese auch Vertragsparteien von Europol, sobald sie die Europol-Konvention ratifiziert haben. Da ein angemessener Datenschutz im Polizeibereich Voraussetzung für den Beitritt zur Konvention ist (vgl. Artikel 14 der Konvention), hat die Kontrollinstanz sich zunächst mittels eines Fragebogens und anschließender Diskussion über den Stand des Datenschutzes in den neuen Mitgliedsstaaten unterrichten lassen. Inzwischen haben die meisten Mitgliedstaaten die Europol-Konvention ratifiziert. Die Erweiterung stellt neue Anforderungen an die Organisation der GKI, denn nunmehr nehmen bis zu 50 Vertreter an ihren Sitzungen teil.

Der Beschwerdeausschuss hat im Berichtszeitraum zwei weitere Verfahren rechtskräftig abgeschlossen (vgl. 19. TB Nr. 16.1). Von besonderer Bedeutung ist die Entscheidung, wonach Europol auf das Auskunftsersuchen eines Betroffenen nach Artikel 19 der Konvention in der Sprache antworten muss, die der Antragsteller verwendet hat, soweit es sich um eine der offiziellen EU-Amtssprachen handelt. Bis dato hatte Europol grundsätzlich seine Korrespondenz in englischer Sprache geführt, was für Petenten, die deren nicht mächtig waren, fast einem Ausschluss des Rechtsweges gleichkam.

Kasten zu Nr. 3.3.1.2

Zusammensetzung und Aufgaben der Gemeinsamen Kontrollinstanz von Europol

Die GKI tritt ca. fünf bis sechs Mal im Jahr zusammen und beschließt Stellungnahmen zu Errichtungsanordnungen (Art. 12 der Konvention) und zu Drittstaatsabkommen (Art. 18 der Konvention). Daneben wird in bilateralen Gesprächen mit der Leitung von Europol über bestimmte Problembereiche verhandelt.

Artikel 24 des Europol-Übereinkommens – Gemeinsame Kontrollinstanz

Absatz 1

Es wird eine unabhängige Gemeinsame Kontrollinstanz eingesetzt, deren Aufgabe darin besteht, nach Maßgabe dieses Übereinkommens die Tätigkeit von Europol daraufhin zu überprüfen, ob durch die Speicherung, die Verarbeitung und die Nutzung der bei Europol vorhandenen Daten die Rechte der Personen verletzt werden. Darüber hinaus kontrolliert die Gemeinsame Kontrollinstanz die Zulässigkeit der Übermittlung der von Europol stammenden Daten. Die Gemeinsame Kontrollinstanz setzt sich aus höchstens zwei Mitgliedern oder Vertretern jeder nationalen Kontrollinstanz zusammen; diese werden gegebenenfalls von Stellvertretern unterstützt und von jedem Mitgliedstaat für fünf Jahre ernannt. Sie bieten jede Gewähr für Unabhängigkeit und besitzen die nötige Befähigung. Jede Delegation hat bei Abstimmungen eine Stimme. Die Gemeinsame Kontrollinstanz benennt aus ihren Reihen einen Präsidenten. Bei der Wahrnehmung ihrer Aufgaben nehmen die Mitglieder der Gemeinsamen Kontrollinstanz von keiner Behörde Weisungen entgegen.

Website der GKI: http://europoljsb.ue.eu.int

3.3.2 Schengen

3.3.2.1 SIS II – Schengener Informationssystem weiterhin bloß Ausschreibungsdatei?

Wesentliche datenschutzrechtliche Fragen beim Ausbau des Schengener Informationssystems (SIS) im Zuge der Erweiterung der Europäischen Union sind noch ungeklärt.

Ein Beispiel für die offenbar weitgehend unkoordinierten Aktivitäten zur grenzüberschreitenden Vernetzung der Sicherheitsbehörden bildet die Fortentwicklung des SIS zu einem „Schengener Informationssystem der zweiten Stufe (SIS II – vgl. 19. TB Nr. 16.2.1).

Das ursprüngliche SIS hat eine Kapazität für maximal 18 Teilnehmerstaaten, die mit der geplanten teilweisen Einbeziehung Großbritanniens und Irlands sowie der Assoziierung der Schweiz im Jahr 2006 ausgeschöpft sein wird. Auch die seit 1. Mai 2004 der EU angehörenden zehn neuen Mitgliedstaaten sind gehalten, sich dem SIS

anzuschließen. Mit einem Beitritt von Rumänien und Bulgarien könnten in einigen Jahren 30 Länder gemeinsam das SIS betreiben, dessen derzeitige Kapazitäten dem nicht gewachsen wären.

Es geht jedoch nicht nur um eine kapazitätsmäßige Erweiterung dieser europaweiten polizeilichen Fahndungsdatei mit mehr als zwölf Millionen Datensätzen, sondern auch um eine technische Fortentwicklung des vor 15 Jahren entwickelten Systems. Zudem soll der bereits beschlossene Europäische Haftbefehl (vgl. Nr. 7.9.2) im SIS technisch integriert werden. Datenschutzrechtlich problematisch wäre die Umsetzung der von Polizeibehörden insbesondere nach dem 11. September 2001 erhobenen Forderungen nach neuen Funktionalitäten wie der Einführung biometrischer Merkmale und erweiterten Zugriffsrechten. Denn dann würde das System seinen Charakter als polizeiliche Ausschreibungsdatei, die dem anfragenden Polizeibeamten Treffer anzeigt, verändern und zu einem umfassenden polizeilichen Informationssystem werden, das wegen seiner komplexen Struktur von der Gemeinsamen Kontrollinstanz (GKI) und von den nationalen Datenschutzkontrollinstanzen nur unter Schwierigkeiten zu kontrollieren wäre. Hinzu käme noch die Frage nach der Verantwortung für eine solche europaweite Datenbank.

In einem ersten Schritt hat der Rat mit der Verordnung (EG) Nr. 871/2004 vom 29. April 2004 (ABl. EU-Nr. L 162 S. 29) u. a. die rechtlichen Voraussetzungen für einen Teilzugriff von Europol und der nationalen Mitglieder von Eurojust auf das SIS geschaffen. Die Verordnung kann jedoch wegen eines nationalen Parlamentsvorbehalts, der bei Redaktionsschluss noch bestand, nicht angewendet werden.

Die GKI hat sich – ebenso wie das Europäische Parlament – frühzeitig in die Vorarbeiten zum SIS II eingeschaltet. Hierzu fand am 6. Oktober 2003 ein Symposium im zuständigen Ausschuss des Europäischen Parlaments statt, in dem sowohl der verantwortliche EU-Kommissar wie auch namhafte Datenschutzexperten ihre Vorstellungen von einem künftigen SIS darlegten. Die GKI, die nur sporadisch in den Ausbau des SIS einbezogen wurde, hat in einer umfassenden Stellungnahme auf die Gefahren für die Bürgerrechte hingewiesen, die von einem schleichenden Ausbau des geltenden SIS zu einem europaweiten polizeilichen Informations- und Recherchesystem ausgehen können. Insbesondere hat die GKI kritisiert, dass die Kommission den Ausbau mit maximalen Vorgaben vorantreibt, ohne dass eine politische Grundsatzentscheidung über Aufgaben und Zweck des künftigen SIS II getroffen wurde. Damit würden informationstechnische Fakten geschaffen, ohne dass zuvor der europäische Gesetzgeber die notwendigen rechtlichen Grundlagen durch eine Anpassung des Schengener Durchführungsübereinkommens (SDÜ) geschaffen hat. Hinzu kommt die insgesamt noch defizitäre Datenschutzstruktur innerhalb der so genannten Dritten Säule der EU. Ich habe diese Stellungnahme, die für die europäischen Institutionen bestimmt war, auch den zuständigen Ausschüssen des Deutschen Bundestages und der Bundesregierung zugeleitet.

Ich erwarte von der Bundesregierung, dass sie sich auf europäischer Ebene dafür einsetzt, die Weiterentwicklung des SIS unter strikter Beachtung datenschutzrechtlicher Vorgaben fortzusetzen und den hierfür notwendigen rechtlichen Rahmen mit dem Ziel einer Stärkung der Bürgerrechte anzupassen.

Die Empfehlungen sind abrufbar unter www.bfd.bund.de; Stichwort „Europa/Internationales“.

3.3.2.2 Datenschutzrechtliche Kontrolle von Ausschreibungen nach Artikel 96 des Schengener Durchführungsübereinkommens

Ausschreibungen bezüglich Drittausländern, die zur Einreiseverweigerung registriert sind, bilden den Großteil der Ausschreibungen zu Personen im SIS. Die GKI hat eine gemeinsame Kontrolle dieser Ausschreibungen bei den Mitgliedstaaten durchgeführt.

Auf Grund von Hinweisen auf möglicherweise unzulässige Ausschreibungen hat sich die GKI auf eine Kontrolle der Ausschreibungen nach Artikel 96 SDÜ bei den Vertragsparteien verständigt. Zu diesem Zweck wurde in einem ersten Schritt mittels Fragebogens eine Bestandsaufnahme des Verfahrens nach Artikel 96 SDÜ bei den Mitgliedstaaten durchgeführt.

Aufgrund der Antworten des BMI ergibt sich hinsichtlich der von Deutschland veranlassten Ausschreibungen das folgende Bild: Zum Zeitpunkt der Umfrage im Spätsommer 2003 bestanden von Seiten Deutschlands ca. 270 000 der insgesamt 800 000 Ausschreibungen nach Artikel 96 SDÜ im SIS. Deutschland hatte damit nach Italien die meisten Ausschreibungen veranlasst. Die weitaus überwiegende Anzahl der Ausschreibungen erfolgt nach Artikel 96 Abs. 3 SDÜ, also bei Einreiseverweigerung durch die zuständigen Ausländerbehörden der Länder. Ein kleiner Teil ergeht auf der Grundlage des Artikel 96 Abs. 2 SDÜ zur Gefahrenabwehr und erfolgt in der Regel durch den BGS. Anlässlich der Fragebogenaktion hat mich das BMI ersucht, die eigentliche datenschutzrechtliche Kontrolle erst nach der für den 1. Mai 2004 anstehenden Erweiterung der EU durchzuführen, weil damit ca. 60 000 Ausschreibungen zu Drittausländern gelöscht würden, die nach diesem Zeitpunkt Unionsbürger sind.

Die zweite Stufe der Überprüfung begann mit der Auswahl der zu überprüfenden Datensätze beim BKA auf der Basis eines Zufallsgenerators. Die ca. 400 ausgewählten Datensätze (ca. jeder 500ste) wurden anschließend von den Landesbeauftragten für den Datenschutz im schriftlichen Verfahren oder vor Ort bei den Ausländerbehörden überprüft. Lediglich in neun Fällen handelte es sich um Ausschreibungen gem. Artikel 96 Abs. 2 SDÜ durch den BGS. Als Ergebnis lässt sich festhalten:

– Die nach Artikel 96 SDÜ notwendige Entscheidung ist zumeist in der Ausländerakte dokumentiert.

- Es handelt sich in allen geprüften Fällen um Drittausländer. Die Daten der Betroffenen aus den Beitrittsländern wurden umgehend gelöscht.
- In den meisten Prüffällen lag der Ausschreibung eine rechtsgültige Ausweisungs- oder Abschiebeverfügung zu Grunde; in immerhin etwa 20 % der Fälle waren Betroffene nur zum Zweck der Aufenthaltsermittlung im SIS ausgeschrieben, was eine Ausschreibung nicht rechtfertigt.
- Die nach Artikel 112 Abs. 1 SDÜ vorgeschriebene Prüfung der weiteren Erforderlichkeit einer Ausschreibung nach Fristablauf war vielfach in den Akten nicht dokumentiert und konnte deshalb nicht kontrolliert werden. Mehrfach bestand die Dokumentation ausschließlich in der Meldung des BKA über die verlängerte Speicherung ohne eigenständige Entscheidung des zuständigen Sachbearbeiters.
- Mangels Dokumentation konnten vielfach keine Angaben zur Dauer der Ausschreibung festgestellt werden, was einen schwerwiegenden Mangel bedeutet. Die zulässige Ausschreibungsdauer beträgt, sofern kein Trefferfall eintritt, bei erstmaliger Speicherung drei Jahre, kann jedoch bei fortbestehendem Ausschreibungsgrund verlängert werden. So wurden auch einige Fälle festgestellt, bei denen die Ausschreibung bereits neun Jahre zurücklag.
- In knapp 50 Prozent der Fälle war die Ausschreibungsfrist im SIS an das unbefristet wirkende nationale Einreiseverbot nach § 8 Abs. 2 Ausländergesetz gekoppelt; in den restlichen Fällen erfolgte die Ausschreibung, der Regelung des Artikel 112 SDÜ folgend, nicht unbefristet.
- Mit der Löschung der Ausschreibung im SIS erfolgt nicht zwangsläufig die Vernichtung der zu Grunde liegenden Unterlagen. Vielfach werden diese noch in den Akten zur Dokumentation der Inpol-Ausschreibung aufbewahrt.

Insgesamt hat die Kontrolle auf nationaler Ebene einige – teilweise erhebliche – Mängel aufgezeigt, die nachteilige Konsequenzen für die Rechte der Betroffenen nach sich ziehen. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eine Arbeitsgruppe eingesetzt, die sich mit dem Prüfungsergebnis befassen soll.

Nach Abschluss der Kontrollen auf nationaler Ebene wird sich die GKI mit der Auswertung der Ergebnisse aus allen Schengenstaaten befassen und ggf. weitere Maßnahmen beschließen. Bei Redaktionsschluss waren die Beratungen in der GKI noch nicht abgeschlossen.

3.3.2.3 Multilaterales Übereinkommen zur polizeilichen Zusammenarbeit mit den Benelux-Staaten und Österreich

Zwischen Deutschland, den Benelux-Staaten und Österreich ist ein weitreichendes Übereinkommen zur polizeilichen Zusammenarbeit vorgesehen.

Seit 2003 laufen Verhandlungen zu einem Übereinkommen für die Vertiefung der polizeilichen Zusammenarbeit, insbesondere in den Bereichen Terrorismus, grenzüberschreitende Kriminalität und illegale Migration (Schengen III) zwischen Deutschland, den Benelux-Staaten und Österreich. Bereits der erste Vertragsentwurf enthielt weitreichende Regelungen zur grenzüberschreitenden Zusammenarbeit. Gegen Ende 2004 wurde ich beteiligt.

Zu diesem Zeitpunkt war der ursprüngliche Vertragsentwurf allerdings schon erheblich entschärft worden. So war jetzt vorgesehen, den gegenseitigen Zugriff bezüglich der Fingerabdruck- und DNA-Daten nur noch auf sog. Fundstellendatensätze zu begrenzen und ein sog. Hit/No hit-Verfahren durchzuführen. Dabei werden die Fundstellendatensätze, z. B. eine DNA-Spur oder ein Fingerabdruck, zunächst daraufhin untersucht, ob sich in der Datei bereits ein entsprechender Datensatz befindet. Erst in einem zweiten Schritt wird im Trefferfall in einem Rechtshilfeverfahren entschieden, ob auch die dazugehörigen Personalien übermittelt werden. Hierzu schlug ich vor, den Zugriff auf DNA- und Fingerabdruckfundstellendatensätze nur zum Zweck der Zuordnung offener Tatspuren zuzulassen. Andernfalls würde der Abruf von Fundstellendatensätzen, bei denen die Personalien der zugehörigen Person bereits bekannt sind, bei den anderen Vertragsstaaten lediglich zu zusätzlichen Erkenntnissen führen, ohne dass über die Zulässigkeit der Übermittlung in einem Rechtshilfeverfahren entschieden würde. Der Zugriff auf die zuvor genannten Datenbanken sollte zu benennenden nationalen Kontaktstellen vorbehalten bleiben.

Die neu in den Entwurf aufgenommene Regelung zum gegenseitigen umfassenden Zugriff auf die Kfz-Register halte ich im Hinblick auf seine Tragweite für unverhältnismäßig, weil er u. a. auch zur Verfolgung von Verkehrsordnungswidrigkeiten eingeräumt werden sollte. Erhebliche Bedenken habe ich auch gegen eine sog. Öffnungsklausel in dem Entwurf vorgetragen, wonach der gegenseitige schreibende und lesende Zugriff auf andere geeignete Datensammlungen ausgedehnt werden können soll. Hierfür sehe ich keinen Bedarf, denn neben der im Vertragsentwurf vorgesehenen Vernetzung daktyloskopischer und DNA-Datenbestände gibt es für die EU-weite Fahndung bereits das SIS sowie das im Entstehen begriffene Europäische Informationssystem (EIS) als europaweiten Kriminalaktennachweis bei Europol, sodass weitere europaweite Datensammlungen zur polizeilichen Zusammenarbeit nicht erforderlich erscheinen. Zu begrüßen ist dagegen die vertragliche Datenschutzklausel, in der die unabdingbaren Rechte des von einer Datenverarbeitung Betroffenen, eine umfassende Protokollierung und die datenschutzrechtliche Kontrolle ausdrücklich geregelt sind.

Die Vertragsverhandlungen dauerten bei Redaktionsschluss an.

3.3.3 Zollinformationssysteme der EU-Mitgliedstaaten und Aktennachweissystem FIDE

Das Zollinformationssystem (ZIS) wird von den nationalen Zollverwaltungen bisher wenig genutzt. Deutschland hat als einziger EU-Mitgliedstaat das FIDE-Protokoll ratifiziert.

Das ZIS der EU-Mitgliedstaaten, eine EU-weite Ausschreibungsdatei im Bereich des Zolls, ist ebenso wie das EG-ZIS für den Bereich des Binnenmarktes seit 24. März 2003 im Wirkbetrieb (vgl. Kasten zu Nr. 3.3.3, vgl. auch 18. TB Nr. 7.9, 13.4). Beide Datenbanken, die logisch voneinander getrennt sind, werden von der Europäischen Kommission und dort von dem Amt für Betrugsbekämpfung betrieben. Die Vertreter der Kommission standen im Berichtszeitraum der gemeinsamen Datenschutzaufsichtsbehörde, der die datenschutzrechtliche Kontrolle des Systems obliegt, für Auskünfte zur Verfügung. Danach ist das ZIS zwar in Betrieb, seine Akzeptanz bei den Nutzern, den nationalen Zollverwaltungen, jedoch denkbar gering. So waren Anfang Dezember 2004 nur ca. 135 Ausschreibungen registriert. Die Kommission führt die geringe Akzeptanz auf die Vielzahl von Datenbanken zurück, die im Zollbereich bereits existieren. Sie hat im übrigen eine Kampagne bei den potentiellen Nutzern gestartet, um auf die Existenz und die Vorteile des Systems hinzuweisen. Ich sehe hierin auch ein Indiz dafür, dass die Schaffung immer neuer Instrumente, Befugnisse und Datenbanken mit sich teilweise überschneidenden Aufgaben nicht unbedingt zu mehr Sicherheit bzw. zur Optimierung der Aufgabenwahrnehmung beiträgt.

Deutschland ist dem ZIS-Übereinkommen am 30. April 2004 beigetreten, nachdem das ZIS-Ausführungsgesetz vom 31. März 2004 (BGBl. II S. 482), gegen das ich im Gesetzgebungsverfahren keine Einwendungen erhoben hatte, am 1. April 2004 in Kraft getreten war.

Das Automatisierte Aktennachweissystem im Zollbereich FIDE (vgl. 19. TB Nr. 16.3.1) soll in Ergänzung zu den ZIS-Systemen, die reine Ausschreibungsdatenbanken sind, den nationalen Zollbehörden mit erweiterten Datenkategorien auch für zoll- und strafrechtliche Recherchen zur Verfügung stehen. Rechtsgrundlage ist ein Protokoll gem. Artikel 34 des Vertrages über die Europäische Union zur Änderung des Übereinkommens über den Einsatz der Informationstechnologie im Zollbereich. Die Bundesrepublik Deutschland hat als bisher einziger EU-Mitgliedstaat das FIDE-Protokoll ratifiziert. FIDE befindet sich noch in der technischen Entwicklung. Die Mitgliedstaaten wurden im Jahre 2004 aufgefordert, ihre Benutzeranforderungen gegenüber der Kommission zu spezifizieren, was für Deutschland durch das BMF erfolgt ist. Die Kommission beabsichtigt, FIDE auch auf den Anwendungsbereich des EG-ZIS auszudehnen. Hierbei ist jedoch zu beachten, dass die EU-Dienststellen für Zoll keine Strafverfolgungskompetenz besitzen. Vor einer solchen Ausdehnung des Anwendungsbereichs von FIDE bedarf es im übrigen noch einer Rechtsgrundlage. Die Kommission hat bisher noch keinen genauen Zeitpunkt für die Aufnahme des Wirkbetriebs von FIDE genannt. Ich werde die weitere Entwicklung mit Aufmerksamkeit verfolgen.

Die gemeinsame Aufsichtsbehörde hatte für November 2004 eine erste datenschutzrechtliche Kontrolle des ZIS-Systems vorgesehen. Diese musste wegen offener Organisationsfragen jedoch verschoben werden.

Kasten zu Nr. 3.3.3

Aufgaben und Arbeitsweise des ZIS

Das ZIS hat die Aufgabe, schwere Verstöße gegen einzelstaatliche Rechtsvorschriften im Zollbereich zu verhindern und ihre Ermittlung und Verfolgung zu unterstützen. Durch eine rasche Informationsverbreitung soll die Effizienz von Kooperations- und Kontrollmaßnahmen der Zollverwaltungen der Mitgliedstaaten gesteigert werden.

Das ZIS besteht aus zwei Datenbanken, auf welche die Zollstellen sowie die für die Zollfahndung zuständigen Stellen der Mitgliedstaaten unmittelbaren Zugriff haben. In der ersten Datenbank, dem eigentlichen ZIS werden personenbezogene Daten für zollamtliche Kontrollzwecke, d. h. für Zwecke der Feststellung und Unterrichtung, der verdeckten Registrierung oder der gezielten Kontrolle gespeichert. In das „Aktennachweissystem für Zollzwecke (FIDE)“, der zweiten Datenbank, dürfen personenbezogene Daten eingegeben werden, um andere Mitgliedstaaten über die Existenz von Ermittlungsakten zu unterrichten. Auf diese Weise sollen Amtshilfeersuchen erleichtert werden.

Beide Datenbanken werden in jedem Mitgliedstaat als nationale Dateien angesehen. Vorbehaltlich besonderer Bestimmungen des ZIS-Übereinkommens finden damit die Datenschutzregelungen der Mitgliedstaaten auf das ZIS Anwendung.

3.3.4 Intensivierung des Informationsaustauschs in der Europäischen Union zur Bekämpfung von Kriminalität und Terrorismus

Die Intensivierung des Informationsaustauschs zwischen den Strafverfolgungsbehörden der Mitgliedstaaten ist nur bei Gewährleistung des Datenschutzes vertretbar.

Zur Fortentwicklung Europas zu einem „Raum der Freiheit, der Sicherheit und des Rechts“ (Artikel 29 Abs. 1 EU-Vertrag) wurden im Jahre 2004 neue Initiativen mit dem Ziel einer Intensivierung des Informationsaustausches zwischen den Sicherheitsbehörden in der Union gestartet, die erhebliche datenschutzrechtliche Fragen aufwerfen. Die wichtigsten Initiativen in diesem Bereich sind

– der Entwurf eines Rahmenbeschlusses über die Vereinfachung des Informationsaustausches zwischen den Strafverfolgungsbehörden der Mitgliedstaaten der Europäischen Union, insbesondere in Bezug auf

schwerwiegende Straftaten einschließlich terroristischer Handlungen (sog. Schwedische Initiative, Ratsdok. 10 215/04 CRIMORG 46) sowie

– ein Vorschlag der Kommission für einen Ratsbeschluss über den Informationsaustausch und die Zusammenarbeit betreffend terroristischer Straftaten (Dokument 8200/04 JAI 109).

Die Bundesregierung hat mich an der Vorbereitung einer deutschen Stellungnahme zu den Entwürfen beteiligt. Ich habe darauf hingewiesen, dass es hier nicht nur um die Schaffung einzelner Rechtsakte zum Informationsaustausch geht, sondern vielmehr eines datenschutzrechtlichen Gesamtkonzepts für den Bereich der sog. Dritten Säule (polizeiliche und justizielle Zusammenarbeit in der EU) der Europäischen Union bedarf.

Im November 2004 erhielt ich Gelegenheit zu einer Stellungnahme vor einem Unterausschuss des Ausschusses für Bürgerrechte, Justiz und Innere Angelegenheiten (LIBE) des Europäischen Parlaments. Ich habe mich dabei insbesondere zu der Schwedischen Initiative geäußert. Ein Hauptproblem sehe ich in der Abgrenzung dieses Projekts zu anderen Rechtsinstrumenten der EU, u. a. dem EU-Rechtshilfeübereinkommen in Strafsachen. Ich habe ferner auf die verfassungsrechtlichen Aspekte hingewiesen, die sich aus einem solchen Rahmenbeschluss ergeben. Insbesondere müssen die Anforderungen der öffentlichen Sicherheit in einem ausgewogenen Verhältnis zu den Freiheitsrechten des Bürgers stehen, die durch die Verfassungen der Mitgliedstaaten und durch den Entwurf einer Europäischen Verfassung gesichert werden sollen. Schließlich habe ich vorgetragen, dass ich die Schaffung einheitlicher Datenschutzbestimmungen in der Dritten Säule für wesentlich erfolgversprechender halte als eine Vielzahl von Einzelregelungen, wie etwa dem auf der Schwedischen Initiative basierenden Entwurf eines Rahmenbeschlusses.

Ich habe angeregt, vor einer Entscheidung über den Vorschlag der Kommission für einen Ratsbeschluss über den Informationsaustausch und die Zusammenarbeit betreffend terroristischer Straftaten eine Evaluierung der bisherigen Regelungen zur Terrorismusbekämpfung vorzunehmen. Ferner muss bei der Regelung der Grundsatz der Verhältnismäßigkeit stärker unterstrichen werden.

Die Beratungen über die beiden Rechtsakte sollen bis spätestens Juni 2005 abgeschlossen sein. Ich werde die weitere Entwicklung aufmerksam beobachten.

3.3.5 EG-Richtlinie über die Verpflichtung von Beförderungsunternehmen, Angaben über die beförderten Personen zu übermitteln

In Ergänzung des Schengener Durchführungsübereinkommens werden Fluggesellschaften verpflichtet, bereits vor Abflug bestimmte Passagierdaten an die Grenzkontrollbehörden des jeweiligen EU-Mitgliedstaates zu übermitteln. Anders als das von den USA betriebene System (Advance Passenger Information System) und die in diesem Zusammenhang angeforderten Fluggastdaten ist der Datentransfer innerhalb der EU wesentlich restriktiver geregelt.

Die im Mai 2004 in Kraft getretene EG-Richtlinie 2004/82/EG (ABl. L 261 vom 6. August 2004, S. 24 ff.) zielt auf eine Verbesserung der Grenzkontrollen und der Bekämpfung der illegalen Einwanderung ab. Hierzu werden die Luftverkehrsunternehmen verpflichtet, Angaben über die von ihnen über die Außengrenzen der EU beförderten Personen vorab den für die Grenzkontrollen zuständigen Stellen der EU-Mitgliedstaaten auf deren Anforderung zu übermitteln.

Im Rahmen der Beratungen des Richtlinienentwurfs, an der u. a. die Art. 29-Gruppe der Datenschutzbeauftragten der EU-Mitgliedstaaten beteiligt war, konnte erreicht werden, dass die Regelungen der Richtlinie in wesentlichen Punkten datenschutzrechtlichen Anforderungen genügen: Die Übermittlung von Passagierdaten ist nur zum Zwecke der Grenzkontrolle und der Bekämpfung der illegalen Einwanderung zulässig. Die Art der zu übermittelnden Fluggastdaten ist auf das Notwendigste begrenzt und orientiert sich strikt am Übermittlungszweck. Auch die Speicherdauer für diese Daten bei den Beförderungsunternehmen und den Grenzschutzbehörden ist eng begrenzt. Schließlich werden die Beförderungsunternehmen verpflichtet, die Passagiere gemäß den Bestimmungen der europäischen Datenschutzrichtlinie 95/46/EG zu informieren. Der Entwurf hebt sich damit aus datenschutzrechtlicher Sicht vorteilhaft von dem von den USA betriebenen Verfahren ab (vgl. Nr. 22.2).

In einer Reihe von Einzelfragen hätte ich mir allerdings andere Regelungen gewünscht.

Um den Kreis der von der Datenerhebung Betroffenen auf das erforderliche Maß zu beschränken, hatte ich angeregt, den Anwendungsbereich der Richtlinie auf Problemrouten zu begrenzen und die nationalen Behörden zu verpflichten, die Daten bei den Luftverkehrsgesellschaften erst auf Grund einer entsprechenden Risikoabschätzung anzufordern. Eine derartige Einschränkung hielt ich auch deshalb für wichtig, weil sich der personelle Anwendungsbereich der Richtlinie auch auf Unionsbürger erstreckt. Im Hinblick auf den auf die Grenzkontrolle und die Bekämpfung der illegalen Einwanderung beschränkten Verwendungszweck für die Daten bin ich der Auffassung, dass die Verarbeitung und Nutzung der Daten von Unionsbürgern durch die Grenzkontrollbehörden der Mitgliedstaaten nicht erforderlich und damit nicht zulässig ist. Die Regelung berücksichtigt zudem nicht, dass Bürger aus den EU-Mitgliedstaaten bei der Einreise in die EU nach dem SDÜ einem anderen Kontrollregime unterliegen als Drittstaatsangehörige. Schließlich hielt ich es für angemessen, den Zeitpunkt der Datenübermittlung auf den Abschluss des „boarding check“ zu verlegen. Damit würde sichergestellt, dass nur personenbezogene Daten derjenigen Passagiere an die Grenzübergangsstellen übermittelt werden, die die Reise auch tatsächlich angetreten haben. Bedenken bestehen ferner gegen die in den Erwägungsgründen der Richtlinie eröffnete Möglichkeit nationaler Regelungen, nach denen Luftverkehrsgesellschaften zu weitergehenden Mitteilungen, z. B. betreffend Rückflugtickets verpflichtet werden können. Auch eine Aus-

weitung der Übermittlungspflicht auf biometrische Daten der Flugpassagiere, wie es in den Erwägungsgründen vorgesehen ist, wäre ein wesentlich stärkerer Eingriff in die Rechte der Passagiere, für den ich derzeit keine Notwendigkeit sehe.

Vor diesem Hintergrund bleibt die weitere Entwicklung der Passagierdatenübermittlung innerhalb der EU abzuwarten. Dies gilt insbesondere für die noch ausstehende Umsetzung der Richtlinie in das deutsche Recht.

3.3.6 Interpol-Aufbau einer DNA-Datenbank

Die DNA-Technik wird auf internationaler Ebene zunehmend für Zwecke der Verbrechensbekämpfung eingesetzt. Auch bei IKPO-Interpol gibt es entsprechende Vorhaben.

Beim Generalsekretariat von Interpol ist die dateimäßige Verarbeitung und Nutzung von DNA-Identifizierungsmustern zur Verbrechensbekämpfung in Vorbereitung. Zu diesem Zweck wird dort seit März 2000 ein Pilotprojekt zur Einführung einer internationalen DNA-Datenbank entwickelt. Rechtsgrundlage für diese Datensammlung ist die Interpol-Charta „Internet-DNA-Gateway“, in der die Voraussetzungen für Speicherung und Nutzung von DNA-Daten bei Interpol aufgelistet sind. Danach sollen im Zusammenhang mit dem Verdacht auf ein internationales Verbrechen DNA-Daten gespeichert werden von Beschuldigten/Verurteilten, Tatortspuren, Vermissten und unbekannten Toten.

In dieser Verbunddatei sollen die Identifizierungsmuster der genannten Personenkategorien – ohne direkt identifizierende Angaben wie Namen und Anschriften – sowie von Spuren erfasst werden, wobei die Muster bestimmte Merkmale des nicht codierenden Bereichs der DNA enthalten müssen. Dies bedeutet, dass Daten mit Aussagekraft hinsichtlich bestimmter genetischer Dispositionen nicht gespeichert werden dürfen. Die Datenbank soll in der Interpol-Zentrale auf einem stand-alone-PC betrieben werden; die teilnahmeberechtigten Mitgliedstaaten, die grundsätzlich für die eingegebenen Daten verantwortlich bleiben, werden auf die Datenbank im automatisierten Verfahren Zugriff erhalten. Auf eine DNA-Suchanfrage werden die anfragenden Staaten im Trefferfall unterrichtet, damit sie in Kontakt mit den anderen Datenbesitzern treten können. Erst dann wird die Identität eines Betroffenen offengelegt.

Im Juli 2003 ersuchte Interpol über 100 Mitgliedstaaten, darunter auch das Bundeskriminalamt als Nationales Zentralbüro von Interpol für Deutschland, entsprechendes Datenmaterial anzuliefern. Nachdem das Ersuchen auf nationaler Ebene mit den zuständigen Stellen der Länder – unter anderem als verantwortliche Datenbesitzer – erörtert worden war, bat mich das BMI im Mai 2004 um eine datenschutzrechtliche Stellungnahme.

Ich habe die Auffassung vertreten, dass die Datensammlung Personenbezug aufweist, weil die gespeicherten Daten unter Einschaltung der verantwortlichen „Datenbesitzer“ einzelnen Personen zugeordnet werden können, ja dies gerade Zweck der Datenbank ist. Wegen des Personenbezugs bemisst sich die Datenanlieferung durch Deutschland nach Maßgabe des § 14 BKAG. Hieran knüpft meine Forderung, dass nur Mitgliedstaaten mit vergleichbarem Datenschutzstandard Zugriff auf von Deutschland angelieferte DNA-Muster erhalten dürfen (vgl. § 14 Abs. 7 BKAG). Dies müsste von Interpol sichergestellt werden. Ferner habe ich zur Wahrung des Verhältnismäßigkeitsprinzips betont, dass nur solche Identifizierungsmuster von Straftätern bzw. von Spuren an Interpol übermittelt werden dürfen, bei denen aufgrund bestimmter Tatsachen ein Auslandsbezug besteht. Ferner habe ich im Hinblick auf den sensiblen Charakter des DNA-Materials auf eine effektive datenschutzrechtliche Kontrolle bei Interpol gedrängt, was auf Grund des Fehlens einer unabhängigen Datenschutzkontrollinstanz für Interpol problematisch ist.

Das BMI hat mir nach meiner Stellungnahme unter anderem einen Bericht des BKA zur Errichtung einer internationalen DNA-Datenbank bei Interpol übersandt, der die datenschutzrechtliche Zulässigkeit einer deutschen Beteiligung unterstreicht. Allerdings seien noch entsprechende Ergänzungen der einschlägigen Errichtungsanordnungen erforderlich, insbesondere zur DNA-Analysedatei beim BKA, aber auch der Datei VERMI/UTOT. Dieser Bericht ist im Herbst 2004 vom Arbeitskreis II der Innenministerkonferenz zustimmend zur Kenntnis genommen worden. Das BMI teilt meine Auffassung, dass es sich bei den für Interpol bestimmten DNA-Mustern grundsätzlich um personenbezogene Daten handelt, die allerdings pseudonymisiert seien. Hingegen werden meine Bedenken hinsichtlich der „Auslandsrelevanz“ der zu übermittelnden Muster schon aus praktischen Erwägungen nicht geteilt, weil sich ein Auslandsbezug vielfach erst im Trefferfall bei Interpol nachweisen lasse.

Bei der Anhörung zu den geänderten Errichtungsanordnungen gemäß § 34 BKAG werde ich dafür eintreten, dass bei der Einstellung von Daten in die Interpol-Datenbank das Prinzip der Verhältnismäßigkeit gewahrt und die Auslandsrelevanz der übermittelten Daten gewährleistet wird. Eine Übermittlung von DNA-Mustern, die zur internationalen Verbrechensbekämpfung nicht benötigt werden, sollte unterbleiben. Ein weiteres Anliegen bleibt, den Zugriff auf von Deutschland eingestellte DNA-Datensätze auf Interpol-Mitgliedstaaten mit vergleichbarem Datenschutzniveau zu begrenzen.

4 Technologischer Datenschutz

4.1 Allgegenwärtige Datenverarbeitung – lückenhafter Datenschutz?

Die Miniaturisierung der Informations- und Kommunikationstechnik dient der Verbesserung unserer Lebens- und Arbeitsbedingungen. Der Einsatz von technischen Systemen muss transparent und unter Wahrung des Selbstbestimmungsrechts der Betroffenen erfolgen.

Die Informations- und Kommunikationstechnik entwickelt sich permanent weiter: Die Rechenleistung und Vernetzungsdichte der Systeme steigt, die Übertragungsbandbreite nimmt zu und die Komponenten werden immer kleiner. Besonders die Miniaturisierung hat zu Visionen über neue Einsatzfelder für IT-Systeme geführt.

Die mit den Schlagworten „Pervasive Computing“, „Ubiquitous Computing“ und „Ambient Intelligence“ verbundenen Konzepte führen zu miniaturisierten IT-Systemen, die unsere Alltagswelt durchdringen, ohne das sie noch als „Computer“ erkannt werden. Trends, die diese Entwicklung vorantreiben, sind etwa

– leistungsfähigere, kleinere Prozessoren und Speicherbausteine,
– höhere Integration der Netze (UMTS, WiMax, GSM, WLAN, Bluetooth) mit neuen Diensten etwa zur spontanen Vernetzung von IT-Systemen, sowie
– neue Sensoren, langlebige und sehr kleine Batterien.

Durch diese IT-Systeme wird der Einsatz von Informationstechnik weitgehend unsichtbar, z. B. wenn Mikroprozessoren in Alltagsgegenstände integriert sind. Mit der Radio Frequency Identification (RFID) rückt die Vision dieser allgegenwärtigen Datenverarbeitung näher. Dies bringt neue Gefahren für die Persönlichkeitsrechte der Bürgerinnen und Bürger mit sich. Daher sind Konzepte zum Schutz der Privatsphäre gefragt, die bereits beim Systementwurf greifen und nicht erst nachträglich „aufgepfropft“ werden. Nachträglicher Datenschutz ist nicht nur weniger effektiv, sondern auch teuerer als eingebauter (System-)Datenschutz.

Wenn die Zahl, die Komplexität und die Verarbeitungskapazität der IT-Systeme zunehmen, muss auch die Sicherheit Schritt halten, etwa durch Ansätze wie das „Trusted Computing“. Die Trusted Computing Group (TCG) hat sich zum Ziel gesetzt, vertrauenswürdige PC zu entwickeln. Die Vertrauenswürdigkeit soll dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten eines Rechners überprüft, ob die installierte Hardware und das Betriebssystem mit den zertifizierten hinterlegten Konfigurationsangaben übereinstimmen. Ist das System vertrauenswürdig, können sicherheitskritische Anwendungen aufgerufen werden. Besonders wichtig ist auch die Möglichkeit der anonymen Nutzung der Vertrauenswürdigkeitsprüfung und der darauf basierenden Anwendungsprogramme. Hier sehe ich noch weiteren Klärungsbedarf, wie auch bei der Frage des offenen Zugangs zu den Standards der TCG. Insbesondere ist sicherzustellen, dass nicht heimlich Nutzerdaten registriert und damit weitere Überwachungsmechanismen installiert werden.

Immer mehr Menschen nutzen Funknetze. Damit wird die räumliche und zeitliche Ortung – auch Tracking oder Profiling genannt – von Personen und Gegenständen immer einfacher (vgl. auch Nr. 13.2.2). Von wenigen Metern bis zu einigen Kilometern reicht die Lokalisierung bei Bluetooth, WLAN und WiMax. Und da viele Geräte standardmäßig (beispielweise Mobiltelefon und Personal Digital Assistant) die Funktechnik aktiviert haben, können Personen oder Fahrzeuge sehr leicht geortet werden. Deshalb halte ich mehr Transparenz über diese zusätzlichen Fähigkeiten bei diesen Funksystemen für unabdingbar.

In den vergangenen Jahren haben Viren, Würmer und Trojaner weiterhin erhebliche Schäden verursacht. Besonders kritisch ist dabei die Beobachtung, dass sich Würmer immer noch über das Internet ausbreiten konnten, obwohl bereits Software-Updates zum Schließen der Sicherheitslücken vorhanden waren. Sind die Anwender zu nachlässig bei der Pflege der Systeme oder informieren die Anbieter von Betriebssystemen ihre Kunden nicht ausreichend über die Gefahren? So wurden „normale“ PC so manipuliert, dass sie als Mail-Server ohne Zutun des rechtmäßigen Benutzers Spam-E-Mails mit Schadensprogrammen versenden und damit zur Flut der unerwünschten E-Mail (vgl. auch Nr. 13.8) beitragen.

Weitere Beobachtung verdienen PC-Schnittstellen wie die USB-Schnittstelle (vgl. Nr. 4.2.3). Einerseits können sensible Daten schnell auf externen Festplatten gespeichert und anschließend sicher verwahrt werden, andererseits können über diese Schnittstelle leicht Daten unkontrolliert kopiert oder unerwünschte Programme genutzt werden. Hier fehlen den gängigen Betriebssystemen Funktionen zur kontrollierten Verwendung dieser Schnittstellen, mit denen sich ein derartiger Missbrauch verhindern lässt. Ob die jüngsten Maßnahmen der Hersteller von Betriebssystemen und Schutzprogrammen greifen, wird sich noch zeigen (vgl. Nr. 4.3.3).

In großen IT-Projekten werden häufig Sicherheitsmaßnahmen zur vertraulichen Datenübertragung und sicheren gegenseitigen Authentifizierung im Internet bereitgestellt. Leider wird jedoch die verfügbare und erprobte Technik nicht überall eingesetzt (vgl. auch Nr. 8.6) und immer noch wird bei der Konzeption von IT-Systemen der Datenschutz nicht ausreichend berücksichtigt (vgl. auch Nr. 16.1.3). Verfahren ohne abgestufte Zugriffsrechte, eine viel zu umfangreiche Datenerhebung und generell unsichere IT-Systeme sind die Folge.

Hersteller, Anwender und Nutzer der Informationstechnik sind aufgefordert, Fragen des Datenschutzes und der Datensicherheit mehr Aufmerksamkeit entgegen zu bringen, um Fehlentwicklungen und Missbrauch wirksam zu verhindern. Auch durch die überfällige Umsetzung des Konzepts unabhängiger Datenschutzzertifizierung gem. § 9a BDSG (Datenschutzaudit – vgl. Nr. 2.2) ließen sich Sicherheitsmängel vermeiden und damit das Vertrauen in die Informationstechnik stärken. Hier sehe ich den Gesetzgeber in der Pflicht.

4.1.1 Identitätsmanagement – Welche Identitäten verwenden Sie?

Die Authentizität des Kommunikationspartners, die Qualität und der Umfang der auszutauschenden Daten im Internet müssen sichergestellt werden. Dabei ist jedoch zu gewährleisten, dass Daten, die von verschiedenen Stellen erhoben wurden, grundsätzlich nur mit Einwilligung des Nutzers zusammengeführt werden können.

Ob über das Internet oder beim Besuch einer Behörde, überall sind personenbezogene Daten erforderlich. Dazu gehören beispielsweise Anschrift, E-Mail-Adressen, Kontodaten, Sozialversichertennummer oder Krankenversichertennummer. Wenn jedoch für die verschiedensten Verfahren dieselben Identifizierungsdaten (ID) verwendet werden, ist zu befürchten, dass die Inhaltsdaten unter Verwendung dieser ID verknüpft werden. Der Nutzer steht also vor dem Dilemma, sich entweder eine Vielzahl unterschiedlicher ID merken zu müssen oder sich

dem Risiko auszusetzen, dass seine Daten verknüpft und zu einem Profil zusammengeführt werden. Das Identitätsmanagement beschreibt einen Ausweg aus diesem Dilemma.

Ein datenschutzfreundliches Identitätsmanagement muss sichere Prozesse zur Authentifizierung und Übermittlung der Daten des Nutzers zur Verfügung stellen. Nur dadurch wird die Vertraulichkeit von Mitteilungen erreicht und beiden Seiten wird die Identität der Gegenseite verlässlich mitgeteilt. Dabei sollen nur die für diesen Vorgang notwendigen personenbezogenen Daten verarbeitet werden.

Am Schalter einer Behörde ist die Sicherheit für den Betroffenen leicht zu erkennen und zu bewerten (so kann er feststellen, ob sich andere Klienten in Hör- oder Sichtweite befinden). Bei der Kommunikation über das Internet ist das nicht so. Daher sind hier IT-Sicherheitsmaßnahmen erforderlich – etwa Maßnahmen zur Verschlüsselung, die eine unberechtigte Kenntnisnahme durch Dritte ausschließen.

Es gibt heute zwar kein allgemein anwendbares Konzept zu einem datenschutzfreundlichen Identitätsmanagement, aber einige Grundregeln:

- Nur in den Fällen, in denen eine Identifizierung erforderlich ist, sollten Identifizierungsdaten überhaupt erhoben werden. So ist bei einem reinen Informationsdienst eine persönliche Identifizierung der Nutzer im Regelfall entbehrlich.
- Wenn ein Personenbezug auf Dauer nicht notwendig ist, kann durch nachträgliche Anonymisierung der Daten die Zuordnung zu einer Person unterbunden werden.
- Durch Verwendung unterschiedlicher Identitäten – etwa verschiedener Pseudonyme für unterschiedliche Verfahren – kann eine unberechtigte Verknüpfung von Datenbeständen verhindert werden.
- Temporäre Identitäten – etwa zur Abwicklung einer einmaligen Bestellung – vermeiden die Übermittlung nicht notwendiger Daten und die Missbrauchsgefahr.
- Kryptographische Verfahren können die Sicherheit bei der Erzeugung und Nutzung von unterschiedlichen Identitäten unterstützen oder den Diebstahl einer Identität (Identity Theft) verhindern. Insbesondere bei der Nutzung unsicherer Netze (Internet) können Nutzer durch Verwendung dieser Technologien die Hoheit über ihre Daten behalten bzw. zurückgewinnen.
- Der Nutzer sollte weitgehend selbst kontrollieren können, mit welchen Identitäten er welche Leistungen in Anspruch nimmt. Die dabei verwendeten Daten sollten verschlüsselt, etwa auf einer Chipkarte, gespeichert werden. Hilfreich ist auch eine nutzerseitige Protokollierung der jeweils durchgeführten Transaktionen.

Zu den konkreten Problemen bei der Vergabe elektronischer Identitäten vgl. insbesondere Nr. 4.1.1.1 (JobCard-Verfahren) oder Nr. 17.1.3 (einheitliche Krankenversichertennummer).

4.1.1.1 Elektronische Identitäten – Die Identifizierung im JobCard-Verfahren

Im JobCard-Verfahren muss sichergestellt werden, dass der Betroffene sowohl bei der Meldung als auch beim Abruf der Daten eindeutig identifiziert werden kann. Identifizierungsverfahren dürfen jedoch nicht zu einer verfahrensübergreifenden Registrierung der Betroffenen führen.

Das Problem der elektronischen Identifizierung einer Person wird dringender, wenn in immer mehr Verfahren nicht mehr konventionelle Ausweis- oder Berechtigungspapiere durch einen Sachbearbeiter geprüft werden. Dabei geht es nicht allein darum, Verwechselungen (etwa aufgrund von Namensgleichheit) zu vermeiden; vielmehr müssen auch wirksame Mittel gefunden werden, die einen Missbrauch von elektronischen Identitäten ausschließen. Von zentraler datenschutzrechtlicher Bedeutung ist dabei, dass die Identifizierungsverfahren nicht zu einer umfassenden Verknüpfung unterschiedlicher Datenbestände führen.

Sei es für die Gewährung von Leistungen der Arbeitsagenturen oder im Bereich der Krankenversicherung (vgl. hierzu auch Nr. 17.1.3), überall ist die technisch eindeutige Identifizierung des Betroffenen ein wesentlicher Teil des Verfahrens. Gleiches gilt auch im JobCard-Verfahren (vgl. auch Nr. 15.2). Die Nutzung der dort gespeicherten Daten setzt eine einwandfreie Identifizierung des Betroffenen voraus und damit die Einführung eines eindeutigen Ordnungsmerkmals. Ursprünglich war geplant, hierzu die Rentenversicherungsnummer zu nutzen.

Nach der Rechtsprechung des Bundesverfassungsgerichts würde die Einführung und Verwendung eines allgemeinen Personenkennzeichens, das eine Zusammenführung aller Daten eines Menschen ermöglichen würde, dem Grundgesetz widersprechen. Eine Kennummer darf daher nur bereichspezifisch vergeben und genutzt werden. Die derzeitige gesetzliche Regelung ist eindeutig: § 18f SGB IV verbietet es, die Rentenversicherungsnummer (§ 147 SGB VI) außerhalb der gesetzlichen Aufgabe des Sozialgesetzbuches als Ordnungskriterium zu verwenden. Genutzt werden darf sie darüber hinaus nur von den in § 18f SGB IV genannten Sozialleistungsträgern. Bei der einzigen derzeit vorgesehenen Ausnahme im Steuerrecht (§ 90 Einkommenssteuergesetz) handelt es sich um eine steuerliche Regelung zur Nutzung der Rentenversicherungsnummer als „Zulagennummer“ bei der sog. „Riesterrente“. Dem Gedanken, die Nutzung der Rentenversicherungsnummer für weitere Zwecke – insbesondere im JobCard-Verfahren – zu öffnen, habe ich mich entgegengestellt, weil ich die Gefahr sehe, dass aus der Rentenversicherungsnummer ein verfassungsrechtlich unzulässiges allgemeines Personenkennzeichen wird. Es konnte eine Lösung gefunden werden, die ich aus Datenschutzsicht mittragen kann:

Das eigentliche Ordnungsmerkmal soll die Kartennummer der vom Arbeitnehmer im JobCard-Verfahren angemeldeten Signaturkarte (Unique-ID) werden. Die Unique-ID besteht im Modellprojekt aus der Seriennummer des Zertifikats und wird im Wirkbetrieb zur Sicherstellung der Eindeutigkeit noch um die Kennung des Trust Centers ergänzt. Gleichwohl ist es notwendig, eine

Verbindung zur Rentenversicherungsnummer herzustellen, da dem Arbeitgeber im JobCard-Verfahren die Unique-ID der vom Arbeitnehmer angemeldeten Signaturkarte nicht bekannt ist und der Arbeitgeber verpflichtet sein wird, auch die Rentenversicherungsnummer an die Zentrale Speicherstelle (ZSS) zu übermitteln. Hinzu kommt, dass auf eine Verbindung mit der Rentenversicherungsnummer nicht verzichtet werden kann, damit nach Ablauf der Gültigkeit der digitalen Signatur oder bei Verlust der Signaturkarte eine neue Signaturkarte im Verfahren gemeldet werden kann. Auf diese Weise kann auch auf Daten zugegriffen werden, die in der ZSS unter der ungültig gewordenen Unique-ID abgelegt sind.

Die Registratur Fachverfahren (RFV) übernimmt die Verknüpfung der Rentenversicherungsnummer mit der Unique-ID des Teilnehmers. Hierzu muss der Verfahrensteilnehmer sich mit der Rentenversicherungsnummer und der Unique-ID bei der RFV melden. Dadurch ergibt sich noch ein weiterer positiver Nebeneffekt: Bestehende Signaturkarten können ohne großen Zusatzaufwand in das Verfahren integriert werden. Dies bedeutet im Weiteren, dass ein freier Wettbewerb zwischen Trustcentern ermöglicht wird. Ein Arbeitnehmer kann also sowohl bei Trust Center A als auch bei Trust Center B seine Signaturkarte erstehen und durch die Registrierung bei der RFV für das Fachverfahren anmelden. Der Betroffene kann auf diese Weise selbst beeinflussen, ob seine Daten für alle Fachverfahren unter einer Unique-ID oder unter verschiedenen Unique-ID für die unterschiedlichen Fachverfahren abgelegt werden, ohne dass dadurch die Verfahrenssicherheit beeinträchtigt wird.

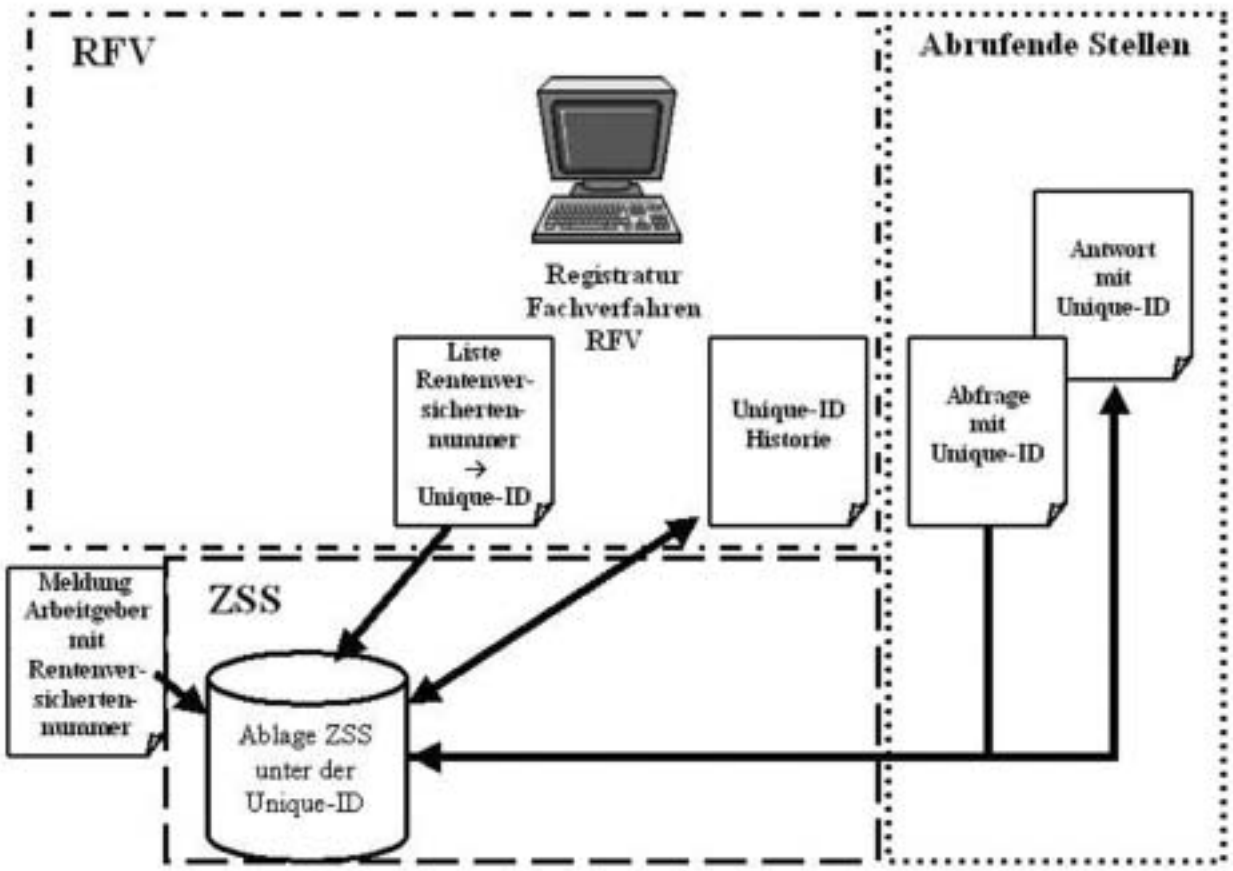
Die Zuordnung Rentenversicherungsnummer zu Unique-ID wird innerhalb der ZSS benötigt, um die Datensätze unter der Unique-ID abzuspeichern. Dies wird nach jeder Meldung des Arbeitgebers vorgenommen. Die Rentenversicherungsnummer dient somit nicht als Ordnungsmerkmal in der ZSS. Die Unique-ID-Historie wird in der ZSS benötigt, um mit einer Anfrage zu einer Unique-ID auch alle alten (oder neueren) Unique-ID zu ermitteln und um so die Datensätze, die zu einer Rentenversicherungsnummer gehören, entsprechend auslesen zu können.

Die ZSS greift in regelmäßigen Zeitabständen auf die RFV zu und holt sich die entsprechenden Dateien. Der Zugriff auf die Daten erfolgt also nur über die Unique-ID bzw. die dazu gehörende Historie (vgl. Abbildung RFV).

Aus meiner Sicht stellt das Verfahren einen tragbaren Kompromiss dar.

Abbildung 1 (zu Nr. 4.1.1.1)

Die Registratur Fachverfahren



4.1.1.2 Pseudonymisierung von Sozialversichertendaten mit einem Höchstmaß an Sicherheit

Aufgrund rechtlicher Vorgaben im SGB V müssen die Spitzenverbände der Krankenkassen und die Kassenärztliche Bundesvereinigung eine Vertrauensstelle und eine Datenaufbereitungsstelle einrichten und die übermittelten Leistungs- und Abrechnungsdaten pseudonymisieren.

Das Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG) enthält auch Vorschriften zur Pseudonymisierung der Leistungs- und Abrechnungsdaten (§§ 303a, 303c SGB V). Um dem Transparenzgebot Rechnung zu tragen und zugleich den Datenschutz zu gewährleisten, muss technisch sichergestellt werden, dass aus den Daten nicht auf die Identität des einzelnen Versicherten geschlossen werden kann. Hierzu soll in Zusammenarbeit mit dem BSI ein Verfahren entwickelt werden, das auch datenschutzrechtlichen Anforderungen Rechnung trägt: Die Daten sollen unter einem Pseudonym gespeichert werden. Das Pseudonymisierungsverfahren ist so zu gestalten, dass die Abrechnungs- und Leistungsdaten für alle Leistungsbereiche dem nicht namentlich gespeicherten Versicherten und dem Leistungserbringer periodenübergreifend zugerechnet werden können. Ferner muss das Pseudonym für den Versicherten Angaben zum Geburtsjahr, Geschlecht, Versichertenstatus sowie die ersten beiden Ziffern der Postleitzahl und für den Leistungserbringer Angaben zur Art des Leistungserbringers, Spezialisierung sowie ebenfalls die ersten beiden Ziffern der Postleitzahl enthalten.

Wie die ersten Gespräche ergaben, sollte die Erzeugung eines Pseudonyms auf dem Verfahren zur Erzeugung einer einheitlichen Krankenversichertennummer aufbauen (vgl. hierzu Nr. 17.1.3). Hier wie dort ergab sich aus datenschutzrechtlicher Sicht das Problem der eindeutigen Zuordnung der Daten zu einem Versicherten, die zwangsläufig mit der Erhebung eines umfangreichen Datenkranzes eines jeden Versicherten verbunden wäre. Um trotzdem mit möglichst wenig Daten auskommen zu können, habe ich darauf gedrungen, dass die einheitliche Krankenversichertennummer in das neu zu entwickelnde Verfahren einfließt.

Die Gespräche zur Entwicklung des Verfahrens sind noch nicht abgeschlossen. Meine Position habe ich den Beteiligten wie folgt dargelegt: Auf der Basis der einheitlichen dublettenfreien Krankenversichertennummer, ergänzt um die im Gesetz genannten weiteren Daten für den Versicherten und den Leistungserbringern sollte ein Verfahren entwickelt werden, das ein Pseudonym erzeugt, das eindeutig ist und eine Reidentifizierung nicht ermöglicht – entsprechend der einheitlichen Krankenversichertennummer (vgl. Nr. 17.1.3) mit einer Hash-Funktion und einem Verschlüsselungsalgorithmus.

Weiterhin müssen beide Verfahren in der Vertrauensstelle technisch, organisatorisch und personell strikt getrennt voneinander eingerichtet werden. Die Trennung der pseudonymisierten Daten von den Leistungs- und Abrechnungsdaten muss ebenfalls sichergestellt werden. Eine Weiterleitung der Daten an die Datenaufbereitungsstelle darf nur unter der Verwendung des Pseudonyms erfolgen. Nach der Übermittlung der pseudonymisierten Daten an die Datenaufbereitungsstelle sind die Daten bei der Vertrauensstelle unverzüglich zu löschen.

Die Wahl des Pseudonymisierungsverfahrens muss in Abhängigkeit vom Zweck der Datenauswertung getroffen werden. So muss beispielsweise bei Langzeitbeobachtungen trotz Veränderung von personenidentifizierenden Daten (z. B. Kassenwechsel, Namensänderung) sichergestellt sein, dass für die Betroffenen weiterhin dasselbe Pseudonym erzeugt wird. Außerdem ist zu prüfen, ob eine Depseudonymisierung, d. h. die nachträgliche Zuordnung der pseudonymisierten Daten zum Träger des Pseudonyms, im Einzelfall möglich sein muss und mit welchem Aufwand dies verbunden wäre. Aus Datenschutzsicht ist hier allerdings ein Einweg-Pseudonymisierungsverfahren zu bevorzugen, da hierbei eine Depseudonymisierung wesentlich aufwändiger und damit weniger wahrscheinlich wäre. Die Sicherheit hängt beim Einweg-Pseudonym nicht nur vom „Geheimnis“ (Algorithmus, Schlüssel, Zuordnungstabelle) ab, sondern außerdem von sämtlichen der Pseudonymisierung zugrunde liegenden Personendaten von allen in die Auswertung einbezogenen Personen und der Anzahl der pseudonymisierenden Stellen. Je mehr Stellen Kenntnis desselben Algorithmus und Schlüssels haben, um so angreifbarer wird das Verfahren. Deshalb halte ich das Konzept einer Vertrauensstelle zur Erzeugung und Pflege des pseudonymisierten Datenbestands für sinnvoll.

Die Gefahr der Depseudonymisierung aufgrund von Alleinstellungsmerkmalen einzelner Personen, etwa das Zusammentreffen einer sehr seltenen Krankheit mit weiteren Merkmalen, die nur in geringer Häufigkeit auftreten, ist letztlich nur zu vermeiden, wenn derartige Kombinationen bei Auswertungen mit anderen Fallgruppen zusammengefasst und nicht einzeln verwendet werden.

Darüber hinaus ist ein Verfahren zu entwickeln wie mit Pseudonymen umgegangen wird, die durch Sicherheitslücken oder andere Mängel aufgedeckt und ihren Trägern zugeordnet wurden.

4.1.1.3 Personalbefragung, immer anonym oder zumindest pseudonym!

Mitarbeiterbefragungen werden neuerdings auch mit Hilfe der Informationstechnik durchgeführt. Die Anonymität oder zumindest Pseudonymität müssen auch bei elektronischen Erhebungen gewährleistet werden.

Immer wieder werde ich um Beratung zu einer „Online“-Mitarbeiterbefragung gebeten, verbunden mit der Bitte, die dabei zu beachtenden technischen und organisatorischen Voraussetzungen zu benennen (zu den rechtlichen Voraussetzungen vgl. Nr. 10.2.4). Grundsätzlich sind bei einer Befragung die freiwillige Teilnahme und die Anonymität der Befragten zu wahren.

Wird aus wirtschaftlichen oder organisatorischen Gründen die Erhebung und Auswertung mit Hilfe der Informationstechnik durchgeführt, müssen sich diese Grundsätze

in der Gestaltung des Verfahrens wiederfinden. Der Verfahrensaufbau muss sich an den Prinzipien des § 3a BDSG orientieren und könnte wie folgt aussehen: Im Intranet der betreffenden Behörde wird ein Mitarbeiterbefragungsportal eingerichtet. Hierzu wird ein spezieller, nur für diese Aufgabe bestimmter (Datenbank-) Server eingerichtet, zu dem ausschließlich Personen, die mit der Mitarbeiterbefragung betraut wurden, direkten Zugang haben. Über das Mitarbeiterportal werden die Fragebögen zum Abruf bereit gehalten. Der Abruf erfolgt über einen Internetbrowser. Die Mitarbeiter können so Fragebögen ausdrucken, ausfüllen und anschließend abgeben. Soll die Erhebung ebenfalls „online“ erfolgen, müssen hierfür spezielle, keinem Mitarbeiter zugeordnete Arbeitsstationen eingerichtet werden. Hierdurch soll verhindert werden, dass über die Protokolle des Intranetservers Antworten einem Mitarbeiter zugerechnet werden können und damit die Anonymität aufgehoben werden würde. Eine Zusammenführung mit anderen Personaldaten ist zu unterbinden.

Ein solches Verfahren würde die Anonymität der Mitarbeiter sicherstellen. Um Mehrfachbeteiligungen derselben Person zu verhindern, könnte ein Pseudonymisierungsverfahren eingesetzt werden, bei dem eine Vertrauensstelle anhand automatisch generierter Zufallszahlen die Pseudonyme vergibt. Es wird nicht registriert, welchem Mitarbeiter welches Pseudonym zugeordnet wird. Mit dem Pseudonym kann sich der Mitarbeiter an der Befragung beteiligen, wobei jede Zufallszahl nur einmal verwendet werden kann. In der Vertrauensstelle wird sichergestellt, dass ein Mitarbeiter nur ein Pseudonym erhält. Die Kommunikationsvorgänge des Verfahrens sollten verschlüsselt erfolgen.

Das Modell hat beispielsweise der Bundesgrenzschutz für seine Mitarbeiterbefragung verwendet. Ich werde die Befragung dort weiterhin begleiten und die Erfahrungen in weiteren Beratungen berücksichtigen.

4.1.2 Verschlüsselung sinnvoll einsetzen!

Verschlüsselungsverfahren zählen zu den Datenschutzbasistechnologien. Ob ein bestimmtes Verschlüsselungsverfahren eingesetzt werden kann, hängt nicht allein von seiner technischen Sicherheit, sondern auch von der Praktikabilität der jeweiligen Lösung ab. Diese Frage wird beim JobCard-Verfahren intensiv diskutiert.

Im Rahmen des JobCard-Projektes (vgl. hierzu Nr. 15.2) wurden auch die Sicherheitsstandards getestet, die im Wirkbetrieb zum Einsatz kommen sollen. Sie sollen dem Stand der Technik entsprechen und zugleich eine nachhaltige Senkung der Kosten, eine spürbare Entbürokratisierung der Verwaltung und eine deutliche Entlastung der Bürger etwa bei Vorlage von Bescheinigungen berücksichtigen. Aus Gründen des Datenschutzes muss sichergestellt sein, dass nur ein gesicherter elektronischer Zugriff auf die zentral gespeicherten Arbeitnehmerdaten möglich ist. Insgesamt sollen Medienbrüche bei der Ausstellung und Verwaltung von elektronischen Verdienstbescheinigungen vermieden und eine schnelle Bearbeitung von Anträgen/Bescheiden erzielt werden.

Ohne angemessene Sicherheit kann und wird das Verfahren keine Akzeptanz in der Bevölkerung und bei der Wirtschaft finden. Die diskutierten Sicherheitsmaßnahmen konzentrieren sich auf die folgenden Modelle:

- Zugriffsschutzmodell:
  Bei diesem Modell werden alle Daten sowohl beim Einstellen der Daten in die Zentrale Speicherstelle (ZSS) als auch beim Abruf der Daten durch berechtigte Stellen verschlüsselt übertragen. Die Speicherung in der ZSS erfolgt ebenfalls verschlüsselt. Hierzu steht ein sog. Master-Session-Schlüssel zur Verfügung, der von einer unabhängigen öffentlichen Betreibergesellschaft generiert wird und nur dieser Stelle bekannt ist. Die Daten liegen nach der Übertragung und dem Plausibilitätstest nur verschlüsselt in der ZSS vor. Die Entschlüsselung erfolgt bei Vorlage einer berechtigten Abfrage mit Signatur des Betroffenen und nur durch das Zusammenwirken des unabhängigen Betreibers und der ZSS. Der Schutz der Daten konzentriert sich auf die Einhaltung der gesetzlichen Vorgaben im JobCard-Gesetz durch ZSS und Betreibergesellschaft (beides per Gesetz öffentliche Stellen), die Kontrolle durch den Bundesbeauftragten für den Datenschutz sowie auf die geplante gesetzliche Verpflichtung einer regelmäßigen Überprüfung des tatsächlichen Datenschutzstandards (Datenschutzaudits).
- Ende-zu-Ende-Verschlüsselungsmodell:
  Beim Ende-zu-Ende-Verschlüsselungsmodell werden die Daten mit dem öffentlichen Schlüssel des Arbeitnehmers verschlüsselt und dann an die ZSS übermittelt. Die Speicherung in der ZSS erfolgt unter der vollständigen Kontrolle des Betroffenen. Ein Abruf der Daten kann nur dann stattfinden, wenn der Betroffene seine JobCard zum Abruf vorlegt und die Daten dann bei der abfragenden Stelle entschlüsselt werden können.

Datenschutzrechtlich traten bei den Modellen folgende Fragestellungen und Probleme auf:

– Beim Zugriffsschutzmodell liegen die Daten zum Plausibilitätstest kurzzeitig unverschlüsselt in der ZSS vor. Dabei könnte die ZSS Kenntnis von den Daten nehmen.

– Zwar sind in der Datenbank der ZSS die Daten verschlüsselt. Beim Zusammenwirken von ZSS und Betreibergesellschaft zur Schlüsselverwaltung könnten jedoch alle Daten entschlüsselt und einem Dritten übergeben werden.

– Beim Ende-zu-Ende-Verschlüsselungsmodell muss ein Ersatzverfahren eingerichtet werden, damit bei Verlust oder Zerstörung der Signaturkarte weiterhin auf Daten zur Berechnung von Leistungen zugegriffen werden kann, etwa indem alle Arbeitgeber die übermittelten Daten weiterhin speichern oder durch Hinterlegung des geheimen elektronischen Schlüssels des Betroffenen. Die Speicherung der geheimen Schlüssel wäre zwar technisch umsetzbar, führte aber zu einem Register, in dem alle Verschlüsselungsschlüssel aller Arbeitnehmer gespeichert und zum Abruf bereitgehalten würden. Auch wäre nach dem Zugriff auf das zentrale Register eine Entschlüsselung der Daten ohne Mitwirken des Betroffenen möglich.

– Die Ende-zu-Ende-Verschlüsselung könnte zu einer wesentlichen Mehrbelastung auf Seiten der Arbeitnehmer führen. So müssten bei Sozialleistungen, bei denen mehrere Personen Daten bei der abrufenden Stelle frei schalten müssen, alle Betroffenen bei der abrufenden Stelle erscheinen, z. B. beim Wohngeld alle Mitbewohner mit eigenem Einkommen.

– Jeder Abruf der Daten aus der ZSS muss bei Verwendung der Ende-zu-Ende-Verschlüsselung im Beisein des Arbeitnehmers durch diesen erfolgen. Dies führt dazu, dass bei Nachmeldungen, Korrekturmeldungen etc. das Erscheinen des Arbeitnehmers bei der Antragsbehörde erforderlich ist, da sonst die Daten nicht entschlüsselt werden können.

– Beim Arbeitergeber selbst müssen beim Ende-zu-Ende-Verschlüsselungsmodell vor der Verschlüsselung alle Daten entsprechend den Anforderungen einzelner Sozialverfahren (Wohngeld, Arbeitslosengeld, ALG II) geordnet und in einzelnen Blöcken verschlüsselt werden, damit ein gezielter Abruf stattfinden kann. Andernfalls würden alle Daten allen Abfragestellen zur Verfügung stehen. Dies wäre aus datenschutzrechtlicher Sicht nicht zulässig.

– Die Arbeitnehmer müssten jeden Wechsel ihres Signaturschlüssels unverzüglich dem Arbeitgeber anzeigen und durch Vorlage der Karte dokumentieren.

Angesichts der ungelösten Fragen beim Ende-zu-Ende-Modell habe ich bisher das Zugriffsschutzmodell präferiert. Das Restrisiko, das bei diesem Modell besteht, könnte durch weitere Maßnahmen reduziert werden, wie

– strenge gesetzliche Zweckbindung, auch für Zugriffe der Sicherheitsbehörden und der Justiz,

– strenge datenschutzrechtliche Kontrolle durch den Bundesbeauftragten für den Datenschutz,

– der Verpflichtung zu einem regelmäßigen Audit und zur Überprüfung der Sicherheitsstandards in der ZSS.

Vor der endgültigen Entscheidung, welches Modell beim JobCard-Verfahren eingesetzt wird, habe ich mich zusammen mit meinen Länderkollegen gemeinsam dafür ausgesprochen, ein Gutachten erstellen zu lassen, das beide Modelle unter dem Blickwinkel des Datenschutzes, der Sicherheit, der Bürgernähe, der Benutzerfreundlichkeit, der Entbürokratisierung und der Entlastung aller Beteiligten nochmals prüft und somit allen Beteiligten eine Entscheidungshilfe liefert.

4.2 Neue Technologien

4.2.1 RFID – Funkchips für jede Gelegenheit?

Kleine Funkchips, sogenannte „RFID“, sind dabei, die Welt zu erobern. Die Zukunftsvision der allgegenwärtigen Datenverarbeitung könnte schon bald realer sein, als es so manchem lieb ist, wenn z. B. erst Kleidungsstücke unbemerkt Auskunft über Ihren Träger geben.

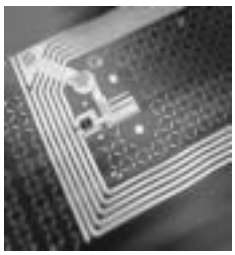
Die Radio Frequency Identification bezeichnet eine Mikrochiptechnologie zur kontaktlosen Speicherung von Daten. Diese werden mittels einer Funkübertragungstechnik abgefragt und mit Energie versorgt (Foto RFID). Die im Sprachgebrauch oft nur mit „Tags“ bezeichneten Chips gelten bisher als attraktive Ergänzung zur Strichcodetechnologie, bekannt durch Etiketten oder Aufdrucke auf Lebensmitteln und Konsumgütern, oder finden z. B. bei der Zugangs- und Diebstahlsicherung, bei der Kennzeichnung von Tieren oder in der Automobilindustrie bei Wegfahrsperren Anwendung.

Schon in naher Zukunft sollen RFID den heutigen Strichcode verdrängen und in viele Bereiche des täglichen Lebens Einzug halten. Aktuell ist geplant, RFID u. a. auch zur Speicherung biometrischer Merkmale in Reisepässen (vgl. Nr. 6.2) oder zur Fälschungssicherung und somit zur Unterbindung des Schwarzhandels von Tickets, etwa zur WM 2006 (vgl. Nr. 5.3.7), einzusetzen. Die „allgegenwärtige“ Datenverarbeitung könnte mittels RFID in naher Zukunft bereits Realität sein. Die Befürchtungen sind deshalb groß, dass z. B. das Einkaufsverhalten von Kunden durch die an mitgeführten Gegenständen angebrachten RFID mit einer eindeutigen Seriennummer ausspioniert und unbemerkt detaillierte Kauf- oder Bewegungsprofile erstellt werden. Die RFID-Technologie wird bereits heute in vielen Logistiksystemen oder Fertigungsanlagen zur Identifizierung und Prozesssteuerung eingesetzt. Weltweit planen Konzerne den Einsatz von RFID zur Kontrolle der Warenströme bis hin zum Endkunden.

Insbesondere bei der großflächigen Einführung von RFID-Chips im Handel werden Aufklärungs- und Schutzmaßnahmen für Bürgerinnen und Bürger notwendig. Denn es besteht die Gefahr, dass RFID-Systeme personenbezogene (oder personenbeziehbare) Daten speichern, ohne dass Verarbeitungsvorgänge ausreichend transparent werden oder sogar Dritte diese Daten auslesen oder verändern können, ohne dass der Nutzer dies bemerkt oder unterbinden kann. Die Befürchtungen sind nicht übertrieben, da ein Zugriff auf die relativ robusten und langlebigen RFID bei einigen Systemen bis zu einigen Metern möglich ist.

Abbildung 2 (zu Nr. 4.2.1)

Miniaturisierter Funkchip



RFID existieren in Versionen mit und ohne eigene Stromversorgung. Letztere werden induktiv über ein Schreib-/Lesegerät über die „Luftschnittstelle“, also kontaktlos ohne Kabel, mit Strom versorgt. Zur Kennzeichnung von Waren und zur Automatisierung im Logistikbereich werden derzeit RFID verwendet, die über eine vom Hersteller vergebene eindeutige und nicht löschbare Seriennummer verfügen. Daneben existieren weitere Bauformen, die

über einen wiederbeschreibbaren Bereich verfügen und Daten bis zu einer Größenordnung von einigen hundert Byte aufnehmen können. Darauf können z. B. Informationen, wie etwa das Mindesthaltbarkeitsdatum von Tiefkühlwaren und auch personenbezogene Angaben gespeichert werden. Das Normungskonsortium EPC-Global (European Product Code-Global) will diesen Bereich zum Aufbringen des European Product Codes zur einheitlichen Warenkennzeichnung, ähnlich dem heute bekannten Strichcode, standardisieren. Der EPC kennzeichnet – im Gegensatz zum Strichcode, mit dem nur Warengruppen unterschieden werden – jedes einzelne Produkt mittels einer eindeutigen Produkt-ID. Diese ID kann von allen an einer Logistikkette teilnehmenden Partnern, also vom Hersteller eines Produktes bis zur Abfallentsorgung, zur eindeutigen Identifizierung genutzt werden.

Um größere Datenmengen, wie etwa biometrische Merkmale, auf einem RFID-Chip speichern und z. B. komplexe Verschlüsselungsfunktionen bereitstellen zu können, werden Smartcards ähnlich der in Mobiltelefonen eingesetzten Simkarten als RFID-Version verwendet. Diese Chips verfügen quasi über eigene „Intelligenz“ mit Mikroprozessor und Speicher und finden wegen der derzeit noch relativ hohen Kosten vornehmlich dort Anwendung, wo größere Datenmengen auf einem RFID nicht nur gespeichert, sondern auch weiter verarbeitet werden sollen, etwa in Ausweisdokumenten.

Im Gegensatz zu Mikrochips, die über Kontakte der Leiterbahnen mit einem Schreib-/Lesegerät kommunizieren, sind Daten auf RFID wegen der kontaktlosen Kommunikation weiteren Gefahren ausgesetzt. Wenn die Kommunikationsvorgänge ohne spezielle Absicherungen stattfinden, könnten diese auch von einem Dritten initiiert, abgehört oder manipuliert werden. Der Inhalt von Tags könnte unbemerkt abgefragt werden, da RFID einen Kommunikationsvorgang nicht signalisieren und bisher auch nicht über Mechanismen zur temporären oder endgültigen Deaktivierung verfügen. Ferner besteht die Gefahr, dass RIFD wegen ihrer geringen Abmessungen nicht als solche erkannt werden oder bereits unkenntlich in Produkte eingearbeitet sind. Auch die Lesegeräte könnten in alltägliche Gegenstände, etwa in Türrahmen, integriert werden.

Eine besondere Rolle beim Einsatz von RFID kommt der Verknüpfung mit Hintergrunddatenbanken zu. Gibt ein Kunde bei einem Bezahlvorgang seine Identität etwa durch Vorlegen einer Kunden-, EC- oder Kreditkarte preis, kann der Personenbezug zudem am bzw. im Artikel angebrachten RFID hergestellt und gespeichert werden. Die Person, die den entsprechenden Gegenstand mit sich führt, könnte auch von anderen Lesegeräten wegen der eindeutigen Seriennummer des Tags wiedererkannt werden. Ein Personenbezug, z. B. bis hin zur Kopplung mit Videokameras, war bereits Gegenstand von Feldversuchen im Handel.

Aus Sicht des Datenschutzes muss der Einsatz von RFID deshalb für die Betroffenen transparent erfolgen. Unzulässig wäre es, wenn RFID-Tags versteckt angebracht und verdeckt ausgelesen werden, Daten der RFID-Chips aus verschiedenen Produkten mit personenbezogenen Daten zusammengeführt oder Verhaltens-, Nutzungs- und Bewegungsprofile erzeugt und gespeichert werden.

Nur durch einen transparenten Umgang mit dieser Technologie können auch zukünftig die in den Datenschutzgesetzen geforderte Zweckbindung, Datensparsamkeit und Vertraulichkeit bei der Verarbeitung personenbezogener Daten sichergestellt werden. Bei der Verwendung komplexer RFID, die eine Verarbeitung von Daten ähnlich einer Smartcard ermöglichen, greifen bereits derzeit Regelungen des BDSG (§§ 3 Abs. 10 und 6c). Bei einfachen RFID mit unlöschbarer Seriennummer findet das BDSG allerdings keine direkte Anwendung, sofern keine Verknüpfung mit personenbezogenen Identifikationsdaten erfolgt. Hier ist aus Datenschutzsicht eine gesetzliche Kennzeichnungspflicht von Produkten, die RFID enthalten, sowie eine Kennzeichnung von Lese-/Schreibgeräten und Kenntlichmachung von Kommunikationsvorgängen angemessen, weil immer die Möglichkeit besteht, dass der Personenbezug nachträglich, ggf. durch unberechtigte Dritte, hergestellt wird. Sollten diese Datenschutzanforderungen nicht über eine Selbstregulierung und Selbstverpflichtung von Herstellern und Handel gewährleistet werden, hielte ich zur Gewährleistung des Rechts auf informationelle Selbstbestimmung eine gesetzliche Regelung im BDSG für notwendig.

Weiterführende Informationen zu RFID: Art. 29-Gruppe, WP 105, http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2005/wp105_en.pdf.

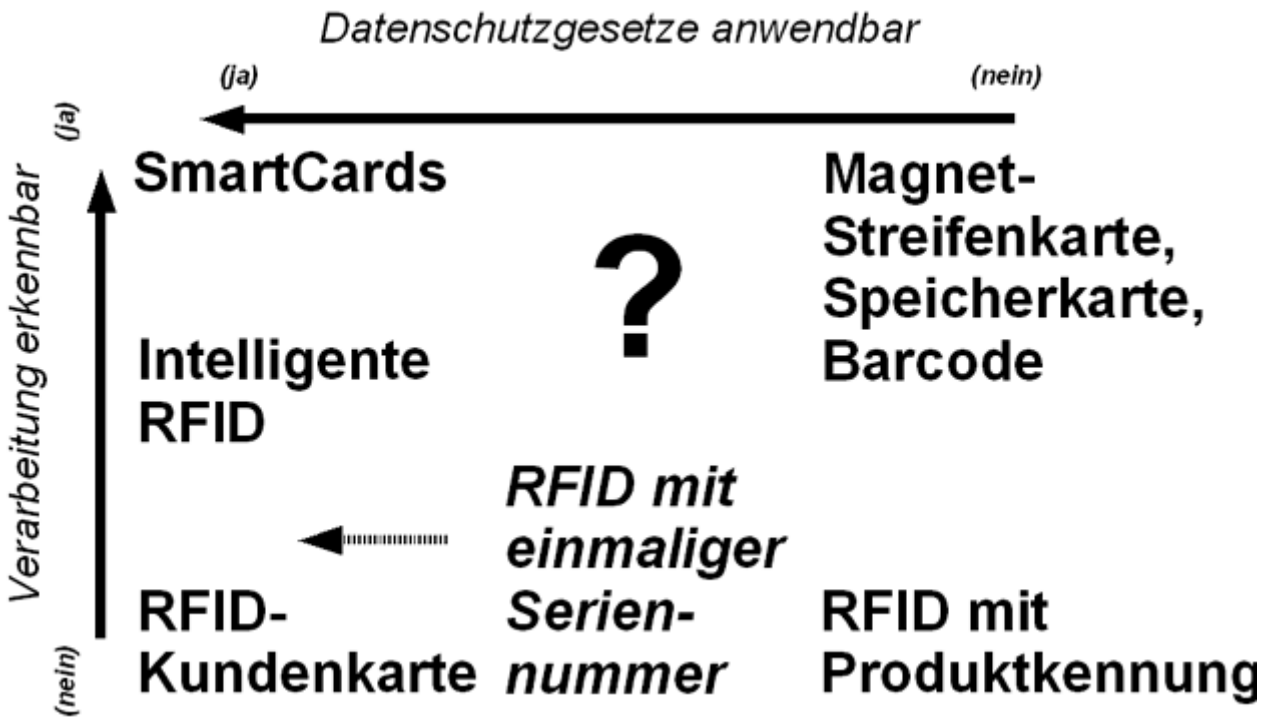
Kasten zu Nr. 4.2.1

Beim **Einsatz von RFID** sind Hersteller und Betreiber von RFID gekennzeichneten Waren und der Handel aufgefordert,

- die Betroffenen umfassend über Einsatz, Verwendungszweck und Inhalt von RFID-Chips zu informieren,
- Möglichkeiten zur Deaktivierung/Löschung von RFID-Chips zu schaffen, insbesondere dann, wenn Daten für die spezifischen Zwecke nicht mehr erforderlich sind,
- RFID Daten nur so lange zu speichern, wie es zur Erreichung des Zwecks erforderlich ist,
- bei RFID-Chips wirksame Blockierungsmechanismen, mit denen ein Auslesen der gespeicherten Daten unterbunden werden kann, zu entwickeln, so dass kein Nutzungszwang gegeben und anonymes Kaufen weiterhin möglich ist,
- die Vertraulichkeit der gespeicherten und der übertragenen Daten durch wirksame Authentisierung der beteiligten Geräte und Verschlüsselung sicherzustellen und
- bei RFID-Technologie mit Verarbeitungsfunktion Systeme anzubieten, die keine Seriennummer tragen, da eine eindeutige Identifikation eines Produkts nicht immer erforderlich ist.

Abbildung 3 (zu Nr. 4.2.1)

Anwendung der Datenschutzgesetze beim Einsatz von RFID



4.2.2 Biometrie vor dem Durchbruch?

Die Versprechen über Vorteile und Sicherheit der biometrischen Systeme werden mit der heute verfügbaren Technik nur bedingt gehalten.

Die Diskussion über Vor- und Nachteile des Einsatzes von Biometrie geht weiter (vgl. 19. TB Nr. 1.11). Diese Technologie eröffnet zwar ein sehr weiträumiges Spektrum von Anwendungsmöglichkeiten, etwa biometrische Zugangssysteme für Sicherheitsbereiche und Passwortersatz am Rechner, doch hat sie den Durchbruch noch nicht erreicht. Angesichts ihrer vielfältigen Einsatzmöglichkeiten wird die Biometrie auch für das Identitätsmanagement erheblich an Bedeutung gewinnen.

Die erste Massenanwendung wird voraussichtlich die Verwendung biometrischer Merkmale in Pässen und Ausweisen sein (vgl. Nr. 6.2). Inwieweit sich die Biometrie bei derartigen Massenanwendungen alltagstauglich erweisen wird, muss aber noch ermittelt werden. Neben den datenschutzrechtlichen Fragen stellen die Zuverlässigkeit der Systeme und der Kosten-/Nutzenaspekt die größte Hürde dar.

Die datenschutzrechtlichen Anforderungen an die im Ausweis einzusetzende Technik wurden in Stellungnahmen der Art. 29-Gruppe zur EU-Pass-Verordnung formuliert. Ich trete dafür ein, dass diese Anforderungen bei der Formulierung der technischen Feinkonzepte berücksichtigt und dem Stand der Technik entsprechend weiterentwickelt werden (z. B. Schutz der biometrischen Daten auf einem RFID-Chip gegen Manipulation und heimliches Auslesen).

Im Bereich des Bundes wurden im Berichtszeitraum verschiedene Tests mit biometrischen Systemen durchgeführt. Sie sollten u. a. die Nutzbarkeit/Einsatztauglichkeit der Systeme für Ausweisdokumente prüfen. Die getesteten Systeme haben als biometrische Merkmale Gesicht, Finger und Iris eingesetzt. Die Tests haben Hinweise auf noch weitgehend ungelöste Probleme ergeben; so ist bei der Fingerabdruck- und auch bei der Iriserkennung nicht zu vermeiden, dass einige Personen grundsätzlich nicht erfasst werden können, weil Merkmale fehlen oder nicht ausgeprägt sind. Bei der Fingerabdruckerkennung ist die Erkennungsleistung bei bestimmten Berufsgruppen nicht gewährleistet und nimmt zudem mit dem Alter der Anwender ab. Bei der Gesichtserkennung treten häufig system- und umgebungsbedingte Schwierigkeiten auf. Die Lichtempfindlichkeit der Systeme ist sehr hoch, hier ist deshalb die optimale Ausleuchtung – sowohl bei der Erstellung der Referenzbilder, als auch bei der späteren

Verifikation – notwendig. Auch ist die Verwechselungswahrscheinlichkeit bei Brillenträgern mit bestimmten Brillentypen sehr hoch. Bei der Iriserkennung wurde eine schlechtere Erkennungsleistung für Brillenträger festgestellt und es treten erhebliche Bedienungsschwierigkeiten bei Anwendern auf, die das System nur selten nutzen.

Der größte Mangel der Systeme wurde bei Tests der Überwindungssicherheit deutlich: Bei der Fingerabdruckerkennung waren Überwindungsversuche mit einfachen Mitteln erfolgreich, die selbst geschultem Grenzpersonal nicht auffallen würden. Die Überwindungssicherheit bei der Iriserkennung ist weitaus höher als bei anderen biometrischen Merkmalen.

Die hierbei aufgefallenen Schwachstellen sind nicht nur unter Datenschutzgesichtspunkten kritisch zu beurteilen, sondern auch im Hinblick auf die anstehenden Sicherheitsaspekte.

Vgl. hierzu auch den TAB-Arbeitsbericht Nr. 93 „Biometrie und Ausweisdokumente“, Bundestagsdrucksache 15/4000, www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf; TAB-Brief Nr. 26, Juni 2004, S. 22 „Biometrische Ausweisdokumente kommen“; Stellungnahme der Art. 29-Gruppe, www.bfd.bund.de/information/sn-7-2004-art2.html.

4.2.3 USB-Sticks am Arbeitsplatz: Neue Technik – alte Gefahren!

Die Verwendung von USB-Anschlüssen ist mit vielen Risiken aber auch mit Vorteilen verbunden. Den Risiken muss mit angemessenen Maßnahmen begegnet werden.

Praktisch jeder derzeit verkaufte PC ist ausschließlich mit USB (Universal Serial Bus)-Schnittstellen ausgestattet, über die externe Geräte wie Tastatur, Maus und Arbeitsplatzdrucker angeschlossen werden.

Mit dem USB-Anschluss steht dem Benutzer in der Regel ein universeller Anschluss für eine Vielzahl von Hardwarekomponenten zur Verfügung. Die Betriebssystemunterstützung ist in der Regel so ausgelegt, dass USB-Geräte vom PC selbstständig erkannt werden und sofort betriebsbereit sind. Sicherheitsrelevant sind insbesondere Netzwerkadapter, Modems oder ISDN-Adapter, da mit ihnen unerlaubte „Seiteneingänge“ in das behördliche oder betriebliche Netz geschaffen werden können, die die zentralen Sicherheitseinrichtungen unterlaufen. Auch über USB anschließbare Speichermedien – so genannte memory sticks – bergen Sicherheitsrisiken in sich. Memory sticks sind Geräte in der Größe eines Schlüsselanhängers, die über einen Speicher von derzeit bis zu einem GB verfügen. Sie werden vom PC technisch wie eine Festplatte angesprochen. Kritisch wäre es, wenn auf ihnen unzulässigerweise schutzwürdige Daten gespeichert werden oder wenn nicht freigegebene Programme auf diese Weise in das dienstliche System eingeschleust werden oder wenn Betriebssysteme gestartet werden, mit denen Sicherheitsmechanismen unterlaufen werden können. Auch mobile Festplatten in der Größe einer EC-Karte mit einer Speicherkapazität von bis zu 80 GB hält der Markt bereit. Über solche Geräte lassen sich ganze Datenbanken aus dem System kopieren.

Neben diesen Risiken eröffnet diese neue Technik aber auch Möglichkeiten für die Datensicherheit. So erscheint es durchaus sinnvoll, besonders vertrauliche Datenbestände auf memory sticks oder USB-Festplatten zu speichern. Den physischen Zugriff auf dieses Medium kann man auf einfache Weise einschränken und so die Chancen eines potenziellen Angreifers mindern. Der Zugang kann auch über ein biometrisches Merkmal wie den Fingerabdruck abgesichert werden, so dass nur berechtigte Personen darauf zugreifen können. Auch die Authentifizierung und damit der Zugang zum Rechner kann über den USB-Anschluss technisch abgesichert werden. Grundsätzlich sollte beim Einsatz von USB-Sticks oder USB-Festplatten die Speicherung immer verschlüsselt erfolgen, um bei Verlust des Mediums unbefugte Zugriffe zu verhindern.

Weiterführende Information: Orientierungshilfe „Datensicherheit bei USB-Geräten“ des Arbeitskreises „Technische und organisatorische Datenschutzfragen“ des Bundes und der Länder http://www.bfd.bund.de/technik/usb.pdf.

4.2.4 Funknetze (WLAN) im täglichen Einsatz, immer ein Risiko?

Funknetze stellen eine kostengünstige Möglichkeit dar, ein Netzwerk schnell und flexibel aufzubauen. Eine Orientierungshilfe gibt Hinweise zum sicheren Betrieb von Funknetzen.

„Anytime, Anywhere“ ist das Stichwort für die mobile Kommunikation. Diese Vision ist Realität geworden: Die mobile Nutzung elektronischer Dienste ist heute gängige Praxis. Die Möglichkeiten gehen dabei weit über das einfache Telefonieren hinaus: Personal Digital Assistents (PDA) lotsen Autofahrer und Fußgänger durch Straßennetze, Handys senden und empfangen E-Mails, Notebooks eröffnen im Cafe, Restaurant oder im Hotel den Zugang ins Internet. Die Anwendungen sind vielfältig. Notwendige Basis für die meisten der mobil nutzbaren Dienste ist eine Vernetzung der Kommunikationsgeräte. Dafür existieren neben den Mobilfunknetzen für die Telefonie (GSM, GPRS) zunehmend andere Technologien für die lokal begrenzte Kommunikation (z. B. Wireless Local Area Network – WLAN oder Bluetooth).

Durch die drahtlose Kommunikationsinfrastruktur werden Komfort, Effizienz und Flexibilität verbessert. Arbeitsplätze können kurzfristig ohne kostenintensive Neuverkabelung eingerichtet werden; in denkmalgeschützten Gebäuden wird eine Vernetzung von Arbeitsplätzen untereinander oft erst durch diese Infrastruktur ermöglicht. Mobile Arbeitskräfte, z. B. Außendienstmitarbeiter können problemlos mit ihrem Notebook am Firmennetz teilnehmen, sobald sie in der Firma tätig sind.

Leider wird diese Verbesserung von Mobilität und Flexibilität oft durch einen Sicherheitsverlust für die via Funk übertragenen Daten sowie die drahtgebundenen Netze, an die die Funkkomponenten angeschlossen sind, erkauft.

Zudem besteht die Gefahr von Verlust oder Diebstahl mobiler Endgeräte und somit der darauf gespeicherten Daten. Für den Datenschutz und die Datensicherheit ist der Vorteil der drahtlosen Kommunikation gleichzeitig eine Gefahr: Es besteht keine direkte physikalische Verbindung der Geräte untereinander; sie sind Teilnehmer an einem offenen Medium. Offen bedeutet dabei, dass eine räumliche Begrenzung auf bestimmte Bereiche, z. B. nur die Geschäftsräume eines Unternehmens, nahezu unmöglich ist. Funkwellen breiten sich unkontrolliert und unbegrenzt aus. Ist ein Gebäude komplett mit der Funkinfrastruktur „ausgeleuchtet", so ist mit an Sicherheit grenzender Wahrscheinlichkeit auch immer außerhalb des Gebäudes ein Empfang der Funkwellen möglich. Angriffe auf die Daten in Form von Mitschnitten, Auswertungen und Manipulationen sind möglich. Denial-of-Service-Attacken (DoS-Attacken) sind in ungeschützten Funknetzen relativ einfach durchführbar, ebenso wie Man-in-the-middle-Attacken, bei denen durch geschickte Positionierung von Funkkomponenten echte Gegenstellen vorgegaukelt werden und dadurch z. B. die Datenübertragung zu bestimmten Netz-Segmenten protokolliert oder blockiert werden kann. Große Sicherheitsrisiken bestehen bereits, wenn Geräte „Out-Of-The-Box" eingesetzt werden, also ohne Anpassung der Konfiguration und mit „Default"-Passwörtern. Auch wer sich auf die eingebauten, im jeweiligen Standard definierten Sicherheitsmechanismen verlässt, ist oft nicht sicher.

Zwar unterstützen die gängigen WLAN-Komponenten lediglich das Wired Equivalent Privacy (WEP) – Verfahren, das im Standard zu WLAN festgeschriebene Verschlüsselungsverfahren, doch selbst dies ist in der Voreinstellung der meisten Access-Points und WLAN-Karten deaktiviert. Zudem bietet es keine hinreichende Sicherheit, wenn im Netz sensible Daten übertragen werden sollen. Entsprechende Angriffswerkzeuge und Informationen darüber, wie diese einzusetzen sind, können leicht aus dem Internet heruntergeladen werden. Werden zusätzlich herstellerspezifische, außerhalb des jeweiligen Standards liegende Sicherungsmöglichkeiten angeboten, ist eine genaue Prüfung dieser Mechanismen wichtig. So kann es beispielsweise sein, dass bestimmte Sicherungsmechanismen (bei WLAN-Technologien) nur zwischen Client und Access-Point funktionieren, die gleichen Mechanismen zwischen Access-Points (wenn diese z.B. als Funkbridge eingesetzt werden) aber nicht möglich sind. Hintergrundinformationen kann hier in vielen Fällen das Internet liefern.

Die Angriffsszenarien ließen sich hier beliebig fortführen. Wie bereits dargestellt, reichen in der Regel die voreingestellten Sicherheitseinstellungen der Geräte nicht aus, um sich gegen Angriffe zu schützen. Jeder Anwender muss wissen, dass Funknetze nur mit zusätzlichen Sicherheitsmaßnahmen den Anforderungen des Datenschutzes genügen.

Weiterführende Information: Orientierungshilfe „Datenschutz in drahtlosen Netzen" des Arbeitskreises „Technische und organisatorische Datenschutzfragen" des Bundes und der Länder http://www.bfd.bund.de/technik/oh_funknetze.pdf.

Kasten zu Nr. 4.2.4

WLAN: So können Sie sich schützen

- Standard-Netzwerknamen ändern
- Standard-Passworte an allen Komponenten ändern
- MAC-Adress-Filterung einschalten
- WEP Verschlüsselung mit maximaler Schlüssellänge einschalten und Schlüssel periodisch wechseln
- Sendeleistung am Access-Point optimieren
- DHCP-Server am Access-Point abschalten
- Funk-LAN-Komponenten nur bei Gebrauch einschalten
- Konfiguration des Access-Point nur über sichere Kanäle (SSL benutzen)
- Zusätzliche Verschlüsselung (VPN-Tunnel) verwenden
- Einsatz eines Authentifikations-Servers (Radius-Server)
- Alle Clients vor Computerviren schützen

4.3 Kontroll- und Beratungsbesuche

4.3.1 Zur Frage des Einsatzes von Hack- und Crackwerkzeugen

Der Einsatz von Hack- und Crackwerkzeugen bei Kontrollen ist kritisch zu sehen. Gleichwohl gibt es Situationen, in denen solche Werkzeuge Erkenntnisse über die Unsicherheiten in einem Netz liefern können.

Bei einer Kontrolle im Personalbereich fanden meine Mitarbeiter offene CD-ROM-Laufwerke mit der Möglichkeit, den Startvorgang durch Änderung der BIOS-Konfiguration von diesen Laufwerken auszuführen (vgl. hierzu auch Nr. 4.3.2). Um eventuell vorhandene weitere Sicherheitslücken erkennen zu können, haben meine Mitarbeiter den Startvorgang mittels einer speziellen CD Live Linux Knoppix, die vom BSI 2002 herausgegebenen worden ist, vorgenommen. Durch Starten mit „Knoppix" konnten die lokalen Zugriffsbeschränkungen umgangen und auf eine Vielzahl von Daten, sowohl auf der lokalen Festplatte wie im Netzwerk, zugegriffen werden. Da das CD-ROM-Laufwerk nicht gesichert war, konnte mit der Knoppix-CD festgestellt werden, ob der Rechner und welche Programme sich starten ließen sowie welche Daten im Netzwerk im direkten Zugriff waren.

Die mit der CD gefundenen Sicherheitslücken habe ich gegenüber der verantwortlichen Stelle beanstandet. Diese monierte, ich hätte bei der Kontrolle Hack- und Crackwerkzeuge eingesetzt, die zu Beeinträchtigungen des IT-Betriebes geführt hätten. Selbstverständlich ist die von mir verwendete Software kein „Hack- und Crackwerkzeug", wie dies im Internet oftmals angeboten wird. Meines Erachtens sollte jeder, der für IT-Sicherheit zuständig ist, Werkzeuge wie nessus, etherreal oder airsnort einsetzen, um ein realistisches Bild vom Sicherheitsniveau eines

Systems zu erhalten und um ggf. gezielt Gegenmaßnahmen ergreifen zu können. Insoweit unterstütze ich den Einsatz von Knoppix für Sicherheitsüberprüfungen und werde auch in Zukunft ggf. darauf zurückgreifen.

Im übrigen stehen Werkzeuge zum Sicherheitscheck von Systemen bereits seit Längerem zur Verfügung:

– als Bestandteil bekannter Universal-Distributionen (z. B. SUSE-Edition),

– als Bestandteil von speziellen sicherheitsorientierten Minimaldistributionen wie Trinux,

– als separate Tools frei verfügbar in verschiedenen Systemumgebungen, auch unter MS-Windows.

Kann der Anwender beliebige Programme ausführen oder ist das Booten einer CD möglich, ist dies häufig auf Defizite im administrativen Bereich zurückzuführen. Dies führt dann zu einer Bedrohung durch die entsprechenden Tools. Das bedeutet auch, dass das Starten des Betriebssystems von einem externen Datenträger aus unterbunden werden muss.

Meine Mitarbeiter halten sich bei Kontrollen an folgende Regeln:

- Die eingesetzten Programme verändern keine Systeme, Systemparameter und/oder Systemkonfigurationen, Programme und/oder Daten.
- Die Herkunft der Programme ist zweifelsfrei geklärt, und die Programme sind frei von Schadensfunktionen (Viren, Trojaner).
- Direkte Angriffswerkzeuge, die über das Ausnutzen von Sicherheitslücken hinausgehen, werden nicht eingesetzt. Hierzu zählen beispielsweise Passwortcracker, soweit sie nicht auf Trivialpasswörter testen.
- Es werden Programme eingesetzt, die versuchen, Dateien zu lesen, zu ändern oder auf Datenbanken zuzugreifen. Nur so können Konfigurationseinstellungen oder geschützte/ungeschützte Anwendungsdaten überprüft werden.

Grundsätzlich sollte jede IT-Administration mit den hier genannten Tools vertraut sein. Mit ihnen können Schwachstellen gefunden, echte Angriffe besser verstanden und hoffentlich verhindert werden.

4.3.2 Ungeschützte Laufwerke in Rechnernetzen – unkalkulierbares Risiko

Nach wie vor muss ich bei Kontrollen feststellen, dass Laufwerke mit Personaldaten ohne besondere Sicherheitsmechanismen in Rechnernetzen allen Benutzern zur Verfügung gestellt wurden. Mit dieser Praxis sind große Sicherheitsrisiken verbunden.

Die Verarbeitung von Personaldaten erfolgt inzwischen weitgehend elektronisch. Vor diesem Hintergrund habe ich im Berichtszeitraum vermehrt die Sicherheit der Datenverarbeitung im Personalbereich kontrolliert. Hierbei habe ich festgestellt, dass in Behörden des Bundes – insbesondere im Bereich der Personalverwaltung – Mängel im Umgang mit Mitarbeiterdaten bestehen, deren Beseitigung ich zum Teil schon vor Jahren angemahnt hatte.

Allerdings habe ich auch feststellen können, dass sich die Sensibilität der Mitarbeiterinnen und Mitarbeiter in den Behörden hinsichtlich der Datensicherheit zumindest im konventionellen Verfahren deutlich erhöht hat. Die sichere Verwaltung von Personaldaten auf Papier oder das Wegschließen von Akten nach Dienstschluss wird in den überwiegenden Fällen als Selbstverständlichkeit angesehen.

In den meisten Fällen gibt es zwar Dienstanweisungen über den sicheren und datenschutzgerechten Umgang mit Personaldaten, die technisch-organisatorische Umsetzung entspricht diesen aber leider nicht immer.

So genügte die Passwortvergabe nicht in allen Fällen den datenschutzrechtlichen Anforderungen. Unter diesen Umständen wäre es den Mitarbeiterinnen und Mitarbeitern oder sogar dritten Personen ohne viel Aufwand möglich gewesen, unbefugt Personaldaten zu lesen und zu ändern. Im Zugriff waren dabei auch sensible Daten aus dem Disziplinarbereich, Beurteilungen von Mitarbeitern, Protokolle von Personalführungsgesprächen und medizinische Daten. In einem schwerwiegenden Fall habe ich dies beanstandet.

Weitere gravierende Feststellungen bei Kontrollen waren:

– Benutzerrechte waren mangelhaft festgelegt. Nach den datenschutzrechtlichen Vorgaben dürfen Mitarbeiterdaten nur auf einem Server abgelegt werden, der dem Personalwesen zugeordnet ist. Eine Datenspeicherung auf der lokalen Festplatte ist datenschutzrechtlich nicht vertretbar. In dem geprüften Fall hatten die Benutzer jedoch die Vorgabe, Mitarbeiterdateien, z. B. Word- und Exceldateien, immer auf der lokalen Festplatte zu speichern. Die lokale Festplatte war aber auch für den Zugriff anderer Benutzer im Netzwerk freigegeben, mit der Folge, dass auch Benutzer, die nicht im Personalbereich tätig waren, diese Dateien lesen konnten. Um eine saubere Trennung von Benutzer-, Mitarbeiter- und projektspezifischen Daten untereinander sowie von Programmen und Daten des Betriebssystems durchzusetzen, sollte dafür auf dem Personalserver eine geeignete Verzeichnis- und Dateistruktur festgelegt werden, mit der eine datenschutzgerechte Dateiablage unterstützt wird. Dies wird in vielen Fällen nicht beachtet, was dazu führt, dass jeder Mitarbeiter eine eigene Verzeichnisstruktur und Dateiablage anlegt, wofür in der Mehrzahl der Fälle die lokale Festplatte verwendet wird.

  Bei der Verarbeitung von Personaldaten müssen die Vorgaben des Bundesbeamtengesetzes (§ 90 ff.) berücksichtigt werden. Dies erfordert besondere technisch-organisatorische Maßnahmen, beispielsweise die Abschottung des Personalbereiches von den restlichen Organisationsbereichen im Netzwerk und die Abschottung besonders sensibler Daten wie Disziplinarangelegenheiten, Beihilfedaten und Leistungsbeurteilungen von den restlichen Daten im Personalwesen. Zu einer sachgerechten Umsetzung müssen entsprechende Anweisungen an alle Mitarbeiter im Personalwesen gegeben und in Abstimmung mit der Administration eine geeignete Dateiablage eingerichtet werden.

– Bei einigen im Personalwesen eingesetzten PC fand ich ungesicherte Disketten- und CD-ROM-Laufwerke. Dies war in einem Fall deshalb besonders gravierend, weil außerdem noch der Zugriff auf die Startoptionen (BIOS-Einstellungen) des Rechners möglich war. Der Startvorgang des Rechners erfolgt in der Regel von der lokalen Festplatte, kann aber über Änderung an der PC-Konfiguration (BIOS-Einstellungen) auch vom CD-ROM-Laufwerk, von der USB-Schnittstelle (vgl. hierzu Nr. 4.2.3) oder dem Diskettenlaufwerk ausgeführt werden. Die Änderung dieser Startoption war bei allen geprüften PC im Personalbereich möglich. So konnte unter Umgehung der installierten Zugriffsbeschränkungen auf alle Dateien des PC sowie auf die offenen Laufwerke im Netzwerk zugegriffen werden.

4.3.3 Windows XP sicher nutzen

Das meist verbreitete PC-Betriebssystem der Firma Microsoft, Windows XP, muss durch regelmäßige Updates und durch Installation von Zusatz-Sicherheitstools ergänzt werden, wenn personenbezogene Daten verarbeitet werden sollen.

Der überwiegende Teil aller neuen PC wird mit dem vorinstallierten Betriebssystem Windows XP der Firma Microsoft ausgeliefert und ist nicht zuletzt deshalb Ziel für viele Angriffe. Der Nutzer ist daher weiterhin gehalten, sich um die Sicherheit seines PC selbst zu kümmern. Hier bietet die Orientierungshilfe „Datenschutz bei Windows XP professional“ des Landesbeauftragten für Datenschutz Mecklenburg-Vorpommern Hinweise zur Verbesserung der IT-Sicherheit mit besonderer Berücksichtigung datenschutzrelevanter Aspekte.

Sicherheitsupdates sollten immer durchgeführt werden. Allerdings müssen die Hersteller von Betriebssystem- und Anwendungs-Software für den Anwender transparente Update-Verfahren anbieten. Beispielsweise sollten bei Software-Updates benutzerinitiierte und überprüfbare Update-Verfahren zum Einsatz kommen. Zusätzlich müssen auch weiterhin datenträgerbasierte Update-Verfahren angeboten werden, bei denen nur die für den Datenträgerversand notwendigen Anwenderdaten übertragen werden. Insbesondere haben die Anbieter zu gewährleisten, dass bei allen Update-Verfahren personenbezogene Daten nur übermittelt werden, wenn der Verwendungszweck bekannt ist und der Nutzer in die Verarbeitung eingewilligt hat.

Weiterführende Hinweise:
Orientierungshilfe „Datenschutz bei Windows XP professional“ des Landesbeauftragten für Datenschutz Mecklenburg-Vorpommern: http://www.lfd.m-v.de/informat/dsbeiwxp/oh_wxp.html

Weitere Informationen – auch zu aktuellen Programmen mit Schadensfunktionen – finden Sie beim BSI unter http://www.bsi.de/av/ und http://www.bsi-fuer-buerger.de/toolbox/

Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zum automatischen Software-Update vom 7. August 2003: http://www.bfd.bund.de/information/DS-Konferenzen/65_66_ent4.pdf

Kasten zu Nr. 4.3.3

Nutzerinnen und Nutzer sollten folgende Grundregeln beachten:

– Begrenzen Sie die Zugriffsberechtigungen: Nach der Installation von Windows XP startet der PC automatisch mit Administratorrechten. Für die tägliche Arbeit richten Sie sich ein Benutzerkonto mit eingeschränkten Rechten ein. So hat auch ein Eindringling nur beschränkte Rechte.

– Richten Sie eine Firewall ein: Die Firewall kontrolliert den zwischen PC und Internet ausgetauschten Datenfluss. So können Sie selbst festlegen, welches Programm Kontakte ins Internet aufnehmen darf und welches nicht.

– Installieren Sie Viren-Schutzprogramme: Viren-Schutzprogramme sollten stets aktiviert sein. Dieser Schutz funktioniert nur, wenn Informationen über Schädlinge regelmäßig aktualisiert werden. Spyware spioniert ihren Computer aus. Dabei werden Daten gesammelt und an eine Adresse ins Internet verschickt. Dagegen helfen Programme, mit denen sich die Spyware entfernen lässt.

– Konfigurieren Sie Ihre Browser- und Mailsoftware: Alle gängigen Programme, mit denen Sie ins Internet „gehen“, sollten Sie so konfigurieren, dass ein Höchstmaß an Sicherheit gewährleistet ist. Ggf. bietet es sich auch an, Alternativen für die ausgelieferte Software Outlook und Internet Explorer zu verwenden, die auf Grund ihrer Verbreitung bei Hackern besonders beliebt sind.

– Kontrollieren Sie Ihre E-Mailanhänge: Schädlinge gelangen auch als Anhänge (Attachments) von E-Mails auf den PC. Ein Viren-Schutzprogramm, das permanent im Hintergrund läuft, ist auch hier eine gute Vorsorge. Zusätzlich ist aber auch der Nutzer zur Vorsicht aufgerufen, insbesondere bei unbekannten E-Mailadressen mit Anhängen. Aber auch bei bekannten E-Mailadressen ist Vorsicht geboten, denn der PC des Absenders könnte mit einem Wurm infiziert sein, der automatisch diese E-Mail generiert hat. Richten Sie Ihr Mailprogramm so ein, dass E-Mails standardmäßig nicht im html-Format angezeigt werden.

– Führen Sie regelmäßige Datensicherungsmaßnahmen durch: Regelmäßige Datensicherungsmaßnahmen, insbesondere Backups für alle wichtigen Daten, auf externe Medien bewahren Sie vor unheilsamen Überraschungen, vor allem bei der Installation neuer Programme und bei Updates.

4.3.4 LINUX datenschutzgerecht einsetzen

Zunehmend wird das Betriebssystem Linux auch in der öffentlichen Verwaltung eingesetzt. Wie man den Einsatz datenschutzgerecht gestaltet, soll hier geschildert werden. Gleichzeitig gibt es zu diesem Thema ein Angebot im Internet.

In der öffentlichen Verwaltung wird zunehmend das Betriebsystem Linux eingesetzt. Meine Länderkollegen und ich haben eine gemeinsame Arbeitsgruppe gegründet, um den Behörden zur besseren Orientierung eine Hilfe an die Hand zu geben und der weiteren Verbreitung Rechnung zu tragen. Damit soll ein besonders datenschutzgerechter Einsatz des Linux-Systems erfolgen. Für andere Betriebssysteme ist ein zwischen den Datenschutzbeauftragten abgestimmter Leitfaden bisher noch nicht verfügbar.

Die Dokumente sind auf einem im Internet verfügbaren Rechner abgelegt. Zurzeit erarbeitet die Gruppe die Version 1. Die Orientierungshilfe Linux gibt einen Überblick über das Linux-System unter datenschutzrechtlichen Aspekten.

Das Angebot ist im Internet unter https://info.bfd.bund.de abrufbar. Da es nach der Erstellung der Version 1 allgemein zugänglich sein wird (auch zum Einbringen von Kommentaren), ist dies gleichzeitig ein Angebot der Initiative BundOnline 2005.

5 Innere Sicherheit

5.1 Neue Sicherheitsarchitektur

5.1.1 Intensivierung der Zusammenarbeit der Sicherheitsbehörden zur Terrorismusbekämpfung

Eine Intensivierung der Zusammenarbeit zwischen Polizei und Nachrichtendiensten ist nur in engen datenschutzrechtlichen Grenzen vertretbar.

Zur Bekämpfung des internationalen Terrorismus soll nach den Beschlüssen der Innenministerkonferenz die Zusammenarbeit von Polizei und Nachrichtendiensten des Bundes und der Länder intensiviert und eine „Neue Sicherheitsarchitektur“ geschaffen werden.

Ein wichtiger Baustein dieser neuen Sicherheitsarchitektur ist das im Dezember 2004 in Berlin neu errichtete Terrorismusabwehrzentrum. In zwei getrennten Auswertungs- und Analysezentren sollen jeweils die Spezial- und Analyseeinheiten des BKA und des BfV zum Zweck der Gefährdungsbewertung, des operativen Informationsaustauschs, der Fallauswertung, der Erstellung von Strukturanalysen sowie zur Aufklärung des islamistisch-terroristischen Personenpotentials kontinuierlich und intensiv zusammenarbeiten. Einbezogen in diese Tätigkeit sind der BND, der BGS, das Zollkriminalamt, der MAD, die Verfassungsschutzbehörden der Länder sowie die Landeskriminalämter.

Ich halte eine derartige Kooperation für datenschutzrechtlich vertretbar, sofern das verfassungsrechtliche Trennungsgebot beachtet wird und besondere zusätzliche Vorkehrungen getroffen werden, die einen Missbrauch der Daten ausschließen. Aus dem Trennungsgebot folgt nicht nur die Verpflichtung zur organisatorischen Trennung von Polizei- und Nachrichtendiensten. Das Trennungsgebot, das auf den sog. Polizeibrief der Alliierten von 1949 zurückgeht, bestimmt auch die Grenzen der informationellen Zusammenarbeit von Polizei und Nachrichtendiensten. So darf sich beispielsweise der Verfassungsschutz nicht über eine gemeinsame Datei der Datenerhebungsbefugnisse der Polizei bedienen. Umgekehrt ist es der Polizei versagt, auf diesem Wege generell auf Daten zuzugreifen, die sie aufgrund ihrer Aufgaben und Kompetenzen nicht erheben dürfte und die von einem Nachrichtendienst unter Einsatz nachrichtendienstlicher Mittel gewonnen wurden. Das Trennungsgebot hat demnach wesentliche Auswirkungen auf die unter Federführung des BMI 2004 begonnenen Beratungen zur Schaffung gesetzlicher Grundlagen für gemeinsame Projektdateien sowie für eine gemeinsame Indexdatei von Polizei und Nachrichtendiensten.

Nach dem derzeitigen Beratungsstand sollen gemeinsame Projektdateien sowohl unter der Leitung des BKA, des BfV als auch des BND geführt werden können. Da die geltenden Polizei- und Dienstegesetze des Bundes einen wechselseitigen Zugriff auf die bei Polizei und Nachrichtendiensten geführten Informationssysteme nicht vorsehen, müssen im BKAG, BVerfSchG und BNDG entsprechende Rechtsgrundlagen geschaffen werden. Um deren inhaltliche Ausgestaltung wurde unter Federführung des BMI bei Redaktionsschluss noch gerungen. Auf eine gemeinsame Projektdatei sollen – jedenfalls nach Vorstellung des BMI – alle an dieser Datei beteiligten Polizeibehörden und Nachrichtendienste im automatisierten Verfahren lesenden und schreibenden Zugriff erhalten.

Aufgrund des Trennungsgebotes und im Hinblick auf das vom Bundesverfassungsgericht im Volkszählungsurteil (BVerfGE 65, 1, 43 ff.) postulierte Prinzip der informationellen Gewaltenteilung sind insbesondere die geltenden Aufgaben-, Befugnis- und Übermittlungsvorschriften strikt zu beachten. Demnach dürfen die beteiligten Behörden personenbezogene Daten in der gemeinsamen Datei nur speichern, sofern sie die einzustellenden Daten nach den geltenden Übermittlungsvorschriften allen anderen teilnehmenden Behörden übermitteln dürfen. Gemeinsame Dateien dürfen nur projektorientiert zur Bekämpfung des internationalen Terrorismus und des ihn unterstützenden Extremismus errichtet werden. Sie sind nur als ultima ratio zulässig. Strikt zu wahren ist auch die Zweckbindung der Daten. Die Herkunft der Daten muss im gesamten Verarbeitungsprozess durch eine entsprechende Kennzeichnung ersichtlich sein. Zudem muss stets erkennbar sein, welche Stelle die Daten weitergegeben hat. Zum Zweck einer effektiven datenschutzrechtlichen Kontrolle muss eine umfassende Vollprotokollierung aller Zugriffe erfolgen. Die Rechte der durch die Datenverarbeitung Betroffenen, insbesondere das Auskunftsrecht, sind uneingeschränkt zu gewährleisten. Nach Ablauf einer an-

gemessenen Höchstspeicherfrist, die sich aus der Dauer des Projektes ergibt, sind die Daten zu löschen.

Brisanter ist die Schaffung einer umfassenden gemeinsamen Indexdatei von Polizei und Nachrichtendiensten, die zeitlich nicht befristet sein soll. Zwar sollen in dieser Datei lediglich Fundstellenhinweise auf Informationen aufgenommen werden, die in polizeilichen oder nachrichtendienstlichen Sammlungen gespeichert sind. Gleichwohl weisen auch die Indexdaten einen deutlichen Inhaltsbezug auf, z. B. weil das Aktenzeichen eine eindeutige Zuordnung der jeweiligen Person zu bestimmten Fall- und Deliktgruppen erlaubt. Das erklärte Ziel dieser Datei ist es, den beteiligten Behörden zu ermöglichen, sich schnell davon Kenntnis zu verschaffen, wo welche Informationen zu bestimmten Personen vorhanden sind. Ob diese Informationen übermittelt werden sollen, entscheidet die verantwortliche Stelle auf Basis der für sie einschlägigen Rechtsvorschriften. Nach Auffassung des BMI sollen in der Indexdatei auch solche personenbezogenen Daten gespeichert werden – und damit zur Kenntnis der anderen Beteiligten gelangen –, die die verantwortliche Stelle nach den geltenden Übermittlungsvorschriften an die anderen beteiligten Behörden nicht übermitteln dürfte. Nach meiner Auffassung muss die Befugnis zur Datenspeicherung in der Indexdatei ebenso wie bei den Projektdateien auf diejenigen Daten beschränkt werden, die die speichernde Behörde aufgrund der hierfür geltenden Vorschriften an alle anderen teilnehmenden Behörden übermitteln darf und die zum Auffinden einer Aktenfundstelle erforderlich sind. Die Beschränkung ist auch deshalb erforderlich, da es keinen Sinn macht, solche Hinweiseinträge in die gemeinsame Indexdatei einzustellen, zu denen den übrigen beteiligten Stellen die vollständigen Daten nicht übermittelt werden dürften.

Inwieweit das BMI meinen Anregungen folgt, stand bei Redaktionsschluss noch nicht fest.

5.1.2 Auswirkungen der Rechtsprechung des Bundesverfassungsgerichts auf Eingriffsbefugnisse zu präventiven Zwecken

Das Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung („Großer Lauschangriff") hat gravierende Auswirkungen auf die Ausgestaltung präventiver Eingriffsbefugnisse.

Das Urteil des BVerfG vom 3. März 2004 (1 BvR 2378/98) zur akustischen Wohnraumüberwachung betrifft zwar unmittelbar das Recht auf unbeobachtete Kommunikation in den durch Artikel 13 GG geschützten Räumen sowie die verfassungsrechtlichen Anforderungen an den Einsatz technischer Mittel zum Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes in diesem Bereich (vgl. Nr. 7.1.1). Die Bedeutung des Urteils betrifft jedoch auch die Ausgestaltung verdeckter Eingriffsbefugnisse von Polizei und Nachrichtendiensten des Bundes und der Länder.

Kasten a zu Nr. 5.1.2

67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25. und 26. März 2004

Entschließung:
Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff und zur präventiven Telekommunikationsüberwachung

Das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zum Großen Lauschangriff ist ein wichtiger Orientierungspunkt in der rechts- und sicherheitspolitischen Diskussion um den sachgerechten Ausgleich zwischen dem staatlichen Auftrag zur Verfolgung und Verhütung von Straftaten einerseits und dem Schutz der grundgesetzlich garantierten Bürgerrechte andererseits. Das Urteil bekräftigt den hohen Rang des Grundrechts auf Unverletzlichkeit der Wohnung und des Rechts auf informationelle Selbstbestimmung. Das Gericht betont, dass der absolut geschützte Kernbereich privater Lebensgestaltung nicht zugunsten der Strafverfolgung eingeschränkt werden darf. Damit darf es keine Strafverfolgung um jeden grundrechtlichen Preis geben.

Die Ausführungen des Bundesverfassungsgerichts sind nicht nur für die Vorschriften über die akustische Wohnraumüberwachung in der Strafprozessordnung von Bedeutung. Auf den Prüfstand müssen jetzt auch andere Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung und andere Formen der verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung gestellt werden, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder.

Insbesondere angesichts zunehmender Bestrebungen, auch die Telefonüberwachung für präventive Zwecke in Polizeigesetzen zuzulassen, ist darauf hinzuweisen, dass das Bundesverfassungsgericht in einem Beschluss zum Außenwirtschaftsgesetz ebenfalls am 3. März 2004 der präventiven Überwachung des Postverkehrs und der Telekommunikation klare Grenzen gesetzt hat.

Die Datenschutzbeauftragten fordern die Gesetzgeber des Bundes und der Länder deshalb auf, zügig die einschlägigen Vorschriften nach den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 zu korrigieren. Die mit der praktischen Durchführung der gesetzlichen Eingriffsbefugnisse befassten Gerichte, Staatsanwaltschaften und die Polizeien sind aufgerufen, die Vorgaben des Gerichts schon jetzt zu beachten.

Ausgangspunkt der Ausführungen des BVerfG ist die von ihm in ständiger Rechtsprechung getroffene Feststellung, dass bei jeder staatlichen Beobachtung ein aus der Achtung der Menschenwürde des Artikel 1 Abs. 1 GG

abzuleitender unantastbarer Kernbereich privater Lebensgestaltung zu wahren ist. Zur Entfaltung der Persönlichkeit in diesem Kernbereich gehört die Möglichkeit, innere Vorgänge wie Empfindungen und Gefühle sowie Überlegungen, Ansichten und Erlebnisse höchstpersönlicher Art zum Ausdruck zu bringen. Maßstab für die Wahrung der Menschenwürde bei staatlichen Eingriffen in Grundrechte bilden außer Artikel 13 GG im Wohnungsbereich und Artikel 10 GG im Bereich des Brief-, Post- und Fernmeldegeheimnisses auch der Schutzbereich der Artikel 1 und 2 GG hinsichtlich des Persönlichkeitsrechts. In dieser Konsequenz hat das BVerfG in seinem Beschluss vom 3. März 2004 zu den §§ 39 ff. Außenwirtschaftsgesetz (1 BvF 3/92) dem Gesetzgeber aufgegeben, bei einer Neuregelung der Überwachungsbefugnisse zur Straftatenverhütung im Außenwirtschaftsverkehr auch die Grundsätze zu beachten, die das Gericht u. a. in seinem Urteil zur akustischen Wohnraumüberwachung niedergelegt hat. Damit wird der Gesetzgeber ausdrücklich verpflichtet, die hier getroffenen verfassungsrechtlichen Vorgaben auch bei der präventiven polizeilichen Telekommunikationsüberwachung zu beachten.

Vor diesem Hintergrund haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung der 67. Datenschutzkonferenz (vgl. Kasten a zu Nr. 5.1.2) gefordert, alle Formen verdeckter Datenerhebung zu Präventivzwecken wie die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz von Vertrauenspersonen und anderer nachrichtendienstlicher Mittel an den Maßstäben der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 auszurichten und die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder ggf. neu zu fassen (vgl. Kasten b zu Nr. 5.1.2).

Die unterschiedliche Bewertung der Auswirkungen der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 auf präventive Eingriffsbefugnisse zeigt sich vor allem hinsichtlich des Erfordernisses kernbereichsschützender Regelungen. So ist das Gesetz zur Neuregelung der präventiven Telekommunikations- und Postüberwachung durch das Zollkriminalamt (ZKA) vom Deutschen Bundestag ohne Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung verabschiedet worden (vgl. Nr. 5.4.3). Es bedarf zwar noch der Prüfung, wie die vom BVerfG im o. g. Urteil zur akustischen Wohnraumüberwachung aufgestellten Grundsätze insgesamt auf präventive Eingriffsbefugnisse – vor allem im Hinblich auf deren praktische Anwendbarkeit – übertragbar sind. Das Absehen von jeglicher kernbereichsschützender Regelung wäre aus meiner Sicht verfassungsrechtlich nicht vertretbar. Zu diesem Ergebnis kamen auch die Vertreter der Wissenschaft anlässlich des von mir veranstalteten Symposiums zum „Großen Lauschangriff“ (vgl. Nr. 7.1.3).

Die rechtspolitische Diskussion dürfte jedoch erst am Anfang stehen. Insofern begrüße ich die Entscheidung des Deutschen Bundestages, die Gültigkeit der Befugnisse zur präventiven Telekommunikations- und Postüberwachung durch das ZKA auf ein Jahr zu befristen, verbunden mit der Aufforderung an die Bundesregierung, die Auswirkungen der verfassungsgerichtlichen Rechtsprechung zu überprüfen. Ich erwarte, dass auch die anderen präventiven Eingriffsbefugnisse für die Polizei und die Nachrichtendienste auf den Prüfstand gestellt werden. Zusätzliche Hinweise hierfür dürfte das noch ausstehende Urteil des BVerfG zu der Verfassungsbeschwerde gegen die Befugnis zur präventiven Telekommunikationsüberwachung zum Zwecke der Straftatenverhütung nach dem Niedersächsischen Sicherheits- und Ordnungsgesetz geben, zu der auch ich eine datenschutzrechtliche Stellungnahme abgegeben habe.

Kasten b zu Nr. 5.1.2

Bei der Umsetzung der verfassungsgerichtlichen Entscheidungen vom 3. März 2004 ist insbesondere auf folgende Aspekte zu achten:

- Schaffung von Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung, insbesondere bei Gesprächen mit Familienangehörigen oder Vertrauten sowie mit Berufsgeheimnisträgern;
- Überprüfung der Straftatenkataloge bei Eingriffsbefugnissen, bei denen der Gesetzgeber ein bestimmtes Gewicht der zu verhütenden Tat voraussetzt;
- Normenklare Eingrenzung der Eingriffsbefugnisse für heimliche Überwachungsmaßnahmen, indem an Tatsachen angeknüpft wird, die einen erfahrungsgemäß hinreichend sicheren Schluss auf die Tatsachenbasis und auf den Grad der Wahrscheinlichkeit der geplanten Tat zulassen;
- Einhaltung des Grundsatzes der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten sowie Normierung einer Kennzeichnungspflicht zur Sicherstellung dieser Zweckbindung;
- Normierung einer Pflicht zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen, von der nur in den vom Gericht genannten Ausnahmefällen abgesehen werden darf.

5.1.3 Kfz-Kennzeichenerfassung

Einige Bundesländer beabsichtigen, die automatische Kfz-Kennzeichenerfassung als neues Fahndungsmittel einzusetzen. Der Abgleich der Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Kfz mit Fahndungsdaten betrifft ganz überwiegend völlig unbescholtene Autofahrer.

Seit Ende 2003 wird in den Gremien der Innenministerkonferenz die Einführung der automatisierten Kfz-Kennzeichenerfassung als neues Fahndungsmittel beraten. Beim Einsatz dieser Technik werden die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmer zum Abgleich mit dem polizeilichen Fahndungssystem aufgenommen. Entsprechende Pilotverfahren wurden in Bayern und Thüringen durchgeführt. In Rheinland-Pfalz und in Hessen sind die jeweiligen

Landespolizeigesetze um eine Rechtsgrundlage für die Kfz-Kennzeichenerfassung erweitert worden. Entsprechende Gesetzesvorhaben werden auch in Bayern und Hamburg betrieben. Andere Länder lehnen die Kfz-Kennzeichenerfassung bisher hingegen ab.

Die Datenschutzbeauftragten des Bundes und der Länder haben in einer Entschließung (vgl. Kasten zu Nr. 5.1.3) auf die datenschutzrechtlichen Probleme des Einsatzes automatisierter Kfz-Kennzeichen-Lesesysteme durch die Polizei hingewiesen.

Kasten zu Nr. 5.1.3

67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25. und 26. März 2004

Entschließung:
Automatische Kfz-Kennzeichenerfassung durch die Polizei

Die Datenschutzbeauftragten des Bundes und der Länder betrachten einen anlassfreien und lageunabhängigen Einsatz von automatischen Kfz-Kennzeichen-Lesesystemen im Straßenverkehr mit Sorge, weil sich diese Maßnahmen zu einem weiteren Schritt zur Überwachung aller Bürgerinnen und Bürger entwickeln können.

Es ist zu befürchten, dass mit dem Einsatz der automatischen Kfz-Kennzeichenerfassung eine neue Infrastruktur geschaffen wird, die künftig noch weit tiefergehende Eingriffe in das Persönlichkeitsrecht ermöglicht.

Die Nutzung dieser neuen Technik hätte zur Folge, dass die Kfz-Kennzeichen aller an den Erfassungsgeräten vorbeifahrenden Verkehrsteilnehmerinnen und -teilnehmer erfasst und mit polizeilichen Fahndungsdateien abgeglichen würden. Schon der mit der Feststellung gesuchter Fahrzeuge verbundene Abgleich würde zu einem neuen Eingriff in das Recht auf informationelle Selbstbestimmung von Personen führen, die weit überwiegend keinen Anlass für eine polizeiliche Verarbeitung ihrer personenbezogenen Daten gegeben haben.

Auf jeden Fall muss ausgeschlossen werden, dass Daten über unverdächtige Personen gespeichert werden und dass ein allgemeiner Datenabgleich mit polizeilichen Informationssystemen durchgeführt wird.

Die Datenschutzbeauftragten weisen darauf hin, dass schon mehrere Länder eine Kfz-Kennzeichen-Erfassung ablehnen.

5.2 Bundeskriminalamt

5.2.1 Rasterfahndung vom Herbst 2001

Auch zwei Jahre nach Abschluss der Rasterfahndungen der Länder aus Anlass der Terroranschläge vom 11. September 2001 liegt mir keine Stellungnahme des BMI zu meiner datenschutzrechtlichen Kontrolle der vom BKA hierfür geleisteten Unterstützungstätigkeit vor.

In meinem 19. Tätigkeitsbericht (Nr. 13.1) habe ich über die in Folge der Terroranschläge vom 11. September 2001 durchgeführte Rasterfahndung zur Identifizierung islamistischer Terroristen berichtet. Nach Abschluss der polizeilichen Maßnahmen habe ich im September 2002 eine datenschutzrechtliche Kontrolle der vom BKA gegenüber den Länderpolizeien geleisteten Unterstützung bei der Vornahme der Rasterfahndungsmaßnahmen durchgeführt. Den Bericht über meinen Kontrollbesuch habe ich dem BMI im Dezember 2002 zugeleitet.

In der Folgezeit hat mir das BMI mitgeteilt, dass zunächst ein vom BKA zu erstellender Abschluss- und Erfahrungsbericht zur Rasterfahndung abgewartet werde müsse, bevor zu meinem Kontrollbericht eine Stellungnahme abgegeben werde könne. Nach mehrfacher Erinnerung informierte mich das BMI im April 2004, dass ein Entwurf dieses Berichts in einer Bund-Länder-Gruppe konkretisiert und anschließend der IMK zugeleitet werde. Seitens des BMI wurde zugesichert, dass mir der Bericht übermittelt werde, sobald er in gebilligter Fassung vorliege. Dieser Bericht vom 17. August 2004 ging erst am 30. Dezember 2004 hier ein; seine Auswertung ist noch nicht abgeschlossen. Bis Redaktionsschluss lag mir zudem noch keine Stellungnahme des BMI auf meinen Prüfbericht vom Dezember 2002 vor.

Vor dem Hintergrund, dass die landesgesetzlichen Regelungen zur Rasterfahndung eine rechtsstaatlich solidere Grundlage darstellen als die derzeit geltenden Normen des BKAG – in einigen Ländern unterliegt die Anordnung von Rasterfahndungsmaßnahmen dem Richtervorbehalt und der jeweilige Landesdatenschutzbeauftragte ist von der Durchführung der Maßnahme zu unterrichten (vgl. 19. TB Nr. 13.1) –, hatte ich in meinem Prüfbericht u. a. empfohlen, bei künftigen Rasterfahndungen auf massenhafte Erhebung personenbezogener Daten durch das BKA zu verzichten. Ich bedauere es daher, dass es hierüber bisher nicht zu dem von mir angeregten Gedankenaustausch mit dem BMI gekommen ist. Im Hinblick auf die rechtsstaatliche Problematik der Rasterfahndung halte ich es für dringend geboten, sich über Möglichkeiten und Grenzen dieses Fahndungsinstruments Rechenschaft zu geben, insbesondere wenn es arbeitsteilig von Bund und Ländern genutzt werden soll. Eine baldige Diskussion hierüber ist umso dringlicher, als im BMI Überlegungen angestellt werden, das Instrument der Rasterfahndung auf die Mitgliedstaaten der EU auszudehnen.

5.2.2 Geldwäsche

Im BKA habe ich einen Beratungs- und Kontrollbesuch zu den dort vorgenommenen Maßnahmen zur Geldwäschebekämpfung durchgeführt.

Im Bereich der Geldwäschebekämpfung ist das BKA im Rahmen seiner Zentralstellenfunktion nach dem BKAG „Clearingstelle“ für den Bund. Weitere „Clearingstellen“ wurden bei den Landeskriminalämtern eingerichtet, wo Polizei und Zoll als „Gemeinsame Finanzermittlungsgruppe (GFG)“ zusammenarbeiten. Hier werden geldwäscherelevant erscheinende Sachverhalte, insbesondere Geldwäscheverdachtsanzeigen der nach den §§ 11

bis 13 Geldwäschegesetz (GwG) zur Anzeige Verpflichteten im Hinblick auf Straftaten nach § 261 bzw. §§ 129a, 129b Strafgesetzbuch abgeklärt und bewertet (vgl. 18. TB Nr. 11.5). Die meisten Datensätze in der Verbunddatei „Geldwäsche“, insbesondere sämtliche auf inländischen Verdachtsanzeigen beruhenden Informationen, werden durch die GFG bei den Ländern eingestellt, während das BKA vor allem die Daten speichert, die aus dem Ausland übermittelt werden.

Daneben wurde im August 2002 in Umsetzung des novellierten § 5 GwG sowie zur Umsetzung des EU-Ratsbeschlusses vom 17. Oktober 2000 über eine „Zusammenarbeit zwischen den zentralen Meldestellen der Mitgliedstaaten beim Austausch von Informationen“ beim BKA als nationale Zentralstelle für Verdachtsanzeigen die deutsche „Financial Intelligence Unit“ eingerichtet, für deren Aufgabenerfüllung die Auswertedatei „FIU“ geführt wird.

Beide Dateien habe ich datenschutzrechtlich kontrolliert und dabei folgendes festgestellt:

Die Speicherung von Daten in der Datei „Geldwäsche“ erfolgt nach Maßgabe der §§ 7, 8 BKAG, wobei die Errichtungsanordnung zur Datei festlegt, dass nur die Daten Beschuldigter und Verdächtiger sowie von deren Kontaktpersonen oder von Personen, die als Veranlasser oder Zielpersonen der verdächtigen Transaktion anzusehen sind, gespeichert werden dürfen. Für bedenklich halte ich, dass die Daten Verdächtiger, die den Großteil der Speicherungen bilden, auch bei ergebnislosem Abgleich der Daten mit anderen Dateien des BKA sowie der Zolldatei nicht gelöscht werden. Nach der Errichtungsanordnung zur Datei „Geldwäsche“ sind die Speicherungen der Daten Verdächtiger nur dann zu löschen, wenn innerhalb der Aussonderungsprüffrist keine ermittlungsrelevanten weiteren Erkenntnisse zur Person hinzu gekommen sind. Jedoch wurde meine Anregung im Rahmen des Anhörungsverfahrens nach § 34 Abs. 1 BKAG umgesetzt, die maximale Aussonderungsprüffrist nach § 32 Abs. 3 BKAG für diesen Personenkreis auf vier Jahre zu beschränken.

Darüber hinaus findet die Regelung des § 33 Abs. 2 Nr. 2, 2. Alt. BKAG keine Anwendung, nach der personenbezogene Daten in Akten zu sperren sind, wenn für diese eine Löschungsverpflichtung nach § 32 Abs. 3 bis 5 BKAG besteht. Diese Unterlassung halte ich ebenfalls für bedenklich, da z. B. die Daten einer Kontaktperson zwar nicht mehr im DV-System recherchiert, jedoch – soweit nicht gesperrt – weiterhin als Teil der Akte zum Beschuldigten oder Verdächtigen verwertet werden können.

Die Datei „FIU“ dient zum einen der Analyse und Auswertung sämtlicher Verdachtsanzeigen im Hinblick auf das Erkennen neuer Typologien und Methoden der Geldwäsche. Die Ergebnisse der Auswertung werden den Strafverfolgungsbehörden und – in abstrakter Form – den nach dem GwG zur Verdachtsanzeige „Verpflichteten“ mitgeteilt. Daneben enthält die Datei einen Bereich „Schriftverkehr“, in dem das BKA als Koordinator für den Austausch von Informationen anlässlich von Erkenntnisanfragen zwischen ausländischen „FIU“ und den Polizeibehörden der Bundesländer tätig wird. Auch die in diesem Zusammenhang gespeicherten Daten sind nach spätestens vier Jahren zu löschen.

Anlässlich der datenschutzrechtlichen Überprüfung trug das BKA die Überlegung an mich heran, beide Dateien zu einer Verbunddatei zusammen zu führen, in der sämtliche inländischen Verdachtsanzeigen gespeichert sind, und die zugleich die Grundlage für die Clearingverfahren beim BKA und bei den Ländern bildet. Vor dem Hintergrund, dass die Daten einer Person häufig in beiden Dateien gespeichert werden und das Löschen eines Datensatzes in der Datei „Geldwäsche“ durch ein Land – soweit das BKA darüber überhaupt informiert wird – nicht die Verpflichtung des BKA zum Löschen des entsprechenden Datensatzes in der Datei „FIU“ nach sich zieht, habe ich mich diesen Überlegungen nicht von vornherein verschlossen und prüfe, ob innerhalb der Vorgaben des BKAG und des GwG eine Lösung entwickelt werden kann. Bevor ich eine abschließende Bewertung vornehmen kann, muss das Vorhaben vom BMI bzw. vom BKA noch konkretisiert werden.

5.2.3 INPOL-neu

Nach jahrelangen Vorarbeiten ist INPOL-neu im August 2003 in den Wirkbetrieb gegangen. Dies war jedoch nur ein erster Schritt auf dem Weg zur Fortentwicklung des polizeilichen Informationssystems.

Bereits seit vielen Jahren betreiben die Polizeien des Bundes und der Länder das Verbundsystem INPOL, in dem für die polizeiliche Arbeit erforderliche Daten eingestellt und abgerufen werden können. Dabei liegt die datenschutzrechtliche Verantwortung jeweils bei der Polizeibehörde, die die Daten eingegeben hat.

Die Einführung des neuen polizeilichen Informationssystems INPOL-neu erfolgte zum 16. August 2003. Dabei wurden in einem ersten Schritt die jeweiligen Systeme der Verbundteilnehmer umgestellt (BKA, LKÄ der 16 Bundesländer, BGS, Zollkriminalamt und Dienststellen der Zollverwaltung, soweit sie grenzpolizeiliche Aufgaben wahrnehmen). Über die wesentlichen Neuerungen (vgl. 19. TB Nr. 13.8), insbesondere die vereinfachte Anwendung durch Gestaltung der Benutzeroberfläche in Internettechnologie, konnte ich mich im Rahmen einer BKA-Präsentation im September 2003 unterrichten. Ein zweiter Schritt erfolgte im Juli 2004, wobei insbesondere zusätzliche Personeninformationen aufgenommen wurden.

Im Vorfeld der Einführung des neuen Systems habe ich gegenüber dem BKA die aus datenschutzrechtlicher Sicht kritischen Punkte angesprochen. Das gravierendste Problem bleibt die Abbildung der kriminellen Historie in der Verbunddatei „Kriminalaktennachweis“ (vgl. 18. TB Nr. 11.2.2). Meinen diesbezüglichen Bedenken wurde leider nicht Rechnung getragen. Vielmehr bestehen die Polizeien des Bundes und der Länder darauf, sämtliche strafbaren Handlungen einer Person in der Datei „Kriminalaktennachweis“ vorzuhalten, wenn zumindest eine der Straftaten die Aufnahmekriterien für die Datei erfüllt, es

sich also um eine Straftat von erheblicher, länderübergreifender oder internationaler Bedeutung handelt. Dies bedeutet, dass auch eine Vielzahl Daten über weniger bedeutsame Straftaten bundesweit abgerufen werden kann.

Im Verlauf des Jahres 2004 wurden auf der Grundlage eines Fragebogens, der von Vertretern der Landesbeauftragten für den Datenschutz und mir erarbeitet wurde, mehrere intensive Gespräche mit dem BKA geführt. Außerdem haben Vertreter der LfD und meiner Dienststelle eine Arbeitsgruppe INPOL-neu eingerichtet, die sich an der konzeptionellen Entwicklung des Systems beteiligen und damit Problemfelder frühzeitig herausarbeiten und klären will. Ich halte die Teilnahme eines Vertreters dieser Arbeitsgruppe an den entsprechenden fachlichen INPOL-Gremien beim BKA für dringend geboten, damit falsche Weichenstellungen vermieden werden. Daneben habe ich in Zusammenhang mit der Neufassung von Errichtungsanordnungen festgestellt, dass sich bei den „Fall-Dateien“ die Anzahl der Freitextfelder, deren Inhalt nur bei Einzelkontrollen überprüft werden kann, wesentlich erhöht hat. Freitextfelder sind deshalb problematisch, weil – anders als bei vordefinierten Merkmalen – keine technische Begrenzung auf bestimmte Begriffe erfolgt. Insofern besteht hier ein besonderes Risiko, dass unzulässige oder diskriminierende Daten gespeichert werden. Dieses Problem habe ich dem BMI gegenüber angesprochen. Ich werde die Fortentwicklung von INPOL-neu sorgfältig begleiten und darauf achten, dass der gesetzliche Rahmen des BKAG beachtet wird.

5.2.4 „Schlafende Bestände“ über Fingerabdruckmaterial und DNA-Identifizierungsmuster

Die mit der Schaffung sog. „Schlafender Bestände“ über Fingerabdruckdaten und DNA-Identifizierungsmuster angestrebte längerfristige Speicherung dieser Daten über die bestehenden Aussonderungsfristen hinaus wäre von zweifelhaftem Wert.

In den Gremien der IMK wird derzeit beraten, unter welchen Bedingungen Fingerabdruckmaterial und DNA-Identifizierungsmuster nach fristgemäßer Aussonderung der Unterlagen, zumeist nach Ablauf von zehn Jahren, in einem gesonderten Recherchepool in Form eines sog. „Schlafenden Bestandes“ längerfristig vorgehalten werden können. Auch nach Löschung der Daten eines Täters/Tatverdächtigen soll eine Täteridentifizierung über die Tatortspur gewährleistet werden, wenn eine neue Spur an diesem „Schlafenden Bestand“ vorbeigeführt wird. Ein Zugriff auf die Identifikationsdaten soll jedoch nur noch im Falle eines Treffers beim Datenabgleich, nicht aber über die Personeneingabe oder andere Suchkriterien zulässig sein. Andere polizeiliche Dateien sollen keine Hinweise enthalten, die auf die Speicherung von Fingerabdruckdaten und DNA-Identifizierungsmustern einer Person in dieser gesonderten Datei schließen lassen. Technisch realisiert werden soll dies entweder innerhalb der bestehenden, beim BKA geführten Fingerabdruck- bzw. DNA-Analysedatei oder durch Aufbau einer gesonderten Datenbank, in die die betreffenden Datensätze zu überführen sind.

Im Hinblick darauf, dass das Recht auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse und nur soweit dies zum Schutz öffentlicher Interessen unumgänglich ist, eingeschränkt werden darf, wirft das Vorhaben eine Reihe von Fragen auf. Zweifel bestehen bereits bezüglich der Geeignetheit „Schlafender Bestände“ für die angestrebte Steigerung der Ermittlungseffektivität zum Schutz der Bevölkerung. Diese wäre allenfalls dann zu bejahen, wenn es sich – durch empirisch festgestellte Rechtstatsachen belegt – erweisen sollte, dass Straftäter in einem signifikanten Umfang erst zehn Jahre oder später nach Begehung einer Straftat – und damit weit nach Ablauf polizeilicher Speicherfristen – rückfällig werden. Kriminologische Erkenntnisse, die dies belegen, wurden nicht vorgetragen. Bei der Erörterung der Thematik wird zudem nicht hinreichend berücksichtigt, dass es sich bei den zu beachtenden Fristen für die Speicherung von Fingerabdruckmaterial bzw. DNA-Identifizierungsmuster nicht um Höchstspeicherfristen, sondern um sog. Aussonderungsprüffristen handelt. Bei Ablauf dieser Fristen, die nach dem BKAG bei Erwachsenen grundsätzlich zehn Jahre betragen, sind die Daten nämlich nicht automatisch zu löschen, sondern es ist zu prüfen, ob ihre Kenntnis für die weitere Aufgabenerfüllung der Polizei erforderlich ist. Bei einer prognostizierten künftigen Straffälligkeit des Betroffenen kann die Frist entsprechend verlängert werden. Im Falle der Verbüßung einer Freiheitsstrafe beginnt die Aussonderungsprüffrist zudem erst zu laufen, wenn der Betroffene aus der Justizvollzugsanstalt entlassen oder die mit einer Freiheitsentziehung verbundene Maßnahme der Besserung und Sicherung beendet ist. Eine angestrebte längerfristige Nutzung von Fingerabdruckdaten und DNA-Identifizierungsmustern lässt sich somit – soweit erforderlich – bereits bei Ausnutzung der bestehenden gesetzlichen Möglichkeiten erreichen. Für die Schaffung eines „Schlafenden Bestandes“ fehlt es daher an der notwendigen Erforderlichkeit.

Bedauerlicherweise hat sich die IMK im November 2004 mehrheitlich für eine befristete weitere Speicherung von Fingerabdruckdaten und DNA-Identifizierungsmustern in einem „Schlafenden Bestand“ ausgesprochen. Die Schaffung eines „Schlafenden Bestandes“ würde Änderungen der Landespolizeigesetze sowie des DNA-Identitätsfeststellungsgesetzes und – soweit die Datei zentral beim BKA vorgehalten werden sollte – des BKAG erforderlich machen.

5.2.5 Auswertedateien

Das BKA nutzt weiterhin Auswertedateien zur Erfüllung seiner Aufgaben als Zentralstelle der Polizeien des Bundes und der Länder. Diese „Vordateien“ werden in Form einer Amtsdatei (Nr. 5.2.5.1), aber auch als Verbunddateien (Nr. 5.2.5.2,) des polizeilichen Informationssystems geführt. Im Hinblick auf das Fehlen einer normenklaren Rechtsgrundlage im BKAG ist dies unter datenschutzrechtlichen und rechtsstaatlichen Gesichtspunkten problematisch.

5.2.5.1 Datei „Global“

Ein Beispiel für eine Auswertedatei, in der sämtliche Informationen zu bestimmten Projekten vorläufig gespeichert und erst anschließend auf ihre Relevanz für polizei- oder ermittlungstaktisches Vorgehen bewertet werden, stellte die Datei „Global“ dar, die im Zusammenhang mit gewalttätigen Aktionen und anderen Straftaten militanter Globalisierungsgegner geführt wurde (19. TB Nr. 13.2.2).

Meine Bedenken gegen Auswertedateien, wonach der Personenkreis, über den Daten gespeichert werden, nicht präzise genug bestimmt ist und Informationen ungeachtet ihrer Relevanz für die polizeiliche Aufgabenerfüllung erfasst werden, haben sich im April 2003 anlässlich eines Beratungs- und Kontrollbesuches im BKA im Wesentlichen bestätigt: Die Polizeirelevanz bestimmter Daten ergab sich allein daraus, dass diese von Polizeidienststellen des In- und Auslandes stammten. Die Informationen betrafen auch Personen, die nur mittelbar in den Themenzusammenhang mit der Globalisierungsgegnerschaft gestellt werden konnten. Auf diese Weise wurden in der Datei auch Daten zu Personen undifferenziert gespeichert, die lediglich an Anti-Globalisierungsveranstaltungen teilgenommen oder Kundgebungen hierzu ordnungsgemäß angemeldet hatten, ohne dass gegen sie strafrechtliche Ermittlungen eingeleitet worden waren. Nach meinen Feststellungen kam die Datei „Global“ in ihrer Zielsetzung einer vom BKA geführten Vorsorgedatei gleich. Der für Vorsorgedateien durch § 8 BKAG vorgegebene Rahmen ist jedoch erheblich überzogen worden. So wurden Informationen auch im Rahmen von strafrechtlichen Ermittlungsverfahren gegen Unbekannt verarbeitet und genutzt, obwohl zu den betreffenden Personen über ihre Demonstrationsteilnahme hinaus keine weiteren Erkenntnisse vorlagen, die eine Kategorisierung gem. § 8 BKAG gerechtfertigt hätten. Eine normenklare Rechtsgrundlage, die dies zulassen würde, besteht nicht. Auch § 7 BKAG, der nach Auffassung des BMI die Speicherung personenbezogener Daten in Auswertedateien erlaubt, trägt dem nicht Rechnung, weil sich aus ihm Voraussetzungen und Umfang der Einschränkungen des informationellen Selbstbestimmungsrechts nicht klar und für den Betroffenen erkennbar ergeben. Vor diesem Hintergrund hatte ich das BMI aufgefordert, von einer Weiterführung der Datei „Global“ abzusehen.

Das BMI ist meiner Empfehlung gefolgt und hat die Datei „Global“ mittlerweile gelöscht. Sofern die gesetzlichen Voraussetzungen des § 8 BKAG im Einzelnen vorlagen, wurden in ihr enthaltene Daten in eine Zentraldatei des BKA überführt.

Trotzdem besteht die Problematik der Auswertedateien weiter fort. Nach dem Muster der Datei „Global“ werden im BKA noch weitere Auswertedateien zur Erkenntnisgewinnung über andere gesellschaftliche Erscheinungen und Entwicklungen geführt. Nicht zuletzt im Hinblick auf die strengen Anforderungen des Bundesverfassungsgerichts an eine wirksame Einschränkung des informationellen Selbstbestimmungsrechts halte ich es daher für dringend geboten, das Führen von Auswertedateien auf eine normenklare Rechtsgrundlage zu stellen.

5.2.5.2 Indexdatei zum islamistischen Terrorismus

Die Auswertedateien sind gemäß ihrer Errichtungsanordnungen so ausgestaltet, dass Übermittlungen personenbezogener Daten an andere Stellen grundsätzlich unzulässig sind und nur ein begrenzter Personenkreis im BKA Zugriff auf die Dateien hat. Die zur Bekämpfung des islamistischen Terrorismus als Auswertedatei im März 2003 eingerichtete Indexdatei weicht erstmals von dieser Konzeption ab. Die darin gespeicherten personenbezogenen Daten werden im Rahmen des polizeilichen Datenverbundes von den Polizeien des Bundes und der Länder unmittelbar in die Datei eingegeben bzw. für diese zum unmittelbaren Zugriff bereit gehalten. Nach Mitteilung des BMI handelt es sich dabei um sog. weiche, d. h. unbewertete Daten von Personen, die in keinem direkten Zusammenhang mit Straftaten oder einer Gefährdung stehen. Diese Daten waren vom BKA und den Landespolizeidienststellen bisher nur lokal in eigene Dateien eingestellt worden, ohne dass ein gegenseitiger Zugriff darauf möglich war. Um die daraus entstandenen Informationsdefizite zu beseitigen, hatten die Gremien der IMK die Einrichtung einer Datei empfohlen, in der das BKA und die Landespolizeien die Personalien von Personen, die in „irgendeiner Form bei der Bekämpfung des islamistischen Terrorismus bekannt geworden sind“, speichern dürfen. Dies führte dazu, dass in der Indexdatei Daten zu Personen erfasst werden, die weit über die in § 8 Abs. 1 bis 5 BKAG vorgesehen Personenkategorien hinausgehen.

Dies ist nach den Regelungen des BKAG nicht zulässig. Im Hinblick auf die mit einer Verbundanwendung einhergehende weite Verbreitung personenbezogener Daten reicht es nicht aus, dass der Kreis der von der Speicherung betroffenen Personen allein durch den ohnehin stets zu beachtenden Grundsatz der Erforderlichkeit für die Erfüllung der Zentralstellenaufgabe des BKA gem. § 7 Abs. 1 BKAG begrenzt wird. Vielmehr gibt § 8 BKAG den Rahmen vor, innerhalb dessen sich Datenspeicherungen zum Zweck künftiger Strafverfolgung halten müssen, wenn sie im polizeilichen Informationssystem des Bundes und der Länder erfolgen sollen. Anderenfalls käme der Regelung des § 8 BKAG keine eigenständige Bedeutung zu.

Bei Ressortbesprechungen zur Ausgestaltung von Rechtsgrundlagen für das Führen gemeinsamer Dateien durch Polizei und Nachrichtendienste (vgl. Nr. 5.1.1) wurde ein Entwurf für einen neuen § 8a BKAG vorgelegt, der die Verarbeitung personenbezogener Daten in Auswertedateien des BKA auf eine normenklare Rechtsgrundlage stellen sollte. Am Beispiel der Bekämpfung des islamistischen Terrorismus begründete das BMI die Notwendigkeit derartiger Dateien damit, dass den Polizeien des Bundes und der Länder Informationen über Personen vorlägen, die nicht unter die Kategorie der sog. „sonstigen Personen“ im Sinne von § 8 Abs. 5 BKAG gefasst werden könnten, auf die aber gleichwohl nicht verzichtet werden könne.

Aus Anlass der Gesetzesberatungen habe ich mich durch einen Informationsbesuch über die Qualität der Daten,

auf die in der Indexdatei verwiesen wird, im BKA informiert. Zweck der Datei ist der Nachweis und die Vernetzung von Fundstellen über das Vorliegen präventiver und repressiver personenbezogener polizeilicher Erkenntnisse aus dem Bereich des islamistischen Terrorismus. In der Datei werden die Personalien sowie Aktenzeichen und aktenführende Dienststelle gespeichert. Zudem kann über eine Detailanzeige u. a. die „Rolle“ der Person, unterteilt in die Kategorien „Hinweisgeber“, „Verdächtiger/Störer“, „sonstige Person“ und „Opfer/Gefährdeter“, abgerufen werden. Zum Zeitpunkt des Informationsbesuchs im Mai 2004 waren in dieser Auswertedatei Daten zu ca. 6 000 Personen gespeichert. Entsprechend der Empfehlungen der Gremien der IMK wird jede den Polizeien des Bundes und der Länder bekannt gewordene Information, die in einem wie auch immer gearteten Zusammenhang mit dem islamistischen Terrorismus steht, erfasst. Eine Speicherung erfolgt z. B. auch dann, wenn Informationen von einer Person stammen, die seitens der Polizei als nicht vertrauenswürdig eingestuft wird. Die von mir stichprobenweise gesichteten BKA-Akten, auf die im Fundstellennachweis hingewiesen wird, enthielten zudem Informationen, bei denen eine Relevanz nicht erkennbar war. Eine derartige Datenverarbeitung ist mit dem BKAG nicht vereinbar. Auf meinen Hinweis hin hat das BKA einige Fundstelleneinträge gelöscht und die dazugehörigen Aktenvorgänge vernichtet. Inwieweit mein Besuch zum Anlass genommen wurde, den Inhalt der gesamten Datei auf seine Erforderlichkeit hin zu überprüfen, müssen spätere datenschutzrechtliche Kontrollen zeigen. Seitens des BKA wurde jedoch deutlich gemacht, dass zur Erreichung des Zwecks der Datei eine Vielzahl von Speicherungen – auch wenn diese zunächst irrelevant erscheinen mögen – erwünscht und erforderlich seien.

Wegen der rechtsstaatlichen Problematik von Auswertedateien hatte ich die Absicht des BMI begrüßt, den Entwurf einer Rechtsgrundlage für das Führen dieser Dateien auszuarbeiten. Offenbar vor dem Hintergrund der Schwierigkeiten, eine normenklare Regelung zu schaffen, die den Anforderungen des Bundesverfassungsgerichts an eine zulässige Einschränkung des informationellen Selbstbestimmungsrechts Rechnung trägt, wird das Vorhaben derzeit nicht weiter betrieben. Die Indexdatei wird weiterhin als Auswertedatei – ohne Rechtsgrundlage – geführt.

5.2.6 Durchführung des Konsultationsverfahrens nach Artikel 17 Abs. 2 SDÜ durch das Bundeskriminalamt

Visabewerber aus bestimmten Ländern müssen sich vor Erteilung eines Visums für einen Schengenstaat einem Verfahren unterziehen, bei dem ihre Daten durch die Sicherheitsbehörden des betreffenden Schengenstaates überprüft werden. Dabei lässt das BKA in vielen Fällen die ihm obliegende Pflicht zur Überprüfung der Daten, auf die ein ablehnendes Votum gegen die Erteilung eines Schengenvisums gestützt wird, vermissen.

Im Berichtszeitraum habe ich mich über die Durchführung des Konsultationsverfahrens gem. Artikel 17 Abs. 2 Schengener Durchführungsübereinkommen (SDÜ) (vgl. 19. TB Nr. 16.2.3) bei den auf nationaler Ebene zu beteiligenden Behörden BKA, BfV und BND unterrichtet. Dem BKA kommt im nationalen Verfahren eine entscheidende Rolle zu, da die überwiegende Anzahl der im Konsultationsverfahren durch deutsche Auslandsvertretungen abgelehnten Anträge auf Erteilung eines Schengenvisums auf ein negatives Votum des BKA zurückzuführen sind.

Kasten zu Nr. 5.2.6

So funktioniert das Konsultationsverfahren

1. Das Verfahren auf der Ebene der EU
   - Die Schengen-Staaten legen auf Listen fest, bei welchen Staatsangehörigen sie die Erteilung eines Schengenvisums von der Konsultation der zentralen Behörde der betroffenen Vertragspartei und ggf. von der Konsultation der zentralen Behörden der anderen Vertragsparteien abhängig machen. Es handelt sich dabei um Visumsanträge von Staatsangehörigen bestimmter „Problemstaaten“, bei denen pauschal ein erhöhtes Risiko für die nationale Sicherheit unterstellt wird.
   - Das Verfahren, in dessen Rahmen Bedenken gegen die Visumserteilung erhoben werden können, muss binnen sieben Arbeitstagen abgeschlossen sein.
   - Werden Bedenken geltend gemacht, wird grundsätzlich kein Visum ausgestellt.
   - Die Durchführung des Konsultationsverfahrens erübrigt sich, sofern das Visum bereits wegen einer bestehenden Fahndungsausschreibung im Schengener Informationssystem nicht erteilt wird.
2. Die nationale Ausgestaltung des Konsultationsverfahrens in Deutschland
   - Zentrale Behörde in Deutschland ist das Auswärtige Amt. Es leitet die Anträge der Visastellen automatisiert an die Sicherheitsbehörden (BKA, BfV, BND, ZKA) weiter.
   - Die Sicherheitsbehörden gleichen die Daten aus den Visaanträgen mit den bei ihnen vorliegenden Erkenntnissen ab.
   - Innerhalb der o. g. Bearbeitungsfrist teilen die Sicherheitsbehörden den betreffenden Visastellen über das Auswärtige Amt automatisiert mit, ob Bedenken gegen die Visaerteilung bestehen.
   - Gründe für die Ablehnung werden dabei nicht genannt. Die Antwort wird zudem systemtechnisch so erteilt, dass für die Visastellen nicht ersichtlich ist, welche Sicherheitsbehörde Bedenken erhoben hat.

In einer Reihe von Fällen, in denen mich Petenten um eine Prüfung gebeten hatten, habe ich festgestellt, dass das BKA ein ablehnendes Votum allein schon bei Vorhandensein einer Speicherung von Daten des Betroffenen in

Dateien des BKA abgibt, ohne dass im Einzelfall eine Relevanzprüfung der den Speicherungen zugrunde liegenden Gründe vorgenommen wird. Da in vielen Fällen die Gründe für die Speicherung und damit für die Geltendmachung von Einreisebedenken nur von den Stellen, die dem BKA den betreffenden Sachverhalt mitgeteilt haben, beurteilt werden können, muss das BKA jedoch in jedem Einzelfall – ggf. durch eine Rückfrage bei diesen Stellen – prüfen, ob die zur Geltendmachung von Einreisebedenken bestehenden Gründe nach wie vor Bestand haben. Nur dann ist ein ablehnendes Votum, welches für den Betroffenen zur Folge hat, dass er in das gesamte Schengen-Gebiet nicht einreisen darf, gerechtfertigt. In vielen der von mir überprüften Fälle wäre es bei Beachtung der sich aus § 32 Abs. 3 BKAG ergebenden Überprüfungsverpflichtung nicht zu den Ablehnungen der Visumsanträge gekommen.

Ich verkenne zwar nicht, dass das Konsultationsverfahren für das BKA aufwändig und zugleich an knappe Zeitvorgaben gebunden ist. Dies kann jedoch das BKA nicht generell von seiner Pflicht zur Überprüfung personenbezogener Daten nach § 32 Abs. 3 BKAG entbinden. Adressat dieser Verfahrensregelungen ist das BKA. Nur für die in Verbunddateien des polizeilichen Informationssystems gespeicherten Daten obliegen die Löschungs- und Prüfungsverpflichtungen den jeweiligen INPOL-Teilnehmern, die den betreffenden Datensatz eingegeben haben (§ 11 Abs. 2 BKAG). In den von mir geprüften Fällen war jedoch das BKA selbst speichernde Stelle.

Kritisiert habe ich auch den Umfang der vom BKA herangezogenen Informationen im Zusammenhang mit der Prüfung von Visumsanträgen im Konsultationsverfahren, die weit über den mit dem Verfahren verfolgten Zweck hinausgehen.

Im Rahmen des Konsultationsverfahren sollen nur Versagungsgründe gem. § 8 Abs. 1 Nr. 5 Ausländergesetz (AuslG) festgestellt werden. Damit soll sichergestellt werden, dass Erkenntnisse über Personen im Rahmen des Visumsverfahrens berücksichtigt werden, die nicht oder nicht mehr im Ausländerzentralregister (AZR) bzw. im Schengener Informationssystem (SIS) gespeichert sind, jedoch beschränkt auf Angehörige bestimmter „Problemstaaten“ und auf vorhandene Verdachtsmomente für Terrorismus. Diejenigen Personen, die terroristische Aktivitäten entfalten oder unterstützen, sollen kein Einreise- oder Aufenthaltsrecht erhalten. Damit werden Bestrebungen erfasst, die gegen die freiheitliche demokratische Grundordnung sowie gegen die Sicherheit des Bundes oder eines Landes gerichtet sind. Der Hinweis des BMI auf die Regelung des § 64a Abs. 3 Satz 2 AuslG, wonach die Sicherheitsbehörden die Antragsdaten auch speichern und nutzen dürfen, wenn das zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist, geht hier fehl. Das Konsultationsverfahren dient also nicht der allgemeinen Gefahrenabwehr.

Angesichts der unterschiedlichen Auffassungen habe ich dem BMI Gespräche angeboten, um praktikable und datenschutzgerechte Lösungsmöglichkeiten zu entwickeln. Bis Redaktionsschluss haben diese noch nicht stattgefunden.

5.3 Bundesgrenzschutz

5.3.1 Änderung des BGS-Gesetzes – ohne meine Beteiligung

Der BGS darf weiterhin verdachtsunabhängige Personenkontrollen auf Bahnhöfen und Flughäfen durchführen.

Mit der Regelung des § 22 Abs. 1a BGSG wurde am 25. August 1998 eine Rechtsgrundlage für die Durchführung verdachts- und ereignisunabhängiger Kontrollen auch außerhalb der bis dato geltenden 30 km-Zone geschaffen. Diese Regelung ermächtigt den BGS, in Zügen, auf Bahnhöfen und Bahnanlagen sowie auf Flughäfen mit grenzüberschreitendem Verkehr Personen wie bei einer Schleierfahndung kurzfristig anzuhalten, zu befragen und mitgeführte Ausweispapiere oder Grenzübertrittspapiere zu prüfen sowie mitgeführte Sachen in Augenschein zu nehmen. Ich hatte seinerzeit erhebliche Bedenken gegen diese Regelung geäußert, weil damit jedermann in das Visier der Polizei geraten kann, ohne zuvor als Störer oder Verdächtiger polizeilich in Erscheinung getreten zu sein (vgl. 17. TB Nr. 12.1). Nach dem ursprünglichen Gesetzesentwurf war sogar die Möglichkeit einer anlasslosen Kontrolle vorgesehen. Die Regelung wurde jedoch dahin gehend eingeschränkt, dass eine Kontrolle nur durchgeführt werden kann, wenn aufgrund bestimmter Lageerkenntnisse oder grenzpolizeilicher Erkenntnisse anzunehmen ist, dass die entsprechenden Züge oder Bahnanlagen zur unerlaubten Einreise genutzt werden.

Nicht zuletzt aufgrund meiner Anregungen wurde die neue Ermächtigung bis zum 31. Dezember 2003 befristet. Damit war die Möglichkeit einer intensiven Evaluierung gegeben, da innerhalb dieses Zeitraums in ausreichendem Maße rechtstatsächliche Erkenntnisse über die Wirksamkeit der Maßnahmen gewonnen und ausgewertet werden konnten. Die Notwendigkeit einer Evaluierung wurde auch im Rahmen der parlamentarischen Ausschussberatungen deutlich, bei denen das BMI gebeten wurde, die innerhalb dieses Zeitraums gesammelten Erfahrungen zu einem späteren Zeitpunkt zu beurteilen.

Da bis Anfang September 2003 keine aussagekräftige Bewertung der Maßnahme vorlag, ging ich davon aus, dass die gesetzliche Regelung mit Ablauf des Jahres 2003 außer Kraft treten würde. Mit einem entsprechenden Schreiben hatte ich das BMI gleichzeitig aber darum gebeten, mich für den Fall, dass gleichwohl eine Verlängerung der Regelung geplant sei, zu beteiligen. Dieses Schreiben blieb unbeantwortet. Auch wurde mir der Erfahrungsbericht des BMI vom 29. August 2003 zunächst nicht zugeleitet. Im Oktober 2003 habe ich mich deshalb erneut an das BMI gewandt und deutlich gemacht, dass entsprechend der GGO der BfD frühzeitig über die Aktivitäten des Bundes, sofern sie datenschutzrechtliche Aspekte berühren, zu informieren ist, damit er die ihm obliegende Beratung und Kontrolle der öffentlichen Stellen des Bundes und die Unterrichtung des Deutschen Bundestages über wesentliche Entwicklungen des Datenschutzes vornehmen kann. Auch dieses Schreiben blieb bis jetzt unbeantwortet, wenngleich mir am 11. November 2003 der von der Bundesregierung dem Deut-

schen Bundestag bereits Anfang September 2003 zugeleitete Erfahrungsbericht vom 29. August 2003 zuging. Dies erfolgte genau einen Tag vor der abschließenden Beratung eines entsprechenden Gesetzesentwurfs zur Änderung des Ersten Gesetzes zur Änderung des BGSG.

Mit diesem Gesetz vom 22. Dezember 2003 (BGBl. I S. 2770) wurde die Verlängerung der Regelungen aus dem Jahre 1998 bis zum 30. Juni 2007 beschlossen. Im Gesetz wurde außerdem festgeschrieben, dass die Maßnahme vor Ablauf der Befristung zu evaluieren ist. Auf diese Evaluierung wird es besonders ankommen, zumal auch die Europäische Kommission die in einigen Bundesländern eingeführte Schleierfahndung im Hinblick auf den Wegfall der Grenzkontrollen im Schengengebiet prüfen will. Ich hoffe, dass ich an der Evaluation diesmal rechtzeitig beteiligt werde.

5.3.2 Projektgruppe „Mehr Datenschutz beim BGS“

Das Pilotprojekt zur Verbesserung des Datenschutzes beim BGS wird nach fast zweijähriger Unterbrechung endlich fortgesetzt.

Die Neukonzeption des „Bundesgrenzschutzaktennachweises (BAN)“ war als eine der wichtigsten und am häufigsten genutzten Dateianwendungen des BGS Gegenstand des ersten Teilprojekts, mit dessen Durchführung eine beim Bundesgrenzschutzamt Schwandorf gebildete Projektarbeitsgruppe beauftragt wurde (19. TB Nr. 14.2). Am 11. Juni 2003 wurde der Abschlussbericht dem BMI zur weiteren Bewertung übergeben. Diese Bewertung sowie das Ergebnis der Überprüfung des Abschlussberichts durch das BGS-Amt Berlin standen bis Redaktionsschluss aus. Das BMI hat aber am 26. August 2004 eine geänderte Errichtungsanordnung für die Datei BAN endgültig genehmigt, ohne dass dabei erkennbar Empfehlungen der Projektarbeitsgruppe berücksichtigt wurden.

Mit Erlass vom 7. November 2004 hat das BMI die Fortsetzung des Projekts angeordnet. Im Verlauf des weiteren Teilprojekts sollen das Verfahren „PAVOS-Zentral“ und die Anwendung „Elektronisches Tagebuch“ (ETB – vgl. Nr. 5.3.3), insbesondere deren Verhältnis zum „BAN“ untersucht werden.

Die Weisung des BMI, das Pilotprojekt fortzusetzen, begrüße ich. Die Projektarbeitsgruppe werde ich dabei weiterhin in allen datenschutzrechtlichen Fragen beratend unterstützen. Eine Bewertung des abgeschlossenen Teilprojekts BAN durch das BMI halte ich gerade im Hinblick auf den weiteren Projektfortschritt für dringend geboten. Es muss Klarheit über die Konzeption der Datei BAN bestehen, insbesondere wenn deren Verhältnis zu den Verfahren PAVOS-Zentral und ETB untersucht werden soll.

Eineinhalb Jahre nach Übergabe des Abschlussberichts zur Gestaltung der Datei BAN an das BMI darf erwartet werden, dass dessen Bewertung nunmehr abgeschlossen wird. Das Erarbeiten von Empfehlungen der Projektarbeitsgruppe „auf Halde“ hielte ich nicht für angemessen.

5.3.3 Ausbau der Informationstechnik beim BGS

Die Einführung eines BGS-weiten Vorgangsbearbeitungs- und Recherchesystems auf der Grundlage des elektronischen Tagebuchs genügt den datenschutzrechtlichen Anforderungen im Wesentlichen.

Alle polizeilich erheblichen Ereignisse werden beim BGS in sog. Tagebüchern dokumentiert, die damit einen chronologischen Nachweis des polizeilichen Handelns darstellen. Die bei jeder Dienststelle des BGS geführten Tagebücher wurden – vor etwa vier Jahren – in ein elektronisches System, das „Elektronische Tagebuch“, überführt, das allerdings weiterhin nur auf der Ebene der einzelnen Dienststellen ohne Datenverbund eingesetzt wurde. Ein automatisierter Zugriff auf die Daten anderer Dienststellen war ebenso ausgeschlossen wie ein automatisiertes Übermittlungsverfahren.

Im Rahmen des Projekts PAVOS (Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem) BGS wurde im Jahr 2003 beim BGS ein zentrales Datenhaltungssystem entwickelt, mit dem sowohl die Vorgangsbearbeitung als auch eine bundesweite Recherche möglich wurde. Grunderfassungsmodule für die „PAVOS-Zentral“ genannte Datenbank sind die lokalen ETB: Die hier dokumentierten Straftaten, Ordnungswidrigkeiten und polizeilichen Maßnahmen und die in diesem Zusammenhang eingegebenen Daten werden in PAVOS-Zentral oder „ETB-Zentral“ gespiegelt. Zwar besteht keine unmittelbare Verbindung zwischen den einzelnen weiterhin auf lokaler Ebene geführten ETB, jedoch sind über das zentrale System PAVOS Online-Recherchen im gesamten BGS-Bestand bundesweit möglich. Dabei wird hinsichtlich der Zugriffsberechtigungen differenziert: Während jeder BGS-Bedienstete Zugriff auf die Personengrunddaten hat, um feststellen zu können, bei welcher Dienststelle ein Vorgang zu einer bestimmten Person geführt wird, können weitergehende Abfragen und Recherchen in „PAVOS-Zentral“ nur von besonders autorisierten BGS-Bediensteten durchgeführt werden.

Gegen die Einführung eines BGS-weiten Vorgangsbearbeitungs- und Recherchesystems bestehen keine grundlegenden datenschutzrechtlichen Bedenken. Insbesondere begrüße ich das vorgesehene Berechtigungskonzept, welches sicherstellen soll, dass der jeweilige BGS-Bedienstete nur auf die Daten zugreifen kann, deren Kenntnis zur Erfüllung seiner Aufgaben erforderlich ist.

Im Rahmen des Anhörungsverfahrens gem. § 36 Abs. 2 Satz 1 BGSG zur Errichtungsanordnung für die Datenbank PAVOS-Zentral wurde auch die Frage nach deren Abgrenzung zur Datei „Bundesgrenzschutzaktennachweis (BAN)“ (vgl. 18. TB Nr. 12.2.1; 19. TB Nr. 14.1) erörtert. Zwar bestehen zwischen den beiden Datenbanken einige wesentliche Unterschiede: So ist der BAN ausschließlich ein Aktennachweissystem, auf welches auch – anders als bei PAVOS-Zentral – externe Stellen, wie die beauftragten Polizeibehörden Bayerns, Hamburgs und Bremens sowie der Grenzzolldienst Zugriff haben. Auch

gelten unterschiedliche Aussonderungsprüffristen für die gespeicherten personenbezogenen Daten. Gleichwohl kann auch mit Hilfe des BAN festgestellt werden, ob und welche Maßnahmen gegen eine Person bereits getroffen wurden. Gerade in dieser Recherchefunktion bestehen zwischen PAVOS-Zentral und dem BAN Anwendungsüberschneidungen. Schließlich sind auch der Personenkreis, über den Daten gespeichert werden, sowie der Umfang dieser Daten partiell identisch.

Inwieweit es vor diesem Hintergrund erforderlich ist, die Konzeption von PAVOS-Zentral einerseits und „BAN" andererseits zu überarbeiten, vermag ich derzeit nicht abschließend zu beurteilen, da dies auch von der endgültigen Gestaltung des Vorgangsbearbeitungs- und Recherchesystems abhängt. So habe ich einer Agenturmeldung entnommen, dass der BGS das von der Polizei Schleswig-Holstein verwendete Vorgangsbearbeitungssystem „@rtus" zu übernehmen beabsichtigt. Welche Auswirkungen dies auf die Konzeption von PAVOS-Zentral haben wird, bedarf noch der Erörterung.

Ich begrüße es daher, dass das BMI die Projektarbeitsgruppe „Datenschutz und BGS – bessere Lösungen für Grundrechtsschutz" damit beauftragt hat, die Datenanwendung PAVOS-Zentral und insbesondere deren Verhältnis zur Datei BAN zu untersuchen (vgl. Nr. 5.3.2).

5.3.4 Grenzüberschreitende Zusammenarbeit von Polizei- und Zollbehörden – Gemeinsame Zentren der Polizei in Kehl und in Luxemburg

Der Aufbau von gemeinsamen Lagezentren der Polizei- und Zollbehörden von Deutschland und seinen westlichen Nachbarstaaten schreitet voran.

Im 19. TB (Nr. 14.3) berichtete ich über einen Kontrollbesuch in dem gemeinsamen Zentrum der **deutsch-französischen Polizei- und Zollzusammenarbeit** in Offenburg, das zwischenzeitlich seinen Sitz nach Kehl verlegt hat. Soweit eine gemeinsame Verarbeitung personenbezogener Daten vor Ort erfolgt, hielt ich die Vorlage einer Errichtungsanordnung für das „Elektronische Tagebuch" im Zentrum für erforderlich. Diesem Petitum ist das BMI im November 2003 nachgekommen.

Durch einen Länderkollegen hatte ich im Oktober 2002 Kenntnis von einem Vertragsentwurf erhalten, der Rechtsgrundlage für eine **gemeinsame Stelle der grenzüberschreitenden Polizeizusammenarbeit** mit Sitz in Luxemburg werden soll. Beteiligte Staaten waren zunächst neben Deutschland das Königreich Belgien und das Großherzogtum Luxemburg, später auch Frankreich. Abgesehen davon, dass das Zentrum, das keine eigenständige Behörde ist, seinen Sitz außerhalb des deutschen Hoheitsgebietes hat, stellen sich je nach der Intensität der personenbezogenen Informationsverarbeitung ähnliche Probleme wie bei dem Zentrum in Kehl. Das gemeinsame Zentrum in Luxemburg ist am 25. Februar 2003 eröffnet worden. Der entsprechende Vertrag ist jedoch wegen eines Sprachvorbehalts noch nicht in Kraft getreten, so dass die Informationsverarbeitung in dem Zentrum auf nicht gesicherter Rechtsgrundlage abläuft.

Vor Abgabe einer datenschutzrechtlichen Beurteilung musste ich mir zunächst Klarheit über die Breite der Informationsverarbeitung in dem Zentrum verschaffen, zumal die ersten Vertragsentwürfe in dieser Hinsicht nicht eindeutig waren. Es macht einen Unterschied, ob die im Zentrum zu bearbeitenden grenzüberschreitenden Vorgänge nur zur Dokumentation in einer gemeinsamen Datei gespeichert werden oder ob diese Informationen auch zur Verhütung und Verfolgung von Straftaten operativ genutzt werden sollen. Der nach längeren Verhandlungen gefundenen datenschutzrechtlichen Lösung einer eigenständigen Datenverarbeitungsklausel für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten in der gemeinsamen Datei durch die beteiligten Stellen, ohne ergänzenden Rückgriff auf nationale Regelungen, konnte ich zustimmen. Das Regierungsübereinkommen war bei Redaktionsschluss noch nicht unterzeichnet.

5.3.5 Automatisierte und biometriegestützte Grenzkontrolle

Der BGS führt am Flughafen Frankfurt/Main ein Pilotprojekt zur automatisierten und biometriegestützten Grenzkontrolle durch. Die dabei gewonnenen Erkenntnisse müssen offen diskutiert werden.

Am 12. Februar 2004 wurde die automatisierte und biometriegestützte Grenzkontrolle am Flughafen Frankfurt/Main als Testverfahren durch den BGS in Betrieb genommen. Allen volljährigen Bürgerinnen und Bürgern aus EU- bzw. EWR-Mitgliedsstaaten wird hier die Möglichkeit geboten, die Grenze im Non-Schengen-Flugverkehr – also mit Staaten außerhalb des Schengener Vertragsgebiets – ohne manuelle Überprüfung durch die Grenzschutzbehörden zu überschreiten. Die Teilnehmer müssen ihre personenbezogenen Daten aus dem mitzuführenden Ausweisdokument und die biometrischen Merkmale ihrer Augeniris durch den BGS registrieren lassen. Die Daten werden digitalisiert und für die Dauer des Projekts verschlüsselt in einer Datenbank gespeichert. Bei nachfolgenden Grenzübertritten dienen sie dem Nachweis der biometrischen Verifikation, d h. sowohl bei der Registrierung als auch bei jedem Grenzübertritt werden die ausgelesenen Personendaten zur Abfrage des polizeilichen Informationssystems des Bundes und der Länder und des Schengener Informationssystems (SIS) weitergeleitet. Der Grenzübertritt wird automatisiert freigegeben, wenn die Verifikation anhand des Irisvergleichs gelingt und keine Fahndungsnotierung vorliegt. Mit dem Pilotprojekt soll getestet werden, ob sich die Iris als geeignetes biometrisches Merkmal zur Aufnahme in Reisedokumenten erweist und ob sich das Verfahren zur Erhöhung des Sicherheitsniveaus bei Grenzkontrollen sowie der Reduzierung von Wartezeiten für die Reisenden eignet.

Das Pilotprojekt habe ich von Beginn an begleitet. Dabei kam es mir besonders darauf an, dass die von den Teilnehmern in diesem Zusammenhang abzugebende Ein-

willigungserklärung über die Erhebung und Verarbeitung ihrer personenbezogenen Daten den Vorgaben des § 4a BDSG entspricht. Das BMI hat meine Empfehlungen für die inhaltliche Ausgestaltung der Einwilligungserklärung in wesentlichen Teilen übernommen.

Da es sich um ein Testverfahren handelt, hatte ich keine Einwände dagegen, dass die von den Teilnehmern erhobenen personenbezogenen Daten sowie die Merkmale ihrer Augeniris in einer vom BGS geführten Datenbank zentral gespeichert werden. Sollten die Iris oder andere biometrische Merkmale künftig in Ausweisdokumente aufgenommen werden, wäre eine Speicherung dieser Daten in einer zentralen Datei nach dem Passgesetz und dem geänderten Gesetz über Personalausweise unzulässig.

Inwieweit biometrische Merkmale in Personaldokumenten dazu beitragen können, die Identität der kontrollierten Personen verlässlich zu verifizieren, bleibt abzuwarten. Das BMI hat das Pilotprojekt, das zunächst auf sechs Monate befristet war, um weitere zwölf Monate verlängert. Nach Angaben des BMI haben sich bis August 2004 über 8 600 Reisende beim BGS für die Teilnahme an dem Testverfahren registrieren lassen. Mit Erkenntnissen über die Geeignetheit der Iriserkennung, die auch ich mir von dem Ergebnis des Pilotprojekts erwarte, wird jedoch in absehbarer Zeit nicht zu rechnen sein. Ich werde das Pilotprojekt auch in Zukunft begleiten.

Im Hinblick auf die Planungen zur obligatorischen Einführung biometrischer Merkmale in Personalpapiere halte ich es für dringend erforderlich, die Öffentlichkeit umfassend über die bei den Tests gewonnenen Erkenntnisse zu informieren. Dazu gehören insbesondere Angaben zur Zahl der Falscherkennungen und die zu Unrecht zurückgewiesenen Personen, die sich einer verschärften Kontrolle unterziehen müssen (vgl. hierzu auch Nr. 6.2).

5.3.6 Videoüberwachung auf Bahnhöfen

Der BGS nutzt die von der Deutschen Bahn AG (DB AG) auf Bahnhöfen eingesetzte Videoüberwachungstechnik zur Erfüllung bahnpolizeilicher Aufgaben. Die jeweiligen Verantwortlichkeiten der beteiligten Stellen müssen klar geregelt werden.

Bis 2001 wurden auf 22 Bahnhöfen sog. „3-S-Zentralen“ eingerichtet, die von der DB AG zur Erfüllung ihrer aus dem Hausrecht erwachsenden Aufgaben betrieben werden. Insbesondere findet eine ständige Videoüberwachung des gesamten Bahnhofsbereichs statt. Der BGS, der gem. § 27 Satz 1 Nr. 2 i.V.m. § 23 Abs. 1 Nr. 4 BGSG befugt ist, selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte einzusetzen, um Gefahren für Anlagen und Einrichtungen der Eisenbahn und der sich dort befindlichen Personen und Sachen zu erkennen, nutzt die Videotechnik der DB AG ebenfalls zur Erfüllung dieser Aufgaben. Zu diesem Zweck überspielt die DB AG die Videoaufnahmen auf einen dem BGS zur alleinigen Nutzung zur Verfügung gestellten Ringspeicher. Ein Zugriff auf die darauf gespeicherten Bilddaten ist nur autorisierten Mitarbeitern des BGS möglich.

Als Folge eines Bombenkofferfundes am Dresdner Hauptbahnhof im Juni 2003 ist in der Videoüberwachungszentrale der DB AG zusätzlich ein ständig von einem BGS-Bediensteten besetzter Arbeitsplatz eingerichtet worden. Von diesem Platz aus kann der BGS anlassbezogen bestimmte Bereiche des Bahnhofs gezielt videoüberwachen, indem er die Führung der betreffenden Kamera selbst bestimmt.

Im Herbst 2004 habe ich die Videoüberwachung durch den BGS am Kölner Hauptbahnhof kontrolliert. Sie begegnet mit wenigen Einschränkungen keinen datenschutzrechtlichen Bedenken: So habe ich festgestellt, dass auf dem durch den BGS genutzten Ringspeicher Datensätze erfasst waren, die weder zur Abwehr einer gegenwärtigen Gefahr noch zur Verfolgung einer Straftat oder Ordnungswidrigkeit (§ 27 Satz 3 BGSG) benötigt wurden und somit hätten gelöscht werden müssen. Zudem ist die Transparenz der Videoüberwachung im Kölner Hauptbahnhof verbesserungsbedürftig. Der Einsatz selbsttätiger Bildaufnahme- und Bildaufzeichnungsgeräte durch den BGS muss gem. § 23 Satz 2 BGSG erkennbar sein. Jeder muss ohne weiteres erkennen können, dass er sich im Einzugsbereich hoheitlich betriebener Videoüberwachung befindet. Da die Videoüberwachung sowohl durch die DB AG als auch durch den BGS durchgeführt wird, halte ich es für geboten, beide als verantwortliche Stelle auf entsprechenden Hinweistafeln auszuweisen. Diese Maßnahmen sind auf allen Bahnhöfen umzusetzen, die vom BGS videoüberwacht werden.

Indem die DB AG dem BGS die von ihren Videokameras erfassten Bilddaten beschafft, liegt eine Auftragsdatenverarbeitung der DB AG für den BGS vor. Ich habe das BMI auf die Notwendigkeit einer schriftlichen Auftragserteilung, die den Anforderungen des § 11 BDSG Rechnung trägt, hingewiesen. Diese lag, wie auch die Stellungnahme zu meinem Kontrollbericht, bei Redaktionsschluss noch nicht vor.

5.3.7 Fußball-Weltmeisterschaft 2006

Die Fußball-Weltmeisterschaft 2006 wirft eine Reihe datenschutzrechtlicher Fragen auf. Sie betreffen vor allem die Ausgestaltung des derzeit vom Bund und den Ländern erarbeiteten polizeilichen Rahmenkonzepts und den Verkauf der Eintrittskarten.

Seit geraumer Zeit befasse ich mich mit den datenschutzrechtlichen Aspekten der Vorbereitung und Durchführung der Fußball-Weltmeisterschaft 2006. Dabei stimme ich mich eng mit dem eidgenössischen Datenschutzbeauftragten und den Datenschutzaufsichtsbehörden und Datenschutzbeauftragten der Länder ab.

Durch die IMK ist ein Bund-Länder-Ausschuss eingerichtet worden, der unter Leitung des BMI ein „Nationales Sicherheitskonzept“ erarbeiten soll. Das Kernstück

dieses Sicherheitskonzepts bildet ein polizeiliches Rahmenkonzept über den Einsatz und die Aufgaben der Polizeien des Bundes und der Länder. Für mich ist hier von besonderem Interesse, in welchem Umfang personenbezogene Daten von Stadionbesuchern erhoben und verarbeitet werden sollen.

Auch die beabsichtigte Personalisierung der Eintrittskarten und der Einsatz von RFID-Chips werfen datenschutzrechtliche Fragen auf. Bei der Online-Ticketbestellung werden personenbezogene Daten des Bestellers erhoben. Um zu verhindern, dass Personen, denen gegenüber ein Stadionverbot ausgesprochen wurde, Eintrittskarten erhalten, werden diese Daten mit der beim Deutschen Fußballbund (DFB) geführten Stadionverbotsdatei abgeglichen. Ein Abgleich mit der von den Polizeien des Bundes und der Länder geführten Datei „Gewalttäter Sport" findet dagegen nicht statt. Einige der bei der Ticketbestellung erhobenen personenbezogenen Daten wie Name, Geburtsdatum, Pass- oder Personalausweisnummer, werden auf die Eintrittskarte gedruckt. Es ist vorgesehen, die Kontrolle des Zugangs zu den Stadien in mehreren Phasen durchzuführen. Bei einer stichprobenartig durchgeführten Ausweiskontrolle erfolgt ein optischer Abgleich des Ausweispapiers mit dem Ticketaufdruck. Im Rahmen einer weiteren technischen Kontrolle wird geprüft, ob die auf dem RFID-Chip gespeicherten Daten mit den Daten aus dem Ticketverkaufssystem identisch sind. Erhebliche Zweifel habe ich an der Zulässigkeit der Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer von Karteninteressenten, die der DFB aufgrund entsprechender Sicherheitsempfehlungen des BMI vorsieht. Nach dem Pass- bzw. Personalausweisgesetz ist die Verwendung der Seriennummer im nicht-öffentlichen Bereich unzulässig, soweit mit ihrer Hilfe ein Abruf personenbezogener Daten aus Dateien oder eine Verknüpfung von Dateien möglich ist. Der Gesetzgeber wollte damit die Gefahr einer Nutzung der Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit nicht als Ordnungsmerkmal gespeichert werden. Aber auch darüber hinaus halte ich die Verwendung der Seriennummer durch den DFB nicht für erforderlich, wenn diese nur der Legitimation des Ticketinhabers beim Zutritt zu den Stadien dienen soll.

Meine Bedenken habe ich gegenüber dem BMI und dem für die datenschutzrechtliche Bewertung des Ticketing-Konzepts zuständigen Regierungspräsidium Darmstadt geäußert und angeregt, das Verfahren dadurch datenschutzfreundlicher zu gestalten, indem nur ein Teil der Seriennummer erfasst wird.

Die mit der Vorbereitung und Durchführung der Fußball-Weltmeisterschaft 2006 verbundenen datenschutzrechtlichen Aspekte können erst dann abschließend bewertet werden, wenn alle erforderlichen Informationen über die beabsichtigten Maßnahmen vorliegen. Ich rechne damit, dass mir das BMI die erbetenen Auskünfte kurzfristig erteilen wird.

5.3.8 Kontrolle der Ausschreibungen gem. Artikel 96 Abs. 2 des Schengener Durchführungsübereinkommens durch die Grenzschutzdirektion

Die Grenzschutzdirektion schreibt aufgrund der Erkenntnismitteilung anderer öffentlicher Stellen Drittausländer zur Einreiseverweigerung im SIS aus. Als problematisch erwiesen sich Ausschreibungen aufgrund von Informationen des BfV.

Im Sommer 2003 führte ich in der Grenzschutzdirektion einen Beratungs- und Kontrollbesuch durch, bei dem ich die von ihr vorgenommenen Ausschreibungen zur Einreiseverweigerung im SIS gem. Artikel 96 Abs. 2 SDÜ überprüfte. Die Situation ist dadurch gekennzeichnet, dass die Erkenntnisse, die die Grenzschutzdirektion zum Anlass für die Ausschreibungen nimmt, von anderen öffentlichen Stellen – u. a. BfV, BKA und deutsche Auslandsvertretungen – übermittelt werden. Die Grenzschutzdirektion trägt jedoch die Verantwortung für die Rechtmäßigkeit der Ausschreibungen. Dieser Verantwortung kann sie aber nur gerecht werden, wenn sie den Sachverhalt dahingehend bewertet, ob eine Gefahr für die öffentliche Sicherheit und Ordnung oder die nationale Sicherheit für die Bundesrepublik Deutschland oder einen anderen Schengen-Vertragsstaat besteht. Dies setzt aber voraus, dass der Grenzschutzdirektion konkrete Tatsachen übermittelt werden, die es ihr ermöglichen, das Vorliegen einer Gefahrenlage nach polizeirechtlichen Maßstäben selbst festzustellen.

In vielen der von mir geprüften Ausschreibungsersuchen haben die ihnen zugrunde liegenden Erkenntnismitteilungen diesen Anforderungen nicht genügt. Denn die übermittelnden Stellen beschränken sich auf die Übermittlung der eigenen Einschätzung der Gefahrenlage, ohne dass die Fakten, die zu dieser Einschätzung geführt haben, der Grenzschutzdirektion mitgeteilt werden. Gleichwohl hat die Grenzschutzdirektion allein auf Basis dieser Erkenntnismitteilungen die betreffenden Personen im SIS ausgeschrieben. Die Grenzschutzdirektion hat damit ohne ausreichende Beurteilungsgrundlage die Verantwortung für die Rechtmäßigkeit der von ihr im SIS gespeicherten Datensätze übernommen. Sinn und Zweck der Regeln zur datenschutzrechtlichen Verantwortung laufen damit ins Leere.

Das BMI hat im Wege eines Erlasses diesem Mangel Rechnung getragen. Danach sind der Grenzschutzdirektion Erkenntnisse so zu übermitteln, dass es ihr aufgrund des Inhalts möglich ist, das Vorliegen der Voraussetzungen für eine Ausschreibung im konkreten Einzelfall eigenständig zu bewerten. Der Erlass bezieht sich jedoch nur auf Erkenntnismitteilungen des BfV. Bei Informationen des BKA soll die Grenzschutzdirektion weiterhin darauf vertrauen dürfen, dass das BKA die polizeiliche Bewertung der Ausschreibungsvoraussetzungen nach Artikel 96 Abs. 2 SDÜ bereits selbst sachgerecht vorgenommen hat. Da die Grenzschutzdirektion aber auch in diesen Fällen die datenschutzrechtliche Verantwortung für die Richtigkeit der Ausschreibung trägt, halte ich es

für geboten, den Erlass des BMI auf Ausschreibungsersuchen anderer Behörden auszudehnen.

SIS-Ausschreibungen der Grenzschutzdirektion aufgrund von Erkenntnismitteilungen des BfV beinhalten eine weitere Problematik. Das SIS ist ausschließlich ein polizeiliches Fahndungssystem, in dem nur Informationen gespeichert werden dürfen, wenn eine Gefahrenlage nach polizeirechtlichen Maßstäben vorliegt. Eine Ausnahme sieht das Übereinkommen nur für Ausschreibungen zur verdeckten Registrierung oder gezielten Kontrolle gem. Artikel 99 SDÜ vor. Danach können diese Ausschreibungen – soweit das nationale Recht dies erlaubt – auch auf Veranlassung der Nachrichtendienste eines Mitgliedstaats erfolgen. Diese Ausnahme ist bei Ausschreibungen nach Artikel 96 SDÜ jedoch nicht einschlägig. Das BfV hat weder das Recht, auf die darin gespeicherten Daten zuzugreifen, noch Ausschreibungen darin vorzunehmen bzw. durch die Grenzschutzdirektion vornehmen zu lassen.

Das BMI ist hingegen der Auffassung, dass das BfV gem. § 19 Abs. 1 Bundesverfassungsschutzgesetz (BVerfSchG) befugt ist, u. a. auch der Grenzschutzdirektion Informationen zu übermitteln, wenn diese die Daten zum Schutz der freiheitlichen demokratischen Grundordnung oder sonst für Zwecke der öffentlichen Sicherheit benötigt. Gem. § 19 Abs. 1 Satz 2 BVerfSchG dürfe die Grenzschutzdirektion diese Daten auch verwenden und damit zum Anlass für eine polizeiliche Ausschreibung im SIS nehmen. Auf die Problematik des Artikel 99 Abs. 3 SDÜ geht das BMI dabei nicht ein.

Mit dem BMI konnte bereits vor Jahren Einvernehmen erzielt werden, dass es als Nationale Sicherheitsbehörde berechtigt ist, Ausschreibungen nach Artikel 96 Abs. 2 SDÜ in begründeten Ausnahmefällen zu veranlassen, nachdem es sich zuvor über die Verlässlichkeit der zugrunde liegenden Quellenmeldung vergewissert hat. Von diesem Kompromiss ist das BMI allerdings wieder abgerückt.

Die auf der Grundlage von Erkenntnissen des BfV von der Grenzschutzdirektion im SIS zur Einreiseverweigerung vorgenommenen Ausschreibungen habe ich am 03. Februar 2004 gem. § 25 Abs. 1 BDSG wegen Verstoßes gegen Artikel 96 Abs. 2 SDÜ beanstandet.

Im Rahmen der Kontrolle habe ich zudem festgestellt, dass die Möglichkeit zur Ausschreibung auch dazu genutzt wird, Personen, deren Anwesenheit erhebliche Belange der Bundesrepublik Deutschland beeinträchtigen würde, zur Einreiseverweigerung auszuschreiben. Dies betraf in den USA lebende Personen, denen die Beteiligung an NS-Gewalttaten zur Last gelegt wurde, sowie Personen, denen im Rahmen des zu Anfang des Jahres 2003 aktuellen Transnistrien-Konflikts in der Republik Moldau seitens der EU die Ein- und Durchreise in die Mitgliedstaaten der EU verweigert werden sollte. Diese Personen wurden aufgrund meiner Hinweise mittlerweile im SIS gelöscht. Hingegen bleiben die vom BKA veranlassten SIS-Ausschreibungen von Personen bestehen, zu denen Rechtshilfeersuchen anderer Staaten vorliegen, deren Rechtssystem durch die Anwendung von Folter und Todesstrafe gekennzeichnet ist. Zwar wird den ausgeschriebenen Personen von den Behörden der betreffenden Staaten die Begehung schwerer Straftaten vorgeworfen. Sie könnten damit in die Kategorie von Drittausländern fallen, die gem. Artikel 96 Abs. 2b SDÜ zur Einreiseverweigerung ausgeschrieben werden dürften. Nach meinen Feststellungen ist das Ausschreibungsinstrument hier aber genutzt worden, um Personen, die wegen des im ersuchenden Staat bestehenden Rechts- und Justizsystems nicht nach dorthin ausgeliefert werden können, vom Hoheitsgebiet der Bundesrepublik Deutschland fernzuhalten. Dies ist mit dem Ziel des SIS nicht vereinbar, das u. a. auf die Gewährleistung der öffentlichen Sicherheit und Ordnung in den Mitgliedstaaten gerichtet ist.

5.4 Zollfahndung

5.4.1 Durchführung des Zollfahndungsneuregelungsgesetzes

Bei der Informationsverarbeitung von Zollkriminalamt und Zollfahndung werden weiterhin Richtlinien und Errichtungsanordnungen angewandt, die noch nicht an das Zollfahndungsneuregelungsgesetz angepasst worden sind.

Mit Inkrafttreten des Zollfahndungsneuregelungsgesetzes am 24. August 2002 wurden die für die Tätigkeit des ZKA und der Zollfahndungsämter erforderlichen bereichsspezifischen Datenschutzregelungen in Form des Zollfahndungsdienstgesetzes (ZFdG) geschaffen (vgl. 19. TB Nr. 15.1). Damit war die letzte Regelungslücke im Bereich der Polizeien des Bundes geschlossen.

Anlässlich von Eingaben, die eine datenschutzrechtliche Überprüfung beim ZKA zur Folge hatten, habe ich jedoch festgestellt, dass in der Praxis weiterhin auf die Richtlinien für die Datei „INZOLL“ zurückgegriffen wird, ohne dass diese der neuen Gesetzeslage angepasst worden sind. Dies habe ich auch im Rahmen einer datenschutzrechtlichen Kontrolle der Geldwäschebekämpfung beim Zoll festgestellt (vgl. Nr. 5.4.2).

Seit Jahresbeginn 2004 werden vom BMF Errichtungsanordnungen für vom Zoll benötigte DV-Anwendungen mit Blick auf das ZFdG überarbeitet. Bei den mir zur Anhörung nach § 41 Abs. 1 ZFdG bereits zugeleiteten Errichtungsanordnungen konnte ich feststellen, dass deren Überarbeitung in Umsetzung des ZFdG nahezu abgeschlossen ist. Das BMF hat mir zugesichert, auch die „Richtlinien INZOLL“ in nächster Zeit entsprechend zu überarbeiten. Diese Entwicklung und die Umsetzung in der Praxis werde ich weiterhin kritisch begleiten.

5.4.2 Geldwäschebekämpfung beim Zollkriminalamt

Ein Beratungs- und Kontrollbesuch zu den beim Zoll vorgenommenen Maßnahmen zur Geldwäschebekämpfung bei der Gemeinsamen Finanzermittlungsgruppe (GFG) Nordrhein-Westfalen hat Hinweise auf teilweise unzulässig lange Speicherungen ergeben.

Die GFG Nordrhein-Westfalen, in der Bedienstete des Zolls und des Landeskriminalamts (LKA) Nordrhein-Westfalen zusammenarbeiten, ist Clearingstelle des Landes Nordrhein-Westfalen (vgl. auch Nr. 5.2.2). Die Datenverarbeitung in Zusammenhang mit der Geldwäschebekämpfung erfolgt beim Zoll in der Datei „INZOLL-VHG“. Anlässlich meiner Kontrolle habe ich auch die Zusammenarbeit zwischen den Bediensteten des Zolls und des LKA geprüft und dabei folgendes festgestellt:

Der Großteil der in der Datei gespeicherten Datensätze beruht auf Geldwäscheverdachtsanzeigen der nach dem Geldwäschegesetz zur Anzeige Verpflichteten. Seit März 2004 werden in die Datei allerdings nur noch Daten eingestellt, die durch an den deutschen Grenzübergängen und Flughäfen durchgeführte Bargeldkontrollen (vgl. 19. TB Nr. 15.2) gewonnen wurden, soweit sich bei diesen Anhaltspunkte für Geldwäsche ergeben haben. Die Datei dient dem Clearingverfahren, d.h. der Bewertung des Sachverhalts im Hinblick auf eine Erhärtung des Geldwäscheverdachts durch Abgleich der Daten mit anderen Dateien des Zolls und der Polizei. In Anwendung der im Jahr 1999 letztmals überarbeiteten Errichtungsanordnung zur Datei „INZOLL-VHG“ erfolgt die Speicherung in jedem Fall bis zum 31. Dezember des sechsten auf das Erfassungsjahr folgenden Jahres. Diese Vorgehensweise halte ich für sehr bedenklich, da sie die Regelungen des bereits im August 2002 in Kraft getretenen ZFdG, nach denen die Aussonderungsprüffristen dem Status als Beschuldigter, Verdächtiger, Kontakt- oder Begleitperson o. ä. entsprechend zu differenzieren sind, außer Acht lässt (vgl. Nr. 5.4.1). Allerdings ist eine Überarbeitung der Errichtungsanordnung in Zusammenhang mit der für das Jahr 2005 geplanten Einführung des Systems „INZOLL-neu“ geplant. Bei dieser Gelegenheit müssen verkürzte Speicherfristen für jene Fälle festgelegt werden, bei denen sich der Geldwäscheverdacht im Clearingverfahren nicht erhärtet hat.

Als problematisch sehe ich auch die Tatsache an, dass die im Rahmen einer Bargeldkontrolle mit Geldwäscheverdacht erhobenen Daten dem LKA zur Einstellung in die Datei „FINDUS“ übermittelt werden. Ich habe erhebliche Zweifel, ob diese Vorgehensweise von § 33 Abs. 1 ZFdG abgedeckt wird, da die Rechtsvorschrift eine Einzelfallprüfung hinsichtlich der Erforderlichkeit der Datenübermittlung voraussetzt.

5.4.3 Gesetzgeberische Konsequenzen aus dem Beschluss des Bundesverfassungsgerichts vom 3. März 2004 zu den §§ 39 und 41 Außenwirtschaftsgesetz

Das Bundesverfassungsgericht hat die Ermächtigung zur Telekommunikations- und Postüberwachung gemäß §§ 39 ff. Außenwirtschaftsgesetz (AWG) für verfassungswidrig erklärt. Bei der gesetzlichen Neuregelung sind die Grundsätze zu beachten, die in dem Urteil zur akustischen Wohnraumüberwachung niedergelegt sind.

Am 3. Dezember 2004 verabschiedete der Deutsche Bundestag das Gesetz zur Neuregelung der präventiven Telekommunikations- und Postüberwachung durch das Zollkriminalamt. Das Gesetz war notwendig geworden, nachdem das BVerfG mit Beschluss vom 3. März 2004 (1 BvF 3/92) festgestellt hatte, dass die §§ 39 und 41 AWG nicht mit Artikel 10 GG vereinbar sind. Insbesondere hatte das Gericht bemängelt, dass die Ermächtigung zu Telekommunikations- und Postüberwachung zum Zwecke der Straftatenverhütung nicht den rechtsstaatlichen Anforderungen an die Normenbestimmtheit und -klarheit genügten. Zugleich wurde dem Gesetzgeber aufgegeben, bei einer Neuregelung dieser Befugnisse auch die Grundsätze zu beachten, die das Gericht in seinen Urteilen vom 14. Juli 1999 zum G 10-Gesetz (BVerfGE 100, 313) sowie vom 3. März 2004 zur akustischen Wohnraumüberwachung – 1 BvR 2378/98 – (vgl. Nr. 5.1.2, 7.1.1) niedergelegt hat.

Das vom Deutschen Bundestag nunmehr beschlossene Gesetz, an dessen Ausarbeitung ich von Beginn an beteiligt war, ist von dem Ziel gekennzeichnet, diese Vorgaben umzusetzen:

- Die materiellen Voraussetzungen für die Durchführung einer Telekommunikations- und Postüberwachung wurden konkretisiert und damit normenklarer geregelt. Anknüpfungspunkt für die Eingriffsmaßnahmen ist die auf Tatsachen gestützte Prognose, dass der Betroffene bestimmte im Gesetz enumerativ aufgezählte Straftaten vorbereitet.
- Normenklarer geregelt sind zudem die Zwecke, zu denen die aus der Überwachungsmaßnahme erlangten Daten an andere öffentliche Stellen übermittelt werden dürfen, nämlich durch Auflistung der Empfängerbehörden und Benennung des Zwecks, zu dem die Daten übermittelt werden, u. a. zur Verhütung bestimmter, im Gesetz aufgezählter Straftaten.
- Die aus der Überwachungsmaßnahme erlangten Daten müssen gekennzeichnet werden. Die Kennzeichnung ist auch von der Stelle, an die die Daten übermittelt wurden, aufrecht zu erhalten.
- Von einer Unterrichtung der von den Überwachungsmaßnahmen Betroffenen kann nur in wenigen, im Gesetz genannten Fällen abgesehen werden.
- Die für die Bundesregierung bestehende Berichtspflicht gegenüber dem Deutschen Bundestag wurde dahingehend ergänzt, dass jetzt auch die Ermächtigungsgrundlagen für die präventive Telekommunikations- und Postüberwachung evaluiert werden müssen.

Ein wesentlicher Aspekt der verfassungsgerichtlichen Rechtsprechung bleibt jedoch unberücksichtigt, denn im Gesetz fehlen Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung. Aus meiner Sicht ist das Absehen von jeglicher kernbereichsschützender Regelung in dem Gesetz mit hohem verfassungsrechtlichem Risiko verbunden (vgl. Nr. 5.1.2; 7.1.3). Der Rechtsausschuss des Deutschen Bundestages war daher der Auffassung,

dass diese Frage noch sorgfältig zu prüfen sei. Auf seinen Vorschlag hin wurden die Regelungen zur präventiven Telekommunikations- und Postüberwachung durch das ZKA auf ein Jahr bis zum 31. Dezember 2005 befristet. Dies begrüße ich ausdrücklich.

Erstmals wird in dem neugefassten AWG auch die Kennung des Endgerätes (IMEI = International Mobile Equipment Identity) als Anknüpfungspunkt für heimliche Überwachungsmaßnahmen normiert. Im Rahmen des Gesetzgebungsverfahrens hatte ich auf die Risiken verwiesen, die damit verbunden sind. Sowohl der Herstellungsprozess von Handys als auch nachträgliche Manipulationen durch Kunden können dazu führen, dass eine große Anzahl von Geräten die gleiche IMEI erhalten. Von einer angeordneten Überwachungsmaßnahme würden damit ggf. auch unbescholtene Personen erfasst werden. Ich begrüße es deshalb, dass nach dem Gesetz eine Überwachungsmaßnahme auf der Grundlage der Endgerätenummer nur stattfinden darf, wenn sich die Kennung eindeutig der zu überwachenden Person zuordnen lässt. Es bleibt allerdings noch abzuwarten, ob sich diese gesetzliche Konzeption in der Praxis bewährt oder ob – wie von mir ursprünglich vorgeschlagen – auf die Kennung des Endgerätes als Anknüpfungspunkt für Überwachungsmaßnahmen im Gesetz gänzlich verzichtet werden sollte.

5.5 Verfassungsschutz

5.5.1 Nutzung von NADIS auch für Zwecke der Bekämpfung der Organisierten Kriminalität

Landesämter für Verfassungsschutz (LfV), denen die Beobachtung der Organisierten Kriminalität (OK) als gesetzliche Aufgabe übertragen wurde, nutzen NADIS zur Erfüllung ihrer gemeinsamen Unterrichtungspflicht nach § 5 Abs. 1 BVerfSchG. Da die Beobachtung der OK nicht zu den Aufgaben des BfV gehört, muss sich seine Beteiligung auf die technische Unterstützung beschränken.

Den LfV der Länder Bayern, Hessen, Saarland, Sachsen und Thüringen wurde – im Gegensatz zum BfV und den übrigen LfV – durch das jeweilige Verfassungsschutzgesetz die Beobachtung der OK als gesetzliche Aufgabe zugewiesen. Zur Erfüllung ihrer gegenseitigen Unterrichtungsverpflichtungen aus § 5 Abs. 1 BVerfSchG bzw. den entsprechenden landesrechtlichen Bestimmungen sind diese Länder an das BfV mit dem Wunsch herangetreten, in NADIS einen separaten Teilbestand für den Bereich OK einzurichten. Gegen diese erweiterte Nutzung von NADIS habe ich rechtliche Bedenken geltend gemacht: NADIS dürfe nur im Rahmen des § 6 BVerfSchG genutzt werden, der hinsichtlich der Speicherung personenbezogener Daten auf die §§ 10 und 11 und damit auf den Aufgabenkatalog des § 3 Abs. 1 BVerfSchG verweist.

Nach der geltenden Regelung des § 3 BVerfSchG hat das BfV – im Gegensatz zu den oben genannten LfV – keine Kompetenz zur Beobachtung der OK. Ausgehend von dieser Kompetenzzuweisung dürfen in NADIS von den Ländern nur solche Daten eingestellt werden, die auf einer dem Aufgabenbereich des BfV entsprechenden Rechtsgrundlage erhoben worden sind.

Das BMI vertritt hingegen die Auffassung, die sich aus § 6 Satz 3 i.V.m. § 10 BVerfSchG ergebende Beschränkung von Speichervoraussetzungen in NADIS auf den Aufgabenbereich des § 3 BVerfSchG setze lediglich voraus, dass es sich um eine gemeinsame Datei aller Verfassungsschutzbehörden unter Beteiligung des BfV handelt. Ein solcher gemeinsamer Datenbestand OK aller Verfassungsschutzbehörden sei aber nicht vorgesehen. Beabsichtigt sei lediglich, den betreffenden Landesbehörden die NADIS-Plattform zur Schaffung eines separaten Datenbestandes zur Verfügung zu stellen, auf den weder das BfV noch die übrigen nicht für die Beobachtung der OK zuständigen LfV Zugriff nehmen könnten. Einem solchen Teil-Datenbestand stehe § 6 BVerfSchG nicht entgegen. Es handele sich um eine Verbunddatei eigener Art.

Eine Annäherung der gegensätzlichen Standpunkte konnte auch nach intensiven Erörterungen mit dem BMI und dem BfV nicht erreicht werden. Ich habe letztlich meine Bedenken zurückgestellt, nachdem das BMI zugesagt hatte, von mir geforderte Restriktionen bei der Beteiligung an diesem Projekt zu beachten.

Ob diese in der Praxis eingehalten werden, werde ich bei nächster Gelegenheit kontrollieren.

5.5.2 Ausbau der IT-Struktur beim BfV

Die Einführung der elektronischen Akte macht auch vor dem BfV nicht halt.

Im Rahmen der eGovernment-Strategie der Bundesregierung hat das BfV mit der Umsetzung des DOMEA-Konzeptes („DOMEA"®=Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang) begonnen. Das DOMEA-Konzept beschreibt das Verfahren zur Einführung der elektronischen Akte in der öffentlichen Verwaltung. Wie berichtet (18. TB Nr. 14.1), bestand zwischen dem BfV und mir Einvernehmen, dass die elektronische Aktenführung eine Änderung der §§ 10 und 11 BVerfSchG erforderlich macht.

Wenn das komplette Schriftgut des BfV in der Datei DOMUS elektronisch erfasst und gespeichert wird, können auch Daten über Personen in DOMUS gespeichert werden, deren Daten das BfV nach geltendem Recht nicht in Dateien speichern darf (vgl. §§ 10 Abs. 1, 11 Abs. 1 Satz 2 BVerfSchG), wohl aber in Akten. Technisch wäre es möglich, auch diese Daten in Sekundenbruchteilen elektronisch zu erschließen. Um dies auszuschließen, hatte ich vom BfV gefordert sicherzustellen, dass eine elektronische Recherche nur zu solchen Personen erfolgen kann, deren Daten nach geltendem Recht automatisiert gespeichert werden dürfen. In der mir vorgelegten Dateianordnung hat das BfV diese Beschränkung der Recherchebefugnis ausdrücklich geregelt. Auch wurde die systemseitige Protokollierung sämtlicher Zugriffe für die datenschutzrechtliche Kontrolle in die Dateianordnung aufgenommen.

DOMUS unterstützt das BfV auch bei der Mitwirkung an Sicherheitsüberprüfungen gemäß § 3 Abs. 2 BVerfSchG. Die Mitwirkung des BfV an dieser Überprüfung von Personen, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen, richtet sich nach dem Sicherheitsüberprüfungsgesetz (vgl. § 1 Abs. 1 SÜG). Die umfassende Speicherung personenbezogener Daten in einer „elektronischen Akte“ widerspricht dem SÜG. Dort hat der Gesetzgeber ausdrücklich entschieden, dass nur wenige Grunddaten der von dem Betroffenen in einem Datenerhebungsbogen umfänglich anzugebenden Daten in Dateien gespeichert werden dürfen (Name, Vorname, Geburtsdatum, Geburtsort, Staatsangehörigkeit, Familienstand, ausgeübter Beruf, Wohnsitze und Aufenthalte – vgl. im Einzelnen § 13 Abs. 1 Nr. 1 bis 6 SÜG). Angesichts dieser gesetzlichen Vorgabe habe ich das BfV aufgefordert, personenbezogene Daten, die das BfV im Rahmen seiner Mitwirkung an einer Sicherheitsüberprüfung erlangt hat, erst nach einer entsprechenden Änderung des SÜG in DOMUS zu speichern, die eine Recherche nach Daten, die nicht dateimäßig gespeichert werden dürfen, ausschließt. Das BfV hat zugesagt, die Umsetzung des DOMEA-Konzeptes zunächst auf die Aufgabenerfüllung nach § 3 Abs. 1 BVerfSchG zu beschränken, d. h. nur solche personenbezogene Daten in DOMUS zu speichern, die es im Rahmen der Beobachtung von Bestrebungen und Tätigkeiten im Sinne des § 3 Abs. 1 BVerfSchG erlangt hat.

5.5.3 Meinungsaustausch mit BMI und BfV über datenschutzrechtliche Probleme

Der regelmäßige Meinungsaustausch hat sich bewährt.

Im Jahr 2004 habe ich mit dem BMI und dem BfV regelmäßig Gespräche geführt, in denen zeitnah und konstruktiv aktuelle datenschutzrechtliche Probleme und Fragestellungen, beispielsweise zu DOMEA (vgl. Nr. 5.5.2) sowie die verstärkte Kooperation der Sicherheitsbehörden (vgl. Nr. 5.5.1) und die Ergebnisse durchgeführter Kontrollen erörtert wurden. Diese Gespräche wurden von allen Beteiligten positiv bewertet, da sie wesentlich zur Lösung bzw. Vermeidung datenschutzrechtlicher Probleme sowie zur Intensivierung der vertrauensvollen Zusammenarbeit beigetragen haben.

Aus diesem Grunde besteht Einvernehmen, diesen regelmäßigen Meinungsaustausch fortzuführen.

5.5.4 Evaluierung der Eingriffsbefugnisse aufgrund des Terrorismusbekämpfungsgesetzes von 2002

Durch das Terrorismusbekämpfungsgesetz (TBG) haben die Sicherheitsbehörden neue Befugnisse erhalten. Von zentraler Bedeutung ist die Evaluierung dieser Befugnisse.

Die durch das TBG neu geschaffenen Befugnisse der Sicherheitsbehörden sind nach Artikel 22 Abs. 3 TBG vor Ablauf der Geltungsdauer dieses Gesetzes (10. Januar 2007) zu evaluieren.

Die Evaluierung der dem BfV, BND und MAD gewährten Befugnisse (vgl. Artikel 1 bis 3 TBG) richtet sich nach § 8 Abs. 10 BVerfSchG. Demnach erstattet das Parlamentarische Kontrollgremium (PKGr) dem Deutschen Bundestag nach Ablauf von drei Jahren nach Inkrafttreten des TBG (1. Januar 2005) zusammenfassend zum Zweck der Evaluierung einen Bericht über die Durchführung sowie über Art, Umfang und Anordnungsgründe der aufgrund der neuen Befugnisse angeordneten Maßnahmen. Wie im 19. TB (Nr. 2.3.1) dargelegt, gehe ich davon aus, dass das PKGr die Evaluierung, ggf. mit wissenschaftlicher Begleitung, auf der Grundlage der Berichte der Ministerien (vgl. § 8 Abs. 10 Satz 1 BVerfSchG) durchführen soll.

Kasten zu Nr. 5.5.4

§ 8 Abs. 10 BVerfSchG:

Satz 1

Das nach Absatz 9 Satz 3 zuständige Bundesministerium unterrichtet im Abstand von höchstens sechs Monaten das Parlamentarische Kontrollgremium über die Durchführung der Absätze 5 bis 9; dabei ist insbesondere ein Überblick über Anlass, Umfang, Dauer, Ergebnis und Kosten der im Berichtszeitraum durchgeführten Maßnahmen nach den Absätzen 5 bis 8 zu geben.

Satz 2

Das Gremium erstattet dem Deutschen Bundestag jährlich sowie nach Ablauf von drei Jahren nach Inkrafttreten dieses Gesetzes zusammenfassend zum Zweck der Evaluierung einen Bericht über die Durchführung sowie Art, Umfang und Anordnungsgründe der Maßnahmen nach den Absätzen 5 bis 8; dabei sind die Grundsätze des § 5 Abs. 1 des Kontrollgremiumgesetzes zu beachten.

Das BMI hatte mir mitgeteilt, dass es, der zeitlichen Vorgabe im Koalitionsvertrag folgend, der eine Evaluierung bis Mitte der Legislaturperiode vorsieht, zur Prüfung und Aufbereitung eines etwaigen gesetzgeberischen Handlungsbedarfs in Bezug auf die TBG-Befugnisse entsprechende Daten beim BfV erheben werde. Angesichts der dem PKGr obliegenden Evaluierungspflicht (vgl. § 8 Abs. 10 Satz 2 BVerfSchG) hatte ich das BMI gebeten, diese Datenerhebung auch zur Unterrichtung des PKGr durchzuführen, zumal die Prüfung eines gesetzgeberischen Handlungsbedarfs nur auf der Grundlage dieser Evaluierung zu belastbaren Ergebnissen führen kann. Bedauerlicherweise ist das BMI meiner Anregung nicht gefolgt.

Das PKGr hat mir mitgeteilt, dass es auf der Grundlage der ihm zugeleiteten Halbjahresberichte (vgl. § 8 Abs. 10 Satz 1 BVerfSchG) voraussichtlich bis Mitte 2005 einen Evaluierungsbericht erstellen und dem Deutschen Bundestag zum Zweck der Evaluierung zuleiten werde.

5.5.5 Datenschutzrechtliche Kontrollen beim BfV – Probleme mit der Kontrollkompetenz

Meine Kontrollbefugnis erstreckt sich auch auf die Kontrolle der Datenverarbeitungsprogramme beim Verfassungsschutz. Aus Quellenschutzgründen darf eine Beschränkung meiner Kontrollbefugnis nur zum Schutz der Anonymität natürlicher Personen erfolgen.

Anlässlich der Kontrolle einer Datei beim BfV hatte das BMI als zuständige Fachaufsichtsbehörde einer Kontrolle des Datenverarbeitungsprogramms durch eine Einsichtnahme in das Programm widersprochen, da eine derartige Kontrollmaßnahme des BfD generell unzulässig sei. Nach meinem Hinweis auf die mir auch insoweit vom Gesetzgeber verliehene Kontrollbefugnis nach § 24 Abs. 4 Satz 2 Nr. 1 BDSG hat das BMI seine Auffassung revidiert.

Auch hatte das BMI zunächst die Auffassung vertreten, dass Informationen beim BfV, die von dritter Seite, beispielsweise von Partnerdiensten, stammen, in Gänze dem Quellenschutz unterfielen und damit von meiner Kontrollkompetenz ausgenommen seien. Dies habe ich als eine unzulässige Beschränkung meiner Kontrollkompetenz erachtet und das BMI um die Änderung seiner Auffassung gebeten. Meinem Petitum ist das BMI insoweit nicht gefolgt, als es eine Offenlegung des jeweiligen Nachrichtengebers unter Hinweis auf den Quellenschutz weiterhin verwehrt. Nach Auffassung des BMI umfasst der Quellenschutz die Pflicht zur Wahrung der Anonymität aller Nachrichtengeber, d.h. sowohl von natürlichen als auch von juristischen Personen. Dieser Auffassung habe ich widersprochen und darauf hingewiesen, dass nur das Anonymitätsinteresse natürlicher Personen schutzwürdig ist und insoweit eine Einschränkung meiner Kontrollkompetenz rechtfertigen könnte; die zwischen dem BfV und mir getroffene Quellenschutzvereinbarung habe ich stets in diesem Sinne interpretiert (vgl. 17. TB Nr. 14.1, 18. TB Nr. 14.2). Die weite Interpretation durch das BMI und das BfV hätte zur Folge, dass ich im Falle der Speicherung eines Nachrichtengebers in einer Datei generell keine unmittelbare Einsicht in diese Datei nehmen könnte, auch wenn die Einsichtnahme zur Kontrolle des Datenverarbeitungsprogramms unerlässlich ist. Technisch ist es derzeit nicht möglich, den Hinweis auf den Nachrichtengeber auszublenden. Da viele Dateien des BfV Quelleninformationen von Organisationen wie etwa anderen Nachrichtendiensten enthalten, hätte die weite Auslegung zur Folge, dass ich meinen gesetzlichen Kontrollauftrag in Bezug auf die Kontrolle der Datenverarbeitung nach § 24 Abs. 4 Satz 2 Nr. 1 BDSG vielfach nicht oder nur sehr eingeschränkt erfüllen könnte. Daher habe ich das BMI und das BfV gebeten, ihre Auffassung zu ändern. Zudem steht es dem BfV frei, seine DV-Programme so zu modifizieren, dass geschützte Quellen bei Prüfungen nicht aufgedeckt werden. Die Gespräche zur Erarbeitung eines gemeinsamen Lösungskonzeptes waren bei Redaktionsschluss noch im Gange.

5.6 Militärischer Abschirmdienst

5.6.1 Änderung des Gesetzes über den MAD

Der mir zur Anhörung zugeleitete Entwurf einer Dienstvorschrift zum automatisierten Abruf aus dem Personalführungs- und Informationssystem der Bundeswehr durch den MAD wird den gesetzlichen Vorgaben nicht gerecht.

Nach langjährigen Erörterungen mit dem BMVg hat der Deutsche Bundestag am 8. März 2004 das Erste Gesetz zur Änderung des MADG verabschiedet. Damit ist er meiner Forderung nachgekommen, den Zugriff des MAD auf Daten aus dem Personalführungs- und Informationssystem der Bundeswehr (PERFIS) auf eine gesetzliche Grundlage zu stellen (vgl. 18. TB Nr. 15.1 und 19. TB Nr. 18.1.1). Nach dem ergänzten § 10 Abs. 2 MADG darf der MAD im Rahmen der Erfüllung seiner Aufgaben zur Feststellung, ob eine Person dem Geschäftsbereich des BMVg angehört oder in ihm tätig ist, den Familiennamen, den Vornamen, frühere Namen, das Geburtsdatum, den Dienstgrad, die Dienststellennummer und das Dienstzeitende des Betroffenen aus PERFIS abrufen. Nähere Einzelheiten zum Kreis der zum Abruf berechtigten Angehörigen des MAD und zum Verfahren sind in einer Dienstvorschrift zu regeln, vor deren Erlass ich angehört werde. Im Rahmen dieser Anhörung habe ich festgestellt, dass der MAD einen vom Gesetz vorgesehenen Abruf von Daten im automatisierten Verfahren nicht beabsichtigt und stattdessen an dem vor der Gesetzesänderung praktizierten Verfahren festhält. Dieses Verfahren sieht die Übermittlung der genannten Daten aller Angehörigen des Geschäftsbereichs des BMVg mittels eines Datenträgers an den MAD vor. Im MAD-Amt werden diese Daten gespeichert. Hierdurch entsteht eine MAD-eigene Datei, die für die Fachbereiche des MAD zur Nutzung bereit gehalten wird.

Bei diesem Verfahren, mit dem ich mich bereits vor Jahren nur vorübergehend und unter Vorbehalt einer gesetzlichen Änderung einverstanden erklärt hatte, handelt es sich um die Übermittlung von Daten im Sinne von § 3 Abs. 4 Nr. 3 Buchst. a) BDSG. Durch die Übermittlung und anschließende Speicherung des Gesamtbestandes aller Angehörigen des Geschäftsbereichs des BMVg aus PERFIS – wenn auch auf die nach § 10 Abs. 2 MADG zulässigen sieben Daten beschränkt – entsteht beim MAD-Amt ein Datenbestand, der überwiegend nicht zur Aufgabenerfüllung des MAD erforderlich und somit unzulässig ist.

Die Fortführung des bisher praktizierten Verfahrens trotz der Gesetzesänderung ist mit dem Wortlaut des Gesetzes und mit dem Willen des Gesetzgebers nicht vereinbar und daher unzulässig. Ich habe das BMVg gebeten, ein dem § 10 Abs. 2 MADG entsprechendes automatisiertes Abrufverfahren einzurichten. Eine Stellungnahme des BMVg lag mir bei Redaktionsschluss noch nicht vor.

5.6.2 Stellung des behördlichen Datenschutzbeauftragten beim MAD

Der MAD bedarf als Nachrichtendienst eines eigenen Beauftragten für den Datenschutz. Es genügt nicht, für den „Beauftragten für den Datenschutz in der Bundeswehr" beim MAD einen „Vertreter vor Ort" zu bestellen.

Nach § 4f Abs. 1 BDSG sind sowohl öffentliche wie auch nicht-öffentliche Stellen verpflichtet, einen Beauftragten für den Datenschutz zu bestellen. Der gesetzlichen Verpflichtung folgend, hat das BMVg mit Wirkung vom 1. Oktober 2003 einen „Beauftragten für den Datenschutz in der Bundeswehr“ (BfDBW) bestellt. Dessen Zuständigkeit erstreckt sich auf den gesamten Ressortbereich, d. h. auf die Bundeswehr insgesamt und damit auch auf den MAD als integraler Bestandteil der Bundeswehr. Zur Begründung verweist das BMVg auf die Regelung des § 4f Abs. 1 Satz 5 BDSG. Danach genügt die Bestellung eines Beauftragten für den Datenschutz für mehrere Bereiche, soweit dies aufgrund der Struktur der öffentlichen Stelle erforderlich ist. Beim MAD-Amt ist für den BfDBW ein ziviler Dienstposten eingerichtet worden.

Gegenüber dem BMVg vertrete ich die Auffassung, dass angesichts der besonderen Stellung und Funktion des MAD als Geheim- bzw. Nachrichtendienst die Bestellung eines rechtlich eigenständigen Beauftragten für den Datenschutz beim MAD-Amt erforderlich ist. Als Nachrichtendienst erhebt, verarbeitet und nutzt der MAD in erheblichem Umfang auch höchst sensible und damit äußerst schutzbedürftige personenbezogene Daten. Das MAD-Amt ist beispielsweise in seiner Funktion als „mitwirkende Behörde“ (vgl. § 3 Abs. 2 Sicherheitsüberprüfungsgesetz (SÜG)) jährlich an der Durchführung von ca. 42 000 Sicherheitsüberprüfungen beteiligt, d. h. an der Überprüfung von Personen, die mit einer sicherheitsempfindlichen Tätigkeit betraut werden sollen (vgl. § 1 Abs. 1 SÜG). Im Rahmen dieser Überprüfungen werden auch höchstpersönliche Daten (ggf. auch über Gesundheit, Sexualleben, politische Meinungen etc.) gemäß § 3 Abs. 9 BDSG der Betroffenen erhoben und verarbeitet. Ein ablehnendes Votum der „mitwirkenden Behörde“ kann den Ausschluss der betroffenen Person von der sicherheitsempfindlichen Tätigkeit und ggf. auch dienst- oder arbeitsrechtliche Konsequenzen bis hin zum Verlust des Arbeitsplatzes zur Folge haben. Zur Begründung meiner Forderung habe ich zudem auf eine mögliche Interessenkollision in Bezug auf die datenschutzrechtliche Bewertung eines Sachverhaltes aus ministerieller und spezifisch nachrichtendienstlicher Sicht des MAD-Amtes hingewiesen. Diese Gefahr ließe sich im Falle der Bestellung eines eigenständigen behördlichen Datenschutzbeauftragten des MAD-Amtes vermeiden.

Das BMVg hat meiner Forderung, an der ich nach wie vor festhalte, bislang nicht entsprochen.

5.6.3 EXA 21

Die mit der Einführung des „Elektronischen Büros“ beim MAD verbundenen Datenschutzprobleme konnten weitgehend gelöst werden.

Die Informationsverarbeitung im MAD-Amt soll durch die Einführung eines Dokumentenmanagement-, Archiv- und Workflowsystems (EXA 21) wesentlich verbessert und erweitert werden (vgl. 19. TB Nr. 18.2).

Folge der elektronischen Aktenführung ist, dass das komplette Schriftgut des MAD elektronisch erfasst und gespeichert wird und somit auch Daten von Personen erfasst werden, die der MAD nach geltendem Recht nicht speichern darf (vgl. § 6 Abs. 1 Satz 1 MADG i.V.m. § 10 Abs. 1 BVerfSchG). Insofern besteht ein vergleichbares Problem wie bei der Einführung der elektronischen Akte im Bundesamt für Verfassungsschutz (vgl. Nr. 5.5.2). Meine Forderung, dass nur gesetzlich zulässigerweise speicherbare Daten recherchiert werden dürfen, hat der MAD nicht nur durch eine entsprechende Dienstanweisung, sondern auch systemtechnisch umgesetzt. Recherchierbar sind nur diejenigen gespeicherten Daten, die von den zuständigen Bearbeitern elektronisch markiert worden sind.

In Bezug auf den aktuellen technischen Systementwurf von EXA 21 hat der MAD zugesagt, meine weiteren datenschutzrechtlichen Forderungen weitestgehend umzusetzen. So wird beispielsweise eine Löschroutine eingeführt, wodurch bestimmte Dokumente nach einem festgelegten Zeitablauf automatisiert gelöscht werden. Zugesagt wurde auch die von mir geforderte technische Umsetzung einer physischen Löschung der auf den Datenträgern (WORM-Platten) gespeicherten Daten sowie die Beschränkung der Höchstspeicherfrist für diese Daten.

Hinsichtlich der Verwendung von Protokolldaten habe ich den MAD aufgefordert, die gesetzliche Zweckbeschränkung für diese Daten zu beachten. Danach dürfen Protokolldaten ausschließlich zum Zweck der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs der Datenverarbeitungsanlage verwendet werden (vgl. § 7 Abs. 1 MADG i.V.m. § 12 Abs. 4 BVerfSchG). Eine Verwendung zu sonstigen, beispielsweise spezifisch nachrichtendienstlichen Zwecken, ist demnach ausgeschlossen. Ob der MAD insoweit meinem Petitum folgt, stand zum Zeitpunkt des Redaktionsschlusses noch nicht fest.

5.7 Bundesnachrichtendienst

5.7.1 Artikel 10-Gesetz (G 10)

Auch nach der Novellierung des G 10 im Jahre 2001 sieht die Bundesregierung gesetzgeberischen Handlungsbedarf.

Bei der Beschlussfassung über die Novellierung des G 10 (vgl. 19. TB Nr. 19.2) im Mai 2001 hat der Gesetzgeber die Bundesregierung aufgefordert, ihn nach Ablauf von zwei Jahren über die mit der Novellierung gemachten Erfahrungen, insbesondere unter dem Gesichtspunkt des Datenschutzes, zu unterrichten. Dieser Unterrichtung habe ich mit großem Interesse entgegen gesehen, weil mit dem Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl I. S. 361) erstmals eine gesetzliche Verpflichtung zur Evaluierung statuiert wurde. Die Bundesregierung ist dem Petitum des Parlaments mit einem Bericht über die Erfahrungen mit dem G 10 im November 2003 nachgekommen (vgl. Bundestagsdrucksache 15/2042).

Bei den Vorarbeiten zu dem Bericht hatte ich darauf hingewiesen, dass der Bundestag zwar keine Evaluierung der Befugnisse aber die Darlegung von Erfahrungen mit den

neuen Befugnissen aus dem neu gefassten G 10 verlangt hatte. Im Verlauf der Beratungen wurde der Bericht erheblich umgestaltet. Die nunmehr ausgewogen erscheinende Endfassung verschafft dem Parlament die Möglichkeit zu prüfen, inwieweit bei den neuen Befugnissen auch die Belange des Datenschutzes gewahrt sind. Dabei ist zu berücksichtigen, dass nach Ablauf von zwei Jahren seit Inkrafttreten der Novelle zu einigen Neuregelungen noch keine oder nicht genügend aussagekräftige Erfahrungen vorlagen. Jedoch enthält der Bericht neben den Erfahrungen bei der Anwendung des G 10 weiterhin ein Kapitel über den aktuellen und mittelfristigen Prüfbedarf zur Änderung des Gesetzes. Dieser führte im Jahre 2004 zu einem Rohentwurf zur Änderung des G 10. Der formelle Abstimmungsprozess über diesen Entwurf innerhalb der Bundesregierung hat jedoch bei Redaktionsschluss noch nicht begonnen. Offen blieb bei den Beratungen bisher die Frage, inwieweit die beiden Entscheidungen des Bundesverfassungsgerichts vom 3. März 2004 zur akustischen Wohnraumüberwachung (vgl. Nr. 7.1.1) und zur präventiven Telekommunikations- und Postüberwachung nach §§ 39 ff. Außenwirtschaftsgesetz (vgl. Nr. 5.4.3) im Rahmen des G 10 zu berücksichtigen sind.

5.7.2 Zugriff externer Stellen im automatisierten Verfahren auf Dateien beim BND

Ein Zugriff externer Stellen im automatisierten Verfahren auf Dateien des BND ist rechtlich unzulässig.

Wie bereits berichtet (19. TB Nr. 19.4), hatte der BND beabsichtigt, zugunsten einer Behörde außerhalb des BND eine Online-Verbindung einzurichten, um dieser Behörde den Abruf personenbezogener Daten des BND im automatisierten Verfahren (vgl. § 10 BDSG) zu ermöglichen. Inzwischen hat der BND beim Bundeskanzleramt den Antrag einer Genehmigung der Dateianordnung, die diesen Online-Zugriff vorsah, zurückgezogen.

Die Einrichtung eines Online-Zugriffs zugunsten von Drittstellen auf personenbezogene Daten des BND erachte ich weiterhin für unzulässig. Das BNDG enthält hierfür keine Rechtsgrundlage. Die Regelung des § 10 BDSG, die einen Abruf personenbezogener Daten im automatisierten Verfahren gestattet, gilt nicht für den BND, da § 11 BNDG die Anwendbarkeit dieser Norm explizit ausschließt.

Zu meiner Stellungnahme hat mir der BND mitgeteilt, dass er im o. a. Fall auf die Einrichtung eines Zugriffs im automatisierten Verfahren verzichtet, jedoch die grundsätzliche Frage der Zulässigkeit von Online-Zugriffen in einer gemeinsamen Diskussionsrunde unter Beteiligung des Bundeskanzleramtes erörtern will.

5.7.3 Kontrolle beim BND

Infolge einer Kontrolle konnten wesentliche datenschutzrechtliche Verbesserungen, insbesondere in Bezug auf die Bereinigung der sog. Altdatenbestände, erzielt werden.

Anlässlich einer Kontrolle habe ich die Verarbeitung personenbezogener Daten in mehreren Fachdateien des BND kontrolliert. Die Auswahl der kontrollierten Daten erfolgte nach dem Zufallsprinzip. Dabei wurde insbesondere folgendes festgestellt:

– Der BND speichert Daten, die nach den gesetzlichen Vorgaben hätten überprüft werden müssen. Der BND räumte ein, seine mir gegebene Zusage zur Bereinigung der Altdatenbestände bis spätestens 2004 (19. TB Nr. 19.4) nicht erfüllen zu können. Der Abschluss der Arbeiten werde sich aufgrund der begrenzten personellen Ressourcen voraussichtlich weiter verzögern. Unter Hinweis darauf, dass eine Überschreitung der gesetzten Frist einen schwerwiegenden Verstoß gegen die dem BND obliegende Datenbereinigungspflicht (vgl. § 5 BNDG i.V.m. §12 Abs. 3 BVerfSchG) darstellen und von mir beanstandet werden würde, habe ich den BND zur Vorlage eines tragfähigen Konzeptes zur Bereinigung der Altdatenbestände aufgefordert. Dieser Aufforderung ist der BND nachgekommen. Inzwischen sind die Altdatenbestände in Teilbereichen durch intensiven Personaleinsatz vollständig abgebaut worden. Ich habe den BND aufgefordert sicherzustellen, dass die Bereinigung der Datenbestände nunmehr fristgerecht erfolgt.

– In einer im Zusammenhang mit Petenteneingaben stehenden Datei sind in Einzelfällen Rechtsverstöße (Eingabe falscher Daten, verspätete Dateneingaben) festgestellt worden, die auf menschlichem Fehlverhalten beruhen. Der BND hat diese Mängel unverzüglich beseitigt.

– An den BND hatten sich Petenten mit der Bitte um Auskunft gewandt, die befürchteten, abgehört worden zu sein. Der BND verwies diese Petenten an das BMI. Ich habe den BND aufgefordert, die Betroffenen entsprechend dem geltenden Recht unmittelbar an die nach § 15 Abs. 5 und 6 des G 10 zuständige G 10-Kommission des Deutschen Bundestages zu verweisen. Der BND hat dies zugesagt.

– Der behördliche Datenschutzbeauftragte (bDSB) des BND wirkt nach § 4g Abs. 1 BDSG auf die Einhaltung der datenschutzrechtlichen Bestimmungen beim BND hin und ist als behördeninternes Kontrollorgan dem Präsidenten des BND unmittelbar unterstellt, wobei er in Ausübung seiner Fachkunde auf dem Gebiet des Datenschutzes weisungsfrei ist. Gemäß § 4f BDSG ist er Ansprechpartner für die Mitarbeiterinnen und Mitarbeiter des BND und zur Verschwiegenheit über die Identität eines Betroffenen, auch gegenüber dem Präsidenten des BND, verpflichtet. Angesichts dieser besonderen Stellung des bDSB habe ich den BND aufgefordert, ihn und seine Stellvertreterin förmlich zu bestellen und dienstweit bekannt zu machen. Dies ist inzwischen geschehen.

– Die Mitwirkung des BND im Rahmen des Konsultationsverfahrens nach Artikel 17 Abs. 2 Schengener Durchführungsübereinkommen (vgl. Nr. 5.2.6) ist in den vergangenen Jahren erheblich angewachsen. Der

BND hat jedoch nur in vergleichsweise wenigen Fällen Bedenken gegen die Erteilung eines Visums erhoben. Eine detaillierte Kontrolle des Konsultationsverfahrens im BND habe ich mir vorbehalten.

– Eine beim Bundesverwaltungsamt durchgeführte Kontrolle gab Veranlassung, ein mit dieser Behörde praktiziertes Verfahren zum Austausch von Dokumenten beim BND zu überprüfen. Aufgrund dieser Kontrolle wurde das Verfahren geändert und datenschutzkonform ausgestaltet (vgl. Nr. 6.1.3).

– Ebenso wie im BfV (vgl. Nr. 5.5.2) und beim MAD (vgl. Nr. 5.6.3) erfolgt auch im BND eine weitreichende Umgestaltung bzw. Neustrukturierung der IT-gestützten Datenverarbeitung. Dies hat nicht nur Auswirkungen auf die innerstaatliche Datenverarbeitung, sondern auch auf die internationale Kooperation mit anderen Diensten. Aus Geheimschutzgründen ist mir eine detailliertere Darstellung nicht möglich. Der BND hat zugesagt, mich auch in die Entwicklung dieser (Groß-)Projekte frühzeitig beratend einzubeziehen. Erste Sondierungsgespräche sind bereits geführt worden.

5.8 Sicherheitsüberprüfung

5.8.1 Luftsicherheitsgesetz

Neue Bestimmungen im Luftsicherheitsgesetz über Zuverlässigkeitsüberprüfungen auf dem Gebiet des Luftverkehrs enthalten datenschutzrechtlich problematische Regelungen.

Im Sommer 2004 hat der Bundestag das Gesetz zur Neuregelung von Luftsicherheitsaufgaben (Luftsicherheitsgesetz-LuftSiG) verabschiedet. Aus datenschutzrechtlicher Sicht bedeutsam ist, dass mit diesem Gesetz die Regelungen über die Zuverlässigkeitsüberprüfungen auf dem Gebiet des Luftverkehrs, die bisher im Luftverkehrsgesetz niedergelegt waren, auf eine neue gesetzliche Grundlage gestellt wurden. Die Zielsetzung des Gesetzes ist vergleichbar mit dem im Jahre 2002 durch das Terrorismusbekämpfungsgesetz in § 1 Abs. 4 Sicherheitsüberprüfungsgesetz (SÜG) normierten vorbeugenden personellen Sabotageschutz (vpS). Die Voraussetzungen und das Verfahren für die Zuverlässigkeitsüberprüfung sind nunmehr in § 7 LuftSiG geregelt, der an die Stelle des mit diesem Gesetz aufgehobenen § 29d Luftverkehrsgesetz tritt. Bereits in meinen ersten Stellungnahmen zu den Arbeitsentwürfen des BMI hatte ich einige Regelungen kritisiert. Erfreulicherweise wurden im Gesetzgebungsverfahren einige problematische Gesetzesvorschläge entschärft. Jedoch enthält das Gesetz weiterhin datenschutzrechtlich unbefriedigende Regelungen insbesondere zur Zuverlässigkeitsüberprüfung, die in vielen Punkten von den Regelungen zum vpS stark abweichen und eine erheblich höhere Eingriffsintensität aufweisen.

Meine Kritikpunkte sind im Wesentlichen:

– Nach § 7 Abs. 2 Satz 4 Nr. 2 entfällt eine Zuverlässigkeitsüberprüfung, wenn der Betroffene der erweiterten Sicherheitsüberprüfung nach § 9 SÜG oder der erweiterten Sicherheitsüberprüfung mit Sicherheitsermittlungen nach § 10 SÜG unterliegt. Folglich entbindet eine einfache Sicherheitsüberprüfung nach § 8 SÜG, die für den vpS ausreichend ist, nicht von einer Zuverlässigkeitsüberprüfung nach dem LuftSiG.

– Die Anfrage bei dem gegenwärtigen Arbeitgeber des Betroffenen nach § 7 Abs. 3 Satz 1 Nr. 5 und insbesondere die Unterrichtung des gegenwärtigen Arbeitgebers über das Ergebnis der Zuverlässigkeitsprüfung nach § 7 Abs. 7 Satz 2 halte ich angesichts der besonderen Sensibilität der Daten für äußerst bedenklich. Sie findet keine Entsprechung im SÜG. Besonders bedenklich sind diejenigen Fälle, in denen eine Zuverlässigkeitsüberprüfung auf Grund einer Bewerbung des Betroffenen bei einem neuen Arbeitgeber erfolgt, da der gegenwärtige Arbeitgeber auf diese Weise zwangsläufig Kenntnis von einer Bewerbung erlangt – mit möglicherweise weitreichenden Folgen für den Betroffenen.

– Auch die Befugnis der Luftsicherheitsbehörden zur Unterrichtung der in § 7 Abs. 7 genannten übrigen Stellen und die Nachberichtspflicht der beteiligten Stellen nach § 7 Abs. 9 ist datenschutzrechtlich fragwürdig. Die vergleichbaren Regelungen im SÜG sehen derart weitreichende Übermittlungsbefugnisse zu Lasten des Betroffenen nicht vor.

– Nach § 17 Abs. 1 wird das BMI ermächtigt, die Einzelheiten der Zuverlässigkeitsüberprüfung, insbesondere die Frist für eine Wiederholung der Überprüfung sowie Einzelheiten der Erhebung und Verwendung personenbezogener Daten durch Rechtsverordnung, die der Zustimmung des Bundesrates bedarf, zu regeln. Solange diese Verordnung noch nicht erlassen ist, gelten nach der Gesetzesbegründung die Vorschriften der Luftverkehr-Zuverlässigkeitsüberprüfungsverordnung (vgl. 19. TB Nr. 20.2) weiter, soweit § 7 nicht ausdrücklich anderslautende gesetzliche Regelungen trifft. Diese Verordnungsermächtigung steht im Widerspruch zur Wesentlichkeitstheorie des Bundesverfassungsgerichts, die es dem Gesetzgeber auferlegt, im Hinblick auf die Verarbeitung personenbezogener Daten unter anderem verfahrensrechtliche Vorkehrungen zu treffen, die der Gefahr einer Verletzung des Persönlichkeitsrechts entgegen wirken (vgl. BVerfGE 65, 1(44)). Zwar hat der Gesetzgeber in § 7 Regelungen zur Speicherung, Löschung und Übermittlung personenbezogener Daten selbst getroffen. Jedoch sind weitere wesentliche Regelungen zur Erhebung, Verarbeitung und Nutzung personenbezogener Daten im Gesetz nicht festgelegt worden.

5.8.2 Sicherheitsüberprüfung bei nicht-öffentlichen Stellen

5.8.2.1 Initiative des BMWA zur Online-Bearbeitung von Sicherheitserklärungen

Das Vorhaben des BMWA, Sicherheitserklärungen bei Wirtschaftsunternehmen künftig nur noch in elektronischer Form zu erstellen und zu übermitteln, setzt eine vorherige Änderung des SÜG voraus.

Im Zuge eines eGovernment-Projekts hat das BMWA das Projekt „Sicherheitserklärung Online“ entwickelt, das einer Forderung der Wirtschaft entspricht. Daneben sollen auch das überarbeitete Geheimschutzhandbuch mit der Verschlankung zahlreicher Verwaltungsprozeduren und der Internetauftritt des Geheimschutzes im nicht-öffentlichen Bereich (www.bmwa-sicherheitsforum.de) zu einer Entbürokratisierung beitragen.

Nach den Plänen sollen in einem ersten Schritt die nach § 13 SÜG abzugebenden Sicherheitserklärungen von Betroffenen bei Wirtschaftunternehmen künftig nur noch in elektronischer Form erstellt und den beteiligten Behörden (BMWA und Bundesamt für Verfassungsschutz – BfV) im Online-Verfahren übermittelt werden. Als zweiter Schritt ist beabsichtigt, die bislang in Papierform vorhandenen Akten generell durch sog. „elektronische Akten“ zu ersetzen.

Ich habe das BMWA bei der Vorstellung des Projekts darauf hingewiesen, dass die Speicherung von personenbezogenen Daten der Sicherheitserklärung durch § 20 SÜG auf die in § 13 Abs. 1 Nr. 1 bis 6 SÜG genannten Grunddaten begrenzt wird. Bei einer elektronischen Bearbeitung der Sicherheitserklärung sollen jedoch darüber hinaus weitere, zum Teil sehr sensible Daten elektronisch erfasst werden. Gleiches gilt auch für die zu einem späteren Zeitpunkt vorgesehene Ersetzung der vorhandenen Papierakten durch sog. „elektronische Akten“. Meine Einschätzung wird auch von dem für das SÜG federführenden BMI geteilt, das ebenso wie ich für eine Umsetzung des Vorhabens eine vorherige Änderung des Gesetzes für erforderlich hält. Ein entsprechender Änderungsvorschlag für die §§ 11, 18, 20, 22 und 31 SÜG ist nach Auskunft des BMI in Vorbereitung.

Die Speicherung personenbezogener Daten in Dateien hat der Gesetzgeber in § 20 SÜG bewusst restriktiv geregelt. Bei einer Änderung des SÜG, der ich mich mit Blick auf die fortschreitende Automatisierung von Verwaltungsabläufen nicht verschließe, müssen daher bei der Datenübertragung besondere Vorkehrungen mittels einer Verschlüsselung getroffen werden. Ferner ist ein hinreichender Schutz vor einem unberechtigten Zugriff auf die gespeicherten Daten sicherzustellen. Dies könnte – so auch die Auffassung des BMI und des Bundesamtes für Sicherheit in der Informationstechnik – eine Höherstufung des Geheimhaltungsgrades erforderlich machen; nach gegenwärtigem Stand sind Sicherheitserklärungen mit dem VS-Grad NfD eingestuft.

Bis Redaktionsschluss lag noch kein Gesetzentwurf zur Änderung des SÜG vor.

5.8.2.2 Datenschutzrechtliche Kontrollen der Sicherheitsüberprüfungen in der Privatwirtschaft

Eine Kontrolle des Verfahrens der Sicherheitsüberprüfungen in der Privatwirtschaft zeigt die Notwendigkeit für einige grundlegende Verbesserungen.

Im Berichtszeitraum habe ich ein größeres privates Unternehmen kontrolliert, das eine relativ große Zahl von sicherheitsüberprüften Mitarbeitern beschäftigt. Die Mehrzahl der Mitarbeiter war sicherheitsüberprüft. Hinzu kamen viele Mitarbeiter, die unter den durch das Terrorismusbekämpfungsgesetz neu eingeführten vorbeugenden personellen Sabotageschutz fallen. Bei der Kontrolle einzelner Sicherheitsakten in dem Unternehmen habe ich keine gravierenden Mängel festgestellt. Allerdings haben sich im organisatorischen Bereich und bei der dateimäßigen Bearbeitung personenbezogener Daten Mängel gezeigt, die teilweise von erheblicher und grundsätzlicher Bedeutung sind. Ferner haben sich bei den Gesprächen mit dem Sicherheitsbevollmächtigten (Sibe) Probleme und Fragen ergeben, die noch einer Klärung bedürfen:

Die Sicherheitsakten bei dem Unternehmen wurden in demselben Raum aufbewahrt und bearbeitet, in dem auch die Berechtigungsausweise für den Zutritt zum Unternehmensgelände ausgestellt werden. Aufgrund des häufig herrschenden regen Publikumsverkehrs sind die dort tätigen Mitarbeiter mit der Bearbeitung von Zutrittsausweisen und der gleichzeitigen Verhinderung einer unbefugten Einsichtnahme in Unterlagen mit personenbezogenen Daten überfordert. Ich habe daher eine räumliche Trennung der beiden Aufgabenbereiche – Besuchskontrollverfahren und personeller Geheimschutz – angeregt.

Die elektronische Bearbeitung der Sicherheitsakten erfolgte mittels eines Datenbanksystems, auf das sowohl die Mitarbeiter des personellen Geheimschutzes als auch die Mitarbeiter des vpS Zugriff haben. Aufgrund meiner Kritik an diesem wechselseitigen Zugriff wurde eine technische Systemmodifikation (Einrichtung sog. „Benutzerrollen“ zur Vergabe differenzierter Zugriffsberechtigungen) veranlasst. In dem System steht für die Mitarbeiter des Sibe eine logische Verzeichnisstruktur (Abteilungsordner) zur Verfügung. Der Sibe hat auf meine Anregung hin eine Prüfung zugesagt, die Verzeichnisstruktur noch stärker nach Aufgabengebieten zu segmentieren. Außerdem sollte mittelfristig geprüft werden, die Arbeitsabläufe dieser Stabsabteilung insgesamt in ein besonders gesichertes Netz zu verlagern, bei dem die Daten verschlüsselt und gespeichert werden.

Weder das SÜG noch die Allgemeine Verwaltungsvorschrift (AVV) des BMWA zu §§ 24 bis 31 SÜG enthalten Regelungen über die Funktion und Aufgaben eines Sibe bei nicht-öffentlichen Stellen. Lediglich das „Handbuch für den Geheimschutz in der Wirtschaft (Geheimschutzhandbuch-GHB)“ enthält entsprechende Hinweise. Die Kontrolle gab Veranlassung zu der Frage, inwieweit der Sibe Aufgaben wahrnehmen darf, die nach dem SÜG der zuständigen Stelle oder der mitwirkenden Behörde zustehen.

Ein Beispiel verdeutlicht die Problematik: Der Sibe hat einen sicherheitsüberprüften Mitarbeiter nach einem Verstoß gegen Geheimhaltungsvorschriften schriftlich abgemahnt und den zuständigen Vorgesetzten hierüber unterrichtet. Von einer Mitteilung an das BMWA hat er jedoch abgesehen, obwohl in solchen Fällen Kontakt mit dem BMWA aufzunehmen gewesen wäre. Ich halte diese Unterrichtung des Vorgesetzten im Hinblick auf die restriktiv gefassten Übermittlungsregelungen des § 21 SÜG datenschutzrechtlich für unangemessen. Geringfügige

Verstöße gegen Geheimschutzvorschriften sollten im Regelfall lediglich in anonymisierter Form den jeweiligen Fachbereichen bekannt gegeben werden.

Hierzu habe ich das BMWA um Stellungnahme gebeten, insbesondere zu der Frage, inwieweit die Aufgaben des BMWA als zuständiger Stelle nach dem SÜG auf den Sibe delegiert werden können.

Des weiteren habe ich festgestellt, dass Vermerke und sonstige schriftliche Unterlagen zu Anhörungen, Feststellungen und Abmahnungen vom Sibe gesondert in einem Aktenordner aufbewahrt werden. Nach § 18 SÜG sind jedoch sämtliche die Sicherheitsüberprüfung betreffenden Unterlagen in der Sicherheitsakte zu der betroffenen Person aufzunehmen.

Die Aufgaben der nicht-öffentlichen Stelle sind nach § 25 Abs. 3 SÜG grundsätzlich von einer von der Personalverwaltung getrennten Organisationseinheit wahrzunehmen. Damit ist grundsätzlich auch die Mitgliedschaft des Sibe und seiner Mitarbeiter in Personalvertretungen unvereinbar. Eine im Aufgabenbereich des vpS tätige Mitarbeiterin war zum Zeitpunkt des Kontrollbesuchs Mitglied des Betriebsrats.

Eine Stellungnahme des BMWA zu meinem Kontrollbericht lag mir bei Redaktionsschluss noch nicht vor.

5.8.3 Kontrolle des Verfahrens der Sicherheitsüberprüfung beim MAD

Bei einer Kontrolle der Sicherheitsüberprüfungen durch den MAD habe ich schwerwiegende Verstöße gegen das SÜG festgestellt.

Der MAD ist nach § 3 Abs. 2 SÜG mitwirkende Behörde für die Sicherheitsüberprüfungen der Bediensteten des Geschäftsbereichs des BMVg. Bei Bewerbern und Mitarbeitern des eigenen Dienstes führt er nach § 3 Abs. 3 SÜG die Sicherheitsüberprüfung allein durch. Der MAD ist somit bezüglich seiner eigenen Mitarbeiter und für seine Bewerber gleichzeitig zuständige Stelle und mitwirkende Behörde.

Bei einer Kontrolle der Sicherheitsüberprüfungen des MAD habe ich schwerwiegende Verstöße festgestellt, die ich in zwei Fällen förmlich beanstandet habe. Zu den Feststellungen im Einzelnen:

– Nach § 12 Abs. 1 Nr. 1 SÜG darf der MAD zum Zweck der Bewertung der Angaben in der Sicherheitserklärung Erkenntnisse der Verfassungsschutzbehörden zum Betroffenen selbst, zu seinem Ehegatten oder Lebenspartner sowie zu den übrigen in der Sicherheitserklärung angegebenen Personen beiziehen. Eine Anfrage an den BND ist nach § 12 Abs. 1 Nr. 3 SÜG nur zulässig in Bezug auf die betroffene und auf die einzubeziehende Person. In zahlreichen Fällen hat der MAD jedoch auch Anfragen an den BND zu anderen in der Sicherheitserklärung genannten Personen (z. B. Verwandte des Betroffenen oder der einzubeziehenden Person) gerichtet. Die generelle Einbeziehung von Erkenntnissen des BND zur Bewertung der in der Sicherheitserklärung gemachten Angaben stellen schwerwiegende Verstöße gegen die Restriktionen des § 12 Abs. 1 Nr. 1 SÜG dar, weswegen ich diese Praxis nach § 25 Abs. 1 BDSG beanstandet habe. Das BMVg hat diesen Verstoß eingeräumt und zugesagt, die kontrollierten Akten zu bereinigen. Darüber hinaus habe ich das BMVg gebeten, die rechtswidrige Praxis des MAD künftig einzustellen.

– Vor der Einstellung eines Bewerbers führt der MAD mit den Bewerbern sog. „Informationsgespräche". Hierbei wurden von den Bewerbern auch personenbezogene Daten abgefragt, die zum Teil über die nach § 13 Abs. 1 Satz 1 Nr. 1 bis 20 SÜG zulässigen Daten hinausgingen, obgleich zu diesem Zeitpunkt noch keine für die Einleitung einer Sicherheitsüberprüfung notwendige Zustimmung des Bewerbers, aufgrund derer personenbezogene Daten hätten erhoben werden können, vorlag. In einigen der kontrollierten Akten habe ich festgestellt, dass solche unzulässig erhobenen Daten in die zu einem späteren Zeitpunkt durchgeführte Sicherheitsüberprüfung einbezogen wurden. Das BMVg hat bestätigt, dass Informationen aus den Personalauswahl- und Personalgewinnungsverfahren nicht im Rahmen der Sicherheitsüberprüfung verwendet werden dürfen und dass diese Praxis, die ich als Verstoß gegen § 11 Abs. 1 SÜG förmlich beanstandet habe, eingestellt wird. Die in den Akten enthaltenen unzulässigen Inhalte wurden nach Angaben des BMVg vernichtet.

– In einigen Fällen wurde die Befragung von Referenz- oder Auskunftspersonen in Anwesenheit dritter Personen durchgeführt. Ich halte dies für datenschutzrechtlich bedenklich, da bei den Befragungen persönliche Verhältnisse der betroffenen Person dargelegt werden, die oft sehr sensibel sind. Ich habe daher das BMVg gebeten sicherzustellen, dass bei der Befragung zukünftig keine Dritten anwesend sind. Ergibt sich aus einer Befragung die Notwendigkeit zur Befragung weiterer Personen, so können diese nach § 12 Abs. 3 SÜG gesondert befragt werden.

  Das BMVg, das meine Auffassung grundsätzlich teilt, hält jedoch die Anwesenheit Dritter bei Befragungen ausnahmsweise für erforderlich, wenn

  – die zu befragende Person darum bittet, weil die dritte Person zu dem Gegenstand der Befragung genauere Kenntnisse hat oder

  – die zu befragende Person von sich aus die Teilnahme an der Befragung aus anderen Gründen wünscht.

  Ich habe das BMVg gebeten, seine Auffassung zu revidieren.

– Bei einer überprüften Person hat der MAD sicherheitserhebliche Erkenntnisse wegen finanzieller Probleme festgestellt und abweichend von § 17 Abs. 2 SÜG bereits nach drei Jahren eine vollständige Wiederholungsüberprüfung durchgeführt. Ich sehe hier keine Notwendigkeit für eine komplette Wiederholungsüberprüfung, da die gezielte Überwachung einer erteilten Auflage nach meiner Auffassung eine geeignete und auch ausreichende Maßnahme darstellt. Das

BMVg hält jedoch eine Auflagenüberwachung allein nicht für ausreichend. Die Objektivierung der sicherheitserheblichen Erkenntnisse sei nur durch eine Wiederholungsüberprüfung möglich. Ich halte demgegenüber eine Wiederholungsüberprüfung nur in den Fällen für hinnehmbar, in denen mehrere Erkenntnisse zusammentreffen, die verschiedenen Sicherheitsrisiken zuzuordnen sind. In der Regel sind bei Vorliegen einer einzelnen sicherheitserheblichen Erkenntnis jedoch Einzelmaßnahmen ausreichend, z. B. Befragung geeigneter Auskunftspersonen oder Stellen in Bezug auf die vorliegende sicherheitserhebliche Erkenntnis.

– Der MAD richtet nach § 12 Abs. 1 Nr. 1 SÜG zum Zweck der sicherheitsmäßigen Bewertung der Angaben in der Sicherheitserklärung Anfragen an das BfV und an die Landesämter für Verfassungsschutz (LfV). Ich halte die unmittelbare Anfrage an die LfV für unzulässig und habe daher das BMVg gebeten, diese Praxis einzustellen. Zulässig ist nach meiner Auffassung zunächst lediglich eine Anfrage an das BfV zur Abfrage im Nachrichtendienstlichen Informationssystem (NADIS). Erst wenn durch die Antwort des BfV Hinweise auf Erkenntnisse von LfV sichtbar werden, halte ich weitere gezielte Anfragen an die jeweils betroffenen LfV für zulässig. Ich habe das BMVg zudem darauf hingewiesen, dass auch die Allgemeine Verwaltungsvorschrift des BMI zu § 12 Abs. 1 Nr. 1 SÜG zum Zwecke der Bewertung der Angaben in der Sicherheitserklärung von einer NADIS-Anfrage ausgeht. Das BMVg ist meiner Auffassung bislang nicht gefolgt.

– Die Sicherheitsüberprüfungsakten enthalten vielfach umfangreiche Personalaktenauszüge u. a. mit Hinweisen zur bisherigen Verwendung der betroffenen Person, absolvierte Laufbahnlehrgänge mit Abschlussnoten, Beförderungen, Beurteilungsnoten, letzte Beurteilungen und teilweise auch Personaldaten naher Angehöriger. Die Aufnahme solcher Auszüge in Sicherheitsüberprüfungsakten stellt eine Umgehung der gesetzlichen Beschränkung des Rechts auf Einsichtnahme in die Personalakte nach § 13 Abs. 6 Satz 3 und 5 SÜG dar und verstößt damit gegen die vom Gesetzgeber mit dieser Beschränkung intendierte Schutzfunktion. Das BMVg hat inzwischen mitgeteilt, dass Personalaktenauszüge in den Sicherheitsüberprüfungsakten, die über den Rahmen der nach der einschlägigen Dienstvorschrift aufzunehmenden Personalaktenauszüge hinausgehen, künftig nicht mehr in die Akten aufgenommen werden und dass die betreffenden Akten entsprechend bereinigt wurden.

5.8.4 Sicherheitsüberprüfung durch US-amerikanische und britische Streitkräfte in der Bundesrepublik Deutschland

Die US-amerikanischen und die britischen Streitkräfte wollen Sicherheitsüberprüfungen entsprechend den Regelungen des SÜG durchführen. Nach mir vorliegenden Hinweisen ist dies in der Praxis noch nicht umgesetzt.

Im Berichtszeitraum wandten sich Petenten an mich, die als Mitarbeiter deutscher Firmen für den Zugang zu US-amerikanischen und britischen Streitkräften in Deutschland einen Zugangsausweis benötigen und sich zu diesem Zweck einer Sicherheitsüberprüfung zu unterziehen haben. Davon betroffen sind auch Zivilangestellte der Streitkräfte sowie Mitarbeiter von Behörden, die die Liegenschaften aus dienstlichen Gründen betreten müssen. Die Beschwerden richteten sich vor allem gegen den Umfang und die Art der abgefragten Daten, die Weiterleitung der Daten an US-amerikanische bzw. britische Regierungsstellen außerhalb Deutschlands, die Aufnahme biometrischer Daten in die Zugangsausweise, die zu unterzeichnende Einwilligungserklärung zur Durchführung einer Sicherheitsüberprüfung sowie die Verweigerung von Auskünften. Den Eingaben war zu entnehmen, dass vor allem die US-amerikanischen Stellen nach den Anschlägen vom 11. September 2001 die Regelungen zur Zugangskontrolle und zur Sicherheitsüberprüfung offensichtlich verschärft haben.

Wesentliche Rechtsgrundlagen für die Überprüfung deutscher und ausländischer Staatsangehöriger durch ausländische Streitkräfte bilden das NATO-Truppenstatut (NTS), das Zusatzabkommen zum NTS (ZA-NTS) und § 33 SÜG. Nach Artikel II NTS haben eine Truppe und ihr ziviles Gefolge sowie deren Angehörige die Pflicht, das Recht des Aufnahmestaates zu achten. Demnach sind die NATO-Truppen auch bei der Durchführung von Sicherheitsüberprüfungen an deutsches Recht gebunden. Da das BDSG auf ausländische öffentliche Stellen jedoch keine Anwendung findet, habe ich gegenüber den US-amerikanischen und britischen Streitkräften keine Kontrollbefugnis. Ich habe daher die Problematik an die Bundesregierung herangetragen. Im Zuge der Erörterungen mit dem AA, dem BMI und dem BfV wurde einvernehmlich festgestellt, dass die Mitwirkung des BfV nach § 33 SÜG bei den von US-amerikanischen und britischen Stellen veranlassten Sicherheitsüberprüfungen nicht den Vorschriften des SÜG und des BDSG entsprach. Das BMI habe ich deshalb gebeten, die vom BfV unzulässig erhobenen und übermittelten Daten zu löschen.

In einer Verbalnote des AA vom 4. Dezember 2003 wurde der Botschaft der USA mitgeteilt, dass die von den Betroffenen zu unterzeichnende Zustimmungserklärung zur Durchführung einer Sicherheitsüberprüfung schon aufgrund ihrer Unbestimmtheit unwirksam ist und dass deutsche Behörden nach Artikel 3 Abs. 3 Buchst. b) des ZA-NTS bei der Zusammenarbeit mit den Truppenbehörden in Bezug auf die Übermittlung von personenbezogenen Daten im Übrigen nicht zur Durchführung von Maßnahmen verpflichtet seien, die gegen deutsche Gesetze verstoßen würden. Daraufhin haben auf meine Initiative hin Verhandlungen zwischen dem BMI und den US-amerikanischen und britischen Streitkräften – teilweise unter meiner Beteiligung – mit dem Ziel stattgefunden, die durch sie durchzuführenden Sicherheitsüberprüfungen dem deutschen Recht entsprechend zu regeln und einen angemessenen datenschutzrechtlichen Zustand herbeizuführen.

Ein am 22. Juli 2004 im BMI geführtes Gespräch mit den US-amerikanischen und britischen Streitkräften, an dem ich beteiligt war, hat dabei im Wesentlichen zu folgenden erfreulichen Ergebnissen geführt:

- Sicherheitsüberprüfungen entsprechend § 8 SÜG – einfache Sicherheitsüberprüfung (Ü 1) – nur für zivile Bedienstete und Personen, die die Liegenschaften täglich oder häufig betreten müssen (keine Besucher);
- Keine Einbeziehung von Ehegatten oder Lebenspartnern, lediglich Erfassung ihrer persönlichen Daten nach deren Zustimmung;
- Keine Sicherheitsüberprüfung von Personen mit Dienstausweisen von Bundes- oder Landesbehörden;
- Durchführung der Sicherheitsüberprüfung ausschließlich unter Mitwirkung des BfV (Zentralstellenfunktion);
- Verwendung der Daten nur für Zwecke der Sicherheitsüberprüfung; keine Weiterleitung der Daten an Dritte, insbesondere in die USA bzw. nach Großbritannien;
- Rechtliches Gehör vor einer negativen Entscheidung;
- Grundsätzliche Pflicht zur Auskunftserteilung über gespeicherte Daten;
- Speicherung der Daten nur solange sie benötigt werden, d.h. solange das Beschäftigungsverhältnis andauert (GB) bzw. bis zwei Jahre nach Beendigung des Beschäftigungsverhältnisses (US);
- Wiederholungsüberprüfung nach zehn Jahren (GB) bzw. fünf Jahren (US) für Mitglieder von sog. Sonderprogrammen (z. B. Wachpersonal);
- Verwendung eines der Sicherheitserklärung (Ü 1) entsprechenden Formulars mit einer dem deutschen Recht entsprechenden Einwilligungserklärung.

Ob die vom BMI erstellte und mit mir abgestimmte Niederschrift, über diese Besprechung von US-amerikanischer und britischer Seite offiziell bestätigt worden ist, hat mir das BMI bislang noch nicht mitgeteilt.

Nach dieser Besprechung wurden mir Hinweise bekannt, dass die Sicherheitsüberprüfungen – zumindest durch die US-Streitkräfte – entgegen dem am 22. Juli 2004 erzielten Besprechungsergebnis nach wie vor nach dem bisherigen, nicht dem deutschen Recht entsprechenden Verfahren durchgeführt werden. Insbesondere soll die Einwilligungserklärung nicht die Anforderungen des § 4a BDSG erfüllen. Weiterhin sollen über die nach dem SÜG zulässigen Daten hinaus personenbezogene Daten abgefragt und über die Mitwirkung des BfV hinaus zusätzliche eigene Überprüfungen durch die US-Streitkräfte durchgeführt werden. Ferner soll die Einverständniserklärung den Hinweis enthalten, dass erhobene Daten an das US-Verteidigungsministerium und an Stellen außerhalb des US-Verteidigungsministeriums weitergegeben werden können. Hierzu habe ich das BMI um Stellungnahme und Klärung gebeten. Sollten sich diese Hinweise bestätigen, stünde dies in eklatantem Widerspruch zu dem am 22. Juli 2004 erzielten Besprechungsergebnis. Eine Stellungnahme des BMI lag mir bei Redaktionsschluss allerdings noch nicht vor.

6 Innere Verwaltung, Statistik

6.1 Zuwanderung

6.1.1 Das Zuwanderungsgesetz

Das am 1. Januar 2005 in Kraft getretene Zuwanderungsgesetz vom 30. Juli 2004 (BGBl. I S. 1950) bringt datenschutzrechtlich Licht und Schatten.

Wesentlicher Bestandteil des Zuwanderungsgesetzes ist das Aufenthaltsgesetz (AufenthG), das das Ausländergesetz (AuslG) ablöst. In ihm wurden die bisherigen Datenübermittlungsregelungen der §§ 75 bis 80 AuslG mit geringen Änderungen übernommen. Weitgehend gelten jedoch die datenschutzrechtlichen Regelungen des BDSG und der Landesdatenschutzgesetze. Die Datenschutzvorschriften des AufenthG kommen nur zur Anwendung, soweit sie von den allgemeinen Regelungen abweichen. Einerseits freut mich zwar diese gesetzestechnische Lösung. Auf der anderen Seite bedeuten die Regelungen im AufenthG, dass z. T. ohne stichhaltige Begründungen zu Lasten der Betroffenen von den datenschutzfreundlicheren Regelungen im allgemeinen Datenschutzrecht durch das AufenthG abgewichen wird. Dazu gehört z. B. die Regelung über den Ausschluss des Widerspruchsrechts nach § 20 Abs. 5 BDSG durch § 91 Abs. 3 AufenthG. Die in der amtlichen Begründung zu dieser Vorschrift (Bundestagsdrucksache 15/420 S. 98) gegebene Erläuterung, wonach ansonsten die Gefahr einer „erheblichen Verfahrensverzögerung“ bestünde und der „Gesichtspunkt der Verfahrensbeschleunigung im Ausländerrecht von besonderer Bedeutung“ sei, überzeugt mich nicht. Mit dem Zuwanderungsgesetz ist am 1. Januar 2005 auch die Durchführungsverordnung zum Zuwanderungsgesetz vom 25. November 2004 (BGBl. I S. 2945) in Kraft getreten, deren wesentlicher Bestandteil die Aufenthaltsverordnung (AufenthV) ist.

Besonders bedeutsam aus Sicht des Datenschutzes ist, dass dem aus dem Bundesamt für die Anerkennung ausländischer Flüchtlinge (BAFl) hervorgegangenen Bundesamt für Migration und Flüchtlinge (BAMF) u. a. folgende Aufgaben übertragen wurden:

- Entwicklung und Durchführung von Integrationskursen für Ausländer und Spätaussiedler;
- Führung des Ausländerzentralregisters (die tatsächliche Datenverarbeitung erfolgt allerdings als Datenverarbeitung im Auftrag weiterhin durch das Bundesverwaltungsamt, § 1 Abs. 1 Ausländerzentralregistergesetz – AZRG);
- Wissenschaftliche Forschung über Migrationsfragen;
- Koordinierung der Information über Arbeitsmigration zwischen Ausländerbehörden, der Bundesagentur für Arbeit und den deutschen Auslandsvertretungen.

Die Förderung von Integrationskursen durch den Bund, die ich mir im Berichtszeitraum angesehen habe, wird von einer Förderung der Träger von Integrationsveranstaltungen in eine Förderung der Teilnehmer an Integrationskursen umgestellt (vgl. Nr. 6.1.2.2).

Die von mir in den letzten beiden Tätigkeitsberichten (19. TB Nr. 34.1; 18. TB Nr. 5.1.3) geforderte Rechtsgrundlage für ausländerrechtliche Vermerke in ausländischen Pässen findet sich in § 99 Abs. 1 Nr. 10 AufenthG und § 56 Nr. 8 AufenthV. Damit sind auch die Kontrollstempel („Eintragungen über die Einreise, die Ausreise, das Antreffen im Bundesgebiet und über Entscheidungen der zuständigen Behörden zu solchen Papieren“) umfasst.

Inhaltlich unverändert geblieben ist im AufenthG die Regelung über die Beteiligung der Sicherheitsbehörden und Nachrichtendienste im Visumverfahren und bei der Erteilung von Aufenthaltserlaubnissen (§ 73 AufenthG). Für die Visumverfahren selbst und für die Erteilung von Aufenthaltserlaubnissen hat es dagegen eine Reihe von Änderungen gegeben. Dies gilt insbesondere für Fragen der Identitätsfeststellung sowie der Datenerfassung und -speicherung. So sind z. B. in der AufenthV Regelungen über die Speicherung von Daten von Bürgern aufgenommen worden, die visumpflichtige Ausländer einladen („Einladerdateien“). Es handelt sich dabei jedoch nicht um eine Zentraldatei, sondern um die Erfassung der Einladernamen bei den jeweiligen Auslandsvertretungen. Diese Daten müssen bei Gewährung des Visums ein Jahr nach Ablauf, wenn das Visum versagt wird, fünf Jahre nach der Entscheidung über den Antrag gelöscht werden. Forderungen nach Einführung einer zentralen Einladerzentraldatei lehne ich nach wie vor als unverhältnismäßig ab (vgl. 17. TB Nr. 5.5).

Über die Anwendung mit der durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) in das AuslG eingeführten Regelung (§ 64a) durch die Sicherheitsbehörden im Konsultationsverfahren nach Artikel 17 Schengener Durchführungsübereinkommen – SDÜ berichte ich an anderer Stelle (vgl. Nr. 5.2.6).

6.1.2 Bundesamt für Migration und Flüchtlinge

Anlässlich meiner Beratungs- und Kontrollbesuche beim Bundesamt stellte ich einen erfreulich hohen Datenschutzstandard fest.

Bislang war das Asylverfahren die Hauptaufgabe des BAFl. Das hat sich mit dem Inkrafttreten des Gesetzes zur Steuerung und Begrenzung der Zuwanderung und zur Regelung des Aufenthalts und der Integration von Unionsbürgern und Ausländern – Zuwanderungsgesetz – geändert (BGBl. I S. 1950).

Dem Bundesamt wurden am 1. Januar 2005 neue Aufgaben auf dem Gebiet der Migration und Integration von Unionsbürgern und Ausländern übertragen. Hierzu gehören u. a. die Entwicklung und Durchführung von Integrationskursen (Sprach- und Orientierungskurse) für Zuwanderer, die Neuausrichtung der Migrationserstberatung und die Förderung von Projekten zur sozialen und gesellschaftlichen Eingliederung der in Deutschland dauerhaft lebenden Spätaussiedler und Ausländer. Das Bundesamt wird zu einer zentralen Steuerungsstelle in Zuwanderungs- und Migrationsfragen umgestaltet.

Meine Beratungs- und Kontrollbesuche haben sich sowohl mit dem Asylverfahren als auch mit Zuwanderungs- und Migrationsfragen beschäftigt.

6.1.2.1 Alternierende Telearbeit für Einzelentscheider

Im 19. Tätigkeitsbericht (Nr. 7.1.3) hatte ich das Pilotprojekt „Alternierende Telearbeit für Einzelentscheider“ dargestellt. Das Pilotprojekt war zunächst auf zwei Jahre befristet und endete mit Ablauf des Jahres 2002. Nach dem mir im Anschluss daran vorgelegten Erfahrungsbericht bestand bei den Beschäftigten der übereinstimmende Wunsch diese weiterzuführen. Zur besseren Auslastung der telearbeitenden Einzelentscheider bat mich das Bundesamt um Prüfung, ob eine Ausweitung der (enggefassten) Dienstanweisung möglich wäre, ohne die berechtigten Interessen der Asylbewerber zu vernachlässigen.

Die Bitte war schon anlässlich eines Beratungs- und Kontrollbesuches im November 2002 an mich herangetragen worden. Um die Praktikabilität prüfen zu können, ließ ich mir sowohl Akten vorlegen, die aus Sicht des Einzelentscheiders und des Referatsleiters telearbeitgeeignet waren, als auch solche, die die Telearbeit ausschlossen. Ich habe festgestellt, dass gemäß den engen Regelungen in der Dienstanweisung viele Akten nicht telearbeitgeeignet waren. Die Dienstanweisung wurde daraufhin in Abstimmung mit mir überarbeitet und das Pilotprojekt um ein Jahr verlängert. Danach ist nun u. a. auch das Korrekturlesen sämtlicher Anhörungen und Bescheide des Einzelentscheiders am Telearbeitsplatz unter der Bedingung möglich, dass die am Telearbeitsplatz korrekturzulesenden Schriftstücke keine sog. Kopfleiste (Name, Geburtsdatum, Wohnort, Rechtsanwalt) sowie (im Text) keine schützenswerten Daten Dritter aus dem Herkunftsland des Asylbewerbers enthalten.

Der Erfahrungsbericht, den das Bundesamt im Frühjahr 2004 vorgelegt hat, kommt zu positiven Ergebnissen. Durch die Anpassung der Dienstanweisung konnte die Praktikabilität der Telearbeit für Einzelentscheider mit dem berechtigten Datenschutzinteresse der Asylbewerber in Einklang gebracht werden.

6.1.2.2 Das Bundesamt und die Integrationskursverordnung

Im Herbst 2004 habe ich einen Beratungs- und Kontrollbesuch beim Bundesamt im Rahmen einer Ablaufkontrolle mit den Schwerpunkten Integrationsmaßnahmen, Integrationsprogramme und Rückkehrförderung auf der Grundlage der zu dem Zeitpunkt aktuellen Rechtslage durchgeführt. Der Besuch sollte insbesondere zur Information im Hinblick auf die geplante Verordnung über die Durchführung von Integrationskursen für Ausländer und Spätaussiedler (Integrationskursverordnung) dienen. Die Ressortabstimmung wurde vom BMI unmittelbar im Anschluss an meine Kontrolle eingeleitet, sodass die Ergebnisse meines Besuches in die Beratungen einfließen konnten. Die Verordnung ist am 17. Dezember 2004 veröffentlicht worden (BGBl. I S. 3370 ff.). Wie die Regelungen in der Praxis umgesetzt werden können, bleibt

zunächst abzuwarten; ggf. müssen sie evaluiert werden. Ich werde die Entwicklungen beobachten.

Die kontrollierten Arbeitsabläufe entsprachen grundsätzlich den datenschutzrechtlichen Anforderungen. Das Bundesamt hat meine Hinweise und Anmerkungen umgesetzt und will sie auch in die Entwicklung und Einführung von IT-Anwendungen zur Unterstützung der Aufgabenerledigung einfließen lassen.

Die Auswirkungen der Integrationskursverordnung, die zum 1. Januar 2005 in Kraft getreten ist, auf die von mir kontrollierten Arbeitsabläufe bleiben abzuwarten. Ich habe dem Bundesamt meine Beratung bei der Umsetzung der Anforderungen, die sich aus dem Zuwanderungsgesetz für das Bundesamt ergeben, angeboten.

6.1.3 Passsammelstelle und Fundpapierdatenbank beim Bundesverwaltungsamt

Aufgefundene ausländische Ausweisdokumente werden beim Bundesverwaltungsamt gesammelt.

Häufig stellt sich die Frage, wie mit Pässen und anderen Personaldokumenten umgegangen werden soll, die von Ausländern in Deutschland verloren und hier aufgefunden wurden. Zu diesem Zweck hat das Bundesverwaltungsamt (BVA) eine Passsammelstelle eingerichtet, der ich im Juni 2003 einen Kontroll- und Beratungsbesuch abstattete.

Das Verfahren richtet sich nach den „Richtlinien über die Behandlung ausländischer Pässe, Passersatzpapiere, Personalausweise und Personenstandsurkunden“ des BMI. Diese sehen vor, dass die vorgenannten Personaldokumente von Ausländern, die nicht im Ausländerzentralregister erfasst sind und für die keine zuständige (Ausländer-)Behörde festgestellt werden kann, als Fundsache dem BVA (an die sog. **Passsammelstelle**) zuzuleiten sind. Das BVA gibt die Ausweisdokumente nach Prüfung an die jeweils zuständige konsularische oder diplomatische Vertretung des ausstellenden Staates in der Bundesrepublik Deutschland ab. Sofern der ausstellende Staat nicht ermittelt werden kann, werden die Ausweisdokumente für die Dauer von zehn Jahren beim BVA aufbewahrt. Dem BVA werden monatlich rund 200 Personaldokumente zugeleitet.

Bei der Kontrolle wurden sowohl Verfahrensmängel im Verantwortungsbereich des BVA als auch solche, die in der Zusammenarbeit mit dem BND begründet sind, festgestellt. Letztere konnten beim BVA nicht abschließend (auf-)geklärt werden. Ich habe das zum Anlass genommen, auch beim BND einen Beratungs- und Kontrollbesuch durchzuführen. Aufgrund dieser Kontrolle wurde das Verfahren geändert und datenschutzkonform ausgestaltet (vgl. Nr. 5.7.3).

Die Kontrolle ergab, dass in der Passsammelstelle auch Daten aus dem Ausländerzentralregister, die nicht zum Betroffenen gehören, in den Vorgängen abgelegt wurden. Dies widerspricht § 10 Abs. 3 Ausländerzentralregistergesetz, wonach die ersuchende Stelle solche Daten aus dem Ausländerzentralregister unverzüglich zu löschen und entsprechende Aufzeichnungen zu vernichten hat. Ich habe aber von einer Beanstandung abgesehen, weil das BVA seinerzeit die umgehende Beachtung der Vorschrift zugesagt hatte. Die entsprechenden Daten werden nunmehr unverzüglich vernichtet.

Im September 2004 hat die Bundesregierung einen Gesetzentwurf zur Änderung des Aufenthaltsgesetzes und weiterer Gesetze eingebracht, wonach ein Teil der bisher der Passsammelstelle zugeleiteten Personaldokumente in einer Datenbank **(Fundpapierdatenbank)** beim BVA gespeichert werden soll. Durch den Einsatz biometrischer Verfahren, insbesondere der Gesichtserkennung (vgl. auch Nr. 4.2.2), soll eine Zuordnung von aufgefundenen ausländischen Ausweispapieren zu Ausländern erleichtert werden. Dabei handelt es sich um Dokumente von Staatsangehörigen, die beim Überschreiten der Außengrenzen im Besitz eines Visums sein müssen, sowie von Personen aus Staaten, die von der Visumspflicht befreit sind. Ein Teil der Aufgaben der Passsammelstelle würde dadurch hinfällig. Dieser sollen künftig nur noch die aufgefundenen Ausweisdokumente von visafrei einreisenden Ausländern zugeleitet werden. Die dem BVA zugeleiteten Ausweisdokumente dieses Personenkreises sollen in der neu einzurichtenden Fundpapierdatenbank erfasst werden.

Gegen die Schaffung einer Fundpapierdatenbank habe ich keine grundsätzlichen Bedenken. Allerdings hat der Bundesrat den Gesetzentwurf abgelehnt, nachdem im Vermittlungsausschuss kein Kompromiss gefunden werden konnte. Strittig war aber nicht die Fundpapierdatenbank, zumal die Innenministerkonferenz das BMI gebeten hatte, einen Gesetzentwurf für eine dateigestützte Passabgleichstelle vorzulegen. Ich gehe daher davon aus, dass die Bundesregierung erneut einen entsprechenden Gesetzentwurf einbringen wird.

6.1.4 Gehören Daten von Staatsangehörigen eines Mitgliedstaates der EU ins Ausländerzentralregister?

Bislang werden Staatsangehörige eines Mitgliedstaates der EU, die ihren Wohnsitz in der Bundesrepublik Deutschland haben, im Ausländerzentralregister gespeichert. Aus meiner Sicht verstößt dies gegen europäisches Datenschutzrecht.

Die Frage, ob Daten von Staatsangehörigen eines Mitgliedstaates der EU mit Wohnsitz in der Bundesrepublik Deutschland im Ausländerzentralregister (AZR) gespeichert werden dürfen, ist nach wie vor nicht abschließend geklärt. Ende 2000 stammte jeder vierte im AZR gespeicherte Ausländer aus einem Mitgliedstaat der EU. Mit der Erweiterung der EU zum 1. Mai 2004 hat sich diese Zahl weiter erhöht.

Bereits 1999 wurde mir vom Europäischen Parlament eine entsprechende Petition zur Stellungnahme übersandt (vgl. 18. TB Nr. 5.1.1). Meine Prüfung ergab, dass die generelle Speicherung gegen die EG-Datenschutzrichtlinie 95/46/EG verstößt. Nur in Einzelfällen, dann wenn es um die Registrierung ausländerrechtlicher Entscheidungen wie Ausweisung oder Abschiebung geht, kann eine Speicherung zulässig sein. Das BMI hat mir daraufhin mitgeteilt, es prüfe, ob eine Änderung des AZRG in das Gesetzgebungsverfahren zum Zuwanderungsgesetz aufgenommen werden könnte, mit der die Speicherung

von Daten über Unionsbürger im AZR aufgehoben würde (vgl. 19. TB Nr. 34, dort Nr. 6). Dies ist nicht geschehen (vgl. auch Nr. 6.1.1).

Zwar sind im Entwurf des Gesetzes zur Änderung des Aufenthaltsgesetzes und weiterer Gesetze (Bundestagsdrucksache 15/3784) auch umfangreiche Änderungen des AZRG vorgesehen. Dennoch wurde meiner wiederholten Forderung im Rahmen der Abstimmung dieses Entwurfes, die generelle Speicherung der Daten von Unionsbürgern im AZR auszuschließen, nicht entsprochen.

Die Europäische Kommission hat am 7. Juli 2004 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Sie vertritt die Auffassung, dass eine generelle Verarbeitung personenbezogener Daten von Unionsbürgern in einem zentralen (Ausländer-)Register nicht notwendig ist im Hinblick auf Artikel 7 Buchst. e) der EG-Datenschutzrichtlinie. Ferner widerspräche die Verarbeitung dieser Daten in einem gesonderten Register für Ausländer dem Nichtdiskriminierungsprinzip aufgrund der Staatsangehörigkeit für jene, die ihr Recht ausüben, sich frei als Unionsbürger auf dem Gebiet eines Mitgliedstaates aufzuhalten, und verstoße damit gegen Artikel 12, 17 und 18 des EG-Vertrages. Das AZRG stehe daher in diesen Punkten nach Auffassung der Kommission nicht im Einklang mit dem EG-Vertrag und der europäischen Datenschutzrichtlinie.

Ich teile diese Auffassung und werde das Verfahren ebenso aufmerksam verfolgen wie das aufgrund des Vertragsverletzungsverfahrens zur Zeit ruhende verwaltungsrechtliche Verfahren, mit dem der Petent die Löschung seiner Daten aus dem AZR verfolgt.

6.1.5 Eurodac – eine Erfolgsgeschichte?

Seit 15. Januar 2003 ist Eurodac in Betrieb.

Das **Euro**päische **dac**tyloskopische Fingerabdrucksystem Eurodac, über dessen Regelungen ich berichtete (vgl. 17. TB Nr. 5.7; 19. TB Nr. 7.1.1), hat planmäßig am 15. Januar 2003 seine Tätigkeit aufgenommen.

Ich habe dies zum Anlass genommen, mich bei den für die nationale Umsetzung der Eurodac-Verordnung zuständigen Stellen über die Arbeitsabläufe zu informieren. Dazu habe ich die Zentrale des Bundesamtes für Migration und Flüchtlinge (früher: Bundesamt für die Anerkennung ausländischer Flüchtlinge) sowie eine Außenstelle und das BKA besucht. Gegen die Arbeitsabläufe zur Erstellung, Bearbeitung und Übermittlung der sog. Eurodac-Treffer bestehen keine Bedenken. Die zentrale Datenbank in Luxemburg wird durch den europäischen Datenschutzbeauftragten kontrolliert (vgl. Nr. 3.2.3)

Erfahrungsgemäß weckt eine solche Datenbank Begehrlichkeiten. So hat Deutschland bereits im Herbst 2001 vorgeschlagen, die in der zentralen Eurodac-Datenbank gespeicherten Daten auch für polizeiliche Zwecke zu nutzen. Die Einbeziehung des Eurodac-Datenbestandes würde dabei die Zuordnung polizeilicher Erkenntnisse zu Fingerabdrücken von Personen, die sich in anderen Mitgliedstaaten als Asylbewerber aufhalten, ermöglichen. Hierdurch würde die Strafverfolgung erheblich erleichtert und auch Sicherheitsrisiken könnten bereits im Vorfeld erkannt werden.

Eine solche Nutzung der Daten für polizeiliche Zwecke ist aufgrund der strikten Zweckbindung der Eurodac-Verordnung an das Dubliner Übereinkommen nicht möglich. Die Daten dürfen nur zur Bestimmung des für die Prüfung des Asylantrages zuständigen Mitgliedstaates bzw. nur zur entsprechenden Prüfung des Asylantrages verwendet werden. Für darüber hinausgehende Vorstellungen wäre eine Änderung der Eurodac-Verordnung notwendig.

Ich werde die Entwicklungen in diesem Bereich weiter verfolgen.

6.2 Biometrie in Ausweisdokumenten

Biometrische Verfahren sollen – trotz erheblicher Zweifel an der Zuverlässigkeit der vorgesehenen Technik – in Ausweisdokumente integriert werden.

Das Lichtbild ist seit jeher Bestandteil von Ausweisdokumenten. Durch die Einbringung eines digitalisierten Lichtbildes wird es grundsätzlich möglich sein, nach der abgebildeten Person in einer Datenbank zu suchen. Fingerabdrücke waren in anderen Staaten bereits Bestandteil von Ausweisdokumenten (vgl. 19. TB, Nr. 2.2.3, 2.3.4).

Die Notwendigkeit der Einführung elektronisch auswertbarer biometrischer Merkmale wird vor allem mit Sicherheitsgewinnen begründet:

– Die Fälschungssicherheit der Papiere werde erhöht.
– Die Verwendung falscher oder gestohlener Dokumente werde unterbunden.
– Kontrollen in sicherheitsempfindlichen Bereichen, etwa an Flughäfen, würden beschleunigt.

Auf Basis der inzwischen gewonnenen Erkenntnisse habe ich Zweifel, ob die biometriegestützten Reisedokumente tatsächlich die versprochenen Sicherheitsgewinne mit sich bringen, denn

– bereits heute ist die Fälschungssicherheit deutscher Pässe und Personalausweise weitestgehend gewährleistet (vgl. 19. TB Nr. 7.2),
– wenn biometriegestützte Pässe in Staaten ohne geordnetes Personenstandswesen ausgestellt werden, kann die Ausstellung von biometriegestützten Dokumenten auf andere Personen nicht verhindert werden,
– angesichts hoher Fehlerquoten bei automatisierten Auswertungsverfahren ist mit erheblichen individuellem Nachbereitungsaufwand zu rechnen.

Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) waren in das Passgesetz (§ 4 Abs. 3 und 4 PassG) und in das Personalausweisgesetz (§ 1 Abs. 4 und 5 PersauswG) Regelungen eingefügt worden, die prinzipiell die Aufnahme biometrischer Merkmale in Ausweisdokumente vorsehen. Auf ihrer 63. Sitzung im März 2002 hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit dem Thema befasst und eine Entschließung verabschiedet, in der sie bestimmte Anforderungen an die

Einführung biometrischer Merkmale in Ausweispapieren stellt (vgl. Kasten zu Nr. 6.2).

Im nationalen wie im internationalen Bereich gab es in der Folgezeit zahlreiche Aktivitäten zur Einführung biometrischer Merkmale in Ausweisdokumente. Maßgebliche Impulse kommen dabei von der Internationalen Zivilluftfahrt-Organisation (International Civil Aviation Organization – ICAO), einer Sonderorganisation der Vereinten Nationen (VN), die sich bereits seit Jahren mit der Einführung biometrischer Verfahren in Ausweisdokumente befasst. Seit September 2000 favorisiert die ICAO das Gesichtserkennungsverfahren. Nach dem 11. September 2001 wurden die Arbeiten deutlich intensiviert. Die ICAO und die von ihr beauftragte Internationale Standardisierungsorganisation ISO arbeiten anderen nationalen Standardisierungsorganisationen zu, wie z. B. dem Deutschen Institut für Normung e. V. An den Vorgaben der ICAO sowohl hinsichtlich der Frage, welche biometrischen Merkmale in Ausweisdokumente eingeführt werden sollen, als auch hinsichtlich der Nutzung bestimmter Techniken orientieren sich sowohl die Europäischen Kommission und der Europäische Rat sowie die Bundesregierung. Die Vorgaben der ICAO bilden damit – obwohl sie völkerrechtlich nicht verbindlich sind – einen faktischen internationalen Standard bei der Einführung biometrischer Merkmale und Verfahren.

Hinsichtlich des praktischen Nutzens biometrischer Merkmale – sowohl zur Verifikation wie auch zur Identifikation – sei nur auf die Vielzahl technischer Probleme hingewiesen, die zum großen Teil noch nicht gelöst sind. Der vom Büro für Technikfolgenabschätzung (TAB) dem Deutschen Bundestag vorgelegte Bericht verweist darauf, dass für die prinzipiell gut erforschten biometrischen Anwendungen von digitaler Hand- und Iriserkennung die Erkennungsleistung bislang noch nicht großflächig getestet wurden. Aber auch bei den genauer untersuchten Fingerabdruck- und Gesichtserkennungsverfahren ist festzuhalten, dass im Masseneinsatz immer noch eine sehr große Anzahl von Personen falsch erkannt wird. So können Fingerabdrücke nicht bei allen Menschen abgenommen werden.

Eine hohe Falscherkennung bzw. Falschakzeptanz wären bei einem biometrischen System unter Sicherheitsaspekten Ausschlusskriterien, d. h. diese Verfahren wären für einen Masseneinsatz ungeeignet. Fehlerhafte Rückweisungen hätten hingegen für die Betroffenen nicht nur diskriminierende Auswirkungen und würden zu einer schlechten Akzeptanz des Verfahrens beim Nutzer führen. Die Falschrückweisungsproblematik lässt sich auch nicht durch Kombination verschiedener biometrischer Merkmale – etwa Fingerabdruck und Gesichtserkennung – lösen; vielmehr würde möglicherweise nunmehr eine Person bereits dann zurückgewiesen, wenn nur ein biometrisches Merkmal nicht passt. Im Ergebnis würde sich dadurch die Falschrückweisungsquote eventuell noch erhöhen.

Das TAB hat in seinem Bericht zudem auf den hohen finanziellen Aufwand bei der Einführung biometrischer Verfahren hingewiesen.

Hinweis: „Zweiter Sachstandbericht – Biometrie und Ausweisdokumente“ des TAB, Bundestagsdrucksache 15/4000, www.tab.fzk.de/de/projekt/zusammenfassung/ab93.pdf

Kasten zu Nr. 6.2

63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 7. und 8. März 2002

Entschließung:
Biometrische Merkmale in Personalausweisen und Pässen

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat eingehend über Geeignetheit, Erforderlichkeit und Angemessenheit der beabsichtigten Einführung biometrischer Merkmale in Ausweisen und Pässen diskutiert. Sie hat ein Positionspapier des Arbeitskreises Technik, das detaillierte Prüfpunkte für die Erprobungsphase einer solchen Maßnahme nennt, zustimmend zur Kenntnis genommen. Für den Fall, dass das Vorhaben trotz noch bestehender Bedenken realisiert werden sollte, hat sie übereinstimmend folgende Anforderungen formuliert:

1. Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.
2. Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.
3. Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.
4. Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.
5. Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

6.2.1 Die EU-Pass-Verordnung

Künftig soll der Pass der EU-Bürger einen RFID-Chip enthalten, in dem auch biometrische Merkmale gespeichert werden.

Am 13. Dezember 2004 hat der Rat der Europäischen Union (Ministerrat) die „Verordnung (EG) Nr. 2252/2004 des Rates über Normen für Sicherheitsmerkmale und biometrische Daten in von den Mitgliedstaaten ausgestellten Pässen und Reisedokumenten“ beschlossen (EU-Pass-Verordnung – ABl. Nr. L 385 vom 29. Dezember 2004, S. 1). Mit dieser Verordnung werden die Pässe in den Mitgliedstaaten der Europäischen Union weiter vereinheitlicht. Die beschlossene EU-Pass-Verordnung zielt auf die Schaffung einheitlicher Normen für Sicherheitsmerkmale sowie auf die Einführung biometrischer Merkmale in die Pässe der EU-Bürger.

Bei der Diskussion über die Einführung biometrischer Merkmale in die Pässe der EU-Bürger bestand zwischen den EU-Staaten Einigkeit hinsichtlich des digitalisierten Lichtbildes als aufzunehmendes biometrisches Merkmal. Allerdings gab es unterschiedliche Auffassungen darüber, in welcher Form die Lichtbilddaten in einen in den Pass integrierten Chip aufgenommen werden sollen: lediglich als Template – d. h. in Form eines elektronischen Referenzmusters des Lichtbildes – oder als Rohdaten. Da man sich auf europäischer Ebene weitgehend an die Vorgaben der ICAO halten will, hat man sich für die Speicherung des Rohdatensatzes entschieden.

Die Diskussion über ein zweites biometrische Merkmal konzentrierte sich rasch auf den digitalen Fingerabdruck. Umstritten war allerdings, ob dieses zweite biometrische Merkmal verbindlich vorgeschrieben oder fakultativ bleiben sollte. Während einige Mitgliedstaaten im Sommer 2004 noch mit ihrem Ansinnen, das zweite biometrische Merkmal verbindlich vorzuschreiben, gescheitert waren, führten interne Beratungen der sog. G-5-Gruppe (Deutschland, Frankreich, Italien, Spanien, Vereinigtes Königreich) dazu, dass der Ministerrat für Justiz und Inneres bei seiner Sitzung am 25. Oktober 2004 den bereits im Konsultationsverfahren im Europäischen Parlament (EP) befindlichen Verordnungsvorschlag ohne weitere Begründung dahingehend änderte, den digitalisierten Fingerabdruck als weiteres verbindliches Merkmal vorzusehen. Nur wenige Tage vor Verabschiedung der Stellungnahme des EP wurde diesem daher ein geänderter Verordnungsvorschlag übersandt. Das EP hat diesen neuen Vorschlag zur Kenntnis genommen, seine Stellungnahme aber zu dem alten Vorschlag abgegeben, der lediglich die fakultative Aufnahme von digitalisierten Fingerabdrücken vorsah.

Ein weiteres datenschutzrechtliches Problem war in den Erwägungsgründen des Verordnungsentwurfs nur am Rande erwähnt worden. Dort war unter dem Aspekt „langfristige Perspektive“ die Schaffung eines europäischen Passregisters, d. h. einer europäischen Zentraldatei mit den Angaben zu allen in den EU-Mitgliedstaaten herausgegeben Pässen angesprochen. Hiergegen hat sich nicht nur die Art. 29-Gruppe mit einem Schreiben vom 18. August 2004 an den Vorsitzenden des Rates, den Präsidenten der Europäischen Kommission, den Präsidenten des EP und weitere europäische Stellen gewandt. Auch das EP hat sich in seiner Stellungnahme vom 2. Dezember 2004 ausdrücklich gegen eine zentrale Datenbank der Pässe und Reisedokumente ausgesprochen.

Am 13. Dezember 2004 hat der Ministerrat die EU-Pass-Verordnung beschlossen, ohne inhaltlich die Stellungnahme des EP in wesentlichen Teilen zu berücksichtigen. Die Art. 29-Gruppe unterstützt die Position des EP und fordert, dass

- in den Verordnungstext ein ausdrückliches Verbot einer zentralen Datenbank aufgenommen wird,
- die biometrischen Daten nur verwendet werden dürfen, um die Echtheit des Dokuments und die Identität des Inhabers mittels direkt verfügbarer vergleichbarer Merkmale zu prüfen (Verifikation), wenn das Vorzeigen des Passes gesetzlich vorgeschrieben ist,
- auf dem Pass keine weiteren Daten als die gesetzlich zugelassenen gespeichert werden,
- der Zweck, zu dem die Daten aus dem Pass gelesen, gespeichert, verändert oder gelöscht werden dürfen, ebenso konkret bestimmt sein soll, wie die staatlichen Stellen, die die Daten lesen, speichern, verändern oder löschen dürfen.

Außerdem halten es alle Datenschutzkontrollinstanzen in den Mitgliedstaaten der EU für wünschenswert, wenn der in der EU-Pass-Verordnung vorgesehene Ausschuss bei seinen Beratungen vor der Beschlussfassung von Beauftragten der Art. 29-Gruppe datenschutzrechtlich beraten wird, damit die festzulegenden technischen Spezifikationen von vornherein datenschutzrechtlichen Anforderungen genügen.

6.2.2 Neue Techniken für Reisedokumente bei der Bundesdruckerei GmbH

Bei der Bundesdruckerei GmbH habe ich mich über die technischen Möglichkeiten der Einführung biometrischer Merkmale in Pässe und andere Ausweispapiere informiert.

Mit der Einführung biometrischer Merkmale in den Reisepass aufgrund der EU-Pass-Verordnung (vgl. Nr. 6.2.1) soll eine neue Technik in die Reisedokumente eingeführt werden. Dabei bleiben Zweifel, ob die Einführung biometrischer Merkmale einen Gewinn für die Fälschungssicherheit von Reisedokumenten bedeutet. Soweit eine zusätzliche Fälschungssicherheit für Reisedokumente angesprochen wird, wird dies eher auf die Einführung einer Chiptechnologie zurückzuführen sein. Dabei soll aber nicht verkannt werden, dass schon die bisherigen deutschen Reisepässe und Personalausweise ein sehr hohes technisches Niveau im Hinblick auf Fälschungssicherheit haben.

Bei Besuchen in der Bundesdruckerei habe ich mich erkundigt, welche technischen Möglichkeiten zur Implementierung eines Chips in den Reispass bestehen. Deutlich wurde dabei, dass nach den Vorgaben der ICAO nur ein 2D-Barcode oder ein sogenannter RFID-Chip (Radio Frequency Identification-Chip, vgl. Nr. 4.2.1) für die Aufnahme biometrischer Merkmale in Ausweisdokumente in

Frage kommen. Die 2D-Barcode-Technologie soll für die internationalen Berufsausweise für Seeleute (vgl. Nr. 6.2.5) genutzt werden. Demgegenüber sieht die EU-Pass-Verordnung die Nutzung eines RFID-Chips vor.

6.2.3 Biometrische Merkmale bei Visa- und Aufenthaltserlaubnissen

Im Rahmen der gemeinsamen Visapolitik der Europäischen Union soll Biometrie in die Visaverfahren und in Aufenthaltstitel für Drittstaatsangehörige integriert werden.

Bereits vor dem 11. September 2001 hatten das Auswärtige Amt und das BMI damit begonnen, das Lichtbild in das Visumetikett aufzunehmen. Mit der Verordnung (EG) Nr. 334/2002 vom 18. Februar 2002 (ABl. Nr. L 53 S. 7) hat der Rat festgelegt, dass ein nach „Hochsicherheitsnormen hergestelltes Lichtbild“ in das Visumetikett integriert wird.

Am 24. September 2003 legte die Kommission einen Verordnungsvorschlag vor, der nicht nur die Einführung biometrischer Merkmale (digitales Lichtbild, zwei digitale Fingerabdrücke vom flachen Finger) in Visa und Aufenthaltstiteln für Drittstaatenangehörige vorsah, sondern auch die Schaffung einer nationalen wie auch einer gemeinschaftlichen Datenbank (VIS = Visa Information System) mit alphanumerischen Informationen (z. B. Name, Adresse, Geburtsdaten), biometrischen Daten (digitalisiertes Lichtbild, Fingerabdrücke) sowie sonstigen eingescannten Dokumenten (gedacht war an Pässe, Geburtsurkunden etc.) der Visaantragsteller.

Unter dem Eindruck der Anschläge vom 11. März 2004 in Madrid forderte der Rat die Kommission auf, Vorschläge zur Verbesserung der Interoperabilität europäischer Datenbanken vorzulegen und außerdem zu erkunden, welche Synergieeffekte zwischen bestehenden und künftigen Informationssystemen (SIS II, VIS und Eurodac) zur Verhütung und Bekämpfung des Terrorismus erzielt werden könnten.

Nach dem am 8. Juni 2004 gefallenen Beschluss des Rates zur Bereitstellung der Finanzmittel haben die Vorarbeiten zur Errichtung dieses Systems begonnen. Dabei wird von Seiten der Kommission eine identische technische Plattform wie das neue Schengen Informationssystem (SIS II – vgl. Nr. 3.3.2.1) angestrebt.

Alle Maßnahmen in diesem Bereich wirken sich erheblich auf die Grundrechte der Ausländer aus, die ein Visum zur Einreise in einen sog. Schengenstaat beantragen. Im erweiterten Europa rechnet man ab 2007 mit etwa 20 Mio. Visaanträgen pro Jahr. Die Datenbank wird daher im laufenden Verfahren bis zu 100 Mio. Menschen betreffen.

Die Art. 29-Gruppe (vgl. Nr. 3.2.1) hat sich mit ihrer Stellungnahme Nr. 7/2004 vom 11. August 2004 kritisch mit den Vorschlägen der Kommission auseinandergesetzt. Sie betont, dass bei allem Verständnis für das Bestreben „Visa-Shopping“ und „Identitätsdiebstahl“ zu bekämpfen, der Schutz der Grundrechte gewahrt werden muss. Sie hat Bedenken geäußert, ob bei der Schaffung einer Zentraldatei mit biometrischen Merkmalen aller Ausländer, die ein Visum beantragt haben, der Grundsatz der Verhältnismäßigkeit beachtet wird. Außerdem wurde dringend die Schaffung von präzisen Zweckbestimmungsregelungen angemahnt. Insbesondere für den Chip, der nach den ursprünglichen Plänen auf dem Visum aufgebracht werden sollte, wurden hohe Anforderungen an die Sicherheit formuliert. Für den Fall von Erkennungsfehlern bei biometriegestützten Grenzkontrollen müssen die betroffenen Personen über die Ursachen der Zurückweisung unterrichtet werden. Ferner müssen sie die Möglichkeit erhalten, ihren Standpunkt darlegen zu können, bevor eine Entscheidung getroffen wird (Artikel 15 der EG-Datenschutzrichtlinie).

Ein am 28. Dezember 2004 vorgelegter neuer Verordnungsvorschlag der Kommission berücksichtigt einen Teil dieser Forderungen. Er sieht vor, in VIS alphanumerische und biometrische Daten (digitalisiertes Lichtbild, Fingerabdrücke), aber keine sonstigen eingescannten Dokumente zu speichern. Dafür sollen aber Verknüpfungen zu anderen Anträgen gespeichert werden. Für die Daten ist eine Löschungsfrist von fünf Jahren vorgesehen. Der Vorschlag enthält auf Grund von Schwierigkeiten bei der Verwendung der RFID-Technik keine Regelung über die Speicherung biometrischer Merkmale in den Visaetiketten. Genutzt werden soll das VIS nicht nur bei Visaverfahren, sondern auch im Asylverfahren und zur Identifizierung und Rückführung illegaler Einwanderer. Die Art. 29-Gruppe beabsichtigt, zu dem Entwurf kurzfristig Stellung zu nehmen und damit zu einer Berücksichtigung datenschutzrechtlicher Belange bei der anstehenden Beratung des EP beizutragen.

Kasten zu Nr. 6.2.3

Das VIS soll folgenden Zwecken dienen:

- Unterstützung im Kampf gegen Betrug,
- Verbesserung der konsularischen Zusammenarbeit zwischen den Mitgliedstaaten bei der Erteilung von Visa,
- Unterstützung bei der Identifizierung des Visuminhabers,
- Prävention gegen „Visa-Hopping“ („Bekomme ich das Visum nicht von dem einen Schengenstaat, gehe ich zur Auslandsvertretung eines anderen Schengenstaates“),
- Prävention gegen „Visa-Shopping“ (Suche nach dem „vorteilhaftesten“ Visum),
- Unterstützung bei Anfragen nach dem Dubliner Übereinkommen,
- Unterstützung bei der Identifizierung und der Rückführung von Drittstaatsangehörigen,
- Beitrag zur internationalen Sicherheit und im Kampf gegen den Terrorismus.

6.2.4 Pilottestverfahren zur Gesichtserkennung im Bundesverwaltungsamt

Gesichtserkennung in Visaverfahren reicht als alleiniges Suchkriterium nach früheren Visaentscheidungen nicht aus.

Durch das Terrorismusbekämpfungsgesetz vom 9. Januar 2002 (BGBl. I S. 361) wurde § 29 Abs. 1 Ausländerzentralregistergesetz dahingehend geändert, dass in der beim Bundesverwaltungsamt (BVA) geführten zentralen Visadatei auch das Lichtbild des Visumantragstellers gespeichert werden kann. In der zentralen Visadatei waren mit Ablauf des Berichtszeitraums mehr als drei Mio. Entscheidungen über Visaanträge aus mehr als 175 Auslandsvertretungen gespeichert. Zu diesen Datensätzen waren Ende 2004 mehr als 1,7 Mio. Lichtbilder von Visumantragstellern aufgenommen worden.

Das BVA hat in dem Pilotprojekt „Biometrie im VISA-Verfahren des Bundesverwaltungsamtes“ die sog. „Kleine Biometrielösung“ entwickelt, wobei ich die frühe und gute Zusammenarbeit mit dem BVA hervorheben möchte (vgl. auch Nr. 4.2.2.). Ziel des Projektes war zunächst die Prüfung, ob die Leistungsfähigkeit biometrischer Gesichtserkennungsverfahren für den geplanten Einsatz in dem Masseverfahren Visaerteilung ausreicht. Wesentliches Ergebnis der Tests war, dass der Datensatz in der Visadatei mit Hilfe des Gesichtserkennungsverfahrens im Regelfall wiedergefunden wird, wenn der betreffende Visumantragsteller dasselbe Bild einreicht, das er auch bei seinem letzten Antrag vorgelegt hat. Legt er ein anderes Bild vor, verschlechtert sich die Wiedererkennungsrate jedoch deutlich. Unterschiede bei der Erkennungsleistung aufgrund des Herkunftslandes oder der ethnischen Zugehörigkeit des Visumantragstellers konnten bei den Tests nicht nachgewiesen werden.

Insgesamt zog das BVA das Fazit, dass die Gesichtserkennung im Visaverfahren zwar nicht als alleiniges Suchkriterium ausreicht, herkömmliche alphanumerisch/phonetischen Suchkriterien jedoch sinnvoll ergänzen kann. Da die Gesichtserkennungsverfahren – wie alle anderen biometrischen Verfahren auch – aufgrund der laufenden Forschung sich in den nächsten Jahren noch deutlich verbessern können, werde ich die Entwicklungen auch hier aufmerksam verfolgen. Zur entsprechenden europäischen Entwicklung vgl. Nr. 6.2.3.

6.2.5 Der Seefahrer-Ausweis

Auch die Seefahrer-Ausweise werden in Zukunft digitalisierte Lichtbilder und Fingerabdrücke enthalten. Zusätzlich sollen die Daten in einer nationalen Datenbank zur Überprüfung der Echtheit des Ausweises gespeichert werden.

Die Internationale Arbeitsorganisation (International Labour Organization – ILO) hat am 5. Juni 2003 das „Übereinkommen Nr. 185 über Ausweise für Seeleute“ verabschiedet, das im Februar 2005 in Kraft treten wird. Es sieht die Aufnahme des digitalisierten und/oder Originallichtbildes sowie von Fingerabdrücken in den Ausweis für Seeleute in Form eines 2D-Barcodes vor. Dieser Ausweis für Seeleute ist ein Berufsausweis, der nach dem Übereinkommen ausdrücklich kein Reisedokument ist, dem Inhaber aber bestimmte Vergünstigungen gewährt (Landgang während der Liegezeit des Schiffes ohne Beantragung eines Visums, Transit vom oder zum Schiff oder zwischen Schiffen mit Visum unter erleichterten Bedingungen). Zusätzlich zur Aufnahme biometrischer Merkmale in diesen Berufsausweis sollen die Daten der weltweit ca. 1,2 Mio. Seeleute im Ausgabeland des Ausweises, d. h. dezentral in nationalen Datenbanken, gespeichert werden.

Für das Vorhaben gelten prinzipiell dieselben Vorbehalte wie gegenüber der Verwendung biometrischer Daten in sonstigen Ausweisdokumenten. Das „Übereinkommen über Ausweise für Seeleute“ enthält einige datenschutzrechtlich erfreuliche Regelungen. Dazu gehört, dass die in der nationalen Datenbank gespeicherten Merkmale abschließend geregelt sind und nur der Verifikation dienen sollen. Ausdrücklich wird in dem Übereinkommen gefordert, die Datensicherheit zu garantieren und das Recht des Betroffenen auf Datenschutz („right of privacy“) zu beachten. Auch das Auskunftsrecht des betroffenen Seemanns ist – sowohl hinsichtlich der auf der Ausweiskarte als auch hinsichtlich der in der Datenbank gespeicherten Daten – datenschutzrechtlich zufriedenstellend geregelt. Bedenken habe ich lediglich hinsichtlich der Datenübermittlungsregelungen, die mit den Vorgaben der EG-Datenschutzrichtlinie dann kollidieren können, wenn – was sehr wahrscheinlich ist – die Daten von Seeleuten aus EU-Mitgliedstaaten von Behörden aus Drittstaaten ausgelesen und/oder an diese übermittelt werden, wenn diese nicht das von der EG-Datenschutzrichtlinie geforderte angemessene Datenschutzniveau besitzen. Eine derartige Datenübermittlung könnte jedoch dadurch gerechtfertigt sein, dass sich die Mitgliedstaaten, die das Übereinkommen ratifiziert haben, verpflichten, die Daten nur für Zwecke der Verifikation des Ausweises zu nutzen.

6.3 Die Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) und das Stasi-Unterlagen-Gesetz (StUG)

Dem sensiblen Bereich der BStU gilt nach wie vor mein besonderes Augenmerk. Ich habe die Zentrale der BStU in Berlin und eine Außenstelle besucht und im schriftlichen Verfahren beraten.

6.3.1 Der „Fall Kohl“ – Fortsetzung

Auch nach einer weiteren Runde im Rechtsstreit sind die Konsequenzen im „Fall Kohl“ nicht absehbar.

Nach dem ersten Urteil des Bundesverwaltungsgerichts vom 8. März 2002 (vgl. 19. TB Nr. 7.6.1) galt zunächst, dass die BStU im Fall Kohl gegen dessen Willen in keinem Fall Unterlagen herausgeben durfte. Dies war nach der neu gefassten Abwägungsklausel des § 32 StUG (5. Gesetz zur Änderung des Stasi-Unterlagen-Gesetzes)

vom 6. September 2002 jedoch wieder zweifelhaft. Zur Klärung haben die Parteien erneut die Gerichte angerufen.

Nach dem zweiten Urteil des Bundesverwaltungsgerichts (BVerwG, 3 C 41.03 vom 23. Juni 2004) ist das geänderte StUG einschränkend verfassungskonform auszulegen und anzuwenden. Hierfür hat das Gericht Kriterien festgelegt. Die BStU hat angekündigt, ihre internen Richtlinien für die Herausgabe von Akten zu überarbeiten und die Praxis entsprechend zu ändern. Konkrete Angaben über die Änderungen und deren Bedeutung für die Praxis liegen mir bisher nicht vor. Fest steht, dass eine Herausgabe von Unterlagen ohne Zustimmung des Betroffenen noch sensibler geprüft werden muss und nur noch in ganz besonderen Ausnahmefällen möglich ist.

Die Urteile im Wortlaut finden Sie unter http://www.bundesverwaltungsgericht.de.

6.3.2 „Steckbriefe“ von Stasi-Mitarbeitern im Internet

Ehemalige Stasi-Mitarbeiter beschwerten sich über die Veröffentlichung ihrer Lebensläufe mit Lichtbild auf den Seiten einer Außenstelle der BStU im Internet.

Durch mehrere Eingaben von Petenten und den Hinweis einer Landesbeauftragten für den Datenschutz wurde ich im Februar 2004 darauf aufmerksam, dass auf den Internetseiten der BStU personenbezogene Daten ehemaliger Stasi-Mitarbeiter veröffentlicht wurden. Die Eingaben der Petenten richteten sich vor allem auch gegen die Art und Weise der Veröffentlichung, weil sie einem „Steckbrief“ ähnlich sei. Nach einer ersten Überprüfung habe ich die BStU gebeten, die Rechtsgrundlage für eine solche Veröffentlichung auch in Bezug auf Art und Weise ihrer Darstellung noch einmal zu prüfen. Die BStU hat sich für die Veröffentlichung auf ihren Gesetzesauftrag gemäß § 37 Abs. 1 Nr. 5 StUG berufen, die Öffentlichkeit umfassend über den Staatssicherheitsdienst der DDR zu informieren. Wegen der Art und Weise der Veröffentlichung wurden die beanstandeten Seiten jedoch umgehend entfernt. Die BStU hat darüber hinaus den Vorgang zum Anlass genommen, eine interne Arbeitsgruppe mit der Erarbeitung von Richtlinien für eine Veröffentlichung personenbezogener Daten im Internet zu beauftragen. Diese liegen noch nicht vor. Ich gehe davon aus, dass die BStU sich wieder weitgehend an ihre ursprüngliche Praxis halten wird: Seit längerem werden über das Führungspersonal des ehemaligen Ministeriums für Staatssicherheit nach einer ausführlichen erläuternden Vorbemerkung Kurzbiografien in Blockform und ohne Bild veröffentlicht.

6.4 Datenschutz im Bundesministerium des Innern

2003 habe ich einen Beratungs- und Kontrollbesuch beim BMI durchgeführt. Das BMI hat die dabei festgestellten Mängel inzwischen weitgehend beseitigt.

Bei einem Beratungs- und Kontrollbesuch im Bundesministerium des Innern habe ich den Umgang mit personenbezogenen Daten im nicht-automatisierten Verfahren sowie die Führung von Personalakten und der Versorgungsakten sowie der Teilakten „Besoldung, Vergütung, Löhne, Beihilfen“, die beim Bundesverwaltungsamt – Außenstelle Berlin-Lichtenberg – bearbeitet werden, kontrolliert (Prüfergebnisse zum Bereich Personalwesen vgl. Nr. 10.5).

Zum Zeitpunkt des Besuches verfügte das BMI nicht mehr über einen behördlichen Datenschutzbeauftragten (bDSB). Der bisherige bDSB war in den Ruhestand gegangen und ein Nachfolger – entgegen der zwingenden Vorschrift des § 4f BDSG – noch nicht bestellt. Ich habe das BMI gebeten, dafür Sorge zu tragen, dass die dringend erforderliche Bestellung eines bDSB umgehend vorgenommen wird. Zudem habe ich deutlich gemacht, dass ich die lediglich nominelle Bestellung eines bDSB als Zusatzfunktion zu seinen sonstigen Aufgaben in einer so großen und vielgestaltigen Behörde wie dem BMI für nicht ausreichend halte. So sind vielmehr die Bereitstellung entsprechender Arbeitskapazitäten in Form einer – zumindest teilweisen – Freistellung von anderen Aufgaben sowie nötigenfalls die Zuweisung von Hilfspersonal gem. § 4f BDSG und die Anbindung an die Leitungsebene zwingend erforderlich. Da das BMI diesen Forderungen – wenn auch mit fast einem Jahr Verspätung – durch Bestellung einer Referatsleiterin auf einer halben Stelle, allerdings ohne Unterstützungspersonal, weitgehend nachgekommen ist, habe ich von einer förmlichen Beanstandung abgesehen. Dies auch, weil ich bei der Kontrolle keine sonstigen schwerwiegenden datenschutzrechtlichen Mängel beim Umgang mit personenbezogenen Daten in den kontrollierten Abteilungen festgestellt hatte. Zudem hat das BMI meine Anregungen übernommen und entsprechende Änderungen veranlasst.

Diesen ersten Beratungs- und Kontrollbesuch im BMI habe ich bewusst auf vier Abteilungen beschränkt; ich habe mir aber weitere Besuche, insbesondere des Sicherheitsbereichs, ausdrücklich vorbehalten.

6.5 Neues bei der Bundesakademie für öffentliche Verwaltung

Das Interaktive Fortbildungssystem für die Bundesverwaltung – IFOS-Bund – soll den am Fortbildungsprozess Beteiligten die Arbeit und den Informationsaustausch erleichtern.

Die Bundesakademie für öffentliche Verwaltung (BAköV) hat zusammen mit der Fachhochschule des Bundes für öffentliche Verwaltung (FH Bund) das System **IFOS-Bund** entwickelt. Dieses intranet-/internetbasierte System erleichtert es den am Fortbildungsprozess Beteiligten, Planungen, Veröffentlichungen und Buchungen von Fortbildungsveranstaltungen sowie die erforderliche Kommunikation und Information in Fortbildungsangelegenheiten zu erledigen.

Ich habe IFOS-Bund im November 2002 kontrolliert. Meine dabei geäußerten Anregungen und Empfehlungen hinsichtlich der Gestaltung des Anfrageformulars und der

Speicherdauer der Formulardaten wurden von der BAköV in das System eingearbeitet. Als besonderes positiv habe ich folgende Systemeinstellungen bewertet:

– Die Zugriffsberechtigungen der Mitarbeiter der BAköV, insbesondere auf die Daten der Teilnehmer, sind stark eingegrenzt.

– Alle bearbeitenden Zugriffe werden protokolliert und können so nachvollzogen werden.

Mittelfristig soll das System IFOS-Bund zu einer „**virtuellen Lernplattform**“ ausgebaut werden. Bereits jetzt stellt das System Lerninhalte webbasiert zur Verfügung. Allerdings wurden notwenige Zusatzfunktionen, beispielsweise die Einrichtung von veranstaltungsbegleitenden oder veranstaltungsunabhängigen Foren und Chaträumen oder die Nutzung eines sog. Persönlichen Schreibtisches in einer E-Learning-Umgebung, noch nicht in das System implementiert.

Die Lernplattform soll unterteilt werden in einen öffentlich-zugänglichen Bereich, einen geschützten und einen besonders geschützten Bereich, in dem der Zugang ausschließlich durch die Fortbildungsverantwortlichen in den Behörden erfolgen kann. Der Zugang soll sowohl über die Lernplattform selbst als auch über IFOS-Bund möglich sein.

Im Januar 2005 beginnt ein einjähriger Probebetrieb. Dabei sind vor allem die Funktionalitäten zur Bearbeitung der personenbezogenen Angaben bei der Benutzerkennung, bei der Erwartungsabfrage vor dem Seminar, bei der Abgabe von Arbeitsproben, bei der Überprüfung von Zugriffsberechtigungen, bei der Speicherung der Anmeldedaten und bei den Löschungsfristen von datenschutzrechtlichem Interesse. Da es sich bei der Lernplattform um einen Teledienst handelt, müssen insbesondere die Regelungen des Teledienstedatenschutzgesetzes beachtet werden.

Ich werde den Praxistest und die Weiterentwicklung des Gesamtsystems weiter begleiten.

6.6 Personenkennziffer im Melderecht

Im Meldewesen sind datenschutzrechtlich problematische Entwicklungen festzustellen.

Wiederholt stellte ich fest, dass der datenschutzrechtliche Standard des Melderechtsrahmengesetzes (MRRG) wenig befriedigend ist (zuletzt 19. TB Nr. 7.3). Die Situation hat sich im Berichtszeitraum noch verschlechtert, weil aus den unterschiedlichsten Gründen Änderungen im Melderecht vorgenommen wurden, um zusätzliche Wünsche an Meldedaten zu befriedigen. So wird über das Steuerrecht praktisch ein zentrales Melderegister eingeführt. Zudem sollen sowohl in den kommunalen Melderegistern als auch in dem Zentralregister einheitliche steuerliche Identifikationsnummern gespeichert werden. Es muss verhindert werden, dass sich hieraus eine vom Bundesverfassungsgericht in seinem Volkszählungsurteil abgelehnte Personenkennziffer (vgl. Nr. 8.2) entwickelt.

Gleichzeitig gibt es verstärkten Informationsbedarf zwischen Waffen- und Meldebehörden aufgrund der Neuregelung des Waffenrechtes. Zu Aufregung führten auch Wählerpotenzialanalysen, für die Wahlforschungsinstitute Meldedaten nutzten, um Aussagen über die politischen Präferenzen der Wahlberechtigten zu gewinnen. Ich vertrete hierzu die Auffassung, dass aufgrund der engen Zweckbindung des § 22 MRRG ein Abgleich der nur für Wahlwerbezwecke den Parteien übermittelten Meldedaten mit anderen Daten unzulässig ist. Aufmerksam beobachte ich ferner die Entwicklungen im eGovernment mit elektronischen Abfragen und Abgleichen und den Bestrebungen um eine grenzüberschreitende europaweite Melderegisterauskunft.

6.7 Personenstandsgesetz – Ahnenforschung

Die Ahnenforschung soll durch eine Reform des Personenstandsrechts erleichtert werden.

Das Ziel der vom BMI seit langem geplanten Reform des Personenstandsgesetzes ist es, die immer beliebter werdende Ahnenforschung zu erleichtern. Die Ahnenforscher stoßen nicht selten auf Schwierigkeiten, weil die Nutzung der staatlichen Personenstandsbücher denselben strengen Regeln unterworfen ist, wie die Verwendung aktueller Beurkundungen. Die Nutzung kann nur von Personen verlangt werden, auf die sich der Eintrag bezieht sowie von deren Ehegatten, Vorfahren und Abkömmlingen. Andere Personen (z. B. Verwandte der Seitenlinie) haben nur dann ein Benutzungsrecht, wenn sie „ein rechtliches Interesse glaubhaft machen“, was für die Ahnenforschung nach allgemeiner Rechtsauffassung verneint wird, da ihr nur ein berechtigtes Interesse zugestanden wird. Mich erreichen deshalb viele Eingaben von Familienforschern, die fälschlich annehmen, dass der Datenschutz diese strenge Regelung erfordert. In Anlehnung an einen von mir vor geraumer Zeit unterbreiteten Vorschlag ist nunmehr seitens des BMI daran gedacht, die Benutzung schon bei berechtigtem Interesse zuzulassen, wenn die Betroffenen seit mindestens 30 Jahren verstorben sind oder – sollte der Todestag nicht bekannt sein – wenn deren Geburtsdatum mindestens 110 Jahre zurückliegt.

Weitere Schwerpunkte der vorgesehenen Reform sind die Einführung elektronischer Personenstandsregister, die Abschaffung des Familienbuchs und die Reduzierung der Beurkundungsdaten. Das BMI hat angekündigt, einen entsprechenden Änderungsentwurf 2005 vorzulegen.

6.8 Staatsangehörigkeitsdatei

Endlich gibt es konkrete Hoffnungen auf die Schaffung einer Rechtsgrundlage für die Staatsangehörigkeitsdatei des Bundesverwaltungsamtes (BVA).

Ich habe bereits in früheren Tätigkeitsberichten (16. bis 19. TB vgl. dort zuletzt Nr. 7.7) darauf hingewiesen, dass beim BVA seit 1982 eine Datei zum Nachweis der Staatsangehörigkeit (Staatsangehörigkeitsdatei – STADA) ohne ausreichende Rechtsgrundlage geführt wird. Nach mehreren vergeblichen Anläufen wurde zur Schaffung der

erforderlichen Rechtsgrundlage bei dem federführend zuständigen BMI eine Arbeitsgruppe eingerichtet, die in Abstimmung mit den Ländern entsprechende Vorschläge für bereichsspezifische datenschutzrechtliche Regelungen im Staatsangehörigkeitsrecht erarbeitet hat. Diese sollen – neben anderen Regelungen – in den Referentenentwurf eines weiteren „Gesetzes zur Änderung des Aufenthaltsgesetzes und anderer Gesetze“ Eingang finden. Der Referentenentwurf soll im Frühjahr 2005 in die Ressortabstimmung gehen, so dass die Änderung hoffentlich im Herbst 2005 in Kraft treten kann und die STADA dann endlich eine Rechtsgrundlage hat.

6.9 Richtlinie der Bundesregierung zur Korruptionsprävention

Die Richtlinie zur Korruptionsprävention in der Bundesverwaltung wurde 2004 neu gefasst.

Zur Verbesserung der Korruptionsprävention wurde die Richtlinie zur Korruptionsprävention in der Bundesverwaltung 2004 neu gefasst (BAnz Nr. 148 S. 17745). Problematisch war vor allem die Nutzung von Daten aus Sicherheitsüberprüfungen für die Korruptionsprävention.

Eine Nutzung der im Rahmen einer Sicherheitsüberprüfung erhobenen Daten für andere Zwecke ist nur nach Maßgabe des § 21 Sicherheitsüberprüfungsgesetz (SÜG) zulässig, wobei der Gesetzgeber eine strenge Zweckbindung vorgesehen hat. Ich habe mich gegen die Überlegung gewandt, § 21 SÜG dahingehend zu erweitern, die im Rahmen einer Sicherheitsüberprüfung erhobenen Daten auch für Zwecke der Korruptionsprävention zu nutzen. Die in § 21 Abs. 1 Nr. 2 SÜG normierte Beschränkung auf den Bereich der Repression ist durch keine Form der Auslegung dieser Norm zu relativieren. Insoweit wäre eine Novellierung des SÜG erforderlich gewesen.

Auch nach den vorliegenden Erkenntnissen sind die Ergebnisse einer Sicherheitsüberprüfung im Hinblick auf die Korruptionsprävention nicht einschlägig. Es ist auch kein Fall bekannt, in dem eine Personalunion zwischen der Ansprechperson für Korruptionsprävention und dem Sicherheitsbeauftragten verhindert hätte, dass eine ungeeignete Person in einem besonders korruptionsgefährdeten Bereich eingesetzt wurde.

Ich begrüße deshalb die ausdrückliche Klarstellung in der Empfehlung zu Nr. 5 der Richtlinie, dass zur Ansprechperson nicht bestellt werden kann, wer der für Sicherheitsüberprüfungen zuständigen Organisationseinheit angehört.

6.10 Flexibilisierung der amtlichen Statistik

Aus Sicht der Statistiker wäre die Nutzung von Verwaltungsdaten hilfreich, da dies die Erhebungskosten senken könnte. Ein generelles Zugangsrecht der Statistik zu Verwaltungsregistern begegnet aber erheblichen rechtlichen Bedenken.

Im Berichtszeitraum sind aus dem Bereich der amtlichen Statistik Wünsche laut geworden, in verstärktem Umfang bereits vorhandene Verwaltungsregister zu nutzen. Eine solche Flexibilisierung führe zu einer nennenswerten Entlastung der Wirtschaft, da anstelle der Befragung der Betroffenen *nur* die Verwaltung eingebunden werde.

Die Nutzung von Verwaltungsregistern ist kein datenschutzrechtliches Tabu-Thema, denn bereits heute werden Verwaltungsdaten bei mehr als 40 Prozent der Erhebungen genutzt. Dieser „Vereinfachungsweg“ – anstelle der Betroffenen die Verwaltung zu befragen – darf aber nicht zu Beeinträchtigungen auf Seiten der Betroffenen führen. Unter datenschutzrechtlichen Aspekten macht es nämlich keinen großen Unterschied, ob der Bürger direkt und mit Auskunftszwang befragt wird oder ob die Daten, ohne den Betroffenen im Einzelfall zu informieren, durch Rückgriff auf vorhandene Verwaltungsdaten besorgt werden. Amtliche Statistik mit Auskunftszwang ist Eingriffsverwaltung. Und Eingriffe des Staates in die Verhältnisse seiner Bürger bedürfen einer gesetzlichen Legitimation. Unter diesem Gesetzesvorbehalt steht auch ein allgemeines Zugangsrecht der Statistik zu Verwaltungsregistern. Insbesondere, wenn es sich um eine pauschale gesetzliche Regelung handelt, welche die mit einer Auskunftspflicht verbundenen Erhebungen bei Betroffenen ersetzen soll. Ein Zwang zur Angabe personenbezogener Daten setzt voraus, dass der Gesetzgeber den Verwendungszweck bereichsspezifisch und präzise bestimmt und die Angaben für diesen Zweck geeignet und erforderlich sein müssen. Zwar kann für statistische Zwecke eine enge und konkrete Zweckbindung der Daten nicht verlangt werden, zum Ausgleich dafür müssen aber der Informationserhebung und -verarbeitung entsprechende Schranken gegenüberstehen.

Die bisherige Vorgehensweise, gesetzlich festzulegen, welche Daten für welche Auswertungen benötigt werden und woher die Daten kommen sollen, hat sich in der Praxis durchaus bewährt.

Ein vom damaligen Bundesministerium für Wirtschaft und Technologie in Auftrag gegebenes Gutachten des Instituts für Angewandte Wirtschaftsforschung von 1999 hat sich mit genau dieser Fragestellung auseinandergesetzt. Die Registerinventur, in die „alle irgendwie brauchbar erscheinenden Register“ einbezogen wurden, ergab, dass letztendlich nur drei bis vier Register für eine Substitution tauglich erscheinen, und zwar die Betriebs- und Versichertendatei der Bundesagentur für Arbeit, die Dateien der Finanzverwaltung, Dateien kommunaler Ämter für öffentliche Ordnung/Gewerbeämter sowie Dateien der Industrie- und Handelskammer und Handwerkskammern. Selbst bei diesen Registern seien mehr oder weniger umfangreiche EDV-Änderungen und sog. Trimmungen – das sind inhaltliche Veränderungen der Register, damit sie den statistischen Erfordernissen genügen – erforderlich. Ein allgemeines Zugangsrecht zu Verwaltungsregistern könnte daher nur dann nützlich sein, wenn der Statistik zugleich das Recht eingeräumt würde, die Verwaltungsregister auf die statistischen Belange inhaltlich und organisatorisch auszurichten und trotz föderaler Verwaltungshoheit die Vereinheitlichung von kommunalen und Länderregistern vorzuschreiben.

Insofern scheint nicht ein fehlendes allgemeines Zugangsrecht der Statistik das Problem, sondern die nicht vorhandenen gebrauchsfertigen Verwaltungsregister.

Ich sehe somit für die Schaffung eines generellen gesetzlichen Zugangsrechts der Statistik zu Verwaltungsdaten weder eine verfassungsgemäße Möglichkeit, noch eine praktikable Verbesserung der Situation. Aus meiner Sicht kann und sollte jedoch darüber diskutiert werden, inwieweit künftig ein Stammdatensatz pro Unternehmen, der für verschiedene Statistiken herangezogen werden kann, Erleichterungen bringt. Diskutabel ist ferner die Rückmeldung plausibilisierter Daten in Einzelfällen (z. B. Anschrift, Rechtsform, Wirtschaftszweig, Organzugehörigkeit) und die Zusammenarbeit mit der Verwaltung bei der Gestaltung der Verwaltungsregister.

Der Datenschutz ist kein unüberwindbares Hindernis für die Verwendung von Verwaltungsdaten für Wirtschaftsstatistiken. Deshalb bin ich sicher, dass sich vertretbare Lösungen finden lassen werden.

6.11 Mikrozensusgesetz – was gibt es Neues?

Durch das Mikrozensusgesetz 2005 werden nicht mehr alle Erhebungsmerkmale im Gesetz selbst, sondern durch eine Rechtsverordnung festgelegt.

Die Grundidee des Mikrozensus ist, mit einer Auswahl der Bevölkerung nach mathematisch-statistischen Verfahren ein annähernd wirklichkeitsgetreues Abbild der gesamten Bevölkerung darzustellen. Die Ergebnisse bilden eine Grundlage für politische Entscheidungen, z. B. im Bereich der Arbeits-, Sozial-, Familien-, Gesundheits- oder Bildungspolitik; sie finden Eingang in Regierungsberichte, in das Jahresgutachten des Sachverständigenrates zur Begutachtung der gesamtwirtschaftlichen Entwicklung und stehen Wissenschaft und Forschung zur Verfügung.

Das Mikrozensusgesetz 2005 (MZG) ist – wie seine Vorgänger – zeitlich befristet und gilt für acht Jahre, um den Erhebungsbedarf überprüfen und gegebenenfalls anpassen zu können. Nachdem im Mikrozensusgesetz 1996 den Anregungen des BfD Rechnung getragen worden war (vgl. 16. TB Nr. 30.4), habe ich mich auf die Änderungen dieses Gesetzes konzentriert. Die entscheidende Veränderung besteht darin, nicht mehr sämtliche Einzelfragen (Erhebungsmerkmale) im Gesetz selbst zu regeln, sondern die Regelung auf Fragenkomplexe zu beschränken, aus denen dann die konkreten Fragen entwickelt und im Wege einer Rechtsverordnung gesetzlich festgelegt werden können. So kann z. B. das im MZG formulierte Merkmal „Art, Anlass und Dauer der Arbeitssuche“ zu mehreren Fragen führen: Einerseits nach dem Grund (z. B. Entlassung, eigene Kündigung und freiwillige Unterbrechung) und andererseits nach der Tätigkeit (z. B. Selbständiger, Arbeitnehmer und Voll- oder Teilzeit). Ich habe dabei geprüft, ob die gewählten Umschreibungen dem Gebot der Normenklarheit entsprechen, d. h. ob die Fragenkomplexe hinreichend deutlich Inhalt und Umfang der Erhebungsmerkmale bestimmen. Da der Fragebogen aber erst im Zusammenhang mit der späteren Rechtsverordnung entwickelt werden soll, wird sich meine Prüfung bei jeder konkreten Fragestellung fortsetzen. Die Umstellung wurde gewählt, um eine größere Flexibilität für statistische Erhebungen zu erreichen, indem neue Fragestellungen einbezogen oder andere nuanciert werden können, ohne das Gesetz selbst ändern zu müssen. Die Auskunftspflicht der Befragten besteht für die meisten Daten fort. Die zur freiwilligen Beantwortung stehenden Fragen wurden mit ganz geringen Ausnahmen (z. B. fehlende Antworten zum Schulabschluss mit der Folge mangelnder Aussagefähigkeit, daher jetzt Auskunftspflicht) beibehalten.

Ich habe deshalb noch einmal die generelle Auskunftspflicht der Befragten zur Diskussion gestellt und nach Alternativen mit geringerem Eingriffcharakter für den Bürger gefragt. Die Statistiker haben eingewandt, dass bei einer 1 Prozent Stichprobe die Datenbasis zu gering sei, um Ausfälle durch eine Beantwortungsquote, die unter 50 Prozent liegen würde, aufzufangen. Man sei aber bemüht, dem Grundrecht auf informationelle Selbstbestimmung Rechnung zu tragen, indem Fragen nach sensiblen Daten weitgehend der freiwilligen Auskunft überlassen seien. Gleichwohl habe ich auf die vom Bundesverfassungsgericht angemahnte Methodendiskussion hingewiesen, die sich auch auf Stichprobenerhebungen und Entwicklungen sozialwissenschaftlicher Hochrechnungsverfahren erstreckt. Weitere Neuerungen betreffen eher technisch-organisatorische Maßnahmen. Ich werde mich an der weiteren Konkretisierung des Fragenprogramms im Rahmen der zu erlassenden Rechtsverordnung beteiligen.

6.12 Volkszählungstest – Beginn eines neuen Zeitalters?

Bei künftigen Volkszählungen könnte möglicherweise auf aufwändige Befragungen aller Einwohner verzichtet werden. In den letzten Jahren wurde getestet, ob Dateien der Verwaltung geeignet sind, zu gleichen Ergebnissen zu gelangen.

Auf der Grundlage des Zensustestgesetzes vom 27. Juli 2001 (vgl. 19. TB Nr. 7.9) haben die Statistischen Ämter des Bundes und der Länder Tests zur Erprobung eines registergestützten Zensusverfahrens durchgeführt, deren erste Ergebnisse nun vorliegen. Dabei wurde ein Alternativkonzept getestet, das anstelle der herkömmlichen Volkszählung – soweit möglich – die Nutzung vorhandener Verwaltungsregister, insbesondere der Melderegister und Dateien der Bundesagentur für Arbeit (BA), vorsieht. Gegenstand des Tests waren: Die Qualität der Melderegister und der Dateien der BA, die Verfahren zur statistischen Bereinigung der Melderegisterdaten und der Zusammenführung der verschiedenen Daten sowie das Verfahren zur Generierung von Haushaltszusammenhängen. Dazu wurden zu einem bestimmten Stichtag Daten aus den Melderegistern und den Dateien der BA für ausgewählte Gemeinden und Gebäude an die Statistischen

Ämter übermittelt sowie eine Gebäude- und Wohnungsstichprobe bei den Eigentümern der ausgewählten Gebäude durchgeführt. Ferner wurde eine Befragung bei den Bewohnern durchgeführt und deren Angaben mit den Registerdaten verglichen.

Der Zensustest hat nach Einschätzung des BMI ergeben, dass ein registergestützter Zensus möglich ist und die getesteten statistischen Methoden und Verfahren geeignet erscheinen. Die Registernutzung müsse jedoch durch primärstatistische Elemente ergänzt werden. Insbesondere müssten die Melderegisterdaten als Grundlage belastbarer amtlicher Einwohnerzahlen überprüft und gegebenenfalls korrigiert werden, wozu Stichprobenerhebungen vorgesehen seien. Vor dem Hintergrund der für das Jahr 2010 durch die EU geplanten gemeinschaftsweiten Zensusrunde könnte das neue Verfahren zu diesem Zeitpunkt zur Anwendung kommen. Ich werde die weiteren Vorbereitungsmaßnahmen aufmerksam begleiten und dabei insbesondere darauf achten, dass – entsprechend der Entscheidung des Bundesverfassungsgerichts in seinem Volkszählungsurteil vom 15. Dezember 1983 (BVerfGE 65, 1 ff.) – keine für die Statistik erhobenen Daten für Verwaltungszwecke genutzt werden, also eine unzulässige Zweckänderung vermieden wird.

6.13 Archivbestände und ihre objektive Wahrheit

Archivbestände können auch Unterlagen enthalten, die nicht der objektiven Wahrheit entsprechen. Betroffene haben in diesen Fällen die Möglichkeit, eine eigene Darstellung zu den Archivalien hinzuzufügen.

Ein Petent teilte mir mit, dass er beim Bundesarchiv in der NSDAP-Mitgliederkartei als Mitglied gespeichert sei. Tatsächlich sei er jedoch zu keinem Zeitpunkt Mitglied der NSDAP gewesen; zum Zeitpunkt des angeblichen Beitritts sei er noch nicht volljährig gewesen, so dass er bereits aus diesem Grund nicht Mitglied der NSDAP hätte werden können. Das Bundesarchiv lehnte einen Antrag des Petenten auf Löschung ab.

Das Recht auf informationelle Selbstbestimmung verleiht dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung personenbezogener Daten zu entscheiden. Das Bundesarchivgesetz enthält in § 4 Abs. 3 eine Regelung, die diesem Schutzzweck Rechnung tragen will. Dort heißt es: *Wird festgestellt, dass personenbezogene Angaben unrichtig sind, so ist dies in den Unterlagen zu vermerken oder auf sonstige Weise festzuhalten. Bestreitet ein Betroffener die Richtigkeit personenbezogener Angaben, so ist ihm die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.* Vor diesem Hintergrund hat das Bundesarchiv eine Gegendarstellung des Petenten zu den Unterlagen genommen. Mit diesem Verfahren war der Petent jedoch nicht einverstanden, er beharrte vielmehr auf der Löschung der fehlerhaften Angaben.

Ich habe zwar einerseits großes Verständnis für den Ärger des Petenten, verstehe aber andererseits auch die Intention des Gesetzgebers. Das Problem liegt darin, dass es gerade zu den Aufgaben des Archivs zählt, Situationen und Lebenssachverhalte so zu dokumentieren, wie sie sich aufgrund der archivierten Aufzeichnungen darstellen. Wenn das Handeln von Stellen der NSDAP fehlerhaft war und innerhalb des nationalsozialistischen Gewaltsystems rechtswidrige Merkmale aufwies, dann ist gerade die Aufbewahrung derartiger Unterlagen als Beleg solchen Handelns unverzichtbar. Auch die Regelung in § 4 Abs. 3 BArchG verfolgt denselben Zweck, da durch die Hinzufügung der Gegendarstellung die Nachvollziehbarkeit und Offenlegung des fehlerhaften Handelns belegt wird. Der damit einhergehende Eingriff in das Recht auf informationelle Selbstbestimmung ist bei Abwägung der unterschiedlichen Rechtsgüter hinzunehmen. Zum Schutz der Persönlichkeitsrechte werden solche Unterlagen nicht in Bibliotheken mit freiem Zugang aufbewahrt, sondern in Archiven, wo sie nur unter besonderen Voraussetzungen eingesehen werden dürfen. So darf beispielsweise Archivgut, das sich auf natürliche Personen bezieht, grundsätzlich erst 30 Jahre nach dem Tod der Betroffenen durch Dritte genutzt werden. Diese Schutzfrist kann verkürzt werden, wenn die Nutzung für ein wissenschaftliches Forschungsvorhaben unerlässlich ist und schutzwürdige Belange der Betroffenen angemessene Berücksichtigung finden. Eine Veröffentlichung oder eine andere Form der Bekanntgabe in personenbezogener Form ist archivrechtlich und datenschutzrechtlich unzulässig. Auch wenn es für den Petenten im konkreten Einzelfall unbefriedigend ist, so halte ich die gesetzliche Regelung im BArchG für angemessen.

7 Rechtswesen

7.1 Akustische Wohnraumüberwachung

Zu den wichtigsten Ereignissen im Berichtszeitraum zählt das Urteil des Bundesverfassungsgerichts vom 3. März 2004 zur akustischen Wohnraumüberwachung.

7.1.1 Urteil des Bundesverfassungsgerichts vom 3. März 2004

Das Urteil des Bundesverfassungsgerichts zum „Großen Lauschangriff“ ist ein wichtiger Orientierungspunkt bei der Abwägung zwischen den Belangen der inneren Sicherheit und den Rechten des Einzelnen.

In seinem richtungsweisenden Urteil hat das BVerfG deutliche Grenzen für das heimliche Abhören von Wohnungen mit akustischen Hilfsmitteln gesetzt (vgl. Kasten zu Nr. 7.1.1). Eine Minderheit des Senats hat den Artikel 13 Abs. 3 GG, der die verfassungsrechtliche Grundlage der Wohnraumüberwachung darstellt, als „verfassungswidriges Verfassungsrecht“ gewertet. Nach der Meinung der Senatsmehrheit muss Artikel 13 Abs. 3 GG restriktiv und in einer an der Menschenwürde orientierten Weise interpretiert werden. Es muss sichergestellt sein, dass die akustische Wohnraumüberwachung nicht in den unantastbaren Bereich der privaten Lebensgestaltung eindringt. Die Fortentwicklung dieses in ständiger Recht-

sprechung herausgearbeiteten und aus der Menschwürde abgeleiteten Begriffs bildet in meinen Augen den Schwerpunkt des Urteils. In diesen Kernbereich darf die Überwachung auch nicht im Interesse der Strafverfolgung eingreifen. Dies bedeutet, dass heimliches Abhören zu unterbleiben hat, wenn sich eine Person allein oder ausschließlich mit Personen in der Wohnung aufhält, zu denen sie in einem besonderen, diesen Kernbereich betreffenden Vertrauensverhältnis steht und keine konkreten Anhaltspunkte dafür bestehen, dass die zu erwartenden Gespräche einen unmittelbaren Straftatbezug aufweisen. Gemeint sind Familienangehörige oder sonstige enge Vertraute, also auch persönliche Freunde. Der Schutz des Kernbereichs schließt daher jede Überwachung rund um die Uhr und auch eine durchgängige automatische Aufzeichnung aus.

Die akustische Wohnraumüberwachung kann im Übrigen nur dann gerechtfertigt sein, wenn es um die Aufklärung besonders schwerer Straftaten geht. Der mit § 100c Abs. 1 Nr. 3 Strafprozessordnung (StPO) 1998 eingeführte Straftatenkatalog geht nach den Feststellungen des Gerichts weit über den zulässigen Rahmen hinaus. So nennt er bereits zahlreiche Vergehen, teilweise ohne Mindeststrafe, als Voraussetzung für die Anordnung eines großen Lauschangriffs. Von einer besonderen Schwere der Tat im Sinne des Artikel 13 Abs. 3 GG ist aber nur dann auszugehen, wenn die Höchststrafe mindestens fünf Jahre beträgt.

Mit begrüßenswerter Deutlichkeit hat das BVerfG auch die nur mangelhafte Berücksichtigung der Aussage- und Zeugnisverweigerungsrechte gerügt. So müssen die gesetzlichen Regelungen das Abhören und Aufzeichnen untersagen, wenn absolut geschützte Gespräche erfasst werden sollen. § 100d Abs. 3 StPO genügt dem nicht, da für Zeugnisverweigerungsberechtigte, zu denen insbesondere die engsten Familienangehörigen gehören, in der Vorschrift kein generelles Überwachungsverbot, sondern nur ein Beweisverwertungsverbot vorgesehen ist und für Gespräche mit sonstigen engsten Vertrauten keinerlei Einschränkungen bestehen. Zudem fehlt es auch an einer Löschungsverpflichtung für solcher Art erlangte Daten.

Bedeutsam ist auch die Forderung des Gerichts, dass nach einem Lauschangriff grundsätzlich sämtliche von dieser Maßnahme betroffenen Personen zu unterrichten sind, da nur so der gerichtliche Rechtsschutz garantiert werden kann.

Darüber hinaus betreffen das Urteil zur akustischen Wohnraumüberwachung und der ebenfalls am 3. März 2004 verkündete Beschluss zur Post- und Telefonüberwachung nach dem Außenwirtschaftsgesetz (vgl. Nr. 5.4.3) wichtige Vorschriften der StPO, mit denen die Telefonüberwachung geregelt wird. Auf den Prüfstand gehören deshalb auch weitere Eingriffsbefugnisse insbesondere zur verdeckten Datenerhebung mit zwangsläufigen Berührungen zum Bereich privater Lebensgestaltung, wie etwa die längerfristige Observation, der verdeckte Einsatz technischer Mittel, der Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern. Hiervon betroffen sind nicht nur Bundesgesetze, sondern beispielsweise auch die Polizei- und Verfassungsschutzgesetze der Länder. Auch wenn diese Gesetze nicht ausdrücklich in dem Urteil erwähnt sind, weil sie nicht Gegenstand des Verfahrens waren, strahlen doch die in dem Urteil zum Ausdruck kommende Wertentscheidung und die maßgebliche Argumentation des Gerichts auf diese Eingriffsbefugnisse aus (vgl. Nr. 5.1.2).

Kasten zu Nr. 7.1.1

BVerfG – Urteil vom 3. März 2004

Leitsätze:

1. Artikel 13 Abs. 3 GG in der Fassung des Gesetzes zur Änderung des Grundgesetzes (Artikel 13) vom 26. März 1998 (BGBl. I S. 610) ist mit Artikel 79 Abs. 3 GG vereinbar.
2. Zur Unantastbarkeit der Menschenwürde gemäß Artikel 1 Abs. 1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung. In diesen Bereich darf die akustische Überwachung von Wohnraum zu Zwecken der Strafverfolgung (Artikel 13 Abs. 3 GG) nicht eingreifen. Eine Abwägung nach Maßgabe des Verhältnismäßigkeitsgrundsatzes zwischen der Unverletzlichkeit der Wohnung (Artikel 13 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG) und dem Strafverfolgungsinteresse findet insoweit nicht statt.
3. Nicht jede akustische Überwachung von Wohnraum verletzt den Menschenwürdegehalt des Artikel 13 Abs. 1 GG.
4. Die auf die Überwachung von Wohnraum gerichtete gesetzliche Ermächtigung muss Sicherungen der Unantastbarkeit der Menschenwürde enthalten sowie den tatbestandlichen Anforderungen des Artikel 13 Abs. 3 GG und den übrigen Vorgaben der Verfassung entsprechen.
5. Führt die auf eine solche Ermächtigung gestützte akustische Wohnraumüberwachung gleichwohl zur Erhebung von Informationen aus dem absolut geschützten Kernbereich privater Lebensgestaltung, muss sie abgebrochen werden und Aufzeichnungen müssen gelöscht werden; jede Verwertung solcher Informationen ist ausgeschlossen.
6. Die Vorschriften der Strafprozessordnung zur Durchführung der akustischen Überwachung von Wohnraum zu Zwecken der Strafverfolgung genügen den verfassungsrechtlichen Anforderungen im Hinblick auf den Schutz der Menschenwürde (Artikel 1 Abs. 1 GG), den vom Rechtsstaatsprinzip umfassten Grundsatz der Verhältnismäßigkeit, die Gewährung effektiven Rechtsschutzes (Artikel 19 Abs. 4 GG) und den Anspruch auf rechtliches Gehör (Artikel 103 Abs. 1 GG) nicht in vollem Umfang.

7.1.2 Neuregelung der akustischen Wohnraumüberwachung

Der Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung ließ zunächst wichtige Forderungen unberücksichtigt.

Das BMJ hat im Juni 2004 einen Gesetzentwurf zur Abstimmung vorgelegt, in dem die beanstandeten Regelungen überarbeitet worden waren. Die Neuregelung beschränkt sich allein auf die akustische Wohnraumüberwachung in der StPO und lässt andere Befugnisse, insbesondere zu verdeckten Ermittlungsmaßnahmen, bei denen auf Grund der BVerfG-Entscheidung ebenfalls Reformbedarf besteht, außer Acht. In einem Gespräch mit der Bundesministerin der Justiz habe ich auf den weiteren Reformbedarf hingewiesen, der bezüglich der StPO vor allem die Überwachung der Telekommunikation nach den §§ 100a ff. StPO betrifft, aber auch andere Formen der verdeckten Datenerhebung mit zwangsläufiger Berührung der privaten Lebensgestaltung, wie etwa die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz von Vertrauenspersonen oder von verdeckten Ermittlern umfasst (vgl. hierzu auch die Entschließungen der Datenschutzbeauftragten des Bundes und der Länder, Kasten zu Nr. 5.1.2, 7.1.2).

Darüber hinaus enthielt der erste Entwurf vom Juni 2004 insbesondere zwei kritische Punkte:

– Die Möglichkeit, Gespräche mit Ärzten, Psychologen, Rechtsanwälten, Journalisten oder Seelsorgern abzuhören, sollten nicht etwa eingeschränkt, sondern erweitert werden. Ein absoluter Schutz vor Abhörmaßnahmen sollte nur noch für Gespräche mit Strafverteidigern im Rahmen ihres Mandats sowie für Beichtgespräche mit Seelsorgern gelten. Bei den übrigen Berufsgeheimnisträgern enthielt der Referentenentwurf lediglich eine Abwägungsklausel. Dagegen ist bereits nach geltendem Recht durch Verweis auf § 53 StPO sichergestellt, dass wenigstens Gespräche mit Berufsgeheimnisträgern auch bei akustischer Wohnraumüberwachung weitgehend geschützt werden.

– In den Straftatenkatalog des § 100c Abs. 1 Nr. 3 StPO dürfen nach Vorgabe des BVerfG nur Straftaten mit einer Höchststrafe von mehr als fünf Jahren aufgenommen werden. Offenbar um in erster Linie diesem Maßstab zu genügen, sollte die Bildung krimineller Vereinigung in einem besonders schweren Fall (§ 129 Abs. 4 Strafgesetzbuch) statt mit bisher fünf Jahren künftig mit bis zu zehn Jahren Freiheitsstrafe bedroht werden.

Diese beiden Punkte wurden in den von der Bundesregierung im September 2004 beschlossenen Entwurf nicht übernommen. Darüber hinaus wurden auch einige weitere von mir angeregte Änderungen berücksichtigt. Allerdings erfolgte keine klare Definition des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und auch der Kreis der Menschen „des persönlichen Vertrauens“ blieb offen.

Kasten zu Nr. 7.1.2

68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. Und 29. Oktober 2004 in Saarbrücken

Entschließung:
Gesetzentwurf der Bundesregierung zur Neuregelung der akustischen Wohnraumüberwachung

Die Bundesregierung hat einen Gesetzentwurf zur Neuregelung der akustischen Wohnraumüberwachung vorgelegt. Sie setzt damit in großen Teilen das Urteil des Bundesverfassungsgerichts vom 3. März 2004 um, wonach die Vorschriften der Strafprozessordnung zum „großen Lauschangriff“ in wesentlichen Teilen verfassungswidrig sind. Allerdings sind zentrale Punkte, wie die Begriffsbestimmung des „unantastbaren Kernbereichs der privaten Lebensgestaltung“ und die Bestimmung des Kreises der Menschen „des persönlichen Vertrauens“ offen geblieben.

Ungeachtet dessen drohen im weiteren Verlauf des Gesetzgebungsverfahrens schwerwiegende Verschlechterungen: So wird diskutiert, die Vorgaben des Bundesverfassungsgerichts dadurch zu unterlaufen, dass auch bei erkannten Eingriffen in den absolut geschützten Kernbereich die technische Aufzeichnung fortgesetzt wird. Dies steht in eklatantem Widerspruch zur eindeutigen Vorgabe des Bundesverfassungsgerichts, die Aufzeichnung in derartigen Fällen sofort zu beenden. Darüber hinaus wird versucht, den Anwendungsbereich der akustischen Wohnraumüberwachung dadurch auszuweiten, dass auch nicht strafbare Vorbereitungshandlungen einbezogen werden. Auch dies widerspricht den verfassungsgerichtlichen Vorgaben und verwischt die Grenzen zwischen Strafverfolgung und Gefahrenabwehr.

Die Datenschutzbeauftragten bekräftigen im Übrigen ihre Forderung, dass es im Hinblick auf die Heimlichkeit der Überwachung und ihrer zwangsläufigen Berührung mit dem Kernbereich privater Lebensgestaltung erforderlich ist, alle Formen der verdeckten Datenerhebung an den Maßstäben der verfassungsgerichtlichen Entscheidung vom 3. März 2004 zu messen und auszurichten sowie die einschlägigen gesetzlichen Befugnisregelungen des Bundes und der Länder auf den Prüfstand zu stellen und ggf. neu zu fassen. Dies gilt etwa für die präventive Telekommunikationsüberwachung, die längerfristige Observation, den verdeckten Einsatz technischer Mittel, den Einsatz nachrichtendienstlicher Mittel und von verdeckten Ermittlern. Dabei sind insbesondere Regelungen zum Schutz des Kernbereichs privater Lebensgestaltung und zum Schutz vertraulicher Kommunikation mit engsten Familienangehörigen und anderen engsten Vertrauten sowie mit Personen, die einem Berufsgeheimnis unterliegen, zur Einhaltung der Zweckbindung bei Weiterverwendung der durch die Eingriffsmaßnahmen erlangten Daten, zu der dazu erforderlichen Kennzeichnungspflicht und zur Benachrichtigung aller von der Eingriffsmaßnahme Betroffenen sowie zur detaillierten Ausgestaltung von Berichtspflichten gegenüber den Parlamenten vorzusehen.

Positiv bewerte ich, dass der Entwurf eine besondere qualifizierte Begründungspflicht für die Anordnung oder Verlängerung der Maßnahme sowie einen detaillierten Katalog von Kriterien für die Berichte an die obersten Justizbehörden, die Bundesregierung und den Deutschen Bundestag vorsieht, vor allem die Vorgabe, alle von der Überwachungsmaßnahme betroffenen Personen in den Berichten aufzuführen.

Der Bundesrat hat zu dem Entwurf der Bundesregierung im November 2004 Stellung genommen. Danach soll etwa die technische Aufzeichnung fortgesetzt werden können, selbst wenn Eingriffe in den absolut geschützten Kernbereich festgestellt wurden, um danach erst über deren weitere Verwendung zu entscheiden. Außerdem sollen nach Auffassung des Bundesrates auch nicht strafbare Vorbereitungshandlungen in den Straftatenkatalog des § 100c Abs. 1 Nr. 3 StPO aufgenommen werden. Beides widerspricht den verfassungsgerichtlichen Vorgaben. Ich begrüße es, dass die Bundesregierung in ihrer Gegenäußerung den Vorschlägen des Bundesrates nicht zugestimmt hat (Bundestagsdrucksache 15/4533). Im Rechtsausschuss des Deutschen Bundestages habe ich mich zu dem Gesetzentwurf geäußert. Dabei habe ich darauf gedrängt, dass die Ergebnisse des am 1. November 2004 vom BMJ vorgestellten Gutachtens des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg zur „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung“ soweit wie möglich bereits in diesem Gesetzgebungsverfahren berücksichtigt werden (vgl. Nr. 7.1.4).

7.1.3 Symposium: „Staatliche Eingriffsbefugnisse auf dem Prüfstand“

Einhelliges Ergebnis des Symposiums zu den Folgerungen aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung: Alle Befugnisregelungen des Bundes und der Länder zu verdeckten Datenerhebungen sind jetzt auf den Prüfstand zu stellen und in weiten Bereichen neu zu fassen.

Um die rechtspolitische öffentliche Diskussion zu den Folgerungen aus dem Urteil des BVerfG zur akustischen Wohnraumüberwachung voranzubringen, habe ich am 8. November 2004 zu einem Symposium in der Berliner Staatsbibliothek eingeladen, dessen Schwerpunkt die Frage bildete, inwiefern neben der akustischen Wohnraumüberwachung auch andere staatliche Eingriffsbefugnisse, wie etwa die Telekommunikationsüberwachung, an die Vorgaben des BVerfG anzupassen sind. Die Universitätsprofessoren Spiros Simitis (Frankfurt), Manfred Baldus (Erfurt), Friedhelm Hufen (Mainz) und Christoph Gusy (Bielefeld) äußerten sich zu diesem Problemkreis. Anschließend fand eine Podiumsdiskussion mit Rechts- und Innenpolitikern der Fraktionen des Deutschen Bundestages statt: Für die SPD-Fraktion Dr. Dieter Wiefelspütz, für die CDU/CSU-Fraktion Stephan Mayer, für die Fraktion BÜNDNIS 90/DIE GRÜNEN Jerzy Montag und für die FDP-Fraktion Rainer Funke. Als Vertreter der Kläger vor dem BVerfG nahm der ehemalige Vizepräsident des Deutschen Bundestages, Dr. Burkhard Hirsch, teil. Die Veranstaltung fand mit rund 200 Gästen aus Politik, Wissenschaft, Verwaltung und den Sicherheitsbehörden eine bemerkenswerte Resonanz.

Alle Beteiligten würdigten die Entscheidung des BVerfG wegen ihrer herausragenden Bedeutung, die weit über den Einzelfall hinaus geht und Auswirkungen auf alle staatlichen Eingriffsbefugnisse zu heimlichen Ermittlungen hat.

Die Rechtslehrer kamen übereinstimmend zu dem Ergebnis, dass angesichts des hohen Stellenwertes, den das BVerfG dem „absolut geschützten Kernbereich privater Lebensgestaltung“ beimisst, auch die gesetzlichen Ermächtigungen zu anderen strafprozessualen, aber auch zu präventiv-polizeilichen Überwachungsmaßnahmen reformbedürftig sind. Bislang enthalten die Polizei- und Verfassungsschutzgesetze keine Vorschriften zum Schutz dieses Kernbereichs privater Lebensgestaltung. Hinzu kommt, dass auch die verfahrensrechtlichen Regelungen zur Benachrichtigung der durch die heimlichen Maßnahmen betroffenen Personen und zur Kennzeichnung der verdeckt gewonnenen Daten entsprechend der Vorgaben des BVerfG angepasst werden müssen.

Die Teilnehmer der Podiumsdiskussion waren sich parteiübergreifend ebenfalls einig, dass das Urteil auf die politische Debatte und die Gesetzgebung bei sämtlichen staatlichen Eingriffsbefugnissen ausstrahlen wird.

Über das Symposium wurde ein Tagungsband erstellt, der über meine Behörde zu beziehen ist. Er kann auch auf meiner Homepage abgerufen werden.

7.1.4 Gutachten zur Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung

Eine Studie des Max-Planck-Instituts belegt geringe Anwendungszahlen, zeigt aber auch erhebliche Problembereiche auf.

Das BMJ stellte am 1. November 2004 ein Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht in Freiburg zur „Rechtswirklichkeit und Effizienz der akustischen Wohnraumüberwachung (großer Lauschangriff) nach § 100c Abs. 1 Nr. 3 StPO“ vor. Die Studie beruht vor allem auf einer Aktenanalyse sämtlicher 119 Verfahren, in denen im Erhebungszeitraum von 1998 bis 2001 eine akustische Wohnraumüberwachung in Deutschland beantragt wurde. Ergänzt wurden die Erkenntnisse der Aktenanalyse durch Expertengespräche mit Richtern, Staatsanwälten und Polizeibeamten.

Das Gutachten kommt zu dem Ergebnis, dass die rechtlich hohen Voraussetzungen für den Einsatz der akustischen Wohnraumüberwachung, insbesondere der Grundsatz, diese Maßnahme nur als letztes Mittel umzusetzen, im Wesentlichen gewahrt werden und bei der Anordnung eine wirksame rechtliche Kontrolle stattfindet. Die Studie lässt aber auch erhebliche Problembereiche erkennen, die

durch den Gesetzentwurf (vgl. Nr. 7.1.2) noch nicht hinreichend berücksichtigt werden. So wies die akustische Wohnraumüberwachung nur in rund der Hälfte der Fälle einen Bezug zur Organisierten Kriminalität auf, deren Bekämpfung sie jedoch primär dienen sollte. Die Anwendungshäufung der akustischen Wohnraumüberwachung bei den Mord- und Totschlagsverfahren beinhaltet kritische Aspekte. Denn gerade im Bereich der Tötungsdelikte betrifft sie überwiegend die Kommunikation des Beschuldigten mit Personen seines Vertrauens und damit den unantastbaren Kernbereich privater Lebensgestaltung. Auch weist die Maßnahme nach den Ergebnissen des Gutachtens nur eine sehr niedrige Erfolgsquote auf. Nahezu die Hälfte der Maßnahmen führte zu keinerlei Ergebnis und ein wesentlicher Teil allenfalls zu indiziellen Belastungen. Neben einer begrenzten Effizienz der akustischen Wohnraumüberwachung (nur 30 Prozent der angeordneten Maßnahmen wurden als erfolgreich oder bedingt erfolgreich eingestuft, nur in 7 Prozent der Fälle brachten sie einen direkten Tatnachweis) belegt die Studie maßgebliche Schwierigkeiten bei der praktischen Umsetzung der Maßnahme, wie z. B. bei der Installation der technischen Mittel.

Im 19. TB (Nr. 8.4) hatte ich die Erforderlichkeit der Aufnahme bestimmter Delikte in den Anlasstatenkatalog des § 100c Abs. 1 Nr. 3 StPO bezweifelt. Auch aufgrund des Gutachtens sind – von der Bundesregierung damals noch für verfrüht gehaltene – Rückschlüsse aus der tatsächlichen Verteilung der Anlasstaten nunmehr möglich. Ich bedauere daher, dass die Reform der Bestimmungen zur akustischen Wohnraumüberwachung bislang nicht dazu genutzt wurde, den Anlasstatenkatalog auch unter dem Aspekt des tatsächlichen Bedarfes einer kritischen Prüfung zu unterziehen. Auf eine solche werde ich weiterhin drängen.

Link zur Studie: http://www.bmj.de/enid/2c5c8db1101fd6acfec919029ad0267e,55a304092d09/pr.html

7.2 Telekommunikationsüberwachung

Mit Sorge nehme ich zur Kenntnis, dass die Anzahl der Telefonüberwachungen nach den §§ 100a, 100b Strafprozessordnung weiter angestiegen ist. Wurden im Jahr 2002 noch 21.874 Überwachungsmaßnahmen angeordnet, waren es gemäß der Statistik der Regulierungsbehörde für Post und Telekommunikation im Jahr 2003 bereits 24 441. Der Trend ist seit Jahren ungebrochen. Angesichts des massiven Eingriffs der Maßnahmen in das Grundrecht nach Artikel 10 GG gibt die Entwicklung immer wieder Anlass zur Kritik (vgl. 18. TB Nr. 6.4.2; 19. TB Nr. 8.2.5).

7.2.1 Reform der §§ 100a ff. Strafprozessordnung

Die StPO-Vorschriften zur Telekommunikationsüberwachung sind dringend reformbedürftig.

Über die Effizienz der Telekommunikationsüberwachungsmaßnahmen nach der StPO und die Verhältnismäßigkeit ihres Einsatzes gab es bislang kaum Erkenntnisse, was angesichts des deutlichen Anstiegs der angeordneten Überwachungsmaßnahmen besonders misslich war. Nunmehr liegen die – mit Spannung erwarteten (vgl. 18. TB Nr. 11.9; 19. TB Nr. 8.3) – Ergebnisse einiger Forschungsvorhaben vor, insbesondere der vom BMJ in Auftrag gegebenen Untersuchung „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§100a,100b StPO und anderer verdeckter Ermittlungsmaßnahmen“ des Max-Planck-Institutes für ausländisches und internationales Strafrecht. Die Ergebnisse sind unter verschiedenen Gesichtspunkten bemerkenswert.

– Die Effizienz des Einsatzes der Telekommunikationsüberwachungsmaßnahmen darf bezweifelt werden. In lediglich 23 Prozent der untersuchten Fälle bezogen sich die Ermittlungserfolge direkt auf den die Telefonüberwachung begründenden Verdacht. Die übrigen Erfolge waren nur mittelbarer Natur, wovon etwa zwei Drittel als „Hinweise auf Straftaten Dritter“ den größten Raum einnahmen.

– Die Häufigkeit der Anordnung von Überwachungsmaßnahmen führt offensichtlich nicht zu einer höheren Aufklärungsrate der davon erfassten Kriminalitätsbereiche, insbesondere im Vergleich vor allem mit Großbritannien und den USA.

– Keinen Anlass zur Entwarnung geben die Ergebnisse der Untersuchung auch, soweit es um die Verhältnismäßigkeit des Einsatzes dieser Ermittlungsmaßnahmen geht. So gibt es Gründe für die Annahme, dass die Telekommunikationsüberwachung nicht, wie gesetzlich vorgesehen, stets das letzte Mittel der Ermittlungsmaßnahmen ist. Der kontinuierliche Anstieg ihres Einsatzes kann gemäß der Studie zwar partiell damit erklärt werden, dass die Anzahl der Mobilfunkteilnehmer in den letzten Jahren stark gewachsen ist. Diese Entwicklung auf dem Telekommunikationsmarkt allein vermag jedoch nicht zu begründen, warum in immer mehr Verfahren zu dem Mittel der Telekommunikationsüberwachung gegriffen wird.

Die Ergebnisse der Untersuchung lassen auch in anderer Hinsicht Defizite erkennen, die dringender Abhilfe bedürfen. Hierauf haben die Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung hingewiesen (vgl. Anlage 14). So muss der Straftatenkatalog des § 100a StPO im Sinne einer Reduzierung dringend überarbeitet werden. Die Untersuchung hat ergeben, dass sich etwa 90 Prozent aller Überwachungsmaßnahmen in diesem Bereich auf nur fünf der achtzehn Deliktsgruppen als Anlasstaten erstrecken. Eine Reduzierung des Kataloges ist aber auch deshalb geboten, weil nach wiederholten Erweiterungen inzwischen an der dem Katalog eigentlich gedachten Begrenzungsfunktion gezweifelt werden muss.

Besondere Missstände hat die Untersuchung in Bezug auf den Richtervorbehalt erkennen lassen. Diesem kommt in der Praxis teilweise nicht die Wirksamkeit zu, die ihm von Gesetzes wegen gebührt. Beispielsweise waren von den untersuchten richterlichen Beschlüssen nur

ca. 24 Prozent substanziell begründet. Die Beschlüsse ergingen in der Regel sehr schnell und orientierten sich ausschließlich an der polizeilichen oder staatsanwaltschaftlichen Vorlage. Dass die Ermittlungsrichter ihre Kontroll- und Dokumentationspflichten oft nur unzureichend erfüllen, hatte ein Forschungsprojekt der Universität Bielefeld zu „Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen“ gezeigt. Da eine Verbesserung der richterlichen Kontrolle dringend erforderlich ist, haben die Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung einige Vorschläge gemacht.

Ein großes Manko der derzeitigen Überwachungspraxis hat die Untersuchung auch hinsichtlich der Benachrichtigungspflichten offenbart, denen in der Praxis nur unzureichend nachgekommen wird. Hier ist ebenfalls dringender gesetzlicher Handlungsbedarf gegeben, der sich nicht nur zu dieser Problematik, sondern auch darüber hinaus (z. B. hinsichtlich der Berücksichtigung des „absolut geschützten Kernbereichs privater Lebensgestaltung“, Einführung von Kennzeichnungspflichten etc.) aus dem Urteil des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung vom 3. März 2004 (vgl. dazu Nr. 7.1.1) ergibt.

Eine Reform der Vorschriften zur Telekommunikationsüberwachung ist daher dringend notwendig.

Bei diesem Vorhaben sollten aus meiner Sicht folgende weitere Probleme gelöst werden. Regelungsbedürftig ist meines Erachtens die Ermittlungsmaßnahme der sog. „stillen SMS“. Dabei schickt die ermittelnde Person eine Kurznachricht an ein empfangsbereites Handy, auf dessen Display sie nicht angezeigt wird. Daraufhin verlangt die ermittelnde Person beim Mobilfunkanbieter die Verbindungsdaten und kann so das Gerät auf bis zu 50 Meter genau orten. In einem Schreiben an das BMJ habe ich dargelegt, dass bereits das Versenden der sog. stillen SMS (und nicht erst die Übermittlung der Verbindungsdaten) einen Eingriff in das grundrechtlich verbürgte Fernmeldegeheimnis darstellt, der keine rechtliche Grundlage in den §§ 100a ff. StPO findet. Ebenso wie einige andere technische Überwachungsmaßnahmen, z. B. der IMSI-Catcher oder das Abfragen der Stand-By-Daten von Mobiltelefonen, dient sie nicht der inhaltlichen Überwachung der Telekommunikation, sondern der heimlichen Standortfeststellung des Betroffenen. Diese Ortungsmaßnahmen, von denen lediglich der Einsatz des IMSI-Catchers – wie bereits im 19. TB (Nr. 8.2.4) berichtet – eindeutig in der StPO geregelt ist (§ 100i), bedürfen ebenfalls einer (einheitlichen) Regelung in der StPO.

Problematisch ist des weiteren die derzeitige Ausgestaltung der Anordnungen zur Auskunft über Verbindungsdaten (§ 100h Abs. 1 S. 3 i.V.m. § 100b Abs. 1 StPO); denn die geltende Regelung ermöglicht, dass eine bei Gefahr im Verzug von der Staatsanwaltschaft getroffene Anordnung für die Dauer von drei Tagen wirksam bleibt, auch wenn sie nicht vom Richter bestätigt wird. Vielfach wird deshalb von vornherein auf die richterliche Entscheidung verzichtet. Der Richtervorbehalt droht daher zumindest für die Fälle ins Leere zu laufen, in denen bereits vorliegende Verbindungsdaten abgefragt werden. M.E. sollte für diese Fallgestaltung zumindest die obligatorische nachträgliche Einschaltung des Richters vorgesehen werden. Auch darauf habe ich das BMJ aufmerksam gemacht.

Sehr wichtig ist darüber hinaus, die Transparenz der Telekommunikationsüberwachung zu verbessern. Während für Maßnahmen der akustischen Wohnraumüberwachung Berichtspflichten der Staatsanwaltschaften an die jeweils zuständigen obersten Justizbehörden gesetzlich vorgesehen sind (vgl. Nr. 7.1.2), auf deren Grundlage die Bundesregierung den Bundestag jährlich über die durchgeführten Maßnahmen unterrichtet, fehlen für Telekommunikationsüberwachungsmaßnahmen vergleichbare Regelungen. Die vorhandene Datenbasis ist hier bisher sehr lückenhaft.

Schließlich hat der Gesetzgeber die Geltungsdauer der §§ 100g, 100h StPO mit Gesetz vom 9. Dezember 2004 (BGBl. I S. 3231) verlängert. Über diese Vorschriften, welche die Rechtsgrundlage für Auskunftsverlangen der Strafverfolgungsbehörden über Telekommunikationsverbindungsdaten bilden, habe ich im 19. TB (Nr. 8.2.1) berichtet. Die §§ 100g, 100h StPO waren ursprünglich bis zum 31. Dezember 2004 befristet, weil der Gesetzgeber sie bis dahin in einer Gesamtreform der §§ 100a ff. StPO aufgehen lassen wollte. Da die Reform aber nach wie vor aussteht, wurde die Geltung der §§ 100g, 100h StPO bis zum 31. Dezember 2007 verlängert. Kritisch bewerte ich diese Entscheidung vor allem deshalb, weil ihr keine Evaluation der Wirksamkeit dieser Eingriffsbefugnisse vorausgegangen war. Ich erwarte, dass die Wirksamkeit dieser Befugnisnormen nunmehr rechtzeitig vor dem Ende der neuen Frist evaluiert wird.

Weiterführende Hinweise: Untersuchung des Max-Planck-Instituts für ausländisches und internationales Strafrecht „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100a, 100b StPO und anderer verdeckter Ermittlungsmaßnahmen“ (Freiburg/Br., edition iuscrim, 2003); Forschungsprojekt der Uni Bielefeld zu „Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen“ (Backes/Gusy, Wer kontrolliert die Telefonüberwachung?, Frankfurt a. M., Lang, 2003).

7.2.2 Datenschutzkontrollen beim Generalbundesanwalt und beim Bundeskriminalamt

Der Generalbundesanwalt und das BKA teilen meine Ansichten hinsichtlich des datenschutzrechtlichen Standards bei Telekommunikationsüberwachungsmaßnahmen weitgehend.

Maßnahmen zur Überwachung der Telekommunikation und zur akustischen Wohnraumüberwachung nach §§ 100a ff. StPO bildeten den Schwerpunkt meiner

Beratungs- und Kontrollbesuche beim Generalbundesanwalt beim Bundesgerichtshof (GBA) und beim Bundeskriminalamt (BKA).

Bei meinem ersten Besuch beim GBA habe ich die Umsetzung der dortigen „Richtlinie für die Überwachung und Aufzeichnung von Telekommunikationsvorgängen gemäß §§ 100a ff. StPO“ anhand von Verfahrensakten kontrolliert. Dabei ist mir aufgefallen, dass die nach Beendigung einer Überwachungsmaßnahme durchzuführenden Überprüfungen, ob und was gelöscht werden kann, sowie die Löschungen von Wortprotokollen in den Vorgängen nicht dokumentiert waren. Auch waren entgegen der Richtlinie Vermerke über die Benachrichtigung bzw. die Tatsache, dass die Beschuldigten nicht benachrichtigt wurden, offensichtlich nicht dem Abteilungsleiter vorgelegt worden. Auf meine Anregung hin hat der GBA die Richtlinie dahingehend ergänzt, dass zur Fristenüberwachung und vereinfachten Dokumentation ein Kontrollblatt zu führen ist. Da sich zudem die vorgesehene Benachrichtigung des Anschlussinhabers in bestimmten Fällen als unzweckmäßig erwiesen hatte, passte der GBA die Richtlinie entsprechend meiner Empfehlung diesbezüglich an. Außerdem war ich mit dem GBA darin einig, dass von der Benachrichtigung der Beteiligten nur dann abgesehen werden kann, wenn anderenfalls in die Rechte des Beschuldigten unverhältnismäßig eingegriffen würde, was im Regelfall erst durch eine umfassende Einzelfallabwägung und nicht durch einen bloßen Hinweis auf die Richtlinie festzustellen ist. Gemäß meiner Anregung hat der GBA zudem angeordnet, dass die Richtlinie auch für Maßnahmen der akustischen Wohnraumüberwachung entsprechend anzuwenden ist. Denn die Durchsicht der mir ebenfalls zur Verfügung gestellten Sonderhefte „Wohnraumüberwachung“ hatte ergeben, dass die Führung von Kontrollblättern oder die Ablage der Wortprotokolle mangels verbindlicher Regelung nicht einheitlich gehandhabt wurde. Auch existierte keine ausdrückliche Klarstellung über den Umgang mit nicht mehr benötigten Wortprotokollen.

Weiterer Prüfungsgegenstand war die Frage, wie technisch ausgeschlossen werden kann, dass nicht verfahrensrelevante Gesprächsaufzeichnungen weiter benutzt werden. Hierzu habe ich mich auch beim BKA informiert. Dabei ergab sich, dass eine elektronische Sperrung von Gesprächen nur während der Auswertung erfolgen kann, solange die Gesprächsdaten noch in der DV-Anlage gespeichert sind. Die Gesprächsdaten werden allerdings in den Ermittlungsreferaten des BKA aus Gründen der Beweisführung nicht gesperrt, da erst die Staatsanwaltschaft bzw. das Gericht entscheidet, was beweisrelevant ist. Vielmehr wird in entsprechenden Fällen vermerkt, dass es sich um ein „irrelevantes Gespräch“ handelt. Aus Sicht des GBA erscheint eine Sperrung nicht möglich, da selbst bei abgeschlossenen Verfahren gegen einen Beschuldigten zumindest in sog. Strukturverfahren nach §§ 129, 129a Strafgesetzbuch Gespräche für weitere Ermittlungen relevant sein könnten.

Offen geblieben war, ob Auswertungsvermerke des BKA über Telekommunikations- oder Wohnraumüberwachungen Bestandteile der Sachakten seien und somit – anders als die Wortprotokolle – nicht vernichtet werden müssten. Ein Meinungsaustausch mit den Landesbeauftragten für den Datenschutz bestärkte mich in der Ansicht, dass eine weitere Aufbewahrung von Auswertungsvermerken, die Teile von Wortprotokollen enthalten, die Regelung in § 100b Abs. 6 StPO unterläuft und solche Vermerke ebenfalls nach Abschluss einer Überwachung zu vernichten sind. Der GBA hat angekündigt, die Richtlinie dahingehend zu ergänzen, dass Sachaktenvermerke keine wörtlichen Zitate aus Überwachungsmaßnahmen mehr enthalten sollen.

Ein weiterer Schwerpunkt war die Errichtungsanordnung gemäß § 490 StPO über automatisierte Dateien. Zu den von mir geäußerten Bedenken hat der GBA die Bereitschaft signalisiert, die elektronische Aufbewahrungsfrist für das StR-Register (Revisionen in Strafsachen) – vorbehaltlich der Zustimmung des Bundesgerichtshofs – von 50 Jahren auf 30 Jahre herabzusetzen und so der Aufbewahrungsfrist für Handakten über Revisionen in Strafsachen anzupassen. Auch hat er angekündigt, die Sonderdatei „Telekommunikationsüberwachung“ alsbald in der Errichtungsanordnung gemäß § 490 StPO aufzunehmen. Der GBA will hingegen an der Praxis festhalten, den Datenbestand des BJs-/StE-Verfahrensregisters (Ermittlungsverfahren) erst drei Jahre nach Erledigung des Verfahrens zu reduzieren, da dieser Zeitraum zur Durchführung des Bund-/Länder-Finanzausgleichs erforderlich sei. Ich halte diese Argumentation nicht für überzeugend. Finanzwirtschaftliche Erwägungen können eine fortdauernde Speicherung dieser sensiblen personenbezogenen Daten m.E. nicht rechtfertigen.

Hinsichtlich der innerbehördlichen Datenübermittlung habe ich kritisch angemerkt, dass auf das Register der Abteilung I (Revision in Strafsachen) abteilungsübergreifend zugegriffen werden kann. Der GBA hat eine alsbaldige Beschränkung der Zugriffsmöglichkeiten zugesagt. Der in diesem Zusammenhang von mir besonders problematisierte behördenweite Zugriff auf das Register über allgemeine oder nicht unmittelbar einem Vorgang zuzuordnende Eingaben ist hingegen nach Ansicht des GBA für die tägliche Arbeit aller Abteilungen unverzichtbar. Ich hoffe, dass der GBA die von mir kritisierte Praxis noch korrigieren wird.

7.3 Genomanalyse im Strafverfahren

Die unbestreitbaren Ermittlungserfolge unter Einsatz der DNA-Analyse rechtfertigen nicht den Wegfall der für dieses Instrument bestehenden rechtlichen Vorgaben.

In der Praxis der Strafverfolgungsbehörden hat sich die DNA-Analyse zu einer wirkungsvollen Ermittlungsmethode entwickelt. In der kriminalpolitischen Diskussion wird deshalb die Forderung immer lauter, die aus verfassungsrechtlichen Gründen vom Gesetzgeber errichteten rechtlichen Vorgaben für die Nutzung der DNA-Analyse zur Identitätsfeststellung in Strafverfahren ganz oder teilweise zu beseitigen. Allerdings muss dabei klar sein, dass Feststellung, Speicherung und Verwendung des DNA-

Identifizierungsmusters nicht unerhebliche Eingriffe in das Recht auf informationelle Selbstbestimmung darstellen, wie das Bundesverfassungsgericht in mehreren Entscheidungen (vgl. insbes. den Kammerbeschluss vom 15. März 2001, NJW 2001, S. 2320) dargelegt hat.

Derartige Eingriffe bedürfen einer gesetzlichen Legitimation unter Beachtung des Grundsatzes der Verhältnismäßigkeit im überwiegenden Interesse der Allgemeinheit. An diesen Kriterien ist das geltende Recht ausgerichtet. Entscheidend ist, dass bei der Nutzung der DNA-Analyse auch in Zukunft Augenmaß bewahrt und die wertsetzende Bedeutung des Rechts auf informationelle Selbstbestimmung beachtet wird (vgl. Entschließung der Datenschutzbeauftragten von Bund und Ländern vom 16. Juli 2003 – Kasten zu Nr. 7.3).

Kasten zu Nr. 7.3

Entschließung
zwischen der 65. und 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 16. Juli 2003

Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

Derzeit gibt es mehrere politische Absichtserklärungen und Gesetzesinitiativen mit dem Ziel, die rechtlichen Schranken in § 81g StPO für die Entnahme und Untersuchung von Körperzellen und für die Speicherung der dabei gewonnenen DNA-Identifizierungsmuster (sogen. genetischer Fingerabdruck) in der zentralen DNA-Analyse-Datei des BKA abzusenken.

Die Vorschläge gehen dahin,

- zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr – wie vom geltenden Recht gefordert – in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,
- zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass die Anordnung der Entnahme und Untersuchung von Körperzellen zur Erstellung und Speicherung eines genetischen Fingerabdrucks einen tiefgreifenden und nachhaltigen Eingriff in das Recht auf informationelle Selbstbestimmung der Betroffenen darstellt; dies hat auch das Bundesverfassungsgericht in seinen Beschlüssen vom Dezember 2000 und März 2001 bestätigt.

Selbst wenn bei der DNA-Analyse nach der derzeitigen Rechtslage nur die nicht-codierenden Teile untersucht werden: Schon daraus können Zusatzinformationen gewonnen werden (Geschlecht, Altersabschätzung, Zuordnung zu bestimmten Ethnien, möglicherweise einzelne Krankheiten wie Diabetes, Klinefelter-Syndrom). Auch deshalb lässt sich ein genetischer Fingerabdruck mit einem herkömmlichen Fingerabdruck nicht vergleichen. Zudem ist immerhin technisch auch eine Untersuchung des codierenden Materials denkbar, so dass zumindest die abstrakte Eignung für viel tiefer gehende Erkenntnisse gegeben ist. Dies bedingt unabhängig von den gesetzlichen Einschränkungen ein höheres abstraktes Gefährdungspotential.

Ferner ist zu bedenken, dass das Ausstreuen von Referenzmaterial (z. B. kleinste Hautpartikel oder Haare), das mit dem gespeicherten Identifizierungsmuster abgeglichen werden kann, letztlich nicht zu steuern ist, so dass in höherem Maß als bei Fingerabdrücken die Gefahr besteht, dass genetisches Material einer Nichttäterin oder eines Nichttäters an Tatorten auch zufällig, durch nicht wahrnehmbare Kontamination mit Zwischenträgern oder durch bewusste Manipulation platziert wird. Dies kann für Betroffene im Ergebnis zu einer Art Umkehr der Beweislast führen.

Angesichts dieser Wirkungen und Gefahrenpotentiale sehen die Datenschutzbeauftragten Erweiterungen des Einsatzes der DNA-Analyse kritisch und appellieren an die Regierungen und Gesetzgeber des Bundes und der Länder, die Diskussion dazu mit Augenmaß und unter Beachtung der wertsetzenden Bedeutung des Rechts auf informationelle Selbstbestimmung zu führen. Die DNA-Analyse darf nicht zum Routinewerkzeug jeder erkennungsdienstlichen Behandlung und damit zum alltäglichen polizeilichen Eingriffsinstrument im Rahmen der Aufklärung und Verhütung von Straftaten jeder Art werden. Auf das Erfordernis der Prognose erheblicher Straftaten als Voraussetzung einer DNA-Analyse darf nicht verzichtet werden.

Im Hinblick auf die Eingriffsschwere ist auch der Richtervorbehalt für die Anordnung der DNA-Analyse unverzichtbar. Es ist deshalb auch zu begrüßen, dass zur Stärkung dieser grundrechtssichernden Verfahrensvorgabe für die Anordnungsentscheidung die Anforderungen an die Begründung des Gerichts gesetzlich präzisiert wurden. Zudem sollte die weit verbreitete Praxis, DNA-Analysen ohne richterliche Entscheidung auf der Grundlage der Einwilligung der Betroffenen durchzuführen, gesetzlich ausgeschlossen werden.

7.3.1 Erweiterung des Katalogs der Anlassdelikte

DNA-Analysen dürfen jetzt auch bei weniger schwerwiegenden Straftaten gegen die sexuelle Selbstbestimmung und zur Feststellung des Geschlechts angeordnet werden.

Mit dem Gesetz zur Änderung der Vorschriften über die Straftaten gegen die sexuelle Selbstbestimmung und zur Änderung anderer Vorschriften vom 27. Dezember 2003 (BGBl. I S. 3007) ist am 1. April 2004 inzwischen das sechste Gesetz in Kraft getreten, das seit 1997 die DNA-Analyse berührt. Neben Änderungen des materiellen Strafrechts mit der Einführung neuer Straftatbestände ändert das Gesetz in Artikel 3 Vorschriften über die Genomanalyse in der Strafprozessordnung. Danach ist auch die Bestimmung des Geschlechts in einem anhängigen Strafverfahren durch molekulargenetische Untersuchungen zulässig, während sie bisher nur erlaubt war zur „Feststellung der Abstammung oder der Tatsache, ob aufgefundenes Spurenmaterial von dem Beschuldigten oder dem Verletzten stammt“ (§ 81e Abs. 1 Satz 1 StPO). Darüber hinaus ist die Geschlechtsbestimmung auch zur Identitätsfeststellung in künftigen Strafverfahren nach § 81g Abs. 1 StPO und in Fällen eines Leichenfundes nach § 88 StPO zulässig.

Aus meiner Sicht ist gegen die molekulargenetische Bestimmung des Geschlechts nichts einzuwenden, da es sich bei einem bekannten Verdächtigen um ein offenkundiges Merkmal handelt und der Eingriff im Verhältnis zum kriminaltechnischen Nutzen hinnehmbar ist. Bei aufgefundenem Spurenmaterial ist die Kenntnis des Geschlechts eines Spurenlegers für die Strafverfolgung ein wichtiger Ermittlungsansatz, dem schutzwürdige Interessen des noch unbekannten Betroffenen schwerlich entgegengehalten werden können.

Nach der Neufassung des § 81g Abs. 1 StPO ist die DNA-Identitätsfeststellung für künftige Strafverfahren auch dann zulässig, wenn der Beschuldigte einer Straftat gegen die sexuelle Selbstbestimmung verdächtig ist, auch wenn keine Straftat von erheblicher Bedeutung vorliegt.

Entscheidend ist, dass an dem Erfordernis einer qualifizierten richterlichen Prognose festgehalten wird. Danach ist eine DNA-Identitätsfeststellung für künftige Strafverfahren nur dann zulässig, wenn ein Richter entscheidet, es bestehe Grund zu der Annahme, dass der Verdächtige aufgrund seiner Persönlichkeit und wegen der Art oder Ausführung der Tat oder sonstiger Erkenntnisse auch in Zukunft Straftaten von erheblicher Bedeutung begehen werde (Negativprognose). In diesem Zusammenhang begrüße ich ausdrücklich, dass mit der Gesetzesnovelle auch die Anforderungen an die Begründung des Gerichts für die Anordnungsentscheidung präzisiert wurden (§ 81g Abs. 3 Satz 2 StPO). Für die Prognoseentscheidung ist es erfreulicherweise dabei geblieben, dass die künftige Straftat nach wie vor ein Delikt von erheblicher Bedeutung sein muss, selbst wenn die Anlassstraftat nicht dieser qualifizierten Deliktsgruppe zuzurechnen ist. Dazu hat das Bundesverfassungsgericht in seinem Kammerbeschluss vom Dezember 2001 (NJW 2001, S. 2320) eine auf den Einzelfall bezogene richterliche Entscheidung gefordert und weiter ausgeführt, dass die Prognoseentscheidung nach § 81g StPO von Verfassungs wegen voraussetze, dass eine zureichende Sachaufklärung insbesondere durch Beiziehung der verfügbaren Straf- und Vollstreckungsakte, des Bewährungsheftes und zeitnaher Auskünfte aus dem Bundeszentralregister vorangegangen ist und die für sie bedeutsamen Umstände nachvollziehbar abgewogen werden. Ich kann mir kaum vorstellen, wie eine solche abwägende Prognoseentscheidung ohne die Indizwirkung einer einschlägigen Anlassstraftat von einigem Gewicht möglich sein soll. Den gänzlichen Verzicht auf eine bestimmte Anlassstraftat – wie in der kriminalpolitischen Diskussion bisweilen gefordert – halte ich deshalb nicht für vertretbar. Aber selbst der pauschale Verweis auf „eine Straftat gegen die sexuelle Selbstbestimmung (§§ 174 bis 184f des Strafgesetzbuches)“, wie in der Neufassung des § 81g StPO vorgesehen, ist in meinen Augen nur bei verfassungskonformer einschränkender Auslegung in dem Sinne haltbar, dass als Anlassstraftat nur die schwerwiegenderen Delikte dieses Abschnitts des StGB in Betracht kommen. Dies hat offenbar auch der Rechtsausschuss des Deutschen Bundestages so gesehen, als er in seinem Bericht an das Plenum vom 1. Juli 2003 ausführte, dass in den Fällen der §§ 184d und 184e StGB (Prostitution an bestimmten Orten und jugendgefährdende Prostitution) „eine molekulargenetische Erfassung mangels Erforderlichkeit und Angemessenheit der Maßnahme im Einzelfall nahezu nie in Betracht kommen wird“.

7.3.2 Sind der genetische und der herkömmliche Fingerabdruck gleichzusetzen?

Vielfach wird gefordert, die DNA-Analyse als normale erkennungsdienstliche Maßnahme zu gestalten, obgleich ihr Erkenntnispotential weit über Fingerabdruck, Foto und Vermessungen hinausgeht.

Im politischen Raum werden gerade in jüngster Zeit immer wieder Forderungen erhoben, die auf eine breitere Anwendung der DNA-Analyse abzielen. Die Ständige Konferenz der Innenminister und -senatoren der Länder hat gefordert, die DNA-Analyse im nicht-codierenden Bereich mit den sonstigen erkennungsdienstlichen Maßnahmen im Rahmen des § 81b 2. Alt. StPO gleichzustellen. Die Justizministerkonferenz beauftragte ihren Strafrechtsausschuss mit der Prüfung, ob und ggf. in welchen verfassungsrechtlichen Grenzen die DNA-Analyse entsprechend den erkennungsdienstlichen Maßnahmen zum Zweck der Identifizierung in künftigen Strafverfahren genutzt werden kann.

Anlässlich einer Expertenanhörung der CDU/CSU-Bundestagsfraktion am 18. September 2003 und bei einem öffentlichen Fachgespräch der Fraktion des Bündnis 90/DIE GRÜNEN am 1. März 2004 sowie in einem Gespräch mit der BMJ am 15. Juni 2004 habe ich betont, dass sich eine Gleichstellung der DNA-Analyse mit einem herkömmlichen Fingerabdruck schon deshalb verbietet, weil das Aussagepotential des DNA-Probenmaterials ungleich größer ist. Auch nach heutigem Stand der Technik sind bei der DNA-Analyse schon Rückschlüsse

auf personenbezogene Merkmale wie Alter, gewisse Krankheiten oder die Zuordnung zu bestimmten Ethnien möglich, selbst wenn nur die sog. nicht-codierenden Teile der DNA untersucht werden. Außerdem darf nicht verkannt werden, dass die Entnahme von Körperzellen für die DNA-Analyse als körperlicher Eingriff anzusehen ist, der nach § 81a StPO nur von einem Richter angeordnet und nur von einem Arzt vorgenommen werden darf. Dem gegenüber dürfen nach § 81b StPO Lichtbilder und Fingerabdrücke auch gegen den Willen des Betroffenen von der Polizei oder der Staatsanwaltschaft aufgenommen werden.

Gegen eine Gleichstellung der DNA-Analyse mit einem herkömmlichen Fingerabdruck sprechen aber noch andere gewichtige Gründe: Zunächst ist das Gefährdungspotential zu nennen, das dem Verfahren der DNA-Analyse innewohnt. Sobald die Körperzellen für die DNA-Untersuchung in die damit beauftragten Labors gelangen, besteht die Gefahr, dass dort missbräuchlich auch die codierenden Teile der in den Zellen enthaltenen DNA untersucht werden und somit Rückschlüsse auf Persönlichkeitsmerkmale wie Eigenschaften und Aussehen gezogen werden. Erst nachdem das Identifizierungsmuster erstellt, in der DNA-Datenbank beim Bundeskriminalamt gespeichert und das untersuchte Körpermaterial vernichtet ist, ist diese Gefahr nicht mehr gegeben. Der Gesetzgeber hat deshalb für die DNA-Analyse zahlreiche verfahrenssichernde Schritte vorgesehen. Hierzu gehört die strikte Zweckbindung der §§ 81d und 81e StPO und die Tatsache, dass gem. § 81f Abs. 2 StPO mit der Durchführung der Untersuchung nur bestimmte zuverlässige Sachverständige beauftragt werden dürfen. Ferner muss das Untersuchungsmaterial den Sachverständigen nach § 81f Abs. 2 StPO in anonymisierter Form übergeben werden und es ist unverzüglich zu vernichten, sobald es für die Untersuchung nicht mehr erforderlich ist (§§ 81a Abs. 3, 81g Abs. 2 StPO).

Der Forderung, die DNA-Analyse zu einem Routinewerkzeug jeder erkennungsdienstlichen Behandlung zu machen, ist entgegenzuhalten, dass diese Untersuchung wegen des von Verfassungs wegen zu beachtenden Übermaßverbotes auf besondere Fälle zu beschränken ist. Das BVerfG (vgl. Nr. 7.3.1) sah diese Beschränkung bei der gegenwärtigen Rechtslage als gegeben an, weil sie eine vorangegangene Verurteilung des Betroffenen wegen einer Straftat von erheblicher Bedeutung und die auf bestimmte Tatsachen gestützte negative Prognose voraussetzt. Das besondere Interesse des Betroffenen an effektivem Grundrechtsschutz sah das Gericht durch den Richtervorbehalt gem. §§ 81g Abs. 3, 81a Abs. 2 StPO berücksichtigt. Zum andern hat das BVerfG festgestellt, dass eine tragfähig begründete Entscheidung im Falle des Eingriffs in das Recht auf informationelle Selbstbestimmung voraussetzt, dass ihr eine zureichende Sachaufklärung, insbesondere durch Beiziehung der verfügbaren Straf- und Vollstreckungsakten, des Bewährungshefts und zeitnaher Auskünfte aus dem Bundeszentralregister vorausgegangen ist und in den Entscheidungsgründen die bedeutsamen Umstände abgewogen wurden, wobei stets eine auf den Einzelfall bezogene Entscheidung gefordert ist.

Ich halte den Richtervorbehalt und die qualifizierte Negativprognose verfassungsrechtlich für unverzichtbar. Der Richtervorbehalt kann schon deshalb nicht ohne Weiteres durch die Möglichkeit eines nachträglichen Rechtsschutzes ersetzt werden, weil er eine wichtige verfahrenssichernde Funktion hat. Bezüglich der Prognoseentscheidung sind Abstriche wegen des verfassungsrechtlichen Übermaßverbotes und der daraus folgenden Beschränkung der DNA-Analyse auf besondere Fälle – wie vom BVerfG mehrfach betont – nicht zu vertreten.

Zwar ist auch für die Abnahme eines herkömmlichen Fingerabdrucks nach § 81b StPO eine Prognoseentscheidung insoweit erforderlich als Anhaltspunkte dafür vorliegen müssen, dass der Beschuldigte in ähnlicher oder anderer Weise erneut straffällig werden könnte und die erkennungsdienstlichen Unterlagen zur Förderung der dann zu führenden Ermittlungen geeignet erscheinen. Dieser Prognosemaßstab erfüllt aber die verfassungsrechtlichen Ansprüche in Bezug auf den genetischen Fingerabdruck keineswegs. Er ist deutlich geringer als der in § 81g Abs.1 StPO bzw. den §§ 2 und 3 DNA-Identitätsfeststellungsgesetz. Nach § 81b StPO ist auch keine richterliche Entscheidung vorgesehen. Wie aber Polizei oder Staatsanwaltschaft eine den Anforderungen des BVerfG genügende umfassende Prognoseentscheidung treffen können sollen, ist mir nicht ersichtlich.

Dagegen habe ich wiederholt erklärt, dass ich einer Abschaffung des Richtervorbehalts bei der Untersuchung von unbekanntem Spurenmaterial (vgl. u. a. Bundestagsdrucksache 15/4136) nicht widersprechen würde, da eine richterliche Prüfung in den Fällen wenig sinnvoll erscheint, in denen der Richter den Spurenleger gar nicht kennt.

7.3.3 Ersetzt Einwilligung die Prognoseentscheidung des Richters?

Der Verzicht auf den Richtervorbehalt bei der Speicherung der im laufenden Strafverfahren gewonnenen DNA-Identifizierungsmuster beruht auf einer gesetzlichen Lücke.

Schon mehrfach habe ich bemängelt, dass § 3 Satz 3 des DNA-Identitätsfeststellungsgesetzes vom 7. September 1998 (BGBl. I S. 2646), der die Speicherung der im laufenden Strafverfahren gewonnenen DNA-Identifizierungsmuster zulässt, nicht auf den Richtervorbehalt in § 81g Abs. 3 StPO verweist (vgl. zuletzt 19. TB Nr. 8.2.3.3). Danach kann das Identifizierungsmuster eines Beschuldigten nach dem BKA-Gesetz gespeichert werden, wenn die in § 81g Abs. 1 StPO genannten Voraussetzungen vorliegen. Die Verweisung allein auf diese Vorschrift führt aber dazu, dass der Beschuldigte zwar einer Straftat von erheblicher Bedeutung verdächtig sein muss und wegen Art oder Ausführung der Tat, der Persönlichkeit des Beschuldigten oder sonstiger Erkenntnisse die Gefahr neuer, erheblicher Straftaten besteht. Dies wird aber nach der derzeitigen Rechtslage auch durch die Polizei oder die Staatsanwaltschaft beurteilt und entschieden und nicht zwingend ausschließlich durch den Richter. Diese Gesetzeslücke sollte geschlossen werden.

7.3.4 DNA-Massenscreening

Soll der DNA-Massentest gesetzlich geregelt werden?

Sog. „Massengentests“, bei denen auf Basis der Einwilligung Speichelproben von hunderten oder tausenden Personen untersucht wurden, haben zur Aufklärung einiger Kapitalverbrechen beigetragen. Da die Einwilligung als Rechtsgrundlage für den DNA-Massentest problematisch ist, habe ich für eine klarstellende gesetzliche Regelung plädiert, die die rechtsstaatlichen Rahmenbedingungen eines DNA-Massentests festlegt (vgl. 19. TB Nr. 8.2.3.2.). Wichtig ist dabei, dass DNA-Reihenuntersuchungen ultima ratio der strafprozessualen Ermittlungen bleiben müssen. Gegenüber anderen gesetzlich geregelten Ermittlungsmaßnahmen muss diese Untersuchung subsidiär sein. Anlass zu einer solchen Reihenuntersuchung darf zudem nur eine besonders schwere, gegen Leib oder Leben gerichtete Straftat sein. Der Teilnehmerkreis ist vor Durchführung der Maßnahme durch eine Fallanalyse hinreichend zu begrenzen. Keinesfalls darf die Verweigerung der Teilnahme einen Anfangsverdacht begründen. Die wirksame Einwilligung der Teilnehmer setzt sorgfältig gestaltete Formulare voraus, die insbesondere den Erhebungszweck, die Freiwilligkeit der Teilnahme und die Widerruflichkeit der Einwilligung deutlich machen sowie auf die Nutzung und Löschung der erhobenen Daten hinweisen. Ferner müssen die erhobenen Daten einer strengen Zweckbindung unterliegen. Sie dürfen deshalb nur mit den Tatortspuren abgeglichen und nicht in die DNA-Analysedatei des BKA eingestellt werden. Nutzungen für andere Zwecke müssen ausgeschlossen sein. Nach einem Negativergebnis der Analyse sind sowohl die DNA-Probe als auch das gewonnene Identifizierungsmuster zu vernichten. Die übrigen Daten der Betroffenen müssen spätestens nach Abschluss des Verfahrens gelöscht werden. Wichtig ist schließlich, dass alle Verfahrensschritte hinreichend dokumentiert werden.

Inzwischen hat der „Arbeitskreis Justiz“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Positionspapier zu den Anforderungen an die Durchführung von DNA-Reihenuntersuchungen verfasst (Kasten zu Nr. 7.3.4). Die Konferenz der Justizministerinnen und Justizminister scheint eine gesetzliche Regelung der Reihentests zu befürworten. Jedenfalls hat sie ihren Strafrechtsausschuss gebeten, eine solche gesetzliche Regelung näher zu prüfen und hierzu Vorschläge zu unterbreiten (Beschluss anlässlich der 75. Konferenz am 17. und 18. Juni 2004 TOP II.1).

Kasten zu Nr. 7.3.4

Anforderung an die Durchführung von DNA-Reihenuntersuchungen
Positionspapier des Arbeitskreises Justiz der Datenschutzkonferenz

Die rechtsstaatliche Problematik der DNA-Reihenuntersuchungen liegt in einer faktischen Umkehr der Beweislast durch Durchbrechung der Unschuldsvermutung. Gegen die Betroffenen muss nicht einmal ein Anfangsverdacht bestehen, damit sie zur Teilnahme an der Untersuchung aufgefordert werden können. Vielmehr genügt hierfür bereits die Zugehörigkeit zu einer durch ganz allgemeine Kriterien wie Wohnort und Alter umschriebenen Gruppe. Deshalb dürfen DNA-Reihenuntersuchungen nur unter strengen rechtsstaatlichen Anforderungen durchgeführt werden. Dazu gehört die Beachtung folgender Kriterien:

- Anlasstat muss eine schwere, gegen die Rechtsgüter Leib oder Leben gerichtete Straftat sein.
- Gegenüber gesetzlich geregelten Ermittlungsmaßnahmen muss die DNA-Reihenuntersuchung subsidiär sein und als ultima ratio eingesetzt werden.
- Der Teilnehmerkreis muss durch eine Fallanalyse hinreichend eingegrenzt werden. Ein Massentest „ins Blaue hinein“ kann unter keinen Umständen zulässig sein.
- Die Tests müssen im Rahmen der Verhältnismäßigkeit in konzentrischen Kreisen durchgeführt werden, soweit der Kreis nicht klar und bestimmt ist. Eine Ausweitung auf den nächstgrößeren Kreis darf jeweils nur erfolgen, wenn die Maßnahme im engeren Kreis erfolglos geblieben ist.
- Die wirksame Einwilligung der Teilnehmer setzt sorgfältig gestaltete Formulare voraus, die insbesondere deutlich auf den Erhebungszweck, die Freiwilligkeit der Teilnahme und die Widerruflichkeit der Einwilligung sowie auf die Nutzung und Löschung der erhobenen Daten hinweisen. Diese Formulare müssen vorab übersandt werden, damit die Betroffenen ihre Entscheidung hinreichend und unbeeinflusst überdenken können. Die Maßnahmen zur Durchführung der DNA-Analyse (entsprechend § 81f Abs. 2 StPO) einschließlich der zur Analyse in Frage kommenden Institute sind darzulegen. Missverständliche Hinweise auf die Möglichkeit der Erwirkung von Gerichtsbeschlüssen zur zwangsweisen Durchsetzung der Maßnahmen dürfen in keinem Fall gegeben werden.
- Die erhobenen Daten müssen einer strengen Zweckbindung unterliegen. Sie dürfen nicht mit der DNA-Analyse-Datei des Bundeskriminalamtes abgeglichen oder in diese eingestellt werden. Zweckdurchbrechende Nutzungen nach §§ 474 ff. StPO müssen ausgeschlossen sein.
- Nach einem Negativergebnis der Analyse sind die DNA-Probe und das DNA-Muster unverzüglich zu vernichten. Die gespeicherten Daten sind zu löschen, nach Abschluss des Verfahrens auch Namen und Negativergebnis.
- Die Verweigerung der Teilnahme allein darf keinen Anfangsverdacht begründen (BVerfG, NJW 1996, S. 3071 ff). Sie rechtfertigt es auch nicht, die Betroffenen als „andere Personen“ im Sinne von § 81c StPO anzusehen.
- Die Verfahrensschritte sind hinreichend zu dokumentieren.

7.4 Zeugnisverweigerungsrechte bei heimlichen Ermittlungsmaßnahmen

Die uneinheitlichen und unvollkommenen Regelungen der Strafprozessordnung müssen durch ein stimmiges Gesamtkonzept ersetzt werden.

Die Bundesregierung hatte bereits im Jahr 2001 angekündigt, den „Schutz von Zeugnisverweigerungsberechtigten bei heimlichen Ermittlungsmaßnahmen in einem stimmigen Gesamtkonzept“ zu regeln (Bundestagsdrucksache 14/7008 S. 8). Diese umfassende Neuregelung steht leider bis heute aus, obwohl die in Auftrag gegebenen Gutachten inzwischen vorliegen.

Die Neuregelung darf nicht auf die lange Bank geschoben werden. Denn bisher sind die Zeugnisverweigerungsrechte bei den Ermittlungsmaßnahmen der Strafprozessordnung uneinheitlich und unvollkommen geregelt. So sind die Zeugnisverweigerungsrechte bei einigen Überwachungsmaßnahmen überhaupt nicht berücksichtigt, obwohl diese teilweise tief in die Rechte der Betroffenen eingreifen. Dies gilt z. B. für Telekommunikationsüberwachungsmaßnahmen nach §§ 100a, 100b StPO, bei denen auf eventuell bestehende Zeugnisverweigerungsrechte überwachter Personen nach dem Wortlaut des Gesetzes keinerlei Rücksicht genommen werden muss. Bei der Verbindungsdatenabfrage nach den §§ 100g, 100h StPO sind nur bestimmte Berufsgeheimnisträger geschützt; schon deren Berufshelfer (§ 53a StPO) sind ungeschützt, ebenso wie zeugnisverweigerungsberechtigte Angehörige. Andererseits gibt es aber auch Bereiche, in denen ein umfassender Schutz durch Beweiserhebungs- und Beweisverwertungsverbote gewährt wird, so etwa hinsichtlich der Zeugnisverweigerungsrechte sämtlicher Berufsgeheimnisträger bei der akustischen Wohnraumüberwachung nach §§ 100c Abs. 1 Nr. 3, 100d Abs. 3 StPO (vgl. Nr. 7.1.2). Bereits diese Beispiele zeigen, wie dringend ein „stimmiges Gesamtkonzept“ ist. Ich hoffe deshalb, dass dieses Vorhaben in nächster Zukunft angegangen wird und werde darauf hinwirken, dass dabei – unter Berücksichtigung auch der neuesten Rechtsprechung des Bundesverfassungsgerichts zur akustischen Wohnraumüberwachung (vgl. Nr. 7.1.1) – für alle Zeugnisverweigerungsberechtigten, also Familienangehörige nach § 52 StPO sowie Berufsgeheimnisträger und deren Berufshelfer nach §§ 53, 53a StPO ein möglichst hohes Schutzniveau erreicht wird.

Weiterführende Hinweise: vgl. vor allem das im Auftrag des BMJ erstellte und von diesem in Zusammenarbeit mit Wolter/Schenke herausgegebene Gutachten „Zeugnisverweigerungsrechte bei (verdeckten) Ermittlungsmaßnahmen“ vom September 2002)

7.5 Heimliche Bildaufnahmen (§ 201a Strafgesetzbuch)

Der neue Straftatbestand des § 201a StGB schützt den Einzelnen weitgehend vor heimlichen Bildaufnahmen in seinem Privatbereich.

Mit Gesetz vom 30. Juli 2004 (BGBl. I S. 2012) ist der neue Straftatbestand der Verletzung des höchstpersönlichen Lebensbereiches durch Bildaufnahmen in das Strafgesetzbuch eingefügt worden (§ 201a). Mit dieser Vorschrift kam der Gesetzgeber einer auch von mir erhobenen Forderung zur Schließung einer Strafbarkeitslücke nach. Anders als beim vertraulich gesprochenen Wort (§ 201 StGB) war der Einzelne vor unbefugten Bildaufnahmen bisher nicht ausreichend strafrechtlich geschützt (vgl. 19. TB Nr. 8.1).

Die gesetzliche Regelung stellt einen Kompromiss dar und enthält deshalb Einschränkungen des Schutzbereiches in räumlicher Hinsicht. Nicht jedes Herstellen, Übertragen, Gebrauchen oder Zugänglichmachen einer Bildaufnahme, das den höchstpersönlichen Lebensbereich einer Person verletzt, ist unter Strafe gestellt, sondern nur dann, wenn Personen sich innerhalb einer Wohnung oder einem gegen Einblick besonders geschützten Raum aufhalten. Dabei muss es sich laut Begründung zum Gesetzentwurf nicht notwendig um einen umschlossenen Raum im Sinne des § 243 Abs. 1 Nr. 1 StGB handeln, sondern der Schutz kann sich z. B. auch aus einer dichten Hecke oder Mauer ergeben. Befinden sich Personen in der Öffentlichkeit, bleiben die beschriebenen Handlungen nach wie vor straffrei. Dies bedeutet, dass etwa die Herstellung einer Bildaufnahme von einer Person, die sich in einer Umkleidekabine aufhält, strafbar ist, während z. B. reißerische Aufnahmen von Unfallorten und Unfallopfern weiterhin straflos bleiben.

7.6 Jugendstrafvollzugsrecht – in einem Gesetz zusammengefasst

Das BMJ hat einen Gesetzentwurf vorgelegt, der den Jugendstrafvollzug erstmals zusammenfassend regelt.

Der Jugendstrafvollzug ist bisher in verschiedenen Gesetzen geregelt. So sind beispielsweise die Grundsätze und einige organisatorische Bestimmungen im Jugendgerichtsgesetz und das Arbeitsentgelt, die Ausbildungsbeihilfe sowie der unmittelbare Zwang im Strafvollzugsgesetz (StVollzG) enthalten. Das BMJ hat nun einen Gesetzentwurf zur Regelung des Jugendstrafvollzuges (GJVollz-E) vorgelegt, in dem die Rechte und Pflichten der jungen Gefangenen sowie die Eingriffsbefugnisse und Leistungspflichten der Vollzugsbehörden zusammengefasst sind.

Grundsätzlich begrüße ich diesen Entwurf, allerdings erscheinen mir insbesondere drei Regelungen bedenklich:

§ 37 Abs. 4 GJVollz-E sieht vor, dass die Vollzugsbehörde im Rahmen der Einbeziehung fachbezogener außervollzuglicher Einrichtungen und Organisationen nach § 7 GJVollz-E personenbezogene Daten der Gefangenen grundsätzlich nur mit deren Einwilligung übermitteln darf. Eine Datenübermittlung ohne Einwilligung der Gefangenen soll aber auch zulässig sein, wenn die Vollzugskonferenz deren Erforderlichkeit festgestellt hat. Auch wenn die Übermittlung personenbezogener Daten der jungen Gefangenen an Jugendämter, Schulen, Einrichtungen für berufliche Bildung etc. sachgerecht sein mag, halte ich den Kreis der nach § 7 GJVollz-E einzubeziehenden außervollzuglichen Einrichtungen und Organisationen, die als Datenempfänger in Betracht kommen, sehr

weit gezogen und für die Gefangenen kaum überschaubar. Ich habe daher gegenüber dem BMJ angeregt, den Entwurf dahingehend zu ändern, dass die Vollzugskonferenz die Erforderlichkeit dieser Maßnahme erst feststellen darf, nachdem der Gefangene und der Personensorgeberechtigte angehört worden sind.

Der Entwurf sieht zwar vor, dass der Schriftverkehr des Gefangenen mit seinem Verteidiger und Beistand entsprechend der Vorschrift in § 29 Abs. 1 StVollzG nicht überwacht wird. Allerdings findet sich im Entwurf keine weitergehende Regelung, nach der auch Schreiben des Gefangenen an Volksvertretungen sowie deren Mitglieder, an europäische Institutionen und die Datenschutzbeauftragten nicht überwacht werden (vgl. § 29 Abs. 2 StVollzG). Dies hätte zur Folge, dass der Verkehr mit den genannten Institutionen, der bei Erwachsenen keiner Überwachung unterliegt, bei Minderjährigen untersagt werden könnte, soweit Personensorgeberechtigte nicht damit einverstanden sind. Die besondere Funktion der genannten Institutionen wird dabei nicht berücksichtigt. Das Recht auf jederzeitige Anrufung des Datenschutzbeauftragten beispielsweise ergibt sich aus dem Grundrecht auf informationelle Selbstbestimmung. Die Grundrechtsmündigkeit beginnt nicht erst mit der Volljährigkeit. Die Ausübung dieses Rechts kann deshalb nicht von der Zustimmung eines Personensorgeberechtigten abhängig gemacht werden.

Der Entwurf enthält Regelungen für die auf freiwilliger Grundlage in der Anstalt verbleibenden oder zurückkehrenden Gefangenen, die dort ihre begonnene Ausbildungs- oder Behandlungsmaßnahme abschließen oder aus fürsorgerischen Gründen zunächst dort bleiben möchten. Den Anforderungen an die Freiwilligkeit trägt der Entwurf allerdings nur unzureichend Rechnung. Ich vertrete die Auffassung, dass Eingriffe in die informationelle Selbstbestimmung, wie z. B. Besuchs- und Briefkontrollen bei den genannten Gefangenen, wenn überhaupt, nur unter deutlich engeren Voraussetzungen durchgeführt werden dürfen als vor dem Entlassungszeitpunkt. Es sollte dabei auch festgelegt werden, dass Kontrollen nur unter Beachtung der geregelten Ausbildungs-, Behandlungs- oder Fürsorgezwecke zulässig sind. Aus der Tatsache, dass sich der Betroffene freiwillig in der Anstalt befindet, darf nicht auf eine wirksame Einwilligung in künftige Kontrollen geschlossen werden.

7.7 Zentrales Staatsanwaltschaftliches Verfahrensregister (ZStV)

Die Kontroverse über den Umfang des Auskunftsanspruch aus dem ZStV ist beigelegt. Das „Gesetz zur effektiven Nutzung von Dateien im Bereich der Staatsanwaltschaften" beschränkt diesen Anspruch. Die technische Sicherheit der Kommunikation mit dem ZStV ist noch immer nicht gewährleistet.

Über einen längeren Zeitraum hinweg habe ich mit dem BMJ über den Umfang des Auskunftsanspruches aus dem ZStV kontrovers diskutiert (vgl. 18. TB Nr. 6.11.3; 19. TB Nr. 8.8). Wie berichtet, hatten einige Landesjustizverwaltungen wegen befürchteter „Ausforschungsgefahren" dem Register keine Ermittlungsverfahren gemeldet oder dies nur lückenhaft getan. Das BMJ sprach sich deshalb dafür aus, Auskünfte generell nur noch über abgeschlossene oder dem Betroffenen bereits bekannt gewordene Ermittlungsverfahren zu erteilen. Eine solche Beschränkung des Auskunftsanspruchs lehnte ich ab.

Meinen Bedenken ist teilweise Rechnung getragen worden, denn mit dem „Gesetz zur effektiveren Nutzung von Dateien im Bereich der Staatsanwaltschaften" vom 10. September 2004 (BGBl. I S. 2318) ist der Auskunftsanspruch der Betroffenen zwar eingeschränkt worden, jedoch in einer weniger weitgehenden Weise als ursprünglich vorgesehen. Bayern hatte vorgeschlagen, Auskünfte nur über abgeschlossene Verfahren zu erteilen. Dies lehnte die Bundesregierung unter Hinweis auf das Recht auf informationelle Selbstbestimmung ab. Sie schlug stattdessen vor, den Auskunftsanspruch des Betroffenen auf solche Verfahren oder Eintragungen zu beschränken, die bereits ein bestimmtes „Alter" erreicht haben, wobei die Bemessung des maßgeblichen Zeitraums gestuft nach einer von der Staatsanwaltschaft zu beurteilenden Geheimhaltungsbedürftigkeit des Verfahrens erfolgen solle. Diesem Vorschlag folgte schließlich auch der Deutsche Bundestag. Es ist demnach vorgesehen, dass über Verfahren, deren Einleitung bei der Staatsanwaltschaft im Zeitpunkt der Beantragung der Auskunft noch nicht mehr als sechs Monate zurückliegt, keine Auskunft erteilt wird. Die Staatsanwaltschaft kann diese Frist auf bis zu 24 Monate verlängern, wenn wegen der Schwierigkeit oder des Umfangs der Ermittlungen im Einzelfall ein Geheimhaltungsbedürfnis fortbesteht. Eine weitere Fristverlängerung kann durch den Generalstaatsanwalt, in Verfahren der Bundesanwaltschaft durch den Generalbundesanwalt angeordnet werden. Der Antragsteller ist auf diese generelle Verfahrensweise hinzuweisen.

Im Interesse der Funktionsfähigkeit des ZStV halte ich eine Auskunftsbeschränkung, gestaffelt nach dem Alter der Eintragung und des Geheimhaltungsbedürfnisses, zwar für vertretbar. Entgegen meinem Vorschlag wurde jedoch nicht die entsprechende Vorschrift im Abschnitt über das ZStV geändert (§ 495 StPO), sondern die für alle staatsanwaltschaftlichen Register geltende (§ 491 StPO). Die Regelung des § 495 StPO enthält nur eine Verweisung hierauf. Bisher richtete sich der Auskunftsanspruch von Verfahrensbeteiligten nicht nach § 491 StPO, sondern nach § 487 Abs. 2 StPO. Es ist nicht abzusehen, was dies in Bezug auf Verfahrensbeteiligte bedeutet, die in Zukunft Auskunft aus „normalen" staatsanwaltschaftlichen Registern begehren. Kritisch sehe ich außerdem, dass das Gesetz entgegen meinen mehrfach vorgetragenen Anregungen keine Höchstfrist für die Auskunftsbeschränkung vorsieht. Es ist deshalb zu befürchten, dass in Einzelfällen der Auskunftsanspruch völlig leer laufen wird.

In technischer Hinsicht wurde die von mir mehrfach angemahnte (vgl. 18. TB Nr. 6.11.3; 19. TB Nr. 8.8) „Ende-zu-Ende-Verschlüsselung" der zum und vom ZStV übermittelten Daten leider immer noch nicht umgesetzt. Ich hoffe, dass der nunmehr angekündigte Pilotbetrieb der vom Bundeszentralregister entwickelten IPSec-Implementierungslösung zügig aufgenommen werden wird.

7.8 Bundeszentralregister

Bei Kontrollen habe ich keine schwerwiegenden Mängel bei den durch das BZR erteilten Auskünften festgestellt.

Anlässlich mehrerer Informations- sowie Beratungs- und Kontrollbesuche bei der Dienststelle Bundeszentralregister des Generalbundesanwalts beim Bundesgerichtshof (BZR) habe ich Einzelfälle aufgrund von Petenteneingaben erörtert und eine Ablaufkontrolle der Auskunftsersuchen aus dem Register und Eintragungen in das Register durchgeführt. Schwerwiegende datenschutzrechtliche Mängel habe ich dabei nicht festgestellt, meine Anregungen wurden aufgegriffen. Allerdings konnten die beim BZR vorgesehenen umfassenden Änderungen aufgrund technischer Probleme sowie neuer Anforderungen aus den Fachbereichen bisher nicht vollständig realisiert werden. Dies wird erst im Laufe des Jahres 2005 möglich sein. Ich habe deshalb mit dem BZR weitere Gespräche vereinbart.

7.9 Europäische Zusammenarbeit in Strafsachen

7.9.1 Eurojust

Das Eurojust-Gesetz, durch das die nationale Ermächtigungsgrundlage für die Informationsübermittlung an Eurojust geschaffen wurde, lässt einige Wünsche offen.

Eurojust, durch Beschluss des Rates der Europäischen Union vom 28. Februar 2002 errichtet, hat im Dezember 2002 seine Arbeit aufgenommen. Der Ratsbeschluss musste auch in Deutschland umgesetzt werden, denn er ist zwar für alle EU-Mitgliedstaaten verbindlich, auf innerstaatlicher Ebene jedoch nicht unmittelbar wirksam (vgl. Artikel 34 Abs. 2 Satz 2 lit. c EU-Vertrag). Insbesondere war die Schaffung von Ermächtigungsgrundlagen für die Datenübermittlung nationaler Behörden an Eurojust notwendig (vgl. 19. TB Nr. 8.9). Die Umsetzung erfolgte durch das Eurojust-Gesetz (EJG), das am 18. Mai 2004 in Kraft trat (BGBl. I S. 902 ff.). Neben Normen, die die Informationsübermittlung an Eurojust regeln, enthält das Gesetz vor allem Regelungen zu Rechten und Pflichten des nationalen Eurojust-Mitgliedes.

Bei den Beratungen des Gesetzes wurden meine Forderungen nur zum Teil berücksichtigt. So halte ich etwa die Vorschrift zur Informationsübermittlung (§ 4 Abs. 1 EJG) für zu unbestimmt. Aus ihr ist für die übermittelnden Stellen nicht hinreichend ersichtlich, in welchen Fällen eine Datenübermittlung konkret zulässig ist. Weiter hatte ich darauf hingewiesen, dass das in § 7 Abs. 1 Satz 4 EJG gewährte Recht der nationalen Anlaufstellen, die Informationen in Arbeitsdateien zu verwenden, nur unvollständig geregelt ist. Ich halte es nicht für ausreichend, die erforderlichen datenschutzrechtlichen Regelungen in einer Rechtsverordnung zu treffen und hätte es deshalb begrüßt, wenn im Gesetz selbst datenschutzrechtliche Regelungen, etwa zu Speicherungs- und Löschungsfristen, aufgenommen worden wären. Aufgrund der von mir geäußerten Bedenken wurde im parlamentarischen Verfahren lediglich § 7 Abs. 1 EJG noch um folgenden Satz ergänzt: „Dem Schutz personenbezogener Daten ist angemessen Rechnung zu tragen.“ In der Eurojust-Anlaufstellen-Verordnung vom 17. Dezember 2004 (BGBl. I S. 3520), die neben datenschutzrechtlichen Regelungen insbesondere auch die Benennung des Generalbundesanwalts (GBA) als nationale Terrorismus-Anlaufstelle für Eurojust enthält, wurden jedoch einige von mir eingebrachte Vorschläge berücksichtigt, so etwa hinsichtlich der Zweckbestimmung der beim GBA einzurichtenden Datei sowie der Verpflichtung, durch technische und organisatorische Maßnahmen eine Trennung dieser Datei von sonstigen Dateien und Registern zu gewährleisten.

Kasten zu Nr. 7.9.1

Die Aufgaben von Eurojust

Eurojust soll bei bestimmten Delikten der schweren und insbesondere der Organisierten Kriminalität (z. B. aus dem Bereich des Terrorismus, des illegalen Drogenhandels, der Computerkriminalität), sofern zwei oder mehr Mitgliedstaaten betroffen sind,

- die Koordinierung der in den Mitgliedstaaten laufenden Ermittlungen und Strafverfolgungsmaßnahmen zwischen den zuständigen nationalen Behörden fördern,
- die Zusammenarbeit zwischen den zuständigen nationalen Behörden verbessern, insbesondere die internationale Rechtshilfe und die Erledigung von Auslieferungsersuchen erleichtern,
- die zuständigen nationalen Behörden anderweitig mit dem Ziel unterstützen, die Wirksamkeit ihrer Ermittlungen und Strafverfolgungsmaßnahmen zu erhöhen.

7.9.2 Neueste Entwicklungen

Der Grundsatz der gegenseitigen Anerkennung von Entscheidungen in Strafsachen gefährdet die Schutzrechte des Einzelnen.

Die Rechtsetzung der EU zur Verwirklichung eines Raumes der Freiheit, der Sicherheit und des Rechts im strafrechtlichen Bereich schreitet voran. Ich befürworte eine Verbesserung der europäischen Zusammenarbeit in Strafsachen, beobachte aber mit Sorge, dass die Schutzrechte des Einzelnen dabei in den Hintergrund zu treten drohen. Die gegenseitige Anerkennung von Entscheidungen in Strafsachen, die vom Europäischen Rat zum „Eckstein“ der justiziellen Zusammenarbeit erklärt wurde, birgt die Gefahr einer europaweiten Durchsetzung der jeweils strengsten Strafrechtsordnung. Ich halte es daher für unabdingbar, dass dabei auch die Rechte des Einzelnen umfassend berücksichtigt werden. Soweit der Datenschutz betroffen ist, gilt leider nach wie vor, dass im Bereich der sog. Dritten Säule erhebliche Defizite bestehen. Es liegt ebenfalls im Interesse einer verbesserten europäischen justiziellen Zusammenarbeit, dass auch auf diesem Gebiet gemeinsame hohe datenschutzrechtliche Standards gewährleistet werden (vgl. auch Nr. 3.2.6).

Als eine der ersten Maßnahmen im Bereich der gegenseitigen Anerkennung in Strafsachen wurde der **Europäische Haftbefehl** geschaffen, der durch das „Gesetz zur Umsetzung des Rahmenbeschlusses über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten der Europäischen Union“ vom 21. Juli 2004 (BGBl. I S. 1748) in nationales Recht umgesetzt wurde. Inzwischen hat das Bundesverfassungsgericht bereits am 24. November 2004 (2 BvR 2236/04) im Wege einer einstweiligen Anordnung die erste Auslieferung aufgrund eines Europäischen Haftbefehls ausgesetzt. Man darf gespannt sein, inwiefern die noch ausstehende Entscheidung über die zugrunde liegende Verfassungsbeschwerde Konsequenzen für das Instrument des Europäischen Haftbefehls und möglicherweise auch für andere Maßnahmen der gegenseitigen Anerkennung haben wird.

Auf das Prinzip der gegenseitigen Anerkennung stützt sich auch der Vorschlag der Europäischen Kommission für einen Rahmenbeschluss über die **Europäische Beweisanordnung** zur Erlangung von Sachen, Schriftstücken und Daten zur Verwendung in Strafverfahren (KOM(2003) 688 endg.; Ratsdok. 15221/03). Diese Maßnahme, die eine zügigere und effizientere justizielle Zusammenarbeit in Strafsachen ermöglichen soll, ist äußerst problematisch, worauf ich das BMJ sowie den Rechtsausschuss des Bundestages in einer gemeinsamen Stellungnahme mit den Datenschutzbeauftragten der Länder hingewiesen habe. So ist die Verwendungsregelung für personenbezogene Daten in Artikel 10 Abs. 1 des Vorschlags zum Teil weiter gefasst als die Zweckbindungsvorschriften des deutschen Rechts. Während etwa nach der Strafprozessordnung Daten, die aus bestimmten heimlichen Überwachungsmaßnahmen erlangt wurden, nur in solchen Strafverfahren verwendet werden dürfen, die bestimmte Katalogtaten betreffen, können nach dem Vorschlag derartige im Vollstreckungsstaat bereits erhobenen Daten auch zur Verfolgung geringfügiger Straftaten oder sogar für Ordnungswidrigkeitenverfahren im Anordnungsstaat verwendet werden. Es besteht damit die Gefahr, dass nationale Zweckbindungsstandards im justiziellen Bereich ausgehöhlt werden. Fraglich ist auch, ob Zeugnisverweigerungsrechte und Beschlagnahmeverbote angemessene Beachtung finden. Besonderen Grund zur Sorge bereitet schließlich die in der Begründung des Vorschlags aufgezeigte Zukunftsperspektive eines für sämtliche – insbesondere auch für erst noch zu erhebende – Beweismittel geltenden gemeinsamen Instruments. Dieses würde noch tiefer in die Grundrechte eingreifen, da es etwa auch die Durchführung von Telekommunikationsüberwachungen oder DNA-Analysen auf einem weitaus niedrigerem als dem derzeitigen nationalen Sicherungsniveau erlauben würde. Ich begrüße daher, dass sich auch der Bundestag in seiner Stellungnahme gegenüber der Bundesregierung kritisch zu dem Vorschlag der Kommission geäußert und Ergänzungen u. a. auch in datenschutzrechtlicher Hinsicht gefordert hat (Bundestagsdrucksache 15/3831).

Als Reaktion auf die Anschläge von Madrid am 11. März 2004 hat die Kommission die Einrichtung eines **Europäischen Strafregisters** erwogen (KOM(2004) 221 endg.; Ratsdok. 8200/04). Einem solchen Register stehe ich sehr zurückhaltend gegenüber, da ein dem deutschen Recht entsprechender Datenschutzstandard kaum realisierbar sein dürfte und es zu einer doppelten Datenspeicherung käme. Akzeptabel erscheint mir hingegen der Vorschlag des BMJ sowie schließlich auch des Rates der Justiz- und Innenminister der EU, statt eines zentralen europäischen Registers – entsprechend einem derzeit zwischen Deutschland, Frankreich und Spanien laufenden Projekt – eine Vernetzung der bestehenden nationalen Strafregister anzustreben, soweit dabei die Rechte der Betroffenen gewährt bleiben. Dem Ziel, den Informationsaustausch zwischen den Strafverfolgungsbehörden der EU-Mitgliedstaaten zu erleichtern, dient zudem die sog. „Schwedische Initiative“, über die ich unter Nr. 3.3.4 berichtet habe.

Angesichts uneinheitlicher verfahrensrechtlicher Standards in den einzelnen Mitgliedstaaten begrüße ich das Grundanliegen eines weiteren Vorschlags der Kommission für einen Rahmenbeschluss des Rates über bestimmte Verfahrensrechte in der Europäischen Union (KOM(2004) 328 endg.; Ratsdok. 9318/04), der gemeinsame Mindestnormen festlegen soll. Allerdings enthält der Vorschlag Regelungen zu Audio- und Videoaufzeichnungen, die nach datenschutzrechtlichen Maßstäben äußerst lückenhaft sind. Zumindest aber müsste meines Erachtens nach Art und Schwere des Tatvorwurfs sowie nach der Bedeutung der Aussage für das Verfahren differenziert werden. Außerdem wären Ergänzungen betreffend Löschungs- und Zweckbindungsvorschriften sowie den Ausschluss von Vervielfältigungen erforderlich. Hierauf habe ich im Einvernehmen mit den Datenschutzbeauftragten der Länder das BMJ hingewiesen, welches ebenso wie der Bundesrat (Bundesratsdrucksache 409/04) meine Auffassung im Wesentlichen teilt.

7.10 Papierakte ade – Justiz goes online

Mit dem Gesetzentwurf eines Justizkommunikationsgesetzes (JKomG) sollen elektronische Kommunikationsformen gleichberechtigt neben die herkömmlichen Mitteilungsformen treten.

Ein Gesetzentwurf der Bundesregierung vom 28. Oktober 2004 (Bundestagsdrucksache 15/4067) soll die Justiz weiter für den elektronischen Rechtsverkehr öffnen (vgl. 19. TB Nr. 8.10.2). Danach sollen mit dem JKomG die Voraussetzungen für eine umfassende elektronische Aktenbearbeitung innerhalb der Gerichte ermöglicht werden. Ziel ist die Gleichbehandlung der bisherigen schriftlichen und mündlichen Form mit der neuen elektronischen Form. Im elektronischen Rechtsverkehr wird durch elektronische Signaturen die Identität und Authentizität einer Willenserklärung gewährleistet. Um die herkömmlichen Formerfordernisse auf die elektronische Arbeit zu übertragen, unterscheidet der Gesetzentwurf zwischen einfacher, fortgeschrittener, qualifizierter oder einer elek-

tronischen Signatur, die auf einem dauerhaft überprüfbaren Zertifikat beruht. Es soll sichergestellt werden, dass ein Zertifikat so lange überprüfbar ist, wie es das Verfahren erforderlich macht. Derzeit bieten nur akkreditierte Zertifizierungsdienstleister (sog. Trustcenter) derartige Zertifikate an.

Erfreulich ist, dass das JKomG auch Regelungen über die Aufbewahrung von Schriftgut der Gerichte, Staatsanwaltschaften und Justizvollzugsbehörden nach Beendigung des Verfahrens enthält. Damit wird eine Forderung der Datenschutzbeauftragten des Bundes und der Länder erfüllt (vgl. Entschließung der 58. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, 18. TB Anlage 16 zu Nr. 6.15). Der Entwurf koppelt die Aufbewahrungsfristen an den Zweck der Aufbewahrung unter Berücksichtigung des Verhältnismäßigkeitsgrundsatzes. Die Länder werden ermächtigt, die konkrete Dauer der Aufbewahrungsfristen durch Rechtsverordnung festzulegen.

7.11 Zentrales Vorsorgeregister der Bundesnotarkammer

Die Bundesnotarkammer hat ein zentrales Register über Vorsorgevollmachten zu führen. Dabei sind auch die schutzwürdigen Belange der registrierten Bevollmächtigten angemessen zu berücksichtigen.

Eine Krankheit oder ein Unfall können dazu führen, dass man seine persönlichen Dinge nicht mehr selbst regeln kann und auf die Mitwirkung anderer angewiesen ist. Der nächste Verwandte bzw. Ehegatte oder Lebensgefährte kann in solchen Situationen nicht automatisch rechtlich an die Stelle der betroffenen Person treten. Das Vormundschaftsgericht müsste in einer solchen Situation ein Betreuungsverfahren einleiten. Dies kann zu dem Ergebnis führen, dass dritte Personen ein Entscheidungsrecht erhalten, was nicht immer im Interesse des Betroffenen liegt.

Durch eine Vorsorgevollmacht erhält der Bevollmächtigte das Recht, in allen persönlichen und vermögensrechtlichen Angelegenheiten zu entscheiden, die aus dem Notfall heraus entstehen. Gegenstand der Vorsorgevollmacht können z. B. sein: Gesundheitsfürsorge, Vermögensverwaltung, Regelungen über den Aufenthaltsort (Einweisung in Krankenhaus oder Pflegeheim), Fragen der Heilbehandlung. Das Problem in der Praxis besteht darin, dass der in Form der Vorsorgevollmacht erklärte Wille des Betroffenen im Notfall nicht immer aufzufinden ist. Um dem Selbstbestimmungsrecht des Betroffenen Geltung zu verschaffen, sollen die Vormundschaftsgerichte über eine zentrale Registerstelle Auskunft erhalten, ob eine Vorsorgevollmacht existiert und wer der Bevollmächtigte ist. Mit diesem soll sich das Gericht dann in Verbindung setzen.

Bei der Bundesnotarkammer (BNotK) wurde bisher ein Register nur für solche Vorsorgevollmachten geführt, die vor einem Notar abgegeben worden waren. Um eine zentrale Registrierung auch der privatschriftlichen Vorsorgevollmachten zu ermöglichen, wurde § 78a der Bundesnotarordnung (BNotO) dahingehend geändert, dass die BNotK die Pflicht hat, ein automatisiertes Register über alle Vorsorgevollmachten zu führen (BGBl. 2004 I S. 599). Die Einzelheiten soll eine Rechtsverordnung regeln. Umstritten war, ob und wie der Bevollmächtigte an der Registrierung seiner personenbezogenen Daten zu beteiligen ist. Nach § 4 Abs. 1 BDSG ist eine Datenerhebung nur zulässig, wenn das BDSG oder eine andere Rechtsvorschrift dies erlaubt oder der Betroffene eingewilligt hat. In § 78a Abs. 1 Satz 2 BNotO ist nur geregelt, dass in dem Register der BNotK Angaben über Bevollmächtigte aufgenommen werden. Näheres zu Art und Umfang der Daten und dem Zweck der Datenerhebung enthält das Gesetz nicht. Ich halte es daher für fraglich, ob diese Vorschrift den Anforderungen an eine Datenerhebungsnorm entspricht, die das Bundesverfassungsgericht in seinem Volkszählungsurteil (BVerfGE 65, 1 ff.) aufgestellt hat.

Ich habe mich dafür eingesetzt, dass die zum zentralen Register zu erlassende Rechtsverordnung eine Beteiligung der Bevollmächtigten vorsieht. Die Ansichten über das „Wie“ der Beteiligung waren auf Bundes- und Landesebene sehr unterschiedlich. Der erste Entwurf der Rechtsverordnung durch das BMJ sah eine Einwilligung des Bevollmächtigten vor. Hiergegen wurde seitens der Bundesländer vorgebracht, dass die sog. Einwilligungslösung ein zu aufwändiges Verfahren darstelle, das den Erfolg und die Akzeptanz des Registers gefährden würde. Das BMJ legte daraufhin dem zweiten Entwurf der Rechtsverordnung die sog. Widerspruchslösung zu Grunde. Danach sollten die Daten des Bevollmächtigten dann eingetragen werden, wenn er nach vorheriger Information nicht innerhalb einer bestimmten Frist widersprochen hat. Angesichts der Tatsache, dass das Register keine sensiblen Daten beinhaltet und nur einer überschaubaren Anzahl von Vormundschaftsgerichten Auskunft erteilt wird, ist das Missbrauchsrisiko der Registerdaten relativ gering. Aus diesem Grunde hätte ich die Widerspruchslösung mittragen können. Doch auch gegen das Widerspruchsmodell wandte sich die überwiegende Zahl der Bundesländer. Als neues Argument wurde vorgetragen, dass die mit der verwaltungsmäßigen Vor- und Nachbearbeitung der Widersprüche verbundenen Mehrarbeiten zu erhöhten Kosten bei der BNotK und damit zu einer Gebührenerhöhung zu Lasten der Vollmachtgeber führen würden. Die Bundesländer sprachen sich stattdessen in großer Mehrheit für eine Benachrichtigungslösung aus. Dieses Verfahren sieht vor, dass die Bevollmächtigten nach der Speicherung ihrer Daten schriftlich informiert werden.

Da der Bevollmächtigte bei diesem Verfahren im Gegensatz zur Einwilligungs- oder Widerspruchslösung erst nach vollzogener Datenspeicherung in Kenntnis gesetzt wird, habe ich meine Bedenken gegen dieses Modell angemeldet. Ich hoffe, dass diese im weiteren Gesetzgebungsverfahren angemessen berücksichtigt werden.

7.12 Überwachung des Internet durch Provider?

Zwei Gesetzgebungsvorhaben führten zu heftigen Diskussionen darüber, ob Internetprovider verpflichtet werden können, Inhabern von Urheberrechten Auskunft über die hinter einer IP-Adresse stehenden Kunden zu erteilen.

Das Phänomen ist bekannt: Um in den Genuss von Musikstücken oder Filmwerken zu gelangen, wird von einigen Internetnutzern auf sog. Tauschbörsen zurückgegriffen. Um Urheberrechtsverstöße im Internet verfolgen zu können, wenden sich die Rechteinhaber bisweilen an die Internetzugangsprovider und fordern diese auf, den Kunden, der mit einer bestimmten dynamischen IP-Adresse auffällig geworden ist, namentlich zu benennen. Denn i. d. R. vergeben die Provider eine bestimmte IP-Adresse nur für eine Internetsession, also dynamisch, und nicht dauerhaft. Anhand von Protokolldateien, in denen aufgezeichnet wird, welcher Kunde zu welchem Zeitpunkt welche IP-Adresse zugewiesen bekommen hat, ist es den Providern in vielen Fällen möglich, den hinter der IP-Adresse stehenden Kunden zu identifizieren. Da die Provider solchen Auskunftsanforderungen regelmäßig nicht nachkommen und eine ausdrückliche Gesetzesgrundlage für einen solchen Anspruch gegen einen (unbeteiligten) Dritten nicht existiert, stellt sich die Frage, ob der Gesetzgeber regelnd eingreifen soll. Diese Überlegung wurde sowohl auf europäischer wie auf nationaler Ebene diskutiert. Da die Daten über die Nutzung des Internet dem Fernmeldegeheimnis unterliegen, ist ihre Herausgabe ohne eine spezialgesetzliche Regelung aus meiner Sicht nicht zulässig (vgl. Nr. 7.12.2).

7.12.1 IPR-Enforcement-Richtlinie

Die Richtlinie 2004/48/EG des Europäischen Parlaments und des Rates vom 29. April 2004 zur Durchsetzung der Rechte des geistigen Eigentums (sog. IPR-Enforcement-Richtlinie) harmonisiert Verfahren und Rechtsbehelfe, mit denen Rechte des geistigen Eigentums sichergestellt werden sollen. Artikel 8 der Richtlinie enthält einen Auskunftsanspruch gegenüber Personen und Stellen, die an der Verbreitung urheberrechtsgeschützten Materials mitwirken. Die Mitgliedstaaten müssen danach sicherstellen, dass die zuständigen Gerichte in einem Verfahren wegen Verletzung eines Rechts des geistigen Eigentums auf einen begründeten und die Verhältnismäßigkeit wahrenden Antrag des Klägers hin anordnen können, dass Auskünfte über den Ursprung und die Vertriebswege von Waren oder Dienstleistungen, die ein Recht des geistigen Eigentums verletzen, auch von bestimmten anderen Personen außer dem eigentlichen Verletzer erteilt werden. Der endgültige Wortlaut der Richtlinie enthält gegenüber dem ursprünglichen Entwurf einige datenschutzrechtliche Verbesserungen, die auch auf Grund meiner Anregungen erreicht werden konnten.

Die Richtlinienvorgaben bedeuten für den nationalen Gesetzgeber, dass ein Auskunftsanspruch nur im Rahmen eines bereits anhängigen Klageverfahrens gegen einen namentlich bekannten Rechtsverletzter möglich sein wird (Richtervorbehalt). Ein Verfahren gegen Unbekannt, welches eine Ausforschung durch den Rechteinhaber möglich machen würde, ist damit nicht vorgesehen. Der Auskunftsanspruch besteht auch nur gegenüber gewerblich handelnden Dritten, also nicht gegenüber Privatpersonen. Erfreulich ist schließlich auch der Verzicht auf eine im Entwurf enthaltene Regelung, wonach Zoll- und Polizeibehörden Informationen, die sie im Zusammenhang mit einer Rechtsverletzung erlangen, automatisch an die Rechteinhaber übermitteln sollten, um diese in die Lage zu versetzen, rechtliche Schritte gegen die Betroffenen einzuleiten.

7.12.2 „Zweiter Korb“ der Novellierung des Urheberrechts

Im Zusammenhang mit der Novellierung des Urheberrechts hat sich der Gesetzgeber bereits intensiv mit einem Auskunftsanspruch gegen Internetprovider auseinandergesetzt. In einem „Ersten Korb“ wurde das Urheberrecht am 13. September 2003 novelliert und damit die EG-Richtlinie 2001/29/EG vom 22. Mai 2001 zum Urheberrecht in der Informationsgesellschaft (teilweise) umgesetzt (Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft, BGBl. I S. 1774). Alles, was auf Grund der Richtlinie nicht zwingend fristgemäß von den Mitgliedstaaten umzusetzen war, blieb der weiteren Regelung in einem „Zweiten Korb“ vorbehalten. An den Beratungen zu diesem „Zweiten Korb“ war ich beteiligt. Bis zum Abschluss der Beratungen war offen, ob es einen gesetzlich verankerten Auskunftsanspruch gegenüber Internetprovidern geben soll. Der im September 2004 vom BMJ vorgelegte Referentenentwurf zur Änderung des Urheberrechts brachte dann Klarheit: Ein Auskunftsanspruch ist nicht vorgesehen.

Dies ist aus folgenden Gründen, die ich auch gegenüber dem BMJ vorgetragen hatte, zu begrüßen: IP-Adressen, die für die Inanspruchnahme des Internet vom Zugangsprovider vergeben und aufgezeichnet werden und eine Identifizierung eines Rechteverletzers ermöglichen, sind als Verkehrsdaten i.S.d. Telekommunikationsgesetzes zu beurteilen und unterliegen deshalb dem Fernmeldegeheimnis. Ein zivilrechtlicher Auskunftsanspruch würde letztlich dazu führen, dass alle Verkehrsdaten verpflichtend über einen unbegrenzten Zeitraum gespeichert und zum Abruf bereitgehalten werden. Das geltende Telekommunikationsrecht lässt aber eine Speicherung nur zu bestimmten abschließend aufgeführten Zwecken zu (vgl. Nr. 13.1.1). Soweit die Verkehrsdaten für diese Zwecke, insbesondere für die Abrechnung und den Aufbau weiterer Verbindungen nicht erforderlich sind, müssen sie nach Beendigung der Verbindung unverzüglich gelöscht werden. Die Speicherung von IP-Adressen über den gesetzlich vorgegebenen Rahmen hinaus wäre eine unzulässige Vorratsdatenspeicherung.

Vor dem Hintergrund, dass aufgrund des gesetzlichen Auskunftsanspruchs nach §§ 100g, 100h Strafprozessordnung bereits ein wirksames Instrument zum Zugriff auf Verkehrsdaten für Zwecke der Strafverfolgung vorhanden

ist, sollte auf einen solchen erheblichen zusätzlichen Eingriff verzichtet werden. Zudem würde eine unbegrenzte Speicherung und Vorhaltung der IP-Adressen die unbeobachtete Nutzung des Internet als Kommunikationsmittel der freien Gesellschaft erheblich gefährden. Der Missbrauch des Mediums Internet durch einen kleinen Personenkreis darf nicht zu einer „Kriminalisierung“ und Überwachung sämtlicher Internetnutzer führen.

Es bleibt abzuwarten, ob und wie das BMJ Artikel 8 der IPR-Enforcement-Richtlinie möglicherweise in einem „Dritten Korb“ umsetzen wird. Meine Position habe ich deutlich gemacht. Sie gilt unverändert.

7.13 Verbesserter Schutz für Kapitalanleger

Mit einem Kapitalanleger-Musterverfahrensgesetz (KapMuG) sollen „Massenprozesse“ im Kapitalmarktbereich erleichtert werden. Die Beteiligten sollen vom Gericht in ein elektronisches Klageregister eingetragen werden.

Die Bundesregierung hat einen Gesetzentwurf vorgelegt, der vorsieht, dass Kapitalanleger, die wegen falscher Kapitalmarktinformationen Schadensersatzansprüche geltend machen, die Einleitung eines Musterverfahrens beantragen können. Der Musterfeststellungsantrag soll vom Gericht in einem neuen Klageregister im elektronischen Bundesanzeiger öffentlich bekannt gemacht werden. Werden zehn oder mehr Musterfeststellungsanträge innerhalb von vier Monaten gestellt, die dieselbe Musterfrage zum Gegenstand haben, soll das Prozessgericht einen Musterentscheid beim zuständigen Oberlandesgericht einholen. Der Musterentscheid bindet die am Verfahren Beteiligten und wird zur Grundlage der Entscheidung im jeweiligen Einzelprozess vor dem Landgericht.

Um die Klagen bzw. die Ansprüche der geschädigten Anleger zu bündeln und dadurch Kosten zu sparen, soll das elektronische Klageregister für jedermann über das Internet einzusehen sein. Interessierte sollen jederzeit feststellen können, wer in welcher Sache mit welchem Ziel klagt, um sich dann für oder gegen eine eigene Klage zu entscheiden. Der ursprüngliche Gesetzentwurf sah vor, dass sowohl der Name des Antragstellers als auch des Antragsgegners öffentlich über das Klageregister bekannt gemacht werden. Damit wäre es in jedem Fall auch zu einer Veröffentlichung des Namens des geschädigten Kapitalanlegers im Internet gekommen. Abgesehen davon, dass dem Kläger durch eine solche Bekanntmachung im Internet Nachteile entstehen könnten, ist dieser Personenbezug auf Anlegerseite zur Erreichung des Gesetzeszwecks nicht erforderlich.

Daher begrüße ich es, dass mein Vorschlag, als Zuordnungsmerkmal anstelle des Namens das gerichtliche Aktenzeichen des Rechtsstreits zu verwenden, in den Regierungsentwurf übernommen wurde. Bekannt zu machen sind danach nur noch Name und Anschrift des Beklagten. Beklagter wird in der Regel die Bank oder ein sonstiges Unternehmen des Kapitalmarktes sein. Ich hatte darauf hingewiesen, dass es auch Fallkonstellationen geben kann, in denen der Kapitalanleger in der Rolle des Beklagten ist. In diesem Fall müssten streng genommen seine personenbezogenen Daten (Name und Anschrift) im Klageregister bekannt gemacht werden. Da die Angabe der Daten des Anlegers nicht erforderlich ist, besteht an dieser Stelle noch Nachbesserungsbedarf.

7.14 Modernisierung des Zwangsvollstreckungsrechts

Durch eine Reform des Zwangsvollstreckungsrechts sollen Gläubiger in die Lage versetzt werden, Forderungen effektiver durchzusetzen. Ein Internetregister zahlungsunfähiger Schuldner darf es aber nicht geben.

Die Bund-Länder-Arbeitsgruppe „Modernisierung des Zwangsvollstreckungsrechts/des Zwangsvollstreckungsverfahrens“ befasst sich u. a. mit der Reform der Sachaufklärung bei der Vollstreckung von Geldforderungen. Nach geltendem Recht kann der Gläubiger die Aufstellung eines Vermögensverzeichnisses erst nach einem erfolglosen Vollstreckungsversuch verlangen. Dieses vorgeschaltete Verfahren hat sich als unpraktikabel erwiesen. Durch die gleichzeitige Abgabe der eidesstattlichen Versicherung, die in das Schuldnerverzeichnis eingetragen wird, droht dem Schuldner zugleich der „bürgerliche Tod“, was auch nicht im Interesse des Gläubigers liegt. Das von der Arbeitsgruppe entwickelte Konzept sieht daher vor, das gegenwärtige Verfahren zur Abnahme der eidesstattlichen Versicherung durch eine zu Beginn der Vollstreckung abzugebende Vermögensauskunft des Schuldners zu ersetzen. Die eidesstattlich bekräftigte Vermögensauskunft soll nicht mehr automatisch in das Schuldnerverzeichnis eingetragen werden.

Das berechtigte öffentliche Interesse an einer effektiven Zwangsvollstreckung darf die schutzwürdigen Belange der von diesen Maßnahmen betroffenen Personen nicht unberücksichtigt lassen. Zwei besonders kritische Gesichtspunkte des Konzepts sind hervorzuheben. Zum einen soll eine zentrale Datei eingerichtet werden, in der alle Vermögensauskünfte gespeichert werden. Zwar soll der Zugriff auf diese Vermögensauskunftsdatei nur Gerichtsvollziehern vorbehalten bleiben. Eine derartige Datei birgt aber das Risiko zukünftiger Zweckänderungen. Zum anderen beobachte ich mit Sorge, dass das Schuldnerverzeichnis nach dem Vorschlag der Arbeitsgruppe als öffentliches Register im Internet ausgestaltet werden soll. Damit würde die Zahlungsunfähigkeit des Schuldners weltweit zugänglich. Zudem stellt sich die Frage, ob und wie die im Internet veröffentlichten Angaben jemals wieder gelöscht werden können.

Den Vorschlag eines Internetregisters kann ich daher nicht unterstützen. Ich werde die weitere Entwicklung der Reformarbeiten weiterhin kritisch begleiten.

7.15 Forderungssicherungsgesetz – FoSiG

Zur Sicherung ihrer Ansprüche und zur verbesserten Durchsetzung ihrer Forderungen gegenüber einem Schuldner können Werkunternehmer künftig nicht die

Polizei um Hilfe bitten. Möglicherweise sind ihnen dabei aber bald die Sozialbehörden behilflich.

Im Februar 2003 übersandte mir das BMJ den erneut eingebrachten Bundesratsentwurf eines Gesetzes zur Sicherung von Werkunternehmeransprüchen und zur verbesserten Durchsetzung von Forderungen (Forderungssicherungsgesetz – FoSiG, Bundestagsdrucksache 14/9848). Eine darin enthaltene Vorschrift in der Zivilprozessordnung (ZPO) hätte zu Gunsten von Gläubigern vorgesehen, sich mittels einer Ausschreibung zur Aufenthaltsermittlung der Fahndungsmaßnahmen der Polizei zu bedienen und so ihre Schuldner ausfindig zu machen. Diese Regelung hätte einen schwerwiegenden Eingriff in das informationelle Selbstbestimmungsrecht des Schuldners im Hinblick auf eine wesentliche Erweiterung der Fahndung über den Bereich der Strafverfolgung hinaus dargestellt. Im weiteren Beratungsverfahren wurde diese Regelung erfreulicherweise ersatzlos gestrichen.

Auch die nunmehr vorgeschlagene Regelung, nach der Sozialdaten durch Sozialleistungsträger an Private zur Durchsetzung privatrechtlicher Ansprüche übermittelt werden dürften, halte ich für unverhältnismäßig. Bei Sozialdaten handelt es sich um besonders schutzwürdige personenbezogene Daten (§ 35 SGB I). Die Übermittlung von Sozialdaten würde einen tiefen Eingriff in das Recht auf informationelle Selbstbestimmung bedeuten.

Hilfsweise habe ich angeregt, in den Entwurf des § 68a Abs. 1 Satz 1 SGB X die vom privaten Empfänger anzugebenden Personalien des Schuldners konkret und abschließend zu bezeichnen. Schließlich habe ich eine Vorschrift empfohlen, wonach bei Auskünften gemäß § 68a SGB X die betroffenen Schuldner unter Angabe des Gläubigers unverzüglich zu unterrichten sind, soweit nicht überwiegende schutzwürdige Interessen des Empfängers entgegenstehen. Eine solche Unterrichtungspflicht ginge zwar über die Regelungen in § 21 Melderechtsrahmengesetz und § 68 SGB X hinaus, wäre jedoch sachlich gerechtfertigt. Während das Melderegister seiner originären Zweckbestimmung nach der Auskunftserteilung an Private dient, die Betroffenen daher mit Auskünften zu ihrer Person ohne weiteres rechnen müssen, werden die nach § 68a SGB X-Entwurf zu übermittelnden Daten primär für andere Zwecke erhoben. Anders als in den Fällen des § 68 SGB X würde daher bei Auskünften an private Vollstreckungsgläubiger im Einzelfall durchaus das Risiko einer missbräuchlichen Verwendung der übermittelten Daten durch den Empfänger bestehen.

Bei dem Entwurf des § 68a SGB X ist der Bundesrat leider meinen Anregungen nicht gefolgt. Lediglich die Bagatellgrenze wurde im Gegensatz zum ursprünglichen Entwurf von 600 Euro auf 3 000 Euro angehoben, um dem Verhältnismäßigkeitsgrundsatz Rechnung zu tragen und die Sozial- bzw. Zulassungsbehörden vor Auskunftsersuchen in Bagatellsachen zu schützen.

Im Herbst 2004 haben die parlamentarischen Beratungen im Deutschen Bundestag begonnen.

7.16 Veröffentlichung personenbezogener Daten in Gerichtsentscheidungen

Die Veröffentlichung von personenbezogenen Daten der Verfahrensbeteiligten ist nicht in jedem Fall erforderlich.

Bereits im 19. TB (Nr. 8.11) hatte ich mich mit der Frage befasst, inwieweit Verfahrensbeteiligte bei der Veröffentlichung von Gerichtsentscheidungen hinnehmen müssen, dass personenbezogene Daten über sie bekannt werden. In dieser Berichtsperiode wandte sich ein Petent an mich, weil der Beschluss bezüglich seiner nicht zur Entscheidung angenommenen Verfassungsbeschwerde auf der Homepage des Bundesverfassungsgerichts veröffentlicht worden war. In den Beschlussgründen wird mitgeteilt, bei welcher Landeskirche er als Geistlicher beschäftigt und in welcher Kirchengemeinde er eingesetzt ist. Zwar wird sein Nachname mit dem Anfangsbuchstaben nur abgekürzt aufgeführt. Da es sich aber um eine kleine Kirchengemeinde handelt, besteht für jedermann die Möglichkeit, die Identität des Petenten zu ermitteln.

Die genaue Angabe der Dienststelle war nicht erforderlich, da diese Information für die Entscheidung in der Sache keine Bedeutung hatte. Das BVerfG hat mir inzwischen mitgeteilt, dass die Entscheidung in seiner amtlichen Sammlung in einer auch hinsichtlich des Ortes der Kirchengemeinde anonymisierten Fassung veröffentlicht wird. Auch wird das Gericht die Entscheidung nicht auf seiner Homepage veröffentlichen und in Papierform nur in einer auch hinsichtlich des Ortes der Kirchengemeinde anonymisierten Fassung übermitteln.

8 Finanzwesen

8.1 Auskunftsrecht in der Abgabenordnung

Die Einführung eines datenschutzrechtlichen Auskunftsanspruchs in die AO lässt auf sich warten.

Zahlreiche Eingaben zeugen von dem gescheiterten Versuch, eine Auskunft über Freistellungsaufträge für Kapitalerträge beim Bundesamt für Finanzen (BfF) zu erhalten. Das BMF vertritt den Standpunkt, dass durch eine Auskunftserteilung der nach § 45d Einkommensteuergesetz (EStG) verfolgte Kontrollzweck gefährdet würde, der nur erreicht werden könne, wenn für den Betroffenen unklar bleibe, ob dem BfF tatsächlich alle freigestellten Beträge bekannt sind. Nur in Ausnahmefällen (z. B. Erbfall) wird ein berechtigtes Interesse Auskunftssuchender anerkannt. Hingegen ist das BfF nach § 19 Abs. 1 BDSG grundsätzlich zur Auskunftserteilung über die zur Person gespeicherten Daten verpflichtet, da nicht davon auszugehen ist, dass jeder nachfragende Steuerpflichtige unredliche Absichten verfolgt (vgl. 18. TB Nr. 7.6.1).

Vor diesem Hintergrund ist es dringend notwendig, das Auskunftsrecht in der AO zu verankern (vgl. 19. TB Nr. 9.1). Diese Forderung wurde durch die Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstrichen (vgl. Anlage 13). Darin haben meine Länderkollegen und ich erneut angemahnt, die Aufnahme datenschutzrechtlicher Grundsätze in die

AO unverzüglich anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen. Nach einem Anwendungserlass zu § 91 AO kann die Finanzbehörde zwar nach pflichtgemäßem Ermessen im Einzelfall Auskunft erteilen und Akteneinsicht gewähren. Dieses Ermessen kann im Einzelfall sogar auf Null reduziert sein, sodass Auskunft zu erteilen ist. Zwischen den Beteiligten in der Koordinierungsrunde AO war jedoch klar, dass ein darüber hinausgehender gesetzlicher Auskunftsanspruch in die AO aufgenommen werden sollte. Auch das BMI und das BMJ halten die Aufnahme des Auskunftsrechts in die AO für unverzichtbar.

Ein Ergebnis der Sitzung der Koordinierungsrunde AO Ende Oktober 2003 war die Zusage des BMF, ein Auskunftsrecht analog § 19 BDSG noch im Jahre 2004 in die AO aufzunehmen.

Die Gelegenheit hierfür bot sich beim „Entwurf eines Gesetzes zur Umsetzung von EU-Richtlinien in nationales Steuerrecht und zur Änderung weiterer Vorschriften (Richtlinien-Umsetzungsgesetz)“. Der Referentenentwurf vom 17. Juni 2004 enthielt in dem die AO betreffenden Artikel 8 nicht nur ein Auskunftsrecht, sondern eine allgemeine Sanktionsvorschrift bei missbräuchlicher Verwendung der steuerlichen Identifikationsnummer (vgl. Nr. 8.2 und 8.5). Die vom BMF vorgesehene Formulierung des Auskunftsanspruchs fand jedoch weder meine Zustimmung noch die von BMJ und BMI. Denn es fehlten darin z. B. die Auskunftsverpflichtungen über die Herkunft der Daten (§ 19 Abs. 1 Nr. 1 BDSG) und den Zweck der Speicherung (§ 19 Abs. 1 Nr. 3 BDSG). Die Kabinettvorlage vom 23. Juli 2004 enthielt den Hinweis, dass eine Bestimmung über den Auskunftsanspruch in das parlamentarische Verfahren eingebracht werden sollte, wenn zwischen den beteiligten Stellen eine Einigung über den Regelungswortlaut erzielt würde. Dies gelang jedoch nicht: Zwar waren in weiteren Gesprächen zwischen BMF, BMI, BMJ und mir die Auskunftserteilung über die Herkunft und den Zweck der Daten und der Verweis auf § 19 Abs. 6 BDSG bzw. entsprechende landesrechtliche Regelungen bei Verweigerung der Auskunftserteilung erreicht worden. In diesem Fall wäre die Auskunft den Datenschutzbeauftragten des Bundes und der Länder zu erteilen gewesen. Allerdings verweigerten die vom BMF eingeschalteten Länderfinanzvertreter ihre Zustimmung hierzu. Als Grund nannten sie einen befürchteten starken Anstieg von Auskunftsersuchen. Gemeinsam mit BMI und BMJ hielt ich jedoch an dem Hinweis zur Überprüfung durch die Datenschutzbeauftragten fest, da nicht ersichtlich war, dass es in den Ländern zu der befürchteten „Antragslawine“ gekommen wäre. Auch Erfahrungen etwa mit den in einigen Ländern bereits in Kraft getretenen Informationsfreiheitsgesetzen können derartige Befürchtungen nicht bestätigen.

Im Ergebnis wurde der Auskunftsanspruch nicht in das Richtlinien-Umsetzungsgesetz eingebracht. Ich habe trotzdem die Hoffnung noch nicht aufgegeben, dass die AO noch in dieser Legislaturperiode datenschutzgerecht gestaltet wird.

8.2 Identifikationsnummer für steuerliche Zwecke

Die datenschutzrechtlich problematischsten Aspekte des Steueränderungsgesetzes 2003 sind das Vorhaben der Einführung eines bundeseinheitlichen Ordnungsmerkmals (steuerliche Identifikationsnummer) und die Bildung einer Datenbank beim Bundesamt für Finanzen, die einem Zentralregister der Gesamtbevölkerung der Bundesrepublik Deutschland gleichkommt.

Das Zweite Gesetz zur Änderung steuerlicher Vorschriften (Steueränderungsgesetz 2003 vom 15. Dezember 2003, BGBl. I S. 2645 ff.) sieht die Einführung eines bundeseinheitlichen Ordnungsmerkmals vor, das der eindeutigen und raschen Identifizierung Betroffener im Steuerverfahren und damit nach Auffassung des BMF einer erheblichen Effizienzsteigerung dienen soll. Diese Identifikationsnummer (§§ 139a bis 139d Abgabenordnung – AO) soll jedoch nicht nur im steuerlichen Bereich, sondern auch von den Meldebehörden bei der Übermittlung von Daten an das Bundesamt für Finanzen (BfF) genutzt werden, wofür beim BfF eine umfangreiche Datenbank vorgesehen ist. Darin sollen künftig – das BMF spricht von einer Vorlaufzeit bis 2008 – die in § 139b Abs. 3 AO aufgeführten Daten der Steuerpflichtigen – insbesondere die aktuellen Adressen – zentral gespeichert werden. Nach § 1 Einkommensteuergesetz (EStG) fallen auch Neugeborene darunter. In dieser zentralen Datenbank als zentralem Register der Gesamtbevölkerung sehe ich das datenschutzrechtliche Hauptproblem des Steueränderungsgesetzes 2003. Ein derart umfangreiches Bevölkerungsregister weckt Begehrlichkeiten anderer Stellen.

In Ressortgesprächen wurden einige Verbesserungen erreicht, wie die Reduzierung des Datenkatalogs der Datenbank beim BfF, die Unterrichtungspflicht über die Zuteilung des Identifikationsmerkmals, die Verpflichtung der Bundesregierung, durch Rechtsverordnung „organisatorische und technische Maßnahmen zur Wahrung des Steuergeheimnisses, insbesondere zur Verhinderung eines unbefugten Zugangs zu Daten“ (§ 139d AO), zu treffen und Löschungsfristen zu bestimmen sowie die ausschließliche Übermittlungsbefugnis zwischen den Meldeämtern und dem BMF.

Ich hatte mit Schreiben vom 17. Oktober 2003 an den Finanzausschuss darauf hingewiesen, dass ich es für unbedingt erforderlich hielte, Zugriffsmöglichkeiten bzw. Auskunftsrechte öffentlicher und nicht-öffentlicher Stellen außerhalb der Finanzverwaltung durch strikte Zweckbindungen sowohl bei der Identifikationsnummer (für natürliche Personen) als auch bei der Wirtschaftsidentifikationsnummer (für wirtschaftlich handelnde natürliche Personen) auszuschließen. Nur so könne ich den Entwurf, wenn auch unter Zurückstellung weiterer Bedenken, mittragen. Meiner Empfehlung, ohne drängende Eile eine gesellschafts- und auch datenschutzpolitische Diskussion

über das Vorhaben im parlamentarischen Bereich zu führen, wollten jedoch weder die Bundesregierung noch die Koalitionsfraktionen folgen. Allerdings kam es, von Abgeordneten initiiert, zu weiteren intensiven Gesprächen mit dem BMF und dem BMJ.

Die am 5. November 2003 vom Finanzausschuss des Deutschen Bundestages mehrheitlich verabschiedete Fassung des Gesetzentwurfs enthielt nunmehr strikte Zweckbindungen (§ 139b Abs. 5 und § 139c Abs. 7 AO); sie verbieten die Verwendung der beim BfF vorgesehenen Datenbank für andere Zwecke, vor allem für Auskünfte an andere öffentliche oder nicht-öffentliche Stellen.

Darüber hinaus sagte das BMF dem Finanzausschuss zu, im Rahmen der Abstimmung der Rechtsverordnung nach § 139d AO mit den Ressorts noch offene Detailfragen unter meiner Beteiligung zu erörtern, wie beispielsweise den Zeitpunkt der Vergabe des Ordnungsmerkmals, insbesondere bei Kindern. Im Rahmen der Abstimmung der Verordnung soll zudem geklärt werden, inwieweit Bedarf für Änderungen oder Ergänzungen der gesetzlichen Regelungen besteht.

Die datenschutzrechtliche Diskussion um die steuerliche Identifikationsnummer ist damit jedoch nicht beendet. Gemeinsam mit meinen Kollegen aus den Ländern habe ich auf die Gefahr hingewiesen, dass sich aus der Einführung von einheitlichen Personennummern im Steuerbereich, aber auch im Arbeits-, Gesundheits- und Sozialbereich ein verfassungswidriges Personenkennzeichen entwickeln kann. Da einmal vorhandene Dateien leichter miteinander zu verknüpfen sind, muss verhindert werden, dass die Erschließung von Datenverbunden durch ein einheitliches Personenkennzeichen oder ein sonstiges Ordnungsmerkmal möglich wird. Das BVerfG hat im Volkszählungsurteil die Zusammenführung einzelner Lebens- und Personaldaten zur Erstellung von Persönlichkeitsprofilen der Bürgerinnen und Bürger für unzulässig erklärt (BVerfGE 65, 1, 53). Daher hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder an den Gesetzgeber appelliert, solche Personennummern nur zuzulassen, wenn sie unerlässlich sind und der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsieht (vgl. Kasten zu Nr. 8.2).

Erfreulich ist, dass durch das Gesetz zur Umsetzung von EU-Richtlinien in nationales Steuerrecht und zur Änderung weiterer Vorschriften (Richtlinien-Umsetzungsgesetz) eine Bußgeldvorschrift in die AO eingeführt worden ist, die für die zweckwidrige Verwendung der Identifikationsnummern nach §§ 139a bis 139c AO ein Bußgeld bis zu 10 000 Euro vorsieht (§ 383a AO). Damit ist meine Forderung nach Sanktionen erfüllt worden.

Im Rahmen der Abstimmung der geplanten Rechtsverordnung, mit deren Ausarbeitung Anfang 2005 begonnen werden soll, werde ich noch weitere diskussionswürdige Punkte aufzeigen. Dazu gehört die Frage, welche weiteren Stellen das steuerliche Identifikationsmerkmal in ihren Datenbeständen vorhalten müssen.

Kasten zu Nr. 8.2

67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25. Und 26. März 2004

Entschließung:
Personennummern

Das Bundesverfassungsgericht hat schon in seinem „Volkszählungsurteil“ aus dem Jahre 1983 besonders betont, dass ein Personenkennzeichen nicht verfassungsgemäß ist. Deshalb gibt die Einführung von einheitlichen Personennummern z. B. im Steuerbereich oder auch im Arbeits-, Gesundheits- und Sozialbereich Anlass zu grundsätzlicher Kritik. Der Staat darf seine Bürgerinnen und Bürger nicht zur Nummer abstempeln. Durch die technische Entwicklung sind vorhandene Dateien leicht miteinander zu verknüpfen und könnten zu einer vom Bundesverfassungsgericht strikt abgelehnten allgemeinen Personennummer führen.

Die Konferenz appelliert an die Gesetzgeber, solche Personennummern zu vermeiden. Soweit jedoch im Einzelfall derartige Nummern unerlässlich sind, muss der Gesetzgeber strenge Zweckbindungen und Verwendungsverbote vorsehen.

8.3 Staatliche Kontenabfrage auf dem Prüfstand

Die Bestimmungen zu Kontenabfragen durch Finanzbehörden und eine Vielzahl anderer Behörden wurden im Gesetz zur Förderung der Steuerehrlichkeit nicht normenklar geregelt. Zudem ist fraglich, ob die neuen Abfragebefugnisse dem Grundsatz der Verhältnismäßigkeit entsprechen.

Das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I S. 2928) erlaubt ab dem 1. April 2005 einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24c Kreditwesengesetz vorgehalten werden müssen (vgl. Nr. 11.3.1). Den Finanzbehörden wird nach § 93 Abs. 7 Abgabenordnung (AO), „wenn dies zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht“ gestattet, Kontenstammdaten über das Bundesamt für Finanzen (BfF) bei den Kreditinstituten abzurufen. Zunächst geht es hierbei nicht um Kontenstände und Kontenbewegungen. Gezielte Abfragen wären dann möglich, nachdem der betroffene Steuerpflichtige auf Widersprüche in seiner Steuererklärung hingewiesen wurde, er jedoch bei seinen Angaben geblieben ist. Andere Behörden und Gerichte erhalten nach § 93 Abs. 8 AO die Abfrageberechtigung, wenn das Gesetz, das sie ausführen, an „Begriffe des Einkommensteuergesetzes anknüpft“ und sie versichern, dass eigene Ermittlungen

nicht zum Ziele geführt haben oder keinen Erfolg versprechen.

Vorausgegangen waren Bemühungen des BMF, bessere Kontrollmöglichkeiten einzuführen, um die Finanzverwaltung in die Lage zu versetzen, eine gleichmäßige Besteuerung im Vollzug sicherzustellen.

Mit dem Entwurf eines Steuervergünstigungsabbaugesetzes (StVergAbG) vom 2. Dezember 2002 (Bundestagsdrucksache 15/119) sollten Steuergerechtigkeit und Steuertransparenz erhöht und den öffentlichen Haushalten die notwendigen Einnahmen zur Finanzierung ihrer Aufgaben verschafft werden. Zentraler Punkt war das Vorhaben, unter Eingriff in das Bankgeheimnis des § 30a AO die Kreditinstitute zu verpflichten, dem BfF durch flächendeckende Kontrollmitteilungen Auskunft über Kapitalerträge (Zinsen und Aktiengewinne) ihrer Kunden zu erteilen, was eine bedeutende Ausweitung gegenüber den bisherigen Freistellungsaufträgen bedeutet hätte, die bereits ein gewisses Kontrollsystem darstellen. Durch den Wegfall des § 30a AO wäre nach Auffassung des BMF auch die Möglichkeit geschaffen worden, die in der Vergangenheit liegenden steuerlichen Sachverhalte zu prüfen.

Meine Länderkollegen und ich haben dieses Vorhaben deutlich kritisiert. In das informationelle Selbstbestimmungsrecht werde unverhältnismäßig eingegriffen. Dies habe ich dem Finanzausschuss am 7. Januar 2003 mitgeteilt. Eine von mir als Alternative zu flächendeckenden Kontrollmitteilungen angesehene Abgeltungssteuer als weniger einschneidendes Verfahren, das die umfassenden Anzeigeverpflichtungen der Kreditinstitute vermeidet, wurde dann, noch während des parlamentarischen Verfahrens zum StVergAbG, durch den Referentenentwurf eines Zinsabgeltungssteuergesetzes vom 17. März 2003 in die Diskussion gebracht. Vorgesehen war, die steuerliche Belastung der Kapitaleinkünfte (zunächst nur der Zinsen) durch eine Abgeltungssteuer von 25 % zu begrenzen. Dies wurde jedoch nicht weiterverfolgt.

Mit den neuen Regelungen geht eine Zweckänderung der Verwendung der von den Kreditinstituten ursprünglich allein zur Bekämpfung des Terrorismus und der organisierten Kriminalität (Geldwäsche) vorzuhaltenden Daten einher.

Anders als bei § 93 Abs. 7 AO fehlt in § 93 Abs. 8 AO (vgl. Kasten a zu Nr. 8.3) zudem eine Zweckbestimmung für die Abfragen. Aus dem Gesetz geht nicht deutlich hervor, zu welchem Zweck eine Abfrage erfolgen darf. Um welche Begriffe des Einkommensteuergesetzes es sich handelt, an die das Gesetz anknüpft, das die anfragende Behörde anwendet, ist nicht definiert. Da das Einkommensteuerrecht eine Vielzahl von Begriffen verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ z. B. auch „Wohnung“, „Kindergeld“ und „Arbeitnehmer“), ist nicht hinreichend klar, welche Behörden die Abfrageberechtigung erhalten können. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Es ist auch nicht deutlich, nach welchen Regelungen Auskunftsersuchen erfolgen sollen.

Die Vorschrift steht daher nicht im Einklang mit dem verfassungsmäßigen Gebot der Normenklarheit. Dies hatte ich schon während des Gesetzgebungsverfahrens dem Finanzausschuss vorgetragen. Mit Schreiben vom 7. Oktober 2003 hatte ich vorgeschlagen, eine Abrufmöglichkeit nicht in dieser generellen Form, sondern spezialgesetzlich zu regeln. Mein Vorschlag wurde jedoch nicht aufgegriffen.

Ich habe nach wie vor Zweifel an der Argumentation des BMF, es werde „mit einem Risikomanagement“ in der Lage sein, die Abfragen nur „anlassbezogen und zielgerichtet“ durchzuführen. Konkrete Formen hat ein solches Verfahren jedenfalls noch nicht angenommen. Tatsache ist, dass die Betroffenen von dem Datenabruf zunächst nichts erfahren sollen. Sie erhalten hiervon allenfalls bei einer Diskrepanz zwischen ihren Angaben (z. B. anlässlich der Steuererklärung oder des BAFöG-Antrags) und den Ergebnissen der Kontenabfragen Kenntnis (vgl. auch Entschließung der Datenschutzkonferenz vom 26. November 2004, Kasten b zu Nr. 8.3). Das BMF will jedoch in einer Verwaltungsanweisung auch bei Bestätigung der Angaben des Betroffenen durch den Kontenabruf regeln, dass der Betroffene im folgenden Steuerbescheid über die Kontenabfrage informiert wird (vgl. Kasten c zu Nr. 8.3).

Die Problematik hat lebhafte Resonanz in den Medien gefunden. Die verfassungsrechtliche Dimension zeigt sich in zwei anhängigen Verfassungsbeschwerden mit entsprechenden Eilanträgen. Darüber hatte das Bundesverfassungsgericht bei Redaktionsschluss noch nicht entschieden.

Kasten a zu Nr. 8.3

Rechtsgrundlagen der staatlichen Kontenabfrage

§ 93 AO (Auszug)

(7) Die Finanzbehörde kann bei den Kreditinstituten über das Bundesamt für Finanzen einzelne Daten aus den nach § 93b Abs. 1 zu führenden Dateien abrufen, wenn dies zur Festsetzung oder Erhebung von Steuern erforderlich ist und ein Auskunftsersuchen an den Steuerpflichtigen nicht zum Ziele geführt hat oder keinen Erfolg verspricht.

(8) Knüpft ein anderes Gesetz an Begriffe des Einkommensteuergesetzes an, soll die Finanzbehörde auf Ersuchen der für die Anwendung des anderen Gesetzes zuständigen Behörde oder eines Gerichtes über das Bundesamt für Finanzen bei den Kreditinstituten einzelne Daten aus den nach § 93b Abs. 1 zu führenden Dateien abrufen und der ersuchenden Behörde oder dem ersuchenden Gericht mitteilen, wenn in dem Ersuchen versichert wurde, dass eigene Ermittlungen nicht zum Ziele geführt haben oder keinen Erfolg versprechen.

§ 93b AO

(1) Kreditinstitute haben die nach § 24c Abs. 1 des Kreditwesengesetzes zu führende Datei auch für Abrufe nach § 93 Abs. 7 und 8 zu führen.

(2) Das Bundesamt für Finanzen darf auf Ersuchen der für die Besteuerung zuständigen Finanzbehörden bei den Kreditinstituten einzelne Daten aus den nach Absatz 1 zu führenden Dateien im automatisierten Verfahren abrufen und sie an die ersuchende Finanzbehörde übermitteln.

(3) Die Verantwortung für die Zulässigkeit des Datenabrufs und der Datenübermittlung trägt in den Fällen des § 93 Abs. 7 die ersuchende Finanzbehörde, in den Fällen des § 93 Abs. 8 die ersuchende Behörde oder das ersuchende Gericht.

(4) § 24c Abs. 1 Satz 2 bis 6, Abs. 4 bis 8 des Kreditwesengesetzes gilt entsprechend.

§ 24c KWG (Auszug)

(1) Ein Kreditinstitut hat eine Datei zu führen, in der unverzüglich folgende Daten zu speichern sind:

1. die Nummer eines Kontos, das der Verpflichtung zur Legitimationsprüfung im Sinne des § 154 Abs. 2 Satz 1 der Abgabenordnung unterliegt, oder eines Depots sowie der Tag der Errichtung und der Tag der Auflösung,

2. der Name, sowie bei natürlichen Personen der Tag der Geburt, des Inhabers und eines Verfügungsberechtigten sowie der Name und die Anschrift eines abweichend wirtschaftlich Berechtigten (§ 8 Abs. 1 des Gesetzes über das Aufspüren von Gewinnen aus schweren Straftaten).

Bei jeder Änderung einer Angabe nach Satz 1 ist unverzüglich ein neuer Datensatz anzulegen. Die Daten sind nach Ablauf von drei Jahren nach der Auflösung des Kontos oder Depots zu löschen. Im Falle des Satzes 2 ist der alte Datensatz nach Ablauf von drei Jahren nach Anlegung des neuen Datensatzes zu löschen. Das Kreditinstitut hat zu gewährleisten, dass die Bundesanstalt jederzeit Daten aus der Datei nach Satz 1 in einem von ihr bestimmten Verfahren automatisiert abrufen kann. Es hat durch technische und organisatorische Maßnahmen sicherzustellen, dass ihm Abrufe nicht zur Kenntnis gelangen.

Kasten b zu Nr. 8.3

Entschließung zwischen der 68. und 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26. November 2004

Staatliche Kontenkontrolle muss auf den Prüfstand!

Das „Gesetz zur Förderung der Steuerehrlichkeit“ vom 23. Dezember 2003 (BGBl. I 2003 S. 2928) enthält mit den §§ 93 Abs. 7, 8 und 93b der Abgabenordnung Regelungen, die das Grundrecht auf informationelle Selbstbestimmung aller Bürgerinnen und Bürger im Bereich ihrer finanziellen wirtschaftlichen Betätigung in erheblichem Maße beschränken. Die neuen Regelungen treten am 1. April 2005 in Kraft. Sie sehen vor, dass nicht nur Finanzbehörden, sondern auch eine unbestimmte Vielzahl weiterer Behörden Zugriff auf Bankdaten erhalten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, diese Regelungen mit dem Ziel zu überarbeiten, das Recht auf informationelle Selbstbestimmung zu gewährleisten. Insbesondere das verfassungsrechtliche Gebot der Normenklarheit und die Transparenz des Verfahrens müssen beachtet werden.

Die Neuregelung erlaubt einen Zugriff auf Bankdaten, die von den Kreditinstituten bereits seit April 2003 zur Aufdeckung illegaler Finanztransaktionen vor allem zur Terrorismusbekämpfung nach § 24c des Kreditwesengesetzes vorgehalten werden müssen. Dabei handelt es sich um die Kontenstammdaten der Bankkundinnen und Bankkunden und sonstigen Verfügungsberechtigten, wie z. B. Name, Geburtsdatum, Kontonummern. Mit der neuen Regelung einher geht bereits eine von den Datenschutzbeauftragten des Bundes und der Länder im Gesetzgebungsverfahren Ende 2003 kritisierte Zweckänderung der Verwendung der von den Kreditinstituten vorzuhaltenden Daten.

Nunmehr sollen neben Finanzbehörden auch andere Behörden, z. B. die zahlreichen Stellen der Sozialleistungsträger, Auskunft erhalten, wenn die anfragende Behörde ein Gesetz anwendet, das „an Begriffe des Einkommensteuergesetzes“ anknüpft und eigene Ermittlungen dieser Behörde ihrer Versicherung nach nicht zum Ziel geführt haben oder keinen Erfolg versprechen. Welche Behörden dies sein sollen, geht aus dem Gesetz nicht eindeutig hervor. Da das Einkommensteuerrecht eine Vielzahl von „Begriffen“ verwendet (neben den Begriffen „Einkommen“ und „Einkünfte“ etwa auch „Werbung“, „Kindergeld“, „Arbeitnehmer“), ist wegen fehlender Begriffsbestimmungen nicht abschließend bestimmbar, welche Behörden die Auskunftsersuchen stellen dürfen. Dies jedoch ist nach dem verfassungsrechtlichen Bestimmtheitsgebot unverzichtbar. Zudem wird nicht deutlich, welche Zwecke ein Auskunftsersuchen rechtfertigen und nach welchen Regeln sie erfolgen sollen.

Von der Tatsache des Datenabrufs erfahren Kreditinstitute und Betroffene zunächst nichts. Die Betroffenen erhalten hiervon allenfalls bei einer Diskrepanz zwischen Ihren Angaben (z. B. anlässlich Steuererklärung, BaföG-Antrag) und den Ergebnissen der Kontenabfragen Kenntnis, nicht jedoch bei einer Bestätigung ihrer Angaben durch die Kontenabfragen. Die Auskunft erstreckt sich zwar nicht auf die Kontostände; auf Grund der durch den Abruf erlangten Erkenntnisse können jedoch in einem zweiten Schritt weitere Überprüfungen, dann auch im Hinblick auf die Guthaben direkt beim Kreditinstitut erfolgen.

Dass Betroffene von Abfragen, die zu keiner weiteren Überprüfung führen, nichts erfahren, widerspricht dem verfassungsrechtlichen Transparenzgebot. Danach sind sie von der Speicherung und über die Identität der verantwortlichen Stelle sowie über die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung zu unterrichten. Geschieht dies nicht, hat das zur Konsequenz, dass die Rechtsschutzgarantie des Artikel 19 Abs. 4 Grundgesetz verletzt wird. Die Bürgerinnen und Bürger haben einen substantiellen Anspruch auf eine tatsächlich wirksame gerichtliche Kontrolle (vgl. Volkszählungsurteil, BVerfGE 65, 1, 70).

8.4 Schwarzarbeitsbekämpfungsgesetz

Der Gesetzgeber ist meiner Forderung, irrelevante Daten einer unverzüglichen Löschungspflicht zu unterwerfen, nicht gefolgt.

Mit dem Gesetz zur Intensivierung der Bekämpfung der Schwarzarbeit und damit zusammenhängender Steuerhinterziehung vom 23. Juli 2004 (BGBl. I S. 1842) will die Bundesregierung eine verschärfte Bekämpfung der Schwarzarbeit erreichen. Das Gesetz führt Kontrollregelungen aus Vorschriften verschiedener Gesetze, insbesondere des Sozialgesetzbuchs, zusammen und ergänzt sie wesentlich. Die Prüfungs- und Ermittlungsrechte der nunmehr allein zuständigen Zollverwaltung werden gebündelt. Durch § 436 SGB III sind die Beschäftigten der Arbeitsmarktinspektionen der Bundesagentur für Arbeit zum 1. Januar 2004 in den Dienst des Bundes unter Führung der Zollverwaltung übergeleitet worden. Rund 7 000 Zollfahnder sollen in der neuen Zentralstelle „Finanzkontrolle Schwarzarbeit (FKS)“ und an 113 Standorten, vor allem in den Bereichen Bau-, Gaststätten-, Reise- oder Spielhallengewerbe tätig sein.

Kasten c zu Nr. 8.3

Aus der Entschließung des Deutschen Bundestages zum 19. Tätigkeitsbericht vom 17. Februar 2005, Bundestagsdrucksache 15/4597

„12. Im Rahmen des Gesetzes zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 wurde mit Wirkung ab 1. April 2005 den Finanzbehörden die Möglichkeit eingeräumt, bei Kreditinstituten Informationen über Konto- und Depotverbindungen abzufragen. Der Deutsche Bundestag fordert die Bundesregierung auf, in der geplanten Verwaltungsanweisung auch die Information der Betroffenen über durchgeführte Kontenabfragen vorzusehen.

…“

Der Referentenentwurf enthielt zahlreiche Erhebungs-, Verwendungs- und Übermittlungsbefugnisse und sah eine enge Zusammenarbeit zwischen den Zollbehörden und einer Reihe anderer Behörden vor, enthielt jedoch weder Zweckbindungsregelungen für die Tätigkeiten der beteiligten Stellen noch Regelungen über die vorgesehene zentrale Prüfungs- und Ermittlungsdatenbank. Durch meine Kontrolle in der Informations- und Koordinierungszentrale für die Bekämpfung illegaler Beschäftigung durch die Zollverwaltung in Köln im Mai 2003, der Vorläuferorganisation der FKS, war mir das Vorhaben bekannt, aus der von mir geprüften Datenbank die zentrale Datenbank mit umfassenden Online-Zugriffsberechtigungen aller beteiligten Stellen zu entwickeln.

In intensiven Gesprächen mit dem BMF konnte ich mit Unterstützung des BMJ erreichen, dass meinen datenschutzrechtlichen Bedenken weitgehend Rechnung getragen wurde. Meine Forderung nach einer gesetzlichen Regelung für die zentrale Datenbank wurde durch die §§ 16 ff. Schwarzarbeitsbekämpfungsgesetz (SchwarzArbG) berücksichtigt. In § 16 Abs. 2 SchwarzArbG finden sich detaillierte Vorschriften zum Umfang der Datenspeicherung und in § 16 Abs. 3 und 4 strenge Zweckbindungen. Die gespeicherten Daten dürfen nur für Prüfungen nach § 2 Abs. 1 SchwarzArbG sowie für die Verhütung und Verfolgung von Straftaten und Ordnungswidrigkeiten im Zusammenhang mit den Prüfgegenständen nach § 2 Abs. 1 und in bestimmtem Umfang auch für die Besteuerung verwendet werden. Datenübermittlungen von den Behörden der Zollverwaltung an die FKS dürfen nur zu diesen Zwecken erfolgen.

§ 17 SchwarzArbG regelt Auskünfte an Behörden der Zollverwaltung, an die Polizeivollzugsbehörden der Länder, die Finanzbehörden und an die Staatsanwaltschaft. In § 18 SchwarzArbG wird hinsichtlich der Auskunft an den Betroffenen auf § 83 SGB X verwiesen, der eine datenschutzgerechte Regelung enthält.

Besonders hinzuweisen ist auf die detaillierten Löschungsregelungen in § 19 SchwarzArbG. Zu § 19 Abs. 2 Satz 2 i. d. F. des Gesetzentwurfs – Bundestagsdrucksache 15/2573 – hatte ich allerdings dem Finanzausschuss mit Schreiben vom 26. April 2004 mitgeteilt, dass ich die Empfehlung des Bundesrats nachdrücklich unterstütze, wonach die vorgesehene Löschungsfrist von zwei Jahren im Falle eines rechtskräftigen Freispruchs, der unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens oder der nicht nur vorläufigen Einstellung des Verfahrens durch eine sofortige Löschungsverpflichtung ersetzt werden soll. Der Bundestag ist dieser Empfehlung nicht gefolgt. Das bedeutet, dass Daten von ehemals der Schwarzarbeit Verdächtigen zwei Jahre in der zentralen Datei verbleiben und dem Online-Zugriff der in § 17 SchwarzArbG genannten Behörden unterliegen.

Ende 2004 erklärte das BMF öffentlich, es komme vor, dass Erkenntnisse über ein früheres Verfahren für ein späteres benötigt würden. Diese Erklärung hat mich nicht überzeugt. Soweit es um die Nutzung für ein weiteres Strafverfahren geht, können die Strafverfolgungsbehörden – und zwar nur diese – auf das Zentrale Staatsanwaltliche Verfahrensregister nach §§ 492 ff. StPO zugreifen. Eine doppelte Speicherung für denselben Zweck ist zu vermeiden. Die Nutzung dieser Daten für weitere Zwecke, insbesondere für eine Prüfung nach § 16 Abs. 3 SchwarzArbG, ist unzulässig, wenn die Angaben sich als unzutreffend erwiesen haben.

Ich werde das Gesetz vor allem im Hinblick auf die Datenflüsse kritisch begleiten und in Kürze eine Kontrolle bei der FKS durchführen.

8.5 Alterseinkünftegesetz

Eine weitere große Datenbank zu steuerlichen Zwecken bei der Bundesversicherungsanstalt für Angestellte (BfA) und die steuerliche Identifikationsnummer sorgten für Diskussionsstoff. Eine missbräuchliche Verwendung der Identifikationsnummer wird nunmehr als Ordnungswidrigkeit geahndet.

Das Bundesverfassungsgericht hat dem Gesetzgeber mit Urteil vom 6. März 2002 (BVerfGE 105, 73) aufgegeben, die unterschiedliche Besteuerung der Beamtenpensionen und der Renten aus der gesetzlichen Rentenversicherung verfassungskonform zu regeln. Der darauf hinzielende „Gesetzentwurf zur Neuordnung der einkommensteuerrechtlichen Behandlung von Altersvorsorgeaufwendungen und Altersbezügen – Alterseinkünftegesetz“ vom 9. Dezember 2003 (Bundestagsdrucksache 15/2150) enthielt allerdings eine Reihe datenschutzrechtlicher Probleme:

In einer zentralen Datenbank der BfA als zentraler Stelle nach § 81 Einkommensteuergesetz (EStG) sollten die Meldungen verschiedenster Stellen, auch der privaten Rentenversicherungsträger, durch Rentenbezugsmitteilungen Aufnahme finden. Die zusammengeführten Daten sollten an die jeweils zuständige Landesfinanzbehörde übermittelt werden. Ich habe darauf hingewiesen, dass damit im Bereich der ausschließlich für die Altersvorsorgezulage (sog. Riester-Rente, vgl. 19 TB Nr. 9.4) geschaffenen zentralen Stelle bei der BfA letztlich ein weiterer großer Da-

tenpool mit Sozial- bzw. Steuerdaten entsteht, der fast zwangsläufig neue Begehrlichkeiten hervorruft.

Hinzu kam, dass der erste Gesetzentwurf ein Datenabgleichsverfahren vorsah. Hierfür sollte die zentrale Stelle berechtigt sein, die ihr zur Verfügung stehenden Angaben mit den von den Sozialleistungsträgern übermittelten Daten automatisiert abzugleichen und das Ergebnis den Sozialleistungsträgern mitzuteilen, um einen Sozialleistungsmissbrauch zu verhindern.

Ich habe die Frage gestellt, ob eine solche Regelung überhaupt erforderlich und verhältnismäßig ist. Grundsätzlich sind derartige staatliche Eingriffe in das Recht auf informationelle Selbstbestimmung erst bei Vorliegen bestimmter Anhaltspunkte für rechtswidriges Handeln zulässig. Das BMF konnte jedoch nicht darlegen, dass ein nicht unerheblicher Missbrauch von derartigen Sozialleistungen zu befürchten ist. Durch die beabsichtigte Öffnung für einen Datenabgleich sollte mithin ohne substanzielle Begründung die Möglichkeit einer Überprüfung geschaffen werden. Rentenbezieher wären dadurch mit dem Verdacht belastet worden, Sozialbezüge zu Unrecht zu erhalten. Regelungen, die einen umfassenden und vollständigen Datenabgleich ermöglichen (vgl. 14. TB Nr. 1.1), können daher immer nur ultima ratio sein. Sofern ein Abgleichsverfahren eingeführt werden soll, bedarf dies einer umfassenden Begründung bzw. Abwägung, die auch darlegt, warum die bisherigen gesetzlichen Möglichkeiten wie § 117 Bundessozialhilfegesetz (jetzt § 118 SGB XII) nicht (mehr) ausreichen.

Das BMF hat schließlich meine Bedenken berücksichtigt und die vorgesehene Vorschrift aus dem Entwurf gestrichen.

Eine neue Diskussion begann Ende Februar 2004 mit der Absichtserklärung des BMF, die steuerliche Identifikationsnummer des § 139b AO von allen Sozialversicherungsträgern, d. h. auch den privaten, zwingend erheben zu lassen (im Ersten Entwurf sollte nur die jetzige Steuernummer, soweit bekannt, angegeben werden). Meine Frage war, wie die vorgesehene Möglichkeit der Versicherungsträger, die steuerliche Identifikationsnummer beim Bundesamt für Finanzen (BfF) abzufragen (wenn der Betroffene seiner Verpflichtung zu ihrer Angabe nicht nachkommt), mit dem strikten Zweckbindungsgrundsatz in § 139b AO in Einklang zu bringen sei (vgl. Nr. 8.2). Diese strikte Zweckbindung schließt die Verwendung der Daten in der beim BfF vorgesehenen Datenbank für andere Zwecke als den in § 139b Abs. 4 AO genannten gesetzlich aus. Meine Befürchtung, dass mit einer solchen Datenbank beim BfF weitere Begehrlichkeiten geweckt und hierfür eine rechtliche Grundlage geschaffen werden soll, hätte sich auf diese Weise in einem ersten Schritt bewahrheiten können. Auf die Entschließung der 67. Datenschutzkonferenz zu Personennummern weise ich in diesem Zusammenhang besonders hin (vgl. Kasten zu Nr. 8.2).

Inzwischen hat das BMF meine Bedenken in dieser Frage aufgegriffen. Das Alterseinkünftegesetz vom 5. Juli 2004 (BGBl. I S. 1427) enthält nunmehr eine strikte Zweckbindungsregelung. Die Identifikationsnummer darf nur für Zwecke der Rentenbesteuerung verwendet werden. Auch das Prinzip der Ersterhebung beim Betroffenen wurde berücksichtigt. Erst wenn der betroffene Leistungsempfänger nach Unterrichtung über seine Mitteilungsverpflichtung nach § 22 Abs. 3 EStG den Rentenversicherungsträgern seine Identifikationsnummer trotz Aufforderung nicht mitteilt, ist eine Abfrage beim BfF zulässig.

Besonders erfreulich ist, dass meine Forderung nach einer Sanktion einer missbräuchlichen Verwendung der steuerlichen Identifikationsnummer, die ich bereits beim Steueränderungsgesetz 2003 erhoben hatte, in die Neuregelung des EStG Aufnahme fand. Danach handelt ordnungswidrig, wer vorsätzlich oder leichtfertig entgegen der Zweckbindung in § 22a Abs. 2 Satz 4 EStG die Identifikationsnummer für andere als die dort genannten Zwecke verwendet. Diese Ordnungswidrigkeit kann mit einer Geldbuße bis zu 10 000 Euro geahndet werden (vgl. auch § 383a AO, Nr. 8.2).

8.6 Elektronische Steuererklärung – ELSTER

Die Lücken in der Sicherheit von ELSTER müssen dringend geschlossen werden.

In 1999 hat die Finanzverwaltung die **EL**ektronische **ST**euer**ER**klärung ELSTER zunächst als Verfahren zur elektronischen Übermittlung der Einkommensteuererklärung der Steuerzahler eingeführt. In der Folgezeit wurden mit dem kostenfreien Programm „ELSTER-Formular“ schrittweise immer mehr Möglichkeiten zur elektronischen Abgabe weiterer Steuererklärungen (z. B. Lohnsteuer-Anmeldung, Umsatzsteuer-Voranmeldung) geschaffen. Seit 1. Januar 2004 können Unternehmer Lohnsteuerbescheinigungen gem. § 41b Abs. 1 Einkommensteuergesetz (EStG) elektronisch übermitteln. Nach Aussagen des BMF sind mittels ELSTER bereits mehr als 32 Millionen Steueranmeldungen übermittelt worden. Die Arbeitgeber mit maschineller Lohnabrechnung sind gem. § 41b Abs. 1 Satz 2 EStG verpflichtet, spätestens bis zum 28. Februar 2005 durch Datenfernübertragung an die amtlich bestimmte Übermittlungsstelle eine elektronische Lohnsteuerbescheinigung zu übermitteln und den Arbeitnehmer hierüber zu informieren.

Mit der Übermittlung gem. § 41b Abs. 1 Satz 2 EStG ist eine Zuordnung zur eindeutigen Identifikation des Steuerpflichtigen unabdingbar. Deshalb war bereits zu einem frühen Zeitpunkt durch das BMF beabsichtigt, die Sozialversicherungsnummer als Ordnungsnummer für steuerliche Zwecke im Rahmen von ELSTER zur Identifikation der Steuerpflichtigen zu nutzen. Hiergegen machte ich erhebliche Bedenken geltend. Weder ließ die Rechtslage eine Verwendung der Sozialversicherungsnummer als Ordnungsmerkmal bei der Übermittlung von Lohnsteuerbescheinigungsdaten durch Arbeitgeber an die Finanzverwaltung zu, noch war eine diese Möglichkeit eröffnende Rechtsänderung zum damaligen Zeitpunkt angestrebt. Ich konnte erreichen, dass das BMF auf die Sozialversicherungsnummer als Ordnungsmerkmal verzichtete.

Als Ordnungsmerkmal für die elektronische Übermittlung der Lohnsteuerbescheinigungsdaten durch die Arbeitgeber an die Steuerverwaltung wird stattdessen zur Zeit die eTIN verwendet. Diese ist durch den Arbeitgeber selbst aus dem Namen, Vornamen und Geburtsdatum des Arbeitnehmers nach amtlich festgelegter Regel für den Arbeitnehmer zu bilden und zu verwenden (vgl. § 41b Abs. 2 Satz 1 EStG). Langfristig soll jedoch ein eindeutiges Ordnungsmerkmal die eTIN ablösen. Die rechtlichen Rahmenbedingungen für das allgemeine Ordnungsmerkmal sind in den §§ 139a bis 139d AO enthalten (vgl. Nr. 8.2).

Im Dezember 2004 bin ich durch Eingaben bzw. Presseveröffentlichungen auf die Manipulationsanfälligkeit des ELSTER-Systems aufmerksam geworden. Seit dem 1. Januar 2005 dürfen Steueranmeldungen gem. § 18 Abs. 1 UStG sowie § 41a EStG grundsätzlich nur noch auf elektronischem Wege nach Maßgabe der Steuerdatenübermittlungsverordnung (StDÜV) an das Finanzamt übermittelt werden. Eine sichere Authentifizierung wäre gem. § 87a Abs. 3 Satz 2 AO durch den Einsatz einer qualifizierten elektronischen Signatur zu gewährleisten. Jedoch wurde hierauf wegen der geringen Verbreitung der digitalen Signatur verzichtet. Die Implementierung eines anderen geeigneten Authentifizierungsverfahrens hat sich verzögert und wird nach Aussage des BMF erst ab 2006 erfolgen. In der Zwischenzeit sind allerdings Manipulationen möglich. Unberechtigte Dritte können fingierte Umsatzsteuer-Voranmeldungen unter Nutzung der Steuernummer, die auf Rechnungen gemäß § 14 Abs. 4 Umsatzsteuergesetz ausgewiesen sein muss (vgl. Nr. 29, dort Nr. 3), übermitteln.

Ich habe das BMF in diesem Zusammenhang um Prüfung gebeten, ob und wie in der Übergangszeit bis zur Implementierung eines geeigneten Authentifizierungsverfahrens für das Verfahren ELSTER zur Vermeidung missbräuchlich abgegebener Steueranmeldungen eine „Identifizierung“ der Betroffenen durch das jeweilige Finanzamt, etwa durch Rückrufe, sichergestellt werden kann. Die Antwort des BMF, auch beim früheren Papierverfahren sei ein – wenn auch selten aufgetretener – Missbrauch möglich gewesen, hat mich nicht überzeugt. Es dürfte eine niedrigere Hürde sein, elektronisch beweiserhebliche Daten zu fälschen, als ein Papierdokument mit einer gefälschten Unterschrift zu versehen. Rückrufe im Einzelfall hat das BMF als zu aufwändig abgelehnt. Ich habe daraufhin beim BMF eine verbindliche Zusage der Implementierung des Authentifizierungsverfahrens noch im Jahre 2005, die weiterhin alternative Zulassung der Steueranmeldungen in Papierform und das Einstehen der Finanzverwaltung für durch Missbrauch eintretende Vermögensschäden angemahnt. Eine Antwort des BMF lag bei Redaktionsschluss noch nicht vor.

8.7 Abrufverfahren ZAUBER

Das Bundesamt für Finanzen betreibt ohne ausreichende Rechtsgrundlage das Abrufverfahren ZAUBER seit dem Jahre 2001 zur zentralen Sammlung und Auswertung von Informationen über Umsatzsteuerbetrugsfälle.

Ich habe im März 2003 einen Informations- und Kontrollbesuch im Bundesamt für Finanzen (BfF) in Bonn durchgeführt, um mir ein Bild von der seit dem 1. Januar 2001 betriebenen Datenbank ZAUBER zu machen (vgl. auch 19. TB Nr. 15.3). Dieser Besuch führte u. a. zu folgenden Ergebnissen:

Die Datenbank dient der bundesweiten Sammlung von Betrugsfällen im Bereich der Umsatzsteuer. Es handelt sich dabei um die erste Datenbank der Finanzverwaltung, die von Stellen der Bundes- und der Länderfinanzverwaltung gemeinsam betrieben wird. Nach Auffassung des BMF bildet § 5 Abs. 1 Nr. 13 Finanzverwaltungsgesetz (FVG) i. V. m. § 88a Abgabenordnung (AO) die Rechtsgrundlage für die Datenbank. Nach § 5 Abs. 1 Nr. 13 FVG obliegt dem BfF die zentrale Sammlung und Auswertung der von den Finanzbehörden der Länder übermittelten Informationen über Betrugsfälle im Bereich der Umsatzsteuer. Gemäß § 88a AO dürfen die Finanzbehörden Daten, die gemäß § 30 AO dem Steuergeheimnis unterliegen, auch für Zwecke künftiger Steuerfestsetzungs-, Steuerordnungswidrigkeits- und Steuerstrafverfahren in Dateien und Akten sammeln, soweit dies zur Sicherstellung einer gleichmäßigen Festsetzung und Erhebung von Steuern erforderlich ist.

Die Datenbank ist hinsichtlich ihrer Struktur mit der Verbunddatenbank INPOL vergleichbar (vgl. Nr. 5.2.3). Wie dort können die berechtigten Stellen der Bundes- und der Landesfinanzverwaltungen im Online-Verfahren Daten eingeben und abrufen, wobei ausschließlich die eingebende Stelle die Verantwortung für die Richtigkeit der von ihr eingegebenen Datensätze trägt. Dem BfF kommt eine Zentralstellenfunktion insofern zu, als ihm die Aufrechterhaltung des technischen Betriebs der Datenbank ZAUBER obliegt und indem es für die Dienststellen der Landesfinanzverwaltungen Risikoanalysen anhand der eingestellten Daten durchführt.

Dies bedeutet, dass die Datenbank neben der bundesweiten Erfassung von Betrugsfällen im Bereich der Umsatzsteuer sowie der Unterstützung der Landesfinanzbehörden bei aktuellen Ermittlungen in Fällen von Umsatzsteuerhinterziehung auch der Datenauswertung zur Erkennung von Schwerpunkten der Umsatzsteuerhinterziehung sowie zur frühzeitigen Erkennung neuer Handlungsmuster und Vorgehensweisen bei der Umsatzsteuerhinterziehung dient.

Gegenüber dem BMF habe ich in Frage gestellt, inwieweit § 5 Abs. 1 Nr. 13 FVG i.V.m. § 88a AO als Rechtsgrundlage für die Führung der Datenbank ZAUBER durch das BfF ausreichen. Vor dem Hintergrund der verfassungsrechtlichen Verpflichtung des Gesetzgebers, organisatorische und verfahrensrechtliche Vorkehrungen zu treffen, um damit der Gefahr einer Verletzung des Persönlichkeitsrechts entgegenzuwirken, sowie Beschränkungen des informationellen Selbstbestimmungsrechts auf eine normenklare gesetzliche Grundlage zu stellen, halte ich die gegenwärtig geltenden Regelungen für nicht ausreichend. So fehlen z. B. gesetzliche Regelungen zum Personenkreis, über den Daten gespeichert werden können, wie auch Regelungen über die Art der zu speichernden

personenbezogenen Daten, über Speicherprüffristen und zur Protokollierung. Für problematisch halte ich es auch, dass in ZAUBER in großem Umfang personenbezogene Daten über einen längeren Zeitraum auf Vorrat gespeichert werden. Deshalb halte ich meine Forderung nach einer normenklaren gesetzlichen Grundlage für den Betrieb von ZAUBER aufrecht (vgl. hierzu auch Nr. 8.1).

Ein weiterer datenschutzrechtlich relevanter Punkt ist die Speicherung von Fällen aus dem Bereich des allgemeinen Umsatzsteuerbetruges. Es handelt sich um Fälle von eingeleiteten Strafverfahren (§§ 370, 370a AO) beziehungsweise mit eingeleiteten Bußgeldverfahren, jeweils unabhängig vom späteren Ausgang.

Die unterschiedslose Speicherung dieser Fallgruppe über den Zeitraum von zehn Jahren – unabhängig vom Ausgang etwaiger Straf- oder Bußgeldverfahren und ohne Rücksicht darauf, ob es sich tatsächlich um Umsatzsteuerbetrugsfälle handelt – ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar. Sobald sich der Verdacht eines Umsatzsteuerbetruges als unbegründet herausgestellt hat bzw. bei Kfz-Lieferungen oder der Erzielung von umsatzsteuerlichen Mehrergebnissen kein rechtswidriges Verhalten der betreffenden Unternehmen festgestellt werden kann, dürfen die insoweit angefallenen Daten nicht mehr im Zusammenhang mit der Bekämpfung des Umsatzsteuerbetrugs verwendet werden. Deshalb müssen die Dateispeicherungen regelmäßig, etwa durch Einführung entsprechender Aussonderungsprüffristen, auf ihre inhaltliche Rechtmäßigkeit überprüft werden. Nur so kann eine Löschung personenbezogener Daten unbescholtener natürlicher oder juristischer Personen aus der Datenbank sichergestellt werden.

Das BMF hat mir mittlerweile hierzu mitgeteilt, dass es beabsichtige, die Daten in Anlehnung an § 147 Abs. 3 AO über einen Zeitraum von zehn Jahren zu speichern. Soweit sich im Einzelfall herausstelle, dass Daten zu Unrecht in die Datenbank aufgenommen wurden, weil beispielsweise das eingeleitete Straf- und Bußgeldverfahren eingestellt wurde, werde sichergestellt, dass diese gelöscht werden. Grundsätzlich sei vorgesehen, die Daten nach Ablauf einer Speicherfrist von zehn Jahren automationsgestützt zu löschen. Diese Löschungsregelung ist mir jedoch nicht differenziert genug. Vielmehr strebe ich eine dem § 32 BKAG vergleichbare Regelung an. Darüber bin ich mit dem BMF noch im Gespräch.

8.8 Entwurf einer Steuerdaten-Abrufverordnung – StDAV

Die geplante StDAV wurde auch im Jahre 2004 noch nicht in Kraft gesetzt.

Nach unter meiner Beteiligung erfolgten, intensiven Arbeiten legte das BMF im Februar 2004 einen grundlegend überarbeiteten Entwurf (vgl. 19. TB Nr. 34, dort Nr. 10) einer Steuerdaten-Abrufverordnung (StDAV) vor, die „für neue gesetzliche und auch technische Entwicklungen besser gerüstet“ sein sollte.

Im Abstimmungsverfahren hatte ich insbesondere hinsichtlich folgender Regelung erhebliche datenschutzrechtliche Bedenken: Das BMF wollte in der StDAV die Einrichtung eines Abrufverfahrens unter gewissen Voraussetzungen ermöglichen, ohne dass ein Gesetz dies ausdrücklich vorsieht. Eine Ermächtigung zur Einrichtung von Abrufverfahren sollte nach meiner Auffassung insbesondere dann, „...wenn es wegen des Umfangs der Daten oder ihrer häufigen oder besonders eilbedürftigen Nutzung unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen angemessen ist …“, ausschließlich dem Gesetzgeber vorbehalten bleiben. Mir erschien es unverständlich, gerade dann auf eine ausdrückliche gesetzliche Legitimation zu verzichten, wenn zu erwarten ist, dass Abrufverfahren einen großen Datenumfang nutzen und häufig angewendet werden (vgl. Nr. 8.4).

Auf Grund meiner Intervention hatte der BMF von einer solchen Ermächtigung für die Finanzverwaltung abgesehen, sodass ich nunmehr keine Bedenken mehr gegen die geplante StDAV hatte. Damit wollte das BMF eigentlich die Arbeiten an der StDAV abschließen und das Verordnungsverfahren nunmehr zügig einleiten. Umso mehr hat mich die Tatsache überrascht, dass das BMF kurz vor Redaktionsschluss einen erneut – insbesondere im datenschutzrechtlichen Bereich – überarbeiteten Entwurf vorgelegt hat, dessen Prüfung zur Zeit noch andauert.

8.9 Zentralstelle für Risikoanalyse (Zoll) – ZORA

Ein Beratungs- und Kontrollbesuch in Münster hatte zum Ergebnis, dass bei der ZORA nur in geringem Umfang personenbezogene Daten verarbeitet werden.

Im Jahre 2004 habe ich die Zentralstelle Risikoanalyse (Zoll) – ZORA – in Münster hinsichtlich der Verarbeitung personenbezogener Daten in den dort eingesetzten Verfahren beraten und kontrolliert. Die ZORA wurde mit Wirkung vom 1. Januar 2002 bei der Zoll- und Verbrauchsteuerabteilung der Oberfinanzdirektion (OFD) Köln errichtet und ist zwar organisatorisch der Zoll- und Verbrauchsteuerabteilung der OFD Köln angegliedert, fachlich jedoch unmittelbar dem BMF unterstellt.

Rechtsgrundlage ist § 17a Zollverwaltungsgesetz (ZollVG), der am 6. November 2003 in Kraft getreten ist. Hiernach hat die ZORA die Aufgabe, die Dienststellen der Zollverwaltung, insbesondere den Zollabfertigungs- und Prüfungsdienst, bei deren Aufgabenwahrnehmung durch ein automatisiertes System der Risikoanalyse zu unterstützen. Dazu erstellt die ZORA Maßnahmeempfehlungen in Form von Risikohinweisen für die Warenabfertigung „vor Ort“ an den Zolldienststellen. Zur Vermeidung von Falschanmeldungen (z. B. Schrott anstatt Edelstahl) werden deshalb durch die ZORA in die Datei ATLAS – bei allen Zolldienststellen für die zollamtliche Behandlung ein- und ausgeführter Waren genutzt – entsprechende Warnhinweise eingestellt. Durch einzelfallgesteuerte und individuelle Parameter, die bei der Zollanmeldungseingabe in ATLAS beim betreffenden Zollamt erscheinen (z. B. Codenummer/Ursprungsland), wird gewährleistet, dass die Zollbeamten schon bei der ersten Erfassung im System einen entsprechenden Hinweis auf evtl. Risiken bzw. konkrete Handlungsanweisungen (z. B. Beschau erforderlich) erhalten.

Der Beratungs- und Kontrollbesuch diente im wesentlichen dem Ziel, Informationen über die vom BMF bestimmte Struktur und Arbeitsweise der ZORA zu erlangen. Besonders das Verfahren ATLAS habe ich in diesem Zusammenhang vor Ort geprüft. In ihm werden nur in geringem Umfang personenbezogene Daten verarbeitet; datenschutzrechtliche Bedenken habe ich gegen einen Zugriff der ZORA auf die Datenbestände von ATLAS nicht.

In diesem Zusammenhang ist die Praxis des BMF, durch Erlasse an den Geschäftsbereich auf datenschutzrechtliche Fehler anderer Zolldienststellen zur Vermeidung künftiger Fehler aufmerksam zu machen, besonders hervorzuheben.

8.10 Einscannen von Ausweispapieren bei Duty-free-Shops

Maschinelle Erhebung personenbezogener Daten ohne Sinn und Zweck?

Ein Petent teilte mir mit, dass er in einem Duty-free-Shop im Terminal eines deutschen Flughafens vor seinem Flug ins Ausland Waren gekauft habe. Durch entsprechende Schilder am Eingang war er auf die Notwendigkeit hingewiesen worden, bei der Bezahlung nicht nur die Bordkarte, sondern auch ein Ausweisdokument vorzuzeigen. Seinen Angaben zu Folge ließ sich ein Mitarbeiter des Duty-free-Shops jedoch nicht nur das Ausweispapier zeigen; vielmehr steckte er den Reisepass in ein Lesegerät (Scanner). Durch den Petenten befragt, wurde dieses Verhalten damit erklärt, man müsse „dies wegen der Mehrwertsteuer für den Zoll machen“. Nähere und rechtlich fundierte Auskünfte konnten vor Ort nicht gegeben werden.

Das BMF hat mitgeteilt, dass Ausfuhrlieferungen im nicht-kommerziellen Reiseverkehr – hierunter fallen auch Verkäufe in Duty-free-Shops – von der Umsatzsteuer befreit seien, wenn der Käufer den gekauften Gegenstand im persönlichen Reisegepäck in ein Drittland außerhalb der EU ausführt und er seinen Wohnort im Drittlandsgebiet hat. Dieses müsse vom Unternehmer nachgewiesen werden (§ 6 Abs. 4 Umsatzsteuergesetz). Die Inhaber von Duty-free-Shops könnten somit die Steuerbefreiung für Ausfuhrlieferungen nur bei Nachweis in Anspruch nehmen, dass der Käufer seinen Wohnort im Drittlandsgebiet hat. Dies geschehe in der Regel durch eine Bestätigung an der Grenzzollstelle, aus der hervorgeht, dass die Angaben im Ausfuhrbeleg zu Name und Anschrift des Käufers mit den Eintragungen im vorgelegten Grenzübertrittspapier übereinstimmen (§ 17 Nr. 2 Umsatzsteuerdurchführungsverordnung).

Bei Verkäufen in Duty-free-Shops gilt nach Aussage des BMF die Vorgabe, dass zum Nachweis des Wohnorts im Drittland auch der Pass bzw. Personalausweis zu scannen ist, weil sich die Geschäfte in dem Bereich hinter der Zollabfertigung befinden. Kundendaten werden automatisch nach Filialen abgespeichert und zusammen mit den elektronisch gescannten Verkaufsbelegen auf CD gebrannt. Dem Zoll wird die CD zusammen mit einer Auflistung der Verkaufsdaten zur Kontrolle und Erteilung der Ausfuhrbescheinigung für den Inhaber des Duty-free-Shops übergeben. Die Grenzübertrittspapiere von Käufern mit Wohnort innerhalb der EU – wie im Fall des Petenten – müssen jedoch nicht eingescannt werden. Daher blieb die entscheidende Frage unbeantwortet, warum im vorliegenden Fall dennoch ein Einscannen erfolgte.

Ich habe das BMF um eine ergänzende Stellungnahme gebeten. Diese lag bei Redaktionsschluss noch nicht vor.

8.11 Zinsinformationsverordnung – ZIV

An der Formulierung der inzwischen in Kraft getretenen ZIV wurde ich nicht beteiligt. Sie enthält keine angemessenen Datenschutzregeln.

Durch das BMJ wurde ich erstmals Ende Dezember 2003 auf die Verordnung zur Besteuerung von Zinserträgen (Zinsinformationsverordnung – ZIV) aufmerksam gemacht (vgl. BGBl I S. 128). Dem Verordnungstext konnte ich eine Reihe unzureichender Regelungen zur Übermittlung personenbezogener Daten entnehmen. So wurde versäumt, in §§ 8 und 9 ZIV Regelungen zu treffen, aus denen hervorgeht, welchen Zwecken die Mitteilungspflichten dienen sollen. Entsprechende Regelungen über Zweckbestimmungen sind nach dem Volkszählungsurteil des Bundesverfassungsgerichts jedoch unverzichtbar (vgl. BVerfGE 65, 1, 46f.). Außerdem wurden keine Fristen für die Löschung der Daten beim Bundesamt für Finanzen festgelegt.

Es stellte sich heraus, dass der Bundesrat bereits in seiner Sitzung am 19. Dezember 2003 dieser Verordnung der Bundesregierung gem. Artikel 80 Abs. 2 GG zugestimmt hatte.

Das BMJ und ich haben das BMF auf diesen Missstand hingewiesen und auf eine datenschutzrechtlich konforme Ergänzung in Form einer Novelle der ZIV gedrängt. Die Gespräche dauerten bei Redaktionsschluss noch an.

8.12 Prüfung der Bundesvermögensverwaltung

Mehrere Eingaben von Mietern bundeseigener Wohnungen eines Bundesvermögensamtes nahm ich zum Anlass, mich über den Umgang mit personenbezogenen Daten in diesem Amt zu informieren.

8.12.1 Ausschreibung bundeseigener Objekte im Internet

Ein Mieter einer bundeseigenen Wohnung in einem zur Veräußerung anstehendem Mehrfamilienhaus beschwerte sich darüber, dass im Internet Informationen über eine anhängige Zahlungs- und Räumungsklage veröffentlicht wurden.

Die Bundesvermögensverwaltung (BVV) veräußert ihre Immobilien zunehmend über das Medium Internet und stellt darin Exposés der Objekte ein. So wurde auch das Haus, in dem der Petent eine Wohnung bewohnte, zum Verkauf angeboten. Im Exposé wurden die Kaufinteressenten über die Eigenschaften der Wohnungen informiert.

Ohne die Mieter namentlich zu benennen, fand sich darunter auch eine Übersicht über die zu erwartenden Mieteinnahmen und, bezogen auf eine bestimmbare Wohnung und damit den darin wohnenden Mieter, eine Information über eine anhängige Zahlungs- und Räumungsklage.

Das BMF teilte mir mit, dass die Beschreibung der zum Verkauf angebotenen Immobilien alle relevanten Eigenschaften umfassen müsse. So sei das Mietaufkommen ein wesentliches Merkmal, das der Bund als Verkäufer nennen müsse. Dazu gehörten auch Mietrückstände oder Umstände, die einen Freizug der Wohnung und damit einen Mietausfall erwarten ließen. Dieser Argumentation konnte ich mich nicht anschließen: Ich halte die Information, dass über die Wohnung möglicherweise bald frei verfügt werden kann, auch ohne detaillierte Angabe des Grundes für völlig ausreichend. Zudem könnten entsprechende Informationen zu einem späteren Zeitpunkt, wenn sich das Kaufinteresse konkretisiert hat, gegeben werden.

Zur Verbesserung der Anonymität der Informationen sehen die Behörden der BVV mittlerweile von solchen wohnungsbezogenen Angaben in den Exposés ab.

8.12.2 Führung von Mieterakten

Bei der Prüfung eines Bundesvermögensamtes habe ich festgestellt, dass sämtliche Mietwertfestsetzungen und -ermittlungen über die Wohnung sowie Anschreiben an die jeweiligen Vormieter bei dem aktuellen Mietverhältnis chronologisch in sog. Liegenschaftsakten abgelegt waren.

Die Liegenschaftsakten sind nach den „Vorschriften über die Anlegung und Führung der Liegenschaftsakten bei den Bundesvermögensämtern“ zu verwalten. Eine Einzelakte gliedert sich in verschiedene Sachhefte, wobei sich personenbezogene Informationen überwiegend im sog. Mietersachheft finden; dies besteht aus einzelnen Teilsachheften. In einem dieser Teilsachhefte werden Nutzflächenberechnungen, Mietwertermittlungen und Mietwertfestsetzungen abgelegt. Bei der Durchsicht eines zufällig ausgewählten Mietersachheftes über ein Mietverhältnis in einem bundeseigenen Mehrfamilienhaus fiel mir auf, dass sämtliche Mietwertfestsetzungen und -ermittlungen für die Wohnung und damit einhergehende Anschreiben an die jeweiligen Vormieter chronologisch abgelegt waren. Damit konnte die Belegung der Wohnung nahezu lückenlos dokumentiert und historisiert werden. Das Amt teilte mir mit, dass die früheren Festsetzungen möglicherweise auch in dem aktuellen Mietverhältnis noch von Bedeutung sein könnten und daher im Heft verbleiben sollten.

Die bisherige Praxis entsprach den o. a. Verwaltungsvorschriften. Datenschutzrechtlich bedenklich war es, dass durch die abgelegten Anschreiben alle Mieter der Wohnung als „Karteileichen“ noch im aktuellen Mietersachheft geführt wurden. Vielmehr hätte eine objektbezogene Vorhaltung der Ermittlungs- und Festsetzungsunterlagen ausgereicht. Ich habe daher das BMF gebeten, die bisherige Verfahrensweise zu überprüfen. Aufgrund meiner Bedenken werden nun bei der Anlage eines neuen Mietersachheftes bei Mieterwechsel nur noch die Mietwertermittlungen und -festsetzungen des unmittelbar vorausgehenden Mietverhältnisses abgelegt.

9 Deutscher Bundestag

9.1 Datenschutzordnung für den Deutschen Bundestag – keine neuen Impulse

Die in der 14. Legislaturperiode mit der Bundestagsverwaltung durchgeführten Überlegungen für eine Datenschutzordnung des Parlaments konnten bislang noch nicht zum Ziel geführt werden.

In meinem 19. TB (Nr. 5) hatte ich meine Hoffnung zum Ausdruck gebracht, dass sich der Deutsche Bundestag in dieser Legislaturperiode eine Datenschutzordnung für den parlamentarischen Bereich gibt. Beispiele aus anderen europäischen Ländern zeigen, dass die nationalen Datenschutzgesetze, zum Teil mit nur geringen Anpassungen an die Besonderheiten des parlamentarischen Bereichs, weitgehend Anwendung finden. In Deutschland gibt es mittlerweile nur noch vier Länder, die keine datenschutzrechtlichen Regelungen für ihre Parlamente getroffen haben.

Die Vorarbeiten zu einer Datenschutzordnung des Deutschen Bundestages, die Mitte 2002 weit fortgeschritten waren, hatte ich intensiv begleitet. Vorgesehen war die Ergänzung des BDSG durch eine Parlamentsklausel, nach der das BDSG auf den Deutschen Bundestag keine Anwendung finden sollte, soweit er in Wahrnehmung seiner parlamentarischen Aufgaben tätig wird. Der Deutsche Bundestag ist zwar eine öffentliche Stelle des Bundes im Sinne des § 2 BDSG. Da eine Gleichsetzung mit anderen Behörden jedoch der verfassungsrechtlichen Stellung des Parlaments und der Abgeordneten (Artikel 38 GG) nicht gerecht wird, sollte das BDSG auch weiterhin nicht auf den Deutschen Bundestag anzuwenden sein.

Im Hinblick auf das im Grundgesetz verankerte Persönlichkeitsrecht bedarf es aber auch datenschutzrechtlicher Regelungen für das Parlament. Die Grundlage hierfür sollte ein weiterer Satz der vorgesehenen Parlamentsklausel schaffen, wonach der Deutsche Bundestag sich eine Datenschutzordnung entsprechend den Grundsätzen des BDSG gibt, soweit nicht die Wahrnehmung parlamentarischer Aufgaben abweichende Regelungen erfordert.

Leider ist es bislang noch nicht zur Verabschiedung der Regelungen gekommen. Ich gehe davon aus, dass die Bereitschaft des Deutschen Bundestages, sich eine eigene Datenschutzordnung zu geben, nach wie vor vorhanden ist.

9.2 Nennung von personenbezogenen Daten in Bundestagsdrucksachen

In Beschlussempfehlungen des Wahlprüfungsausschusses werden personenbezogene Daten des Einspruchsführers gegen die Gültigkeit der Wahl zum Deutschen Bundestag seit 2003 anonymisiert.

Im Jahr 2002 machte ich den Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung des Deutschen Bundestages darauf aufmerksam, dass in seinen bisherigen Beschlussempfehlungen – und damit in den Beschlüssen des Deutschen Bundestages – zu den gegen die Gültigkeit der

Bundestagswahl eingegangenen Einsprüchen die Empfehlungen personenbezogen als Bundestagsdrucksache veröffentlicht wurden. Zwar sah ich es für eine sachgerechte Behandlung der Einsprüche als unumgänglich an, den Mitgliedern des Wahlprüfungsausschusses personenbezogene Daten der Einspruchsführer zugänglich zu machen. Eine sachliche Notwendigkeit für eine Veröffentlichung in einer BT-Drucksache, die in vielen öffentlichen Bibliotheken und auch im Internet eingesehen werden kann, sah ich nicht. Meine Bedenken ergaben sich nicht zuletzt daraus, dass nach der bisherigen Praxis teilweise sehr sensible Daten aus der Persönlichkeitssphäre des Einspruchsführers personenbezogen veröffentlicht wurden (z. B. die Tatsache, dass jemand in einer Justizvollzugsanstalt einsaß). Eine entsprechende konkrete Befugnis enthält § 11 Wahlprüfungsgesetz nicht. Danach hat der Wahlprüfungsausschuss zwar den Beschluss schriftlich niederzulegen und dem Deutschen Bundestag eine Entscheidung vorzuschlagen. Eine Rechtsgrundlage zur personenbezogenen Veröffentlichung der Beschlussempfehlung sah ich hierin jedoch nicht.

Da Beschlussempfehlungen des Wahlprüfungsausschusses wie Gerichtsurteile angelegt sind und nach § 9 Wahlprüfungsgesetz für das Verfahren zum Teil die Regelungen des Zivilprozesses gelten, habe ich es für angebracht gehalten, die zur Veröffentlichung von Gerichtsurteilen aufgestellten Grundsätze heranzuziehen. Danach werden Gerichtsentscheidungen grundsätzlich anonymisiert veröffentlicht, es sei denn, die Anonymisierung beeinträchtigt die Verständlichkeit der Entscheidung und das öffentliche Interesse an einer personenbezogenen Veröffentlichung der Entscheidung überwiegt. Durch eine Anonymisierung der Daten der Einspruchsführer jedenfalls wird die Verständlichkeit der Beschlussempfehlung des Wahlprüfungsausschusses nicht beeinträchtigt. Ebenso wenig wird die im Demokratieprinzip verankerte Transparenz des Wahlprüfungsverfahrens durch eine Anonymisierung berührt.

Der Wahlprüfungsausschuss ist meiner Empfehlung gefolgt. Seit Anfang 2003 werden in den Bundestagsdrucksachen nur noch die Initialen des Namens und des Vornamens der Einspruchsführer, die Postleitzahl und der Wohnort sowie das Aktenzeichen angegeben.

Allerdings wies mich Anfang 2004 ein Länderkollege darauf hin, dass der Wahlprüfungsausschuss in den Entscheidungsgründen für die Zurückweisung eines Wahleinspruchs konkret auf zwei frühere Wahlprüfungsverfahren desselben Einspruchsführers hingewiesen hatte, bei denen eine Anonymisierung noch nicht erfolgt war. Tatsächlich konnte sich hierdurch für interessierte Dritte mittelbar doch ein eindeutiger Rückschluss auf die Person des Einspruchsführers sowie auf andere persönliche Umstände ergeben.

Der Wahlprüfungsausschuss hat diesen offensichtlichen Einzelfall zum Anlass genommen, seine Mitglieder über die Problematik zu informieren. Er hat ihnen empfohlen, bei Verweisungen auf frühere Wahlprüfungsverfahren desselben Einspruchsführers darauf zu achten, dass ein mittelbarer Personenbezug nicht hergestellt werden kann, wenn dies nicht zwingend geboten ist. Aus meiner Sicht wird damit dem Datenschutz angemessen Rechnung getragen.

10 Mitarbeiterdatenschutz

10.1 Arbeitnehmerdatenschutzgesetz: Das Warten geht weiter

Immer noch fehlt eine Initiative zur Schaffung eines Arbeitnehmerdatenschutzgesetzes. Führen europäische Vorgaben auch bei uns zu verbessertem Arbeitnehmerdatenschutz?

Eine zunehmende Zahl von Eingaben und Beratungsersuchen macht deutlich, dass sowohl auf Arbeitgeber- als auch auf Arbeitnehmerseite erhebliche Unsicherheit über den Umgang mit personenbezogenen Daten von Mitarbeiterinnen und Mitarbeitern herrscht. Gleichzeitig zeigen viele Fragen, dass der automatisierten Verarbeitung von Mitarbeiterdaten eine immer größere Bedeutung zukommt. Dies betrifft vor allem die beschleunigte Einführung von Personalverwaltungs- und -informationssystemen in Behörden, Betrieben und Unternehmen und die damit verbundenen Auskunfts- und Informationsmöglichkeiten.

Aber auch die ständig voran schreitende Entwicklung auf anderen Gebieten, insbesondere im Gesundheitswesen, hat Konsequenzen für den Arbeitnehmerdatenschutz. So erlangen neue Diagnosemöglichkeiten zunehmende Bedeutung für das Arbeitsverhältnis. Hier bedarf es dringend klarer gesetzlicher Vorgaben, die den am Arbeitsverhältnis Beteiligten sowohl die Einsatzmöglichkeiten als auch die Grenzen neuer medizinischer Methoden und den Umgang mit sensiblen Gesundheitsdaten aufzeigen.

Auch wenn sich inzwischen in Teilbereichen des Arbeitnehmerdatenschutzes gesetzliche Regelungen abzeichnen – so im Rahmen der Umsetzung der Antidiskriminierungsregelung der EU und der Arbeiten an einem Gendiagnostikgesetz, in dem voraussichtlich auch Regelungen über den Einsatz von Gentests im Arbeitsleben enthalten sein werden – bleibt die Notwendigkeit, wesentliche Kernfragen des Datenschutzes im Arbeitsverhältnis gesetzlich zu regeln. Rechtsklarheit und Transparenz müssen in diesem Bereich dringend hergestellt werden.

Befürchtungen, ein Arbeitnehmerdatenschutzgesetz führe zu einer einseitigen Belastung auf Arbeitgeberseite, halte ich für nicht gerechtfertigt. Eine ausgewogene gesetzliche Regelung zum Arbeitnehmerdatenschutz wird vielmehr auch für Arbeitgeber und Unternehmen vorteilhaft sein.

Dies gilt einerseits im Bezug auf die innerbetrieblichen Abläufe: Unsicherheiten über den Umgang mit Daten der Mitarbeiterinnen und Mitarbeiter fallen weg; ungerechtfertigten Befürchtungen der Beschäftigten, etwa im Hinblick auf eine unzulässige Überwachung durch den Arbeitgeber, wird der Nährboden entzogen. Sofern eine vollständige Überwachung von Arbeitnehmern durch ihre

Arbeitgeber ausgeschlossen und notwendige Kontrollmöglichkeiten transparent geregelt sind, wird dies zu einem guten Betriebsklima beitragen.

Vorteile ergeben sich auch für die Präsentation des Unternehmens nach außen; Arbeitnehmerdatenschutz wird auch ein Wettbewerbsvorteil sein. Ein Unternehmen, das modernste Technik einsetzt und dabei den Datenschutz seiner eigenen Mitarbeiterinnen und Mitarbeiter gewährleistet, wird die Daten von Kunden und Geschäftspartnern entsprechend sorgfältig behandeln. Bereichsspezifische Regelungen sind auch unter dem Gesichtspunkt der Planungssicherheit für Unternehmen und ausländische Investoren bedeutsam, beispielweise bei der Einführung von EDV-Systemen. Schließlich würde der Schutz von Betriebs- und Geschäftsgeheimnissen in einem Arbeitnehmerdatenschutzgesetz den Unternehmen und Betrieben einen sicheren Umgang mit diesen Daten gewährleisten.

Einen entscheidenden Impuls erhoffe ich von den Beratungen zum Arbeitnehmerdatenschutz auf europäischer Ebene. Die Erarbeitung eines rechtlich verbindlichen Gemeinschaftsrahmens zum Arbeitnehmerdatenschutz innerhalb der EU werde ich auch in meiner Funktion als Vorsitzender der Europäischen Datenschutzgruppe unterstützen.

10.2 Personalakten

10.2.1 Personalaktenführung weiter verbesserungsbedürftig

Wenn auch erfreuliche Ansätze zur Behebung der bestehenden Vollzugsdefizite im Bereich des Personalaktenrechts zu verzeichnen sind, waren weitere Initiativen erforderlich, um das Persönlichkeitsrecht der Beamtinnen und Beamten zu stärken.

Ich habe wiederholt ausführlich über Missstände und Defizite bei der Führung von Personalakten berichtet. Die Verstöße gegen die bereits am 1. Januar 1993 in Kraft getretenen §§ 90 ff. Bundesbeamtengesetz (BBG) waren in zahlreichen Fällen so gravierend, dass ich sie beanstanden musste. Ausführliche Darstellungen zur sachgerechten Personalaktenführung und Gliederung von Personalakten (Grund-, Teil-, und Nebenakten) finden sich beispielsweise im 15. Tätigkeitsbericht (Nr. 9.1.2) und 18. Tätigkeitsbericht (Nr. 18.3). Zuletzt hatte ich in meinem 19. Tätigkeitsbericht auf die Hinweise des BMI zur Personalaktenführung bzw. zur laufenden Aktenbereinigung hingewiesen (vgl. 19. TB Nr. 21.2.1 Anlage 27).

Auch wenn es bei einigen Ressorts nunmehr gute Ansätze bei der praktischen Umsetzung dieser Vorschriften gibt (vgl. Nr. 10.4.6), ergaben die von mir im Berichtszeitraum durchgeführten Beratungen und Kontrollen bei der Personalaktenführung weiterhin Handlungsbedarf. Daher habe ich weitere Initiativen ergriffen, um die Akzeptanz und die Umsetzung der Vorschriften zum Personalaktenrecht weiter zu verbessern. So habe ich die Ressorts gebeten, nochmals auf die Umsetzung der Regelungen der §§ 90 ff. BBG hinzuwirken. Angesichts der positiven Reaktionen bin ich zuversichtlich, dass den gesetzlichen Regelungen zur Personalaktenführung jetzt eine erhöhte Aufmerksamkeit erwiesen wird.

Außerdem habe ich für die behördlichen Datenschutzbeauftragten der Obersten Bundesbehörden im Berichtszeitraum eine Veranstaltung zum Personalaktenrecht und Mitarbeiterdatenschutz durchgeführt (vgl. Nr. 10.5), um so dazu beizutragen, die praktische Arbeit in den jeweiligen Häusern durch einen informierten Ansprechpartner zu erleichtern.

10.2.2 Personenbezogene Veröffentlichung von Leistungselementen

Eine namentliche Bekanntgabe der mit Leistungselementen bedachten Beamten darf nicht ohne deren vorherige Einwilligung erfolgen.

Herausragende Leistungen von Beamten oder die Wahrnehmung besonderer Funktionen bzw. Aufgaben können durch die Vergabe von Leistungsstufen, -prämien und -zulagen honoriert werden. Im Berichtszeitraum hatte ich die Frage zu beurteilen, ob die Empfänger in einer Hausmitteilung oder auch im hauseigenen Intranet namentlich genannt werden dürfen.

Die Angabe, welcher Person ein Leistungselement gewährt wurde, stellt ein Personalaktendatum i. S. d. § 90 Abs. 1 Satz 2 BBG dar. Nach dem sog. materiellen Personalaktenbegriff (vgl. Bundestagsdrucksache 12/544 S. 11) ist hierfür maßgeblich, ob die den Beamten betreffenden Unterlagen mit seinem Dienstverhältnis in einem unmittelbaren inneren Zusammenhang stehen. Dies ist bei der Gewährung eines Leistungselements der Fall. Konsequenter Weise sehen auch die Durchführungshinweise des BMI zur Leistungsstufenverordnung bzw. Leistungsprämien- und -zulagenverordnung vor, dass die Tatsache der Gewährung eines Leistungselements mit einer konkreten Begründung zur Personalakte zu nehmen ist (vgl. GMBl. 2003 S. 38 ff.).

Gem. § 90 Abs. 1 Satz 3 BBG dürfen Personalaktendaten nur für Zwecke der Personalverwaltung und der Personalwirtschaft verwendet werden, es sei denn, der Beamte willigt in eine anderweitige Verwendung ein. Zu den genannten Zwecken zählen insbesondere die Begründung, Durchführung, Beendigung und Abwicklung des konkreten Dienstverhältnisses sowie Personalplanung (vgl. Bundestagsdrucksache 12/544 S. 16). Eine Veröffentlichung gewährter Leistungselemente unter Namensnennung im Anschluss an deren Vergabe dient jedoch keinem der genannten Zwecke. Vielmehr ist das Vergabeverfahren mit der Bekanntgabe der Entscheidung an die Betroffenen abgeschlossen, sodass eine Veröffentlichung der Namen ohne vorherige Einwilligung gegen die Vorschrift des § 90 Abs. 1 Satz 3 BBG verstößt.

Da zudem alle Beschäftigten die Möglichkeit erhalten, Kenntnis von diesen Personalaktendaten zu nehmen, wird auch § 90 Abs. 3 BBG verletzt, nach dem nur diejenigen Beschäftigten Zugang zu Personalaktendaten haben dürfen, die im Rahmen der Personalverwaltung mit der Bearbeitung von Personalangelegenheiten beauftragt sind. Eine Rechtsnorm, die den sonstigen Mitarbeitern über

eine Veröffentlichung Zugang zu Personalaktendaten gestattet, ist nicht ersichtlich.

Eine personenbezogene Veröffentlichung gewährter Leistungselemente kommt daher nur mit Einwilligung der Betroffenen in Betracht. Da die Gewährung eines Leistungselements den Mitarbeitern nach den Durchführungshinweisen des BMI schriftlich mitzuteilen ist, würde es auch nicht zu einem wesentlich höheren Verwaltungsaufwand führen, die Einwilligungen einzuholen.

Wie mir von Betroffenen nachvollziehbar dargelegt wurde, gibt es im Einzelfall gute Gründe, ausdrücklich keine Veröffentlichung eines gewährten Leistungselementes zu wünschen (z. B. Angst vor Mobbing).

Um die Vergabe von Leistungselementen gleichwohl für alle Beschäftigten transparent darzustellen, kann beispielsweise eine anonymisierte Übersicht ins Intranet eingestellt oder in einer Hausmitteilung veröffentlicht werden.

Das BMI hat zwar in Kenntnis dieser Bedenken die im Haushaltsjahr 2003 gewährten Leistungselemente unter Namensnennung in den Personalnachrichten veröffentlicht. Da das BMI mir jedoch zugesagt hat, die Fortsetzung dieser Praxis erneut zu überprüfen, habe ich zunächst von einer förmlichen Beanstandung abgesehen.

10.2.3 Beihilfedaten und Innenrevision

Der Zugriff einer Innenrevision auf Daten der Beihilfeabrechnung ist mit dem Bundesbeamtengesetz nicht zu vereinbaren.

Im Berichtszeitraum hat mich der Datenschutzbeauftragte eines Bundesministeriums gefragt, ob und ggf. unter welchen Voraussetzungen die Innere Revision des Ministeriums auf Daten der dortigen Beihilfeabrechnung zugreifen dürfe. Die Aufgabe der Inneren Revision besteht darin, den ordnungsgemäßen haushaltswirksamen Verwaltungsvollzug intern zu kontrollieren und hierzu Belege (Verträge, Auszahlungsanweisungen etc.) in allen Kapiteln/Titeln des Geschäftsbereichs des Ministeriums auf ihre Richtigkeit hin zu überprüfen.

Die Verwendung und Weitergabe von Beihilfeakten bzw. Beihilfedaten richtet sich nach § 90a Satz 4 BBG. Danach darf die Beihilfeakte ohne Einwilligung des Beihilfeberechtigten und eines ggf. zu berücksichtigenden Angehörigen dann für andere als für Beihilfezwecke verwendet werden, wenn dies für die Einleitung oder Durchführung eines im Zusammenhang mit einem Beihilfeantrag stehenden behördlichen oder gerichtlichen Verfahrens nötig ist. Ein solcher Zusammenhang wäre etwa bei einem Widerspruchs- oder Klageverfahren aufgrund eines abgelehnten Beihilfeantrags anzunehmen.

Die Innere Revision hat die ordnungsgemäße Haushaltsführung und damit generell Belege, Verträge und Auszahlungsanweisungen auf ihre Richtigkeit hin zu prüfen; diese Tätigkeit stellt jedoch kein Verfahren dar, das in einem unmittelbaren Zusammenhang mit einem Beihilfeantrag selbst steht. Eine Verwendung von Beihilfedaten durch die Innere Revision ist deshalb nicht von § 90a BBG gedeckt.

Auch die übrigen Regelungen der §§ 90 ff. BBG erlauben den Mitarbeitern der Inneren Revision nicht, auf Beihilfedaten zuzugreifen. Vielmehr schreiben die gesetzlichen Bestimmungen vor, Unterlagen über Beihilfen getrennt von der übrigen Personalakte aufzubewahren und in einer von der übrigen Personalverwaltung getrennten Organisationseinheit zu bearbeiten; Zugang zu den Unterlagen über Beihilfen sollen nur Beschäftigte dieser Organisationseinheit haben (§ 90a Satz 2, 3 BBG). Die Kenntnisnahme von geschützten Daten über Krankheiten, Diagnosen, Behandlungen und Medikationen ist dabei zudem auf das unbedingt notwendige Maß zu begrenzen.

Aus diesen Gründen habe ich dem Datenschutzbeauftragten des Ministeriums mitgeteilt, dass ich einen Zugriff der Inneren Revision auf personenbezogene Daten der Beihilfeabrechnung mangels einer entsprechenden rechtlichen Grundlage für nicht zulässig halte. Die Frage, ob eine solche Rechtsgrundlage geschaffen werden sollte, da ansonsten der Prüfauftrag einer Inneren Revision möglicherweise nicht mehr sachgerecht wahrgenommen werden kann, hätte der Gesetzgeber nach Abwägung mit Blick auf die besonders schutzwürdigen Beihilfedaten zu entscheiden (vgl. auch Bundestagsdrucksache 12/544 S. 17).

10.2.4 Mitarbeiterbefragungen

Die in zunehmendem Umfang von der Verwaltung durchgeführten Mitarbeiterbefragungen werfen eine Reihe datenschutzrechtlicher Fragen auf.

In Mitarbeiterbefragungen werden in der Regel subjektive Einschätzungen über das Arbeitsumfeld abgefragt. Dementsprechend enthalten sie Fragen zur Zufriedenheit (Betriebsklima der jeweiligen Organisationseinheit, Motivation, Arbeitsbelastung), Bewertungen von Entscheidungs- und Kommunikationsabläufen oder zum Führungs- und Vorgesetztenverhalten, etwa zur Einschätzung der fachlichen und sozialen Kompetenz von Vorgesetzten.

Die Befragungen werden oft unter Einsatz von Fragebögen durchgeführt. Immer häufiger werden diese Formulare den Mitarbeitern aber auch über das hauseigene Intranet zur Verfügung gestellt und können von den Beschäftigten „online“ zurückgesandt werden (vgl. Nr. 4.1.1.3).

Bei der Ausgestaltung einer Mitarbeiterbefragung sind die folgenden Punkte zu beachten:

– Mitarbeiterbefragungen sind nur auf freiwilliger Basis zulässig. Wegen der abgefragten subjektiven Einschätzungen und Bewertungen können mangels Rechtsgrundlage Mitarbeiter nicht zur Teilnahme verpflichtet werden.

– Wesentliche Bedeutung kommt einer vorherigen umfassenden Aufklärung und Information der Mitarbeiter zu: Der Hinweis auf die Freiwilligkeit ist in die Fragebögen selbst aufzunehmen und sollte drucktechnisch hervorgehoben werden. Die Information der Mitarbeiter alleine in einer Hausmitteilung oder über das hauseigene Intranet ist nicht ausreichend. Die Mitarbeiter sind über den Ablauf, den Gegenstand und den Zweck

der Befragung und darüber, durch wen und für wen die Daten erhoben und verarbeitet werden, zu informieren. Auch sollten die Beschäftigten darüber aufgeklärt werden, welche Auswertungen konkret vorgesehen sind.

– Die mir im Berichtszeitraum bekannt gewordenen Mitarbeiterbefragungen sahen jeweils eine anonyme Durchführung vor. Entscheidend für die datenschutzkonforme Durchführung einer Mitarbeiterbefragung ist jedoch, dass die zugesagte Anonymität (§ 3 Abs. 6 BDSG) auch tatsächlich sichergestellt werden kann.

– Einer besonderen Prüfung bedürfen insoweit die von den Teilnehmern in der Regel geforderten „statistischen Angaben". Werden hier beispielsweise Angaben des konkreten Tätigkeitsfeldes, einer Vollzeit- oder Teilzeitbeschäftigung, des Geschlechts, des Lebensalters und der jeweiligen Laufbahngruppe gefordert, besteht die Möglichkeit, teilnehmende Mitarbeiter durch eine Kombination dieser Angaben zu reidentifizieren. Ähnliche Schwierigkeiten ergeben sich, wenn eine Auswertung auch bezogen auf kleine Organisationseinheiten vorgesehen ist. Hierdurch kann die zugesagte anonymisierte Auswertung ebenfalls in Frage gestellt werden. Dieses Problem lässt sich durch eine Zusammenfassung der Daten bei der Auswertung lösen.

– Vor der Planung und Durchführung einer Mitarbeiterbefragung ist des weiteren zu prüfen, ob eine Beteiligung der Personalvertretung erfolgen muss. Die mir bekannt gewordenen Mitarbeiterbefragungen wurden in enger Kooperation mit den jeweiligen Personalvertretungen sowie unter Beteiligung des behördlichen Datenschutzbeauftragten durchgeführt.

Diese Voraussetzungen einer datenschutzkonformen Durchführung von Mitarbeiterbefragungen konnte ich im Rahmen meiner Beratung des BMI zu den dort geplanten – IT-gestützten – Mitarbeiterbefragungen im BGS einbringen. Aufgrund meiner frühzeitigen Beteiligung und der Berücksichtigung meiner datenschutzrechtlichen Hinweise und Empfehlungen bestehen gegen die zunächst in einem Grenzschutzpräsidium vorgesehene Erprobung des Konzepts keine Bedenken.

10.3 Automatisierte Personaldatenverarbeitung

10.3.1 Automatisierte Verarbeitung von Personaldaten: Nur mit eingebautem Datenschutz!

Angesichts des immer größeren Umfangs der automatisierten Verarbeitung von Personaldaten muss der Datenschutz regelmäßig bereits in der Planungsphase für neue Vorhaben berücksichtigt werden.

In den Personalabteilungen ersetzen elektronische oder IT-gestützte Verfahren zunehmend manuelle Verfahren. Dabei werden sowohl eigenständig entwickelte als auch Standardprodukte eingesetzt (etwa Personalinformations-/Personalverwaltungssysteme). Zusätzlich werden vorhandene Alt-Systeme in neue technische Umgebungen überführt. Hiermit wachsen auch die datenschutzrechtlichen Anforderungen.

Bereits die Begründung zum Neunten Gesetz zur Änderung dienstrechtlicher Vorschriften aus dem Jahre 1991 (Bundestagsdrucksache 12/544 S. 14) weist auf die Gefährdungen hin, die mit der automatisierten Verwaltung von Personaldaten verbunden sind. Besonderes Augenmerk müsse neben dem Missbrauch, etwa in Form unzulässiger Auswertungen, dem sog. Kontextverlust zuteil werden. Jede EDV-gestützte Personaldatenverarbeitung könne Verknüpfungsergebnisse liefern, die sonst nur unter besonders hohem Aufwand – wenn überhaupt – erzielbar wären. Dass dies nicht nur theoretische Überlegungen sind, zeigen die Ergebnisse meiner Datenschutzkontrollen und Beratungsgespräche (vgl. Nr. 10.4).

Wiederum haben mich viele Ministerien und Bundesbehörden um Unterstützung bei der Einführung neuer Personalinformations-/Personalverwaltungssysteme (vgl. Nr. 10.3.2), aber auch sonstiger Verfahren automatisierter Verarbeitungen von Mitarbeiterdaten (z. B. zur automatisierten Gleitzeitverarbeitung) gebeten. Bei solchen Beratungsgesprächen ist es mir möglich, den beteiligten Stellen frühzeitig noch im Planungsstadium datenschutzrechtliche Hinweise und Empfehlungen zu geben.

Wie wichtig die Berücksichtigung des Datenschutzes beim fortschreitenden Technikeinsatz im Personalwesen ist, zeigen die von mir begleiteten Projekte der Bundesverwaltung zur automatisierten Personaldatenverarbeitung zur Einführung einer elektronischen Beihilfeakte (vgl. Nr. 10.3.3) und die IT-gestützte Durchführung von Mitarbeiterbefragungen (vgl. Nr. 10.2.4 und Nr. 4.1.1.3).

In der Berichtsperiode erreichten mich zahlreiche Eingaben von Bundesbediensteten und Fragen von behördlichen Datenschutzbeauftragten, Beschäftigten in den Personalabteilungen und Personalräten zur automatisierten Verarbeitung von Personaldaten. Immer wieder höre ich, dass Betroffene aufgrund unzureichender Information über in den Personalstellen eingesetzte oder geplante IT-Verfahren befürchten, ihre personenbezogenen Daten würden vom Dienstherrn oder Arbeitgeber nicht ordnungsgemäß verarbeitet. Deshalb empfehle ich allen verantwortlichen Stellen, umfassend über eingesetzte und frühzeitig über neue Verfahren zu informieren. Nur dies führt zu einer entsprechenden Transparenz bei allen Betroffenen, fördert die Akzeptanz und beugt unnötigen Auseinandersetzungen vor.

Auch in Zukunft werde ich mich für datenschutzgerechte Lösungen beim Einsatz moderner Informationstechnologie für die Verarbeitung von Beschäftigtendaten einsetzen.

10.3.2 Neues Personalmanagementsystem EPOS 2.0

Im Auftrag des BMI hat das Bundesverwaltungsamt (BVA) das neue elektronische Personal-, Organisations- und Stellenmanagementsystem EPOS 2.0 entwickelt und mich dabei frühzeitig eingebunden.

EPOS 2.0 ist ein neues elektronisches Personal- Organisations- und Stellenmanagementsystem, dass das bisherige EPOS ablösen soll. In einem konstruktiven Beratungsgespräch zu dieser Neuentwicklung habe ich bereits bei einem sehr frühen Planungsstand umfangreiche datenschutzrechtliche Empfehlungen und Hinweise zum neuen System geben können. Es bestand Einvernehmen, diese bei der weiteren Entwicklung zu berücksichtigen bzw. zu übernehmen.

Ich habe es begrüßt, dass auch in den Entwurf einer Rahmendienstvereinbarung zu EPOS 2.0 meine Anregungen und Hinweise aus dem Beratungsgespräch eingeflossen waren.

Mir war der Hinweis wichtig, dass eine abschließende datenschutzrechtliche Bewertung erst nach einer Prüfung des Verfahrens im Echtbetrieb der jeweiligen Behörden möglich ist. Da es sich um ein sehr flexibles System handelt, kommt es entscheidend auf die konkreten Einsatzbedingungen an.

Bei meiner Beratung habe ich auf die Bedeutung datenschutzgerechter Detailregelungen zum jeweiligen Nutzungskonzept, der (neuen) Möglichkeit der Dateneingabe durch Beschäftigte, der Erreichbarkeitsdaten, der Kommunikationsmöglichkeit der Nutzer untereinander, der Zugriffsberechtigungen sowie der technisch-organisatorischen Maßnahmen hingewiesen.

Bei der Dienstvereinbarung zu EPOS sind meine datenschutzrechtlichen Hinweise und Empfehlungen umfassend berücksichtigt worden. Das BMI hat den Behörden seines Geschäftsbereiches dringend empfohlen, vor einer EPOS-Einführung den behördlichen Datenschutzbeauftragten und mich frühzeitig beratend einzubinden. Erste Bundesbehörden haben bereits entsprechenden Kontakt zu mir aufgenommen.

Kasten zu Nr. 10.3.2

EPOS 2.0

Mit EPOS 2.0 hat das BVA ein webfähiges, praxisorientiertes Personalmanagementsystem entwickelt, das nach dem Prinzip der Gegenseitigkeit an alle Einrichtungen des öffentlichen Dienstes weitergegeben wird. Unter Einsatz modernster Informationstechnologie unterstützt es die Zusammenarbeit der zentralen Verwaltungsbereiche Personal, Organisation und Stellenhaushalt und zeichnet sich bei der Verarbeitung sensibler Personal-/ Personalaktendaten durch die Möglichkeit aus, einen hohen Datenschutzstandard umzusetzen. So bietet das System beispielsweise ein vielschichtiges Zugriffskonzept, das in Abhängigkeit von den Zuständigkeiten der Nutzer verschiedene Autorisierungsgrade innerhalb der definierten Benutzergruppen bis auf Feldebene vergibt. Durch die Flexibilität und Anpassungsfähigkeit des EPOS-Systems können die datenschutzrechtlichen Anforderungen in den unterschiedlichen Behörden angemessen berücksichtigt werden.

10.3.3 Einführung der elektronischen Beihilfeakte

Bei der Bearbeitung von Beihilfen schreitet der Einsatz von moderner Informationstechnologie zügig fort; das BVA habe ich bei der geplanten Einführung einer elektronischen Beihilfeakte datenschutzrechtlich beraten.

Das BVA beabsichtigt, die Arbeitsprozesse in seiner Beihilfestelle, in der es für zahlreiche Bundesbehörden, Zuwendungsempfänger und Stiftungen die Beihilfe bearbeitet, zu optimieren.

Zu dem mir in einem frühen Entwicklungsstadium präsentierten Feinkonzept für die Einführung einer elektronischen Beihilfeakte hat mich das BVA um Beratung gebeten, da das geplante Verfahren für die Bundesverwaltung erstmalig eine digitalisierte Bearbeitung von Beihilfeakten und somit auch eine neue Qualität des Umgangs mit sensiblen Beihilfedaten im Sinne des § 90a BBG bedeutet. Daraufhin habe ich umfassende Hinweise und Empfehlungen gegeben, auch zu den technisch-organisatorischen Regelungen. Diese bezogen sich u. a. auf die Aufbewahrung und Speicherung von Beihilfebelegen, die Zweckbindung und die Löschung. Im Hinblick auf die Sensibilität der Daten müssen strikte Zugriffsregelungen getroffen werden. Hingewiesen habe ich ferner auf die Notwendigkeit, die Beihilfebearbeitung nach unterschiedlichen Behörden technisch und organisatorisch getrennt durchzuführen. Das BVA sagte zu, meine datenschutzrechtlichen Hinweise und Empfehlungen in der Praxis zu berücksichtigen.

Zur Zulässigkeit der geplanten Einführung einer elektronischen Beihilfeakte hat das BVA auf meine Anregung hin eine Stellungnahme des BMI eingeholt. Darin führt das BMI aus, dass es die Einführung einer elektronischen Beihilfeakte im Rahmen des geltenden Personalaktenrechts für zulässig hält. Die erforderliche Abschottung nach § 90a BBG könne im Rahmen der papierlosen Beihilfebearbeitung technisch gewährleistet werden. Auch die übrigen Voraussetzungen des § 90a BBG stellten kein unüberwindbares Hindernis dar.

Ich werde das Projekt, das für die Bundesverwaltung Pilotcharakter hat, weiter aufmerksam begleiten.

10.3.4 Automatisierte Gleitzeitverarbeitung

Daten über die tägliche Arbeitszeit von Beschäftigten finden mehr denn je das Interesse von unterschiedlichen Stellen in Behörden; automatisierte Zeiterfassungssysteme ermöglichen einen technisch einfachen „Einblick“ in das Arbeitszeitverhalten von Beschäftigten.

In der Vergangenheit (vgl. 19. TB Nr. 21.3.3) hatte ich bereits über automatisierte Gleitzeitverarbeitung berichtet und die wesentlichen datenschutzrechtlichen Anforderungen an den Einsatz automatisierter Zeiterfassungssysteme dargestellt. Im Berichtszeitraum haben viele Stellen ihre Gleitzeitdatenverarbeitung und hierzu abgeschlossene Dienstvereinbarungen oder sonstige Regelungen datenschutzgerecht ausgestaltet. Andererseits habe ich bei

meinen Kontrollen unzulässige Verarbeitungen von Mitarbeiterdaten festgestellt. Darüber hinaus zeigen Eingaben, Anfragen und Beratungsersuchen, dass es bei der datenschutzgerechten (automatisierten) Verarbeitung von Arbeitszeitdaten nach wie vor Schwierigkeiten und Handlungsbedarf gibt. Wie auch der nachstehende Beitrag (Nr. 10.3.5) deutlich macht, finden Arbeitszeitdaten mehr denn je das Interesse der am Arbeitsleben beteiligten Stellen und Personen, etwa von Fachvorgesetzten oder Personalräten.

10.3.5 Änderung der Arbeitszeitverordnung

Können Vorgesetzte Einblick in die Gleitzeitkonten der ihnen zugewiesenen Mitarbeiterinnen und Mitarbeiter nehmen?

Der Entwurf einer Arbeitszeitverordnung für die Beamtinnen und Beamten des Bundes (AZV) sah u. a. folgenden Satz vor: „Vorgesetzten ist Einblick in die Gleitzeitkonten der ihnen zugewiesenen Mitarbeiterinnen und Mitarbeiter zu gewähren."

Mit dieser Regelung wäre eine beliebige und uneingeschränkte Kenntnisnahme aller Einzelbuchungen durch die jeweiligen Vorgesetzten möglich gewesen. Nach der Begründung des Entwurfs sollte das vorgesehene Einsichtsrecht der besseren Steuerung der organisatorischen Abläufe dienen; es sei Aufgabe der Vorgesetzen, auf eine gleichmäßige Auslastung ihrer Mitarbeiter zu achten. Daneben wurde auf die Verantwortung des Vorgesetzten abgestellt, die Funktionsfähigkeit seiner Organisationseinheit sicherzustellen.

Unter anderem aus folgenden Gründen habe ich mich gegen die Aufnahme eines solchen Einsichtsrechts in die AZV ausgesprochen:

– Es war nicht erkennbar, aus welchen Gründen Vorgesetzten ein uneingeschränktes Einsichtsrecht in alle täglichen Einzelbuchungen ihrer Mitarbeiter eingeräumt werden soll. Insbesondere ging aus der Begründung nicht hervor, wie durch eine solche Einsichtnahme die Abläufe einer Organisationseinheit im einzelnen besser gesteuert werden könnten.

– Unabhängig davon war die vorgesehene Neuregelung mit dem datenschutzrechtlichen Grundsatz der Erforderlichkeit nicht zu vereinbaren. Die Funktionsfähigkeit einer Organisationseinheit kann durch verbindliche Regelungen zur Gewährleistung des Dienstbetriebes sichergestellt werden. Eine solche Möglichkeit eröffnet § 3a Abs. 1 Satz 1 AZV, wonach eine flexible Arbeitszeitgestaltung nur gestattet ist, wenn dienstliche Belange nicht entgegenstehen. Dem gleichen Zweck dienen die in Dienstvereinbarungen zur gleitenden Arbeitszeit regelmäßig festgelegten sog. Kern- oder Servicezeiten.

Aufgrund der von mir und verschiedenen Ressorts vorgetragenen Bedenken wurde von der Aufnahme eines Einsichtsrechts der Vorgesetzten in dieser Form in die AZV zunächst abgesehen.

Demgegenüber ist eine stichprobenartige Kontrolle sowie eine anlassbezogene Information der Vorgesetzten über den Stand der Gleitzeitkonten (Salden) ihrer Mitarbeiter zulässig, sofern die entsprechenden Anlässe bzw. Voraussetzungen vorher – etwa in einer Dienstvereinbarung – festgelegt sind. In diesem Rahmen sind verschiedene Detailregelungen denkbar. So kann beispielsweise geregelt werden, dass der jeweilige Vorgesetzte bei einem Gleitzeitsaldo von plus 40 Stunden aus Fürsorgegründen und bei einem Gleitzeitsaldo von minus 40 Stunden aus Gründen der Dienstaufsicht informiert wird. Entsprechende datenschutzgerechte Verfahrensweisen bei der gleitenden Arbeitszeit sind bereits in verschiedenen mir bekannten Dienstvereinbarungen vorgesehen und auch erfolgreich umgesetzt. Ich halte diese Regelung für angemessen.

Bemerkenswert ist, dass in einigen Fällen auch Personalvertretungen darauf drängten, die automatisiert erfassten Arbeitszeitdaten der Mitarbeiter personenbezogen zur Verfügung gestellt zu bekommen. So forderte eine Personalvertretung die Befugnis, auf die aktuellen Zeitkonten bzw. Gleitzeitdaten der Beschäftigten zugreifen zu können. Hierzu vertrete ich die Auffassung, dass eine so ausgestaltete Einsichtsbefugnis der Personalvertretung zu deren Aufgabenwahrnehmung nicht erforderlich ist. Vielmehr wird es regelmäßig ausreichen, der Personalvertretung Arbeitszeitdaten gegebenenfalls in anonymisierter Form zur Verfügung zu stellen.

10.4 Kontrollen im Personalwesen: Mehr Schatten als Licht

Im Berichtszeitraum habe ich die automatisierte Personaldatenverarbeitung in einer Deutschen Botschaft, einer Niederlassung der Deutschen Post AG, einer Oberfinanzdirektion, einem Hauptzollamt sowie im Deutschen Patent- und Markenamt kontrolliert und im BMI und einer Außenstelle des Bundesverwaltungsamtes schwerpunktmäßig die konventionelle Verarbeitung von Mitarbeiterdaten.

Hierbei habe ich zahlreiche Verstöße, insbesondere gegen die §§ 90 ff. Bundesbeamtengesetz (BBG) festgestellt und in mehreren Fällen die nachfolgend dargestellten förmlichen Beanstandungen nach § 25 Abs. 1 BDSG ausgesprochen.

10.4.1 Kontrolle einer Deutschen Botschaft

Die Auslandsvertretungen sind bisher für ihre Aufgaben im Bereich der Personalverwaltung/-wirtschaft noch nicht an das eingesetzte zentrale Personalinformations-/Personalverwaltungssystem PEPSY in der Zentrale des Auswärtigen Amtes angeschlossen (vgl. 19. TB Nr. 21.3.4). Das AA hat mir zugesagt, mich bei der geplanten Vernetzung, d. h. Anbindung der Auslandsvertretungen an PEPSY, frühzeitig einzubinden.

Neben der Beratung einer Deutschen Botschaft zu Fragen der Personaldatenverarbeitung habe ich dort auch eine Kontrolle durchgeführt und dabei u. a. festgestellt, dass in verschiedenen Bereichen Personal-/Personalaktendaten

automatisiert in vor Ort selbst entwickelten Personaldateien verarbeitet werden, was teilweise nicht datenschutzkonform war. So fanden sich z. B. für die Aufgabenerfüllung nicht (mehr) erforderliche und somit unzulässig gespeicherte Dokumente mit Personaldaten oder solche mit Echtdaten, die als „Muster“ für zukünftige Vergleichsfälle gespeichert waren. Auch die engen Vorgaben für den Zugang zu Personalakten (§ 90 Abs. 3 BBG) waren in der Praxis nicht vollständig umgesetzt. Mängel gab es auch bei der Führung und Aufbewahrung der dort vorhandenen Personalnebenakten.

Die Kontrolle in der Botschaft hat Mängel und Verstöße im Umgang mit Personal-/Personalaktendaten aufgezeigt, etwa gegen die Regelungen der §§ 90 ff. BBG. Die Botschaft hat sofort Maßnahmen eingeleitet, diese datenschutzrechtlichen Defizite abzustellen. Ferner hat das AA die Kontrollergebnisse umgehend zum Anlass genommen, generelle, datenschutzrechtlich relevante Regelungen für alle Auslandsvertretungen zu treffen. Ich habe deshalb nach § 25 Abs. 2 BDSG davon abgesehen, diese Verstöße förmlich zu beanstanden.

10.4.2 Kontrolle einer Niederlassung der Deutschen Post AG

Durch eine Eingabe bin ich auf das Pilotprojekt „Gleitzeiterfassung über das konzerneigene Intranet“ der Deutschen Post AG aufmerksam geworden. In einer Besprechung hierzu hatte ich erhebliche datenschutzrechtliche Bedenken vorgetragen und dann das Verfahren in der betroffenen Niederlassung überprüft, da es dort bereits nicht mehr in der Erprobung, sondern im Wirkbetrieb mit Personal-/Personalaktendaten war.

Hierbei erfuhr ich, dass meine in der ersten Beratung geäußerten datenschutzrechtlichen Bedenken und Hinweise Anlass gewesen waren, das System unter datenschutzrechtlichen Gesichtspunkten völlig neu zu gestalten.

Zu dem neuen Konzept der Gleitzeitverarbeitung und dem Entwurf der entsprechenden Betriebsvereinbarung habe ich ergänzende datenschutzrechtliche Empfehlungen, z. B. zu den Auswertungsmöglichkeiten und Einsichtsrechten, gegeben. Bei der stichprobenartigen Prüfung des Pilotverfahrens konnte ich feststellen, dass meine Empfehlungen zum Teil bereits umgesetzt waren.

Daneben habe ich in der Niederlassung an mehreren Arbeitsplätzen auch kontrolliert, in welcher Form dort Personal-/Personalaktendaten automatisiert verarbeitet werden. Hierbei habe ich zahlreiche nicht mehr erforderliche und damit unzulässig gespeicherte Dokumente festgestellt, etwa längst eröffnete vollständige Beurteilungen oder alte Bewerbungsschreiben, die umgehend gelöscht wurden. Darüber hinaus hat die Deutsche Post AG sofort eine schriftliche Anweisung an alle Mitarbeiter der Niederlassung erlassen und meine Feststellungen zum Anlass genommen, diese Thematik für das gesamte Unternehmen zu regeln und entsprechend zu kommunizieren.

Hinsichtlich des Pilotverfahrens zur Gleitzeiterfassung gehe ich davon aus, dass nunmehr datenschutzgerecht verfahren wird. Da auch die unzulässig gespeicherten Daten der Beschäftigten noch während meines Besuches gelöscht worden sind und die Deutsche Post AG sofort das Notwendige veranlasst hat, habe ich von einer Beanstandung gem. § 25 Abs. 2 BDSG abgesehen.

10.4.3 Kontrolle des Deutschen Patent- und Markenamtes

Im Rahmen eines ersten Beratungsbesuches während des Berichtszeitraums zu Fragen der Personaldatenverarbeitung in der Dienststelle Jena des Deutschen Patent- und Markenamtes (DPMA) habe ich schwerwiegende datenschutzrechtliche Verstöße festgestellt und dem BMJ und dem DPMA mitgeteilt, dass ich von einer förmlichen Beanstandung nur absehen kann, wenn dieses die Mängel umgehend abstellt. Eine Überprüfung der Hauptstelle des DPMA in der Folgezeit führte zu folgenden Ergebnissen:

Für seine automatisierten Verarbeitungen von Personaldaten konnte mir das DPMA kein Verfahrensverzeichnis nach § 4g Abs. 2 i.V.m. § 4e Satz 1 BDSG vorlegen, etwa zum elektronischen Personal-, Organisations- und Stellenverwaltungssystem oder zu vorgefundenen weiteren Verfahren der automatisierten Personaldatenverarbeitung. Meine Kontrolle wurde hierdurch erheblich erschwert.

Meine stichprobenartige Prüfung zu Personal-/Personalaktendaten in zwei Fachabteilungen des DPMA ergab, dass dort in erheblichem Umfang – ohne Wissen der Personalabteilung, der betroffenen Mitarbeiter, des behördlichen Datenschutzbeauftragten und der Personalvertretung – eigenständig erstellte automatisierte Dateien mit Personal-/Personalaktendaten vorhanden waren. Diese zahlreichen, teilweise veralteten elektronischen Dokumente hatten oft äußerst sensible Personalaktendaten zum Inhalt (z. B. Protokolle über Personalführungsgespräche, längst eröffnete vollständige Beurteilungen sowie Daten zur Schwerbehinderung von Mitarbeitern).

Diese vorgefundene Praxis verstößt gegen zahlreiche Regelungen des BBG (§§ 90 ff.) und stand darüber hinaus auch nicht im Einklang mit einer entsprechenden Hausverfügung des DPMA. Die Führung von Vorgängen zu einzelnen Mitarbeitern – unabhängig, ob in automatisierter oder in manueller Form – ist Aufgabe der Personalabteilung.

Die Prüfung der automatisierten Verarbeitung von sensiblen Beschäftigtendaten hat darüber hinaus große Sicherheitslücken und technisch-organisatorische Mängel, u. a. an den geprüften Arbeitsplatzcomputern in den Personalreferaten, beim Personalinformationssystem und auch hinsichtlich des in der Personalabteilung geprüften Netzwerkes des DPMA ergeben.

Vor dem Kontroll- und Beratungsbesuch hatte mich das DPMA davon in Kenntnis gesetzt, dass die seit 1. Januar 1993 geltenden gesetzlichen Regelungen zur Führung von Personalakten (§§ 90 ff. BBG) noch nicht umgesetzt seien. Ich habe deshalb von einer inhaltlichen Prüfung einzelner Personalakten abgesehen und dem DPMA als verantwortlicher Stelle dringend angeraten, das Notwendige zu veranlassen.

Die zahlreichen trotz meiner seit Jahren erfolgten Beratung des DPMA zum Personaldatenschutz festgestellten Mängel habe ich gegenüber dem BMJ gem. § 25 Abs.1 BDSG als Verstoß gegen §§ 90 ff. BBG beanstandet und wegen der erheblichen technisch-organisatorischen Mängel bei der Verarbeitung von Personal-/Personalaktendaten darüber hinaus eine weitere Beanstandung wegen Verstoß gegen § 9 sowie Anlage zu § 9 Satz 1 BDSG ausgesprochen.

Auch nach Auswertung der Stellungnahme des BMJ zu meinem Kontrollbericht sehe ich noch offene und klärungsbedürftige Fragen. Auch hierfür muss eine datenschutzgerechte Verfahrensweise gefunden werden.

10.4.4 Kontrolle einer Oberfinanzdirektion

Schwerpunkt eines Beratungs- und Kontrollbesuchs zur automatisierten Personaldatenverarbeitung in einer Oberfinanzdirektion (OFD) war die Prüfung des Personalinformationssystems COSINUS. Dieses für die Bundesfinanzverwaltung betriebene System läuft auf einem Server im Bundesamt für Finanzen. Die OFD hat selbst keinen direkten Zugriff auf die Daten der Administration oder der Datensicherung. Bei der Prüfung bin ich auf zahlreiche datenschutzrechtliche Probleme und Mängel grundsätzlicher Art gestoßen, auf die ich das BMF hingewiesen habe. Nicht vereinbar mit den Regelungen der §§ 90 ff. BBG waren u. a. die in der OFD festgestellten (personalreferatsübergreifenden) Zugriffs- und Auswertemöglichkeiten in COSINUS, die Mitarbeitern Zugriff auf Personalaktendaten von Beschäftigten ermöglichten, für die sie selbst nicht zuständig waren (vgl. § 90 Abs. 3 BBG). Diese offenen Punkte müssen im Zusammenwirken mit dem BMF vor Ort einer datenschutzgerechten Lösung zugeführt werden.

Neben COSINUS habe ich in den geprüften Personalreferaten zahlreiche eigenentwickelte Personaldateien vorgefunden, die weder zum Verfahrensverzeichnis gemeldet, noch den betroffenen Mitarbeitern oder dem Datenschutzbeauftragten bekannt waren. In diesen Dateien befanden sich zahlreiche für die Aufgabenerfüllung der Personalreferate nicht mehr erforderliche Dokumente und Inhalte mit Personalaktendaten sowie nicht ausreichend anonymisierte „Musterschreiben“ für zukünftige Fälle. Zu diesen neben dem Personalinformationssystem existierenden sonstigen automatisierten Verarbeitungen von Mitarbeiterdaten gab es bei der OFD keine schriftlichen Datenschutzregelungen. Als schweren datenschutzrechtlichen Verstoß habe ich bewertet, dass auf dem Rechner eines Vorgesetzten noch zahlreiche den Mitarbeitern bereits eröffnete und zu deren Personalakte genommene vollständige Beurteilungen gespeichert waren.

Durch eine Petition eines Mitarbeiters veranlasst, habe ich auch das automatisierte Gleitzeitverfahren geprüft und dabei u. a. in der Gleitzeitstelle eine unter Missachtung der gesetzlichen Löschungsfristen aufbewahrte Sammlung von Korrekturbelegen vorgefunden, ebenfalls Monatsjournale, die nach der entsprechenden Dienstvereinbarung nur der Betroffene und der Vorgesetzte erhalten darf. Weiterhin fanden sich ungebuchte Korrekturbelege sowie eine Liste (Auszug) mit Personalaktendaten aus COSINUS. Letzteres stellt einen Verstoß gegen die Regelungen der §§ 90 ff. BBG dar.

Die festgestellten Mängel habe ich gegenüber dem BMF gem. § 25 Abs. 1 BDSG als Verstoß gegen §§ 90 ff. BBG und § 28 Abs. 1 i. V. m. § 12 Abs. 4 BDSG beanstandet.

Das BMF hat mir zugesagt, umgehend das Notwendige zu veranlassen.

10.4.5 Kontrolle in einem Hauptzollamt

Auch in einem zur vorgenannten OFD gehörigen Hauptzollamt habe ich die automatisierte Personaldatenverarbeitung überprüft. Das Hauptzollamt selbst hat nur einen eingeschränkten Zugriff auf das Personalinformationssystem COSINUS.

Dort fanden sich neben COSINUS ebenfalls noch zahlreiche sonstige, eigenständig entwickelte Personaldateien mit teilweise deckungsgleichen Mängeln wie ich sie bei der OFD festgestellt habe (vgl. Nr. 10.4.4).

Auch bei der automatisierten Gleitzeitverarbeitung habe ich datenschutzrechtlich bedenkliche Verfahrensweisen festgestellt, etwa zum offenen Versand von Monatsjournalen an die Mitarbeiter oder eine auch nach der Dienstvereinbarung unzulässige Auswertung von bestimmtem Buchungsverhalten der Beschäftigten. Das BMF hat mir zugesagt, sich umgehend für eine datenschutzgerechte Verfahrensweise einzusetzen.

Sowohl hinsichtlich der OFD als auch des Hauptzollamtes dauert meine Prüfung noch an.

10.4.6 Kontrolle im BMI

Im Rahmen eines Beratungs- und Kontrollbesuches (vgl. Nr. 6.4) im BMI habe ich mir die Praxis der Personalaktenführung angesehen und im Wesentlichen die gleichen Mängel wie in anderen Behörden festgestellt, über die ich schon in meinem 18. TB unter Nr. 18.3 und im 19. TB unter Nr. 21.2.3 detailliert berichtet hatte.

So musste ich feststellen, dass die Vorschriften über das Personalaktenrecht (§§ 90 ff. BBG), die bereits seit 1. Januar 1993 in Kraft sind, teilweise nicht umgesetzt wurden. Die zahlreichen Verstöße gegen die gesetzlichen Vorgaben der §§ 90 ff. BBG habe ich gegenüber dem BMI im Einzelnen dargestellt und nach § 25 BDSG beanstandet.

Nachdem das BMI in seiner Stellungnahme zu meinem Kontrollbericht bereits die Beseitigung einiger von mir festgestellter Mängel zugesagt und die Prüfung weiterer Maßnahmen angekündigt hatte, konnten die bis dahin noch offenen Punkte in einem gemeinsamen Gespräch mit der behördlichen Datenschutzbeauftragten und weiteren Organisationseinheiten des BMI geklärt werden. Ausdrücklich begrüßt habe ich, dass das BMI bereits zuvor eine „Arbeitsanweisung für die Bearbeitung von Personalakten“ erstellt und mit deren Umsetzung begonnen

hatte. Das BMI teilte mir hierzu mit, entsprechend der Vorgaben dieser Anweisung seien Personalakten bereits in nicht unerheblichem Umfang bereinigt worden. Die Arbeitsanweisung soll auch dem Geschäftsbereich als Muster zur Verfügung gestellt werden.

Insgesamt bin ich mit dem inzwischen erreichten Stand der Umsetzung meiner Empfehlungen nach dem jüngsten Beratungs- und Kontrollbesuch zufrieden.

10.4.7 Kontrolle im Bundesverwaltungsamt

Im Berichtszeitraum habe ich auch die Außenstelle des Bundesverwaltungsamtes (BVA) in Berlin-Lichtenberg besucht und dabei die Führung der Teilakten „Beihilfe", „Besoldung" und „Vergütung/Löhne" von Beschäftigten kontrolliert. Im 19. TB (Nr. 21.4, Anlage 28) hatte ich mich bereits mit der Abschottung der Beihilfebearbeitung befasst und die Auffassung vertreten, dass die Bearbeitung der Beihilfeanträge von der gesamten übrigen Personalverwaltung – also auch von der Bearbeitung der übrigen Personalausgaben – getrennt erfolgen muss. Die derzeitige Organisation in der Außenstelle Berlin-Lichtenberg des BVA entspricht leider nicht dieser Forderung.

Das BVA hat hierzu zwischenzeitlich versichert, ein eigenes Beihilfereferat einzurichten, sobald die Betreuung weiterer Behörden in Berlin übernommen werde. Bis dahin sei eine strikte Trennung der Arbeitsprozesse sichergestellt. In den stichprobenweise eingesehenen Teilakten „Besoldung" und „Vergütung/Löhne" wurden aus datenschutzrechtlicher Sicht keine Mängel vorgefunden.

10.5 Veranstaltung „Personalaktenrecht und Mitarbeiterdatenschutz"

Die von mir im Berichtszeitraum den behördlichen Datenschutzbeauftragten der Obersten Bundesbehörden angebotene Vortragsveranstaltung zum Personalaktenrecht und Mitarbeiterdatenschutz fand großen Anklang.

Im Rahmen des in meinem Hause regelmäßig stattfindenden Erfahrungsaustausches der Datenschutzbeauftragten der Obersten Bundesbehörden (vgl. Nr. 2.4) wurde der Wunsch an mich herangetragen, Fragen des Personalaktenrechts und der Personaldatenverarbeitung vertieft zu behandeln und in diesen Bereichen zum Teil bestehende Unsicherheiten sowie verschiedene Einzelfragen zu klären. Diese Anregung habe ich gerne aufgegriffen und den behördlichen Datenschutzbeauftragten der Obersten Bundesbehörden eine ganztägige Vortrags- und Informationsveranstaltung zum Personalaktenrecht und Mitarbeiterdatenschutz angeboten.

Die Veranstaltung beinhaltete einen einführenden und grundlegenden Vortragsteil zum Personalaktenrecht, der auch Gelegenheit bot, grundlegende und allgemeine Fragen zu den §§ 90 ff. Bundesbeamtengesetz (BBG) zu erörtern. Im Rahmen der sich anschließenden Tagesordnung wurden u. a. die Aufgaben und Befugnisse behördlicher Datenschutzbeauftragter im Bereich Personalwesen näher vorgestellt. Die weiteren Tagesordnungspunkte beinhalteten aktuelle Einzelfragen des Personalaktenrechts bzw. des Mitarbeiterdatenschutzes. Hier wurde u. a. die datenschutzrechtliche Problematik im Zusammenhang mit der personenbezogenen Veröffentlichung von Leistungselementen (vgl. Nr. 10.2.2) vorgestellt und Fragen der Erhebung, Verarbeitung und Nutzung von Arbeitszeit- bzw. Gleitzeitdaten erörtert (vgl. Nr. 10.3.4, 10.3.5).

Angesichts der großen Teilnehmerzahl und der positiven Rückmeldungen, die mich nach der Veranstaltung erreicht haben, bin ich zuversichtlich, dass die behördlichen Datenschutzbeauftragten weiterhin ganz erheblich zu datenschutzgerechten Verfahrensweisen im Bereich des Personalwesens ihrer Häuser beitragen werden.

11 Wirtschaft

11.1 Beratung der Wirtschaftsprüferkammer

Die Wirtschaftsprüferkammer hatte mich zu verschiedenen datenschutzrechtlichen Fragestellungen um Beratung gebeten. Meine Ratschläge sind von der Kammer positiv aufgenommen worden.

Die Wirtschaftsprüferkammer (WPK) ist eine Körperschaft des öffentlichen Rechts mit Sitz in Berlin, die der Aufsicht des BMWA untersteht. Ihre Aufgabe besteht darin, die Gesamtbelange der in ihr zusammengeschlossenen Berufe zu wahren; sie erfüllt ihre Aufgabe im Sinne einer öffentlichen Interessenvertretung und ist die Berufsorganisation aller Wirtschaftsprüfer und vereidigten Buchprüfer. Datenschutzrechtlich besonders relevante Aufgaben der WPK sind die Berufsaufsicht, insbesondere Führung des Berufsregister nach §§ 37 ff. Wirtschaftsprüferordnung (WPO), sowie die Durchführung von Qualitätskontrollen und von Ordnungswidrigkeitenverfahren.

Das Berufsregister ist Ausgangspunkt für die meisten datenschutzrelevanten Vorgänge der WPK. In das Berufsregister, das gemäß § 37 Abs. 2 Satz 1 WPO öffentlich ist, werden persönliche und berufsbezogene Informationen eingetragen. Die WPK stellte die Frage, ob die Übermittlung von Daten aus dem Berufsregister an das Versorgungswerk der Wirtschaftsprüfer und der vereidigten Buchprüfer im Land Nordrhein-Westfalen (WPV) auch im Wege des automatisierten Datenabrufs zulässig sei. Das WPV benötigt eine Vielzahl persönlicher und berufsbezogener Daten zur Feststellung und zur Überprüfung der Mitgliedschaft, des Beitrags und von Leistungsvoraussetzungen. Mitunter sind nicht alle im Register vorhandenen Informationen für das WPV erforderlich; eine Selektion der Daten wäre jedoch mit einem unverhältnismäßigen Aufwand verbunden. Zusätzlich dürfen auch andere, nicht-öffentliche Daten an das WPV übermittelt werden, wenn sie für die Feststellung der Mitgliedschaft, der Beitragspflicht oder der Versorgungspflicht benötigt werden. Gegen die Einführung des automatisierten Verfahrens hatte ich unter der Vorgabe, dass durch entsprechende technische und organisatorische Maßnahmen jegliche Manipulation der Daten von fremder Seite ausgeschlossen ist, keine Bedenken.

Ein anderes Problem betraf den Austausch von Daten zwischen den Abteilungen Berufsaufsicht und Qualitätskontrolle. Berufsaufsicht und Qualitätskontrolle sind zwei unterschiedliche verantwortliche Stellen im Sinne von § 3 Abs. 7 BDSG, bei denen Informationen für verschiedene Zwecke verarbeitet werden. Spezialgesetzliche Regelungen sind nur für die Prüfer für Qualitätskontrolle, nicht jedoch für die zu prüfenden Wirtschaftsprüfer vorhanden (§ 12 Satzung für Qualitätskontrolle), so dass hier die Vorgaben von §§ 14, 15 BDSG zum Tragen kommen. Eine Übermittlung der Daten aus der Berufsaufsicht in die Qualitätskontrolle wäre u. a. nur dann zulässig, wenn sie zur Aufgabenerfüllung der übermittelnden Stelle (Berufsaufsicht) oder des Empfängers (Qualitätskontrolle) erforderlich ist. Dies ist hier jedoch nicht erkennbar und wurde auch seitens des Gesetzgebers nicht vorgesehen. Die Abteilung Berufsrecht/-aufsicht teilt der Kommission für Qualitätskontrolle auf Anfrage mit, ob eine berufsgerichtliche Verurteilung eines Prüfers für Qualitätskontrolle vorliegt; die Wirtschaftsprüfer selbst sind hiervon nicht erfasst. Eine Weitergabe der Informationen ist daher datenschutzrechtlich nicht zulässig.

Wirtschaftsprüfer in eigener Praxis und Wirtschaftsprüfungsgesellschaften sind verpflichtet, sich im Abstand von drei Jahren einer Qualitätskontrolle zu unterziehen, wenn sie gesetzlich vorgeschriebene Abschlussprüfungen durchführen. Die Kontrolle dient der Überwachung, ob die Grundsätze und Maßnahmen zur Qualitätssicherung nach Maßgabe der gesetzlichen Vorschriften und der Berufssatzung insgesamt und im Einzelfall eingehalten werden; sie erstreckt sich auf betriebswirtschaftliche Prüfungen. Einzelheiten zur Durchführung und zum Verfahren der Qualitätskontrolle sind in §§ 57 ff. WPO abschließend geregelt; dabei ist die Übermittlung von Informationen, die dem Prüfer bei der Kontrolle bekannt werden und die eine berufsgerichtliche Maßnahme zur Folge haben könnten, gesetzlich nicht vorgesehen. Die Vorgaben der WPO gehen denen des BDSG als spezialgesetzliche Regelung vor; einer Übermittlung von Informationen aus der Qualitätskontrolle in die Berufsaufsicht – auch nur ausgewählter Informationen und unabhängig von einer Zweckbindung – habe ich daher ebenfalls nicht zugestimmt.

Insgesamt habe ich bei der WPK ein hohes Maß an Sensibilität für den Datenschutz feststellen können. Die WPK hat meine Anregungen und Empfehlungen rasch umgesetzt und gibt ein gutes Beispiel für einen initiativen und konstruktiven Umgang mit dem Datenschutz.

11.2 Bundeseinheitliche Wirtschaftsnummer

Statt einer bundeseinheitlichen Wirtschaftsnummer soll künftig die Wirtschafts-Identifikationsnummer genutzt werden, für die in § 139c Abgabenordnung bereits eine Rechtsgrundlage geschaffen wurde.

Das Gesetz zur Vorbereitung einer bundeseinheitlichen Wirtschaftsnummer (BGBl. 2002, I S. 1644 – vgl. 19. TB Nr. 10.1) bildete die Rechtsgrundlage für die Erprobung in den Jahren 2002 und 2003 in Bayern, die ich in dem beim BMWA eingerichteten Beirat begleitet habe.

In ihrem Schlussbericht kommt die Bundesagentur für Arbeit zu dem Ergebnis, dass eine isolierte Einführung einer bundeseinheitlichen Wirtschaftsnummer von den Unternehmen und den öffentlichen Stellen nicht als Vorteil angesehen wird und dass den dadurch zu erwartenden Kosten keine entsprechenden Synergie- und Einsparungseffekte gegenüberstünden. Positiv sei zu bewerten, dass die beteiligten Stellen Schlussfolgerungen in Bezug auf Vereinheitlichung und Zusammenführung von Nummern- und Registersystemen hätten ziehen können. Inzwischen sei mit Inkrafttreten des Steueränderungsgesetzes 2003 in § 139c Abgabenordnung die Voraussetzung für eine einheitliche, unveränderbare und dauerhafte Wirtschaft-Identifikationsnummer geschaffen worden (vgl. hierzu auch Nr. 8.2). Damit könnten mittelfristig die mit der Erprobung der bundeseinheitlichen Wirtschaftsnummer verknüpften Ziele realisiert werden.

Vor diesem Hintergrund hat der Beirat der Bundesregierung empfohlen, zur eindeutigen Identifizierung der Wirtschaftseinheiten gegenüber Verwaltungsstellen die Wirtschafts-Identifikationsnummer nach deren Einführung zu nutzen. Zur Vorbereitung der Umsetzung wurde das BMF gebeten, Fragen zur Festlegung der Einheiten und der Vergabe- und Kontinuitätsregeln, des Stammdatensatzes und des Datenaustausches zu klären. Ich werde bei den weiteren Arbeiten insbesondere darauf hinwirken, dass sich aus der Wirtschafts-Identifikationsnummer kein allgemeines Personenkennzeichen wirtschaftlich tätiger Personen entwickelt (vgl. auch Kasten zu Nr. 8.2). Hierzu haben bereits erste Gespräche stattgefunden, die aber noch ohne konkrete Ergebnisse geblieben sind.

11.3 Bundesanstalt für Finanzdienstleistungsaufsicht

11.3.1 Automatisierter Abruf von Kontoinformationen

Fast zwei Jahre nach Inkrafttreten des § 24c Kreditwesengesetz (KWG) ist das Verfahren zum automatisierten Abruf von Kontoinformationen durch die Bundesanstalt für Finanzdienstleistungen (BaFin) in Betrieb.

Durch § 24c KWG wurden alle Kreditinstitute verpflichtet, ab dem 1. April 2003 eine Datei zu führen, aus der die BaFin die sog. Kontostammdaten automatisiert und ohne Wissen der Kreditinstitute abfragen kann (vgl. 19. TB Nr. 10.2). Dabei kann die BaFin einerseits zur Erfüllung eigener aufsichtlicher Aufgaben nach dem KWG oder dem Geldwäschegesetz tätig werden, andererseits hat sie auf Ersuchen insbesondere von Strafverfolgungsbehörden Auskunft zu erteilen. Bei dem Abrufverfahren haben alle Bedarfsträger einen besonderen Vordruck zu benutzen, so dass sichergestellt ist, dass alle Auskunftsersuchen schriftlich an die BaFin gestellt und von dieser beantwortet werden. Bei erstmaligem Auskunftsersuchen prüft die BaFin, ob es sich tatsächlich um eine auskunftsberechtigte Stelle im Sinne des § 24c KWG handelt. Danach

erhält diese Stelle eine Bedarfsträger-Kennziffer, die bei weiteren Auskunftsersuchen zu verwenden ist. Die Zulässigkeit der Übermittlung der Daten an den Bedarfsträger prüft die BaFin nur, soweit hierzu ein besonderer Anlass besteht.

Nachdem die BaFin am 24. November 2003 den eingeschränkten Wirkbetrieb aufgenommen hatte, wurden so viele Ersuchen gestellt, dass sich ein Rückstand von mehreren tausend Anfragen bildete. Daraufhin wurden die Bedarfsträger gebeten, sich auf eilbedürftige Ersuchen zu beschränken und das technische Verfahren wurde weiter optimiert. Inzwischen werden täglich ca. 200 Anfragen von ca. 500 registrierten Bedarfsträgern bearbeitet. Von dem datenschutzgerechten Ablauf des Abrufverfahrens habe ich mich vor Ort überzeugt. Die BaFin ist nach § 24c Abs. 4 KWG verpflichtet, bei jedem Abruf bestimmte Protokolldaten für Zwecke der Datenschutzkontrolle zu speichern. Auch dieses Verfahren ist inzwischen so ausgestaltet, dass die gesetzlichen Vorgaben eingehalten werden.

Mit dem „Gesetz zur Förderung der Steuerehrlichkeit“ sollen ab dem 1. April 2005 weitere Behörden Zugriff auf die Bankdaten nach § 24c KWG erhalten, wodurch auch die zunächst vorgesehene enge Zweckbegrenzung für die Abfragen erheblich ausgeweitet wird (vgl. hierzu Nr. 8.3).

11.3.2 Müssen Kreditnehmer ihre wirtschaftlichen Verhältnisse bei laufenden Krediten offen legen, auch wenn sie regelmäßig zahlen?

Bei der Offenlegungspflicht des § 18 KWG im Rahmen laufender Kredite müssen die datenschutzrechtlichen Belange der Kreditnehmer angemessen berücksichtigt werden.

Durch verschiedene Eingaben wurde ich darauf aufmerksam, dass Kreditnehmer, die einen Kreditvertrag zur Finanzierung von Wohneigentum von mehr als 250 000 Euro abgeschlossen haben, von ihrem Kreditinstitut während des laufenden Kreditvertrages zur Offenlegung ihrer wirtschaftlichen Verhältnisse aufgefordert werden, auch wenn sie die von ihnen geschuldeten Zins- und Tilgungsleistungen störungsfrei erbringen. Die Kreditinstitute berufen sich bei dieser gängigen Praxis auf § 18 KWG. Diese Vorschrift soll sicherstellen, dass Kreditinstitute über die mit dem Kreditengagement verbundenen Risiken stets im Bilde und bei gegebenenfalls eintretenden Verschlechterungen in der Lage sind, zeitnah geeignete Maßnahmen zu treffen. § 18 KWG sieht daher eine laufende Offenlegung der wirtschaftlichen Verhältnisse als Regelfall vor. Dem Wortlaut des § 18 Satz 3 KWG zufolge kann das Kreditinstitut hiervon absehen, wenn bestimmte Voraussetzungen vorliegen. Hierzu zählen die Sicherung des Kredits durch Grundpfandrechte auf das selbstgenutzte Wohneigentum, das Nichtübersteigen des Kredits von vier Fünftel des Beleihungswertes des Pfandobjektes und die störungsfreie Zins- und Tilgungsleistung.

Ich habe Verständnis dafür, dass Kreditinstitute die Verlustgefahr für die dem Institut anvertrauten Einlagen begrenzen wollen. Gerade deshalb sind zum Zeitpunkt der Einräumung des Kredits die wirtschaftlichen Verhältnisse des Kreditnehmers eingehend zu prüfen, nicht zuletzt auch, um ihn vor finanziellen Risiken warnen zu können. Wenn danach die Bonität des Kreditnehmers als ausreichend angesehen wird, kann während der Abwicklung des Kredits die regelmäßige Offenlegung der wirtschaftlichen Verhältnisse nur im Falle von Verschlechterungen gefordert werden, etwa wenn die geschuldeten Zins- und Tilgungsleistungen nicht mehr störungsfrei erbracht werden. Solange hierfür jedoch keine Anzeichen erkennbar sind, sehe ich keine Erforderlichkeit, die wirtschaftlichen Verhältnisse laufend offen zulegen.

Bei der in § 18 Satz 3 KWG normierten Ermessensentscheidung müssen die datenschutzrechtlichen Belange der Kreditnehmer in angemessener Weise berücksichtigt werden. Deshalb bin ich der Auffassung, dass die Offenlegungspflicht nach § 18 Satz 3 KWG sehr restriktiv ausgelegt werden sollte.

Ich habe diesbezüglich Gespräche mit der BaFin geführt, die in ihrem Rundschreiben „Überblick über die grundsätzlichen Anforderungen an die Offenlegung der wirtschaftlichen Verhältnisse nach § 18 KWG“ den Kreditinstituten Empfehlungen zur Umsetzung der gesetzlichen Regelung gibt. In diesen Gesprächen hat die BaFin die elementare Bedeutung des § 18 KWG für die Sicherheit der Einlagen und das Vertrauen in die Funktionsfähigkeit des Kreditgewerbes einerseits und für die Sicherung der Bonität des Kreditnehmers andererseits hervorgehoben. Zugleich verschließt sich die BaFin meinen datenschutzrechtlichen Bedenken nicht und erwägt, im Rahmen der anstehenden Überarbeitung des Rundschreibens Ausführungen zu einer datenschutzgerechten Auslegung des § 18 Satz 3 KWG vorzunehmen. Sollte hier keine zufriedenstellende Lösung gefunden werden, werde ich dem Gesetzgeber eine Änderung des § 18 KWG empfehlen.

11.3.3 Dürfen Kreditinstitute Warndateien über abgelehnte Kreditanträge führen?

Die BaFin hat den Kreditinstituten empfohlen, abgelehnte Kreditanträge generell durch die Aufnahme eines Warnvermerks in der EDV zu erfassen. Diese Praxis stößt auf datenschutzrechtliche Bedenken.

Die BaFin hat im Jahre 2002 die Endfassung ihres Rundschreibens über die „Mindestanforderungen an das Kreditgeschäft der Kreditinstitute“ (MAK) veröffentlicht. Im Abschnitt „Kreditgewährung“ führt sie dort unter Teilziffer 46 aus, dass abgelehnte Kreditanträge in geeigneter Weise erfasst werden sollen, z. B. durch die Aufnahme eines Warnvermerks in der EDV. Aus der Zusammenarbeit mit den Datenschutzaufsichtsbehörden der Länder für den nicht-öffentlichen Bereich habe ich

erfahren, dass die Kreditinstitute in der Praxis generell abgelehnte Kreditanträge in eine Warndatei aufnehmen und sich dabei auf diese „Empfehlung“ berufen, die sie allerdings nicht als bloße Empfehlung, sondern als bankenaufsichtliche Weisung der BaFin verstehen.

Ich habe daraufhin der BaFin dargelegt, dass es im Regelfall nicht erforderlich sei, abgelehnte Kreditanträge zu speichern und damit eine Art „schwarze Liste“ von Kreditantragstellern anzulegen. Zwar könne es Einzelfälle geben, bei denen es bestimmte Anhaltspunkte für eine wiederholte Kreditantragstellung gäbe und die Kreditinstitute vermeiden wollten, den gleichen Kreditantrag mehrfach zu prüfen, aber generell müsse die Speicherung abgelehnter Kreditanträge die Ausnahme bleiben. Dieses Regel/Ausnahme-Verhältnis müsse in der Empfehlung deutlich zum Ausdruck kommen. Darüber hinaus fehle für die Einzelfälle, in denen die Speicherung zulässig sei, eine Frist, da eine unbegrenzte Speicherung unverhältnismäßig sei.

Die BaFin hat vor diesem Hintergrund zugesagt, im Rahmen der ohnehin anstehenden Überarbeitung der MAK, auch die in Frage stehende Empfehlung zu überdenken; nach derzeitigem Stand scheint sie erfreulicherweise ganz darauf verzichten zu wollen.

11.4 Die SCHUFA erweitert ihr Geschäftsfeld

Die SCHUFA plant die Erweiterung ihres Geschäftsfeldes. Es sollen nunmehr auch Wirtschaftsbereiche an das Auskunftssystem angeschlossen werden, die nicht zu den „klassischen“ Vertragspartnern der kreditgebenden Wirtschaft gehören.

Die SCHUFA verfolgte im Berichtszeitraum weiter das Ziel, neue Geschäftsfelder zu erschließen. Während der SCHUFA bislang ausnahmslos Vertragspartner der kreditgebenden Wirtschaft angeschlossen waren (Banken, Telekommunikationsunternehmen, Versandhandel, Handel), plant die SCHUFA laut eigener Aussagen nunmehr, alle diejenigen Unternehmen, „die Kredite im weiteren Sinne gewähren, von den SCHUFA-Daten profitieren zu lassen“. Sie öffnet sich daher verstärkt auch Wirtschaftssparten, deren berechtigtes Interesse an den SCHUFA-Daten zweifelhaft ist. Konkret ging es im Berichtszeitraum um den Anschluss der Wohnungswirtschaft, der Versicherungswirtschaft und des Inkassobereichs. Der Anschluss dieser Bereiche war im sog. B-Verfahren geplant, d. h. die Vertragspartner melden Negativmerkmale in den Datenbestand ein, die dann auch von allen anderen Vertragspartnern abgerufen werden können. Auf der anderen Seite wären sie berechtigt, Negativmerkmale aus dem gesamten Datenbestand zu erhalten. Gegen den Anschluss dieser Sparten an den Datenbestand der SCHUFA habe ich große Bedenken geäußert.

Hinsichtlich der Wohnungswirtschaft verweise ich auf die Ausführungen in meinem 19. Tätigkeitsbericht (vgl. 19. TB Nr. 10.5.1; s. auch u. Nr. 11.6). Den in Aussicht genommenen Anschluss der Versicherungswirtschaft halte ich für inakzeptabel, da ein Kreditrisiko für die Versicherungen in aller Regel nicht gegeben ist. Versicherungen können bei Nichtzahlung der Versicherungsprämie den Vertrag kündigen mit der Folge, dass dadurch der Versicherungsschutz erlischt. Zudem hat auch die SCHUFA eingeräumt, dass ein Zusammenhang zwischen einem Schadensrisiko der Versicherung und der Bonität eines Versicherungsinteressenten nicht nachgewiesen sei. Einen SCHUFA-Anschluss von Inkassounternehmen kann ich mir nur in den eng begrenzten Fällen vorstellen, in denen das Inkassounternehmen als „verlängerter Arm“ eines anderen Vertragspartners der SCHUFA tätig wird. Alle darüber hinausgehenden Fälle wären meiner Meinung nach eine unzulässige Ausdehnung der Vertragspartner der SCHUFA ohne das Vorliegen eines berechtigten Interesses.

Die SCHUFA hat derzeit Daten von über 60 Mio. Bundesbürgern gespeichert. Eine weitere Ausdehnung der Vertragspartner bedeutet vor diesem Hintergrund eine noch breitere Streuung von Bonitätsdaten praktisch aller Erwerbstätigen in Deutschland mit all ihren Konsequenzen (vgl. dazu Nr. 11.7). Ich werde mich deshalb weiterhin dafür einsetzen, dass die Begrenzung des Kreises der Anschlussnehmer auf solche, die ein berechtigtes Interesse an der Kreditwürdigkeit der Betroffenen haben, erhalten bleibt.

11.5 Score- und Rating-Verfahren – Kaffeesatz statt harter Fakten?

Score- und Rating-Verfahren erlangen eine zunehmende Bedeutung für kommerzielle Entscheidungen, die den einzelnen Bürger betreffen. Rechtliche Rahmenbedingungen auf diesem Gebiet wären hier hilfreich.

In zunehmendem Maße werden sog. „Score“- und „Rating“-Verfahren für wirtschaftliche Entscheidungsprozesse genutzt. Es handelt sich dabei um Verfahren, die auf mathematisch-statistischer Grundlage Risikoklassen bilden, denen dann Kreditsuchende, Kaufinteressenten etc. zugeordnet werden und die dann angeblich ein Bild deren Bonität zeichnen. Mit den Verfahren soll die Kreditwürdigkeit weitgehend unabhängig vom tatsächlichen Verhalten des Betroffenen beurteilt werden, selbst dann, wenn keinerlei negative Informationen über das Zahlungsverhalten einer Person aus der Vergangenheit vorliegen. Es gibt heute kaum noch wirtschaftliche Entscheidungen, die ohne Hinzuziehung solcher Verfahren getroffen werden. Bestellt man eine Ware per Internet, läuft in der Regel bereits während des Erhebungsvorgangs der Adressdaten ein Scoring-Verfahren ab, von dessen Ergebnis es der Händler abhängig macht, ob er nur Lieferung per Nachnahme oder auch Zahlung gegen Rechnung anbietet.

Die Zunahme der Scoring-Verfahren ist datenschutzrechtlich, aber auch gesellschaftspolitisch bedenklich. Scoring-Verfahren nehmen dem Einzelnen die Möglichkeit, selbst über sein Erscheinungsbild in der Öffentlichkeit zu entscheiden oder dieses durch eigenes rechtstreues Verhalten auch nur beeinflussen zu können.

Deshalb sind hier klare rechtliche Rahmenbedingungen erforderlich, um eine solide Datengrundlage zu gewährleisten, insbesondere eine Beschränkung auf relevante individuelle Informationen zu Zahlungsverhalten, Einkommens- und Vermögensverhältnissen.

Außerdem muss die Transparenz des Verfahrens sichergestellt werden, d. h. der Betroffene muss über die berücksichtigten Daten und Merkmale, deren Gewichtung bei der Berechnung des Score-Wertes und über den Score-Wert selbst informiert werden. Eine Begrenzung des datenschutzrechtlichen Auskunftsanspruchs des Betroffenen unter Berufung auf „Betriebs- und Geschäftsgeheimnisse“ des Unternehmens halte ich nicht für hinnehmbar.

11.5.1 Score-Verfahren bei der SCHUFA

Die SCHUFA ist den Forderungen nach umfassender Transparenz ihres Scoring-Verfahrens bislang nicht nachgekommen. Es ist deshalb zu befürchten, dass ohne gesetzgeberisches Eingreifen dem Betroffenen die Entscheidungsgrundlagen für die Gewährung oder Ablehnung einer Leistung weitgehend verschlossen bleiben.

Seit Jahren kritisieren die Datenschutzaufsichtsbehörden die mangelnde Transparenz des Score-Wertes (vgl. 18. TB Nr. 31.1.1, 31.1.2; 19. TB Nr.34, dort Nr. 14). Die SCHUFA erklärte sich inzwischen zwar bereit, Betroffenen auf Nachfrage deren tagesaktuellen Score-Wert mitzuteilen, nicht jedoch den tatsächlich dem jeweiligen Vertragspartner übermittelten Score-Wert. Im Sinne einer verbesserten Transparenz halte ich es für notwendig, dass der Betroffene auch diesen Wert erfährt, der ggf. zu ihn betreffenden Entscheidungen – etwa zur Ablehnung eines Kreditantrags – beigetragen hat. Auch im Berichtszeitraum haben die Aufsichtsbehörden nachhaltig die Beauskunftung des übermittelten Score-Wertes an den Betroffenen gefordert. Die SCHUFA hält eine Realisierung der Forderung wegen mangelnder technischer Voraussetzungen nicht vor Ende 2006 für realisierbar und hat auch für die Zukunft keine entsprechenden Zusagen gemacht.

Auch die seit Jahren erhobene Forderung der Aufsichtsbehörden nach Beauskunftung der in die Berechnung des Score-Wertes einfließenden Faktoren und deren Gewichtung wird seitens der SCHUFA nach wie vor mit Hinweis auf das Geschäftsgeheimnis abgelehnt. Ohne diese Kenntnisse hat der Betroffene jedoch keine Möglichkeit, einen für ihn ungünstigen und zu einer negativen Entscheidung führenden Score-Wert nachzuvollziehen und ggf. zu beeinflussen. Dies ist vor dem Hintergrund zu sehen, dass kein Betroffener allein aufgrund eines schlechten Score-Werts einen Negativeintrag bei der SCHUFA hat und daher grundsätzlich als kreditwürdige, unbescholtene Person anzusehen ist. Wenn dem Betroffenen aber nicht bekannt ist, dass sich z. B. häufige Umzüge etc. negativ auf den Wert auswirken können, ist ihm auch die Möglichkeit genommen, dies gegenüber seinem Vertragspartner zu erläutern (z. B. Zeitsoldat, berufliche Wechsel etc.).

Kasten zu Nr. 11.5.1

Was ist ein Score-Wert?

Der Score-Wert ist eine Punktzahl, die auf einer bestimmten Skala die Kreditrisikoklasse ausdrückt, in die eine bestimmte Person eingeordnet wird. Der Score-Wert ist das Ergebnis des Score-Verfahrens, das aus verschiedenen Daten auf mathematisch-statistischer Grundlage Risikoklassen bildet, denen dann Kreditsuchende, Kaufinteressenten etc. aufgrund ihres Datengefüges zugeordnet werden. Den Verfahren zugrundegelegt sind nicht immer relevante und individuelle Daten des Betroffenen, z. B. über dessen tatsächliches Zahlungsverhalten oder zu seinen Einkommens- und Vermögensverhältnissen. Die Datengrundlage umfasst vielmehr auch Daten ohne eigene Bonitätsaussage wie z. B. Geschlecht, Wohnort, Wohnumfeld, Anzahl der Umzüge (vgl. Nr. 11.5).

11.5.2 Score-Nutzung bei Telekommunikationsunternehmen, Problematik § 6a BDSG

Bei TK-Unternehmen, die bei der Bonitätsprüfung vor Vertragsabschluss den Score-Wert nutzen, liegt zwar im Regelfall keine unzulässige automatisierte Einzelentscheidung vor. Der Verwendung von – für die Betroffenen weitgehend intransparenten – Scoring-Verfahren stehe ich jedoch auch hier weiterhin kritisch gegenüber.

In meinem 19. TB (Nr. 10.5.2) hatte ich mich mit der Frage beschäftigt, wann die Heranziehung des Score-Wertes (vgl. Nr. 11.5.1) zur Prüfung der Kreditwürdigkeit einer Person eine unzulässige automatisierte Einzelentscheidung im Sinne des § 6a BDSG (vgl. Kasten zu Nr. 11.5.2) darstellt. Hintergrund meiner Ausführungen war damals die Praxis von Kreditinstituten bei der Entscheidung über eine Kreditgewährung. Dabei hatte ich auf den Schutzgedanken dieser Vorschrift hingewiesen, dass eine Bewertung von Persönlichkeitsmerkmalen in jedem Fall eine Beurteilung durch einen Menschen erfordert und nicht ausschließlich das Ergebnis einer standardisierten Computeranalyse sein darf.

Im Berichtszeitraum habe ich nunmehr geprüft, wie TK-Unternehmen Bonitätsprüfungen vor Abschluss eines Telekommunikationsvertrages durchführen und inwieweit dabei auch Score-Werte genutzt werden. Mein besonderes Interesse galt dabei der Frage, ob in jedem Einzelfall eine individuelle Prüfung erfolgt oder auch automatisierte Entscheidungen getroffen werden, die nicht mit § 6a BDSG vereinbar wären, soweit sie für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen. Da Bonitätsprüfungen im Mobilfunkbereich besonders häufig durchgeführt werden, habe ich meine Umfrage auf die Mobilfunkanbieter beschränkt. Dabei stellte sich heraus, dass nur ein Teil der Unternehmen im Rahmen der Bonitätsprüfung den Score-Wert als Kriterium heranzieht. Diejenigen Anbieter, die den Score-Wert einer Entscheidung über den Vertragsabschluss zu Grunde legen, wiesen darauf hin, dass es sich beim Antrag auf Abschluss eines Mobilfunkvertrages

um ein tägliches Massengeschäft handele, welches eine individuelle Prüfung nicht zulasse. Gleichwohl wird zum Teil die Entscheidung, ob eine manuelle oder eine automatische Prüfung erfolgt, von einem intern festgelegten Grenzwert abhängig gemacht. Die Mobilfunkanbieter vertraten übereinstimmend die Auffassung, dass die Bestimmung des § 6a BDSG für die Bonitätsprüfung im Telekommunikationsbereich nicht einschlägig sei. Die Entscheidung über eine Ablehnung des Mobilfunkvertrages ziehe keine rechtlich nachteilige Folge für den Betroffenen nach sich. Eine rechtliche Folge im Sinne von § 6a BDSG könne nur eine durch Rechtsvorschrift angeordnete rechtliche Konsequenz sein. Die Ablehnung eines Mobilfunkvertrages beruhe jedoch auf den Grundsätzen der Vertragsfreiheit. Darüber hinaus führe die Ablehnung auch nicht zu einer vom Gesetz geforderten „erheblichen Beeinträchtigung“ des Betroffenen. Ungeachtet der Frage, ob die Nichtzulassung zu einem Mobilfunknetz – anders als beim Festnetz – bereits als Beeinträchtigung gewertet werden könne, habe der Betroffene jederzeit die Möglichkeit, ein Prepaid-Produkt des gleichen Anbieters zu nutzen, welches keiner Bonitätsprüfung unterfällt. Er werde daher nicht grundsätzlich von der Möglichkeit des mobilen Telefonierens ausgeschlossen.

Auch unter Berücksichtigung dieser rechtlichen Argumentation sehe ich keine Veranlassung, meine grundsätzliche kritische Einstellung gegenüber dem Scoring-Verfahren zu revidieren (vgl. Nr. 11.5.1; 19. TB Nr. 34, dort Nr. 14).

Kasten zu Nr. 11.5.2

§ 6a BDSG
Automatisierte Einzelentscheidung

(1) Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen.

(2) Dies gilt nicht, wenn

1. die Entscheidung im Rahmen des Abschlusses oder der Erfüllung eines Vertragsverhältnisses oder eines sonstigen Rechtsverhältnisses ergeht und dem Begehren des Betroffenen stattgegeben wurde oder
2. die Wahrung der berechtigten Interessen des Betroffenen durch geeignete Maßnahmen gewährleistet und dem Betroffenen von der verantwortlichen Stelle die Tatsache des Vorliegens einer Entscheidung im Sinne des Absatzes 1 mitgeteilt wird. Als geeignete Maßnahme gilt insbesondere die Möglichkeit des Betroffenen, seinen Standpunkt geltend zu machen. Die verantwortliche Stelle ist verpflichtet, ihre Entscheidung erneut zu prüfen.

(3) Das Recht des Betroffenen auf Auskunft nach den §§ 19 und 34 erstreckt sich auch auf den logischen Aufbau der automatisierten Verarbeitung der ihn betreffenden Daten.

11.5.3 Basel II – welche Neuerungen kommen auf Kreditnehmer zu?

Bei der verschärften Überprüfung der Kreditwürdigkeit ihrer Kunden setzen die Banken Rating-Verfahren ein, die umso erfolgreicher sind, je mehr Kundendaten verarbeitet werden. Hier gilt es, ein datenschutzrechtlich zulässiges Maß zu finden.

Hinter „Basel II“ verbirgt sich eine neue Eigenkapitalvereinbarung des Baseler Ausschusses für Bankenaufsicht, die am 26. Juni 2004 verabschiedet worden ist, um für größere Stabilität der weltweit verflochtenen Finanzwirtschaft zu sorgen. Die Banken sollen dazu die Absicherung von Krediten mit Eigenkapital künftig stärker an den individuellen Ausfallrisiken ihrer Kunden orientieren, statt wie bisher alle Kredite pauschal mit einem bestimmten Prozentsatz Eigenkapital zu unterlegen. Die neue Regelung sieht bei der Bestimmung der Eigenkapitalquote eine Reihe neuer Ansätze zur Messung des Kreditrisikos vor. Dies wird dazu führen, dass die Banken die Schuldnerbonität vor Kreditabschluss intensiver prüfen werden als bisher, weil davon das Kreditrisiko und damit auch die Höhe der Eigenkapitalanforderung abhängt. Dafür wiederum werden von den Kreditinstituten verfeinerte Rating-Verfahren angewandt, die im Einzelnen datenschutzrechtliche Probleme aufwerfen können. Diese Verfahren weisen große Ähnlichkeit mit Scoring-Systemen auf, die in anderen Geschäftsbereichen eingesetzt werden (vgl. Nr. 11.5). Die Aussagekraft von Rating-Prognosen hängt maßgeblich von der hierfür genutzten Datengrundlage ab. Je mehr Vergleichsdaten als Erfahrungswissen vorliegen, desto genauer kann die Kreditausfallwahrscheinlichkeit prognostiziert werden. Im Gespräch sind hier z. B. auch Daten abgelehnter Kreditantragsteller. Hier gilt es, frühzeitig auf datenschutzrechtliche Regelungen hinzuweisen, denn nicht alle Daten, die für ein genaues Rating wünschenswert wären, dürfen auch datenschutzrechtlich erhoben, gespeichert und genutzt werden.

Die Eigenkapitalvereinbarung Basel II entfaltet selber keine unmittelbare gesetzliche Wirkung; sie wird jedoch derzeit in eine EU-Richtlinie umgesetzt, die dann in nationales Recht zu transformieren ist. Das BMF hat mich in die Beratungen zur Erarbeitung der Richtlinie einbezogen. Ich werde das Projekt weiter begleiten.

11.6 Warndateien im Wohnungswesen – darf der Vermieter alles wissen?

Vermieter holen immer häufiger bei Auskunfteien Informationen über potentielle Mieter ein. Diese uneingeschränkten Auskünfte führen bei Mietinteressenten häufig zu einer datenschutzrechtlich und sozial bedenklichen Situation.

In ihrem Bestreben, sich vor Mietausfällen zu schützen, greifen potentielle Vermieter verstärkt auf den Datenbestand von Auskunfteien zurück. Neben der SCHUFA, die sich um den Anschluss der gewerblichen Wohnungswirtschaft an den Kreis ihrer Vertragspartner bemüht (vgl. 19. TB Nr. 10.5.1), übermitteln auch andere Auskunfteien Daten an Vermieter. Daneben errichten viele Vermieter als „Gläubigerschutzgemeinschaften“ gemeinsame Warndateien.

Das durchaus berechtigte Interesse, sich vor Mietausfällen zu schützen, darf zu keinem gläsernen Mietinteressenten führen. Die Beschaffung von Wohnraum ist ein elementares Bedürfnis. Eine Erschwernis auf diesem Gebiet ist nicht damit zu vergleichen, nur noch gegen Nachnahme beim Versandhandel bestellen zu können oder keinen Handyvertrag zu bekommen. Besonders problematisch sind branchenübergreifende Auskunftssysteme nicht nur wegen der schwerwiegenden Konsequenzen von Negativauskünften für den Betroffenen, sondern auch im Hinblick auf die Bewertung der jeweiligen Erkenntnisse. So bedeutet ein Fehlverhalten auf einem anderen Gebiet nicht, dass der Betroffene auch bei der Mietzahlung säumig wird. Eine datenschutzpolitisch akzeptable Alternative, die beiden Seiten gerecht würde, wäre eine branchenspezifische Beschränkung der Auskünfte. Vermieter dürften nur Auskünfte erhalten, die sich auf andere Mietverhältnisse des Betroffenen beziehen und die nur solche Daten enthalten, die gesicherte Rückschlüsse auf Mietausfallrisiken zulassen, wie z. B. rechtskräftige Titel zu Zahlungsverzug im Mietbereich, rechtskräftige Urteile zur fristlosen Kündigung wegen Zahlungsverzugs oder sonstiger Vertragsverletzungen.

Die obersten Datenschutzaufsichtsbehörden waren sich darin einig, dass aus der Sicht des Datenschutzes solche branchenspezifischen Auskunftssysteme vorzuziehen sind und eine uneingeschränkte Auskunft über bei branchenübergreifenden Auskunfteien gespeicherte Daten an potentielle Vermieter unzulässig ist.

Kasten zu Nr. 11.6 und 11.7

Aus der Entschließung des Deutschen Bundestages zum 19. Tätigkeitsbericht vom 17. Februar 2005, Bundestagsdrucksache 15/4597:

„10. Der Deutsche Bundestag stellt fest, dass die fortschreitende Digitalisierung und die starke Zunahme von Datenströmen auch im nicht-öffentlichen Bereich zu einer immer stärkeren Verknüpfung von Daten führen können, die für unterschiedliche Zwecke erhoben wurden. Verbunden mit einem wachsenden Netz verschiedener Auskunftssysteme und branchenübergreifender Zentraldateien erscheint es technisch möglich, durch Profilbildung das Verhalten eines bestimmten Menschen ohne dessen Wissen und Wollen abzubilden und ihn so für Dritte berechenbar zu machen. Der Deutsche Bundestag fordert deswegen die Bundesregierung auf, zu prüfen, ob und wie, etwa durch Regelungen zur Beschränkung der Profilbildung, zur Begrenzung der zentralen Auskunfteien auf branchenspezifische Auskunftssysteme und zur Stärkung der Rechtsposition der Betroffenen gegenüber zentralen Auskunfteien und ihren Vertragspartnern, ein wirksamer Schutz der Betroffenen und ihres Restitutionsinteresses insbesondere bei Verarbeitung unrichtiger Daten erreicht werden kann. Der Bundestag bittet, ihm hierzu bis 2005 zu berichten.

…“

11.7 Der Kunde – mehr als ein Auskunftsobjekt

Das Sammeln und Verknüpfen von Daten liegt offenbar im Trend. Dieser Entwicklung muss gegengesteuert werden, um das informationelle Selbstbestimmungsrecht zu bewahren.

Die fortschreitende Digitalisierung und die damit verbundene starke Zunahme der Datenströme führen zu einer Vielzahl personenbezogener Daten. Das Selbstbestimmungsrecht des Einzelnen ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr, wie früher, auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss. Vielmehr können heute Daten über persönliche oder sachliche Verhältnisse einer Person technisch gesehen unbegrenzt gespeichert und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abgerufen werden. Sie können darüber hinaus – vor allem bei integrierten Informationssystemen – mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit beeinflussen und seine Verwendung zureichend kontrollieren kann. Auch für die Werbung, Markt- und Meinungsforschung werden mit immer neuen Ideen immer mehr Kundendaten zusammengetragen und ausgewertet, um zu immer ausgefeilteren Kundenprofilen zu kommen: Kundenkarten, Apotheken-CD, SmartCards etc. helfen dabei.

Es ist schon dann problematisch, wenn vielfältige personenbezogene Daten eines Menschen mit seinem Wissen zusammengestellt werden, weil er im Zweifelsfall die weitreichenden Konsequenzen nicht abschätzen kann. Erfolgt dies aber ohne seine Kenntnis, wird sein informationelles Selbstbestimmungsrecht stark in Mitleidenschaft gezogen.

Die technologische Entwicklung und der rasant wachsende Bestand von personenbezogenen Daten bilden die Grundlage für immer aussagepräzisere Profile. Ein aktuelles Beispiel ist eine CD für nur 15 Euro mit deutschlandweiten Informationen zu Kaufkraft und Zahlungsmoral von Bewohnern einzelner Straßenabschnitte und sogar einzelner Wohnhäuser. Die Daten stammen vor allem aus Inkassodaten und öffentlichen Schuldnerlisten. Da eine direkt personenbezogene Bewertung selbst aus Sicht des Anbieters illegal wäre, hat man bei der Bewertung immer mehrere Haushalte zusammengefasst. Kennt man die Adresse, kann man gleichwohl über das Wohnumfeld des potentiellen Arbeitnehmers oder Kunden sehr aussagekräftige Informationen erhalten. Elektronische Adress- und Telefonverzeichnisse erleichtern dabei die Erkenntnisgewinnung.

Ein weiteres datenschutzrechtliches Problem stellt das wachsende Netz verschiedener Auskunftssysteme dar. Zwar besteht grundsätzlich ein legitimes Interesse der Wirtschaft, sich vor Betrügern, schwarzen Schafen und zahlungsunfähigen oder -unwilligen Kunden zu schützen. Datenschutzrechtliche Gefahren entstehen insbesondere, wenn Systeme zusammengeschaltet werden oder wenn beliebig aus allen Systemen Informationen abgerufen werden können. Es darf nicht dazu kommen, dass z. B. ein junger Mensch, der im Alter von zwanzig Jahren auch

nach einer Mahnung seine Handyrechnung nicht bezahlen konnte, anschließend kein Konto mehr eröffnen kann, keine Wohnung findet, keinen Versicherungsvertrag bekommt und ihm selbst der Zahnersatz nur gegen Vorkasse gewährt wird, weil auch Zahnärzte über Auskunfteien die Bonität ihrer Patienten abfragen, bevor sie an ihnen kostenintensive Behandlungen vornehmen.

Besonders problematisch ist es, wenn der Einzelne ohne eigenes Fehlverhalten in ein elektronisches Warnsystem gerät, sei es aufgrund einer Verwechselung oder durch nachlässiges oder nicht vertragskonformes Meldeverhalten der einzelnen Teilnehmer solcher Systeme. Zwar schreibt das BDSG vor, dass bestrittene Forderungen gesperrt werden müssen bzw. erst gar nicht in ein Auskunftssystem gemeldet werden dürfen. Die Einhaltung dieser Vorgabe wird jedoch nur stichprobenartig von den Auskunfteien überprüft. So belegen viele Eingaben Betroffener, dass Gläubiger bei streitigen Forderungen oftmals mit einer Meldung drohen, um den Schuldner zu einer Anerkennung der Forderung zu „bewegen".

Aus meiner Sicht reicht es nicht aus, dass die jeweils zuständige Datenschutzaufsichtsbehörde im Einzelfall eines Gesetzesverstoßes einschreitet. Ich trete vielmehr dafür ein, dieser besorgniserregenden Entwicklung auch datenschutzpolitisch zu begegnen und habe – meiner gesetzlichen Aufgabe gemäß – dem Deutschen Bundestag verschiedene Lösungsmöglichkeiten aufgezeigt:

Durch gesetzliche Klarstellung sollte dafür gesorgt werden, dass umfassende Zentraldateien durch branchenspezifische Auskunftssysteme abgelöst werden. Nach geltendem Recht gilt für Auskunfteien und Warndateien der § 29 BDSG. Danach dürfen Daten, die eine Auskunftei in ihrem System gespeichert hat, an einen Dritten übermittelt werden, wenn dieser ein berechtigtes Interesse an der Kenntnis der Daten glaubhaft machen kann und der Betroffene kein schutzwürdiges Interesse an der Nichtübermittlung hat.

Unter Berufung auf diese generelle Regelung haben Auskunfteien Zentraldateien aufgebaut, auf die ungefiltert Zugriff genommen werden kann. Hier könnte eine gesetzliche Begrenzung auf branchenspezifische Auskunftssysteme Abhilfe schaffen, die dem Schutzbedürfnis einzelner Wirtschaftssparten angemessen Rechnung tragen und zugleich dem berechtigten Schutzinteresse des Betroffenen genügen.

Darüber hinaus wäre ein gesetzlicher Folgenbeseitigungsanspruch hilfreich: Eingaben belegen, dass viele Bürger ohne eigenes Fehlverhalten in elektronische Warnsysteme geraten, sei es aufgrund einer Verwechslung oder durch sonstige Systemfehler. Selbst wenn die Auskunftei das fehlerhafte Datum berichtigt, erfährt der Betroffene im Regelfall nicht, an wen das falsche Datum bereits übermittelt wurde und welcher Schaden dadurch entstanden ist. Auskunfteien berufen sich in diesen Fällen häufig darauf, nicht gespeichert zu haben, an wen sie wann welche Daten herausgegeben haben. Was für die Auskunftei nur ein „nicht korrektes Datum" unter Millionen anderer Daten ist, kann aber für den Betroffenen existenzgefährdend sein.

Abhilfe könnte ein gesetzlicher Anspruch schaffen, der bei Weitergabe unrichtiger Informationen oder im Falle rechtswidriger Übermittlungen der verantwortlichen Stelle aufgibt, daraus resultierende Folgen für den Betroffenen selbst zu beseitigen, und zwar nicht nur im eigenen System, sondern auch überall dort, wo sich durch Fortpflanzung des Fehlers für den Betroffenen nachteilige Auswirkungen ergeben haben könnten. Konkret müsste die Auskunftei alle die Stellen, an die sie das unrichtige Datum übermittelt hat, von der Unrichtigkeit verständigen. Auch die auf fehlerhaften Daten basierenden Score-Werte müssten korrigiert werden.

Die parlamentarischen Beratungen dauern noch an.

11.8 Zentralruf der Autoversicherer

Eine Datenschutzkontrolle bei dem von der Versicherungswirtschaft eingerichteten Zentralruf der Autoversicherer hat zu einer verbesserten technisch-organisatorischen Absicherung des Verfahrens beigetragen.

In Umsetzung einer EU-Richtlinie über die Kraftfahrzeug-Haftpflichtversicherung (EU-RL 2000/26/EG vom 16. Mai 2000) richtete der Gesetzgeber mit Wirkung vom 1. Januar 2003 eine nationale Auskunftsstelle ein. Sie erteilt Geschädigten, die Schadensersatzansprüche geltend machen wollen, die hierfür erforderlichen Auskünfte. Durch § 8a Pflichtversicherungsgesetz (PflVG) wurden die Aufgaben und Befugnisse der Auskunftsstelle der GDV Dienstleistungs-GmbH & Co. KG – „Zentralruf der Autoversicherer" – in Hamburg (GDV) übertragen. Bei diesem Unternehmen handelt es sich um eine von der Versicherungswirtschaft eingerichtete nicht-öffentliche Stelle, die den Zentralruf der Autoversicherer bereits seit längerem betreibt und Verkehrsunfallgeschädigten und deren Rechtsvertretern die umgehende Kontaktaufnahme zur Kraftfahrzeug-Haftpflichtversicherung des Unfallgegners ermöglicht. Soweit ihr öffentlich-rechtliche Aufgaben gesetzlich übertragen wurden, gilt die GDV seit dem 1. Januar 2003 gemäß § 2 Abs. 4 Satz 2 BDSG als öffentliche Stelle des Bundes. Aus diesem Grund ging die Zuständigkeit für die Datenschutzkontrolle auf mich über.

Kasten zu Nr. 11.8

Zentralruf der Autoversicherer

Der Zentralruf der Autoversicherer dient der gesetzlichen Auskunftsverpflichtung, bei welchem Versicherer am Schadenstag eine Kraftfahrzeug-Haftpflichtversicherung bestand und wer Schadensregulierungsbeauftragter des Versicherers ist. Zu diesem Zweck werden gemäß der Verfahrensbeschreibung Name, Anschrift und Kommunikationsdaten des Versicherungsunternehmens bzw. des Schadensregulierungsbeauftragten, die Police-Nummer sowie das Autokennzeichen erhoben, gespeichert und genutzt. Aus Datenschutzsicht ist von besonderer Bedeutung, dass in der Datenbank weder Namen noch Anschriften der betroffenen Personen gespeichert sind. Für die Identifizierung der Schadensbeteiligten wird lediglich das amtliche Kennzeichen des Fahrzeugs und die Nummer des Versicherungsscheins verwendet, so dass die Person des Kraftfahrzeughalters praktisch pseudonymisiert ist.

Bereits längere Zeit vor dem Inkrafttreten des § 8a PflVG habe ich mit dem Gesamtverband der Deutschen Versicherungswirtschaft und der GDV die mit dem Verfahren zusammenhängenden datenschutzrechtlichen Fragen erörtert. Besondere Aufmerksamkeit galt dabei dem automatisierten Abrufverfahren im Sinne von § 10 BDSG. Da ich frühzeitig beteiligt wurde, konnte ich auf eine datenschutzgerechte Gestaltung des Verfahrens hinwirken, insbesondere auf Änderungen bzw. Ergänzungen des Vertragsentwurfs über Auftragsdatenverarbeitung und Dienstleistungen mit den einzelnen Versicherungsunternehmen. Eine wesentliche Forderung war daneben die grundlegende Überarbeitung des Sicherheitskonzepts, vor allem hinsichtlich der technisch-organisatorischen Trennung der Verarbeitung personenbezogener Daten für Aufgaben des Zentralrufs von den für andere Geschäftsfelder geführten Datenbanken (Trennungsgebot gemäß Anlage zu § 9 BDSG Nr. 8).

Kurze Zeit nachdem die GDV die Aufgaben als deutsche Auskunftsstelle nach § 8a PflVG übernommen und das automatisierte Abrufverfahren eingeführt hatte, habe ich bei der GDV das Verfahren „Zentralruf der Autoversicherer“ sowie das neue automatisierte Abrufverfahren geprüft. Gravierende datenschutzrechtliche Mängel wurden dabei nicht festgestellt. Zu bemängeln war allerdings, dass das automatisierte Online-Abrufverfahren zwar einen sicheren Zugang durch Verschlüsselung und Authentifizierung vorsah, bei der Zulassung zum Online-Verfahren dem Antragsteller bzw. Vertragspartner jedoch die Zugangsdaten, darunter Benutzername und unveränderliches Passwort, offen per E-Mail übermittelt wurden. Daraufhin hat die GDV eine Systemänderung zugesagt, durch die eine Änderung des Passwortes durch den Nutzer, z. B. bei seiner ersten Anmeldung, zwingend vorgegeben wird. Die Zugangsdaten werden auf meine Anregung hin jetzt auf dem Postweg übermittelt. Auch die weiteren festgestellten kleineren Mängel wurden zwischenzeitlich weitestgehend beseitigt.

11.9 Deutsches Forum für Kriminalprävention

Das Deutsche Forum für Kriminalprävention (DFK) verfolgt einen gesamtgesellschaftlichen Ansatz der Kriminalprävention. Der BfD hat an den Beratungen des DFK mitgewirkt.

Die Stiftung DFK wird von Bund und Ländern sowie von privaten Stiftern getragen und versteht sich als nationale Service- und Informationsstelle für die deutsche, europäische und internationale Zusammenarbeit zur Optimierung der Kriminalprävention. Arbeitsschwerpunkte sind neben Ansätzen im primären Bereich die Reduzierung von Tatgelegenheiten und die kriminalitätseindämmende Veränderung gesellschaftlicher Strukturen. Es ist naheliegend, dass dabei auch Fragen des Datenschutzes berührt werden. Ich arbeite deshalb seit 2002 in folgenden DFK-Arbeitskreisen mit:

- Arbeitskreis „Informationsrechte und Kriminalprävention“

  Der Arbeitskreis befasst sich mit grundlegenden Fragen der Informationsbeschaffung und -nutzung bei der Kriminalprävention. Der Arbeitskreis hat einen Leitfaden zu den Möglichkeiten der Informationsgewinnung zum Schutz gegen Wirtschaftskriminalität erarbeitet.

- Arbeitskreis „Kriminalprävention und Biometrie“

  Im Arbeitskreis „Kriminalprävention und Biometrie“ wird der Einsatz der Biometrie im Spannungsverhältnis zwischen Sicherheitsbedürfnis und Schutz der Privatsphäre des Einzelnen betrachtet. Es sollen Rahmenbedingungen für die Einbindung der Biometrie in die Kriminalprävention erarbeitet werden.

  Am 31. März 2004 hat das DFK in Berlin ein Symposium zum Thema „Biometrie und Flughafensicherheit“ durchgeführt. Das dazu erstellte Arbeitspapier berücksichtigt meine datenschutzrechtlichen Forderungen leider nur ungenügend. Dies betrifft unter anderem die Ausführungen zur Videoüberwachung in Verbindung mit Gesichtserkennungssoftware oder die Nutzung von amtlichen Ausweisdokumenten mit gespeicherten biometrischen Daten für private Zwecke. Ich gehe dennoch davon aus, dass das DFK an seiner Leitlinie festhält, Sicherheitsinteressen und Datenschutz ausgewogen zu berücksichtigen.

12 Umwelt

12.1 Wo stehen denn die Mobilfunksender?

Seit 2004 können die Standorte von Mobilfunksendeanlagen aus dem Internet abgerufen werden. Da diese Veröffentlichung in das Recht auf informationelle Selbstbestimmung eingreift, wird auf meine Intervention hin derzeit eine gesetzliche Grundlage geschaffen.

Seit Anfang des Jahres 2004 ermöglicht die Reg TP probeweise eine Online-Recherche nach Messorten der EMF-(elektromagnetische Felder) Messreihen und von Standorten der in Betrieb befindlichen Mobilfunksender. Bislang waren diese Daten nicht der Öffentlichkeit zugänglich. Damit auch der Bürger ohne detaillierte Fachkenntnis eine für ihn lesbare und verständliche Informationsquelle vorfindet, wurden die Inhalte der Datenbank visuell aufbereitet. Die Darstellung wurde für alle Standorte bundesweit einheitlich gestaltet.

Eine Veröffentlichung in dieser Art lässt Rückschlüsse auf den Eigentümer der Immobilie zu, auf der sich die Sendeanlage befindet, und bedarf deshalb einer gesetzlichen Grundlage. Vor diesem Hintergrund habe ich das Vorgehen der Reg TP nur unter der Bedingung akzeptiert, dass eine Rechtsgrundlage erarbeitet wird. Daraufhin hat das BMWA vorgeschlagen, die Veröffentlichung von Standorten von Mobilfunksendeanlagen durch das Gesetz zur Information der Öffentlichkeit über elektromagnetische Felder (EMF-InfoG) zu regeln. Der Ausgleich zwischen Datenschutz- und Informationsinteressen erfolgt durch die Wahl einer kartographischen Darstellung anstelle einer Auflistung nach Straße und Hausnummer. Maßstab und Darstellungsform der Karte sind so zu wählen, dass das

betroffene Grundstück grundsätzlich nicht schon aus dem Kartenmaterial entnommen werden kann. Damit soll eine Ermittlung der Eigentümer in der Mehrzahl aller Fälle verhindert werden. Der Entwurf befindet sich zur Zeit in der Ressortabstimmung.

Link: http://emf.regtp.de

12.2 Das Gentechnikgesetz – öffentliche Grundstücksregister

Nach der Neuordnung des Gentechnikgesetzes wird es auch für die Öffentlichkeit möglich sein, in bestimmte Daten eines Standortregisters Einblick zu nehmen, um Aufschluss über die Freisetzung gentechnisch veränderter Organismen zu erhalten.

Das Gesetz zur Neuordnung des Gentechnikrechts sieht erstmals die Schaffung eines öffentlichen Registers über Grundstücke vor, auf denen gentechnisch veränderte Organismen entweder freigesetzt oder angebaut werden. Diese Regelung in § 16a des Gesetzes setzt die entsprechende Richtlinie 2001/18/EG um. Dieses Standortregister soll zum einen den Behörden die Überwachung etwaiger Auswirkungen der gentechnisch veränderten Organismen ermöglichen und zum anderen Transparenz für die Öffentlichkeit herstellen. Da in das Register personenbezogene oder personenbeziehbare Daten aufgenommen werden sollten, habe ich während des Gesetzgebungsverfahrens gefordert, die Eingriffstiefe so gering wie möglich zu halten. Denn die Angabe des Grundstücks durch die Bezeichnung des Flurstücks ist eine personenbeziehbare Angabe, bei der es gerade in kleinen Gemeinden leicht möglich ist, den jeweiligen Eigentümer des Grundstücks zu identifizieren.

Im weiteren Verlauf der Arbeiten an dem Gesetzentwurf wurde das Register in einen allgemein zugänglichen und einen nicht allgemein zugänglichen Teil aufgeteilt, um zu einer datenschutzgerechten Lösung zu kommen. Der allgemein zugängliche Teil enthält dabei keine personenbezogenen Daten, sondern nur die Bezeichnung und Eigenschaften der Organismen sowie die Postleitzahl und den Ort der Freisetzung bzw. des Anbaus. Um die zusätzlichen Informationen des nicht allgemein zugänglichen Teils zu erhalten, muss der Interessent sein berechtigtes Interesse an den Auskünften glaubhaft machen. Ferner darf kein Grund zu der Annahme bestehen, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Auskunft hat. Bei den zusätzlichen Informationen, die der Interessent unter den genannten Voraussetzungen bekommen kann, handelt es sich einmal um das Grundstück der Freisetzung bzw. des Anbaus und seine Größe und beim Anbau gentechnisch veränderter Organismen um den Namen und die Anschrift desjenigen, der die Fläche bewirtschaftet. Mit Blick auf die dadurch gewonnene Transparenz für die Allgemeinheit ist dies datenschutzrechtlich vertretbar.

12.3 Novellierung des Umweltinformationsgesetzes

Durch die Novellierung des Umweltinformationsgesetzes (UIG) soll der Anspruch der Öffentlichkeit auf Zugang zu umweltbezogenen Informationen erweitert und ihre Verfügbarkeit und Verbreitung, insbesondere über elektronischen Medien, gefördert werden.

Die Neufassung des UIG soll in erster Linie das geltende Recht für die informationspflichtigen Stellen des Bundes an die zwingenden Vorgaben der Richtlinie 2003/4/EG anpassen, die bis Anfang 2005 in nationales Recht umzusetzen ist. Dies soll den Zugangsanspruch der Öffentlichkeit zu bei öffentlichen Stellen vorhandenen Umweltinformationen erweitern, um deren Beteiligung an umweltbezogenen Entscheidungen zu ermöglichen und so einen Beitrag zum Umweltschutz zu leisten. Dabei spielt es keine Rolle, ob die öffentlichen Stellen spezielle Aufgaben im Rahmen des Umweltschutzes haben oder nicht. Der Begriff der Umweltinformationen selbst wird präzisiert, in dem die einzelnen Umweltbestandteile wie z. B. Luft, Wasser und Boden in weitere Einzelteile zerlegt und genauer aufgelistet werden. Um den Zugang der Öffentlichkeit zu erleichtern, müssen die informationspflichtigen Stellen die Öffentlichkeit in angemessenem Umfang auch aktiv und systematisch über die Umwelt unterrichten. Ferner haben sie darauf hinzuwirken, dass die bei ihnen vorhandenen Umweltinformationen zunehmend in elektronischen Datenbanken gespeichert werden, die über elektronische Kommunikationswege abrufbar sind.

Zu Beginn des Gesetzgebungsverfahrens enthielt der Gesetzentwurf einige datenschutzrechtlich bedenkliche Regelungen und Formulierungen. So war angedacht, das Recht auf informationelle Selbstbestimmung einzuschränken. Derzeit besteht kein Auskunftsanspruch, soweit durch das bekannt werden der Informationen personenbezogene Daten offenbart und dadurch schutzwürdige Interessen der Betroffenen beeinträchtigt würden. Geplant war stattdessen die Einführung einer Vorschrift, die den Ermessenspielraum für die Verwaltung unangemessen erweitert hätte. Im Rahmen meiner Beratung konnte ich aber eine datenschutzgerechte Lösung erreichen, der zufolge entweder die Betroffenen zustimmen oder das öffentliche Interesse an der Bekanntgabe überwiegen muss.

13 Telekommunikations- und Teledienste

13.1 Novellierung des Telekommunikationsgesetzes

Das Telekommunikationsgesetz wurde nach Vorgaben der EU überarbeitet; es hat einige wichtige Änderungen mit sich gebracht.

Die Europäische Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) vom 12. Juli 2002 sollte bis 31. Oktober 2003 in nationales Recht umgesetzt werden. In Deutschland erfolgte die Umsetzung verspätet durch Inkrafttreten des Telekommunikationsgesetzes (TKG) am 26. Juni 2004. Der Datenschutz ist jetzt einheitlich im siebten Teil des TKG geregelt, nicht mehr zusätzlich in einer Telekommunikations-Datenschutzverordnung, die in das Gesetz eingegliedert wurde. Ich begrüße dies, da hierdurch eine Vereinfachung im Datenschutz erreicht und Doppelregelungen abgeschafft wurden.

Kasten zu Nr. 13.1.1

Entschließung zwischen der 66. und 67. Konferenz der Datenschutzbeauftragen des Bundes und der Länder vom 21. November 2003

Gravierende Verschlechterung des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar – entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigten, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PINs, PUKs usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu machen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

Die Datenschutzrichtlinie enthält technikneutrale Regelungen für alle Bereiche der elektronischen Kommunikation. Erfasst werden dabei neben Telekommunikationsdiensten auch die sog. Tele- und Mediendienste, d. h. Angebote im Internet. Der deutsche Gesetzgeber ist der europäischen Vorgabe nicht gefolgt, die Regelungen für die Bereiche Telekommunikation sowie Tele- und Mediendienste zusammenzuführen. Da heute diese Dienste immer mehr zusammenwachsen und eine Unterscheidung oft sehr problematisch ist, hätte ich es begrüßt, wenn eine einheitliche Rechtsgrundlage geschaffen worden wäre. Durch die Bezugnahme auf die Rahmenrichtlinie 2002/21/EG in der Begründung zum TKG wird aber deutlich, dass die sog. Internet-Access-Provider unter die Vorschriften des TKG fallen.

Neu ins Gesetz aufgenommen wurde eine Regelung zur Nutzung von Standortdaten im Mobilfunkbereich. Diese

dürfen nur nach Information des Kunden und mit dessen Einwilligung genutzt werden. Außerdem muss dieser die Möglichkeit haben, die Einwilligung zurückzunehmen. Allerdings hat der Gesetzgeber keine konkreten Regelungen für die Umsetzung dieser Vorgaben getroffen. Es soll zunächst den Telekommunikationsunternehmen überlassen bleiben, Lösungen für die unterschiedlichen Dienste zu finden. Für Notrufstellen gibt es eine Sonderregelung. Bei diesen werden die Standortdaten auch zur Verfügung gestellt, wenn der Kunde keine Einwilligung gegeben hat.

Im Gegensatz zur alten Rechtslage ist jetzt die sog. Inverssuche erlaubt, d. h. die Auskunft über Name und gegebenenfalls auch die Anschrift einer Person von der nur die Telefonnummer bekannt ist. Voraussetzung dafür ist aber, dass der Kunde in einem Kundenverzeichnis eingetragen ist und darauf hingewiesen wurde, dass er der Inverssuche widersprechen kann (vgl. Nr. 13.1.3).

Eine Vorratsdatenspeicherung wird es auch in Zukunft im neuen TKG nicht geben (vgl. Nr. 13.1.1).

13.1.1 Speicherung von Daten auf Vorrat oder nicht?

Bei der Novellierung des TKG wurde keine Vorratsdatenspeicherung eingeführt. Auch auf europäischer Ebene sollte auf eine Verpflichtung zur Speicherung von Telekommunikationsdaten verzichtet werden.

Nach alter Rechtslage durften die Verkehrsdaten grundsätzlich um drei Stellen verkürzt bis zu sechs Monate gespeichert werden. Dies hat sich mit dem neuen TKG geändert. Jetzt dürfen die Diensteanbieter im Regelfall alle entstehenden Verkehrsdaten unverkürzt bis zu sechs Monaten nach Versendung der Rechnung speichern. Allerdings kann der Kunde auch weiterhin die Löschung der Daten oder eine Kürzung um drei Stellen nach Rechnungsversand wählen. Die Datenschutzbeauftragten des Bundes und der Länder haben sich in einer Entschließung gegen diese Änderung gewandt, durch die das bisherige Datenschutzniveau von der Initiative der Betroffenen abhängig gemacht wird (vgl. Kasten zu Nr. 13.1.1). Im Gesetzgebungsverfahren hatte der Rechtsausschuss des Bundesrates sogar gefordert, eine Pflicht zur Vorratsdatenspeicherung einzuführen. Auch aufgrund der von den Datenschutzbeauftragten geäußerten verfassungsrechtlichen Bedenken wurde diese Verpflichtung nicht in das TKG übernommen. Verfassungsrechtlich bedenklich wäre eine solche Verpflichtung insbesondere, weil die obligatorische Datenspeicherung ganz überwiegend rechtstreue Nutzer der Telekommunikationsdienste betreffen und damit in unverhältnismäßiger Weise sowohl in das Fernmeldegeheimnis als auch in das Recht auf informationelle Selbstbestimmung eingreifen würde.

Über die Einführung einer Verpflichtung zur Vorratsdatenspeicherung wird jedoch weiter diskutiert. So haben Frankreich, Irland, Schweden und das Vereinigte Königreich auf EU-Ebene den „Entwurf eines Rahmenbeschlusses über die Vorratspeicherung von Daten, die in Verbindung mit der Bereitstellung öffentlicher elektronischer Kommunikationsdienste verarbeitet und aufbewahrt werden, oder von Daten, die in öffentlichen Kommunikationsnetzen vorhanden sind, für die Zwecke der Vorbeugung, Untersuchung, Feststellung und Verfolgung von Straftaten, einschließlich Terrorismus“ vorgelegt. Eine abschließende Entscheidung hierüber ist noch nicht getroffen worden. Wie die Art. 29-Datenschutzgruppe in ihrer Stellungnahme 9/2004 vom 9. November 2004 festgestellt hat, wäre die Pflichtspeicherung aller Arten von Verkehrsdaten der Telekommunikation für Zwecke der öffentlichen Ordnung unverhältnismäßig und deshalb unzulässig nach Artikel 8 der Menschenrechtskonvention (vgl. Anlage 12).

13.1.2 Nutzung von Bestandsdaten für Werbezwecke

Im TKG wurde die Befugnis zur Nutzung der Bestandsdaten erweitert.

Nach alter Rechtslage durften Telekommunikationsanbieter die Bestandsdaten ihrer Kunden (Namen, Anschrift, …) für Werbezwecke nur nutzen, wenn eine Einwilligung vorlag, während für andere Unternehmen immer schon die im BDSG enthaltene Regelung galt, die die Nutzung der Daten nur verbietet, wenn ein Kunde Widerspruch eingelegt hat. Eine derartige Widerspruchslösung (opt-out) wurde jetzt auch ins TKG übernommen. Danach dürfen jetzt die Rufnummer sowie die Post- und E-Mail-Adresse für die Versendung von Text- und Bildmitteilungen verwendet werden. Diese neue Möglichkeit gilt aber nur im Rahmen einer bestehenden Kundenbeziehung und nur für Eigenwerbung der Unternehmen. Außerdem muss der Kunde darüber informiert werden, dass er jederzeit der Nutzung seiner Daten für Werbezwecke widersprechen kann.

Außerhalb bestehender Kundenbeziehungen und für die Nutzung anderer Daten als Rufnummer und Adresse gilt weiterhin der Grundsatz, dass eine Einwilligung des Kunden vorliegen muss. Andernfalls ist die Nutzung der Daten für Werbezwecke nicht zulässig. Dies betrifft insbesondere die sog. offenen Call-by-Call-Dienste, bei denen typischerweise keine dauerhafte Kundenbeziehung besteht. Auch die Weitergabe an Dritte darf nur mit der Einwilligung des Kunden erfolgen.

13.1.3 Neuer Telefonauskunftsdienst „Name und Adresse zur Rufnummer“

Nach dem neuen TKG ist nun – unter bestimmten Umständen – in Deutschland die sog. Rückwärts- bzw. Inverssuche erlaubt.

Das neue TKG regelt in § 105 Abs. 3 die sog. Rückwärts- bzw. Inverssuche. Danach kann man unter bestimmten Voraussetzungen bei der Telefonauskunft durch die Angabe der Rufnummer den Namen sowie die Anschrift des Teilnehmers erfragen. Dies ist aber nur

erlaubt, wenn der Kunde mit diesen Daten im Telefonbuch oder einem öffentlichen elektronischen Kundenverzeichnis eingetragen ist und gegen eine Inverssuche keinen Widerspruch eingelegt hat. Auf dieses Widerspruchsrecht, das nicht befristet ist, muss ihn sein Diensteanbieter hinweisen.

Bis zur Novellierung des TKG war die Inverssuche in Deutschland nicht erlaubt. Man erhielt von der Telefonauskunft die Telefonnummer und die Adresse eines Teilnehmers nur dann, wenn man diesen namentlich kannte. Telefonkunden müssen sich jetzt entscheiden, ob sie der neuen Invers-Telefonauskunft „Name zur Rufnummer" widersprechen wollen.

Angesichts steigender Werbebelästigungen und eines florierenden Adresshandels sollte jede zusätzliche Datenweitergabe sorgfältig überdacht werden. Die Adressdaten der Inverssuche können zum Beispiel für Werbeansprachen von Kunden in bestimmten Wohngebieten verwendet werden, um Werbepost gezielter adressieren zu können. Auch die Bekanntgabe der Handynummer in Zeitungsannoncen, in Kontaktbörsen und Chatrooms im Internet könnte demnächst unangenehme Folgen haben, wenn statt des telefonischen Flirts ein echter Besuch vor der Tür steht.

Aus Sicht des Datenschutzes wäre es wünschenswert gewesen, die Inverssuche nur bei einer ausdrücklichen Einwilligung des Kunden zuzulassen. Der Gesetzgeber hat sich aber für eine Widerspruchslösung entschieden. Deshalb können Daten beauskunftet werden, ohne dass der Betroffene selbst aktiv geworden ist.

Bei der Unterrichtung des Kunden ist zu beachten, dass die Rechtslage eindeutig wiedergegeben wird und dass die Information als solche vom Kunden auch erkannt werden kann. Für Neukunden kann dies über eine entsprechende Abfrage bei der Antragstellung erfolgen. Problematischer gestaltet sich diese Information für Bestandskunden. So wurde von einem großen Telekommunikationsdiensteanbieter zwar ein Informationstext erarbeitet, der den rechtlichen Vorgaben entspricht. Bedauerlicherweise ist diese Information von den angeschriebenen Kunden aber vielfach nicht zur Kenntnis genommen worden, weil sie in die Rechnungsschreiben an die Kunden eingearbeitet worden war. Insbesondere bei Rechnungen, die als Einzelverbindungsnachweise ausgestaltet waren und damit in der Regel mehrere Seiten umfassten, war die Information über § 105 Abs. 3 TKG erst nach längerem Suchen aufzufinden.

13.2 Umgang von Telekommunikationsunternehmen mit personenbezogenen Daten

13.2.1 Speicherung von SMS-Inhalten zum Nachweis von Entgeltforderungen

Die Speicherung von SMS-Inhalten ist rechtswidrig und verstößt gegen das Fernmeldegeheimnis.

Durch verschiedene Eingaben habe ich erfahren, dass Diensteanbieter von sog. Premium-SMS auch deren Inhalte über einen längeren Zeitraum abspeichern. Als Rechtfertigung wurden Beweisgründe genannt, da die Inhaber von Handyanschlüssen sehr oft die Urheberschaft solcher SMS bestritten oder technische Fehler auf Seiten des Netzbetreibers anführten, um nicht bezahlen zu müssen.

Ich habe diese Problematik mit der Regulierungsbehörde für Telekommunikation und Post (RegTP) erörtert. Dabei wurde übereinstimmend festgestellt, dass diese Praxis gegen das Fernmeldegeheimnis verstößt. Diensteanbieter dürfen sich keine Kenntnis von Inhalten der Telekommunikation verschaffen, die über das für die geschäftsmäßige Erbringung dieser Dienste erforderliche Maß hinausgeht. So sind etwa die Speicherung und Kenntnisnahme von Inhalten betrieblich nicht erforderlich, um eine vertragsgemäße Leistungserbringung beweisen zu können, insbesondere weil die Speicherung der Inhalte kein tauglicher Beweis für die Urheberschaft der SMS ist, da etwaige Angaben über die Person des Anschlussinhabers leicht verfälscht werden können.

Auch der zur Begründung angeführte Zweck der Vermeidung des Versands gesetzwidriger Inhalte ist als unzulässige Inhaltskontrolle einzustufen, da diese Verwendung nicht für die Erbringung der Leistung erforderlich ist. Hierzu verweise ich auf § 8 Abs. 2 Satz 1 Teledienstegesetz, der sogar die Anbieter von Telediensten, d. h. von inhaltlichen Angeboten, von einer Verpflichtung zur Überwachung der von ihnen übermittelten oder gespeicherten Informationen ausnimmt und den Schutz des Fernmeldegeheimnis für anwendbar erklärt; dies gilt umso mehr für Telekommunikationsdienste, bei denen die technische Seite der Kommunikation noch stärker im Vordergrund steht als bei Tele- und Mediendiensten.

Ein konkludenter Verzicht der Kunden auf das Fernmeldegeheimnis durch die Nutzung des SMS-Services kann ausgeschlossen werden, da eine inhaltliche Überwachung des SMS-Verkehrs gegen die gesetzlichen Vorgaben des Datenschutz- und Telekommunikationsrechts verstößt und schon deshalb nicht den Erwartungen des allgemeinen Kundenkreises entspricht. Ebenso ist die Aufnahme eines entsprechenden Hinweises in die AGB auf keinen Fall ausreichend.

Wurde eine Speicherung der Inhalte gleichwohl vorgenommen, bleibt es den Betroffenen überlassen, hiergegen gerichtlich vorzugehen, die Löschung der Daten zu verlangen und auf ein Verwertungsverbot der rechtswidrig abgespeicherten SMS-Inhalte hinzuwirken. Darüber hinaus kann sich der Betroffene auch an die RegTP wenden.

13.2.2 Location Based Services

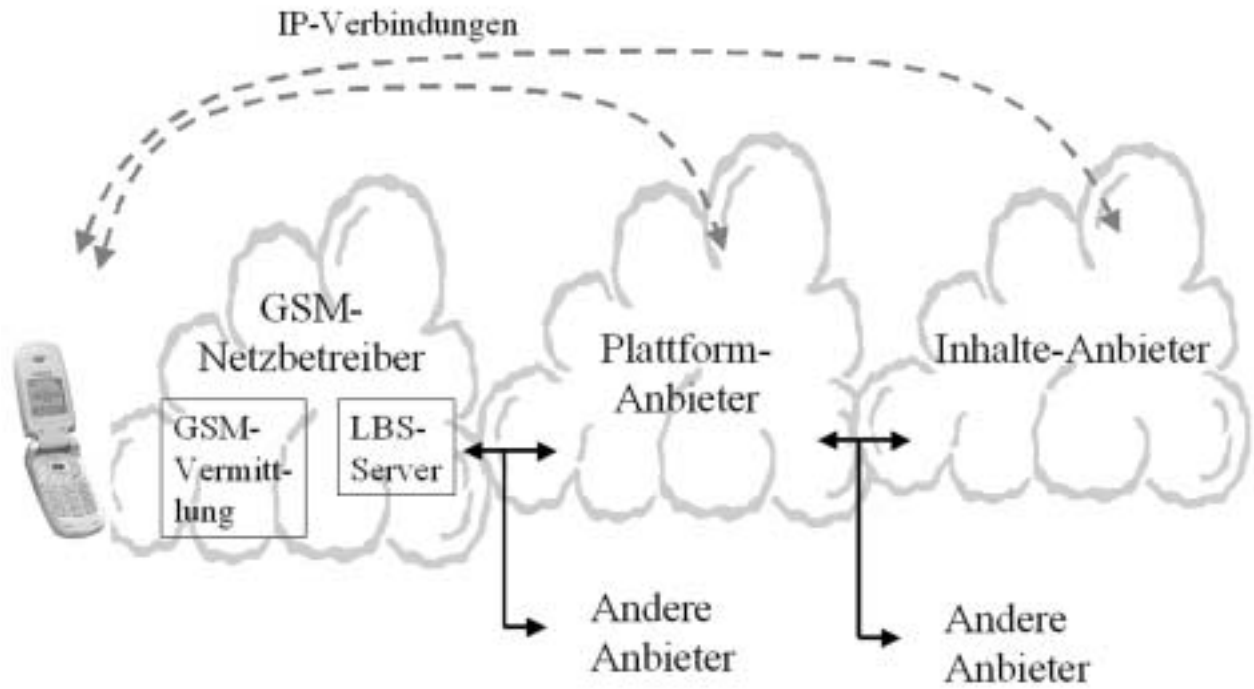
Datenschutz bei ortsbezogenen Diensten muss nicht nur von Mobilfunknetzbetreibern, sondern auch von den Anbietern dieser Dienste gewährleistet werden.

Die Ortung von Mobilfunkteilnehmern ist ein sensibles Thema (vgl. 19. TB Nr. 11.6, 11.10.4). Im Rahmen eines Beratungs- und Kontrollbesuchs bei einem Mobilfunknetzbetreiber bin ich auf ein Problem gestoßen, das unmittelbar mit der internationalen Arbeitsteilung in der Telekommunikationsbranche zusammenhängt.

Die Handyortung findet innerhalb der Mobilfunkinfrastruktur des Netzbetreibers statt, die von sog. Plattform-Anbietern genutzt werden kann. Diese stellen ihrerseits Inhalte-Anbietern einfach zu nutzende Schnittstellen zur Verfügung, die auch für andere Dienstleistungen, insbesondere für Abrechnungszwecke, Verwendung finden. Wenn ein Mobilfunkkunde etwa über die nächstgelegenen Restaurants informiert werden möchte, sorgt der Plattform-Anbieter für die Ortung des Kunden beim Netzbetreiber und die Berechnung der Dienstleistung. Der Inhalte-Anbieter liefert die Informationen über die Restaurants in der Nähe der angegebenen Koordinaten. Dafür erhält er eine Gutschrift vom Plattform-Anbieter, nicht aber die Rufnummer des Kunden, da hierfür nicht erforderlich. Er verarbeitet also keine personenbezogenen Daten, die vollständigen Daten verbleiben ausschließlich beim Plattform-Anbieter (vgl. auch Abbildung zu Nr. 13.2.2).

Abbildung 4 zu Nr. 13.2.2

Schematische Darstellung der Datenverarbeitung



Schematische Darstellung der Datenverarbeitung

Zum Zeitpunkt meines Beratungs- und Kontrollbesuchs wurde die Plattform von einem Unternehmen innerhalb des Konzernverbundes des Netzbetreibers angeboten, das seinen Sitz in einem anderen EU-Land hat. Da diese Firma als Telediensteanbieter beurteilt werden muss und zudem ihren Sitz im Ausland hat, war es mir mangels eigener Zuständigkeit nicht möglich, die dortige Datenverarbeitung zu prüfen. Anhand der freiwilligen Angaben des Plattform-Anbieters konnte aber festgestellt werden, dass dieser Protokolldateien, die auch Ortungsinformationen beinhalten, für einen – zumindest nach deutschem Recht – zu langen Zeitraum aufbewahrt. Durch organisatorische Änderungen soll dieses Problem mittelfristig behoben werden.

13.2.3 Aufbewahrungsfristen für Verkehrsdaten nach der Abgabenordnung

Die langen Aufbewahrungsfristen der Abgabenordnung gelten nicht für die Speicherung von Verkehrsdaten der Telekommunikation.

Verkehrsdaten sind gemäß § 97 Abs. 3 Telekommunikationsgesetz (TKG) grundsätzlich spätestens sechs Monate nach Versendung der Rechnung zu löschen. Bei Kontrollen habe ich allerdings wiederholt festgestellt, dass den Rechnungen beigefügte Einzelverbindungsnachweise wesentlich länger aufbewahrt wurden. Von den Unternehmen wurde auf die Aufbewahrungsfristen der Abgabenordnung (AO) verwiesen. So sind nach § 147 AO Unterlagen, die für die Besteuerung von Bedeutung sind, sechs bzw. zehn Jahre aufzubewahren.

Kasten zu Nr. 13.2.3

Verkehrsdaten sind Daten, die bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden (§ 3 Nr. 30 TKG). Diese Daten unterliegen dem besonderen Schutz des Fernmeldegeheimnisses.

Auf meine Anregung konnte mit dem BMF, den obersten Finanzbehörden der Länder und dem BMJ zu dieser Problematik Einvernehmen erzielt werden: Danach besteht aus steuerlicher Sicht grundsätzlich keine Aufbewahrungspflicht für die Verkehrsdaten durch den Verbindungsnetzbetreiber. Die Aufbewahrung der Rechnung ohne Einzelverbindungsnachweis (EVN) ist ausreichend. Wird in einer Rechnung jedoch nur die Art der Leistung beschrieben und zu deren Umfang auf den als Anlage beigefügten EVN verwiesen, wird dieser Bestandteil der Rechnung und ist mit aufzubewahren. Ich habe deshalb angeregt, die Rechnungen so zu gestalten, dass die erbrachten Leistungen auch ohne Rückgriff auf den EVN nachvollzogen werden können.

Ein vergleichbares Problem betraf die private Nutzung arbeitgebereigener Computer und Telekommunikationseinrichtungen durch den Arbeitnehmer. Bei den Aufzeichnungs- bzw. Aufbewahrungspflichten des Umsatzsteuergesetzes (UStG) muss zunächst unterschieden werden, ob die Privatnutzung gegen Entgelt erfolgt oder nicht. Überlässt der Arbeitgeber seinen Arbeitnehmern die Nutzung betrieblicher Computer oder Telekommunikationsgeräte entgeltlich für Privatzwecke, so handelt es sich um einen steuerbaren und steuerpflichtigen Vorgang. Es liegt eine entgeltliche sonstige Leistung vor. Bemessungsgrundlage für diese Umsätze ist grundsätzlich das vereinbarte bzw. gezahlte Entgelt i. S. d. § 10 UStG. In diesen Fällen ist davon auszugehen, dass die betroffenen Arbeitnehmer zumindest konkludent der Aufzeichnung der zur Abrechnung erforderlichen Daten zugestimmt haben, was regelmäßig zur Durchführung der Umsatzbesteuerung ausreichen dürfte.

Werden dem Arbeitnehmer betriebliche Computer oder Telekommunikationseinrichtungen kostenlos für Privatzwecke überlassen, erbringt der Arbeitgeber ihnen gegenüber grundsätzlich steuerpflichtige unentgeltliche Wertabgaben i. S. d. § 3 Abs. 9a UStG. Bemessungsgrundlage sind sämtliche auf die private Nutzung entfallenden Kosten. Eine Individualisierung der Daten (Aufzeichnung der konkreten Verkehrsdaten) ist aus umsatzsteuerrechtlicher Sicht nicht notwendig; es genügt, für den jeweiligen Abrechnungszeitraum die Entgelte je Arbeitnehmer aufzuzeichnen.

Für den Arbeitnehmer sind die Vorteile aus der privaten Nutzung von betrieblichen Computern und Telekommunikationseinrichtungen seit dem Jahre 2000 nach § 3 Nr. 45 Einkommensteuergesetz steuerfrei. Demnach besteht auch hier keine Erfordernis für die Aufbewahrung von Verkehrs- bzw. Nutzungsdaten über privat genutzte arbeitgebereigene Computer.

13.2.4 „Happy Digits“ machen nicht alle Kunden glücklich

Eklatanter Verstoß gegen Datenschutzrechte von Kunden durch missbräuchliche Anmeldung zur Teilnahme an einem Bonusprogramm.

Wer kennt sie nicht, die Frage: „Haben Sie schon eine Kundenkarte?“ Hierbei handelt es sich um die guten alten Rabattmarken in neuer Verpackung. Immer mehr Firmen in der modernen Wirtschaftswelt versuchen, durch solch spezielle Kundenbindungsprogramme den Umsatz zu steigern. Auch Unternehmen aus dem Bereich der Telekommunikation bedienen sich dieser Marketinginstrumente.

Auf Grund mehrerer Bürgereingaben stellte ich fest, dass Kunden eines großen Telekommunikationsdiensteanbieters immer wieder Post von einer Firma erhielten, die das Bonusprogramm „Happy Digits“ betreut. Darin wurden sie als neue Teilnehmer begrüßt, obschon sie kein entsprechendes Einverständnis erteilt oder sogar der Teilnahme an diesem Programm ausdrücklich widersprochen hatten.

Meine Recherchen ergaben, dass es Mitte des Jahres 2003 zu Unregelmäßigkeiten bei der Meldung neuer Teilnehmer für das Programm durch den Telekommunikationsdiensteanbieter gekommen war. Mitarbeiter des Diensteanbieters hatten Kunden ohne ihr Einverständnis für

„Happy Digits“ angemeldet. Von Seiten des Unternehmens wurde dieser Verdacht überprüft und bestätigt. Diese Mitarbeiter haben durch ihr Verhalten eklatant gegen datenschutzrechtliche Vorschriften verstoßen und das Recht der betroffenen Kunden auf informationelle Selbstbestimmung verletzt. Ein solches Fehlverhalten – so unangenehm es für den Betroffenen auch ist – lässt sich leider nicht immer vollkommen vermeiden.

Mittlerweile hat die Firma in allen bekannt gewordenen Fällen die Daten gelöscht. Da das Unternehmen glaubhaft versicherte, dass es nicht zu weiteren unberechtigten Datenübermittlungen gekommen ist, war in diesen Fällen aus Sicht des Datenschutzes nichts weiter zu veranlassen. Unabhängig davon habe ich aber im Rahmen meiner Datenschutzaufsicht mit dem Diensteanbieter bereits generell erörtert, durch welche Maßnahmen die Fehlerquote zukünftig möglichst gering gehalten werden kann. Die Bemühungen um eine weitere Optimierung des Verfahrens werden fortgesetzt.

13.2.5 Neues Leistungsmerkmal „Kickout“

Ein neues Merkmal soll den Telefonnutzern ermöglichen, sich gegen belästigende Anrufe zu schützen.

Bisher gab es nur für Callcenter die technische Möglichkeit, belästigende oder störende Anrufe – sog. Junk Calls – abzuweisen (vgl. 19. TB Nr. 11.10.1; 18. TB Nr. 10.14). Ein Telekommunikationsunternehmen hat im Berichtszeitraum die Idee eines neuen Leistungsmerkmals entwickelt, mit dessen Hilfe es auch jedem Einzelnen ermöglicht werden soll zu bestimmen, ob störende Anrufe bei ihm ankommen oder erst gar nicht zu ihm durchgestellt werden. Der Kunde kann durch eine bestimmte Tastenkombination an seinem Telefon eine Rufnummer in die Liste der zu sperrenden Rufnummern eintragen. Die Sperrung kann während einer Verbindung, nach einer Verbindung oder nach einem störenden Anklingeln erfolgen. Sie ist unabhängig von der Frage, ob die Rufnummer angezeigt wird oder nicht. Die Liste kann maximal zehn Rufnummern enthalten, danach wird sie überschrieben. Der Kunde kann die gesamte Liste auch selbst löschen, er kann sie aber nicht einsehen. Es ist deshalb unmöglich, die Rufnummern von Personen zu erfahren, die keine Rufnummernanzeige haben. Die Liste der vom Kunden gesperrten Rufnummern wird in der Vermittlungsstelle gespeichert. Eine Einsichtnahme ist nur durch die für die Systemtechnik zuständigen Techniker möglich.

„Kickout“ stellt eine Alternative zur sog. Fangschaltung dar. Es ist als datenschutzrechtlich milderes Mittel anzusehen, weil dem Kunden, der nicht belästigt werden will, keine personenbezogenen Daten bekannt gegeben werden. Bedenklich ist aus Sicht des Datenschutzes, dass keine automatische Löschungsfrist für die einmal gesperrten Telefonnummern festgelegt wird. Deshalb kann eine Nummer über einen sehr langen Zeitraum in der Liste der abzuweisenden Rufnummern verbleiben, wenn diese nicht überschrieben wird. Ich habe mich gegenüber dem Unternehmen dafür eingesetzt, regelmäßige allgemeine Löschungsfristen einzuführen, sobald dies technisch möglich ist.

13.2.6 Zugriffsmöglichkeiten auf Kundendaten im T-Punkt

Lesender Zugriff auf Bestands- und Verbindungsdaten für Mitarbeiter im T-Punkt nur bei sorgfältiger Identifikations- bzw. Legitimationsprüfung.

Ein Telekomkunde, der zwecks Beratung über einen Produktwechsel eine Vertriebsstelle der Deutschen Telekom AG (T-Punkt) aufgesucht hatte, zeigte sich in einer Eingabe an mich darüber verwundert, dass der Mitarbeiter nur auf Grund der Telefonnummer seine letzte Telefonrechnung einsehen konnte. Der Kunde machte insbesondere Bedenken wegen der Missbrauchsmöglichkeiten geltend, die sich vor allem auf den ebenfalls einsehbaren Einzelverbindungsnachweis bezogen. Die Eingabe gab mir Veranlassung, die internen Zugriffsmöglichkeiten auf Kundendaten im T-Punkt datenschutzrechtlich zu überprüfen.

Die Deutsche Telekom AG bestätigte mir, dass die Mitarbeiter in den T-Punkten zur Kundenbetreuung einen generellen Zugriff auf Rechnungsdaten der Kunden benötigen, darunter auch auf die mit der Rechnung versandten EVN. Obwohl der Kunde auch die Möglichkeit habe, für die Klärung von Fragen zu einem bestehenden Vertragsverhältnis oder wegen einer Rechnungsreklamation eine kostenlose Telefon-Hotline zu nutzen, würden Kunden mit solchen Anliegen oft auch die T-Punkte aufsuchen. Der Zugriff der Mitarbeiter auf Rechnungsdaten sei allerdings beschränkt und schließt den Ausdruck der Telefonrechnung sowie des EVN aus. Anlässlich der aktuellen Überprüfung sei zwar festgestellt worden, dass es in einigen T-Punkten wegen eines technischen Fehlers vorübergehend doch möglich gewesen sei, die Daten auszudrucken. Dieser Fehler sei jedoch inzwischen behoben worden. Darüber hinaus hat die Deutsche Telekom AG auf Grund meiner Nachfrage eine betriebliche Regelung für alle T-Punkte eingeführt, die gewährleisten soll, dass Kunden- und Rechnungsdaten nur dem Anschlussinhaber selbst mitgeteilt werden. Sie sieht vor, dass der Mitarbeiter im T-Punkt zur einwandfreien Identifizierung bzw. Legitimierung die Kundennummer, das Buchungskonto, die Rechnungsnummer, Vorwahl und Rufnummer sowie Name, Anschrift und Geburtsdatum des Kunden abfragen muss. Bereits zuvor bestand eine Arbeitsanweisung, dass Dritte eine Einverständniserklärung des Kunden und ihren Personalausweis vorlegen müssen. Außerdem werden die einzelnen Zugriffe auf Kundenbestands- und Rechnungsdaten protokolliert, so dass neben anlassbezogenen Überprüfungen bei einem Missbrauchsverdacht ebenso regelmäßige stichprobenartige Kontrollen möglich und nach dem Datenschutzkonzept der Deutschen Telekom AG auch vorgesehen sind. Diese Maßnahmen, die wie bisher zusätzlich mit begleitenden regelmäßigen Schulungen der Mitarbeiter für den Umgang mit sensiblen personenbezogenen Daten verbunden werden, halte ich für angemessen und ausreichend.

13.2.7 Anonymisierung von Gerichtsurteilen bei einer Verwendung im Zivilprozess

Bei einer Weitergabe von Gerichtsurteilen sind die Persönlichkeitsrechte der Prozessbeteiligten durch die Schwärzung ihrer Namen zu wahren.

Durch die Eingabe einer Petentin wurde ich darauf aufmerksam gemacht, dass ein Telekommunikationsunternehmen im Rahmen eines Zivilprozesses Gerichtsurteile aus anderen Verfahren verwendet hat, in denen die Namen der Prozessbeteiligten nicht unkenntlich gemacht waren. Die Petentin hatte die Befürchtung, dass auch mit einem in eigener Sache ergangenen Urteil so verfahren und ihre personenbezogenen Daten im Urteilstenor ohne Anonymisierung an Dritte weitergegeben werden könnten.

Die Weitergabe von Gerichtsurteilen mit den Namen der Prozessbeteiligten kann gemäß § 28 BDSG nicht akzeptiert werden. Zwar ist die Verwendung bereits ergangener rechtskräftiger Gerichtsurteile zu Prozessführungszwecken durchaus üblich, hierfür sind jedoch die Namen der Beteiligten im Urteilstenor nicht erforderlich. Im Hinblick auf den datenschutzrechtlichen Grundsatz, personenbezogene Daten soweit wie möglich zu anonymisieren, sind vor einer Weitergabe von Urteilskopien darin enthaltene personenbezogene Daten unkenntlich zu machen.

Da es sich über den Einzelfall hinaus um ein generelles Problem handelt, habe ich das Telekommunikationsunternehmen darauf hingewiesen, dass die mit der Führung von Rechtsstreitigkeiten befassten Stellen die Notwendigkeit der Anonymisierung von Urteilskopien vor Weitergabe an Dritte zu beachten haben. Dessen Konzerndatenschutzbeauftragter hat mir daraufhin in einem Schreiben mitgeteilt, dass er meine Auffassung teilt, und versichert, künftig entsprechend zu verfahren.

13.2.8 Umfang des Auskunftsanspruches nach § 34 BDSG

Betroffene haben gegenüber Telekommunikationsunternehmen einen umfassenden Auskunftsanspruch. Dies gilt nicht in bestimmten Ausnahmefällen.

Ein wesentliches Instrument zur Wahrnehmung des Rechts auf informationelle Selbstbestimmung ist für den Einzelnen der in § 19 bzw. § 34 BDSG geregelte Anspruch auf Auskunft über die zu seiner Person gespeicherten Daten. Es verwundert daher nicht, dass in einigen Eingaben Beschwerde darüber geführt wurde, Telekommunikationsunternehmen hätten die erbetene Auskunft nach § 34 BDSG gar nicht oder nur unvollständig erteilt. Wurde eine Auskunft gar nicht erteilt, lag die Ursache häufig darin, dass die Mitarbeiter in der Kundenberatung oder im Beschwerdemanagement nicht erkannt hatten, dass es sich um ein formelles Auskunftsersuchen im Sinne von § 34 BDSG handelte. Die zumeist innerbetrieblich vorgesehene Vorlage an den Datenschutzbeauftragten oder die Rechtsabteilung unterblieb deshalb. Hier kann Besserung nur eine intensivere Datenschutzschulung der Mitarbeiter bringen, auf deren Notwendigkeit ich bei Kontrollen immer wieder aufmerksam mache.

Ein anderes Problem stellte der pauschale Kundenwunsch dar, eine umfassende Auskunft über sämtliche gespeicherten personenbezogenen Daten zu erhalten, ohne die Art der Daten näher zu bezeichnen. Zur Vermeidung eines unnötigen und unverhältnismäßigen Arbeitsaufwands bei der speichernden Stelle muss von dem Betroffenen jedoch verlangt werden können, seinen Auskunftswunsch, wie im Gesetzeswortlaut gefordert, zu präzisieren. Auf der anderen Seite darf sich das Telekommunikationsunternehmen – wie in einem Fall geschehen – nicht darauf beschränken, nur allgemein die Art der gespeicherten Daten zu nennen. Um dem Betroffenen zu ermöglichen, die Richtigkeit der gespeicherten Daten zu überprüfen, müssen diese Daten vielmehr konkret mitgeteilt werden.

In einem Fall hatte ich auf Grund einer Eingabe zu prüfen, ob die Weigerung eines Telekommunikationsunternehmens, sämtliche über den Beschwerdeführer gespeicherten Daten mitzuteilen, berechtigt war. Das Unternehmen berief sich darauf, dass es sich um Daten handele, die für eigene Zwecke des Geschäftsprozesses erhoben, gespeichert und verarbeitet werden. Nach § 34 Abs. 4 BDSG besteht in der Tat keine Auskunftspflicht, wenn der Betroffene nach § 33 Abs. 2 Satz 1 Nr. 2, 3 und 5 bis 7 BDSG nicht zu benachrichtigen ist. Darunter fallen insbesondere Daten, die ausschließlich der Datensicherung oder Datenschutzkontrolle dienen und bei denen eine Auskunft einen unverhältnismäßigen Aufwand erfordern würde. Ferner Daten, die ihrem Wesen nach wegen des überwiegenden Interesses eines Dritten geheim gehalten werden müssen. Schließlich auch Daten, die für eigene Zwecke gespeichert sind und bei denen eine Auskunft die Geschäftszwecke erheblich gefährden würde, es sei denn, dass das Interesse an der Mitteilung die Gefährdung überwiegt.

Wie der von mir überprüfte Fall zeigte, ist eine rechtliche Bewertung, welche gespeicherten Daten im konkreten Einzelfall nicht mitgeteilt werden müssen, schwierig. Die Frage kann nur unter Berücksichtigung aller Umstände des Einzelfalles und nach sorgfältiger Abwägung der widerstreitenden Interessen beantwortet werden. Keine Auskunftsverpflichtung besteht, wenn durch die Auskunft Betriebsgeheimnisse offenbart werden müssen und das Interesse des Betroffenen an der Auskunft nicht höher als das Geheimhaltungsinteresse des Unternehmens zu beurteilen ist. Gleiches gilt m. E., wenn die in Rede stehenden Daten wegen des überwiegenden rechtlichen Interesses eines Dritten (z. B. eines Mitarbeiters) geheim gehalten werden müssen. Das gilt beispielsweise hinsichtlich eines Teils der protokollierten und gespeicherten Telefonnotizen des Callcenters. Andererseits sind dort aber auch Notizen über etwaige Kundenanliegen enthalten, die u. U. Einfluss auf das bestehende Vertragsverhältnis haben. Diesbezüglich muss der Kunde die Möglichkeit haben, die richtige Wiedergabe seines Anliegens zu überprüfen, um evtl. seinen Anspruch auf Berichtigung, Löschung oder Sperrung geltend zu machen. Es bedarf in jedem Fall einer sorgfältigen Güterabwägung, ob

die in Rede stehenden Daten als Betriebsgeheimnisse bzw. Mitarbeiterdaten aufzufassen und wie sie in Bezug zu dem Auskunftsinteresse des Betroffenen zu werten sind. Eine allgemein gültige Antwort auf die Frage, welche konkreten Daten der Auskunftspflicht unterliegen und welche nicht, ist nicht möglich.

13.3 Einzelverbindungsnachweis für Strafgefangene bei der Nutzung von Calling-Card-Diensten in Justizvollzugsanstalten

Strafgefangene, die mit einem Guthabenkonto über die Telefonanlage einer Justizvollzugsanstalt telefonieren, haben keinen Anspruch auf einen Einzelverbindungsnachweis.

Im Berichtszeitraum hat mir der Berliner Datenschutzbeauftragte die Frage vorgelegt, ob die Nutzer einer in einer Justizvollzugsanstalt eingesetzten Telekommunikationsanlage Anspruch auf die Erteilung eines Einzelverbindungsnachweises (EVN) haben. Bei einem EVN handelt es sich um eine Rechnung, in der detailliert alle Anrufe aufgeführt sind, die vom Kunden zu bezahlen sind. Damit erhält der Kunde die Möglichkeit, die ihm konkret in Rechnung gestellten Dienstleistungen effektiv überprüfen zu können. Die Berliner Senatsverwaltung für Justiz vertrat die Meinung, dass ein Anspruch auf einen EVN nicht besteht.

Ich habe dieser Einschätzung im Ergebnis zugestimmt. Die Strafgefangenen telefonieren über ein Guthabenkonto, d. h. über ein System, dass vergleichbar mit einer so genannten Prepaid-Karte ist. Das bedeutet, dass der Kunde im Voraus bezahlt und dieses Guthaben im Laufe der Zeit abtelefonieren kann. Die Besonderheit des Falles besteht darin, dass die Verbindungskosten und das Restguthaben auf dem „Konto“ dem Kunden nach jedem Telefonat angesagt werden.

Die Voraussetzungen für den EVN sind in § 14 Telekommunikations-Kundenschutzverordnung geregelt. Danach besteht ein Anspruch nicht, „wenn nach der besonderen Art der Leistung eine Rechnung üblicherweise nicht erteilt wird“. Zur näheren Erläuterung wird in der amtlichen Begründung darauf verwiesen, dass damit ein Anspruch auf einen EVN, etwa beim Abtelefonieren betragsmäßig limitierter Telefonkarten sowie in vergleichbaren Fällen ausgeschlossen werden sollte.

Das vorliegende Geschäftsmodell entspricht dem Angebot von Prepaid-Karten, Daher steht auch den Strafgefangenen gegenüber ihrem Telekommunikationsdiensteanbieter kein Anspruch auf Erteilung eines EVN zu. Ein Rückgriff auf andere Vorschriften ist nicht möglich. Dies gilt insbesondere für Bestimmungen, die das Verhältnis zwischen Strafgefangenen und Strafvollzugsanstalt regeln. Die Strafgefangenen nutzen für ihre Telefonate zwar die Telekommunikationsanlage der Strafanstalt. Der Vertrag besteht aber ausschließlich mit einem privaten Telekommunikationsdienst.

13.4 Voice over IP – Neuer Dienst mit neuartigen Problemen

Eine neue Technologie für die Übertragung von Sprache birgt auch neue Herausforderungen für den Datenschutz in der Telekommunikation.

Über ein Jahrhundert lang wurde beim Telefonieren die Sprache nur analog übertragen, seit wenigen Jahrzehnten auch digital mit speziellen Protokollen, insbesondere ISDN. In den letzen Jahren zeichnet sich eine weitere Entwicklung ab, die Übertragung von Sprache über das Internetprotokoll (IP). Dies wird Voice over IP (VoIP) genannt und hat verschiedene Vorteile:

- Bei Firmennetzen bzw. privaten Telefonanlagen benötigt man keine separate Verkabelung für die Telefone, das Computernetz (meist Ethernet) kann mitbenutzt werden. Das Telefon lässt sich direkt an einen anderen Arbeitsplatz mitnehmen – bei einem leistungsfähigen Intranet auch an einen weit entfernten Standort des Unternehmens.
- Bei der internen Nutzung durch Telekommunikationsnetzbetreiber kann die preiswertere und flexiblere Technik für Computernetze verwendet werden.
- Bei dem Angebot von VoIP für Endkunden kann das VoIP-Endgerät – z. B. ein spezielles Telefon, ein klassisches Telefon mit Adapter oder ein PC – mit einem Breitbandanschluss verbunden werden, etwa DSL oder einem Firmennetz. Das „klassische“ Telefonnetz wird nicht mehr benötigt. Dadurch können Kosten gespart werden und der feste Ortsbezug entfällt. Meist sind die VoIP-Gespräche zwischen zwei Teilnehmern eines VoIP-Anbieters sogar kostenlos. Auch Zusatzdienste sind möglich bzw. einfach und kostengünstig zu realisieren.

Dabei ist zu beachten, dass sich Sicherheitsmängel im lokalen Computernetz (LAN) auch auf die Sicherheit des Telefondienstes auswirken können. VoIP unterliegt wie das herkömmliche Telefonieren dem Schutz das Fernmeldegeheimnisses. Angemessene Sicherheitsmaßnahmen sollten eigentlich selbstverständlich sein. Manche Berichte, etwa zur Sicherheit von WLAN in Unternehmen und eigene Prüferfahrungen zeigen aber, dass hier oft noch Nachholbedarf besteht.

Bei VoIP-Angeboten für Endkunden sind einige Punkte zu beachten, damit das Fernmeldegeheimnis gewahrt wird. Sind der Internetprovider und der VoIP-Anbieter nicht identisch, wird der IP-Verkehr auf unvorhersehbaren Wegen durch das Internet geleitet. Der Dienst kann unabhängig davon genutzt werden, ob sich der VoIP-Nutzer mit seinem Endgerät zuhause oder in einem brasilianischen Cafe mit WLAN-Hotspot befindet – eine Kommunikationsmöglichkeit über das Internet vorausgesetzt. Wenn ein Tischnachbar mit Laptop oder der Cafe-Besitzer neugierig sind, haben sie durchaus die Chance, das Gespräch mitzuschneiden. Gerade im Internet sind die Werkzeuge und das Wissen zum Abhören der Kommunikation weit verbreitet. Deshalb kann nur empfohlen werden, VoIP zu verschlüsseln. Damit der Nutzer in VoIP das

gleiche Vertrauen haben kann, wie in das klassische Telefonnetz, besteht dringender Handlungsbedarf für die Anbieter des Dienstes, der Endgeräte und der Software.

Für das Angebot von VoIP sind Server erforderlich, die an das Internet angebunden sind. Damit ist es einfach, über das Internet Zusatzangebote zu verwirklichen, etwa einen Verlaufsspeicher, der ähnlich wie bei den Anruflisten eines Handys darstellt, welche Gespräche geführt wurden, und wer versucht hat, anzurufen. Jedoch können die Anrufe und Anrufversuche deutlich übersichtlicher und für einen längeren Zeitraum dargestellt werden. Dies könnte für Anschlüsse, die von mehreren Personen genutzt werden, bedenklich sein. Deswegen sollte es möglich sein, solche Funktionen zu deaktivieren und auch die Speicherdauer auszuwählen. Eine Speicherung der Verkehrsdaten in einem Verlaufsspeicher ist vom Telekommunikationsgesetz (TKG) nicht vorgesehen, und somit ohne Einwilligung der Betroffenen verboten. Ein entsprechender Auftrag müsste bewusst erteilt werden, z. B. im Rahmen des Vertrages über die Nutzung des VoIP-Dienstes, und detailliert erläutert werden. Hier gibt es bei einigen Anbietern noch Nachbesserungsbedarf.

Für einen Telekommunikationsdienst sind noch andere Regelungen des TKG zu beachten, etwa dass ein Einzelverbindungsnachweis (EVN) gemäß § 99 Abs. 1 TKG explizit zu beantragen ist, wobei eine Erklärung über die Information der Mitbenutzer zu geben ist. Auch hier gehe ich davon aus, dass bei den Anbietern noch Aufklärungsarbeit über die Anforderungen des TKG zu leisten ist.

13.5 Kontrollerfahrungen mit dem automatisierten Auskunftsverfahren nach § 112 Telekommunikationsgesetz

Wieder ist ein enormer Anstieg der Abfragen zu verzeichnen.

Bereits in meinem 19. TB (Nr. 11.3.4.2) hatte ich von den Datenschutzkontrollen zum automatisierten Auskunftsverfahren berichtet. Während des Berichtszeitraums gab es nur wenige Anfragen von Polizeibehörden wegen des Verdachts auf unberechtigte Abfragen durch Innentäter. In drei Fällen konnten Daten zurückgemeldet werden, die zu einem Ermittlungsverfahren geführt haben. Die zuständigen Landesbeauftragten für den Datenschutz wurden über die Vorgänge informiert.

Dies zeigt, dass es einerseits zu einigen Missbrauchsfällen kommt, andererseits aber eine effektive Kontrolle möglich ist, wenn ein konkreter Verdacht vorliegt. Es ist zu erwarten, dass diese Kontrollmöglichkeiten einem Missbrauch vorbeugen.

Die Anzahl der Abfragen, über die ich in meinem letzten Tätigkeitsbericht berichtet habe, hat sich auch in den letzten zwei Jahren weiter erhöht, und zwar von ca. 40 000 auf ca. 50 000 Abfragen pro Woche (also etwas über zweieinhalb Millionen pro Jahr). Sicherlich ist eine Abfrage von Bestandsdaten kein allzu schwerwiegender Grundrechtseingriff, dennoch stimmt die hohe Zahl bedenklich. Ob diese Entwicklung parallel zum Anstieg der Überwachungsmaßnahmen in der Telekommunikation verläuft (vgl. Nr. 7.2), bleibt zu prüfen.

Im neuen TKG sind die Erweiterung des Datenbestands, etwa um das Geburtsdatum des Rufnummerninhabers, und Abrufmöglichkeiten unter Verwendung von unvollständigen Daten bzw. einer Ähnlichkeitsfunktion vorgesehen. Damit soll nicht nur Herr Meyer, sondern auch Herr Mayer, Herr Maier oder Herr Meier gefunden werden. Die entsprechenden Verordnungen, durch die diese gesetzlichen Vorgaben konkretisiert werden, liegen noch nicht vor. Ich werde mich dafür einsetzen, dass der Umfang der zurückzumeldenden Informationen bei Anfragen mit unvollständigen oder ähnlichen Daten sich in angemessenen Grenzen hält. Weiterhin muss die Möglichkeit zur effektiven Prüfung der Protokolle gegeben bleiben. Bereits jetzt wird die Protokolldatenbank an der Leistungsgrenze betrieben. Durch die Möglichkeit von mehrfachen Antworten und einem zu erwartenden weiteren Anstieg der Abfragen dürfte sich der Protokolldatenbestand noch deutlich vergrößern.

13.6 Auskunft an Landesdatenschutzbeauftragte über durchgeführte Telefonüberwachungen

Datenschutzaufsicht der Landesdatenschutzbeauftragten über Staatsanwaltschaften mit Hilfe des BfD gewährleistet.

Ein Bürger hatte sich an die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen gewandt, weil er befürchtete, dass die Telefonate mit seiner Rechtsanwältin zu Unrecht abgehört worden seien. Der Landesbeauftragten steht gemäß § 2 Datenschutzgesetz Nordrhein-Westfalen auch die Kontrolle der Einhaltung von Vorschriften des Datenschutzes durch die Staatsanwaltschaften des Landes zu.

Die datenschutzrechtliche Zulässigkeit der strafprozessualen Maßnahme konnte diese aber nicht überprüfen, ohne zu wissen, welche Staatsanwaltschaft für die Abhörmaßnahme verantwortlich gewesen war. Hierüber konnte sie sich nicht über das Zentrale Staatsanwaltschaftliche Verfahrensregister informieren, da Auskünfte nach § 492 Abs. 3 Nr. 2 Strafprozessordnung (StPO) grundsätzlich nur den Strafverfolgungsbehörden für Zwecke eines Strafverfahrens erteilt werden dürfen. Es lag auch kein Ausnahmetatbestand nach § 492 Abs. 4 StPO vor. Die Landesbeauftragte war daher nicht in der Lage, auf diesem Wege selbst die erforderlichen Informationen abzufragen. Eine andere Möglichkeit eröffnet § 143 Abs. 1 Gerichtsverfassungsgesetz i. V. m. §§ 7 ff. StPO. Aber auch hierfür wären weitere Informationen notwendig gewesen, so etwa Kenntnis von der dem Bürger zur Last gelegten Straftat. Zudem hätte es sich um einen Fall der organisierten Kriminalität handeln können, so dass eventuell die Staatsanwaltschaft eines anderen Landes die Maßnahme veranlasst haben könnte. Probleme bei der Sachverhaltsaufklärung haben jedoch nicht zur Folge,

dass die Staatsanwaltschaften der Kontrolle durch die Landesbeauftragte entzogen wären. Das Datenschutzgesetz Nordrhein-Westfalen kennt in derartigen Fällen keine Beschränkung der Kontrollkompetenz.

Vor diesem Hintergrund hat die Landesbeauftragte mich gebeten, bei dem betroffenen Telekommunikationsunternehmen die erforderlichen Informationen einzuholen, das mir gegenüber zur Auskunft über durchgeführte Überwachungsmaßnahmen verpflichtet ist, wie ich bereits im 18. TB berichtet habe (vgl. 18. TB Nr. 10.2.2). Das zuständige Telekommunikationsunternehmen hat mir daher die den Überwachungsmaßnahmen zugrunde liegenden Gerichtsbeschlüsse zugeleitet. Damit die Landesbeauftragte ihrer datenschutzrechtlichen Kontrollaufgabe nachkommen kann, habe ich ihr die fragliche Staatsanwaltschaft genannt, ohne die Überwachungsbeschlüsse selbst zu übersenden.

13.7 Das Telemediengesetz

Bund und Länder haben beschlossen, die Datenschutzregelungen im Bereich der Tele- und Mediendienste zu vereinheitlichen und in einem Bundesgesetz zusammenzuführen.

Nachdem die im Herbst 2002 vom zuständigen BMWA formulierten Strukturüberlegungen, die neben der bestehenden staatlichen Datenschutzaufsicht eine Selbstregulierung durch die Wirtschaft vorsahen (vgl. 19. TB Nr. 11.2.1), keine Zustimmung in den Ländern fanden, sollen nun in einer „kleinen“ Lösung die Regelungen zu Tele- und Mediendiensten vereinheitlicht und – wo möglich und sachgerecht – die behördliche Aufsicht gestrafft werden. Grundlage hierfür ist ein Eckpunktepapier des Bundes und der Länder zur Fortentwicklung der nationalen Medienordnung.

Mit dem im Eckpunktepapier erstmals verwendeten Begriff Telemedien werden die in der praktischen Arbeit der Aufsichtsbehörden ohnehin schwer zu fassenden Grenzen zwischen Telediensten und Mediendiensten aufgehoben. Dementsprechend sollen das Teledienstegesetz und das Teledienstedatenschutzgesetz des Bundes sowie der Mediendienstestaatsvertrag der Länder durch ein Telemediengesetz des Bundes abgelöst werden, in dem die allgemeinen rechtlichen Anforderungen an die Dienste – insbesondere Herkunftslandprinzip, Anbieterkennzeichnung – festgelegt werden sollen. Für die bereichsspezifischen Bestimmungen zum Datenschutz ist ein eigenes Kapitel vorgesehen. Hinsichtlich des Geltungsbereichs soll die seit langem erforderliche Klarstellung aufgenommen werden, dass für die Internetzugangsvermittlung die Datenschutzregelungen des Telekommunikationsgesetzes gelten. Ob und in welchem Umfang Selbstregulierungsmodelle wie z. B. Auditierungsverfahren (vgl. Nr. 2.2) oder Gütesiegel zur Stärkung der Eigenverantwortung der Wirtschaft einbezogen werden, bedarf noch einer eingehenden Prüfung und Diskussion.

Angesichts eines ehrgeizigen Zeitplans, der ein Inkrafttreten des Telemediengesetzes für Ende 2005 vorsieht, werden Arbeitsgruppen aus Vertretern von Bund und Ländern auf Basis des Eckpunktepapiers die bestehenden Regelungen zum Anwendungsbereich und zum Datenschutz hinsichtlich ihres Fortbestandes und eventuell notwendiger Änderungen kritisch prüfen.

Bei Redaktionsschluss lagen noch keine konkreten Ergebnisse vor.

13.8 Spam und kein Ende?

Nach Schätzungen der UN-Organisation ITU sind inzwischen 75 bis 85 Prozent des weltweiten E-Mail-Verkehrs Spam. In zahlreichen Initiativen hat sich der Widerstand gegen dieses lästige Übel formiert.

Jeder, der einen E-Mail-Account hat, ist irgendwann betroffen. Manchmal landet auch ein vertrauenswürdiger E-Mail-Diensteanbieter unversehens auf der „Schwarzen Liste“ einer Anti-Spam-Initiative, was dazu führt, dass über seinen Dienst versendete E-Mails nicht mehr zugestellt werden. Und bisweilen zwingt eine Spam-Attacke den Server eines E-Mail-Diensteanbieters regelrecht in die Knie. Betroffen war im Mai 2004 auch ein E-Mail-Server der Bundesregierung, was zu erheblichen Verzögerungen bei der Zustellung der ein- und ausgehenden E-Mails führte. Auch wenn solche Probleme noch relativ schnell bewältigt werden können, sie kosten Zeit und Geld. So beziffert ein Unternehmensberater den durch Spam verursachten Schaden für deutsche Unternehmen auf jährlich 300 Millionen Euro.

Die Grenze der Leidensfähigkeit ist vielerorts erreicht – bei Nutzern, Unternehmen, Diensteanbietern. Und so haben sich inzwischen mehrere Regierungsorganisationen, Verbände und internationale Institutionen in unterschiedlichen Initiativen zusammengeschlossen, von denen hier nur einige genannt werden. In Deutschland ist es die Anti-Spam-Task Force des eco-Verbandes, auf EU-Ebene eine Arbeitsgruppe der für die Verfolgung von Spam zuständigen nationalen Regierungsstellen und international die Task Force der OECD, die den Kampf gegen Spam aufnehmen wollen. Da sie alle dasselbe Ziel haben, ähneln sich auch die geplanten oder schon angestoßenen Maßnahmen: Aufbau eines Netzwerks von Internetprovidern, provider- und grenzübergreifendes Beschwerdemanagement, Positivlisten für (legale) Massenversender, „Frühwarnsysteme“, Sensibilisierung der Nutzer etc. Diese organisatorischen Maßnahmen sollen von technischen und gesetzgeberischen flankiert werden.

Hierzulande ist schon ein erster Schritt durch die Umsetzung der Datenschutzrichtlinie für elektronische Kommunikation 02/58/EG in deutsches Recht getan. Das zum 1. April 2004 novellierte Gesetz gegen den unlauteren Wettbewerb erlaubt das Zusenden von Werbe-E-Mails nur bei Vorliegen einer Einwilligung des Empfängers und verbietet eine Verschleierung oder Verheimlichung der Identität des Absenders, damit der Empfänger die Möglichkeit hat, gegen den Absender vorzugehen. Diese Regelungen lassen allerdings eines außer Acht: der größte Teil der Spams wird über sog. Zombie-PC verschickt, d. h. Rechner von ahnungslosen Internetnutzern, die von professionellen Hackern der Spam-Dienste gekapert und

in sog. Zombie-Netzwerke eingebunden werden. Die Spammer agieren dann unter der Absenderadresse dieser PC und bleiben selbst unerkannt. Folglich spielt der „Versender“ der Spam-E-Mail – der ahnungslose Internetnutzer – keine Rolle. Es ist vielmehr der Nutznießer, also der Inhaber der Website, die in einer Spam beworben wird, der für die Versendung verantwortlich zu machen ist.

Selbst wenn man rechtlich gegen die eigentlichen Übeltäter vorgehen könnte, so würde dies jedoch durch einen weiteren Umstand erschwert, wenn nicht sogar unmöglich gemacht. Denn die Anbieter von Spam-Websites weichen zunehmend in Länder aus, deren Regierungen der Spam-Plage untätig gegenüberstehen und deren Diensteanbieter als Hoster der Websites das einträgliche Geschäft mitwissend dulden und dadurch davon profitieren.

Die ITU hat auf der Anti-Spam-Konferenz der Vereinten Nationen im Juli 2004 prognostiziert, dass das Spam-Problem durch eine verstärkte Zusammenarbeit bei der Verfolgung von Spammern und eine Harmonisierung der Gesetze innerhalb von zwei Jahren bewältigt werden könnte. Ein ehrgeiziges Ziel, das aus meiner Sicht nur erreicht werden kann, wenn die verschiedenen Initiativen sich zusammenschließen und ihre Arbeit gemeinsam fortsetzen.

Kasten zu Nr. 13.8

So kann ich mich gegen Spam schützen

Oberstes Gebot ist der sorgsame Umgang mit der eigenen E-Mail-Adresse. Und zur Vermeidung von „Folgeschäden“: Beantworten Sie niemals E-Mails unklarer Herkunft und rufen Sie keinen integrierten Link auf. Für bestimmte Internetaktivitäten, z. B. den Besuch von Diskussionsforen, empfiehlt es sich, einen oder mehrere temporäre E-Mail-Accounts bei den kostenfreien E-Mail-Diensten einzurichten. Sollten Sie trotz dieser Vorsichtsmaßnahmen Spams erhalten, nehmen Ihnen Filterprogramme, die inzwischen von allen E-Mail-Diensten angeboten werden, das zeitintensive Sichten und Sortieren Ihrer eingehenden elektronischen Post ab. Löschen müssen Sie die als Spam identifizierten E-Mails allerdings selbst. Wenn Sie einen aktiven Beitrag zur Spam-Bekämpfung leisten wollen, können Sie eine Beschwerde an den Provider des Mailservers und/oder den Hostprovider der beworbenen Website senden. Oder Sie wenden sich an die eco-Hotline, die als zentrale Meldestelle der Internetwirtschaft in Deutschland die Verfolgung von Spammern betreibt. Weitere Informationen finden Sie in einer Studie des BSI, die voraussichtlich im März 2005 veröffentlicht wird.

13.9 Google’s neuer E-Mail-Dienst und andere Geschäftsideen

Die von Google im April 2004 veröffentlichte Ankündigung, in Kürze einen kostenlosen E-Mail-Dienst anzubieten, beschäftigte nicht nur die einschlägige Presse, sondern auch die europäischen Datenschützer.

Noch vor dem offiziellen Start machte sich bei Bürgerrechtlern und Datenschützern Besorgnis breit. Denn was über den neuen Dienst **GMail** von Google zu erfahren war, schien alle gemeinhin geltenden Regeln zum Schutz der Privatsphäre außer Acht zu lassen. Google indes trat die Flucht nach vorn an und setzte sich mit den Datenschutzbehörden einiger EU-Länder in Verbindung, um das neue Produkt zu präsentieren und sich den kritischen Fragen der Datenschützer zu stellen. Im Mai 2004 fand auch in meinem Haus ein Gespräch mit Google-Vertretern statt. Zum Zwecke einer gemeinsamen Bewertung aller europäischen Datenschutzbehörden habe ich angeregt, GMail in der Art. 29-Gruppe (vgl. Nr. 3.2.1) zu behandeln.

Von anderen E-Mail-Diensten unterscheidet sich GMail hauptsächlich durch ein Merkmal, das möglicherweise aufgrund der datenschutzrechtlichen Implikationen bisher noch nicht nachgeahmt wurde: Die E-Mails werden automatisiert nach bestimmten Stichwörtern durchsucht, und kontextbezogene Werbung wird eingeblendet. Das „Durchsuchen“ der E-Mail-Inhalte geschieht jedoch nicht – wie anfangs angenommen – beim Eintreffen der E-Mails auf dem Server von Google, sondern erst in dem Moment, wenn der Nutzer eine E-Mail aus seinem Postfach abruft. Dann wird während der Darstellung des E-Mail-Inhalts im Browser-Fenster seitlich die „passende“ Werbung eingeblendet. Dies alles erfolgt dynamisch, d. h., die Werbeinhalte werden nicht mit der E-Mail gespeichert, sondern bei jedem Lesen dieser E-Mail wird der gesamte Vorgang erneut durchlaufen.

An diesem Verfahren entzündeten sich lebhafte Diskussionen darüber, ob neben der Einwilligung des GMail-Nutzers, also des Empfängers der E-Mails, auch die Einwilligung des Absenders in das automatisierte Durchsuchen der E-Mails vorliegen muss. Denn datenschutzrechtlich geht es hier um Inhalte der Kommunikation, deren Vertraulichkeit während der Übermittlung durch die Diensteanbieter gewährleistet sein muss. Daraus folgt zwangsläufig, dass für ein Abweichen hiervon die Einwilligung beider Kommunikationspartner vorliegen muss. Derzeit beschäftigen noch mehrere Fragen Europas Datenschützer: Handelt es sich bei dem Verfahren um eine Verarbeitung von personenbezogenen Daten? Ist das automatisierte Scannen der E-Mails ein Abhören im Sinne der Datenschutzrichtlinie für elektronische Kommunikation 02/58/EG? Ist der Kommunikationsvorgang schon mit Eintreffen der E-Mail im Postfach des GMail-Nutzers abgeschlossen? Abhängig von den Antworten muss die Beurteilung anders ausfallen: Erforderlich ist keine Einwilligung oder die Einwilligung nur des GMail-Nutzers oder die Einwilligung beider Kommunikationspartner.

Bei Redaktionsschluss lag noch kein endgültiges Ergebnis vor, fest steht jedoch, dass Google den E-Mail-Dienst GMail auch in einigen anderen Punkten nachbessern muss, damit er dem europäischen Datenschutzrecht entspricht. Hierzu hat Google schon Bereitschaft signalisiert.

Vergleichsweise wenig Aufmerksamkeit erregte ein anderer E-Mail-Dienst, der ebenfalls von einem US-amerikanischen Anbieter auf den Markt gebracht wurde: Rampell's **Did-they-read-it.** Dieser für den Absender kostenpflichtige Dienst ermöglicht es dem Nutzer, den Verlauf seiner gesendeten E-Mails zu verfolgen. Durch eine Umleitung über den Server des Anbieters wird die sog. Tracking-Funktion aktiviert, die dem Absender meldet, wann seine E-Mail gelesen wurde, wie lange, wie oft, ob sie weitergeleitet und dann auch gelesen wurde. Diese hinter dem Rücken des Empfängers erlangten Informationen mögen für einige Versender von E-Mails interessant sein, nach dem Datenschutzrecht ist ein solches Verfahren aber ohne vorherige Unterrichtung und Einwilligung des Empfängers nicht zulässig.

Die Art. 29-Gruppe wird sich auch im nächsten Jahr weiter mit diesen und anderen E-Mail-Diensten beschäftigen.

13.10 Websites von Bundesbehörden

Die Nutzung des Internet hat sich als erfolgreiches Instrument für die Öffentlichkeitsarbeit der Bundesbehörden etabliert. Ob dabei auch die datenschutzrechtlichen Vorgaben beachtet werden, habe ich bei den Bundesministerien nachgefragt.

Der Erfolg eines Internetdienstes – und dazu zählen die Angebote der Bundesbehörden – hängt wesentlich vom Vertrauen ab, das ihm seine Nutzer entgegenbringen. Offenheit, Transparenz und hinreichende Informationen seitens des Diensteanbieters können eine solche Vertrauensbasis herstellen. Aus diesem Grund habe ich zu Beginn des Jahres 2004 mittels einer Umfrage bei den obersten Bundesbehörden geprüft, ob die dortigen Internetangebote die wichtigsten Datenschutzstandards erfüllen. Dabei wurden die einschlägigen Vorschriften des Bundesdatenschutzgesetzes, des Teledienstegesetzes, des Tledienstedatenschutzgesetzes sowie des Mediendienstestaatsvertrages zu Grunde gelegt. Untersucht wurden dabei vor allem die Bereiche Anbieterkennzeichnung, Unterrichtung der Nutzer, Einwilligung der Nutzer, Auskunftsrechte der Nutzer, Nutzungsprofile unter Pseudonym, anonyme und pseudonyme Nutzungsmöglichkeiten und Hinweise auf Weiterleitung an Dritte („externe Links").

Die Auswertung der Rückläufe hat ergeben, dass die Internetangebote der obersten Bundesbehörden die gesetzlichen Vorgaben überwiegend erfüllen.

Zur Abrundung meiner schon gewonnenen Erkenntnisse habe ich mit den behördlichen Datenschutzbeauftragten des BMBF bzw. des BMU Beratungsgespräche geführt, in deren Verlauf deutlich wurde, dass die Vertreter der beiden Ministerien aufgeschlossen waren und großen Wert auf eine datenschutzgerechte Gestaltung ihrer jeweiligen Internetangebote legten. Eine ähnliche Erfahrung machte ich auch beim BMVBW. Dort wurde auf meine Anregung hin darauf verzichtet, bei Bürgeranfragen über das Kontaktformular der Internetseite oder per E-Mail die Angabe der Wohnanschrift des ratsuchenden Bürgers zu verlangen, sofern mit der Anfrage nicht der Wunsch nach postalischer Übersendung von Informationsmaterialien verbunden wird.

13.11 Datenschutzprobleme bei Backup-Dateien

Backups sind bei der Datenverarbeitung zwingend erforderlich. Allerdings hat sich die Dauer der Speicherung oftmals als problematisch herausgestellt.

Manch ein PC-Besitzer wird schon die Erfahrung gemacht haben, dass Daten auf seinem Rechner plötzlich „weg" waren. Hierfür kann es viele Ursachen geben, etwa eine defekte Festplatte, ein Virus, eine Fehlbedienung oder den Sohn, der noch etwas Speicherplatz für das neueste Spiel brauchte. Wohl dem, der die Daten gesichert hatte.

Das Streben nach einer möglichst umfassenden Speicherung von Sicherheitskopien steht jedoch häufig im Widerspruch zu der datenschutzrechtlichen Vorgabe, die Daten frühestmöglich – wenn sie zur Aufgabenerfüllung nicht mehr erforderlich sind – zu löschen. Für bestimmte Daten hat der Gesetzgeber eine Höchstspeicherfrist vorgegeben, etwa für die Verkehrsdaten in der Telekommunikation. Sie sind gem. § 96 Abs. 2 Telekommunikationsgesetz (TKG) grundsätzlich unverzüglich nach dem Ende der Verbindung zu löschen, wenn sie nicht für andere im Gesetz ausdrücklich genannte Zwecke benötigt werden. So dürfen etwa gem. § 97 Abs. 3 TKG die Daten, die für Abrechnungszwecke erforderlich sind, höchstens sechs Monate gespeichert werden (vgl. Nr. 13.1.1).

Für ein Telekommunikationsunternehmen kann es den Ruin bedeuten, etwa wenn die Verkehrsdaten verloren gehen und für einen Monat keine Rechnungen geschrieben werden können. Deshalb wäre es fahrlässig, keine Sicherungen, d. h. sogenannte Backups, zu erstellen. Bei Beratungs- und Kontrollbesuchen habe ich jedoch häufig feststellen müssen, dass der Zeitraum, für den das Backup aufbewahrt wird, zu lang gewählt war.

Im Idealfall wären die Daten im Backup zum selben Zeitpunkt wie die Originaldaten zu löschen. Technisch dürfte dies aber meist unangemessen aufwendig sein. Deswegen führt § 31 BDSG u. a. eine besondere Zweckbindung für die Daten ein, die ausschließlich der Datensicherung dienen; eine Nutzung für andere Zwecke ist verboten. Dennoch sollte sich die Speicherdauer für Backups im angemessenen Rahmen halten und an den Löschungsfristen und den technischen Notwendigkeiten orientieren.

Dies gilt insbesondere für Daten, die dem besonderen Schutz des Fernmeldegeheimnisses unterliegen und weder für die Abrechnung noch für sonstige, im TKG genannte Zwecke benötigt werden. Sie sind nach Beendigung der Verbindung unverzüglich zu löschen. Auch in anderen Bereichen, in denen die Speicherdauer rechtlich weniger strikt geregelt ist, dürften diese alten Sicherungen häufig wenig hilfreich sein.

Da manche Schadensereignisse, etwa Softwarefehler, erst nach Tagen bemerkt werden, wird es dennoch erforderlich sein, die Daten für einige Tage zu sichern. Auch die

konkreten organisatorischen Umstände können dazu führen, dass eine kurzfristige und tagesgenaue Löschung der Backups nicht handhabbar ist. Dies gilt etwa für die Auslagerung von Sicherungsbändern in ein anderes Gebäude zur Katastrophenvorsorge oder inkrementelle Backups, bei denen beispielsweise zur Begrenzung des Speicherumfangs eine vollständige Wochensicherung erstellt wird und nur die sich ändernden Daten täglich gesichert werden.

Bei manchen Telekommunikationsunternehmen habe ich allerdings feststellen müssen, dass Backups mit Verkehrsdaten mehrere Monate aufbewahrt werden. Dies wurde in einem Fall damit begründet, dass die gesamten Systeme gesichert werden, um diese ggf. wieder konsistent rekonstruieren zu können. Ferner müsste für andere Zwecke, die nicht im Zusammenhang mit den Verkehrsdaten stehen, eine Wiederherstellung der Systeme auch noch im Laufe eines Jahres möglich sein. Ein Löschen der Verkehrsdaten aus dem Backup wäre nur mit einem immensen Aufwand möglich und könnte zudem die Rekonstruierbarkeit der anderen Daten gefährden. Hier stellt sich die Frage, ob bei der Konzeption der Systeme nicht grundlegende Fehler unterlaufen sind. Einerseits dürften die einzelnen Systembestandteile zu eng verzahnt sein, um ein differenziertes Backup-Konzept zu erstellen. Andererseits lässt der Bedarf für eine langfristige Sicherung Zweifel an der Revisionsfähigkeit der im Wirksystem gespeicherten Daten vermuten. Wie in solchen Fällen weiter verfahren werden soll, ist allerdings sehr problematisch, da einerseits eine Änderung der Systeme einen extrem hohen Aufwand für das betroffene Unternehmen bedeutet, andererseits die Speicherdauer von einem Jahr (zuzüglich der normalen Speicherdauer) weit jenseits des Angemessenen liegt. Langfristig muss jedoch eine datenschutzgerechte Lösung gefunden werden.

Dieses Beispiel zeigt, dass bereits im Vorfeld bei der Konzeption von komplexen Datenverarbeitungssystemen Datenschutzaspekte berücksichtigt werden müssen, um spätere kostenintensive Änderungen zu vermeiden. Ein solcher vorbeugender Datenschutz ist insbesondere dann erforderlich, wenn sensible Daten verarbeitet werden.

13.12 Zusammenarbeit mit der Regulierungsbehörde für Telekommunikation und Post (RegTP)

Gute und vertrauensvolle Zusammenarbeit mit der RegTP.

Die jahrelange enge und gute Zusammenarbeit mit der RegTP wurde im Berichtszeitraum fortgesetzt. Ein wesentlicher Teil der Kooperation war wieder die gegenseitige Unterrichtung, sei es durch Informationsaustausch über die jeweiligen Kontrollvorhaben zur Vermeidung von Terminüberschneidungen, sei es in Einzelfällen bei der Bearbeitung von Bürgereingaben, die verschiedentlich an die RegTP und an mich gerichtet worden waren. Die Regelung des § 115 Abs. 4 Telekommunikationsgesetz n. F. (TKG) sieht vor, dass ich meine Beanstandungen nunmehr an die RegTP richte und ihr nach pflichtgemäßem Ermessen weitere Ergebnisse meiner Kontrollen mitteile.

Zur Koordinierung der Kontrolle des Datenschutzes in der Telekommunikation fanden regelmäßige Besprechungen statt. Erstmals wurde im Jahr 2004 auch ein gemeinsamer Workshop zum Thema „Neue Dienste in und über Internet bzw. Mobilfunk“ durchgeführt, bei dem vor allem die Abgrenzung zwischen Telekommunikations- und Telediensten erörtert und gemeinsam geprüft wurde, inwieweit die Vorschriften des TKG auf die neuen Dienste, wie z. B. SMS-Dienste, Sprachspeicherboxen und Chat-Dienste, Anwendung finden. An dem Vorhaben der RegTP, Regeln für die Vergabe von Telefonnummern an Internetanbieter festzulegen (Stichwort: Voice over IP, vgl. Nr. 13.4), wurde ich frühzeitig beteiligt.

Die TKG-Novelle (vgl. Nr. 13.1) machte es erforderlich, die Telekommunikationsdiensteanbieter gezielt über die eingetretenen Rechtsänderungen zu unterrichten. Hierzu wurde ein gemeinsames Informationspapier erstellt, das von Diensteanbietern bei der RegTP abgerufen werden kann.

13.13 Öffentlichkeit schaffen für den Datenschutz

Symposien und Fachtagungen im Bereich des Datenschutzes bei Telekommunikations- und Telediensten.

Am 4. November 2004 fand bereits zum fünften Mal das Symposium „Datenschutz in der Telekommunikation und bei Telediensten“ statt. Damit habe ich die Tradition meines Amtsvorgängers übernommen, einmal jährlich nach Bonn–Bad Godesberg einzuladen, um aktuelle Fragestellungen des Datenschutzes zu diskutieren. Mit jeweils etwa 100 Teilnehmern hat sich dieses Wissensforum mittlerweile etabliert und wird vom Fachpublikum angenommen. Dabei will das Symposium nicht nur über neue Datenschutzregelungen informieren und von den aktuellen datenschutzpolitischen Tendenzen berichten. Wichtig ist mir, dass die Teilnehmer die Möglichkeit haben, Informationen auszutauschen und Datenschutzthemen offen zu diskutieren.

Im Rahmen des Symposiums 2003 wurde der Entwurf für ein neues Telekommunikationsgesetz vorgestellt. Diskutiert wurden neben den datenschutzrechtlichen Vorschriften auch die Regelungen zur Telekommunikationsüberwachung.

Der Schwerpunkt des Symposiums 2004 galt dem Verhältnis zwischen dem Strafverfolgungsinteresse der Öffentlichkeit bei Internetkriminalität und dem Recht des Einzelnen auf informationelle Selbstbestimmung bei der Nutzung des Internet. Ausgangspunkt war die rasch wachsende Akzeptanz von Internet- und Multimediadiensten und die damit verbundene verstärkte Bedeutung eines datenschutzgerechten Umgangs mit den dabei anfallenden Daten der Nutzer. Einvernehmen bestand darüber, dass sich das Telekommunikationsgeheimnis auch auf Internetdienste erstreckt. Ob und ggf. wie das Spannungsverhältnis zwischen effizienter Strafverfolgung und dem Recht des Einzelnen auf freie Kommunikation im

Internet aufgelöst werden kann, war Gegenstand von drei Vorträgen und einer engagiert wie kontrovers geführten Diskussion. Die Referate können auf meiner Website nachgelesen werden.

Zusätzlich zu dieser allen Interessierten offenstehenden Veranstaltungsreihe führe ich seit dem Jahr 1998 zweimal jährlich den so genannten Jour Fixe Telekommunikation für Anbieter von Telekommunikationsdienstleistungen und entsprechende Fachverbände durch. Auf der Tagesordnung stehen regelmäßig Themen aus meiner Prüf- und Kontrollpraxis. Auch die Teilnehmer können Themen, die ihnen wichtig sind, für die Besprechungen benennen. Im Rahmen des Jour Fixe konnten in der Vergangenheit immer wieder Lösungen für aktuelle Probleme der Datenschutzpraxis im Bereich der Telekommunikation gefunden werden.

Sowohl die Symposien als auch die regelmäßigen Veranstaltungen mit den Telekommunikationsdiensteanbietern haben dazu beigetragen, das gegenseitige Verständnis von Datenschützern und Wirtschaft zu verbessern und damit die Suche nach tragfähigen Lösungen zu erleichtern.

14 Postunternehmen

14.1 Datenübermittlung ins Ausland

14.1.1 US-Behörden verlangen Vorabübermittlung von Paketdaten

Die USA fordern zur Terrorismusabwehr vorab Angaben über die Empfänger und Absender von Paketen in die Vereinigten Staaten. Ob dieses Verlangen mit datenschutzrechtlichen Vorschriften vereinbar ist, bedarf einer Klärung auf europäischer Ebene.

„USA fordern vorab Daten von Paketempfängern“ – mit diesen und ähnlichen Schlagzeilen verkündeten die Nachrichtenagenturen im Sommer 2004, dass US-Behörden von europäischen Postunternehmen vorab Angaben über die Empfänger und Absender von Paketen verlangten, die in die Vereinigten Staaten geschickt werden. In ernsthaftem Zweifel an der Zulässigkeit einer solchen Datenübermittlung habe ich zunächst einmal die Hintergründe dieser Meldungen recherchiert. Die Zoll- und Grenzschutzbehörde der Vereinigten Staaten (US Custom & Border Protection) verlangt aufgrund des am 5. Dezember 2003 in Kraft getretenen „Trade Act of 2002“ die elektronische Übermittlung der Sendungsdaten von Waren, die in die USA geschickt werden. Mit dieser Regelung soll der amerikanischen Forderung nach mehr Sicherheit im Personen- und Warenverkehr Rechnung getragen werden. Hierunter fallen z. B. Frachtsendungen, die per Schiff versandt werden, aber auch Pakete, die auf dem Luftweg von Postdienstunternehmen in die USA gebracht werden. Die Missachtung dieser Vorschriften ist strafbewehrt und kann bis zur Beschlagnahme des Flugzeugs mit der unangemeldeten Ladung führen.

Im Gegensatz zum Cargobereich wird für den postalischen Warenverkehr zur Zeit noch die bislang praktizierte Datenübermittlung per schriftlichem Einzelbeleg auf dem weltweit genutzten Zollvordruck CN 23 geduldet.

Ich halte dieses Ansinnen für hochgradig problematisch und habe insbesondere Zweifel an der Zulässigkeit dieser Datenübermittlung, soweit die Daten nach deutschem Recht dem Postgeheimnis unterliegen. Ich sehe es kritisch, dass – wie schon bei der Vorabübermittlung der Passagierdaten von Flugreisenden (vgl. Nr. 22.2) – die USA versuchen, auch bei Transportunternehmen außerhalb des eigenen Hoheitsbereichs personenbezogene Daten zu erheben. Sollte sich die Befürchtung bestätigen, dass hiervon auch Daten über den Versand von Paketen, Päckchen und Briefen betroffen sind, die dem Postgeheimnis unterliegen, werde ich dies zum Gegenstand der Beratungen mit den Datenschutzbeauftragten der übrigen EU-Mitgliedstaaten machen.

14.1.2 Sendungsdaten in ausländischen Rechenzentren

Die Datenverarbeitung findet heutzutage häufig nicht mehr am Sitz des Unternehmens statt. Problematisch ist dies dann, wenn im Land der Datenverarbeitung kein angemessenes Datenschutzniveau gewährleistet ist. Das Bundesdatenschutzgesetz enthält jedoch Regelungen, um personenbezogene Daten auch im Ausland zu schützen.

Dank schneller Verkehrswege und technischer Möglichkeiten sind viele Unternehmen global tätig. Sie haben ihren Sitz oder Tochtergesellschaften in Ländern der Europäischen Union, Amerika oder Asien. Und so werden auch immer mehr Daten, z. B. Kunden- oder Mitarbeiterdaten in andere Staaten übermittelt.

Während das BDSG Datenübermittlungen in EU-Staaten gem. § 4b Abs. 1 einer Inlandsübermittlung gleichstellt, muss bei einer Übermittlung in Drittstaaten die zusätzliche Voraussetzung eines angemessenen Datenschutzniveaus gewährleistet sein (§ 4b Abs. 2 BDSG). Anderenfalls ist der Datentransfer nur zulässig, wenn ein Tatbestand aus dem Ausnahmekatalog des § 4c Abs. 1 BDSG vorliegt: Danach ist die Übermittlung personenbezogener Daten, auch ohne angemessenes Schutzniveau an andere als die in § 4b Abs. 1 genannten Stellen insbesondere zulässig, sofern der Betroffene seine Einwilligung gegeben hat oder die Übermittlung für die Erfüllung eines Vertrags erforderlich ist, der zwischen dem Betroffenen und der verantwortlichen Stelle geschlossen wurde, oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen wurden. Liegt kein Ausnahmetatbestand vor, so muss das Unternehmen eine Genehmigung nach § 4c Abs. 2 BDSG beantragen. Diese Genehmigung wird erteilt, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gewährleistet. Die Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregelungen ergeben.

Im Sommer 2002 informierte mich United Parcel Service (UPS) über seine Praxis, personenbezogene Kundendaten und Daten von Sendungsempfängern zur Speicherung an das Mutterunternehmen in die USA zu übermitteln. Da in

den USA keine ausreichenden Datenschutzgesetze vorhanden sind, sich der Datenimporteur UPS USA weder den Safe-Harbour-Regelungen (vgl. auch Nr. 3.2.4) unterworfen hatte noch Ausnahmetatbestände nach dem BDSG vorlagen, forderte ich UPS auf, die Datenübermittlung und -verarbeitung mittels einer Einwilligung der Betroffenen oder durch verbindliche Richtlinien gemäß § 4c Abs. 2 BDSG datenschutzkonform zu gestalten. UPS entschied sich, unternehmensinterne Richtlinien für den Datentransfer zu erstellen, die sich an die Standardvertragsklauseln der EU vom 27. Dezember 2001 (EG-Datenschutzrichtlinie 95/46/EG) anlehnen. Nach umfangreichen Verhandlungen ergänzte das Postdienstunternehmen seine Regelungen, so dass nunmehr ausreichende Garantien nachgewiesen waren. Ich habe daraufhin die Datenübermittlung gemäß § 4c Abs. 2 BDSG im Sommer 2003 genehmigt.

Die Regelung des § 4c Abs. 2 BDSG weist mir einen eindeutigen Genehmigungsvorbehalt auf Post- und Telekommunikationsdaten ihrer Kunden zu. Bei einem Post- oder Telekommunikationsdienstleister fallen jedoch nicht nur personenbezogene Kundendaten, sondern auch Daten der Mitarbeiterinnen und Mitarbeiter an. Zwar obliegt die datenschutzrechtliche Kontrolle über den Umgang mit den Beschäftigtendaten der jeweiligen Aufsichtsbehörde für den nicht-öffentlichen Bereich. Um das Genehmigungsverfahren nicht zu verzögern und dadurch das Unternehmen in seiner Handlungsfähigkeit zu blockieren, wurde jedoch in Absprache mit den Aufsichtsbehörden der Länder im März 2004 nach der Vorlage eines weiteren Vertrages auch der Transfer von Beschäftigtendaten von mir bewilligt.

14.2 Track & Trace: Wer verfolgt wen?

Mit dem Service „Track & Trace“ bietet die Deutsche Post AG die Sendungsverfolgung von Postsendungen im Internet an. Durch die mehrfache Vergabe von Identcodes bei Paketen und unsachgemäße Nutzung des Service konnten Daten Dritter eingesehen werden.

Die Deutsche Post AG bietet ihren Geschäftskunden, wie andere Postdienstleister auch, mit dem Service „Track & Trace“ die Sendungsverfolgung von Postsendungen im Internet an. Neben einer Benutzerkennung und einem Passwort erhält jeder Nutzer einen Identcode-Nummernbereich, den er für seine Pakete verwenden und per Internet abfragen kann. Die Benutzerkennung lässt nur eine Abfrage für den *eigenen* Nummernkreis zu. Zwar kann es bei der Vergabe von Identcodes zur Mehrfachvergabe kommen mit der Folge, dass einem Geschäftskunden bei Eingabe eines Identcodes mehrere Sendungsverläufe angezeigt werden. Dabei handelt es sich aber immer um Sendungen seines eigenen Nummernbereichs; Postverkehr anderer Absender kann nicht eingesehen werden. Seitens der Deutschen Post AG wurde Geschäftskunden ermöglicht, die Sendungsverfolgung von großen Paketmengen über eine Direktaufrufschnittstelle durchzuführen. Über diese Schnittstelle konnte der Sendungsstatus automatisiert abgefragt werden. Mitte des Jahres 2003 berichteten Petenten, dass dabei auch Altdaten anderer Kunden zu sehen waren, insbesondere Name, Anschrift und die digitalisierte Unterschrift des Empfängers.

Dieses Problem hatte mehrere Ursachen: Die Mehrfachvergabe und die Weitergabe des Identcodes durch die Geschäftskunden an Dritte sowie die Bereitstellung der technischen Möglichkeit, Sendungsdaten direkt einzusehen. Ich habe auf eine rasche und umfassende Lösung dieses unhaltbaren Zustands hingewirkt. So wurde unmittelbar als Reaktion auf mein Einschreiten die Option „Nachweis anzeigen“ bei der Direktaufrufschnittstelle systemseitig unterbunden. Die digitalen Unterschriften sowie der Postverkehr Dritter kann seither auch im Fall der Mehrfachvergabe von Identcodes nicht mehr aufgerufen werden.

Im Dezember 2003 wurde dann der Zugang zur Direktaufrufschnittstelle mit Unterschriftsanzeige auf Kunden der Deutschen Post AG beschränkt, die ausdrücklich die Verwendung der Direktaufrufschnittstelle für den internen Bedarf gleichermaßen wie die Verwendung von eindeutigen Identcodes zusichern.

Nach diesen Änderungen habe ich keine weiteren Beschwerden über eine fehlerhafte Sendungsverfolgung erhalten.

14.3 EPOS – Fehler im System

Durch einen Systemfehler im elektronischen System zur Erfassung von Dienstleistungen am Schalter – EPOS – war es für Betreiber und Mitarbeiter verschiedener Postagenturen möglich, Einblick in die Datenbestände anderer Agenturen zu nehmen.

Die Deutsche Post AG verfügt über ein elektronisches System (EPOS) zur Erfassung der am Schalter erbrachten Dienstleistungen. Hiermit werden die Ausgabe von Paketen und Postsendungen kontrolliert, Nachnahmebeträge und der Verkauf von Postwertzeichen abgerechnet und der Postbankverkehr abgewickelt. Das System enthält Daten über den Bargeldbestand, die Einnahmen und Ausgaben des Tages sowie über den gesamten Zahlungsverkehr, der für die Postbank abgewickelt wird. Bis Mitte November 2003 konnten die Datenbestände der selbständigen Poststellenbetreiber auch von anderen Agenturnehmern mit geringem Aufwand nachgelesen werden. Dies wurde mir vom Postagenturnehmerverband e.V. Ende November 2003 mitgeteilt und auf Nachfrage von der Deutschen Post AG bestätigt.

Über mehrere Monate waren neben den Adressdaten die Bargelddifferenzen, die Höhe des Verfügungsrahmens und der Bargeldbestand des Vortags anderer Postagenturen einsehbar. Zum Zeitpunkt meiner Nachfrage war die technische Zugriffsmöglichkeit aber bereits auf die Daten der eigenen Filiale beschränkt worden. Die Zuordnung der Kassenfehlbeträge zu den jeweiligen Agenturnehmern konnte auch vor der Systemänderung nicht erfolgen, weil die Kassenfehlbeträge mit dem Tagesjournal abgerechnet werden, das nur für die eigene Kasse einsehbar ist. Kundendaten waren hiervon nicht betroffen.

Nach § 9 BDSG müssen öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, die erforderlichen technischen und organisatorischen Maßnahmen treffen, um den Datenschutz zu gewährleisten. Da auch personenbezogene Daten anderer Partnerfilialen von den EPOS-Nutzern eingesehen werden konnten, trugen die technischen Maßnahmen offensichtlich dieser Vorgabe nicht hinlänglich Rechnung.

Ich habe den technischen Mangel gerügt und die Deutsche Post AG aufgefordert, das System EPOS auf weitere Fehler zu überprüfen und diese ggf. umgehend abzustellen. Entsprechend teilte mir die Deutsche Post AG im Frühjahr 2004 mit, dass keine weiteren technischen Mängel am EPOS- Datenverarbeitungssystem aufgefallen seien. Darüber hinaus unterliegt das System nunmehr einer dauerhaften technischen Prüfung.

14.4 Die Post will's wissen

Die Deutsche Post AG bietet auf ihrer Internetseite die Möglichkeit, Informationen mittels eines Kontaktformulars abzurufen. Bislang musste man dazu seinen Namen und seine Anschrift angeben. Auf meine Anregung ist jetzt auch eine anonyme Anfrage möglich.

Immer mehr Bürgerinnen und Bürger nutzen heute die Möglichkeit, über das Internet Auskünfte einzuholen oder Dienstleistungen in Anspruch zu nehmen. So bietet auch die Deutsche Post AG an, Informationen zu ihren Leistungen online abzurufen. Um die Anliegen der Kunden schnell und ohne aufwändige Rückfragen erledigen zu können, hatte der Interessent – unabhängig vom Grund seiner Anfrage – neben seinem Namen die E-Mail- und die Hausadresse anzugeben. Eine vom Zweck der Kontaktaufnahme unabhängige Abfrage dieser Daten ist jedoch nach dem Teledienstdatenschutzgesetz nicht zulässig. Daher habe ich die Deutsche Post AG aufgefordert, den elektronischen Vordruck so zu gestalten, dass eine Nachricht auch anonym an die Deutsche Post AG gesandt werden kann. Inzwischen bietet die Deutsche Post AG ein weiteres Formular an, in das der Kunde nur seine Nachricht eintragen muss. Sollte er darüber hinaus eine Rückmeldung der Deutsche Post AG wünschen, kann er zusätzlich seine E-Mail-Adresse angeben.

Diese Lösung schafft einen gelungenen Ausgleich zwischen dem Grundsatz der Datensparsamkeit und der Datenvermeidung sowie dem Interesse des Unternehmens an Wirtschaftlichkeit und Kundenzufriedenheit. Mit der Nutzung des Formulars für anonymen Kontakt hat der Kunde die Möglichkeit, sich an das Unternehmen zu wenden, ohne seine persönlichen Daten preisgeben zu müssen.

14.5 Besonderheiten beim Nachsendeantrag

Bei dem Nachsendeverfahren der Deutschen Post AG trat ein Problem bei der Weitergabe von Anschriften der in Frauenhäusern lebenden Frauen auf. Um diesen Personenkreis zu schützen, wurde ein entsprechender Adresszusatz entwickelt.

Im Jahr 2003 hat die Deutsche Post AG ein neues Nachsendeverfahren eingeführt, über das ich bereits in meinem letzten TB berichtet hatte (vgl. Nr. 12.2). In § 7 der Postdienste-Datenschutzverordnung wurden klare Regelungen zur Weitergabe der neuen Anschrift geschaffen. Um die missbräuchliche Nutzung des Nachsendeverfahrens zu verhindern, hat die Deutsche Post AG den Versand einer Kundeninformationskarte an den Antragsteller eingeführt, die Angaben zu den umziehenden Personen sowie zur neuen Anschrift enthält. Doch die neue Regelung hatte eine Lücke: Frauen, die keinen geregelten Umzug durchführen, sondern vielmehr „Hals über Kopf" unter einer neuen Anschrift Zuflucht finden, werden durch diese Kundeninformationskarte erheblich gefährdet. Konkret wies mich ein Frauenhaus auf die mögliche Gefährdung für die Frauen und Kinder hin, die zu Hause der Gewalt von Ehemännern und Vätern ausgesetzt sind. Mit der Kundeninformationskarte wurde diesen die neue Anschrift (des Frauenhauses) „frei Haus" geliefert. Ich habe die Deutsche Post AG gebeten, das Auftragsformular für Nachsendungen nachzubessern: Ab dem 4. Quartal 2003 kann durch den Zusatz „Frauenhaus" im Feld „Adresszusätze" die neue Anschrift in der Auftragsbestätigung ausgeblendet werden. Zudem ist es zwingend erforderlich, dass die Frauen der Weitergabe der neuen Anschrift an andere Postdienstleister und an Dritte widersprechen.

Die Erfahrungen mit dem optimierten Nachsendeauftrag zeigt, dass unerwünschte Anschriftenweitergaben dadurch vermieden werden konnten. Allerdings nutzen nur wenige Frauen das Nachsendeverfahren, teils wegen der Kosten, teils aus Angst, die Adresse könnte trotz aller Vorsichtsmaßnahmen doch mal in „falsche Hände" geraten.

14.6 Konkurrenz belebt das Geschäft

Mit der größeren Anzahl der Postdienstunternehmen erhöhte sich auch die Anzahl der Eingaben und Kontrollen.

Deutschland ist in Europa mit rund 23 Milliarden Euro Umsatz der größte Markt für Postdienstleistungen. Innerhalb der vergangenen zwei Jahre hat die Regulierungsbehörde für Telekommunikation und Post an mehr als 800 Antragsteller Lizenzen für Postdienstleistungen verteilt. Die Überführung des gesamten Postmarkts in den Wettbewerb ist im Postgesetz bereits vorgezeichnet: Die gesetzliche Exklusivlizenz der Deutschen Post AG für bestimmte Postdienstleistungen (insbesondere im Briefverkehr) ist bis zum 31. Dezember 2007 befristet.

Der Wettbewerb führt vermehrt zu Eingaben hinsichtlich privater Postdienstunternehmen. Im Berichtszeitraum habe ich eine erhebliche Anzahl von Kontrollbesuchen bei Kurier-, Paket- sowie Briefdiensten durchgeführt, um mich von den Betriebsabläufen und dem Umgang mit den personenbezogenen Kundendaten zu überzeugen. Dabei zeigte sich, dass die meisten Postdienstleister ihr Geschäft grundsätzlich solide und damit datenschutzgerecht betreiben: Sie verfügen über gute Kenntnisse des Postgeheimnisses sowie der Vorschriften über den Datenschutz im Postverkehr und setzen sie im täglichen Geschäft ein.

Sofern Eingaben Anlass meiner Besuche waren, konnten zufriedenstellende Lösungen gefunden werden. Verstärkt war festzustellen, dass die meisten Unternehmen sich wieder auf ihre Kernkompetenzen konzentrieren. Ich begrüße diese Wendung, weil damit eine Routine in die Arbeit einkehrt, die Platz für Sorgfalt und Aufmerksamkeit schafft, und bei Mitarbeiterinnen und Mitarbeitern einen angemessenen Umgang mit sensiblen Daten fördert.

15 Sozialdatenschutz

15.1 Gesetzgebung zum Sozialdatenschutz

Bei der Sozialgesetzgebung konnte ich sowohl allgemeine als auch konkrete datenschutzrechtliche Verbesserungen einbringen.

15.1.1 Sozialgesetzbuch Achtes Buch – Kinder- und Jugendhilfe

Mit dem am 28. Oktober 2004 vom Deutschen Bundestag beschlossenen Tagesbetreuungsausbaugesetz wurde das Recht der Kinder- und Jugendhilfe (SGB VIII) weiterentwickelt. Auf der Grundlage des am 1. Januar 1991 in Kraft getretenen Achten Buch des Sozialgesetzbuches (Kinder- und Jugendhilfegesetz) sollte eine realitätsbezogene Anpassung der Rechtslage in der Kinder- und Jugendhilfe erfolgen. Das Gesetz verfolgt das Ziel, Elternschaft und Familien zu stärken, frühkindliche Förderungen zu verbessern und junge Menschen in ihren vorhandenen Wünschen und Interessen zu unterstützen. Vor dem Hintergrund dieser Zielsetzung konnten datenschutzrechtliche Verbesserungen in den Entwurf integriert werden, die Mitwirkungsrechte und Selbstbestimmungsrechte der Betroffenen stärken sollen.

15.1.2 Gesetz zur Einordnung des Sozialhilferechts in das Sozialgesetzbuch

Im Berichtszeitraum wurde das Bundessozialhilfegesetz fortentwickelt und mit Wirkung zum 1. Januar 2005 als Zwölftes Buch in das Sozialgesetzbuch eingefügt. Mit dem SGB XII ist eine umfassende Reform des Sozialhilferechts in die Wege geleitet worden, insbesondere wurde ein neues Bemessungssystem der Regelsätze und Leistungen geschaffen. Sowohl das Recht der Sozialhilfe, als auch das Recht der Kinder- und Jugendhilfe werden in Bereichen umgesetzt, die der datenschutzrechtlichen Kontrollkompetenz der Länder unterliegen, so dass im Gesetzgebungsverfahren entsprechende Anregungen von den für den Datenschutz zuständigen Stellen eingebracht wurden. Die datenschutzrechtlichen Anforderungen für die vorgesehenen Verfahren zum Datenabgleich wurden im SGB XII im wesentlichen berücksichtigt. Darin ging es mir insbesondere um die Zusammenarbeit verschiedener Träger und die Zusammenarbeit mit den Trägern der Freien Wohlfahrtsverbände, die gem. §§ 4, 5 SGB XII hinsichtlich der Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten in einer Vereinbarung geregelt werden soll.

15.1.3 Verwaltungsvereinfachungsgesetz

Der Entwurf eines Gesetzes zur Vereinfachung der Verwaltungsvorschriften im Sozialrecht (Verwaltungsvereinfachungsgesetz – Bundestagsdrucksache 15/4228) soll insbesondere eine Rechtsgrundlage für die Auftragsdatenverarbeitung schaffen, die Zugriffsberechtigung bei der elektronischen Gesundheitskarte regeln und ein Problem der Praxis im Zusammenhang mit Leistungen zur sozialen Sicherung von Pflegepersonen lösen:

- Durch eine Ergänzung in § 137f SGB V soll in enger Abstimmung mit mir eine Rechtsgrundlage geschaffen werden, damit die nach der Risikostruktur-Ausgleichsverordnung bestehenden Arbeitsgemeinschaften bei der Durchführung der Disease-Management-Programme auch private Datenverarbeitungsunternehmen mit der Auftragsdatenverarbeitung beauftragen können. Dies war notwendig, weil bei den Arbeitsgemeinschaften nicht genügend Kapazitäten vorhanden sind, derartige Datenmengen zu verarbeiten.

- Die in § 291a SGB V vorgesehene Erweiterung des Kreises der Zugriffsberechtigten auf die elektronische Gesundheitskarte wurden zwischen dem BMGS und mir abgestimmt und erfüllt die datenschutzrechtlichen Anforderungen. Durch diese Regelung soll sichergestellt werden, dass die bisherigen Arbeitsabläufe in Praxen, Apotheken und Krankenhäusern nicht durch eine Einschränkung des zugriffberechtigten Personenkreises bei Einführung der elektronischen Gesundheitskarte behindert werden, indem die Zugriffsrechte auf die dort tätigen Gehilfen, die den gleichen Geheimhaltungspflichten wie Ärzte, Zahnärzte und Apotheker unterliegen, erweitert wurden.

- In § 44 SGB XI wird eine datenschutzrechtliche Erhebungsbefugnis und Übermittlungsverpflichtung für die gesetzliche Pflegekasse bzw. private Pflegeversicherung geschaffen. Hierdurch wird im Interesse der Pflegeperson gewährleistet, dass die Festsetzungsstellen für die Beihilfe und die Dienstherrn zeitnah von ihrer anteiligen Beitragspflicht zur Rentenversicherung erfahren. Hierüber wird unter Wahrung des Transparenzgebotes sowohl die Pflegeperson als auch der Pflegebedürftige informiert.

15.1.4 Grundsicherung

Nachdem die Vorschriften über die Grundsicherung im Alter und bei Erwerbsminderung in das Sozialhilferecht eingegliedert und dabei in wesentlichen Punkten klargestellt wurden, erwarte ich, dass nunmehr auch das Verfahren zur Feststellung der vollständigen Erwerbsminderung datenschutzkonform ausgestaltet wird.

Die Beantragung von Leistungen der Grundsicherung im Alter und bei Erwerbsminderung richtete sich bis zum 31. Dezember 2004 nach dem Grundsicherungsgesetz – GSiG. Datenschutzrechtlich war bei der Anwendung des GSiG insbesondere die Ausgestaltung des Verfahrens

problematisch, mit dem eine dauerhafte volle Erwerbsminderung festgestellt werden sollte. In diesem Zusammenhang war nicht geklärt, ob auch der örtliche Grundsicherungsträger über das Vorliegen einer medizinisch bedingten Erwerbsminderung der Antragsteller befinden konnte, oder ob er insoweit an die (medizinische) Entscheidung des Rentenversicherungsträgers gebunden war. Dementsprechend sahen auch die zur Anforderung medizinischer Unterlagen eingesetzten Schweigepflichtentbindungserklärungen zum Teil eine sehr weitgehende Ermächtigung vor, nach der neben dem Rentenversicherungsträger auch der Grundsicherungsträger befugt sein sollte, sensible medizinische Daten der Antragsteller bei Ärzten, Krankenhäusern und anderen Einrichtungen zu erheben.

Diese Praxis stieß auf erhebliche Bedenken, da nicht sichergestellt war, dass sensible medizinische Unterlagen und Befunde der Antragsteller ausschließlich den Rentenversicherungsträgern als den für eine medizinische Prüfung fachlich geeigneten Stellen zugänglich gemacht wurden. Die nicht geklärte Aufgabenverteilung von Grundsicherungs- und Rentenversicherungsträgern führte zudem zu einer uneinheitlichen Verwaltungspraxis.

Um auf eine datenschutzgerechte Ausgestaltung der Verfahrensweise hinzuwirken, hatte ich – in Abstimmung mit den für die Träger der Grundsicherung zuständigen Landesbeauftragten für den Datenschutz – bereits in der ersten Hälfte des Berichtszeitraums intensive Gespräche mit dem BMGS, Vertretern der Länder, den Kommunalen Spitzenverbänden sowie dem Verband Deutscher Rentenversicherungsträger (VDR) geführt. Hierbei wurde deutlich, dass die datenschutzrechtlichen Probleme nur durch eine gesetzliche Klarstellung hinsichtlich der Aufgabenverteilung von Grundsicherungs- und Rentenversicherungsträgern zu lösen waren.

Inzwischen wurden die Vorschriften über die Grundsicherung in das Sozialhilferecht eingegliedert (BGBl. I 2003 S. 3022) und in wesentlichen Punkten – unter Berücksichtigung der von mir vorgetragenen datenschutzrechtlichen Gesichtspunkte – klargestellt. So legt § 45 Abs. 1 Satz 2 SGB XII nunmehr verbindlich fest, dass die Entscheidung des Trägers der Rentenversicherung für den ersuchenden Träger der Sozialhilfe bindend ist. Ebenso wird geregelt, dass die Rentenversicherungsträger ein derartiges Ersuchen zu prüfen und zu entscheiden haben. Damit dürfen ausschließlich die Rentenversicherungsträger die medizinische Begutachtung durchführen.

Zur Frage, wie der Grundsicherungsträger bzw. der Träger der Sozialhilfe die Wahrscheinlichkeit einer dauerhaften vollen Erwerbsminderung feststellen und dementsprechend ein Ersuchen an den Rentenversicherungsträger richten soll, ist ebenfalls eine Klarstellung erfolgt. Nach § 45 Abs. 1 Satz 1 SGB XII erfolgt ein Ersuchen dann, wenn es aufgrund der „Angaben und Nachweise des Leistungsberechtigten“ als wahrscheinlich erscheint, dass die Voraussetzungen einer dauerhaften vollen Erwerbsminderung gegeben sind. Zur Feststellung dieser Wahrscheinlichkeit ist eine Kenntnisnahme oder Anforderung verschiedener medizinischer (Behandlungs-) Unterlagen bei Dritten nicht erforderlich, da die „Angaben und Nachweise“ von den Betroffenen selbst erhoben bzw. von diesen mit dem Antrag vorgelegt werden können.

Mit Blick auf das Inkrafttreten der geänderten Vorschriften über die Grundsicherung zum 1. Januar 2005 hatte ich gegenüber den Kommunalen Spitzenverbänden und dem VDR die Fortführung der bislang geführten Gespräche zur Grundsicherung angeregt, um rechtzeitig ein bundeseinheitliches und datenschutzkonformes Verfahren zu erreichen. Leider hat bisher nur der VDR auf meine Initiative reagiert.

Unabhängig davon gehe ich aufgrund der eingetretenen Rechtsänderung davon aus, dass auch die Kommunalen Spitzenverbände für eine datenschutzkonforme Anpassung des Verfahrens Sorge tragen werden.

15.2 Das JobCard-Verfahren

Eines der ehrgeizigsten Projekte zur Einführung von elektronischen Signaturverfahren ist das Projekt JobCard. Das neue System zur Vorlage von Verdienst-, Entgelt- und Arbeitsbescheinigungsdaten muss für den Betroffenen transparent gestaltet und effektiv gegen Missbrauch geschützt werden.

Das Projekt zur Einführung elektronischer Signaturverfahren in der Sozialverwaltung läuft unter dem Stichwort „JobCard“. Diese Bezeichnung ist allerdings irreführend: Einerseits handelt es sich um zwei Projekte (JobCard I und JobCard II), die aufeinander aufbauen. Zum anderen handelt es sich um ein Verfahrensprojekt, das zwar die Nutzung einer Signaturkarte vorsieht, bei dem die Daten jedoch auf zentralen Servern gespeichert werden.

Projektziel ist ein neues System zur Vorlage von Verdienst-, Entgelt- und Arbeitsbescheinigungsdaten in sozialrechtlichen Verfahren. Die nach den Sozialgesetzen zur Leistungsberechnung vorgesehenen und vom Arbeitgeber zu bescheinigenden Daten (Höhe von Entgeltzahlungen, Daten zu den Beschäftigungszeiten etc.) sollen zukünftig nicht mehr vom Arbeitgeber auf Papier ausgestellt, sondern von ihm monatlich für alle seine Arbeitnehmer an eine Zentrale Speicherstelle (ZSS) elektronisch übertragen werden. Im Bedarfsfall sollen die im sozialrechtlichen Leistungsverfahren erforderlichen Daten aus der ZSS abgerufen werden und im EDV-System der Sozialbehörde elektronisch zur Verfügung stehen. Die Einführung des JobCard-Verfahrens soll eine erhebliche Kostenersparnis bei den Sozialbehörden und bei den Arbeitgebern bewirken. Die betroffenen Leistungsberechtigten sollen durch die beschleunigten Verwaltungsabläufe in den Sozialbehörden erheblich schneller ihre beantragte Sozialleistung erhalten.

Im (Teil-)Projekt JobCard I wurde zunächst die Möglichkeit untersucht, die Arbeitsbescheinigung nach

§ 312 SGB III digital zur Verfügung zu stellen. Das Konzept wurde ab September 2003 erfolgreich in mehreren Modellprojekten auf seine Praxistauglichkeit getestet. Mit der Übergabe des Projektberichtes durch den Projektnehmer, die Arbeitsgemeinschaft der Spitzenverbände der gesetzlichen Krankenversicherung, an das federführende BMWA ist dieses Projekt mittlerweile abgeschlossen.

Im (Teil-)Projekt JobCard II wird untersucht, ob die für das (Teil-)Projekt JobCard I entwickelten Verfahren auf weitere Sozialleistungen (z. B. Sozialhilfe, Altersrente, Wohngeld) übertragbar sind und dort ebenfalls automatisiert Verdienst- und Entgeltbescheinigungsdaten zur Verfügung gestellt werden können.

Kasten zu Nr. 15.2

Einige datenschutzrechtliche Forderungen bleiben, die im Gesetzgebungsverfahren berücksichtigt werden müssen:

- Der Bürger muss unmittelbar erkennen können, welche der ihn betreffenden Daten für welchen Zweck an welcher Stelle und wie lange gespeichert werden.
- Die Daten dürfen ausschließlich für Bescheinigungszwecke in sozialrechtlichen Verfahren und nur mit Zutun des betroffenen Leistungsberechtigten zur Verfügung gestellt werden. Es ist gesetzlich sicherzustellen, dass andere Behörden keinen Zugang zu den Daten in der ZSS erhalten. Dazu gehört auch ein gesetzlich vorgesehener Beschlagnahmeschutz für die Daten.
- Das JobCard-Verfahren muss für alle Beteiligten transparent sein.
- Die Auskunftsrecht für den Betroffenen muss im gesamten Verfahren gewährleistet werden. Der Betroffene sollte darüber hinaus aktiv über die zu seiner Person gespeicherten Daten informiert werden.
- Die Kontrolle des Verfahrens durch unabhängige Datenschutzbeauftragte muss sichergestellt sein.
- Bei allen Phasen der Datenverarbeitung muss die Datensicherheit gewährleistet werden.

Im Rahmen des JobCard-Verfahrens sollen die gesetzlich vorgesehenen Verdienst-, Entgelt- und Arbeitsbescheinigungsdaten vom Arbeitgeber für jeden Arbeitnehmer monatlich verschlüsselt an die ZSS übermittelt werden. Mit der erfolgreichen Übermittlung ist der Arbeitgeber von der Verpflichtung zur Erstellung der entsprechenden Bescheinigungen befreit.

Der Leistungsberechtigte soll künftig eine Signaturkarte mit gültigem qualifiziertem elektronischen Zertifikat (§ 7 Signaturgesetz) bei der Sozialbehörde vorlegen, wenn er eine Sozialleistung erhalten will. Nur bei Vorlage sowohl der Karte des Leistungsberechtigten als auch des Behördenmitarbeiters können die Daten aus der ZSS abgerufen werden.

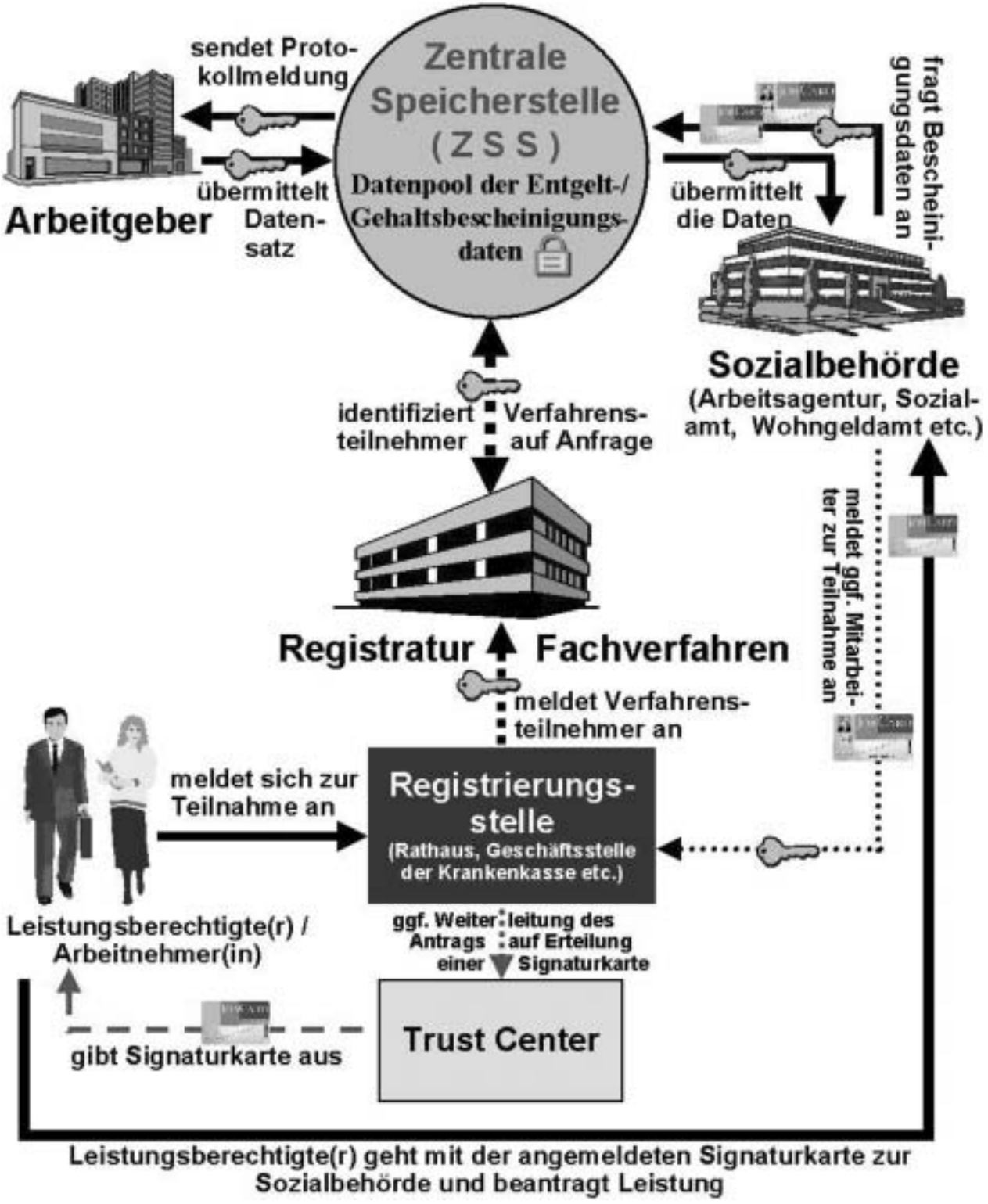
Nach dem Willen der Bundesregierung soll jeder abhängig Beschäftigte – auch die Beamten – verpflichtet werden, eine signaturgesetzkonforme Signaturkarte bei einer Registrierungsstelle (Rathaus, Geschäftsstelle einer Krankenkasse etc.) zum JobCard-Verfahren anzumelden. Eine entsprechende Signaturkarte kann er über die Registrierungsstelle bei einem Trust Center beantragen. Die Registrierungsstelle meldet die Signaturkarte bei der Registratur Fachverfahren im JobCard-Verfahren an. Für das JobCard-Verfahren werden auf der Signaturkarte außer den in § 7 Abs. 1 SigG genannten, für die elektronische Signatur notwendigen Daten keine weiteren Daten gespeichert sein.

Die mit dem Projekt JobCard-Verfahren beabsichtigte personenbezogene zentrale Speicherung von Gehalts-/Verdienstbescheinigungsdaten für aktuelle und ehemalige Mitarbeiter berührt das Grundrecht auf informationelle Selbstbestimmung. Ein solcher Eingriff darf nur auf der Grundlage einer verfassungsgemäßen gesetzlichen Regelung erfolgen. Vorgesehen ist daher eine gesetzliche Regelung darüber, welche personenbezogenen Daten der etwa 40 Millionen abhängig Beschäftigten gespeichert werden und wer zu welchem Zweck auf welche Daten zugreifen darf. Ich begrüße, dass ich bereits bei den Vorarbeiten zu dieser gesetzlichen Regelung beteiligt bin.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich mehrfach mit dem Thema JobCard-Verfahren auseinandergesetzt und gefordert, die Realisierbarkeit eines Ende-zu-Ende-Verschlüsselungsmodells gutachterlich zu prüfen.

Abbildung 5 (zu Nr. 15.2)

Funktionaler Ablauf des JobCard-Verfahrens



16 Arbeitsverwaltung

16.1 Hartz IV und die Folgen

Die Zusammenlegung von Arbeitslosen- und Sozialhilfe schafft zum 1. Januar 2005 eine neue Sozialleistungsform. Und eine Reihe von Problemen.

Arbeitslosenhilfe und Sozialhilfe werden zur neuen Grundsicherung für Arbeitsuchende zusammengeführt. Anspruchsberechtigt sind Personen zwischen 15 und 65 Jahren, die erwerbsfähig und hilfebedürftig sind und ihren gewöhnlichen Aufenthalt in Deutschland haben, sowie ihre mit ihnen in Gemeinschaft lebenden nicht erwerbsfähigen Angehörigen. Eingliederungsleistungen erhalten die Betroffenen nach dem SGB III und Leistungen zum Lebensunterhalt nach dem SGB II vom 24. Dezember 2003 (BGBl. I S. 2954). Wie schon die ersten „Hartz-Gesetze“ beruht auch Hartz IV auf dem Bericht der Kommission zum Abbau der Arbeitslosigkeit und zur Umstrukturierung der Bundesanstalt für Arbeit (sog. „Hartz-Kommission“). Über einige Vorschläge dieser Kommission hatte ich in meinem 19. TB berichtet (Nr. 23.2.2).

Ursprünglich war die Leistungsträgerschaft ausschließlich für die Bundesagentur für Arbeit (BA) vorgesehen. Auf Bestreben der Länder beschloss der Vermittlungsausschuss des Deutschen Bundestages eine wesentliche organisatorische Änderung, die mit dem „Gesetz zur optionalen Trägerschaft von Kommunen nach dem Zweiten Sozialgesetzbuch (Kommunales Optionsgesetz)“ vom 30. Juli 2004 umgesetzt worden ist (BGBl. I S. 2014). Nunmehr regelt § 6 SGB II eine geteilte Zuständigkeit zwischen der BA und den kommunalen Trägern. Letztere sind u. a. für die Leistung für Unterkunft und Heizung zuständig. Das Gesetz sieht in § 44b SGB II vor, dass BA und kommunale Träger ihre jeweiligen Aufgaben einheitlich durch Gründung einer Arbeitsgemeinschaft (ARGE) wahrnehmen, die der Aufsicht der zuständigen obersten Landesbehörden im Benehmen mit dem BMWA unterliegen. Die ARGE nehmen die Aufgaben der Agenturen für Arbeit als Leistungsträger nach dem SGB II wahr. Die kommunalen Träger „sollen“ der ARGE die Wahrnehmung ihrer Aufgaben nach dem SGB II übertragen. Da „sollen“ nicht zwingend „müssen“ bedeutet, kann es zukünftig sein, dass einige Leistungsberechtigte mancherorts zwei Anlaufstellen haben, wenn die Aufgabenübertragung verweigert wird. Darüber hinaus wird maximal 69 Kommunen die Option eingeräumt, alle Aufgaben nach dem SGB II eigenständig wahrzunehmen (sog. zugelassene kommunale Träger).

Dass diese geteilte Zuständigkeit nicht nur organisatorische, finanzielle und verfahrensmäßige Schwierigkeiten aufwirft, liegt auf der Hand. Auch der Datenschutz spielt eine ganz wesentliche Rolle in diesem Reformvorhaben, von dem annähernd drei Millionen Bürgerinnen und Bürger betroffen sein werden. Denn eines stand von Anfang an fest: Ohne Daten kein Starten! Deshalb standen die verantwortlichen Stellen vor der großen Herausforderung, Millionen Datensätze zu erheben und zu verwalten. Für welchen Weg man sich entschieden hat, wird nachfolgend dargestellt.

16.1.1 Das Sozialgesetzbuch II und Datenschutz

Das SGB II nach Art. 1 des Vierten Gesetzes für moderne Dienstleistungen am Arbeitsmarkt vom 24. Dezember 2003 enthielt ursprünglich nur wenige Regelungen zum Datenschutz. Weiteren Handlungsbedarf hatte der Gesetzgeber nicht gesehen, da ergänzend die allgemeinen Vorschriften über den Schutz der Sozialdaten – insbesondere § 35 SGB I und die §§ 67 ff. SGB X – gelten. Im Zuge des Kommunalen Optionsgesetzes, das die Beteiligung der Kommunen und damit die Notwendigkeit des Datenaustausches zwischen den beteiligten Stellen mit sich brachte, wurden auf meine Anregung hin einige datenschutzrechtliche Verbesserungen erreicht. So ist es erfreulich, dass die BA an ihre Kunden jeweils eine neue Nummer vergibt, wenn eine Zeit der Leistungsunterbrechung eintritt. Damit wird vermieden, dass sich die in § 51a SGB II vorgesehene Kundennummer zu einem verfassungsrechtlich problematischen Personenkennzeichen entwickelt (s. Nr. 8.2). Weiterhin enthielt § 51b Abs. 2 SGB II in seiner ursprünglichen Fassung die Formulierung, dass die zuständigen Träger der Grundsicherung „mindestens“ Angaben über bestimmte Einzeldaten erheben. Auf Grund meiner Bedenken wurde das Wort „mindestens“ gestrichen. Und um sicherzustellen, dass die erhobenen Daten nur zu bestimmten, gesetzlich normierten Zwecken verwendet werden, habe ich gefordert, dass eine strikte Zweckbindung in § 51b SGB II aufgenommen wird. Nach dessen Absatz 4 heißt es nun, dass die nach den Absätzen 1 bis 3 erhobenen Daten nur für die im Gesetz näher aufgeführten Zwecke verarbeitet werden dürfen. Damit verbietet das Gesetz eine darüber hinausgehende Nutzung.

16.1.2 Die Fragebögen zum Arbeitslosengeld II

Im Zuge der Einführung des Arbeitslosengeld II entfachten die zunächst 16-Seiten starken Antragsformulare eine Flut an Protesten und Beschwerden. Da ich an der Gestaltung der Formulare nicht beteiligt worden war, konnte ich diese erst nach Drucklegung datenschutzrechtlich prüfen. Bereits eine erste Überprüfung ließ erhebliche datenschutzrechtliche Mängel erkennen. Die Antragsbögen enthielten auch Angaben, die für die Leistungsberechnung nicht erforderlich waren. So war beispielsweise die Frage nach der Bankverbindung des Vermieters besonders kritisch. Viele besorgte Betroffene wandten sich an mich mit der Befürchtung, dass Mietzinszahlungen von der BA direkt auf das Konto der Vermieter gezahlt würden, die auf diesem Weg von der Arbeitslosigkeit erführen. Abgesehen von dieser nachvollziehbaren Sorge ist die Erhebung der Vermieterkonten im Rahmen der Daten-

erfassung auch nicht erforderlich. Die BA hat sich inzwischen dieser Auffassung angeschlossen.

Es fiel auf, dass die Bögen an einigen Stellen unverständlich waren. Insbesondere dort, wo Daten von Verwandten oder Verschwägerten abgefragt wurden, herrschte bei den Antragstellern große Verunsicherung. Nach § 9 Abs. 5 SGB II besteht eine gesetzliche Vermutung, dass Hilfebedürftige, die in Haushaltsgemeinschaft mit Verwandten oder Verschwägerten leben, Leistungen von diesen Personen erhalten, soweit dies nach deren Einkommen und Vermögen erwartet werden kann. Um die finanzielle Leistungsfähigkeit der Verwandten und Verschwägerten zu überprüfen, wollte die BA generell Informationen über deren Einkommens- und Vermögenssituation erlangen. Hier hatte ich allerdings darauf aufmerksam gemacht, dass die Antragssteller nach dem Gesetz diese Vermutung widerlegen können. Ferner sind ihre Daten nur dann relevant für die Leistungsberechnung, wenn feststeht, dass sie den Hilfebedürftigen finanziell unterstützen. Um diese Vermutung zu widerlegen, reicht es aus, wenn die betroffenen Haushaltsmitglieder eine entsprechende Erklärung gegenüber der BA abgeben. In diesem Fall ist es nicht mehr notwendig, weitere Angaben abzufragen. Die BA hat sich dieser Ansicht angeschlossen und dies bei der Neugestaltung der Antragsformulare berücksichtigt.

Ein weiteres Thema war die Vorgabe an Angehörige von Antragstellern, ihr Vermögen auf einem Vordruck der BA anzugeben und ihr Einkommen vom Arbeitgeber bescheinigen zu lassen. Dies war aus datenschutzrechtlicher Sicht in zweifacher Hinsicht bedenklich. Das entsprechende Zusatzblatt zum Antragsformular war ursprünglich als Doppelseite gedruckt. Auf der Vorderseite sollte der Angehörige sein Vermögen eintragen, und auf der Rückseite sollte er sich von seinem Arbeitgeber sein Gehalt bescheinigen lassen. Auf diese Weise konnte der Arbeitgeber Kenntnis von den auf der Vorderseite eingetragenen Vermögensbestandteilen seines Arbeitnehmers erlangen und zugleich erfahren, dass ein Angehöriger seines Arbeitnehmers arbeitslos ist. Diese Informationen gehen den Arbeitgeber nichts an. Meiner Forderung, das Zusatzblatt zu trennen, kam die BA kurzfristig nach. Damit war aber das Problem noch nicht vollständig gelöst. Ich hatte vorgeschlagen, das Einkommen statt durch den BA-Vordruck mittels der üblichen Gehaltsnachweise belegen zu lassen. Entsprechend wird bei der Sozialhilfe verfahren. Die BA bestand jedoch auf der Verwendung ihrer Vordrucke. Immerhin konnte ich noch erreichen, dass die Druckkennung entfernt wurde, die die BA als Urheber der Bescheinigung erkennbar werden ließ.

Daneben zeichnet sich ein Problem im Bereich der Gesundheitsdaten ab. Nach § 21 Abs. 5 SGB II erhalten Hilfebedürftige einen Mehrbedarf, die aus medizinischen Gründen einer kostenaufwändigen Ernährung bedürfen. Die Mehrbedarfsleistung muss im Einzelfall durch ärztliche Bescheinigung festgestellt werden. Hier ist zu gewährleisten, dass die Gesundheitsdaten, die für die Berechnung der Mehrbedarfshöhe erforderlich sind, nicht in den Vermittlungsbereich der Agenturen gelangen. So darf es beispielsweise nicht sein, dass der Antrag eines HIV-Patienten, der Mehrkosten wegen kostenaufwändiger Ernährung geltend macht, von der Person bearbeitet wird, die ihn später in den Arbeitsmarkt vermitteln soll. Daher halte ich es für unabdingbar, dass die Vermittler keine Kenntnis von Krankheiten erhalten. Die BA will zusammen mit mir zu einer einvernehmlichen Lösung kommen.

Die dargestellten Problemfelder sind nur ein Ausschnitt aus der Vielzahl datenschutzrechtlicher Fragen, die sich auf die Antragsformulare bezogen. Gemeinsam mit den Landesbeauftragten für den Datenschutz habe ich die Defizite herausgearbeitet und die BA zur Korrektur aufgefordert (vgl. hierzu die Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Kasten zu Nr. 16.1.2). Eine Neuauflage unter Berücksichtigung der Forderungen der Datenschutzbeauftragten des Bundes und der Länder hat die BA für das Frühjahr 2005 in Aussicht gestellt.

Nachdem die Antragsformulare versandt worden waren, musste eine Lösung gefunden werden, um die Erhebung von nicht erforderlichen und damit unzulässigen Daten wenn nicht ganz zu verhindern, so doch zumindest einzugrenzen. Um dies zu erreichen, entwickelte die BA in kurzer Zeit unter meiner Mitwirkung sog. „Ausfüllhinweise der Bundesagentur für Arbeit zum Antragsvordruck Arbeitslosengeld II“ und stellte diese auf ihre Homepage im Internet zum Abruf ein. Da nicht alle Betroffenen über einen Internetzugang verfügen, habe ich darauf bestanden, die Ausfüllhinweise in den Agenturen auszulegen und dafür Sorge zu tragen, dass jeder Antragssteller, der die Formulare noch nicht abgegeben hatte, davon Kenntnis erlangen konnte. Trotz entsprechender Anweisungen der BA kam es in der praktischen Umsetzung zu erheblichen Schwierigkeiten. Ich erhielt viele Beschwerden, wonach die Ausfüllhinweise in den Agenturen entweder überhaupt nicht auslagen oder nur auf Drängen ausgehändigt wurden. Die Verbindlichkeit der Ausfüllhinweise wurde darüber hinaus von einigen Mitarbeitern der BA gegenüber Kunden in Abrede gestellt.

Außerdem habe ich erfahren, dass viele Agenturen keine diskrete Bearbeitung der Anträge anboten und die Antragsannahme in „Großraumbüros“ stattfand. Schutzwürdige Sachverhalte, die am Nachbartisch behandelt wurden, konnten mitgehört werden. Dieser Zustand ist nicht hinnehmbar. So kann den Antragstellern durch ein deutlich sichtbares Hinweisschild die Möglichkeit einer Beratung in einem Einzelzimmer eingeräumt werden (vgl. Nr. 16.5).

Kasten zu Nr. 16.1.2

68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. und 29. Oktober 2004

Entschließung:
Gravierende Datenschutzmängel bei Hartz IV

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass es bei der praktischen Umsetzung der Zusammenlegung von Arbeitslosen- und Sozialhilfe zu erheblichen datenschutzrechtlichen Mängeln gekommen ist. Diese bestehen sowohl bei den Verfahren der Datenerhebung durch die verwendeten Antragsformulare als auch bei der Leistungsabrechnungs-Software (A2LL). Die Datenschutzdefizite wären vermeidbar gewesen, wenn datenschutzrechtliche Belange von Anfang an angemessen berücksichtigt und umgesetzt worden wären.

Zwar stellt die Bundesagentur für Arbeit (BA) seit dem 20. September 2004 sog. „Ausfüllhinweise zum Antragsvordruck Arbeitslosengeld II“ zur Verfügung, in denen viele Bedenken der Datenschutzbeauftragten aufgegriffen werden. Allerdings ist hierbei zu berücksichtigen, dass durch die Ausfüllhinweise nicht mehr alle antragstellenden Personen erreicht werden können. Umso wichtiger ist es, dass die örtlich zuständigen Leistungsträger die verbindlichen Ausfüllhinweise beachten und die antragstellenden Personen, die ihren Antrag noch nicht eingereicht haben, vor der Abgabe auf diese hingewiesen werden. Personen, die ihren Antrag früher gestellt haben, dürfen nicht benachteiligt werden. Überschussinformationen, die vorhanden sind und weiterhin erhoben werden, sind zu löschen.

Darüber hinaus will die BA die in den Antragsformularen nachgewiesenen Datenschutzmängel in vielen Bereichen in der nächsten Druckauflage korrigieren und für das laufende Erhebungsverfahren zur Verfügung stellen. Gleichwohl ist zu befürchten, dass die Formulare nicht das erforderliche Datenschutzniveau erreichen.

Hinsichtlich der Software A2LL bestehen immer noch wesentliche Datenschutzmängel, die zu erheblichen Sicherheitsrisiken führen. Insbesondere besteht für die Sachbearbeitung ein uneingeschränkter bundesweiter Zugriff auf alle Daten, die im Rahmen von A2LL erfasst wurden, auch soweit diese Daten für die Sachbearbeitung nicht erforderlich sind. Dieser Mangel wird dadurch verschärft, dass noch nicht einmal eine Protokollierung der lesenden Zugriffe erfolgt und damit missbräuchliche Zugriffe nicht verfolgt werden können. Das Verfahren muss über ein klar definiertes Zugriffsberechtigungskonzept verfügen. Die Beschäftigten der zuständigen Leistungsträger dürfen nur den zur Aufgabenerfüllung erforderlichen Zugriff auf die Sozialdaten haben.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA auf, die notwendigen Schritte unverzüglich einzuleiten und nähere Auskunft über den Stand des Verfahrens zu erteilen.

16.1.3 Erhebungs- und Leistungssystem A2LL

Die BA verwendet für die elektronische Datenerfassung aus den Antragsvordrucken für das Arbeitslosengeld II und die Leistungsberechnung das Software-Programm A2LL. Dieses Programm wurde mir vor seinem Einsatz in den Grundzügen vorgestellt. Hierbei musste ich feststellen, dass für die Nutzer die Möglichkeit einer bundesweiten Personensuche im gesamten Datenbestand von A2LL besteht. Eine Begrenzung durch Suchkriterien ist danach ebenso wenig möglich wie eine Protokollierung der lesenden bundesweiten Suchanfragen. A2LL verfügt nicht über ausreichende Sicherungsmaßnahmen gegen einen Datenmissbrauch.

Ich habe die BA darauf hingewiesen, dass ein differenziertes Zugriffsberechtigungskonzept erforderlich ist. Damit soll erreicht werden, dass nur derjenige Mitarbeiter Zugriff auf die in A2LL gespeicherten Sozialdaten erhält, der diese für die Erledigung seiner konkret zugewiesenen Aufgabe benötigt. Durch eine Protokollierung muss kontrolliert werden können, ob die Zugriffe auf Daten des bundesweiten Datenbestands in A2LL erfolgt sind und ob diese zur ordnungsgemäßen Aufgabenerfüllung erforderlich waren. Insbesondere eine nutzerbezogene Protokollierung bundesweiter Zugriffe (mit regelmäßiger Auswertung) muss vorrangig realisiert werden.

Um die Auszahlung des Arbeitslosengeldes II zum 1. Januar 2005 nicht zu gefährden, war ich bereit, den Einsatz von A2LL in den ARGE für einen verbindlich zu erklärenden, kürzeren Übergangszeitraum nicht zu beanstanden, wenn wenigstens datenschutzrechtliche Minimalstandards gewährleistet würden. Insbesondere hatte ich die Protokollierung der bundesweiten Personensuchanfragen in A2LL und eine verbindliche Zusicherung hinsichtlich der Realisierung eines datenschutzgerechten Zugriffsschutzkonzeptes gefordert. Diese Forderung wurde jedoch nicht umgesetzt. Zwar teilt die BA meine Rechtsansicht, dass eine Protokollierung notwendig ist. Die Implementierung einer nutzerbezogenen Protokollierung hätte jedoch nach ihrer Aussage zu erheblichen Umsetzungsproblemen geführt. Dadurch wäre die Einsetzbarkeit des gesamten Verfahrens zum geplanten Termin gefährdet worden. Die Umsetzung meiner Anforderungen wurde erst für einen späteren Zeitpunkt im Jahre 2005 zugesagt.

Ich sehe in den Ausführungen der BA keine Rechtfertigung dafür, dass ein Verfahren in Betrieb genommen wurde, das nicht einmal den datenschutzrechtlichen Basisanforderungen genügt. Vielmehr wäre es durch eine frühzeitige Berücksichtigung der datenschutzrechtlichen Belange in der Planung durchaus möglich gewesen, die wesentlichen Datenschutzmängel zu vermeiden. Ich habe deshalb das Verfahren A2LL als Verstoß gegen das Sozialgeheimnis des § 35 SGB I Abs. 1 i. V. m. § 78a SGB X beanstandet.

Die in § 35 SGB I genannten Stellen, die personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführungen der Vorschriften der Datenschutzgesetze zu gewährleisten. Hierbei ist zu berücksichtigen, dass bereits die Tatsache, dass jemand Bezieher von Arbeitslosengeld II ist, sozialdatenschutzrechtlich geschützt ist. Es muss gewährleistet sein, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können und dass Sozialdaten bei der Verarbeitung und Nutzung sowie nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Anlage zu § 78a Satz 2 Nr. 3 SGB X).

Zu den Kernstücken der gesetzlich vorgeschriebenen organisatorisch-technischen Maßnahmen gehört die enge Begrenzung der befugten Benutzer bzw. das Einrichten einer formalen Benutzerverwaltung und eine Protokollierung von Zugriffen, um Missbrauchsversuchen begegnen zu können. Letzteres bedingt auch eine regelmäßige Auswertung der Protokolle. Dies kann bei größeren Datenmengen auch stichprobenweise oder unter Einsatz entsprechender Tools geschehen.

Über derartige Schutzmechanismen verfügt das Programm A2LL derzeit nicht. Damit ist es jedem Nutzer von A2LL möglich, unkontrolliert eine bundesweite Personensuche im Datenpool von A2LL zu starten. Derartigen Missbrauchsmöglichkeiten stehen keine geeigneten Schutzmaßnahmen entgegen.

Ich habe der BA meine Mithilfe bei der Entwicklung konstruktiver Lösungen angeboten und erwarte eine baldige Umsetzung der Zusagen, insbesondere hinsichtlich der Einführung der Protokollierung bundesweiter Zugriffe im ersten Quartal 2005 und der zügigen Ausarbeitung und Implementierung eines Berechtigungskonzepts.

16.2 Virtueller Arbeitsmarkt – bitte mit realer Sicherheit!

Der virtuelle Arbeitsmarkt birgt Chancen und Risiken für den Benutzer.

Mit der Einführung des Arbeitgeberinformations-Service (AIS), des Stellen-Informations-Service (SIS) und des Ausbildungs-Stellen-Informations-Service (ASIS) hatte die Bundesagentur für Arbeit (BA) ihre Online-Vermittlungsangebote im Internet ausgebaut (vgl. 18. TB Nr. 20.7). Im Rahmen des Projekts „Virtueller Arbeitsmarkt“ (VAM) hat die BA ihre Online-Vermittlungsangebote ab dem 1. Dezember 2003 durch das Serviceportal „Arbeitsagentur.de“ ersetzt. Arbeitgeber wie Bewerber können sich registrieren lassen, behalten aber auch die Möglichkeit, das Angebot anonym zu nutzen. Bewerber und Betriebe, die in den bisherigen Verfahren keinen direkten Zugriff auf offene Stellen und Bewerberprofile hatten, können im VAM ihre Stellen- oder Bewerberdaten auf Wunsch selbst verwalten, wobei jeder Nutzer selbst entscheidet, ob er sein Stellen- oder Bewerberprofil anonym oder offen präsentieren möchte. Registrierte Bewerber können einen sog. Matching-Prozess nutzen, in dem ein Bewerberprofil mit dem Anforderungsprofil einer Stelle verglichen wird.

Die Registrierung im VAM erfolgt, indem Name, Vorname, Geburtsdatum, Geburtsort und aktuelle Wohnanschrift bzw. entsprechende Firmendaten eingegeben werden. Mit dem VAM will die BA eine Vermittlungsleistung zur Verfügung stellen, die die Eigeninitiative unterstützt. Dementsprechend tragen die Nutzer die Verantwortung für von ihnen bereitgestellte Angaben.

Ich habe die BA darauf hingewiesen, dass vor der Registrierung von den Betroffenen eine Einwilligung gem. § 67b SGB X eingeholt werden muss, wobei auf Verständlichkeit und Vollständigkeit der Information zu achten ist. Meiner Anregung, ein Feld „Datenschutz“ auf der Web-Oberfläche des VAM zu installieren, ist die BA gefolgt. Der Nutzer wird inzwischen darauf hingewiesen, dass Risiken und Missbrauchsmöglichkeiten sowie die Gefahr von Spam-Mails bestehen.

Mit dem Projekt VAM ist auch die Ablösung der bisherigen Vermittlungssoftware für die Mitarbeiter der BA verbunden. Das System VerBIS (Vermittlungs-, Beratungs- und Informations-System) soll von der BA mit Beginn des Jahres 2005 zunächst in Pilotagenturen getestet und anschließend bundesweit eingeführt werden. Nach Angabe der BA können mit VerBIS aussagekräftigere Bewerber- und Stellenprofile sowie vom Nutzer selbst eingegebene Daten verwendet werden. Bei der Ablösung von coArb (computerunterstützte Arbeitsvermittlung) und COMPAS (computerunterstütztes Ausbildungsvermittlungssystem) durch VerBIS sollen personenbezogene Daten von VAM-Nutzern in die zentrale Personendatenverwaltung aufgenommen werden. Die VAM-Kunden sollen zusätzlich eine Kundennummer der BA bekommen. Für den Fall, dass der VAM-Kunde später arbeitslos wird und sich bei der BA meldet, soll der Arbeitsvermittler auf die VAM-Daten und zurückliegende Bewerbungsprofile zugreifen können.

Ich halte die von der BA geplante generelle Verwendung von personenbezogenen Daten der VAM-Nutzer in VerBIS für problematisch. Die Speicherung und Nutzung der VAM-Daten erfolgt dann für Zwecke, für die sie zunächst nicht gespeichert wurden (vgl. § 67c Abs. 1 Satz 2 SGB X). Die VAM-Nutzer stellen der BA zum Zeitpunkt der Registrierung ihre personenbezogenen Daten nicht mit der Absicht zur Verfügung, dass diese für die Arbeitsvermittlung nach dem SGB III verwendet werden. Der

Zugriff der BA auf VAM-Daten für die Verwendung in der Arbeitsvermittlung würde somit eine Zweckänderung darstellen, soweit der Betroffene nicht hierin einwilligt. Die automatische Übernahme der Daten von VAM-Nutzern in VerBIS wäre eine unzulässige Nutzung, da zum Zeitpunkt der Datenspeicherung noch nicht feststeht, ob der Fall der Arbeitslosigkeit eintritt.

Ich habe die BA auf diese Rechtsprobleme hingewiesen und für die Verwendung der VAM-Bewerberdaten eine gesetzliche Grundlage gefordert. Solange eine entsprechende gesetzliche Befugnis nicht besteht, muss eine wirksame Einwilligung der Betroffenen eingeholt werden.

16.3 Verwendung von Rentendaten zum Zweck des Forderungsinkassos unzulässig?

Die von der Bundesagentur für Arbeit geplante Nutzung der für die Arbeitsmarktstatistik übermittelten Daten der Rentenversicherungsträger für andere Zwecke ist wegen einer fehlenden Rechtsgrundlage unzulässig.

Die Bundesagentur für Arbeit (BA) prüft einen Datenabgleich ihrer Schuldnerdatei mit den von der Datenstelle der Rentenversicherungsträger (DSRV) für die Arbeitsmarktstatistik übermittelten Daten. Sie beruft sich dabei auf § 281 Satz 2 SGB III. Die BA erhofft sich dadurch eine Effektivierung ihres Forderungsinkassos. Ich halte den angedachten Datenabgleich rechtlich für unzulässig, da für die Verwendung von statistischen Daten für Verwaltungszwecke eine gesetzliche Grundlage fehlt. Zudem würde eine derartige Umwidmung statistischer Daten dem verfassungsrechtlichen Trennungsgebot von Statistik und Verwaltung widersprechen (vgl. BVerfGE 65, 1, 61).

Da von Datenabgleichsverfahren immer auch unbeteiligte Bürger erfasst werden und ihre persönlichen Verhältnisse mit jedem zusätzlichen Datenabgleich immer transparenter und für den jeweiligen Bearbeiter umfassender offen gelegt werden, ist vor der Einrichtung eines solchen Verfahrens zu prüfen, ob es im Interesse des Gemeinwohls zur Erreichung des konkreten Zieles erforderlich und verhältnismäßig ist, wie dies der Deutsche Bundestag bereits am 22. Juni 1995 gefordert hat (Bundestagsdrucksache 13/1636, S. 3). Ein Datenabgleich kann nicht in erster Linie mit einer Verwaltungs- und Geschäftserleichterung begründet werden. Er muss erforderlich sein, um tatsächlich bestehende Missstände abzustellen und künftig zu vermeiden. Sollte der Datenabgleich erforderlich sein, sind die Daten, die zwecks Abgleich übermittelt werden sollen, normenklar im Gesetz selbst oder in einer Rechtsverordnung aufzuführen und die Stellen zu nennen, zwischen denen der Datenabgleich zulässig ist. Daneben ist es unverzichtbar, die Betroffenen durch Hinweise in Vordrucken und Merkblättern auf die Datenabgleiche zur Verhinderung von Leistungsmissbrauch vorher aufmerksam zu machen.

In diesem Zusammenhang kommt auch eine Zweckänderung der vom Verband der Rentenversicherungsträger (VDR) überlassenen Daten durch die BA nicht in Betracht. Dies ergibt sich insbesondere aus § 67c SGB X. So sieht § 67c Abs. 2 Nr. 1 SGB X die Möglichkeit vor, dass die erhebende Stelle gespeicherte Sozialdaten auch für andere Zwecke nutzt als für die, für die sie erhoben worden sind. Voraussetzung ist jedoch, dass die Nutzung der Sozialdaten für die Erfüllung von Aufgaben nach anderen Rechtsvorschriften des SGB X als diejenigen, für die sie erhoben wurden, erforderlich sind. Diese Aufgaben müssen entsprechend dem Volkszählungsurteil des Bundesverfassungsgerichts auf einer gesetzlichen Grundlage beruhen, aus der sich die Voraussetzungen und der Umfang der Beschränkungen klar und für den Bürger erkennbar ergeben (BVerfGE 65, 1, 41 ff.). An einer solchen gesetzlichen Grundlage fehlt es hier. Zwar zählt die Rückforderung von zu Unrecht erbrachten Leistungen zu den Aufgaben der BA. Dass hierfür die Daten genutzt werden sollen, die der BA zur Erstellung der Statistik der sozialversicherungspflichtig Beschäftigten übermittelt werden, ist jedoch unzulässig.

Die Sozialdaten werden von den Arbeitgebern nach § 28a SGB IV gemeldet und von der DSRV gem. § 36 Abs. 3 Datenerfassungs- und -übermittlungsverordnung an die BA weitergeleitet. Hierbei handelt es sich um eine Aufgabenzuweisungsnorm und nicht um eine Norm, die zu einem Datenabgleich ermächtigt. Vor allem ist zu berücksichtigen, dass die Daten ausschließlich für Zwecke der Arbeitsmarktstatistik an die BA übermittelt werden, die dem Statistikgeheimnis unterliegen (§ 16 BStatG). Die BA hat dafür Sorge zu tragen, dass die ihr ausschließlich für Zwecke der Arbeitsmarktstatistik übermittelten Daten unverzüglich in den Statistikbereich gelangen. § 281 SGB III legitimiert gerade nicht dazu, diese Daten für allgemeine Verwaltungszwecke zu nutzen.

Ich habe die BA gebeten, in ihre weiteren Überlegungen eingebunden zu werden. Ich werde den weiteren Verlauf des Vorhabens kritisch begleiten.

16.4 Zweigeteilter Datenschutz in der Bundesagentur für Arbeit

Die Organisation des Datenschutzes in der Bundesagentur für Arbeit ist weiterhin verbesserungsbedürftig.

Der behördliche Datenschutzbeauftragte der BA (BfD/BA) ist seit geraumer Zeit als „Full-Time-Job“ ausgestaltet. Angesichts der Größe der BA (ca. 96 000 Mitarbeiter) habe ich Überlegungen unterstützt, den BfD/BA mit einer ausreichenden Anzahl Mitarbeiter auszustatten, wie dies in § 81 Abs. 4 Satz 1 SGB X i. V. m. § 4f Abs. 5 Satz 1 BDSG vorgegeben ist. Da der BfD/BA die ordnungsgemäße Anwendung der zahlreichen Datenverarbeitungsprogramme überwacht und ihm dabei auch die Vorabkontrolle nach § 4d Abs. 6 BDSG obliegt, die aufgrund der Meldungen für das Verfahrensverzeichnis durchgeführt wird, frage ich mich, wie er dies mit nur zwei Mitarbeitern bewältigen will.

Leider ist die Zusammenführung der Stellen BfD/BA und dem zuständigen IT-Fachreferat – außerhalb des IT-Bereichs – immer noch nicht erfolgt (vgl. 19. TB Nr. 23.1). Aufgrund der Zweiteilung des Datenschutzes in der BA

gibt es zudem Schnittstellen bei der Wahrnehmung der Datenschutzaufgaben, was – wie auch die BA einräumt – vermeidbare Reibungsverluste verursacht. Die BA hat zur Verbesserung dieser Strukturen eine Arbeitsgruppe eingerichtet, die die Aufgabenabgrenzung zwischen dem Fachreferat und dem BfD/BA erörtern und eine Entscheidung für eine neue organisatorische Zuordnung vorbereiten soll. Ich habe der BA meine Mithilfe bei der organisatorischen Neugestaltung angeboten.

16.5 Mangelnde Diskretion in den Agenturen für Arbeit

Verletzung des Datenschutzes durch fehlende Hinweise, welche die Kunden auf die Möglichkeit einer Einzelberatung in den Agenturen für Arbeit aufmerksam machen.

Wieder haben sich zahlreiche Petenten an mich gewandt, die ihre Rechte dadurch verletzt sehen, dass der Vertraulichkeitsschutz in den Kundenservicebereichen der Agenturen für Arbeit aufgrund der räumlich-organisatorischen Struktur (offener Publikumsverkehr an den Anmeldetresen) nicht gewährleistet ist. Beschwerde wurde auch darüber geführt, dass in den anschließenden Gesprächen jeweils zwei Kunden gleichzeitig in einem Büro beraten werden.

Bereits in meinem 18. TB (Nr. 20.3) hatte ich auf diese Problematik im Zusammenhang mit dem unter der Bezeichnung „Arbeitsamt 2000“ entwickelten Konzept der Bundesanstalt für Arbeit – jetzt Bundesagentur für Arbeit (BA) – aufmerksam gemacht und die BA aufgefordert, geeignete Maßnahmen zu ergreifen, damit das unbefugte Mithören von Sozialdaten unterbunden wird. Trotz der daraufhin vorgenommenen raumgestaltenden Maßnahmen wie Diskretionszonen und Trennwänden lässt es sich nicht immer vermeiden, dass auch Sozialdaten von anderen Kunden mitgehört werden. Ich habe dieser Vorgehensweise im Hinblick auf den bei den Agenturen für Arbeit in der Regel großen Publikumsandrang und die vielfach räumlich unzulänglichen Raumkapazitäten nur unter der Voraussetzung zugestimmt, dass jeder Kunde der BA die Möglichkeit hat, auf Wunsch sein Anliegen in einem separaten Büro in einer Einzelberatung vorzutragen. Aus diesem Grunde ist es, wie mit der BA vereinbart, unbedingt erforderlich, dass in den Anmeldestellen und Büros, in denen Doppelberatungen stattfinden, entsprechende Hinweisschilder, die auf die Möglichkeit einer Einzelberatung aufmerksam machen, für die Kunden der BA gut sichtbar aufgestellt werden. Nur so kann der Kunde selbst entscheiden, ob die „Thekenlösung“ bei der Anmeldung oder die gleichzeitige Beratung von zwei Kunden in einem Büro seiner Datenschutzposition gerecht wird.

Leider ist die BA mit der Umsetzung dieser Maßnahme offensichtlich noch im Verzug. Denn zunehmend gehen Beschwerden von Petenten ein, die beklagen, dass die erforderlichen Hinweisschilder in den einzelnen Agenturen für Arbeit nicht vorhanden sind. Ich habe die BA um Abhilfe gebeten und sie aufgefordert, die Maßnahme in allen Agenturen für Arbeit umzusetzen. Ich werde durch Kontrollen überprüfen, ob diese Mängel abgestellt wurden.

16.6 Privatinkasso ohne Rechtsgrundlage

Für die Einschaltung privater Inkassounternehmen durch die Bundesagentur für Arbeit (BA) zur Beitreibung von Forderungen fehlt es an einer Rechtsgrundlage.

Ein Petent hat sich dagegen gewandt, dass die Agentur für Arbeit seine Sozialdaten an ein privates Inkasso-Unternehmen zwecks Beitreibung angeblich zuviel bezahlter Arbeitslosenhilfe weitergegeben hat. Nach Auskunft der BA wurden Geldforderungen der BA bislang durch zwölf Forderungseinzugsstellen eingezogen. Um die Forderungen effektiver und effizienter einzuziehen, laufe derzeit ein Modellversuch in mehreren Regionaldirektionsbezirken, in dem zwei private Unternehmen mit der Einziehung von Forderungen beauftragt wurden. Der Modellversuch sei im Rahmen einer Planung im Sozialleistungsbereich gem. § 75 Abs. 1 Satz 1 Nr. 2 SGB X gestartet worden. Ziel sei es, festzustellen, ob die Einziehung von Forderungen durch private Dritte wirtschaftlicher ist als durch die zwölf Forderungseinzugsstellen der BA.

Ich halte diese Vorgehensweise datenschutzrechtlich für problematisch. Zunächst ist die Feststellung nach § 75 Abs. 1 Satz 1 SGB X erforderlich, dass keine schutzwürdigen Interessen des Betroffenen beeinträchtigt werden oder dass, selbst wenn eine Beeinträchtigung im vorgenannten Sinne vorliegen sollte, im Rahmen einer Interessenabwägung das öffentliche Interesse das Geheimhaltungsinteresse des Betroffenen erheblich überwiegt. Dies wird man nur annehmen können, wenn ansonsten öffentliche Aufgaben nicht erfüllt werden können. Das schutzwürdige Interesse des Betroffenen besteht hier in der Wahrung des Sozialgeheimnisses nach § 35 SGB I. Aus Sicht des Betroffenen besteht ein erheblicher Unterschied, ob eine Einzugsstelle als öffentliche Stelle mit dem Einzugsverfahren betraut ist oder ob es sich um einen privaten Dritten handelt. Eine Rechtfertigung für die Einschaltung eines gewinnorientiert handelnden Dritten ergibt sich auch nicht aus dem Bedürfnis nach einer effizienteren Organisation des Forderungseinzuges, denn den Forderungseinzug können auch die Forderungseinzugsstellen leisten.

Da das öffentliche Interesse gegenüber der Wahrung des Sozialgeheimnisses des Petenten nicht erheblich überwiegt, ist § 75 SGB X keine geeignete gesetzliche Grundlage für die Einschaltung eines privaten Inkassounternehmens zum Zwecke des Forderungseinzuges durch die BA. Ob die Übertragung klassisch hoheitlicher Aufgaben wie der Einzug von Geldforderungen des Staates gegen den Bürger auf private Dritte überhaupt verfassungsrechtlich zulässig ist – ein Problem, dessen Bedeutung über den vorliegenden Fall hinausgeht – ist noch nicht abschließend geklärt. Ich habe die BA auf die Problematik hingewiesen. Eine Stellungnahme hierzu steht noch aus.

16.7 Einzelfälle

16.7.1 Unberechtigte Datenerhebung beim Hausarzt

Fehlende Schweigepflichtentbindungserklärung des Kunden der Agentur für Arbeit bei Auskunftsersuchen an dessen Hausarzt.

Ein Petent bescherte sich darüber, dass sich die für ihn zuständige Agentur für Arbeit unmittelbar mit seinem Hausarzt in Verbindung gesetzt hatte, um dort Daten über seine Arbeitsunfähigkeit und diesbezügliche Arbeitsunfähigkeitsbescheinigungen zu erfragen. Im Rahmen eines Widerspruchsverfahrens gegen den Änderungsbescheid zum Unterhaltsgeld war nach Angaben der Agentur für Arbeit eine Überprüfung erforderlich, ob für unentschuldigte Fehltage Arbeitsunfähigkeit vorgelegen habe. Für die Einholung von Auskünften beim Hausarzt wäre das Vorliegen einer Erklärung des Petenten über die Entbindung von der Schweigepflicht erforderlich gewesen. Da eine Schweigepflichtentbindungserklärung in diesem Fall aber nicht vorgelegen hat, war das Auskunftsersuchen der Agentur für Arbeit an den Hausarzt des Petenten nicht zulässig. Von einer förmlichen Beanstandung habe ich abgesehen, weil die Bundesagentur für Arbeit (BA) meine Rechtsauffassung teilt und die Agentur nachdrücklich auf die Einhaltung der Datenschutzbestimmungen hingewiesen hat.

16.7.2 Verletzung des Grundsatzes der Datenerhebung beim Betroffenen

Unzulässige Datenerhebung bei einer Bank.

Der Ehemann einer Petentin hatte bei der Agentur für Arbeit einen Antrag auf Arbeitslosenhilfe gestellt. In dem Antrag legte er seine Vermögens- und Einkommensverhältnisse sowie die der Petentin offen, verschwieg aber, dass er bei einem Geldinstitut ein Wertpapierkonto führte. Durch die zulässige Anfrage beim Bundesamt für Finanzen (BfF) nach § 45d Abs. 2 Einkommenssteuergesetz erhielt die Agentur für Arbeit Kenntnis von dem Konto. Insoweit war die daraufhin erfolgte Anfrage der Agentur für Arbeit bei dem Geldinstitut, datenschutzrechtlich nicht zu beanstanden. Obwohl gegen die Petentin selbst auf Grund der Anfrage beim BfF keine Verdachtsmomente hinsichtlich eines nicht angegebenen und zu berücksichtigenden Vermögens vorlagen, stellte die Agentur aber auch eine entsprechende Anfrage nach Konten der Petentin bei demselben Geldinstitut. Die Agentur für Arbeit begründete ihre Berechtigung für eine entsprechende Bankauskunft über die Petentin mit dem Missbrauchsverdacht gegen den Ehemann. Ein solcher Generalverdacht ist dem deutschen Rechtssystem jedoch fremd. Eine Anfrage bei dem Geldinstitut war daher datenschutzrechtlich nicht gerechtfertigt. Die Ermittlungen der Agentur für Arbeit haben sich am Grundsatz der Erforderlichkeit und Verhältnismäßigkeit zu orientieren. Dabei hat die Agentur für Arbeit unter mehreren zur Verfügung stehenden Mitteln das den Betroffenen am wenigstens belastende zu wählen. Die Agentur für Arbeit hätte daher die Anfrage im Rahmen des Erstermittlungsgrundsatzes zunächst an die Petentin persönlich richten müssen. Die BA hat sich meiner Rechtsauffassung angeschlossen und ihr Bedauern gegenüber der Petentin zum Ausdruck gebracht. Von einer förmlichen Beanstandung habe ich daher abgesehen.

16.7.3 Unrechtmäßige Anforderung einer Schweigepflichtentbindungserklärung

Die Abgabe einer Schweigepflichtentbindungserklärung fällt nicht unter die Mitwirkungspflichten der §§ 60 ff. SGB I, sondern unterliegt der Freiwilligkeit des Kunden der Agentur für Arbeit.

Eine Petentin, die bei der Agentur für Arbeit eine Trainingsmaßnahme nach § 48 SGB III zur beruflichen Eingliederung krankheitsbedingt abbrechen musste, wurde von der zuständigen Vermittlerin bei der Agentur für Arbeit darüber informiert, dass sie zur Überprüfung ihrer Leistungsfähigkeit ärztlich untersucht werden müsse. In diesem Zusammenhang verlangte die Vermittlerin der Agentur für Arbeit von der Petentin eine Erklärung zur Entbindung ihrer Ärzte von der Schweigepflicht. Dazu war die Petentin jedoch nicht bereit. Die Agentur für Arbeit drohte ihr daraufhin für den Fall, dass die Erklärung am nächsten Tag nicht unterschrieben vorliege, mit dem Entzug der laufenden Geldleistung.

Die Abgabe einer Schweigepflichtentbindungserklärung fällt nicht unter die Mitwirkungspflichten der §§ 60 ff. SGB I, sondern steht im freien Ermessen des Kunden/der Kundin der Agentur für Arbeit. Wird die Erklärung nicht abgegeben, hat der ärztliche Dienst auf die Beiziehung entsprechender Vorbefunde zu verzichten und muss das Leistungsvermögen des Kunden/der Kundin durch eigene Untersuchungen ermitteln. Dies entspricht auch der Rechtslage nach § 62 SGB I. Danach hat sich derjenige, der Sozialleistungen beantragt oder erhält, auf Verlangen des zuständigen Leistungsträgers ärztlichen und psychologischen Untersuchungsmaßnahmen zu unterziehen, soweit diese für die Entscheidung über die Leistung erforderlich sind. Eine Verpflichtung, Dritte von ihrer Schweigepflicht zu entbinden, verlangt das Gesetz nicht. Die BA hat zugesagt, durch Handlungsanweisungen für die Agenturen für Arbeit sicherzustellen, dass derartige Fälle künftig nicht mehr auftreten. Ich werde zu gegebener Zeit kontrollieren, ob diese Zusage beachtet wird.

16.7.4 Sozialdaten in der Mülltonne

Die Entsorgung von personenbezogenen Unterlagen der Agentur für Arbeit im Hausmüll verstieß gegen das Sozialgeheimnis.

Aufgrund einer Eingabe wurde ich auf folgenden Vorfall aufmerksam gemacht:

Ein Passant fand auf dem wenige Meter von der Geschäftsstelle der Agentur für Arbeit entfernten Marktplatz eine große Anzahl herumliegender Schriftstücke, bei denen es sich um Unterlagen aus Kundenakten der Agentur für Arbeit handelte. Diese bestätigte, dass die Schriftstücke mit personenbezogenem Inhalt von einem Mitarbeiter

mit dem Hausmüll entsorgt wurden. Nachdem der Hausmüllcontainer an einem Sonntag für die Leerung am folgenden Montag auf die Straße vor der Agentur gestellt worden war, wurde er umgestoßen, und durch einen Windstoß verteilte sich der Inhalt in der näheren Umgebung.

Wie die BA mir mitgeteilt hat, habe es sich um einen bedauerlichen Einzelfall gehandelt. In der Regel verlaufe die Entsorgung von personenbezogenen Unterlagen nach einem von allen Mitarbeitern praktizierten Verfahren, bei dem man spezielle Container einer Entsorgungsfirma verwendet.

Ich habe den Sachverhalt als Verstoß gegen das Sozialgeheimnis nach § 35 SGB I i. V. m. § 78a SGB X gewertet und ihn nach § 25 Abs. 1 BDSG beanstandet. Der Schutz des Sozialgeheimnisses verpflichtet die BA als den Leistungsträger dazu, durch technische und organisatorische Maßnahmen und durch Handlungsanweisungen die Einhaltung der Datenschutzvorschriften des SGB sicherzustellen. Der Schutz der besonders sensitiven Sozialdaten erfordert eine angemessene Gestaltung der innerbehördlichen Datenschutzorganisation. Hierzu gehört unter anderem, dass schutzwürdige Akteninhalte über Kunden der Agentur für Arbeit datenschutzgerecht entsorgt werden.

17 Krankenversicherung, Pflegeversicherung

17.1 Krankenversicherung

17.1.1 Die Gesundheitsreform und ihre Konsequenzen

Im Gesetz zur Modernisierung der gesetzlichen Krankenversicherung konnte ich in vielen Bereichen datenschutzfreundliche Lösungen erreichen; allerdings bleibt die Veränderung des Abrechnungsverfahrens hinter den datenschutzrechtlichen Anforderungen zurück.

Im Berichtszeitraum habe ich mich intensiv mit dem am 1. Januar 2004 in Kraft getretenen Gesetz zur Modernisierung der gesetzlichen Krankenversicherung (GKV-Modernisierungsgesetz – GMG, BGBl. I 2003 S. 2190) und den damit verbundenen datenschutzrechtlichen Fragestellungen beschäftigt. Vorrangiges Ziel der Gesundheitsreform sind die Begrenzung der Kosten im Gesundheitssystem und die Verbesserung der Qualität der medizinischen Versorgung. Datenschutzrechtlich bedeutsam sind vor allem erweiterte Befugnisse zur Verarbeitung medizinischer Abrechnungsdaten und eine verstärkte Kontrollmöglichkeit gegenüber den Versicherten und den übrigen am Gesundheitssystem Beteiligten. Weiter sollten durch verbesserte individuelle und statistische Informationen die medizinische und informationelle Selbstbestimmung der Patienten und die Transparenz für alle Beteiligten erhöht werden (vgl. Kasten zu Nr. 17.1.1).

Bereits im Vorfeld des ersten Gesetzentwurfs hatten sich die Datenschutzbeauftragen des Bundes und der Länder in einer Entschließung zur Modernisierung der gesetzlichen Krankenversicherung geäußert. Dennoch enthielten die ursprünglichen Entwürfe etliche Regelungen, die den Prinzipien der Erforderlichkeit und Verhältnismäßigkeit nicht genügten. Jedoch ist es gelungen, die meisten datenschutzrechtlichen Einwendungen auszuräumen. Deswegen hat sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer weiteren Entschließung grundsätzlich zustimmend zum GMG geäußert (vgl. Anlage 15).

Eine wesentliche Neuerung ist die Einführung der elektronischen Gesundheitskarte (vgl. dazu ausführlich Nr. 22.1).

Erst kurz vor Abschluss des Gesetzgebungsvorhabens wurden in das Gesetz datenschutzrechtlich problematische Änderungen des Abrechnungsverfahrens aufgenommen. Künftig sollen auch bei der Abrechnung ambulanter Behandlungen die Diagnosedaten versichertenbezogen an die Krankenkassen übermittelt werden, weil die Vergütung ärztlicher Leistungen nicht mehr nach Kopfpauschalen, sondern nach morbiditätsorientierten Regelleistungsvolumina abgerechnet werden soll. Dies hat zur Folge, dass die Krankenkassen umfassende und intime Kenntnisse über ihre Versicherten erhalten. Leider sind in diesem Zusammenhang die Möglichkeiten moderner und datenschutzfreundlicher Technologien, durch die diese datenschutzrechtlichen Risiken hätten vermieden werden können, nicht berücksichtigt worden, z. B. Pseudonymisierungsverfahren. Aufgrund der von den Datenschutzbeauftragten hiergegen geübten Kritik hat der Deutsche Bundestag klargestellt, dass die Krankenkassen diese Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen (strikte Zweckbindung) und dass eine sektorenübergreifende Zusammenführung von Abrechnungs- und Leistungsdaten unzulässig bleibt. Dies haben die Kassen durch technische und organisatorische Maßnahmen sicherzustellen (vgl. Bundestagsdrucksache 15/1600). Zum anderen trägt eine Entschließung des Deutschen Bundestages der Forderung Rechnung, bei der Evaluierung des neuen Abrechnungsverfahrens insbesondere die Grundsätze der Datenvermeidung und Datensparsamkeit zu berücksichtigen und die Möglichkeit von Pseudonymisierungsverfahren einzubeziehen (vgl. Bundestagsdrucksache 15/1584).

Weiter hat das GMG einige der bereits seit Jahren bestehenden Überlegungen zur Datentransparenz umgesetzt. So wird jetzt in den §§ 303a bis 303f SGB V ein Datenpool eingeführt, mit dessen Hilfe insbesondere Auswertungen für Steuerungsaufgaben in der gesetzlichen Krankenversicherung durchgeführt werden sollen. Die datenschutzrechtlichen Anforderungen wurden hierbei berücksichtigt (vgl. 19. TB Nr. 24.1.1). So dürfen die Daten der Versicherten und der Leistungserbringer nur in pseudonymisierter Form zusammengeführt werden. Die Pseudonymisierung wird von einer Vertrauensstelle durchgeführt, die Zusammenführung der pseudonymisierten Daten von einer Datenaufbereitungsstelle. Beide Stellen unterliegen dem Sozialgeheimnis und müssen von den Krankenkassen und den Kassenärztlichen Vereinigungen sowie von den nutzungsberechtigten Stellen räumlich, organisatorisch und personell abgeschottet sein. Auswertungen zu den gesetzlich festgelegten Zwecken

nimmt nur die Datenaufbereitungsstelle vor. Die berechtigte Stelle, die den Auftrag zur Auswertung gegeben hat, erhält nur aggregierte Daten, was neben weiteren Sicherungsmaßnahmen das Risiko einer Reidentifizierung bestmöglich minimiert (vgl. hierzu Nr. 4.1.1.2).

Die ursprünglich vorgesehene Möglichkeit für gesetzliche Krankenversicherungen, ihren Versicherten für ein gesundheitsbewusstes Verhalten Boni zu gewähren, barg das Risiko, dass die Kassen hierfür unter Verwendung detaillierter Informationen über die privaten Lebensgewohnheiten ihre Versicherten überwachen könnten. Wie im GMG jetzt aber klargestellt ist, darf ein Bonus nur für die Teilnahme an den gesetzlichen Früherkennungsuntersuchungen oder an qualitätsgesicherten Leistungen der Krankenkassen zur primären Prävention gewährt werden. Hierfür dürfen die Krankenkassen nur die entsprechenden Teilnahmebescheinigungen und keine weitergehenden Informationen über die Lebensführung der Versicherten erheben und verarbeiten.

Der Datenschutz bei der Gesundheitsreform muss sich in der Praxis noch bewähren.

Kasten zu Nr. 17.1.1

Bei mehr Kontrollmöglichkeiten durch die Krankenkassen muss folgendes beachtet werden:

- Recht der Patienten auf Selbstbestimmung
- Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen
- Grundsätze der Datenvermeidung, der Erforderlichkeit und der Verhältnismäßigkeit
- Informationen und Transparenz für die Betroffenen
- Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten nutzen.

Bei Zugriff auf personenbezogene Behandlungsdaten im Rahmen der Qualitätssicherung und Abrechungskontrolle wird gefordert:

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichproben zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten,
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

17.1.2 Folgeprobleme der Gesundheitsreform

Die Umsetzung des GMG warf in vielen Bereichen datenschutzrechtliche Fragen auf.

Das GMG hat auch die Voraussetzungen und das Verfahren zur Übernahme von Fahrtkosten und Krankentransporten in § 60 SGB V neu geregelt. Danach übernimmt die Krankenkasse diese Kosten nur noch, wenn sie in Zusammenhang mit einer Leistung der Krankenkasse aus zwingenden medizinischen Gründen notwendig sind. Deswegen wurde die Krankentransportrichtlinie entsprechend geändert. Da für Fahrten zu ambulanten Behandlungen nun regelmäßig eine vorherige Genehmigung nötig ist, wurde auch eine Änderung des bisherigen Verordnungsformulars erforderlich. Da dieses vorsah, dass der verordnende Arzt die Diagnose einträgt, konnten Dritte (beispielsweise Taxifahrer) Gesundheitsdaten (Diagnosen) der Versicherten zur Kenntnis nehmen. Nachdem ich unter Hinweis auf den Vorrang der ärztlichen Schweigepflicht auf den hier bestehenden datenschutzrechtlichen Änderungsbedarf hingewiesen hatte, entwickelten die Spitzenverbände der Krankenkassen und die Kassenärztliche Vereinigung als Übergangsregelung ein mit mir abgestimmtes Verfahren, bei dem die Fahrer von Taxen, Mietwagen u. ä. bei Fahrten zu ambulanten Behandlungen keine medizinischen Daten mehr zur Kenntnis erhalten. Ein neues, mit mir abzustimmendes Verordnungsformular, das dann die datenschutzrechtlichen Anforderungen berücksichtigt und dessen Verwendung ab dem 1. Januar 2005 vorgesehen war, wurde mir leider bisher noch nicht vorgelegt.

Aufgrund des GMG wurden auch die Voraussetzungen zur Befreiung von Zuzahlungen geändert. Nach der Neuregelung gelten bestimmte Belastungsgrenzen (2 Prozent des jährlichen Bruttoeinkommens bzw. 1 Prozent bei Vorliegen einer schwerwiegenden chronischen Erkrankung), bei deren Überschreiten die Versicherten keine weiteren Zuzahlungen mehr zu leisten brauchen. Um jedoch die Überschreitung der Belastungsgrenze feststellen zu können, müssen die Krankenkassen die hierfür erforderlichen Daten von den Versicherten erheben, die die Befreiung beantragen. Zur Prüfung der Höhe der jeweiligen persönlichen Belastungsgrenze benötigen die Krankenkassen bestimmte Informationen und Nachweise, etwa zu den (Familien-) Einnahmen (regelmäßige monatliche Bruttoeinnahmen) und den geleisteten Zuzahlungen. Gegen die Erhebung dieser Daten ist aus datenschutzrechtlicher Sicht nichts einzuwenden. Zur Prüfung, ob eine schwerwiegende chronische Erkrankung (und damit die Voraussetzung einer entsprechenden höheren Reduzierung der Belastungsgrenze) vorliegt, wird i. d. R. ein Formular eingesetzt, in dem der behandelnde Arzt das Vorliegen einer chronischen Krankheit bescheinigt. Der Nachweis für die geleisteten Zuzahlungen kann entweder durch entsprechende Belege erfolgen oder in – von den Krankenkassen für diesen Zweck zur Verfügung gestellten – Nachweisheften, in denen dann neben der Bezeichnung der Leistung die gesetzliche Zuzahlung in Euro und eine Bestätigung der abgebenden Stelle (z. B. Stempel, Unterschrift) vermerkt werden. Für den besonderen Fall, dass Ehepartner in unterschiedlichen Krankenkassen versichert sind, haben die Krankenkassen eine generelle Regelung getroffen. Dabei prüft die Krankenkasse, bei der der Antrag auf Befreiung von Zuzahlung zuerst gestellt wird, diesen Antrag für beide Versicherte. Danach übersendet sie das Ergebnis ihrer Berechnung an ihren Versicherten und eine zusätzliche Ausfertigung des Berechnungsbogens für den Angehörigen, der bei einer anderen Krankenkasse versichert ist, mit dem der Versicherte bzw. dessen

Ehepartner dann den Teilerstattungsbetrag bei der für den Ehepartner zuständigen Krankenkasse anfordern kann. Durch dieses für die Versicherten transparente Verfahren tauschen die Krankenkassen untereinander nur in geringem Umfang Sozialdaten der Versicherten aus. Ich halte dies für datenschutzgerecht.

Nach § 194 Abs. 1a SGB V dürfen Krankenkassen jetzt den Abschluss privater Zusatzversicherungsverträge zwischen Ihren Versicherten und privaten Krankenversicherungsunternehmen vermitteln. Von dieser Möglichkeit haben die meisten der bundesunmittelbaren Krankenkassen Gebrauch gemacht und Kooperationsvereinbarungen mit privaten Krankenversicherungsunternehmen geschlossen. Voraussetzung für den Abschluss einer privaten Zusatzversicherung ist die Mitgliedschaft des Versicherten in der kooperierenden Krankenkasse. Dabei muss deutlich dargestellt werden, dass die gesetzliche Krankenkasse für die private Krankenversicherung lediglich eine Vermittlungstätigkeit wahrnimmt, selbst jedoch nicht Vertragspartner ist. Ich halte deswegen die Aufbewahrung und Speicherung von Durchschlägen bzw. Kopien der privaten Versicherungsverträge durch die Kasse wegen der damit verbundenen Kenntnisnahme von teilweise sensiblen personenbezogenen Daten für nicht erforderlich und für nicht durch § 194 Abs. 1a SGB V gedeckt. Diese Problematik habe ich im Rahmen von Beratungs- und Kontrollbesuchen thematisiert (vgl. Nr. 17.1.10). Die Gespräche mit den Krankenkassen zu diesen klärungsbedürftigen Fragen dauern noch an.

17.1.3 Keine Verwendung der Rentenversicherungsnummer als Krankenversichertennummer

Durch eine intensive Beratung der Spitzenverbände der Krankenkassen konnte bei der Neustrukturierung der Krankenversichertennummer eine datenschutzkonforme Lösung gefunden werden, die das Recht auf informationelle Selbstbestimmung der Versicherten wahrt.

Für die bisherige Krankenversichertennummer hatten die Krankenkassen ein eigenes, nicht auf Daten der Versicherten bezogenes Nummernsystem eingeführt. Aufgrund des im Rahmen des GMG geänderten § 290 SGB V wurde zum 30. Juni 2004 eine Neustrukturierung der Krankenversichertennummer erforderlich. Die neue Krankenversichertennummer soll jetzt aus einem unveränderlichen Teil zur Identifikation des Versicherten bestehen sowie aus einem veränderlichen Teil, der u. a. bundeseinheitliche Angaben zur Kassenzugehörigkeit enthalten soll. Dabei ist es Aufgabe der Spitzenverbänden der Krankenkassen, den Aufbau und das Verfahren der Vergabe der neuen Krankenversichertennummer gemeinsam und einheitlich durch Richtlinien zu regeln.

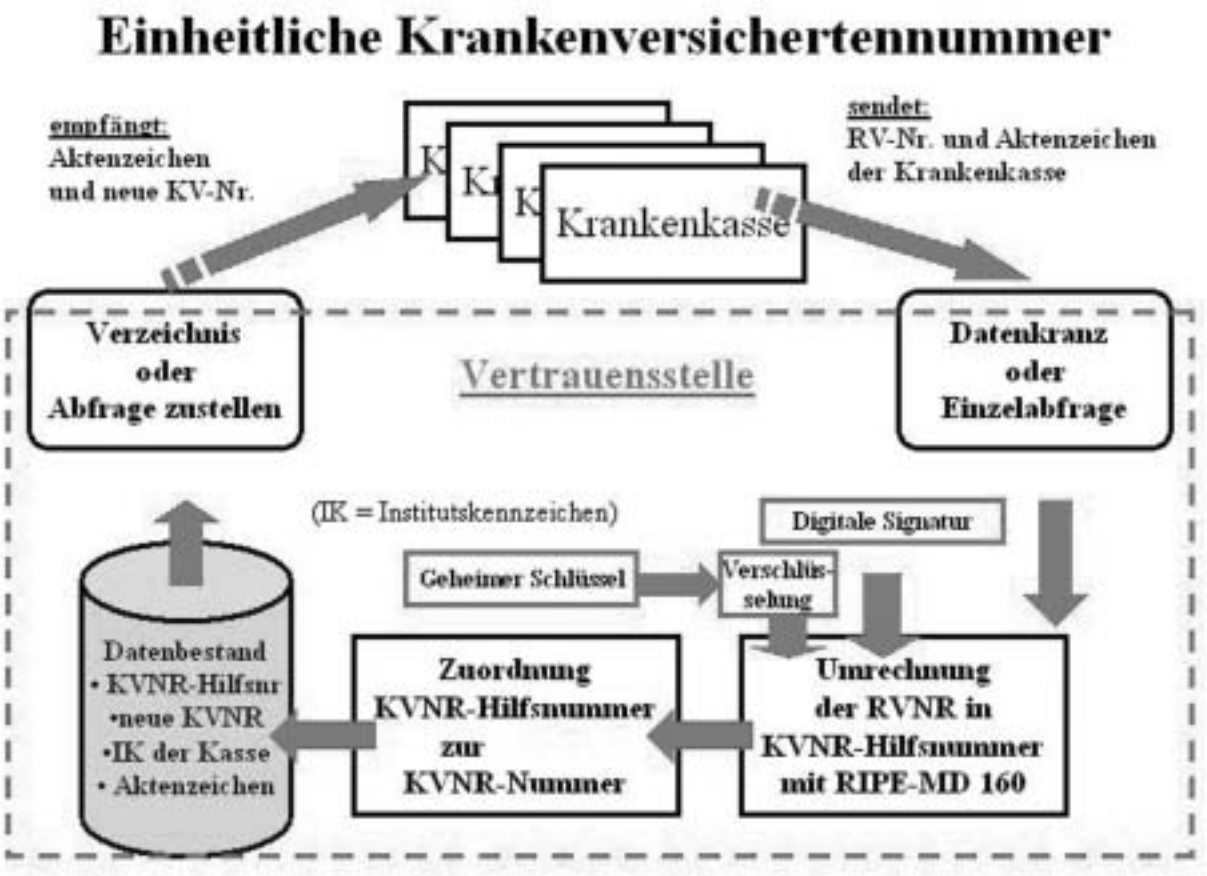
Das ursprünglich von den Spitzenverbänden der Krankenkassen favorisierte Konzept sah eine Verwendung der Rentenversicherungsnummer als Krankenversichertennummer vor. Die Rentenversicherungsnummer stellt ein personenbezogenes Sozialdatum dar und unterliegt dem Sozialgeheimnis, da sie personenbezogene Angaben enthält (Geburtsdatum und Anfangsbuchstaben des Geburtsnamens). Zudem birgt die Verwendung ein und derselben Nummer bei verschiedenen Sozialleistungsträgern erhebliche Risiken. Durch die Möglichkeit der Zusammenführung von Daten, die bei mehreren Sozialleistungsträgern gespeichert sind, könnte diese Nummer den Charakter eines unzulässigen Personenkennzeichens erlangen (vgl. dazu auch die Entschließung der 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder, Kasten zu Nr. 8.2). Deshalb hat der Gesetzgeber in § 290 Abs. 1 Satz 4 SGB V ausdrücklich verboten, die Rentenversicherungsnummer als Krankenversichertennummer zu verwenden. Dies bedeutet zugleich, dass beide Nummern auch nicht voneinander ableitbar sein dürfen. Vor diesem Hintergrund habe ich mich deutlich gegen die Verwendung der Rentenversicherungsnummer als Krankenversichertennummer bzw. als deren Bestandteil ausgesprochen.

Bei Gesprächen mit den Spitzenverbänden der Krankenkassen, dem BMGS und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) konnte ein Verfahren vereinbart werden, das den datenschutzrechtlichen Anforderungen gerecht wird.

In den „Gemeinsamen Richtlinien zur Einführung einer neuen Krankenversichertennummer nach § 290 SGB V“ ist vorgesehen, dass auch die Festlegung der Einzelheiten des technischen und organisatorischen Verfahrens für die Generierung der neuen Krankenversichertennummer und für den Betrieb der Vertrauensstelle mit mir abzustimmen ist, um eine datenschutzkonforme Umsetzung zu gewährleisten.

Das mit mir abgestimmte Konzept sieht Folgendes vor: Die Krankenkassen senden die Rentenversichertennummer (RVNR) und ein Aktenzeichen zur zentralen Vergabestelle (VST). Aus der RVNR wird mit einer Hash-Funktion eine Krankenversicherten-Hilfsnummer (KVNR-Hilfsnummer) berechnet. Die Nutzung des Verfahrens darf nur innerhalb einer Vertrauensstelle erfolgen, um zu verhindern, dass Dritte aus einer bekannten RVNR die Krankenversichertennummer ermitteln können. Daher wird die Prüfziffer zusätzlich mit einem geheimen Schlüssel verschlüsselt. Die Erstellung der KVNR-Hilfsnummer erfolgt in einer gesicherten Umgebung. Die vollständige Anwendung soll vom BSI geprüft und ggf. evaluiert werden. Die Nutzung einer 20-stelligen Nummer ist aus Sicht der Bedarfsträger jedoch nicht praktikabel, da in einigen Verfahren die Krankenversichertennummer manuell auf eine Vorlage übertragen werden muss und dabei leicht Fehler unterlaufen können. Deshalb soll jeder 20-stelligen KVNR-Hilfsnummer nach dem Zufallsprinzip eine zehnstellige Krankenversichertennummer zugeordnet werden. Ich habe diesem Verfahren nur unter der Bedingung zugestimmt, dass aus einer Krankenversichertennummer nicht auf andere gültige Nummern geschlossen werden kann und nur in der VST die Krankenversichertennummer und KVNR-Hilfsnummer zusammen gespeichert werden (vgl. Abbildung zu Nr. 17.1.3).

Abbildung 6 (zu Nr. 17.1.3)



Durch dieses Verfahren wird erreicht, dass die neue Krankenversichertennummer anders als die RVNR keine persönlichen Angaben des Betroffenen enthält. In der Datenbank der VST werden nur die Krankenversichertennummer, die KVNR-Hilfsnummer, das Aktenzeichen der Krankenkasse sowie das Institutionskennzeichen der anfordernden Krankenkasse gespeichert. Durch dieses Verfahren kann die Zahl der über jeden Versicherten in der VST der Krankenversichertennummer gespeicherten notwendigen Daten erheblich reduziert werden. Ein aus meiner Sicht gutes Ergebnis, das zudem noch wirtschaftlich ist, da es der VST die Feststellung der Identität des Versicherten, die Organisation zur Vermeidung von Dubletten und die fortwährende Pflege der Versichertendaten erspart.

Um den besonderen Schutz der Sozialdaten zu gewährleisten, halte ich noch folgende gesetzliche Änderungen für notwendig:

– Festlegung, dass aus der Rentenversicherungsnummer durch ein geeignetes Verfahren der unveränderbare Teil der Krankenversichertennummer gebildet werden darf (ohne dass von der Krankenversichertennummer Rückschlüsse auf die Rentenversicherungsnummer gezogen werden können).

– Festlegung, dass für (noch) nicht rentenversicherungspflichtige Krankenversicherte eine Rentenversicherungsnummer gebildet wird.

– Festlegung, dass die Vertrauensstelle eine von den Krankenkassen und ihren Verbänden unabhängige Stelle sein muss, die dem Sozialgeheimnis unterliegt.

Diese Regelungen sollen nach Auskunft des BMGS noch in das SGB V eingefügt werden.

17.1.4 Disease-Management-Programme

Bei den sog. Disease-Management-Programmen für chronisch Kranke erfolgt die Verarbeitung sensibler Behandlungsdaten durch unabhängige Arbeitsgemeinschaften. Diese dürfen ab 2005 private Dritte mit der Datenverarbeitung beauftragen.

Die Einführung von strukturierten Behandlungsprogrammen, den sogenannten Disease-Management-Programmen (DMP), ist weiterhin ein Thema (vgl. 19. TB

Nr. 24.1.2). Mit dieser besonderen medizinischen Versorgungsform soll der Behandlungsablauf und die Qualität der medizinischen Versorgung chronisch Kranker optimiert werden. Dabei werden verbindliche und aufeinander abgestimmte Behandlungsprozesse festgelegt. Bisher wurden für die Krankheiten Diabetes mellitus Typ 1 und Typ 2, Brustkrebs und koronare Herzkrankheit Behandlungsleitlinien für strukturierte Behandlungsprogramme in der Risikostruktur-Ausgleichsverordnung (RSAV) festgelegt.

Im Rahmen der DMP, an denen die Versicherten auf freiwilliger Basis teilnehmen können, werden auch medizinische Dokumentationen erstellt. Diese Dokumentationsbögen sollen gemäß § 28f Abs. 2 Nr. 1 RSAV an eine selbständige Arbeitsgemeinschaft nach § 219 Abs. 2 SGB V gehen, die diese auf Vollständigkeit und Plausibilität prüfen und pseudonymisieren soll, bevor sie an die Kassenärztlichen Vereinigungen und an die gemeinsame Einrichtung für Zwecke der Qualitätssicherung und der Evaluation weitergeleitet werden. Da die DMP-Arbeitsgemeinschaften jedoch personell und technisch nicht ausreichend ausgestattet sind, um die entsprechende Datenverarbeitung selbst zu erledigen, haben sie diese zunehmend im Wege der Datenverarbeitung im Auftrag auf dritte (private) Stellen übertragen.

Diese Praxis hielt ich für problematisch, da gemäß § 80 Abs. 5 Nr. 2 SGB X die Datenverarbeitung im Auftrag durch private Dritte nicht den gesamten Datenbestand eines Auftraggebers umfassen darf. Um eine praxis- und datenschutzgerechte Lösung zu finden, habe ich mich beim BMGS und beim BVA für eine entsprechende Rechtsgrundlage eingesetzt. Als Lösungsmöglichkeit habe ich eine Ausnahmeregelung zu § 80 Abs. 5 Nr. 2 SGB X vorgeschlagen. Um die datenschutzrechtlichen Anforderungen bei der Verarbeitung dieser sensiblen Gesundheitsdaten beim Auftragnehmer sicherzustellen und eine effektive datenschutzrechtliche Kontrolle zu ermöglichen, soll eine schriftliche Anzeigepflicht der DMP-Arbeitgemeinschaft gegenüber dem zuständigen LfD vorgesehen werden, damit dieser rechtzeitig die Möglichkeit erhält, auf die Einhaltung der für die Datenverarbeitung im Auftrag geltenden Vorgaben des § 80 Abs. 1 bis 5 SGB X hinzuwirken. Dabei kann er auch von der DMP-Arbeitsgemeinschaft verlangen, in dem Vertrag mit dem Auftragnehmer eine Klausel zu vereinbaren, mit der sich dieser der Kontrollbefugnis des für die datenschutzrechtliche Kontrolle der DMP-Arbeitsgemeinschaft zuständigen LfD unterwirft.

Weil bei der Beauftragung eines privaten Dritten durch eine öffentliche Stelle die datenschutzrechtliche Kontrolle bei verschiedenen Datenschutzkontrollinstanzen liegen kann, soll außerdem eine entsprechende Zusammenarbeitsklausel eingefügt werden.

Die Regelung wird als neuer Absatz 6 in § 137f SGB V eingefügt und voraussichtlich Anfang 2005 in Kraft treten.

Des weiteren wurde im Berichtszeitraum eine Änderung des Unterschriftsverfahrens bei den Dokumentationsbögen diskutiert. Nach § 28f Abs. 2 Nr. 3 RSAV musste der an dem DMP teilnehmende Versicherte in jede einzelne Übermittlung des Kurzdatensatzes an die Krankenkasse gesondert schriftlich einwilligen. Diese Regelung, die ursprünglich von der Ärzteschaft selbst gefordert worden war, wurde von dieser nun als zu aufwändig und bürokratisch bewertet. Deshalb schlug das BMGS vor, nur noch eine einmalige Einwilligung des Versicherten bei der Einschreibung in das DMP-Programm vorzusehen. Hierdurch könne sowohl das Problem behoben werden, dass eine erneute Einwilligung erforderlich ist, wenn lediglich Fehler in der Dokumentation durch den Arzt korrigiert werden müssen. Ferner soll die Einführung einer EDV-gestützten Dokumentation erleichtert werden.

Gegen diese Änderung bestehen keine datenschutzrechtlichen Bedenken, denn es handelt sich bei den Daten der Dokumentationsbögen um Befunddaten, die nach Art und Umfang vorher festgelegt sind und damit vom Versicherten im vorhinein konkretisiert werden können. Allerdings muss der Versicherte vorher über die Inhalte des jeweiligen DMP und insbesondere darüber informiert werden, dass Befunddaten auf Grundlage der Dokumentationsbögen an die Krankenkassen übermittelt und von diesen zur Betreuung des Versicherten verarbeitet und genutzt werden. Diese Information muss vom Versicherten schriftlich bestätigt werden. In diesem Zusammenhang waren auch die für die DMP verwendeten Teilnahmeerklärungen sowie das Merkblatt zum Datenschutz zu überarbeiten. Auch Versicherte, die bereits an DMP teilnehmen, müssten über die Änderungen im Verfahrensablauf informiert werden. Meine datenschutzrechtlichen Hinweise wurden in den entsprechenden Änderungen des § 28d Abs. 1 Nr. 2 und 3 RSAV und des § 28f Abs. 2 Nr. 3 RSAV berücksichtigt.

17.1.5 Krankenhausentlassungsberichte

Die Thematik der Krankenhausentlassungsberichte ist in der Praxis immer noch ein Problem. Nach wie vor lassen sich Krankenkassen diese sensiblen Gesundheitsdaten zu Unrecht übermitteln.

Auch im aktuellen Berichtszeitraum hat mich die Problematik der Übermittlung von Krankenhausentlassungsberichten weiter beschäftigt. Bereits in der Vergangenheit (vgl. 18. TB Nr. 21.3; 19. TB Nr. 24.1.4) hatte ich mich hiermit ausführlich auseinandergesetzt. Beratungs- und Kontrollbesuche bei Krankenkassen (vgl. Nr. 17.1.10) sowie entsprechende Bürgereingaben und Anfragen von Ärzten aber zeigen, dass einige Krankenkassen nach wie vor auf Grundlage von Einwilligungserklärungen ihrer Versicherten für sich Krankenhausentlassungsberichte sowie andere ärztliche Berichte und Behandlungsunterlagen anfordern und diese in ihren Akten speichern. Diese Praxis halte ich nach wie vor für unzulässig. Des weiteren musste ich feststellen, dass die Anforderung von Krankenhausentlassungsberichten durch die Krankenkassen, um diese Unterlagen dann an ihren Medizinischen Dienst

(MDK) weiterzuleiten, in der Praxis häufig nicht datenschutzkonform durchgeführt wird: Dieses Verfahren hatte ich unter der Voraussetzung akzeptiert, dass die entsprechenden, zur Weiterleitung an den MDK angeforderten Unterlagen nur in einem verschlossenen, mit der Aufschrift „Ärztliche Unterlagen – nur vom MDK zu öffnen“ versehenen Umschlag über die Krankenkasse an den MDK übermittelt werden dürfen (vgl. 18. TB Nr. 21.3). Diese datenschutzrechtlichen Vorgaben werden in der Praxis jedoch oft nicht beachtet, da die Krankenkassen die entsprechenden Unterlagen unzulässigerweise offen erhalten und einsehen können.

17.1.6 Verarbeitung medizinischer Daten bei der häuslichen Krankenpflege durch die Kassen

Für die Prüfung der Leistungsvoraussetzungen von häuslicher Krankenpflege erheben Krankenkassen Gesundheitsdaten, die unter die ärztliche Schweigepflicht fallen, weil ihnen entsprechende Aufträge an den MDK offenbar zu aufwändig sind.

Bei Beratungs- und Kontrollbesuchen habe ich mich bei mehreren Krankenkassen (vgl. Nr. 17.1.10) über das dort praktizierte Verfahren bei der Bearbeitung der häuslichen Krankenpflege (HKP) informiert und dabei festgestellt:

Die behandelnden Ärzte müssen auf einem Verordnungsformular gegenüber der Krankenkasse bestimmte ärztliche Angaben machen, damit diese ihre Leistungspflicht prüfen kann. Nach Auskunft der zuständigen Mitarbeiter sind die ärztlichen Verordnungen jedoch häufig unvollständig ausgefüllt, so dass die für die Prüfung erforderlichen Angaben fehlen. Deswegen klären die Kassen ergänzende Fragen häufig direkt auf telefonischem Wege mit dem behandelnden Arzt oder holen ergänzende Stellungnahmen des Pflegedienstes ein.

In einzelnen HKP-Akten fanden sich u. a. „Pflegeplanungsbögen“ mit sehr detaillierten Angaben zu Medikamentengaben, pflegerischen Leistungen und weiteren Gesundheitsdaten, teilweise sogar Wundprotokolle mit Fotografien der Wunden pflegebedürftiger Menschen, die über den Umfang der nach der HKP-Verordnung anzugebenden Diagnose- und Gesundheitsdaten bei weitem hinausgingen.

Ich halte diese bei der Krankenkasse gespeicherten Angaben für deren Aufgabenerfüllung nach § 37 SGB V nicht für erforderlich. Im Rahmen der HKP entscheidet die Krankenkasse nach Richtlinien über die Verordnung häuslicher Behandlungspflege. Ein Vergleich der Verordnung von Leistungen der HKP mit der Verordnung anderer Leistungen nach dem SGB V zeigt, dass es sich bei der HKP um eine normale Leistung im Rahmen des SGB V handelt, die rechtlich entsprechend zu behandeln ist, insbesondere mit der Einschaltung des MDK nach § 275 SGB V. Eine Krankenkasse darf nur auf Grundlage der ihr zulässigerweise vorliegenden Unterlagen über den Leistungsanspruch der Versicherten entscheiden. Eine Befugnis, für diese Entscheidung weitere Sozialdaten beim Versicherten oder beim Leistungserbringer zu erheben, liegt darin nicht. Hat die Krankenkasse Zweifel, ob die geltend gemachte Leistung tatsächlich von ihr zu erbringen ist, hat sie gemäß § 275 Abs. 1 Nr. 1 SGB V den MDK einzuschalten.

Da der Arzt für die Verordnung und die damit verbundene Übermittlung von Gesundheitsdaten an die Krankenkasse verantwortlich und insoweit zur Offenlegung befugt ist, halte ich lediglich eine Nachfrage der Kasse beim verordnenden Arzt für zulässig, während eine Nachfrage bei dem betroffenen Pflegedienst selbst m. E. nicht dem datenschutzrechtlichen Verhältnismäßigkeitsprinzip entspricht.

Den Krankenkassen habe ich empfohlen, die nicht benötigten Unterlagen aus den Akten zu entfernen. Ich gehe davon aus, dass die Krankenkassen das Ergebnis meiner Prüfung auch zum Anlass nehmen, das geschilderte Verfahren grundsätzlich unter datenschutzrechtlichen Gesichtspunkten zu prüfen und ggf. neu zu gestalten.

17.1.7 Laborärztliche Untersuchungen

Die Forderung nach einer Pseudonymisierung von Patientendaten bei laborärztlichen Untersuchungen konnte aus rechtlichen Gründen noch nicht umgesetzt werden.

Die Pseudonymisierung von Patientendaten bei laborärztlichen Untersuchungen (vgl. 19. TB Nr. 24.1.5) ist eine seit längerem von den Datenschutzbeauftragten des Bundes und der Länder erhobene Forderung, in der sie auch vom Düsseldorfer Kreis unterstützt werden. Auch die Bundesregierung hat sich in ihrer Stellungnahme zu meinem 19. Tätigkeitsbericht dieser Bewertung angeschlossen; auch nach ihrer Auffassung sollte bei laborärztlichen Untersuchungen eine Offenlegung der Identität der Versicherten vermieden werden.

Problematisch in diesem Zusammenhang ist jedoch u. a. § 295 Abs. 1 Nr. 3 SGB V, der die Aufzeichnungs- und Übermittlungspflichten von Vertragsärzten und ärztlich geleiteten Einrichtungen gegenüber den Krankenkassen regelt. Hier ist vorgeschrieben, dass Vertragsärzte und ärztlich geleitete Einrichtungen – damit auch Laborärzte – in den Abrechnungsunterlagen die Angaben nach § 291 Abs. 2 Nr. 1 bis 10 SGB V anzugeben haben, also u. a. Familienname und Vorname des Versicherten, Geburtsdatum, Geschlecht, Anschrift sowie Krankenversichertennummer. Da die Laborärzte damit gesetzlich verpflichtet sind, personenbezogene Daten zu erheben und zu übermitteln, kann die datenschutzrechtliche Forderung nach einer Pseudonymisierung von Laboraufträgen derzeit nicht wirklich umgesetzt werden.

Ich halte jedoch nach wie vor eine Pseudonymisierung von Laboraufträgen für wünschenswert und werde mich daher weiterhin für entsprechende Lösungen einsetzen.

17.1.8 Einführung eines flächendeckenden Mammographie-Screenings

Für das flächendeckende Mammographie-Screening konnte eine datenschutzfreundliche Konzeption erreicht werden, jedoch besteht auf Landesebene noch Regelungsbedarf.

Das Programm zur Brustkrebsfrüherkennung wird derzeit grundlegend umgestaltet. Im Zentrum steht dabei eine möglichst flächendeckende regelmäßige Ultraschalluntersuchung der Brust (Mammographie) aller Frauen zwischen 50 und 69 Jahren, da in dieser Altersgruppe ein besonders hohes Brustkrebsrisiko besteht. Vor Einführung des Mammographie-Screenings besteht jedoch auf Landesebene noch weiterer Regelungsbedarf.

Die in den Richtlinien vorgesehene Konzeption des Mammographie-Screenings wurde in enger Abstimmung mit mir und einer eigens hierfür gebildeten Arbeitsgruppe der Datenschutzbeauftragten des Bundes und der Länder entwickelt. Bedauerlicherweise musste hierfür erst das BMGS die Krebsfrüherkennungsrichtlinien beanstanden, insbesondere wegen der von mir dargelegten erheblichen datenschutzrechtlichen Bedenken.

In dem nunmehr in Kraft getretenen Konzept sind insbesondere die folgenden Aspekte datenschutzrechtlich bedeutsam:

– Einladungsverfahren

  Die Einladung der anspruchsberechtigten Frauen (50- bis 70jährige) zum Mammographie-Screening soll durch eine öffentliche Stelle i. S. d. § 18 Abs. 4 Melderechtsrahmengesetz (MRRG) erfolgen, die sog. Zentrale Stelle. Diese wird „durch die Kassenärztliche Vereinigung und die zuständigen Verbände der Krankenkassen auf Landesebene in Abstimmung mit den zuständigen Landesbehörden unter Berücksichtigung der landesrechtlichen Bestimmungen“ errichtet. Für die Einladung der Frauen soll die Zentrale Stelle vom Melderegister auf landesrechtlicher Basis die erforderlichen Daten erhalten. Es liegt jetzt bei den Ländern, die noch fehlenden Rechtsgrundlagen zu schaffen, auch für die ggf. erforderliche Aufgabenzuweisung an die Zentrale Stelle.

  Bei der Zentralen Stelle werden aus den vom Melderegister übermittelten Daten drei Datensätze erzeugt:

  – Für jede anspruchsberechtigte Frau eine lebenslange Screening-Identifikationsnummer (Screening-ID), die nicht auf die Identität der Frau zurückgeführt werden kann.

  – Eine ebenfalls nicht reidentifizierbare Kontrollnummer für den späteren Abgleich mit diesen Krebsregistern. Die Kontrollnummer wird zusammen mit der Screening-ID gespeichert.

  – Eine Einladungsliste, die Vorname, Familienname und Screening-ID enthält.

  Anschließend werden die von den Meldebehörden übermittelten Daten gelöscht.

  Die Einladungsliste darf nur für das Einladungsverfahren verwendet werden und wird danach – sowohl bei der Zentralen Stelle als auch bei der Screening-Einheit, bei der die Untersuchungen durchgeführt werden – gelöscht. Bei der Zentralen Stelle werden damit dauerhaft keine personenbezogenen Daten gespeichert, sondern nur anonymisierte Daten zu Evaluationszwecken.

– Qualitätssicherung

  Um einen hohen Qualitätsstandard der Untersuchungen zu gewährleisten, sind umfangreiche Qualitätssicherungsmaßnahmen auf Basis von anonymisierten und aggregierten Daten vorgesehen. Nur für interne Qualitätssicherungsmaßnahmen innerhalb einer Screening-Einheit dürfen personenbezogene Daten verarbeitet werden. Für die Überprüfung der diagnostischen Bildqualität der Röntgenaufnahmen wird von diesen der Vor- und Nachname sowie das Geburtsdatum abgetrennt; nur die Screening-ID bleibt auf der Röntgenaufnahme erhalten.

– Evaluation

  Durch umfassende Evaluationsmaßnahmen soll festgestellt werden, ob das flächendeckende Mammographie-Screening die angestrebten Ziele (u. a. Verbesserung der Brustkrebserkennungsrate und Verringerung der Brustkrebsmortalität) erreicht. Auch die Evaluation erfolgt – außer für die Feststellung von falsch-negativen Diagnosen – auf Basis von anonymisierten und aggregierten Daten.

  Für die Prüfung, ob in der Zeit zwischen zwei Screening-Mammographien Brustkrebs aufgetreten ist, der früher hätte entdeckt werden können (sog. falsch-negative Diagnosen), reichen anonymisierte und aggregierte Daten nicht aus. Hierfür ist ein Abgleich mit den Krebsregistern erforderlich, für den die Kontrollnummern der Frauen (und nur diese), die an dem Screening teilgenommen haben, übermittelt werden. Diese werden mit den im Krebsregister gespeicherten Kontrollnummern abgeglichen. Übereinstimmungen werden vom Krebsregister an die Zentrale Stelle übermittelt. Diese teilt dann der jeweiligen Screening-Einheit sowie dem zuständigen Referenzzentrum die jeweilige Screening-ID mit. Die Screening-Einheit bittet daraufhin die betreffende Frau um Einwilligung zur Übermittlung ihrer medizinischen Daten an das Referenzzentrum, damit dort eine Prüfung erfolgen kann, ob es sich um eine falsch-negative Diagnose gehandelt hat.

  Datenschutzrechtlich relevant ist in diesem Zusammenhang, dass die betroffenen Frauen in der Screening-Einheit anhand der Screening-ID identifiziert werden (müssen), damit sie um ihre Einwilligung für die Übermittlung der medizinischen Daten an das Referenzzentrum gebeten werden können. Damit erfolgt die Datenübermittlung (der Kontrollnummer) von dem jeweiligen Krebsregister im Ergebnis nicht anonym und wäre nach den Krebsregistergesetzen der Länder unzulässig. Durch entsprechende Gesetzesänderungen wird diese Datenübermittlung jedoch legitimiert werden, verbunden mit einer engen Zweckbindung.

Da ein Abgleich mit den Krebsregistern erstmals im Jahre 2007 erfolgt, ist diese auch datenschutzrechtlich vertretbare Lösung auch praktisch umsetzbar.

17.1.9 Schweigepflichtentbindungserklärung in der privaten Krankenversicherung

Die Schweigepflichtentbindungserklärung, die ein Versicherungsnehmer bei Abschluss eines privaten Krankenversicherungsvertrags abzugeben hat, muss an die Anforderungen an eine wirksame Einwilligungserklärung nach § 4a BDSG angepasst werden.

Anders als in der gesetzlichen Krankenversicherung, bei der der Datenfluss zwischen Ärzten und Krankenkasse durch Gesetz geregelt ist, bedarf es für private Krankenversicherungen einer wirksamen Einwilligungserklärung des Patienten, damit Ärzte Patienteninformationen offenbaren dürfen. Daher fordern private Krankenversicherungen bei Abschluss eines Versicherungsvertrages von ihren Kundinnen und Kunden routinemäßig die Unterschrift unter eine umfangreiche Schweigepflichtentbindungserklärung, die auf einem Muster aus dem Jahre 1989 beruht. Dabei erklären sich die Versicherten damit einverstanden, dass die private Krankenversicherung ihre Patientendaten abfragen darf:

– zur Beurteilung eines möglichen Versicherungsrisikos für einen Zeitraum von fünf Jahren ab Antragstellung bei allen Ärzten, Zahnärzten usw., bei denen sich der Antragsteller in den letzten zehn Jahren in Behandlung befand, und

– für die Prüfung der Leistungspflicht unbefristet ab Antragstellung bei den Ärzten, Zahnärzten usw.

Nach meiner Auffassung sind solche pauschalen, lange zurückliegenden Erklärungen keine ausreichende rechtliche Grundlage für die Übermittlung von Gesundheitsdaten (vgl. 19. TB Nr. 1.13).

Gemeinsam mit den anderen Aufsichtsbehörden, die im Düsseldorfer Kreis zusammenarbeiten, habe ich deswegen den Gesamtverband der Versicherungswirtschaft darauf hingewiesen, dass die seit 15 Jahren verwendeten Erklärungen nicht mehr der geltenden Rechtslage entsprechen. Seit der Umsetzung der Europäischen Datenschutzrichtlinie im BDSG 2001 sei für die Übermittlung von (Gesundheits-) Daten eine hinreichend bestimmte Erklärung notwendig. Der Versicherte müsse zum Zeitpunkt seiner Unterschrift erkennen können, welche seiner Patientendaten wann von welchen Ärzten zu welchem Zweck an die Versicherung übermittelt werden sollen.

Aus der derzeit verwendeten Klausel zur Risikobeurteilung ist dem Versicherten nicht ersichtlich, wann von der Erklärung Gebrauch gemacht werden soll und welche Patientendaten angefordert werden. Weil er somit die Reichweite seiner Erklärung nicht erkennen kann, entspricht diese nicht den Voraussetzungen für eine wirksame Einwilligung nach § 4a BDSG. Zudem bestehen Zweifel, ob der zeitliche Umfang der Datenerhebungsbefugnis (zehn Jahre vor und fünf Jahre nach Vertragsbeginn) tatsächlich notwendig ist, so dass die Klausel auch dem datenschutzrechtlichen Grundsatz der Erforderlichkeit widersprechen könnte.

Bei der Erklärung zur Leistungsprüfung können die Versicherten zum Zeitpunkt des Vertragsschlusses nicht erkennen, welche Patientendaten zukünftig anfallen und ob sie damit einverstanden sind, dass diese ohne weitere Nachfrage an ein Versicherungsunternehmen weitergegeben werden. Auch ist ihnen zu diesem Zeitpunkt weder der Name des Arztes noch der Anlass für künftige ärztliche Behandlungen bekannt. Damit bezieht sich seine Erklärung nicht auf konkrete Gesundheitsdaten, was jedoch für eine wirksame Einwilligung erforderlich wäre, und entspricht wegen fehlender Bestimmtheit nicht den Anforderungen des § 4a BDSG.

Das Bemühen, das bisherige Verfahren zu verändern, um mehr Transparenz und eine Stärkung der Patientenrechte zu erreichen, hatte bislang jedoch keinen Erfolg. Die Versicherungswirtschaft war nicht bereit, die Klauseln und das Verfahren den datenschutzrechtlichen Anforderungen anzupassen. Ärzte gehen bei einer auf eine pauschale Schweigepflichtentbindungserklärung gestützten Übermittlung von Patientendaten an private Krankenversicherungen das Risiko ein, ihre ärztliche Schweigepflicht zu verletzen, was strafrechtlich sanktioniert ist.

Im Hinblick auf die Sensibilität der medizinischen Daten halte ich es für geboten, dass die Versicherer für jeden Behandlungsfall eine Schweigepflichtentbindungserklärung beim Patienten einholen. Auf diese Weise hat der Versicherte den Überblick, welche seiner Gesundheitsdaten zu welcher Zeit weitergegeben werden. Auch der Düsseldorfer Kreis hat in seiner Sitzung im Mai 2004 die Ansicht vertreten, dass für jede Rückfrage von Krankenversicherungen bei Ärzten, anderen Angehörigen von Heilberufen oder Krankenanstalten wegen der Erstattung von Rechnungen eine gesonderte Einwilligung erforderlich ist. Diese Auffassung wurde der Bundesärztekammer und der Bundeszahnärztekammer mitgeteilt.

17.1.10 Feststellungen aus Datenschutzkontrollen

Im Zusammenhang mit dem GMG habe ich datenschutzrechtliche Kontroll- und Beratungsbesuche bei zwei großen bundesunmittelbaren Krankenkassen durchgeführt.

Die Kontrolle von zwei großen bundesunmittelbaren Krankenkassen sollte Aufschluss über Fragen bringen, die mit dem GMG in Zusammenhang stehen. Hierbei habe ich mir jeweils eine Geschäftsstelle und eine Servicestelle dieser Kassen angesehen.

Themenbezogene Schwerpunkte meiner Besuche waren das Arbeitsunfähigkeits-Fallmanagement, die Disease-Management-Programme, die häusliche Krankenpflege, die Vermittlung privater Zusatzversicherungen durch

Krankenkassen, das Verfahren der Befreiung von Zuzahlungen (Belastungsgrenze), die sog. Bonusprogramme der Krankenkassen sowie die Übernahme von Fahrtkosten.

Meine Prüfergebnisse, insbesondere zu nicht datenschutzkonformen Verfahrensweisen, sowie weitere datenschutzrechtliche Hinweise und Empfehlungen habe ich beiden Krankenkassen mitgeteilt. Sie betrafen z. B. die bei einer Krankenkasse gespeicherten Durchschläge oder Kopien von nach § 194 Abs. 1a SGB V vermittelten privaten Zusatzversicherungsverträgen mit teilweise sensiblen personenbezogenen Daten (vgl. Nr. 17.1.2), aber auch bei beiden Kassen vorgefundene Krankenhausentlassungsberichte, Behandlungsunterlagen oder sonstige ärztliche Berichte, die diese auf Grundlage von unzulässigen Einwilligungserklärungen der Versicherten angefordert und gespeichert hatten (vgl. Nr. 17.1.5).

In einigen Fällen habe ich detaillierten Handlungsbedarf aufgezeigt, um dort in Zukunft eine datenschutzkonforme Verarbeitung der Sozialdaten der Versicherten sicherzustellen. Dieser bezog sich bei beiden Krankenkassen z. B. auf Sozialdaten (Diagnosen zu Arbeitsunfähigkeitszeiten), die längst hätten gelöscht sein müssen, und bei einer Kasse auf gespeicherte Gesprächs-/Telefonvermerke mit subjektiven und Versicherte negativ-kennzeichnenden und für die Aufgabenerfüllung nicht erforderlichen Inhalten, aber auch auf die sehr problematische Übermittlung sensibler Sozialdaten – auch mit medizinischen Inhalten – an Dritte per Telefax. Die Gespräche mit beiden Krankenkassen dauern noch an.

17.2 Pflegeversicherung

17.2.1 Pflegedokumentation – Objekt der Begierde

Die in der Pflegedokumentation enthaltenen Daten (z. B. Anamnese- und Diagnosedaten) wecken nach wie vor großes Interesse bei den Pflege- und Krankenkassen.

Die Frage, ob die Einsichtnahme in Pflegedokumentationen durch Pflegekassen zulässig ist, hat mich weiterhin beschäftigt (vgl. auch 19. TB Nr. 24.2.2). Meine Auffassung, die Kenntnis vom Inhalt der Pflegedokumentation sei für die Aufgabenerfüllung (z. B. Leistungsprüfung und -abrechnung) der Pflegekasse nicht erforderlich und die Erhebung dieser Daten damit unzulässig, hatte bei den Kranken- und Pflegekassen zunächst hohe Wellen geschlagen.

Vor diesem Hintergrund hat das BMGS diesen gesamten Themenkomplex unter meiner Beteiligung mit den Spitzenverbänden der Kranken- und Pflegekassen diskutiert und in einem Rundschreiben auch die Berufs- und Wohlfahrtsverbände im Bereich der Pflege über die Ergebnisse informiert (vgl. Kasten zu Nr. 17.2.1).

Dabei wurde Einvernehmen erzielt, dass nur im Rahmen des § 114 Abs. 6 Satz 1 SGB XI ein Einsichtsrecht des Vertreters der Pflegekasse in die Pflegedokumentation besteht, wenn dieser im Rahmen einer örtlichen Prüfung der Abrechnungen nach § 114 Abs. 1 bis 3 SGB XI hinzugezogen wird. Für eine Weitergabe der Pflegedokumentation an die Pflegekassen besteht weder eine gesetzliche Grundlage, noch ein Bedarf, weil der Inhalt der Abrechnungsunterlagen in § 105 SGB XI abschließend geregelt ist und die Pflegedokumentation danach keine Abrechnungsunterlage darstellt. Es bestand auch Einvernehmen darüber, dass über § 114 Abs. 6 Satz 1 SGB XI hinaus weder eine Verpflichtung noch eine Berechtigung der Pflegeeinrichtung besteht, die Pflegedokumentation den Pflegekassen zu überlassen.

Wie ich inzwischen erfahren habe, interpretieren einige Pflege- bzw. Krankenkassen das o. g. Rundschreiben des BMGS fälschlicherweise so, dass sie nunmehr berechtigt seien, Abrechnungsprüfungen unter Einbeziehung der Pflegedokumentation durchzuführen. Darüber hinaus wollen einige Pflegekassen einen sog. „Beratungsservice“ anbieten, bei dem nach meinen Informationen ebenfalls eine Einsichtnahme in die Pflegedokumentation erfolgen soll.

Um einer Fehlinterpretation des Schreibens des BMGS vorzubeugen, habe ich gegenüber den Spitzenverbänden der Kranken- und Pflegekassen nochmals meine im 19. Tätigkeitsbericht zum Einsichtsrecht der Pflegekassen in die Pflegedokumentation dargelegte Auffassung bekräftigt. Eine Rechtsgrundlage für Pflegekassen, Pflegedokumentationen für ihre Abrechnungsprüfung einzusehen bzw. anzufordern, stellt § 114 Abs. 6 Satz 1 SGB XI gerade nicht dar. Auch § 284 Abs. 1 Nr. 8 SGB V kann von den Kranken- und Pflegekassen nicht als gesetzliche Grundlage herangezogen werden, da es sich hierbei um eine Vorschrift aus dem Recht der Gesetzlichen Krankenversicherung handelt, die nicht auf das Recht der Pflegeversicherung übertragen werden kann. Weiter habe ich klargestellt, dass die örtliche Prüfung entsprechend dem eindeutigen Wortlaut des § 114 Abs. 1 bis 3 SGB XI allein dem MDK bzw. den von den Landesverbänden der Pflegekassen bestellten (unabhängigen) Sachverständigen obliegt. Für eine Qualitätsprüfung durch die Pflegekassen selbst verbleibt kein Raum.

Sollten auf Landesebene in vertraglichen Vereinbarungen zwischen Pflegekassen und Pflegediensten bzw. deren Landesverbänden entsprechende Befugnisse der Pflegekassen zur Einsichtnahme in die Pflegedokumentation vorgesehen sein, die über den oben aufgezeigten Umfang hinausgehen, wäre dies, auch vor dem Hintergrund des besonderen Schutzes der Persönlichkeitsrechte pflegebedürftiger Menschen (§ 84a Abs. 1 SGB X), eine unzulässige Umgehung der eindeutigen gesetzlichen Regelungen. Die Erhebung, Verarbeitung oder Nutzung personenbezogener Daten könnte deshalb auf solche Verträge nicht gestützt werden.

Kasten zu Nr. 17.2.1

Rundschreiben des Bundesministeriums für Gesundheit und soziale Sicherung an die Spitzenverbände der Kranken- und Pflegekassen vom 9. Januar 2004 Az.: 231 – 43 576/BMG/Abt. 2/33

Einsichtsrecht der Pflegekassen in die Pflegedokumentation

Ich komme zurück auf unsere gemeinsame Besprechung am 20.11.2003 zum 19. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz. In dieser Besprechung wurden die gegenwärtige Rechtslage und die dem Tätigkeitsbericht in diesem Punkt zugrunde liegenden Grundsätze des Datenschutzes erörtert. Es bestand Einvernehmen, dass auch aus Sicht des Bundesbeauftragten für den Datenschutz keine Bedenken gegen die Einsichtnahme eines gemäß § 114 Abs. 6 Satz 1 SGB XI beteiligten Vertreters der betroffenen Pflegekasse in die Pflegedokumentation besteht, sofern der Vertreter der Pflegekasse im Rahmen einer örtlichen Prüfung nach § 114 Abs. 1 bis 3 SGB XI (Einzelproben, Stichproben- und vergleichende Prüfung) hinzugezogen wird, um – wie dies in der Begründung zu dieser Vorschrift ausdrücklich genannt ist – eine wirksame Prüfung der Abrechnungen zu gewährleisten.

Einvernehmen bestand weiterhin, dass darüber hinaus weder eine Verpflichtung noch eine Berechtigung der Pflegeinrichtung besteht, die Pflegedokumentation den Pflegekassen zu offenbaren. Die Pflegedokumentation stellt keine Abrechnungsunterlage i. S. des § 105 SGB XI dar. Der Inhalt der Abrechnungsunterlagen ist in § 105 Abs. 1 SGB XI abschließend geregelt. Insoweit besteht für eine Weitergabe der Pflegdokumentation an die Pflegekassen selbst weder eine rechtliche Grundlage noch ein Bedarf.

17.2.2 Feststellungen aus Datenschutzkontrollen

Zum Einsichtsrecht der Pflegekassen in die Pflegedokumentation pflegebedürftiger Menschen (19. TB Nr. 24.2.2) habe ich mich bei zwei großen Pflegekassen über die Verfahrensabläufe und Vorgehensweisen bei der Gewährung von Leistungen der Sozialen Pflegeversicherung (SGB XI) informiert.

Im Rahmen eines Beratungs- und Kontrollbesuches habe ich in Stichproben Versichertenakten eingesehen, die Unterlagen über den gesamten Verfahrensablauf vom Leistungsantrag über den Prüfauftrag an den Medizinischen Dienst der Krankenversicherung (MDK) bis hin zur Entscheidung der Pflegekasse enthielten. Die in den Akten vorgefundenen Unterlagen waren überwiegend für die Aufgabenerfüllung der Pflegekassen erforderlich. In Einzelfällen wurden von den Pflegebedürftigen selbst oder ihren Angehörigen mit dem Pflegeantrag vorgelegte ärztliche Atteste vorgefunden, die zwar für die Begutachtung durch den MDK, nicht aber für die Entscheidung der Pflegekasse relevant sein konnten. Weil auch die Bearbeiter eine Speicherung dieser Unterlagen nicht für erforderlich hielten, wurden diese noch in Anwesenheit meiner Mitarbeiter vernichtet.

Zu den Arbeitsanweisungen für die Mitarbeiter sowie zur Gestaltung der Vordrucke stehen noch einige Informationen aus. Die Pflegekassen haben jedoch zugesagt, mir die erforderlichen Unterlagen zu überlassen.

18 Rentenversicherung

18.1 Organisationsreform in der gesetzlichen Rentenversicherung

Meine datenschutzrechtlichen Empfehlungen wurden im „Gesetz zur Organisationsreform in der gesetzlichen Rentenversicherung (RVOrgG)“ im Wesentlichen berücksichtigt.

Die Organisation der gesetzlichen Rentenversicherung wird umfassend reformiert. Die Zahl der Bundesträger in der Rentenversicherung wird dabei von vier auf zwei reduziert. Bundesknappschaft, Bahnversicherungsanstalt und Seekasse werden unter dem Namen „Deutsche Rentenversicherung Knappschaft-Bahn-See“ fortgeführt. Der Spitzenverband der gesetzlichen Rentenversicherung (VDR) und die Bundesversicherungsanstalt für Angestellte (BfA) bilden den neuen Bundesträger „Deutsche Rentenversicherung Bund“. Hauptziel des RVOrgG vom 9. Dezember 2004 (BGBl. I S. 3242) ist die Senkung der Verwaltungs- und Verfahrenskosten durch Straffung der Verwaltungsstrukturen.

Mit den Aufgaben des VDR übernimmt die „Deutsche Rentenversicherung Bund“ auch die Datenstelle der Träger der gesetzlichen Rentenversicherung. Die Datenstelle fungiert schon bisher als zentrale Datenannahme- und Verteilerstelle (Vermittlungsstelle) und führt u. a. die sog. Stammsatzdatei mit über 100 Millionen Stammdatensätzen von Versicherten. Mit der Organisationsreform werden ihr weitere Aufgaben übertragen. So wird die Datenstelle die Rentenversicherungsnummer vergeben und damit den zuständigen Träger der Rentenversicherung festlegen. Ferner führt die Datenstelle das Ausgleichsverfahren durch, mit dem der Bestand der Versicherten entsprechend einer gesetzlich vorgesehenen Quote auf die Rentenversicherungsträger verteilt werden soll.

Ich habe empfohlen, das Sozialgeheimnis ausdrücklich durch das Gesetz auf die Datenstelle zu erstrecken. Dem ist in § 35 Abs. 1 Satz 4 SGB I entsprochen worden. Die Datenstelle gilt weiterhin nach § 81 Abs. 3 Satz 3 SGB X als öffentliche Stelle des Bundes.

Bei der Zusammenführung von VDR und BfA unter dem neuen Dach der „Deutschen Rentenversicherung Bund“ war aus meiner Sicht zudem sicherzustellen, dass die Datenbestände, die die „Deutsche Rentenversicherung Bund“ als Träger der Rentenversicherung führt, und die Datenbestände der bisher vom VDR verwalteten Datenstelle der Träger der Rentenversicherung dauerhaft getrennt bleiben. Auch dies hat der Gesetzgeber berücksichtigt.

Weiter wird mit dem RVOrgG die Zuständigkeit für die Auskunfts- und Beratungsstellen der Rentenversicherung vor Ort den Regionalträgern (ehemalige Landesversicherungsanstalten) zugeordnet. Die Grundsätze der Organisation und Aufgabenzuweisung der Auskunfts- und Beratungsstellen nimmt dabei die „Deutsche Rentenversicherung Bund“ wahr.

Die Beratung von Versicherten und Rentnern erfolgt in der gesetzlichen Rentenversicherung bisher schon über ein Netz von Auskunfts- und Beratungsstellen auf Grundlage von Kooperationsvereinbarungen der Rentenversicherungsträger untereinander. Dabei findet eine Auskunft und Beratung nur dann statt, wenn die Versicherten, die in einer Beratungsstelle Informationen erhalten möchte, ihre Berechtigung durch Vorlage eines Ausweispapiers nachweisen. Ehepartner und Bevollmächtigte müssen zudem eine Vollmacht und eine Einwilligungserklärung vorlegen. Im Gesetzgebungsverfahren habe ich die Notwendigkeit der Fortführung dieser bisherigen Praxis deutlich gemacht. Dementsprechend wird in der Begründung des RVOrgG auf die datenschutzrechtlichen Erfordernisse bei der Organisation der Auskunfts- und Beratungsstellen hingewiesen, nach denen u. a. eine Auskunft und Beratung nur nach entsprechender Legitimation der Versicherten erfolgen darf (vgl. Bundestagsdrucksache 15/3654 S. 70). Damit ist weiterhin sichergestellt, dass die dem Sozialgeheimnis unterliegenden Versichertendaten nur den jeweils berechtigten Personen zugänglich gemacht werden.

18.2 Feststellungen aus Datenschutzkontrollen

18.2.1 Kontrolle in der Hauptstelle der BfA

Bei einem im Berichtszeitraum durchgeführten Beratungs- und Kontrollbesuch in einer Leistungsabteilung der Bundesversicherungsanstalt für Angestellte (BfA) konnte ich mich davon überzeugen, dass die Rentenangelegenheiten der Versicherten datenschutzkonform bearbeitet werden.

In den Leistungsabteilungen der BfA werden die Versicherungs- und Rentenangelegenheiten der Versicherten bearbeitet. Neben der Bearbeitung der eigentlichen Rentenanträge umfasst dies etwa auch Kontenklärungen und Rentenauskünfte.

Bei einem Beratungs- und Kontrollbesuch habe ich in verschiedenen Bereichen der BfA (u. a. zentrale Poststelle, Datenein- und -ausgabe in den Servicedezernaten, Sachbearbeitung in einzelnen Teams bzw. an einzelnen Arbeitsplätzen, Registraturen, Archive) den Umgang mit den Versichertendaten geprüft. Dabei konnte ich in der Hauptstelle der BfA und in einer weiteren von mir besuchten großen Berliner Dienststelle der BfA keine wesentlichen datenschutzrechtlichen Mängel feststellen. Dieses positive Ergebnis wurde auch durch die stichprobenartige Einsichtnahme in verschiedene Versichertenakten in beiden Dienststellen der BfA bestätigt.

Während des Besuches konnte ich u. a. feststellen, dass der Zugriff der Mitarbeiter in der Sachbearbeitung auf Versicherten- bzw. Sozialdaten in den entsprechenden Versichertenkonten jeweils auf das zur sachgerechten Aufgabenwahrnehmung erforderliche Maß beschränkt ist. Gleiches gilt für die Dateneingabebereiche, in denen nur den jeweils zuständigen Mitarbeitern ein Zugriff auf die Versichertenkonten zur Wahrnehmung ihrer jeweiligen Aufgaben in dem erforderlichen Umfang gewährt wird. Auch die Abläufe in der zentralen Poststelle der Hauptstelle der BfA und die hierzu bestehenden internen Regelungen der BfA entsprechen den datenschutzrechtlichen Anforderungen.

Verschiedene weitere datenschutzrechtlich relevante Gesichtspunkte konnten noch während meines Besuches gemeinsam mit Vertretern der BfA erörtert und geklärt werden. Angesichts des insgesamt positiven Ergebnisses, bin ich überzeugt, auch die wenigen noch offenen Einzelfragen mit der BfA im weiteren schriftlichen Verfahren abschließend klären zu können.

18.2.2 Kontrolle einer Rehabilitationsklinik der BfA

Bei einem Kontroll- und Beratungsbesuch in einer Rehabilitationsklinik der BfA habe ich die Verarbeitung und Nutzung von Sozialdaten der Patienten und den Umgang mit sonstigen Personal- und Patientendaten geprüft.

Schwerpunkte des Kontroll- und Beratungsbesuches in verschiedenen Bereichen einer Rehabilitationsklinik in der Trägerschaft der BfA waren die Verarbeitung und Nutzung von Sozialdaten der Patienten (insbesondere medizinischer Daten), die Wahrung des Sozialgeheimnisses nach § 35 SGB I, die Umsetzung der Datenschutzrichtlinien für die Reha-Klinikgruppe der BfA (vgl. 19. TB Nr. 25.1) und die Verarbeitung und Nutzung weiterer personenbezogener Daten (Personal-, Patientendaten) im Verwaltungsbereich sowie Fragen zum technischen und organisatorischen Datenschutz.

Insbesondere die Umsetzung der o. a. Datenschutzrichtlinien im medizinischen Bereich hat meinen bei früheren Beratungs- und Kontrollbesuchen gewonnenen positiven Eindruck von den Kliniken in der Trägerschaft der BfA erneut bestätigt. In Einzelfällen festgestellte datenschutzrechtliche Mängel wurden von der BfA abgestellt.

Meine Prüfung der Verarbeitung und Nutzung von sonstigen personenbezogenen Daten der Patienten im Verwaltungsbereich der Klinik, insbesondere von Personal-/Personalaktendaten der in der Klinik Beschäftigten, hat dagegen datenschutzrechtliche Mängel und Verstöße ergeben. Für diesen Bereich habe ich dringenden und grundsätzlichen Handlungsbedarf aufgezeigt und meine Feststellungen eingehend mit der BfA diskutiert. Erfreulicherweise haben meine datenschutzrechtlichen Empfehlungen und Hinweise bereits während der Kontrolle zu ersten Verbesserungen vor Ort geführt.

Weil mir die BfA darüber hinaus innerhalb kurzer Zeit die entsprechende Umsetzung meiner Verbesserungsvorschläge sowie ihre sofort getroffenen Maßnahmen bestätigt hat, mit denen sie die festgestellten unzulässigen Verarbeitungen und datenschutzrechtlichen Defizite

abgestellt hat, war es mir nach § 25 Abs. 2 BDSG möglich, von einer förmlichen Beanstandung abzusehen. Ich habe mir jedoch ausdrücklich eine erneute Kontrolle, insbesondere im Verwaltungsbereich, einer anderen BfA-Klinik vorgemerkt.

19 Unfallversicherung

19.1 Gutachtertätigkeit

Die Gutachterregelung war eines der Herzstücke der Neuregelung des Rechts der gesetzlichen Unfallversicherung und hat bis heute in Konfliktsituationen nichts von ihrer Brisanz eingebüßt.

Die anhaltenden Anfragen und Eingaben von Versicherten sowie Gespräche mit einzelnen Berufsgenossenschaften, dem Hauptverband der Gewerblichen Berufsgenossenschaften und dem Bundesversicherungsamt (BVA) als der zuständigen Aufsichtsbehörde für die Unfallversicherungsträger zeigen die große Bedeutung der Gutachterregelung. Da das medizinische Gutachten zur Kausalität eines Arbeitsunfalls oder einer Berufskrankheit für die Gesundheitsbeeinträchtigung von den Unfallversicherungsträgern in den meisten Fällen zur Grundlage ihrer Entscheidung gemacht wird, ist die Möglichkeit für die Versicherten, an der Auswahl des Sachverständigen mitwirken zu können, von zentraler Bedeutung. Die intensiven Gespräche mit den genannten Stellen und die langen Zeiträume der Versuchs- und Umsetzungsphasen haben in vielen Bereichen der gesetzlichen Unfallversicherung zu deutlichen Verbesserungen geführt. Die noch im 19. TB (Nr. 26.1.2) als ein Schwerpunktthema behandelte Abgrenzung zwischen einem beratenden Arzt und einem Gutachter hatte im Berichtszeitraum deutlich an Bedeutung verloren. Mit Ausnahme des Verfahrens nach dem BK-Report (vgl. Nr. 19.3) haben sich die von dem Hauptverband der Gewerblichen Berufsgenossenschaften, dem BVA und mir entwickelten Abgrenzungskriterien in der Praxis bewährt. Die in Einzelfällen festgestellten Verstöße in diesem Bereich wurden von den jeweiligen Berufsgenossenschaften eingeräumt und die entsprechenden Gutachten gelöscht.

Bei den unverändert sehr problematischen Fragen des Gutachtervorschlagsrechts der Versicherten und der Anwendung datenschutzrechtlicher Regelungen bei der Beauftragung eines Gutachters während eines anhängigen Gerichtsverfahrens zeichnen sich zumindest positive Lösungsansätze ab, sodass ich auch hier eine Verbesserung des informationellen Selbstbestimmungsrechts der Versicherten erwarte.

19.1.1 Vorschlagsrecht des Versicherten

Das BMGS hält eine gesetzliche Normierung des Gutachtervorschlagsrecht für Versicherte nicht für erforderlich; eine Selbstverpflichtung der Unfallversicherungsträger, den Versicherten dieses Recht zu gewährleisten, sei ausreichend.

Meine wiederholte Forderung, den Versicherten in der gesetzlichen Unfallversicherung ein eigenes Vorschlagsrecht für Gutachter einzuräumen, hatte in dem Beschluss des Deutschen Bundestages zu meinem 18. Tätigkeitsbericht (Bundestagsdrucksache 14/9490 Nr. 7) zu einem entsprechenden Prüfauftrag an die Bundesregierung geführt. Nach Gesprächen mit den Geschäftsführern der Berufsgenossenschaften, dem Hauptverband der gewerblichen Berufsgenossenschaften und dem BVA hält das BMGS es aber nicht für erforderlich, eine gesetzliche Regelung in das SGB VII aufzunehmen. Das Ministerium betonte mir gegenüber zwar ausdrücklich, dass der Versicherte in der Praxis das Recht haben solle, selbst einen oder mehrere Gutachter vorzuschlagen; die Unfallversicherungsträger seien aber eine Selbstverpflichtung eingegangen, die in mehreren Pilotverfahren erprobten Verfahrensweisen (18. TB Nr. 23.1.2; 19. TB Nr. 26.1.1) nunmehr flächendeckend umzusetzen. Diese Argumentation ist nicht unproblematisch. Das BMGS, das BVA und die Berufsgenossenschaften greifen bei der Gutachtervorschlagsregelung auf § 20 Abs. 3 SGB X zurück, wonach eine Behörde die Entgegennahme von Anträgen nicht verweigern darf. Diese Vorschrift bleibt aber deutlich hinter dem angestrebten Recht der Versicherten zurück, selbst einen Gutachter vorschlagen zu dürfen. Meine Bedenken habe ich zunächst zurückgestellt, da sich die Berufsgenossenschaften in Abstimmung mit dem BMGS und dem BVA zu einer flächendeckenden Umsetzung des Gutachtervorschlagsrechts verpflichtet haben. Zu der nach Jahresfrist beabsichtigten Evaluierung werde ich mich äußern.

19.1.2 Empfehlungspapier für Gutachtervorschläge

Ein Fortschritt in der Verfahrenstransparenz in der gesetzlichen Unfallversicherung ist die Absicht der Berufsgenossenschaften, eine Liste mit allen von ihnen akzeptierten Gutachtern veröffentlichen zu wollen.

Die Berufsgenossenschaften haben in einem „Empfehlungspapier für Gutachtervorschläge“ ein Verfahren erarbeitet, dass zugleich der Qualitätssicherung und der Lenkung von Gutachtervorschlägen dienen soll. Dazu haben sie in Zusammenarbeit mit Fachgesellschaften, insbesondere mit der Deutschen Gesellschaft für Arbeitsmedizin, Kriterien für die Aufnahme in eine Gutachterliste erstellt: In einem allgemeinen Teil werden von den Berufsgenossenschaften Kriterien vorgegeben, wie z. B. Erfahrungen bei Begutachtungen in der gesetzlichen Unfallversicherung, klinische Ausstattung, Fortbildung, Publikationen. Auf Antrag eines Mediziners oder Sachverständigen wird anhand der aufgestellten Kriterien die Aufnahme in die Liste geprüft. Diese soll anschließend von den Unfallversicherungsträgern veröffentlicht werden.

In der Behandlung der Gutachtervorschläge der Versicherten betonten die Vertreter der Berufsgenossenschaften ausdrücklich, dass Versicherte auch weiterhin Gutachter vorschlagen könnten, die nicht auf der Liste stünden. Sei ein Gutachter nicht in die Liste aufgenommen, stelle das keinen ausreichenden Grund für die Ablehnung des entsprechenden Vorschlages dar. Dieses Verfahren werde ich in Stichprobenkontrollen überprüfen.

19.1.3 Gutachten während des Gerichtsverfahrens

Die Einholung eines Gutachtens durch eine Berufsgenossenschaft während eines anhängigen Gerichtsverfahrens ist aus datenschutzrechtlicher Sicht unzulässig und verfahrensrechtlich unnötig.

Im Berichtszeitraum war ich mit einer Vielzahl von Eingaben befasst, in denen Versicherte vortrugen, ihre Daten seien im Rahmen eines anhängigen sozialgerichtlichen Verfahrens an einen Gutachter übermittelt worden, der auf dieser Grundlage der Berufsgenossenschaft ein Gutachten erstattet habe. In keinem der Fälle wurde den Versicherten ein Widerspruchsrecht gegen die Übermittlung ihrer Daten gewährt.

Die Regelung des § 200 Abs. 2 SGB VII, mit der der Gesetzgeber die Mitwirkungsrechte der Versicherten stärken und die Transparenz des Verfahrens erhöhen wollte, ist von den Berufsgenossenschaften auch dann anzuwenden, wenn sie während eines anhängigen Gerichtsverfahrens unter Verwendung der Daten eines Versicherten ein Gutachten in Auftrag geben (18. TB Nr. 23.1.3.2; 19. TB Nr. 26.1.3). Das von den Berufsgenossenschaften hiergegen vorgebrachte Argument, die Vorschrift gelte nur im Verwaltungsverfahren bei den Berufsgenossenschaften, nicht aber im Gerichtsverfahren, in dem sich Versicherter und Unfallversicherungsträger von Anfang an gleichermaßen gegenüberständen, läuft ebenso ins Leere wie die Berufung auf den Grundsatz des rechtlichen Gehörs, nach dem eine Prozesspartei mit ihrem Vortrag gehört werden müsse. Diese Argumentation der Unfallversicherungsträger rechtfertigt keine Abweichung von dem allgemeinen datenschutzrechtlichen Grundsatz, dass eine Datenübermittlung nur zulässig ist, wenn das Gesetz sie erlaubt oder der Betroffene einwilligt. Das Sozialgerichtsgesetz sieht keine weiterreichende Befugnis für die Datenverarbeitung eines Unfallversicherungsträgers vor. Deshalb können die Berufsgenossenschaften nur im Rahmen des Sozialgesetzbuches die Daten der Versicherten nutzen, um ihre Rechtsauffassung zu stützen. Dem Unfallversicherungsträger kann es in einem Anerkennungsverfahren – auch wenn es vor dem Sozialgericht anhängig ist – nur um eine sachlich richtige Entscheidung gehen. Hierfür hat der Unfallversicherungsträger im Verwaltungsverfahren selbst die Ermittlungen geführt, im Regelfall ein Zusammenhangsgutachten eingeholt und nach bestem Wissen und Gewissen eine Entscheidung in der Hauptsache getroffen. Die Einholung eines neuen Gutachtens durch den Unfallversicherungsträger in einem anhängigen Sozialgerichtsverfahren ist deswegen regelmäßig nicht erforderlich. Ist in diesem Gerichtsverfahren ein neues Gutachten erstellt worden, kann sich der Unfallversicherungsträger für die Auseinandersetzung damit im Rahmen der bereits akzeptierten Abgrenzungskriterien im Verwaltungsverfahren vor der Berufsgenossenschaft beraten lassen. Dies wird nicht durch ein weiteres Gutachten, sondern durch eine Stellungnahme zu Qualität und Aussagekraft des neuen Gutachtens erfolgen. Da der Unfallversicherungsträger in eigener Zuständigkeit alle Ermittlungen für seine Entscheidung durchgeführt hatte, muss er sich im gerichtlichen Verfahren allenfalls noch zum Beweiswert eines neuen Gutachtens beraten lassen.

Das dargestellte Verfahren hat bereits in gemeinsamen Gesprächen mit dem Hauptverband der Gewerblichen Berufsgenossenschaften und dem BVA positive Resonanz gefunden. Das entscheidende Gremium der Unfallversicherungsträger, die Hauptgeschäftsführerkonferenz, hat jedoch noch nicht abschließend entschieden, welche Empfehlung ausgesprochen werden soll. Es ist zu wünschen, dass dieses Gremium auch hier zu einer datenschutzgerechten Regelung kommen wird.

Kasten zu Nr. 19.1.3

§ 200 SGB VII Einschränkung der Übermittlungsbefugnis

(2) Vor Erteilung eines Gutachtenauftrages soll der Unfallversicherungsträger dem Versicherten mehrere Gutachter zur Auswahl benennen; der Betroffene ist außerdem auf sein Widerspruchsrecht nach § 76 Abs. 2 des Zehnten Buches hinzuweisen und über den Zweck des Gutachtens zu informieren.

19.1.4 Zusatzgutachten

Die Unfallversicherungsträger weisen die Versicherten nunmehr auf ihr Recht hin, Gutachter auch bei der Zusatzbegutachtung vorschlagen zu können. Bei der Praxis der Zusatzbegutachtung bleiben noch Fragen offen.

Auf meine Anregung, den Versicherten darauf hinzuweisen, dass er auch bei der Beauftragung eines Zusatzgutachters die in § 200 Abs. 2 SGB VII genannten Rechte wahrnehmen kann, hat der Hauptverband der Gewerblichen Berufsgenossenschaften erfreulicherweise einen Teil dieser Regelung in einem Formblatt klargestellt, das allen Berufsgenossenschaften zur Verfügung gestellt wurde. In dem Informationsschreiben zum Gutachterauswahlverfahren und Gutachtervorschlagsrecht wird dem Versicherten mitgeteilt, dass ihm das Vorschlagsrecht auch bei einer Zusatzbegutachtung zusteht. So sehr ich die schnelle Umsetzung des letztgenannten Hinweises begrüße, so sehr würde ich mir eine datenschutzfreundlichere Handhabung der Gutachterregelung selbst wünschen. Bei unterschiedlichen und komplexen Verletzungen und/oder Erkrankungen, bei denen eine Zusatzbegutachtung zu erwarten ist, sollten schon bevor der Hauptgutachter beauftragt wird auch mindestens drei Zusatzgutachter zur Auswahl genannt und auf das Vorschlagsrecht des Versicherten hingewiesen werden. In Fällen, in denen eine Zusatzbegutachtung nicht absehbar ist, sollte im Formblatt für die Versicherten deutlich erkennbar klargestellt werden, dass die Berufsgenossenschaft „Herr des Verfahrens“ bleibt. Der Versicherte darf sich nicht dazu verpflichtet fühlen, sich mit dem

Hauptgutachter über die Beauftragung des Zusatzgutachters auseinandersetzen zu müssen.

Ich begrüße es, dass mehrere Berufsgenossenschaften ein Verfahren entwickeln wollen, das datenschutzfreundlichen Maßstäben gerecht wird.

19.2 Datenerhebung nach §§ 201, 203 SGB VII

Die von einigen Berufsgenossenschaften immer wieder geforderte Erweiterung der Möglichkeiten zur Datenerhebung wäre unzulässig und würde zudem den Versicherten unzumutbar belasten.

Die Regelung des § 203 Abs. 1 SGB VII verpflichtet Ärzte, die nicht an einer Heilbehandlung beteiligt sind – gemeint ist damit im wesentlichen das Durchgangsarztverfahren –, dem Unfallversicherungsträger auf Verlangen Auskunft über die „Behandlung, den Zustand sowie über Erkrankungen und frühere Erkrankungen des Versicherten“ zu erteilen, soweit dies für die Heilbehandlung und sonstige Leistungen erforderlich ist. Obwohl diese Regelung ihrem Wortlaut nach eindeutig ist, gibt es immer wieder Versuche, den Rahmen der Auskunftspflicht durch Auslegung zu erweitern. So wird bisweilen entgegen der eindeutigen Aufzählung der zu übermittelnden Daten behauptet, dass zusätzlich auch Daten der Versicherten zu beauskunften seien, die über den rein medizinischen Bereich hinausgehen. Auf diese Auffassung gestützt, erfragen verschiedene Berufsgenossenschaften formularmäßig, welche Angaben der Versicherte zu der Entstehung seiner Beschwerden gemacht habe. Zwar wird eingeräumt, dass zur Erhebung dieser Auskünfte kein praktisches Bedürfnis bestehe, da die nicht an einer Heilbehandlung beteiligten Ärzte in aller Regel keine Kenntnis vom Hergang eines Unfalls oder der Exposition an der Arbeitsstelle hätten. Die Erhebung dieser Daten verstößt auch gegen den eindeutigen Wortlaut der Vorschrift. Diese Einschränkung der Auskunftspflicht eines behandelnden Arztes auf die Erkrankung halte ich für unabdingbar, da viele Patienten gegenüber ihrem Arzt nur Mutmaßungen zu der Entstehung einer Erkrankung äußern und mögliche Aufzeichnungen des Arztes nicht überprüfen. Würden solche Äußerungen auch noch nach Jahren zu der Prüfung eines Anspruches in der gesetzlichen Unfallversicherung herangezogen werden können, würde dies nicht nur zu fragwürdigen Ergebnissen führen, sondern auch das Vertrauensverhältnis zwischen Arzt und Patienten stark beeinträchtigen. In dem unfallversicherungsrechtlichen Verfahren wäre es für den Betroffenen dann nahezu unmöglich, seine früheren Angaben zu korrigieren, zumal die Berufsgenossenschaften nicht selten mit dem Argument, die Erinnerung sei kurz nach einem Geschehen besonders frisch und daher zuverlässig, Korrekturen von Angaben generell ablehnen.

Über die Auslegung der §§ 201, 203 SGB VII bin ich weiterhin mit Berufsgenossenschaften, dem Hauptverband der gewerblichen Berufsgenossenschaften sowie dem Bundesversicherungsamt im Gespräch.

19.3 Zweite Auflage des BK-Reports zur Berufskrankheit Nr. 1317

Auch nach Änderungen in der zweiten Auflage des von dem Hauptverband der Gewerblichen Berufsgenossenschaften (HVBG) herausgegebenen Reports zur Berufskrankheit Nr. 1317 werden in den Ermittlungsverfahren zu dieser Berufskrankheit die datenschutzrechtlichen Vorschriften §§ 199 Abs. 3, 200 Abs. 2 SGB VII nicht berücksichtigt.

Die Berufskrankheit Nr. 1317 (Polyneuropathie oder Enzephalopathie durch organische Lösungsmittel oder deren Gemische) ist seit dem 1. Dezember 1997 in die Anlage der Berufskrankheiten-Verordnung aufgenommen worden. Aufgrund des komplexen Krankheitsbildes und der Vielzahl der in Frage kommenden toxischen Stoffe gab der HVBG einen BK-Report zu dieser Berufskrankheit heraus, der in der ersten Auflage auch Empfehlungen zur Sachbearbeitung enthielt. Gegen die in der Erstauflage enthaltenen Bearbeitungshinweise hatte ich im Hinblick auf die Einhaltung der Vorgaben des § 199 Abs. 3 SGB VII und § 200 Abs. 2 SGB VII Bedenken erhoben (18. TB Nr. 23.1.1). Im Berichtszeitraum erschien die überarbeitete zweite Auflage, in deren Erarbeitung ich trotz der schwerwiegenden datenschutzrechtlichen Mängel in der Vorauflage nicht einbezogen wurde. In der zweiten Auflage sind zwar keine detaillierten Bearbeitungshinweise enthalten. Dennoch sehe ich die Gefahr, dass die gesetzlichen Regelungen der §§ 119 Abs. 3, 200 Abs. 2 SGB VII weiterhin nicht beachtet werden, wenn der Sachbearbeitung die Neufassung des Reports zugrundegelegt wird.

Ich werde bei weiteren Kontrollen prüfen, ob in diesem Zusammenhang die Rechte der Versicherten nunmehr gewahrt werden.

20 Rehabilitations- und Schwerbehindertenrecht

Aufgrund fast identischer Zielsetzung von Datenschutz und allgemeinem Selbstbestimmungsrecht sind im Rehabilitations- und Schwerbehindertenrecht lediglich einige Umsetzungsfragen problematisch.

Nach dem das SGB IX prägenden Leitsatz des § 1 SGB IX erhalten behinderte oder von Behinderung bedrohte Menschen Leistungen nach dem Sozialgesetzbuch und den für die Rehabilitationsträger geltenden Leistungsgesetzen, um ihre Selbstbestimmung und gleichberechtigte Teilhabe am Leben in der Gesellschaft zu fördern, Benachteiligungen zu vermeiden oder ihnen entgegenzuwirken. Selbstbestimmung und Teilhabe sind danach nicht nur Ziel des Rehabilitations- und Schwerbehindertenrechts, sondern auch Direktive für die Gewährung und Durchführung von Leistungen. Da dieses Gesetz in Zielsetzung und Methodik mit datenschutzrechtlichen Positionen zu den Rechten Betroffener übereinstimmt, sind keine grundsätzlichen Differenzen und Schwierigkeiten aufgetreten. Im Rahmen meiner Beteiligung an den gemeinsamen Empfehlungen nach

§ 13 SGB IX habe ich die Erfahrung gemacht, dass bereits in den Entwürfen den Mitwirkungs- und Selbstbestimmungsrechten der Betroffenen Rechnung getragen worden war und meine Stellungnahmen Berücksichtigung fanden.

In den Servicestellen, die vorwiegend bei der Information, Beratung und Weiterleitung von Anträgen tätig werden, hat es datenschutzrechtliche Schwierigkeiten nicht gegeben.

Aus dem Bereich des Rehabilitations- und Schwerbehindertenrechts wurden an mich ausschließlich Eingaben herangetragen, die sich auf Datenerhebungen in Formularen bezogen. Zu Recht wandten sich mehrere Betroffene dagegen, dass auf Antragsformularen für eine bestimmte Rehabilitationsmaßnahme eine Vielzahl von Informationen abgefragt wurden, die für die Gewährung der jeweiligen Maßnahme nicht erforderlich waren. Grund dieser in manchen Fällen übermäßigen Datenerhebung ist in der Regel die Verwendung zu allgemeiner Formulare, die nicht speziell auf das Rehabilitations- und Schwerbehindertenrecht abgestimmt sind. Die Rehabilitationsträger nutzten vorhandene Formulare, die noch nicht die Kooperation mit anderen Rehabilitationsträgern und die spezielle Rehabilitationsmaßnahme berücksichtigten. Ich werde mich dafür einsetzen, dass bereits mit den gemeinsamen Empfehlungen i.S.d. § 13 SGB IX eine Anpassung der Formulare erfolgen kann, damit künftig die Datenerhebungen und -nutzungen nur in dem Umfang erfolgen, der für die einzelne Rehabilitationsmaßnahme erforderlich ist.

21 Gesundheit

21.1 Die elektronische Gesundheitskarte

Bereits seit Jahren wird über die Einführung und Nutzung von telematischen Anwendungen im Gesundheitsbereich diskutiert. Die Datenschutzregelungen zur elektronischen Gesundheitskarte müssen nun technisch umgesetzt werden.

Die elektronische Gesundheitskarte soll zum 1. Januar 2006 die bisherige Krankenversichertenkarte ablösen und zusätzlich die Einführung von telematischen Anwendungen unterstützen.

In meinem letzten Tätigkeitsbericht hatte ich bereits über die mögliche Ausgestaltung und die dabei denkbaren Anwendungen einer solchen Karte berichtet (19. TB Nr. 28.2 bis 28.4). Durch die Schaffung der gesetzlichen Grundlage in § 291a SGB V sind nun die vorgesehenen Anwendungen und wichtige technische und organisatorische Voraussetzungen der Verfahren festgelegt. Die Regelungen unterscheiden zwischen Pflicht- und freiwilligen Anwendungen. Zu den Pflichtanwendungen gehören die Verarbeitung der administrativen Daten sowie die Übermittlung des Rezeptes in elektronischer Form (§ 291a Abs. 2). Darüber hinaus soll die Karte auch medizinische Daten elektronisch verfügbar machen, insbesondere Arzneimitteldokumentation, Notfalldaten, Arztbrief, Patientenakte und vom Versicherten selbst zur Verfügung gestellte weitere Gesundheitsdaten. Über die Nutzung dieser Anwendungen soll der Betroffene frei entscheiden können (§ 291a Abs. 3).

Bei der Ausgestaltung des § 291a wurden die wesentlichen datenschutzrechtlichen Anforderungen berücksichtigt. So bleiben die Datenhoheit der Versicherten und der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten gewahrt. Die Versicherten können darüber entscheiden, welche ihrer Gesundheitsdaten aufgenommen und welche gelöscht werden sowie ob und welche Daten sie einem Leistungserbringer zugänglich machen. Ferner haben sie das Recht, die über sie gespeicherten Daten zu lesen und die Löschung der freiwillig erhobenen Daten zu verlangen. Die Zugriffsberechtigung auf die Daten ist detailliert für die jeweiligen Personengruppen geregelt, die zur Versorgung der Versicherten die Daten benötigen. Dies sind in der Regel Ärzte, Zahnärzte und Apotheker. Diese Personengruppen dürfen nur in Verbindung mit einem elektronischen Heilberufsausweis (Health Professional Card – HPC), der über eine qualifizierte elektronische Signatur verfügen muss, auf die Daten zugreifen. Die HPC ist ein elektronischer Identitäts- und Berufsausweis im Gesundheitswesen, der die Datensicherheit durch kryptographische Funktionen wie Verschlüsselung, Signatur und Authentisierung verbessern soll. In jedem Fall muss der Versicherte selbst den jeweiligen Zugriff freigeben.

Ich hatte zusätzlich gefordert, dass die gespeicherten Patientendaten nur unter Wahrung des bestehenden Schutzniveaus (z. B. des Beschlagnahmeschutzes in der Arztpraxis) verwendet werden dürfen und eine missbräuchliche Nutzung mit einem strafbewehrten Verbot belegt werden muss. Dies ist mit einer Änderung des § 97 Abs. 2 Strafprozessordnung – der Ausweitung des Beschlagnahmeverbotes auf mit der Gesundheitskarte gespeicherte Daten – und der Einführung einer Strafnorm in § 307a SGB V verwirklicht worden.

Sowohl bei der Erstellung des Rahmenkonzeptes als auch des – noch nicht vollendeten – Lösungskonzeptes war ich intensiv beteiligt. Bei der Erstellung der Lösungsarchitektur muss sichergestellt werden, dass die hohen gesetzlichen Anforderungen an den Schutz der Gesundheitsdaten technisch und organisatorisch umgesetzt werden:

– Die Datenhoheit der Patienten und der Grundsatz der Freiwilligkeit der Speicherung von Gesundheitsdaten müssen gewahrt werden.

– Die Patienten müssen darüber entscheiden können, welche ihrer Gesundheitsdaten aufgenommen und welche gelöscht werden.

– Die Patienten müssen darüber entscheiden können, ob und welche Daten sie einem Leistungserbringer zugänglich machen.

– Die Patienten müssen die Möglichkeit haben, die über sie gespeicherten Daten zu lesen.

Bei der Planung und Erprobung der Pflichtanwendungen dürfen keine Weichenstellungen getroffen werden, die später – bei Einführung weiterer Funktionalitäten – zu datenschutzrechtlichen Einbußen führen könnten.

Die grundlegenden technisch-organisatorischen Sicherheitsanforderungen ergeben sich aus § 9 BDSG. Aufgrund des sehr hohen Schutzbedarfs medizinischer Daten ergeben sich spezielle Sicherheitsanforderungen. insbesondere hinsichtlich der Verlässlichkeit und Beherrschbarkeit der Systeme. Bei der Lösungsarchitektur ist insbesondere darauf zu achten, dass die Verfügbarkeit, Vertraulichkeit und Nutzungsfestlegung der Daten, die Durchsetzbarkeit der Betroffenenrechte, die Festlegung einer verantwortlichen Stelle sowie Praktikabilität und Alltagstauglichkeit gewährleistet werden. Für die vorgesehenen Pflichtanwendungen müssen diese Anforderungen von Beginn an sichergestellt sein. Es muss darüber hinaus ein Höchstmaß an Interoperabilität für künftige Anwendungen sowie für denkbare, aber noch nicht hinreichend definierte, Funktionen gewährleistet sein. Bis zur endgültigen Spezifikation der elektronischen Gesundheitskarte müssen die in der Lösungsarchitektur zu beschreibenden Funktionalitäten getestet und in Feldversuchen erprobt werden. Dabei ist es mir besonders wichtig, dass alle sinnvollen technische Varianten ergebnisoffen geprüft werden, um auch unter Datenschutzgesichtspunkten eine optimale Lösung zu finden. Dies gilt insbesondere für die Frage, ob die Daten eher auf der Gesundheitskarte oder auf einem Server gespeichert werden sollen.

Kasten zu Nr. 21.1

Aus der Entschließung des Deutschen Bundestages zum 19. Tätigkeitsbericht vom 17. Februar 2005 Bundestagsdrucksache 15/4597:

„7. Der Deutsche Bundestag erwartet von der Bundesregierung, dass sie im Rahmen der Prüfung der Vereinbarung nach § 291a SGB V dafür Sorge trägt, dass die verschiedenen technischen Lösungen zur Einführung einer elektronischen Gesundheitskarte ohne Vorfestlegung auf ein Verfahren (technikoffen) getestet werden, damit die für den betroffenen Bürger datenschutzfreundlichste Lösung gefunden werden kann. Dazu zählt insbesondere, dass die Datenhoheit der Patienten gewahrt bleibt. Mit Blick auf die Sorgen und Ängste der Bürger hinsichtlich des Umgangs mit Gesundheitsdaten kann die flächendekkende Einführung der Gesundheitskarte nur dann erfolgreich gelingen, wenn ein Höchstmaß an Akzeptanz erreicht wird. (19. TB Nr. 1.7, 28.3).

…“

Abbildung 7 (zu Nr. 21.1)

21.2 Massenuntersuchungen bei Neugeborenen

Seit vielen Jahren gibt es ein sog. Neugeborenen-Screening, bei dem in den ersten Lebenstagen entnommenes Blut auf bestimmte Krankheiten untersucht wird. Der Untersuchungsumfang und die Behandlung der Proben wird in den einzelnen Bundesländern unterschiedlich gehandhabt.

Das sog. Neugeborenen-Screening wird zum Teil seit den 60er Jahren durchgeführt. Dabei wird Blut aus der Ferse des Neugeborenen entnommen und auf eine Testkarte aufgebracht. Das Blut wird untersucht, um behandelbare Stoffwechselkrankheiten von Neugeborenen unverzüglich erkennen und heilen zu können. Die Blutentnahme muss spätestens am dritten Tag nach der Geburt erfolgen, da nur bis zu diesem Tag das Vorliegen der Krankheiten erkannt werden kann. Die Aufbewahrung der Restblutmengen und der Befunde erfolgt in einigen Ländern zentral. Datenschutzrechtlich besonders problematisch ist die Archivierung der Testkarten mit den Restblutmengen. Solange diese den betroffenen Personen noch zugeordnet werden können, stellen sie eine – auch gentechnisch auswertbare – zentrale Probensammlung dar, die entsprechende Begehrlichkeiten wecken könnte.

Anlässlich der Beratung dieser Thematik auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellte sich heraus, dass das Neugeborenen-Screening in den einzelnen Bundesländern völlig unterschiedlich gehandhabt wird. Parallel zu diesen Überlegungen hat die 75. Gesundheitsministerkonferenz das BMGS aufgefordert, in Anbetracht künftiger diagnostischer Möglichkeiten eine „nationale Screening Kommission“ zu bilden, die Empfehlungen für die Weiterentwicklung von Screeninguntersuchungen im Kindesalter entwickeln soll.

Daraufhin hat mir der Gemeinsame Bundesausschuss (vgl. § 91 Abs. 5 SGB V) einen Entwurf einer Ergänzung der Richtlinie über die Früherkennung von Krankheiten bei Kindern bis zur Vollendung des 6. Lebensjahres zur Stellungnahme vorgelegt. Dieser Entwurf enthält zum einen die Aufzählung der sog. Zielkrankheiten und zum anderen die Regelung zur Vernichtung der Restblutproben spätestens drei Monaten nach der Entnahme. Eine entsprechende bundeseinheitliche Regelung habe ich in Anbetracht der Sensibilität der Daten im Hinblick auf mögliche spätere gentechnische Analysen und der zentralen Aufbewahrung stets gefordert. Der vorliegende Entwurf, insbesondere die Regelung zum Aufbewahrungszeitraum, ist aus datenschutzrechtlicher Sicht positiv zu bewerten. Ich werde die Entwicklung auch weiterhin begleiten und auf eine datenschutzgerechte Ausgestaltung des Verfahrens achten.

21.3 Apotheken-CD

Durch die sog. Apotheken-CD werden personenbezogene Rezeptdaten unzulässigerweise zu kommerziellen Zwecken verwendet. Eine gesetzliche Klarstellung erscheint dringend erforderlich.

Die Problematik der Nutzung personenbezogener Rezeptdaten von Apothekenkunden für andere als Abrechnungszwecke in Form der sog. Apotheken-CD hat mich auch im Berichtszeitraum weiter beschäftigt (vgl. 19. TB Nr. 28.7.3). Nach § 300 Abs. 2 SGB V ist den Apothekenrechenzentren die personenbezogene Datenverarbeitung allein für Abrechnungszwecke erlaubt. Meine Auffassung wird von dem zuständigen BMGS geteilt. Dagegen vertreten die Datenschutzaufsichtsbehörden der Länder überwiegend die Auffassung, dass die Erstellung und Nutzung der Apotheken-CD dann zulässig sei, wenn sie sich auf

– die Erstellung von Zuzahlungsbescheinigungen für die Patienten,

– Möglichkeiten der Rezeptrecherche für Patienten, Ärzte und Krankenkassen oder

– die Nachvollziehbarkeit der Berechtigung einer Retaxation

beziehen würde.

Das BMGS und ich haben die obersten Datenschutzaufsichtsbehörden wiederholt auf die Unvereinbarkeit der o. g. Auffassung mit dem geltenden Recht hingewiesen. Bedeutsam ist insbesondere, dass die Apothekenrechenzentren Rezeptdaten unzulässigerweise zur kommerziellen Vermarktung nutzen. Dies bewirkt nicht nur eine unterschiedliche Auslegung und uneinheitliche Handhabung sozialrechtlicher Vorschriften in den Ländern. Damit werden auch die strengen Zweckbindungsregeln für sensible Gesundheitsdaten aufgeweicht, was insbesondere vor dem Hintergrund der Einführung der Telematik im Gesundheitswesen (z. B. der Gesundheitskarte) von großer datenschutzrechtlicher Brisanz ist. Die Entwicklung der IT wird zu zunehmenden Datenbeständen im Gesundheitswesen führen, was die Notwendigkeit verstärkt, die Nutzung der Gesundheitsdaten auf einen engen Verwendungszweck zu begrenzen.

Aufgrund der beschriebenen Situation halte ich eine klarstellende Änderung des § 300 Abs. 2 SGB V für unumgänglich, um die unterschiedlichen Interpretationen dieser Vorschrift zu beenden.

22 Verkehr

22.1 Mit dem Brummi auf der Datenautobahn unterwegs

Am 1. Januar 2005 wurde mit der Erhebung der LKW-Maut begonnen. Bereits in der Testphase des Systems wurden personenbezogene Daten erhoben und verarbeitet; ich habe daher vor dem offiziellen Start an Ort und Stelle die Einhaltung der datenschutzrechtlichen Vorgaben geprüft.

Nachdem die gesetzlichen Grundlagen für die Datenverarbeitung bei der Erhebung der LKW-Maut festgelegt waren (vgl. 19. TB Nr. 29.1), standen nun die technische Gestaltung und die Funktionalität des ausgewählten Systems sowie die praktische Umsetzung des Autobahnmautgesetzes (ABMG) im Mittelpunkt meines Interesses. Nach dem Gesetz hatte das Mautsystem die Anforderungen des Datenschutzes auch bereits im Test- und Probebetrieb zu erfüllen. Hierzu haben das Bundesamt für Güterverkehr (BAG) und die Betreiberfirma Toll Collect GmbH (Toll Collect) Datenschutzkonzepte erstellt, die ich bei

der Kontrolle des BAG und von Toll Collect an verschiedenen Standorten herangezogen habe. Darüber hinaus ergaben sich zahlreiche rechtliche Auslegungsfragen. Mit der für den 1. Januar 2005 vorgesehenen Inbetriebnahme des LKW-Mautsystems wird die Diskussion über die damit verbundenen Datenschutzfragen nicht beendet sein. Zum einen wird die Einhaltung der datenschutzrechtlichen Bestimmungen bei der Mauterhebung zu überprüfen sein. Darüber hinaus stellen sich im Zusammenhang mit der diskutierten Ausweitung des Mautsystems auf andere Streckenabschnitte, z. B. Landstraßen, oder auf andere Fahrzeuge (insbesondere PKW) und im Hinblick auf die „Citymaut“ zusätzliche datenschutzrechtliche Fragen. Für mich ist es dabei besonders wichtig, dass für private Verkehrsteilnehmer der Grundsatz der „datenfreien Fahrt“ weiterhin gewährleistet bleibt. Solche Ausweitungen des Mautsystems erscheinen mir nur dann vertretbar, wenn dabei Nutzungs- und Abrechnungsmodelle zum Einsatz kommen, bei denen regelmäßig keine personenbezogenen Daten erhoben oder verarbeitet werden.

22.1.1 Datenverarbeitung im Test- und Probebetrieb des LKW-Mautsystems

Aufgrund technischer Schwierigkeiten konnte die für 31. August 2003 vorgesehene Aufnahme des Wirkbetriebs nicht stattfinden. Im Frühjahr 2004 wurden schließlich die Weichen für eine Fortsetzung des Vertrages mit der Betreibergesellschaft gestellt. Daher musste das System in allen Funktionalitäten weiter getestet werden. Hierzu wurden auch personenbezogene Daten erhoben und verarbeitet. Um möglichen Fehlentwicklungen noch vor Aufnahme des Echtbetriebes begegnen zu können, habe ich mir rechtzeitig ein Bild über die Verarbeitung und Löschung der im Rahmen der Tests erhobenen Daten verschafft. So habe ich im August 2004 ein Rechenzentrum und eine Kontrollzentrale von Toll Collect, eine Mautbrücke sowie das BAG geprüft und eine Fahrt mit einem Kontrollfahrzeug des BAG unternommen.

Das BAG hatte mir vor Beginn des Testlaufs im Frühjahr 2004 mitgeteilt, dass es zu Optimierungs- und Analysezwecken Daten zu allen Durchfahrten, also auch zu denen der nicht mautpflichtigen Fahrzeuge, erheben und 24 Stunden in der Mautbrücke speichern wolle. Daten der Testteilnehmer sollten nach Ende des Tests gelöscht werden. Im Laufe des Tests veränderten sich jedoch die Modalitäten, und ich stellte fest, dass auch Daten von nicht mautpflichtigen Fahrzeugen nicht binnen 24 Stunden gelöscht wurden, sondern für den gesamten Testzeitraum vorgehalten werden sollten. Sie seien für Prüfungen der Systemfunktionen erforderlich. Ich habe hierzu klargestellt, dass der Test- und Probebetrieb keinesfalls im rechts- und kontrollfreien Raum durchgeführt werden könne; Art, Umfang und Dauer der Tests müssten klar geregelt sein. Für die einzelnen Anwendungen liegen nun entsprechend meiner Forderung konkrete Verfahrensanweisungen und Löschkonzepte vor.

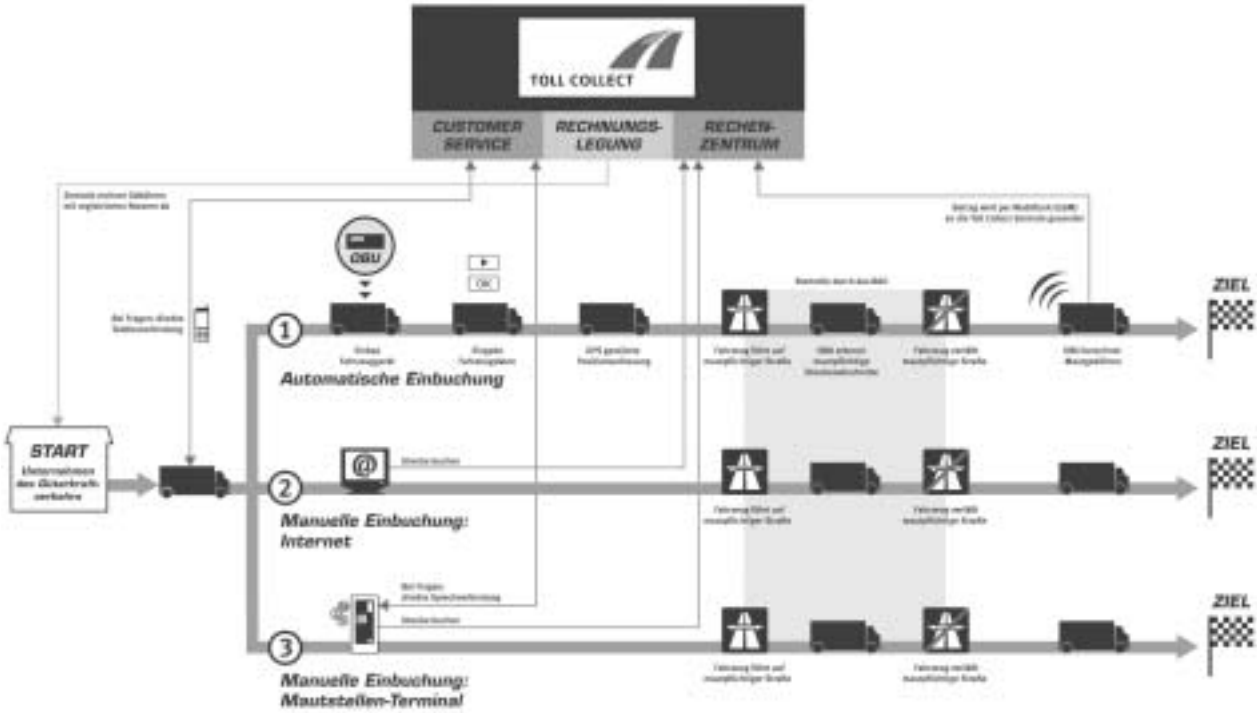
Abbildung 8 (zu Nr. 22.1)

Mautbrücke

An der Kontrollbrücke hatte ich die Möglichkeit, mir den ansonsten nicht sichtbaren technischen Erhebungs- und Kontrollvorgang anzuschauen. Ich habe dabei festgestellt, dass nur die Informationen, die für die Mautberechnung erforderlich sind, erhoben und zwischengespeichert wurden. Die Auswertung und Bearbeitung der dort erhobenen Daten konnte ich mir in der Kontrollzentrale ansehen. Bei der Prüfung des Rechenzentrums standen technisch-organisatorische Maßnahmen des Datenschutzes im Vordergrund. Die auf allen Bearbeitungsfeldern getroffenen Sicherheitsmaßnahmen und die technisch-organisatorischen Vorkehrungen gewährleisten einen angemessenen Datenschutz. Ich habe mich davon überzeugt, dass die Grundlagen für eine Umsetzung der datenschutzrechtlichen Anforderungen des Gesetzes in den Funktionalitäten des Systems auch geschaffen wurden.

Abbildung 9 (zu Nr. 22.1)

Mauterfassung in Deutschland



22.1.2 Zweckbindung der Mautdaten gesichert

Nach einem Beschluss des Amtsgerichtes Gummersbach vom 21. August 2003 sollten im Rahmen strafrechtlicher Ermittlungsverfahren Daten, die im Zusammenhang mit der Mauterhebung erhoben wurden, zur Verfügung gestellt werden. Adressaten des Beschlusses waren Toll Collect als Betreiber des Systems und das BAG als verantwortliche Stelle. Vor diesem Hintergrund stellte sich die Frage, wie die datenschutzrechtlichen Bestimmungen des ABMG auszulegen sind und in welcher Relation sie zu den Vorschriften der Strafprozessordnung (StPO) und des Telekommunikationsgesetzes (TKG) stehen. Hier war ich mir mit dem BMVBW einig, dass die strenge Zweckbindung der für die Mautzahlung erhobenen und gespeicherten Daten nicht unterlaufen werden darf. Bereits bei der ursprünglichen Rechtslage war aus meiner Sicht eine Verwendung der Daten z. B. für Zwecke der Strafverfolgung nicht zulässig. Andere bereichsspezifische Regelungen (z. B. die der StPO) sind gegenüber denen des ABMG nachrangig. Diese Auffassung entsprach der Intention des Gesetzgebers (vgl. Begründung zu § 4 Abs. 2 ABMG, Bundesratsdrucksache 643/01 S. 27f.): „Daten, die im Rahmen der Mauterhebung und der Kontrolle der Einhaltung der Mautpflicht erhoben bzw. übermittelt werden, dürfen ausschließlich für diese Zwecke genutzt werden“. Gegen eine Übermittlung spricht auch § 160 Abs. 4 StPO, der eine Maßnahme als unzulässig bezeichnet, sofern eine bundes- oder landesrechtliche Verwendungsregelung entgegensteht. Dies ist hier mit den Zweckbindungsregelungen in den §§ 4 Abs. 2 und 7 Abs. 2 ABMG der Fall. Für eine strenge Zweckbindung spricht ferner, dass der Gesetzgeber an anderer Stelle Ausnahmen von strengen Zweckbindungsregelungen zugunsten der Strafverfolgungsbehörden in das Gesetz aufgenommen hat. So enthalten §§ 5 Satz 2 und 6 Abs. 5 Satz 5 Teledienstedatenschutzgesetz nach der Novellierung durch das Gesetz über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr eben solche Ausnahmen von der Zweckbindung zugunsten der Strafverfolgungsbehörden mit einem ausdrücklichen Hinweis auf § 160 Abs. 4 StPO.

Mit Blick auf die abweichende Entscheidung des AG Gummersbach hielt ich es dennoch für erforderlich, durch eine gesetzliche Klarstellung für alle Verfahrensbeteiligten Rechtssicherheit zu schaffen. Zwar hatte die Bundesregierung in ihrer Antwort auf eine Kleine Anfrage der Fraktion der FDP (Bundestagsdrucksache 15/2127) meine Auffassung geteilt, dass die im Zusammenhang mit der LKW-Maut erhobenen Daten grundsätzlich nicht für andere Zwecke nutzbar gemacht werden könnten. Gleichwohl habe ich die Novellierung des ABMG (Bundestagsdrucksache 15/3678), in der hauptsächlich eine Regelung zur Festsetzung des neuen Starttermins vorgesehen war, zum Anlass genommen, auf eine Konkretisierung der Zweckbindungsregelung der §§ 4 Abs. 2 und 7 Abs. 2 ABMG hinzuwirken, um die Beschlagnahme dieser Daten auf jeden Fall zu verhindern. Mit Erfolg: Die §§ 4 Abs. 2 und 7 Abs. 2 ABMG wurden um den Satz: „Eine Übermittlung, Nutzung oder Beschlagnahme dieser Daten nach anderen Rechtsvorschriften ist unzulässig“ ergänzt (BGBl. I S. 3121). Durch diese Formulierung besteht nun für alle Beteiligten Rechtsklarheit.

22.1.3 Kein Online-Zugriff auf Kundendateien für die Regulierungsbehörde

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) hatte im September 2003 die Betreiberfirma Toll Collect wegen der Teilnahme am automatisierten Abrufverfahren nach § 112 TKG angeschrieben. Nach dieser Vorschrift können bestimmte Behörden Auskünfte aus den Kundendateien der Telekommunikationsdiensteanbieter erhalten, soweit die Auskünfte zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich sind und die Ersuchen im automatisierten Verfahren vorgelegt werden. Das BAG sprach sich jedoch gegen die Anwendbarkeit des § 112 TKG aus, da eine Verpflichtung des Betreibers, am automatisierten Auskunftsverfahren teilzunehmen, seiner Ansicht nach bereits daran scheitere, dass dieser keine Telekommunikationsdienste anbiete und das automatisierte Verfahren eine geschäftsmäßige Telekommunikation im Sinne der §§ 3 Nr. 10 und 112 Abs. 1 TKG voraussetze. Nach § 3 Nr. 10 TKG sei „geschäftsmäßiges Erbringen von Telekommunikationsleistungen“ das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte. Die Übertragung von Daten über den mautpflichtigen Streckenabschnitt vom Fahrzeuggerät an das Rechenzentrum und im Gegenzug über die sich hieraus ergebende Mauthöhe vom Rechenzentrum an das Fahrzeuggerät, stelle keine Telekommunikation dar. Hierfür spreche u. a., dass Fahrzeuggerät und Karte Eigentum des Betreibers seien, die Karte selbst fest installiert sei und nur durch eine vom Betreiber autorisierte Werkstatt herausgenommen werden könne. Es würden ausschließlich Daten übermittelt, die entsprechend den Festlegungen des Betreibers der Addition von Streckenabschnitten dienten. Damit sei der Betreiber und nicht etwa der Fahrzeugführer oder -eigentümer Nutzer der Einrichtung.

Weiter stellte sich die Frage nach dem Inhalt einer solchen Datei. Nach den Vorgaben des § 112 Abs. 1 TKG sind in die Kundendatei unverzüglich die Rufnummern und Rufnummernkontingente, die zur weiteren Vermarktung oder sonstigen Nutzung an andere vergeben werden, sowie Name und Anschrift der Inhaber von Rufnummern und Rufnummernkontingenten aufzunehmen, auch soweit diese nicht in öffentlichen Verzeichnissen eingetragen sind. Eine Rufnummernzuordnung zur SIM-Karte führt ausschließlich der Netzbetreiber durch. Anschlussinhaber ist Toll Collect. Der Datei wäre deshalb nur zu entnehmen, dass eine Nachricht vom Betreiber an den Betreiber geschickt wurde, da es sich bei Sender und Empfänger um den gleichen Nutzer handelt.

Meine Bedenken habe ich der RegTP vorgetragen. Im Ergebnis schloss sich die Behörde meiner Argumentation an, so dass für Toll Collect keine Verpflichtung besteht, eine Kundendatei für das Abrufverfahren nach § 112 TKG zu führen. Vielmehr ist das Unternehmen als Kunde in den entsprechenden Kundendateien der Mobilfunkbetreiber aufzuführen, mit denen Telekommunikationsdienstleistungsverträge hinsichtlich der eingebauten SIM-Karten abgeschlossen wurden.

22.1.4 Einsatz von Videoaufzeichnungen zur Überprüfung des Betreibervertrages

Das BAG informierte mich darüber, dass es Toll Collect im Rahmen der Qualitätskontrolle durch Videoaufzeichnungen überprüfen wolle, um festzustellen, ob die Betreibergesellschaft ihre Leistungen vertragsgemäß erbringe. Eine Schlechterfüllung würde insbesondere dann vorliegen, wenn innerhalb eines Jahres 500 Mautpflichtige nicht bzw. nicht korrekt zur Entrichtung der Nutzungsgebühr herangezogen würden. Das BAG beabsichtigt, mindestens 10 000 Fahrzeuge einer Gegenkontrolle zu unterziehen. Dazu ist vorgesehen, handelsübliche Videokameras einzusetzen, die den laufenden Verkehr, also mautpflichtige und nicht mautpflichtige Fahrzeuge, parallel zu den für die Mauterhebung erforderlichen Erfassungen, in einer Richtung für ca. vier Stunden aufzeichnen sollen. So kann festgestellt werden, ob das System die mautpflichtigen Fahrzeuge erfasst und korrekt verbucht oder ob es sich um Falsch- oder Nichtzahler handelt.

Gegen die Aufzeichnung der nicht mautpflichtigen Fahrzeuge habe ich datenschutzrechtliche Bedenken geltend gemacht. Ich verkenne zwar nicht, dass der Auftraggeber die ordnungsgemäße Funktionsfähigkeit des Systems gewährleisten muss und ihm Möglichkeiten der Qualitätskontrolle gegeben werden müssen. Diese müssen sich allerdings im Rahmen der gesetzlichen Regelungen bewegen. Eine Aufzeichnung von PKW ist nach dem ABMG nicht vorgesehen: Nicht mautpflichtige Fahrzeuge müssen sofort gelöscht werden (§ 9 Abs. 5 ABMG). Die Vorschrift des § 6b BDSG lässt eine Videobeobachtung öffentlich zugänglicher Räume nur unter eingeschränkten Voraussetzungen zu und fordert eine Unterrichtung der Betroffenen. Wenn jedoch bei der Videoaufzeichnung eine Technik eingesetzt wird, die weder personenbezogene noch personenbeziehbare Daten zu erfassen in der Lage ist, findet das BDSG keine Anwendung. Deshalb habe ich beim BAG angeregt, dass nur eine Videokamera dergestalt eingesetzt wird, mit der Kfz-Kennzeichen oder gar Insassen nicht erkannt werden können, so dass keine personenbezogene Datenerhebung vorliegt. Vor diesem Hintergrund ist eine Bekanntmachung des Aufnahmeverfahrens nach § 6b Abs. 2 BDSG zwar nicht zwingend erforderlich, gleichwohl habe ich dem BAG im Interesse höchstmöglicher Transparenz die Veröffentlichung in seinem Internetportal empfohlen.

22.2 Der gläserne Passagier

Das letzte Wort über das zwischen der USA und der EU geschlossene Abkommen zur Übermittlung von Passagierdaten ist noch nicht gesprochen.

Am 17. Mai 2004 hat die Europäische Union mit den USA ein Abkommen über die Übermittlung von Passagierdaten durch die Fluggesellschaften an die amerikanischen Zoll- und Grenzschutzbehörden geschlossen. Dem vorausgegangen war nach sehr langwierigen und schwierigen Verhandlungen die am 14. Mai 2004 getroffene Feststellung der Kommission, dass das von den zuständigen US Zoll- und Grenzschutzbehörden gewährleistete Schutzniveau angemessen sei.

Mit Abschluss des Abkommens wurde die seit März 2003 praktizierte Datenübermittlung zwar endlich auf eine rechtliche Grundlage gestellt, hinsichtlich der getroffenen Vereinbarungen sowie der nach wie vor praktizierten Art der Datenübermittlung habe ich jedoch erhebliche Vorbehalte. In einer Reihe von Punkten scheint mir das Abkommen nicht ausgewogen, weil es die datenschutzrechtlichen Interessen der Betroffenen nur unzureichend berücksichtigt. Wegen solcher Bedenken hat das Europäische Parlament noch im Juni 2004 den Europäischen Gerichtshof um Überprüfung des Abkommens gebeten. Mit einer Entscheidung ist in 2005 zu rechnen.

Die Art. 29-Gruppe (vgl. Nr. 3.2.1) hat während der Verhandlungen zwischen der Kommission und den USA mehrfach Stellung genommen. Einige der Forderungen der Gruppe wurden daraufhin berücksichtigt, andere hingegen nicht. So ist der Zweck der Datenübermittlung in dem Abkommen immer noch zu weit gefasst. Er umfasst jetzt die Verhütung und Bekämpfung des Terrorismus sowie anderer schwerer Verbrechen, einschließlich des organisierten Verbrechens, ohne dies aber näher zu definieren.

Nicht einverstanden bin ich auch mit dem Umfang der zu übermittelnden Daten. Zwar haben die USA die Liste der Datenfelder von ursprünglich 38 auf jetzt 34 gekürzt, allerdings sind dies immer noch weitaus mehr als die 19 Datenfelder, die die Art. 29-Gruppe für die genannten Zwecke als ausreichend erachtet. Auch bestehen weiterhin Probleme in Bezug auf sensible Daten wie etwa Angaben zu Rasse, Gesundheit, politischen und religiösen Überzeugungen, die in allgemeinen Datenfeldern enthalten sein können. Zwar verpflichten die Vereinbarungen die USA, solche sensiblen Daten herauszufiltern, die europäischen Datenschutzbehörden konnten sich aber bisher nicht von dem einwandfreien Vollzug dieser Maßnahme überzeugen.

Die ursprünglich vorgesehene Speicherfrist von 50 Jahren konnte zwar auf Drängen der Art. 29-Gruppe auf 3 ½ Jahre reduziert werden, aber auch diese Frist ist unverhältnismäßig lang.

Die Behörden der USA erhalten die Passagierdaten im sog. pull-Verfahren, d. h. durch Zugriff auf die Reservierungssysteme der Fluggesellschaften. Sie greifen dabei auf den kompletten Datensatz zu, der zu den einzelnen Passagieren vorliegt. Im Einzelfall können dies sogar mehr als 34 Datenfelder sein. Von Anfang an hat die Art. 29-Gruppe deshalb die Fluggesellschaften dazu aufgefordert, eine Filtersoftware zu installieren, die bewirkt, dass ausschließlich die im Abkommen vereinbarten 34 Datenelemente im sog. „push-Verfahren“ übermittelt werden und gleichzeitig die sensiblen Daten herausgefiltert werden.

Die Europäischen Datenschutzbehörden haben sich auf einheitliche Informationstexte zur Unterrichtung der Passagiere geeinigt. Somit werden nunmehr alle Fluggäste aus Europa in die USA unabhängig von Aufenthaltsort oder Staatsangehörigkeit umfassend über den Umgang mit ihren Daten in den USA und ihre Rechte unterrichtet.

Die Kommission verhandelte im Berichtszeitraum auch mit Kanada und Australien über Abkommen zwecks

Übermittlung von Passagierdaten. Auch diese Verhandlungen werden durch die Art. 29-Gruppe kritisch begleitet.

Kasten zu Nr. 22.2

Diese Daten werden übermittelt

1. PNR-Buchungscode (Record Locator)
2. Datum der Reservierung
3. Geplante Abflugdaten
4. Name
5. Andere Namen im PNR
6. Anschrift
7. Zahlungsart
8. Rechnungsanschrift
9. Telefonnummern
10. Gesamter Reiseverlauf für den jeweiligen PNR
11. Vielflieger-Eintrag (beschränkt auf abgeflogene Meilen und Anschrift(en))
12. Reisebüro
13. Bearbeiter
14. Codeshare-Information im PNR
15. Reisestatus des Passagiers
16. Informationen über die Splittung/Teilung einer Buchung
17. E-Mail-Adresse
18. Informationen über Flugscheinausstellung (Ticketing)
19. Allgemeine Bemerkungen
20. Flugscheinnummer
21. Sitzplatznummer
22. Datum der Flugscheinausstellung
23. Historie über nicht angetretene Flüge (no show)
24. Nummern der Gepäckanhänger
25. Fluggäste mit Flugschein aber ohne Reservierung (Go show)
26. Spezielle Service-Anforderungen (OSI – Special Service Requests)
27. Spezielle Service-Anforderungen (SSI/SSR – Special Service Requests)
28. Information über den Auftraggeber (received from)
29. Alle Änderungen der PNR (PNR-History)
30. Zahl der Reisenden im PNR
31. Sitzplatzstatus
32. Flugschein für einfache Strecken (one-way)
33. Etwaige APIS-Informationen
34. ATFQ-Felder (automatische Tarifabfrage)

22.3 Online-Anbindung der örtlichen Zulassungsstellen an das Kraftfahrt-Bundesamt

Durch Änderungen der Kommunikationswege bei den örtlichen Zulassungsstellen werden auch Anpassungen bei der Datenübermittlung durch das Kraftfahrt-Bundesamt erforderlich.

Seit dem 1. Januar 1999 führt das Kraftfahrt-Bundesamt (KBA) ein Zentrales Fahrerlaubnisregister (vgl. 18. TB Nr. 28.2.1). Darin werden u. a. die in Deutschland erteilten Fahrerlaubnisse, die Probezeit von Fahranfängern und die Fahrerlaubnisse zur Fahrgastbeförderung gespeichert. Die Fahrerlaubnisdaten werden dem KBA von den örtlichen Fahrerlaubnisbehörden zur Verfügung gestellt. Das KBA ist derzeit über verschlüsselte Datenleitungen mit den Kraftfahrzulassungsstellen der Länder verbunden. Für den Datenaustausch stehen in den örtlichen Zulassungsstellen gesonderte Rechner zur Verfügung, auf denen jeweils eine für diese Anbindung entwickelte Software des KBA installiert ist. Die Nutzer müssen sich über ein Passwort der Zulassungsstelle authentifizieren und können dann über eine gesicherte (verschlüsselte) Datenleitung den Abgleich der Zulassungsdaten mit dem KBA vornehmen. Damit ist sichergestellt, dass der Zugriff auf die Daten des KBA nur von einer berechtigten Stelle und über eine gesicherte Datenleitung vorgenommen wird. Wann und von wem eine Änderung des Datensatzes vorgenommen wird, protokolliert das KBA. Meine Forderung, den Datentransfer über eine Ende-zu-Ende-Verschlüsselung sicher zu stellen, wurde somit weitgehend erfüllt.

Im Rahmen der Neuorganisation ihrer IT-Struktur haben viele Kommunen ihre Zulassungsstellen einem kommunalen Rechnerverband angeschlossen, der die verschiedenen Anwendungen betreut und die dazugehörige Software pflegt und verwaltet. Diese Kommunen möchten das oben beschriebene Verfahren nun durch eine Anbindung über ihre Netze zum KBA ablösen. Eine wie bisher durch das KBA garantierte „durchgehende“ Ende-zu-Ende-Sicherheit bis zum Arbeitsplatz des Bearbeiters wäre dann nicht mehr möglich.

Diese geplante Veränderung hat eine grundsätzliche Diskussion der technischen Anbindung der Kommunen/Länder an Stellen des Bundes ausgelöst, die personenbezogene Daten speichern. Die Verantwortlichkeit bezüglich der Daten kann bei einer Umstrukturierung des Datenaustausches nicht mehr ausschließlich bei der datenspeichernden Stelle liegen, sondern muss gleichermaßen von der für das Netz und den Datenverbund zuständigen Stelle getragen werden. Bezüglich der Datenanbindung der Kommunen/Länder an die Datennetze der Bundesbehörden müssen Forderungen nach Datensicherheit und Authentizität jedoch weiterhin erfüllt werden. Die Anbindungen sehen im Gegensatz zum in der Vergangenheit praktizierten File-Transfer neuerdings auch eine Online-Anbindung mit direktem lesenden und schreibenden Zugriff auf die jeweiligen Datensätze vor.

Nach meiner Einschätzung kann die Anbindung der Zulassungsstellen an das KBA auch durch neue Übertragungstechniken datenschutzgerecht realisiert werden. So können beispielsweise die Sicherheitsanforderungen bei der Nutzung des TESTA-Verwaltungsnetzes erfüllt werden. Dagegen sind Festlegungen auf bestimmte Datenübertragungstechniken nicht notwendig und aus wirtschaftlichen und technischen Gründen oft nicht sinnvoll. Die Verantwortlichkeit des KBA für die sichere Anbindung der Zulassungsstellen endet entgegen der bisherigen Lösung dann bei der Übergabe der Daten an die jeweiligen Landesnetze/kommunalen Verbundnetze. Ich habe dem KBA empfohlen, einen Anforderungskatalog zur Datensicherheit für die Anwendungen zu erstellen und Regelungen zur IT-Sicherheit in den angeschlossenen Netzen und in den Zulassungsstellen (z. B. zur Verwendung von Zertifikaten) mit den Ländern abzustimmen. Die neue Übertragungstechnik führt auch zu Veränderungen bei der Datenschutzaufsicht. Während ich für das KBA zuständig bin, sind für den übrigen Bereich die jeweiligen Landesdatenschutzbeauftragten verantwortlich. Um eine einheitliche Regelung auch auf der Ebene der Datenschutzaufsicht zu erreichen, muss die Thematik im Arbeitskreis Technik der Datenschutzkonferenz weiter behandelt werden.

23 Auswärtige Angelegenheiten

23.1 Gefangenenbetreuung im Ausland

Das Auswärtige Amt hat umgehend auf Mängel bei der Aktenführung in der Konsularabteilung einer Botschaft reagiert.

Nach § 7 Konsulargesetz sollen Konsularbeamte in deutschen Auslandsvertretungen deutsche Untersuchungs- und Strafgefangene auf deren Verlangen betreuen und ihnen insbesondere Rechtsschutz vermitteln.

Anlässlich einer Eingabe habe ich mir in der Rechts- und Konsularabteilung einer Botschaft die Bearbeitung von Betreuungsfällen inhaftierter deutscher Staatsbürger angesehen. Entgegen früherer Erfahrung stellte ich fest, dass ärztliche Unterlagen in den Haftakten in verschlossenen Umschlägen abgeheftet werden. In den in der Registratur befindlichen Unterlagen ehemaliger Inhaftierter sowie in den im Archiv im Keller befindlichen Haftakten war dies allerdings noch nicht der Fall. In einigen Haftakten befanden sich Informationen, die Dritte betrafen und die für die Bearbeitung des Haftfalles nicht erforderlich waren.

Das AA hat auf meine Prüfmitteilungen umgehend reagiert und einen detaillierten Runderlass für die Auslandsvertretungen unter meiner Beteiligung erarbeitet. Neben Grundsätzen der Aktenführung werden auch spezielle Probleme wie die Behandlung ärztlicher Gutachten, die Übergabe von Schriftstücken Dritter an den Inhaftierten, private Schriftstücke der Inhaftierten, die Dokumentation der Haftfälle, Listen von Inhaftierten und ehemals Inhaftierten datenschutzkonform geregelt.

23.2 Fehlende Diskretionszonen und Hinweisschilder in Auslandsvertretungen

Zur verbesserten Kommunikation zwischen Bürgern und Bediensteten der Auslandsvertretungen müssen auch Diskretionsschalter vorgesehen werden.

Mehrere Petenten fühlten sich beim Vorbringen ihres Anliegens durch die Behandlung in den Konsulaten und Botschaften in ihren Rechten verletzt. Den Schilderungen zu Folge erfolgte die Kommunikation mit den Bediensteten durch eine dicke Glasscheibe. In einem Fall wurde eine Lautsprecheranlage verwendet. Die Petenten waren gezwungen, ihr Anliegen entweder über die Lautsprecheranlage vorzutragen oder aber wegen der Glasscheibe sehr laut zu sprechen, um vom Personal verstanden zu werden, so dass alle in dem Raum anwesenden Personen den Inhalt des persönlichen Gesprächs mithören konnten. Getrennte Diskretionsschalter waren entweder nicht vorhanden oder die Petenten wurden nicht über diese Nutzungsmöglichkeit informiert.

Ich habe die Vorgänge zum Anlass genommen, das AA darauf hinzuweisen, dass durch Hinweisschilder die Möglichkeit der diskreten Bearbeitung einer Angelegenheit deutlich angezeigt wird. Derartige Diskretionsschilder sind in anderen Bereichen der Bundesverwaltung bereits üblich und haben sich bewährt. Das AA hat die Einrichtung von Diskretionsschaltern, soweit noch nicht vorhanden, zugesagt, und die zügige Umsetzung meiner Empfehlung per Erlass verfügt.

24 Bildung und Forschung

24.1 BAföG-Abgleich – gibt es den gläsernen Studenten?

Um Fälle des Leistungsmissbrauchs bei BAföG aufzudecken, haben die Ämter für Ausbildungsförderung dem Bundesamt für Finanzen Angaben der Auszubildenden im Wege des automatisierten Datenabgleichs übermittelt. Wegen dieser rechtlich problematischen Praxis hat der Gesetzgeber auf meine Initiative hin eine eindeutige Rechtsgrundlage geschaffen.

Beim Antrag auf Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz (BAföG) müssen die Antragsteller Angaben zu ihrem Vermögen machen. Weil es den Ämtern für Ausbildungsförderung (im folgenden BAföG-Ämter) in aller Regel aufgrund der Angaben im Antragsformular nicht möglich ist, Verdachtsfälle aufzudecken, übermitteln sie dem Bundesamt für Finanzen (BfF) den Namen und andere unmittelbar identifizierende Daten derjenigen Personen, die Leistungen nach dem BAföG erhalten, im Wege des automatisierten Datenabgleichs. Das BfF gleicht diese Angaben mit den vorhandenen Daten über die Höhe der gemäß Freistellungsauftrag tatsächlich in Anspruch genommenen Freistellung von der Zinsabschlagsteuer ab und unterrichtet in den Trefferfällen über den Betrag. Aufgrund der Rückmeldungen klären die BAföG-Ämter, ob die vom BfF mitgeteilten Zinseinkünfte dem vom Antragsteller angegebenem Vermögen entsprechen; sind Abweichungen zu

vermuten, wird mit dem Betroffenen zum Zwecke der Klärung des Sachverhaltes Kontakt aufgenommen. Dabei wurde in den vergangenen Jahren ein erheblicher Leistungsmissbrauch festgestellt.

Für die datenschutzrechtliche Bewertung des Sachverhalts sind zunächst die beiden relevanten Übermittlungsvorgänge zu unterscheiden: Eine Befugnis der BAföG-Ämter, die für den Abgleich beim BfF erforderlichen Daten zu übermitteln, war lange umstritten. So könnte sie aus § 69 Abs. 1 Nr. 1 SGB X abgeleitet werden: Danach wäre die Übermittlung von Sozialdaten zulässig, soweit sie für die Erfüllung der Zwecke einer gesetzlichen Aufgabe der übermittelnden Sozialleistungsträger erforderlich ist; also auch zur Überprüfung der Angaben der Leistungsempfänger. Nach einer anderen Ansicht ergibt sie sich weder im Umkehrschluss aus § 45d Abs. 2 Satz 2 Einkommensteuergesetz (EStG) noch aus den Übermittlungsvorschriften des SGB X. Zur Datenübermittlung vom BfF an die BAföG-Ämter ergibt sich die Befugnis nach erfolgtem Abgleich durch das BfF aus § 45d Abs. 2 Satz 2 EStG; sie ist datenschutzrechtlich unbedenklich.

Grundsätzlich wird man davon ausgehen müssen, dass die Regelungen des SGB X nur die Überprüfung von Angaben der Sozialleistungsempfänger im Einzelfall vor Augen haben. Dieser Grundsatz gilt auch bei der Beurteilung der Frage, ob ein vollständiger Abgleich aller Fälle für die Erfüllung der Aufgaben der BAföG-Ämter erforderlich ist. Wenn – wie im vorliegenden Fall – der Leistungsmissbrauch in einem solchen Umfang erfolgt, dass die Durchführung von Stichproben oder die Überprüfung in Verdachtsfällen keine geeigneten Mittel mehr darstellen, könnte ein vollständiger Abgleich vertretbar sein; allerdings nur als ultima ratio und auf Basis einer klaren gesetzlichen Regelung. Sozialdatenabgleiche sind letztlich flächendeckende Jedermann-Kontrollen. Nach der Redlichkeitsvermutung als konstitutivem Merkmal unserer Verfassung darf der Staat nicht jedermann als potentiellen Rechtsbrecher – d. h. als solchen, der Leistungen missbraucht – betrachten. Der Staat hat vielmehr davon auszugehen, dass die Bürger sich an Recht und Gesetz halten. Daher ist die Erforderlichkeit einer solchen Maßnahme in Abständen erneut zu prüfen. Vor diesem Hintergrund habe ich den zuständigen Bundesministerien mitgeteilt, dass ich eine klarstellende Gesetzesänderung für die Übermittlung zu einem vollständigen Abgleich für geboten halte.

Im Einundzwanzigsten Gesetz zur Änderung des Bundesausbildungsförderungsgesetzes (21. BAföGÄndG) vom 2. Dezember 2004 (BGBl. I S. 3127) ist in § 41 Abs. 4 eine ausdrückliche spezialgesetzliche Regelung für den automatisierten Vermögensdatenabgleich geschaffen worden. Aufgrund meiner Initiative wurden darüber hinaus auch die Antragsformblätter zum BAföG überarbeitet. Diese enthalten nun den deutlichen Hinweis, dass im Antrag erhobene Angaben zum Vermögen beim BfF überprüft werden können. Dies entspricht meiner Forderung, dass mit einem weitergehenden Informationsfluss besondere Informationsrechte der Betroffenen verbunden sein müssen.

24.2 Forschungsgeheimnis – Wie weit reicht der Zugang der Wissenschaft?

Seit Längerem fordern Wissenschaftler die Normierung eines Forschungsgeheimnisses, um einen erleichterten Zugang zu personenbezogenen Daten zu erhalten. Ein erster Schritt könnte ein Forschungsgeheimnis für medizinische Daten sein.

Wissenschaftliche Forschungsvorhaben nehmen seit Jahren stetig zu. In vielen Bereichen, insbesondere bei der medizinischen, der kriminologischen und der sozialwissenschaftlichen Forschung, ist die Verarbeitung personenbezogener Daten erforderlich. Diese Datenverarbeitung bedarf einer rechtlichen Legitimation entweder durch Rechtsvorschrift oder mit Einwilligung der Betroffenen. Mit der Datenübermittlung an Forscher verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und Beschlagnahme im Strafverfahren. Den Forschern steht bezüglich dieser Daten auch kein Zeugnisverweigerungsrecht zu. Durch die Einführung eines Forschungsgeheimnisses versprechen sich die Wissenschaftler einen erleichterten Zugang zu den personenbezogenen Daten. Aus datenschutzrechtlicher Sicht könnte dadurch ein besserer Schutz gegen Kenntnisnahme durch Dritte geschaffen werden, sowohl gegenüber anderen Forschern als auch gegenüber staatlichen Behörden.

Vor diesem Hintergrund hat sich die 67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einer Entschließung für die Einführung eines Forschungsgeheimnisses zunächst nur für medizinische Daten ausgesprochen (vgl. Kasten zu Nr. 24.2). Der Bundesgesetzgeber wird aufgefordert, in § 203 Strafgesetzbuch die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen, in den §§ 53, 53a Strafprozessordnung (StPO) ein Zeugnisverweigerungsrecht für Forscher und in § 97 StPO ein Verbot der Beschlagnahme dieser Daten zu schaffen. Die Datenschutzbeauftragten sind sich einig, dass diese Vorschläge nur einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung darstellen. Solche Regelungen sollen zwar kein allgemeines Zugangsrecht der Forscher ermöglichen, aber die rechtlich zulässige Datenübermittlung erleichtern, denn bei der Abwägung zwischen dem öffentlichen Interesse an der Forschung und den schutzwürdigen Belangen der Betroffenen reduzieren sich die Risiken der Betroffenen vor einer missbräuchlichen Verwendung ihrer Daten, wenn die Verschwiegenheit der Forscher gewährleistet ist. In einer ersten Stellungnahme hat das BMJ zugesagt, die Verankerung eines Forschungsgeheimnisses durch Änderungen im StGB sorgfältig zu prüfen. Eine Änderung der StPO werde nicht erwogen, insbesondere da das für die Gewährung eines Zeugnisverweigerungsrechtes maßgebliche besondere Vertrauensverhältnis zwischen Forschern und Betroffenen nicht bestehe; gleiches gelte für die hieran anknüpfenden Beschlagnahmeprivilegien.

Ich werde die Problematik mit dem BMJ weiter erörtern und mich auch in Gesprächen mit den Wissenschaftlern und Forschern für konstruktive Lösungsvorschläge einsetzen; der kürzlich gegründete Rat für Sozial- und Wirtschaftsdaten stellt hierfür ein gutes Forum dar (vgl. Nr. 24.4).

Kasten zu Nr. 24.2

67. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25. und 26. März 2004

Entschließung:
Einführung eines Forschungsgeheimnisses für medizinische Daten

In vielen Bereichen der Forschung werden sensible medizinische Daten der Bürgerinnen und Bürger verarbeitet. Dabei ist häufig eine Verarbeitung auch personenbezogener Daten erforderlich. Diese Daten können mit Einwilligung der Betroffenen insbesondere von Ärztinnen und Ärzten, aber auch von Angehörigen anderer Heilberufe an Forscher und Forscherinnen übermittelt werden. Dies ist im Interesse der Forschung zwar grundsätzlich zu begrüßen. Mit der Übermittlung verlieren die Daten aber regelmäßig den strafrechtlichen Schutz vor Offenbarung und den Beschlagnahmeschutz im Strafverfahren. Auch ein Zeugnisverweigerungsrecht bezüglich dieser Daten steht den Forschenden – anders als insbesondere den behandelnden Ärztinnen und Ärzten – nicht zu. Zum Schutze der Forschung, vor allem aber zum Schutz der durch die Datenübermittlung und -verarbeitung Betroffenen, sollte vom Gesetzgeber deshalb sichergestellt werden, dass die bei den übermittelnden Stellen geschützten personenbezogenen medizinischen Daten auch nach ihrer Übermittlung zu Forschungszwecken den gleichen Schutz genießen.

Die Datenschutzbeauftragten fordern daher den Bundesgesetzgeber auf,

- in § 203 StGB die unbefugte Offenbarung von personenbezogenen medizinischen Forschungsdaten unter Strafe zu stellen,
- in §§ 53, 53a StPO für personenbezogene medizinische Daten ein Zeugnisverweigerungsrecht für Forscher und ihre Berufshelfer zu schaffen,
- in § 97 StPO ein Verbot der Beschlagnahme personenbezogener medizinischer Forschungsdaten zu schaffen.

Die Datenschutzbeauftragten sehen in diesen Vorschlägen einen ersten Schritt zu einer generellen Regelung des besonderen Schutzes personenbezogener Daten in der Forschung.

24.3 Forschungsdatenzentrum des Statistischen Bundesamtes

Ende 2001 hat das Statistische Bundesamt ein Forschungsdatenzentrum gegründet, um den Zugang der Wissenschaft zu Einzeldaten der Statistik zu verbessern. Derzeit bereiten auch die Statistischen Landesämter die Einrichtung eines Forschungsdatenzentrums vor.

Mit der Einrichtung des Forschungsdatenzentrums (FDZ) des Statistischen Bundesamtes wurde eine Empfehlung der „Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik“ aufgegriffen. Dabei ging die Kommission davon aus, dass die Daten – auch solche, die für andere Zwecke im Rahmen staatlichen Handelns entstehen – so effizient wie möglich für wissenschaftliche Analysen genutzt werden müssen, um die Kooperation zwischen Statistik und Wissenschaft zu verbessern.

Das FDZ soll den Zugang zu den amtlichen Einzeldaten unter den gegebenen rechtlichen Rahmenbedingungen für die Datennutzer ausbauen und bestehende Möglichkeiten optimieren. Hierzu zählt der Ausbau des Angebots an faktisch anonymisierten und an absolut anonymisierten Mikrodaten sowie der Aufbau einer Struktur zum Ferndatenzugriff. Der Zugang zu faktisch anonymisierten Mikrodatenbeständen soll hierbei sowohl in Form des on-site als auch des off-site Zugriffs erfolgen. Beim on-site Zugriff werden die Daten in den geschützten Räumlichkeiten des FDZ zur Verfügung gestellt, während bei der off-site Nutzung die Daten, in der Regel in der Form einer CD, für ein fest definiertes Forschungsprojekt außerhalb des FDZ zur Verfügung gestellt werden. Da hierbei für die sachgerechte Verwendung der Daten keine weitere Kontrollmöglichkeit besteht, muss bei der faktischen Anonymisierung der Datenbestände äußerste Sorgfalt angewandt und das der Wissenschaft maximal zur Verfügung stehende Zusatzwissen berücksichtigt werden. Die dargestellten Zugangsformen der Wissenschaft zu den amtlichen Einzeldaten stellen aus rechtlicher Sicht keine Erweiterung der bisherigen Praxis dar, da alle Datenübermittlungen nach den Vorgaben des Bundesstatistikgesetzes erfolgen. Hiervon habe ich mich anlässlich eines Besuches beim FDZ überzeugt.

Mit dem FDZ ist eine zentrale Anlaufstelle für die Wissenschaft eingerichtet worden. Um der Wissenschaft auch den Zugang zu den dezentral erhobenen Statistiken zu ermöglichen, ist auch die Einrichtung eines Forschungsdatenzentrums der Statistischen Landesämter vorgesehen. Dieses soll in Form einer Arbeitsgemeinschaft der Statistischen Landesämter betrieben werden, wobei jedes Statistische Landesamt jeweils einen regionalen Standort des Forschungsdatenzentrums bildet. Hier ergeben sich – im Unterschied zum FDZ, das nur seine „eigenen“ Daten verarbeitet – andere rechtliche Fragestellungen, weil eine Übertragung von statistischen Arbeiten an Dritte vorliegt.

24.4 Rat für Sozial- und Wirtschaftsdaten

Im Jahr 2004 berief das BMBF einen Rat für Sozial- und Wirtschaftsdaten, um die empirische Sozial- und Wirtschaftswissenschaft zu unterstützen. Bereits im Vorfeld habe ich einen konstruktiven Dialog zur Lösung bestehender datenschutzrechtlicher Probleme eingeleitet.

Am 1. November 2004 berief das BMBF den Rat für Sozial- und Wirtschaftsdaten (RatSWD). Dieser ist ein zunächst auf acht Jahre befristet eingerichtetes unabhängiges Gremium von empirisch arbeitenden Wissenschaftlern aus Universitäten, Hochschulen und anderen Einrichtungen unabhängiger wissenschaftlicher Forschung sowie

Vertretern wichtiger Datenproduzenten. Auf der Grundlage der Empfehlungen der „Kommission zur Verbesserung der informationellen Infrastruktur zwischen Wissenschaft und Statistik“ soll er die Situation der empirischen Sozial- und Wirtschaftswissenschaften verbessern, indem er zur Transparenz und besseren Nutzung vorhandener Daten, zur Erhöhung der Synergie zwischen Wissenschaft und Datenproduzenten und zur wissenschaftlichen Fundierung der Politikberatung und Aufklärung der Öffentlichkeit beiträgt.

Bereits im Vorfeld führte der Gründungsausschuss des RatSWD zwei „Konferenzen für Sozial- und Wirtschaftsdaten“ durch, an denen ich mich jeweils durch die Moderation des Forums „Datenschutz und Datensicherheit“ intensiv beteiligt habe. Hier bestand weitgehende Einigkeit zwischen allen Beteiligten, dass – ausgehend von den Rechtsgütern der Forschungsfreiheit und des informationellen Selbstbestimmungsrechts – der verfassungsrechtliche Ausgleich zwischen den widerstreitenden Grundrechten und Gemeinschaftsinteressen nur durch praktische Konkordanz hergestellt werden kann, indem jedem der beiden Rechtsgüter möglichst weitreichende Effektivität verschafft wird. Solche Entscheidungen sind im Regelfall durch den Gesetzgeber zu treffen, der die wissenschaftliche Verfügbarkeit von Daten zu normieren und notwendige Einschränkungen durch eine Abwägung zwischen beiden Grundrechten festzulegen hat. Konkrete praktische Fragestellungen betrafen die Einrichtung von Forschungsdatenzentren bei den Statistischen Ämtern, der Bundesagentur für Arbeit und anderen Datenhaltern sowie die Einführung eines gesetzlichen Forschungsgeheimnisses. Im Ergebnis bleibt festzuhalten, dass durch die Einrichtung des RatSWD ein konstruktiver Dialog zwischen der Wissenschaft und dem Datenschutz eingeleitet worden ist. Aus meiner Sicht sind die Wissenschaftler weiter aufgerufen, die praktischen Probleme speziell im Bereich des Datenzugangs zu benennen, um einen vernünftigen Ausgleich der verschiedenen Interessen zu erreichen.

25 Verteidigung

25.1 PERFIS II – Das neue Personalinformationssystem der Bundeswehr

Die in der Vergangenheit festgestellten Mängel bei der Implementierung von PERFIS II bestehen nach wie vor.

Bei der Prüfung des neuen Personalinformationssystems PERFIS II der Bundeswehr, das das System PERFIS ersetzt hat (19. TB Nr. 30.2), habe ich zahlreiche Mängel festgestellt. Anlässlich der Kontrolle einer Wehrbereichsverwaltung stellte ich fest, dass die bei meiner letzten Kontrolle von PERFIS angesprochenen gravierenden Mängel noch immer bestehen. Seinerzeit hatte ich von einer förmlichen Beanstandung nur aufgrund des Pilotprojektcharakters der Implementierung des Datenbanksystems SAP R/3 HR abgesehen; zudem war mir zugesichert worden, die festgestellten Mängel abzustellen. Ich habe das BMVg um eine detaillierte Erklärung gebeten, warum diese gravierenden Mängel immer noch nicht abgestellt worden sind und wann mit einer datenschutzgerechten Verfahrensweise zu rechnen ist. Eine förmliche Beanstandung nach § 25 BDSG habe ich mir diesbezüglich vorbehalten.

25.2 Kontrollen bei einer Bundeswehreinheit und in einem Bundeswehrkrankenhaus

Soll und Ist des Datenschutzes in der Bundeswehr klaffen noch auseinander.

Bei der Kontrolle eines Bundeswehrkrankenhaus und einer Einheit der Truppe stellte ich fest, dass für den Datenschutz beim hierfür zuständigen „administrativen Datenschutzbeauftragten“ in einem Fall nur 5 Prozent seines Dienstplanes vorgesehen waren und in einem anderen Fall die Einordnung bzw. Vergütung der Stelle ebenfalls nicht der Bedeutung entsprach, die die Aufgabenwahrnehmung des Datenschutzbeauftragten erfordert. Ich habe daher die angemessene Ausstattung und Besetzung des Dienstpostens „Administrativer Datenschutzbeauftragter“ empfohlen.

In beiden kontrollierten Dienststellen musste ich feststellen, dass das Verfahrensverzeichnis DATAV (Dateienerfassungs- und Auswertungs-Verfahren) nach § 18 Abs. 2 BDSG nicht ordnungsgemäß geführt wurde. In beiden Dienststellen wurden Verfahren zur Verarbeitung personenbezogener Daten eingesetzt, die im DATAV verzeichnet waren.

Im Bereich der Personalaktenbearbeitung stellte ich in beiden Einrichtungen fest, dass Personalnebenakten auch personenbezogene Daten anderer Soldaten enthielten sowie Heiratsurkunden, Mietverträge oder Auszüge aus Familienbüchern. Hierbei handelt es sich um Unterlagen und Dokumente, die nicht in die Personalnebenakte gehören, da sie zur Aufgabenerfüllung der Dienststelle nicht erforderlich sind. Eine Kontrolle der Arbeitsplatzcomputer ergab die Speicherung von Word-Dateien mit personenbezogenen Daten auf der lokalen Festplatte, obwohl dies unzulässig ist. Zum Teil wurden Dateien mit Personenbezug in unzulässiger Weise geführt, wobei es sich um sog. Mustervorlagen handelte, die jedoch Echtdaten enthielten. Dagegen hat die Anfertigung von Musterformularen ohne Personenbezug zu erfolgen. Ich habe daher empfohlen, den Dateibestand regelmäßig durch Stichproben zu überprüfen. Dies sollte durch den Datenschutzbeauftragten in Zusammenarbeit mit dem IT-Sicherheitsbeauftragten erfolgen.

Die insgesamt zahlreichen festgestellten Mängel im Bundeswehrkrankenhaus – beispielsweise die Abrufbarkeit der Stammdaten der im Krankenhausinformationssystem KIS eingestellten Patientendaten durch alle Nutzer des KIS oder die unverschlüsselte und unprotokollierte Datenübertragung bei der Fernwartung – habe ich gem. § 25 Abs. 1 BDSG als einen Verstoß gegen die §§ 9 und 18 Abs. 2 BDSG förmlich beanstandet.

26 Zivildienst

26.1 Neuregelung des Rechts der Kriegsdienstverweigerung

Durch eine umfassende Neuregelung des Rechts der Kriegsdienstverweigerung sind u. a. die Befragungen und Überprüfungen durch die Ausschüsse und Kammern weggefallen.

Mit dem Gesetz zur Neuregelung des Rechts der Kriegsdienstverweigerung (Kriegsdienstverweigerungs-Neuregelungsgesetz) vom 9. August 2003 wurde vor allem das Gesetz über die Verweigerung des Kriegsdienstes mit der Waffe aus Gewissensgründen (Kriegsdienstverweigerungsgesetz – KDVG) grundlegend geändert.

Am Gesetzgebungsverfahren bin ich vom Bundesministerium für Familie, Senioren, Frauen und Jugend bereits nach Erstellung des ersten (internen) Referentenentwurfs beteiligt worden. Dies gab mir die Möglichkeit, in einem sehr frühen Stadium eine datenschutzrechtliche Beratung durchzuführen, was ich ausdrücklich begrüßt habe.

Erfreulich ist z. B., dass die obligatorische Vorlage eines Führungszeugnisses nach § 30 Abs. 1 Bundeszentralregistergesetz (BZRG) entfallen ist. Allerdings ist es datenschutzrechtlich problematisch, dass das Bundesamt für den Zivildienst (BAZ) nach § 6 Abs. 3 KDVG ein Führungszeugnis nach § 31 BZRG anfordern kann, wenn seiner Auffassung nach Zweifel an der Wahrheit der Angaben des Kriegsdienstverweigerers bestehen und anzunehmen ist, dass diese Zweifel durch die Einholung eines solchen Führungszeugnisses aufgeklärt werden können. Dies stellt eine grundsätzliche Verschlechterung für die Betroffenen im Vergleich zur früheren Rechtslage dar. Das Führungszeugnis nach § 31 BZRG enthält nämlich gegenüber dem Führungszeugnis nach § 30 Abs. 1 BZRG ggf. zusätzliche (negative) Informationen über sie.

Auf der anderen Seite stellt die Tatsache, dass nur noch in Ausnahmefällen überhaupt ein Führungszeugnis zum Gegenstand des Verfahrens gemacht wird, einen datenschutzrechtlichen Mehrwert dar. Ich habe mich unter Zurückstellung von Bedenken dem Vorschlag des BMJ angeschlossen, wobei ich insbesondere Wert darauf lege, dass der Grund für die Anforderung, die eine Ermessensentscheidung ist, aktenkundig gemacht wird. Die Formulierung: „Wenn Zweifel an der Wahrheit der Angaben der Antragstellerin oder des Antragstellers bestehen und anzunehmen ist, dass diese Zweifel durch die Einholung eines Führungszeugnisses aufgeklärt werden können“ (§ 6 Abs. 3 Satz 1 KDVG), entspricht inhaltlich meinem Vorschlag, nur im begründeten Einzelfall eine solche Auskunft einzuholen und gibt Rechtsanwendern Kriterien für ihre Entscheidung an die Hand.

Ich werde die Praxis des BAZ im Hinblick auf die Erforderlichkeit solcher Anforderungen aufmerksam beobachten.

26.2 Zivildienst und Wehrgerechtigkeit

Nach einem – nicht rechtskräftigen – Urteil des Verwaltungsgerichts Köln ist die Einberufung zum Wehrdienst ungerecht und deshalb rechtswidrig. Führt diese Entscheidung auch zu rechtlichen Konsequenzen für das Einplanungsverfahren des Bundesamts für den Zivildienst (BAZ)?

Die Frage nach der Wehrgerechtigkeit hat im Jahre 2004 sowohl das VG Köln als auch das Bundesverfassungsgericht beschäftigt. Mit Urteil vom 21. April 2004 (Az: 8 K 154/04) gab das VG Köln der Klage eines Wehrpflichtigen statt, der sich gegen seine Einberufung gewendet hatte. Das Gericht sah keine gesetzliche Grundlage für die seit dem 1. Juli 2003 geltenden Einberufungsrichtlinien des BMVg. Nach diesen Richtlinien werden größere Gruppen von Wehrpflichtigen von der Einberufung ausgenommen, wie z. B. verheiratete oder über 23 Jahre alte Männer. Zur Begründung wird auf eine ältere Entscheidung des BVerfG verwiesen, wonach die Wehrgerechtigkeit verlange, dass bei der Einberufung zur Wehrpflicht nicht willkürlich und ohne sachlich zwingenden Grund unterschiedliche Anforderungen gestellt werden. Das Bundesverwaltungsgericht (Az: 6C9.04) hat am 19. Januar 2005 dagegen entschieden, dass trotz der geltenden Ausnahmen die Wehrgerechtigkeit nicht verletzt sei, wenn die Zahl der nach den gesetzlichen Regeln zur Einberufung verfügbaren Wehrpflichtigen „weitgehend“ ausgeschöpft werde, d. h. keine Willkür bei der Einberufung vorliege.

Vor diesem Hintergrund – der Zivildienst ist die alternative Möglichkeit der Erfüllung der Wehrpflicht; die Einberufung zum Zivildienst ist daher Ausfluss der Wehrgerechtigkeit – erhielt ich mehrere Eingaben von Kriegsdienstverweigerern (KDV), deren personenbezogene Daten vom BAZ im Rahmen des Einplanungsverfahrens an Wohlfahrtsverbände übermittelt worden waren. Diese Verbände wandten sich an die KDV, um ihnen einen Zivildienstplatz anzubieten. Hierin sahen die KDV einen Verstoß gegen den Datenschutz. U. a. wurde argumentiert, dass derjenige KDV, der lange genug wartet und sich nicht aktiv um einen Zivildienstplatz bemühe, wegen der begrenzt zur Verfügung stehenden Stellenzahl nicht vom BAZ eingeplant werde. In den Anschreiben der Wohlfahrtsverbände sahen die KDV unzulässige „Werbeschreiben“ und eine nachteilige Aufforderung, sich um einen Zivildienstplatz mit der nachfolgenden Einberufung zum Zivildienst zu bemühen.

Die von mir eingeholte Stellungnahme des BAZ zur Rechtfertigung des Einplanungsverfahrens und der damit verbundenen Datenübermittlung hat mich überzeugt.

§ 5a ZDG regelt, dass Wohlfahrtsverbände mit der Wahrnehmung von Verwaltungsaufgaben beauftragt werden können. Die Aufgabenübertragung auf die Verbände erfolgt auf der Grundlage eines Vertrages zur Übertragung von Verwaltungsaufgaben (sog. ÜVA-Vertrag). Bestandteil dieses Vertrages sind die Richtlinien für die Durchführung übertragener Verwaltungsaufgaben (ÜVA-Richtlinien). Auf Grund dieser vertraglichen Vereinbarungen nehmen die Verbände als beliehene Unternehmer hoheitliche Aufgaben wahr und gelten gemäß § 2 Abs. 4 Satz 2 BDSG als öffentliche Stellen im Sinne des BDSG.

Sie haben zur Durchführung der Aufgaben Verwaltungsstellen gebildet (vgl. Nr. 26.3).

Die Übermittlung der personenbezogenen Daten erfolgt für Zwecke der Durchführung des ZDG. Eine wesentliche Aufgabe des BAZ ist die Einberufung der Dienstpflichtigen (§ 19 ZDG). Hierzu gehört auch deren Einplanung. Grundsätzlich sind die Dienstpflichtigen von Amts wegen einzuberufen. Dies hätte nicht unerhebliche Auswirkungen auf Dienstantrittszeit bzw. -ort und damit letztlich auf die gesamte Lebensplanung des Betroffenen. Daher hat sich die sinnvolle Praxis herausgebildet, nach der die Einberufung im Einvernehmen zwischen dem Dienstpflichtigen und der Beschäftigungsstelle zustande kommt.

Eine nach § 5a ZDG den ÜVA-Auftragnehmern übertragene Verwaltungsaufgabe kann auch die Mitwirkung bei der Einplanungsaufgabe sein. Die Einplanung nach Namensliste (sog. Listeneinplanung) wird unter Ziff. 6.2 der ÜVA-Richtlinie geregelt. Die Verwaltungsstellen erhalten notwendigerweise eine Liste der von ihnen einzuplanenden Zivildienstpflichtigen. Auf Grund des ÜVA-Vertrages sind die Verwaltungsstellen verpflichtet, dem Dienstpflichtigen einen Zivildienstplatz zu verschaffen. Die Entscheidung zwischen eigener Einplanung und der Listeneinplanung liegt im Ermessen des BAZ. Bei der Ermessenausübung hat sich das BAZ an seinem gesetzlichen Auftrag einer bedarfsgerechten Einplanung zu orientieren. Gleichzeitig unterliegt der Bedarf der Zivildienststellen ständigen Veränderungen, auf die das BAZ reagieren können muss. Würde sich das BAZ dazu entscheiden, nicht vermittelte Zivildienstpflichtige generell von Amts wegen einzuberufen, hätten sie keine eigene Einflussnahmemöglichkeit mehr auf die Auswahl der Zivildienststelle.

Eine solche zwangsweise Stellenzuteilung halte ich für kein milderes Mittel im Vergleich zum Listeneinplanungsverfahren. Das Selbstbestimmungsrecht der Dienstpflichtigen wird dadurch gewahrt, dass ihnen noch einmal die Gelegenheit gegeben wird, sich selbst für einen bestimmten Zivildienstplatz zu entscheiden. Hierzu bieten ihnen die Verwaltungsstellen verschiedene Optionen an. Die Dienstpflichtigen können durch eigene Entscheidung Einfluss auf einen wesentlichen Abschnitt ihres beruflichen und sozialen Lebens nehmen. Erst wenn auch dieser Einplanungsversuch keinen Erfolg hat, kommt es zur Einberufung von Amts wegen.

Gegen das Verfahren des BAZ bestehen daher aus datenschutzrechtlicher Sicht keine Bedenken.

26.3 Kontrolle und Beratung einer Zivildienstgruppe und einer Verwaltungsstelle

Personenbezogene Daten von Personen, die durch Zivildienstleistende betreut werden, dürfen nicht in Akten einer Verwaltungsstelle oder einer Zivildienstgruppe gespeichert werden.

Das Bundesamt für den Zivildienst (BAZ) hat mit öffentlich-rechtlichen Verträgen eigene Verwaltungsaufgaben auf Verbände der freien Wohlfahrtspflege übertragen, die zu diesem Zweck Verwaltungsstellen eingerichtet haben. Die Auftragnehmer sind beliehene Unternehmer und unterliegen daher meiner datenschutzrechtlichen Kontrolle. Für Dienststellen, die keinem dieser Verbände angehören, werden diese Aufgaben von den Zivildienstgruppen des BAZ wahrgenommen. Hierzu gehören etwa die Einplanung anerkannter Kriegsdienstverweigerer in bestimmte Zivildienststellen und die Prüfung von Beschwerden sowohl von Zivildienstleistenden (ZDL) als auch von Zivildienststellen (ZDS).

Anlässlich einer Kontrolle bei einer Zivildienstgruppe und einer Verwaltungsstelle habe ich in beiden Einrichtungen in mehreren der geprüften Nebenakten der ZDS, die ZDL in der individuellen Schwerstbehindertenbetreuung einsetzen, personenbezogene Daten der betreuten Personen sowie von ZDL vorgefunden. Diese personenbezogenen Daten sind nicht in den Sachakten über die ZDS zu speichern, die personenbezogene Daten nur dann enthalten dürfen, wenn dies der Sachzusammenhang erfordert, wie beispielsweise den Namen des Beauftragten einer ZDS. Soweit eine Entfernung dieser Daten aus der ZDS-Nebenakte nicht möglich ist, weil es sich zwar um Vorgänge und Belange der Dienststelle handelt, aber in diesem Zusammenhang konkret Daten von ZDL betroffen sind, müssen die entsprechenden Daten unkenntlich gemacht werden, wie etwa durch Schwärzen. Ich habe mit den jeweiligen Stellen vereinbart, dass alle ZDS-Nebenakten im Rahmen der aktuellen Bearbeitung auf solche unzulässigen Daten durchgesehen und bereinigt werden.

In mehreren ZDS-Akten der ZDL, die in der Drogen- und Aids-Hilfe eingesetzt sind, befanden sich die kompletten Ergebnisse des sog. Drogenscreenings. Da nur die amtsärztlichen Unbedenklichkeitsbescheinigungen für die ZDL erforderlich sind, wird das BAZ diese Unterlagen an den behandelnden Arzt mit dem Hinweis zurücksenden, dass aus datenschutzrechtlichen Gründen nur die Unbedenklichkeitsbescheinigung benötigt wird.

27 Internationale Zusammenarbeit und Datenschutz im Ausland

Die Internationale Zusammenarbeit wurde weiter intensiviert. Ich habe angeregt, einen Anstoß zur Entwicklung einer verbindlichen globalen Datenschutzkonvention zu geben.

27.1 Ein Blick in europäische Länder außerhalb der Union

In europäischen Ländern, die nicht der EU angehören, kam der Datenschutz weiter gut voran.

Nachdem ich im Dezember 2002 die damals gerade ernannten Mitglieder der neu eingerichteten **bulgarischen** Datenschutzkommission zu einem Besuch in meiner Dienststelle empfangen hatte, bei dem sie sich über praktische Fragen der Beratung und Kontrolle sowie der Bearbeitung von Eingaben unterrichteten, hielt ich mich im Juli 2003 zu einem Gegenbesuch in Sofia und Varna auf. Bei den Gesprächen mit der Datenschutzkommission

standen Fragen der Unabhängigkeit der Kontrollstellen, der Umgang mit als geheim eingestuften personenbezogenen Daten sowie der grenzüberschreitende Datenverkehr im Vordergrund. Der Vorsitzende und Mitglieder des für Datenschutzfragen zuständigen Parlamentsausschusses für Innere Sicherheit und Öffentliche Ordnung berichteten über die Entstehung des bulgarischen Datenschutzgesetzes, an der der Ausschuss federführend beteiligt war. Auf Einladung des Vorsitzenden der Datenschutzkommission nahm ich an einem Gedankenaustausch über aktuelle Datenschutzfragen mit Mitgliedern des Parlamentsausschusses für Verkehr und Telekommunikation teil. Beim Treffen mit dem stellvertretenden bulgarischen Innenminister standen die Zusammenarbeit Bulgariens mit Europol, Fragen der Videoüberwachung und der Biometrie in Ausweisen und Pässen im Vordergrund. Von meinen Kollegen in Sofia wurde mir wiederholt versichert, dass ihr Besuch in Bonn und mein Gegenbesuch einen wesentlichen Anschub für den Datenschutz und den Bekanntheitsgrad ihrer Behörde in Bulgarien bedeuteten.

Hinsichtlich des Datenschutzniveaus in Drittländern hat die Europäische Kommission im Jahre 2004 die Angemessenheit des Schutzes personenbezogener Daten im Sinne von Artikel 25 Abs. 6 der EG-Datenschutzrichtlinie auf der Kanalinsel **Guernsey** und auf der **Isle of Man** festgestellt (ABl. Nr. L 151 vom 30. April 2004 S. 51, ABl. Nr. L 2008 vom 10. Juni 2004 S. 47). Zuvor hatte die Art. 29-Gruppe (vgl. Nr. 3.2.2) in den Stellungnahmen 5/2003 vom 13. Juni 2003 und 6/2003 vom 21. November 2003 auf der Grundlage ihrer eigenen Feststellungen die Gewährleistung eines angemessenen Datenschutzniveaus auf den Inseln befürwortet (WP 79, 82, vgl. Anlage 12).

27.2 Die Entwicklung im nicht-europäischen Ausland

Die „weißen Flecken" auf der Weltkarte des Datenschutzes sind auch in den vergangenen beiden Jahren weniger geworden, wozu vor allem die Entwicklungen in Asien und Südamerika, aber auch ein erster Schritt auf dem afrikanischen Kontinent beitragen.

Im März 2004 konnte ich eine Delegation der **Japan** Information Processing Development Corporation JIPDEC, einer Organisation des Wirtschaftsministeriums MITI, zu einem Gedankenaustausch über Probleme bei der elektronischen Signatur sowie zu Auditierungs- und Zertifizierungsfragen begrüßen und mich bei dieser Gelegenheit aus erster Hand über das zum 1. April 2005 in Kraft tretende japanische „Grundgesetz für den Datenschutz" unterrichten. Das Gesetz, das erstmals den öffentlichen und den nicht-öffentlichen Bereich gemeinsam regelt, zeichnet sich durch sehr allgemein gehaltene Bestimmungen aus, die durch detaillierte Regelungen auf dem Verordnungswege etwa auf den Gebieten Telekommunikation, Finanzdienstleistungen oder Gesundheitswesen ergänzt werden sollen. Das Grundgesetz des Datenschutzes, das bereits drei Jahre nach seinem Inkrafttreten wieder einer umfassenden Revision unterzogen werden soll, sieht weitgehende Ausnahmevorschriften vor und gilt für Behörden und Unternehmen nur, wenn diese die Daten von mindestens 5.000 Betroffenen verarbeiten. Die Einrichtung einer unabhängigen Datenschutzkontrollinstanz ist bislang nicht vorgesehen.

In **Malaysia** befinden sich die Arbeiten für ein Datenschutzgesetz noch immer im Entwurfsstadium beim zuständigen Ministerium für Energie, Kommunikation und Multimedia. Zwischenzeitlich haben bekannt gewordene Entwurfspassagen für Aufsehen gesorgt, wonach u. a. für das widerrechtliche Sichverschaffen von Daten eine Freiheitsstrafe von bis zu zwölf Jahren vorgesehen sein soll.

Im Juni 2003 lag in **Indien** der Regierungsentwurf eines Datenschutzgesetzes vor, dessen Zielrichtung nicht zuletzt darin lag, europäischen Unternehmen und solchen aus anderen Ländern mit Datenschutztradition die Auslagerung von Datenverarbeitungsprozessen zu erleichtern. Der Entwurf, der aus diesem Grunde die Erfüllung der Mindestanforderungen des europäischen Datenschutzrechts an ein angemessenes Datenschutzniveau vorgesehen hatte, wurde jedoch als Ergebnis einer Konferenz aus Regierungs- und Industrievertretern im Oktober 2003 wieder zurückgezogen. Stattdessen strebt die indische Regierung nunmehr an, die bereits bestehenden Regelungen des Information Technology Act aus dem Jahre 2000 auszubauen und ein Abkommen ähnlich dem Safe-Harbor-Konzept zwischen der Europäischen Union und den USA zu erzielen, um die Anforderungen der EU und anderer Staaten an ein adäquates Datenschutzniveau erfüllen zu können.

Auch ein **pakistanischer** Gesetzentwurf zum Datenschutz hat die Auslagerung der Datenverarbeitung durch ausländische Stellen im Auge und nennt dies in seiner Bezeichnung „Foreign Data Security and Protection Act" auch beim Namen.

In **Korea** hat das Innenministerium einen Gesetzentwurf zum Datenschutz für den öffentlichen Bereich angekündigt, mit dessen Einbringung im Parlament nicht vor dem Sommer 2005 gerechnet wird.

Schließlich wurde auf den **Seychellen** der Entwurf eines Datenschutzgesetzes im Parlament eingebracht, der im wesentlichen dem Datenschutzgesetz des Vereinigten Königreiches nachgebildet ist.

Chile hatte 1999 als erstes südamerikanisches Land die Verarbeitung personenbezogener Daten im öffentlichen und privaten Bereich gesetzlich geregelt, gefolgt von **Argentinien**, das sein Datenschutzgesetz als „Habeas Data" im wesentlichen auf das spanische Datenschutzgesetz und auf Elemente der EG-Datenschutzrichtlinie gründet. Mit Blick auf dieses Gesetz stellte die Europäische Kommission im Jahr 2003 die Angemessenheit des Schutzes personenbezogener Daten i. S. v. Artikel 25 Abs. 6 der EG-Datenschutzrichtlinie in Argentinien fest, nachdem die Art. 29-Gruppe (vgl. Nr. 3.2.2) in ihrer Stellungnahme 4/2002 vom 3. Oktober 2002 sich für die Gewährleistung eines angemessenen Datenschutzniveaus in Argentinien ausgesprochen hatte (WP 63, vgl. Anlage 12). Der dem **brasilianischen** Parlament vorliegende, im wesentlichen an die EG-Datenschutzrichtlinie

angelehnte Regierungsentwurf für ein allgemeines Datenschutzgesetz wurde noch nicht verabschiedet. Inzwischen liegen Entwürfe für allgemeine Datenschutzgesetze auch in **Mexiko** und **Uruguay** vor.

Ähnlich wie in Indien und Pakistan liegen auch in **Südafrika** die Motive für den Ende 2004 vorgelegten Regierungsentwurf eines Datenschutzgesetzes nicht zuletzt in der zunehmenden Auslagerung von Datenverarbeitungsaktivitäten durch verantwortliche Stellen in Europa und in den damit verbundenen Anforderungen an die Angemessenheit des Datenschutzniveaus im Empfängerland.

Im März 2004 konnte ich den **australischen** Datenschutzbeauftragten Mr. Crompton zu einem Gedankenaustausch in meiner Dienststelle begrüßen. Gegenstand der Gespräche waren u. a. die auf australische Initiative zustanden gekommene Entschließung der 25. Internationalen Datenschutzkonferenz 2003 in Sydney, die sich mit der Verbesserung der Bekanntmachung von Praktiken zum Datenschutz befasste (vgl. Nr. 27.3). Aus erster Hand konnte ich berichten, dass sich die Art. 29-Gruppe in Brüssel mit dem in Australien gewährleisteten Schutzniveau bei der Übermittlung von Fluggastdatensätzen von Fluggesellschaften beschäftigt hat. Die am 16. Januar 2004 verabschiedete Stellungnahme war zu dem – vorläufigen – Ergebnis gelangt, dass Australien ein angemessenes Schutzniveau im Sinne der EG-Datenschutzrichtlinie bietet (WP 85, vgl. Anlage 12).

Im Juli 2004 weilte die **kanadische** Datenschutzbeauftragte Ms. Jennifer Stoddart zu einem Besuch in meiner Dienststelle, bei dem wir einen Gedankenaustausch über die Schwerpunkte unserer aktuellen Arbeiten führten und ich über die laufenden Arbeiten der Art. 29-Gruppe (vgl. Nr. 3.2.2) berichtete. Angesichts ihres Besuches informierte mich meine kanadische Kollegin darüber, dass das kanadische Bundesdatenschutzgesetz für den privaten Bereich, der Personal Information Protection and Electronic Documents Act, dessen Anwendung bislang auf die dem Bundesrecht unterstehenden wirtschaftlichen Organisationen begrenzt war, sich seit dem 1. Januar 2004 auf alle Wirtschaftsunternehmen einschließlich der dem Provinzrecht unterliegenden Organisationen bezieht, es sei denn, dass eine Provinz Regelungen erlässt, die in der Substanz dem Bundesgesetz entsprechen. Dies gilt seit dem 1. Januar 2004 für das Datenschutzgesetz – den Personal Information Protection Act – von **British Columbia**, das damit nach **Quebec** als zweite Provinz den Datenschutz für den privaten Bereich regelt. Entsprechende Regelungen hat auch **Alberta** im Mai 2003 eingeführt, die jedoch noch nicht in Kraft getreten sind.

Das Ministerium für Telekommunikation und E-Commerce der **Bermudas** hat den Entwurf eines Datenschutzgesetzes ausgearbeitet, dessen Beratung im Kabinett zum Redaktionsschluss noch nicht abgeschlossen war und mit dessen parlamentarischer Befassung in der ersten Jahreshälfte 2005 gerechnet wird.

Die Datenschutzdiskussion mit den **USA** war in den zurückliegenden zwei Jahren vor allem durch die geforderte Weitergabe personenbezogener Daten durch Fluggesellschaften an amerikanische Behörden geprägt (zur sog. PNR-Diskussion vgl. Nr. 22.2). Von innenpolitischer Bedeutung waren vor allem das am 1. Januar 2004 in Kraft getretene Gesetz gegen den unaufgeforderten Versand von Spam-Mails und der Regierungsentwurf eines Änderungsgesetzes zum Fair Credit Reporting Act. Der sog. CAN SPAM (Controlling the Assault of Non-Solicited Pornography and Marketing) Act, der Vorrang vor bislang erlassenen bundesstaatlichen Gesetzen beansprucht, orientiert sich in seinen wesentlichen Bestimmungen an dem relativ strengen kalifornischen Anti-Spam-Act und sieht empfindliche Geldstrafen (bis zu 750 US-Dollar pro Spam-Mail) und Freiheitsstrafen (bis zu fünf Jahren in schweren Fällen) vor. Das Gesetz ist auch für ausländische Mail-Versender von Bedeutung, da es nach seinem Wortlaut für die Anwendung bereits ausreicht, wenn E-Mails zu kommerziellen Zwecken versandt werden und die Adressaten sich in den USA befinden, während es auf den Sitz des Absenders nicht ankommt. Die beabsichtigten Änderungen des Fair Credit Reporting Act gehen vor allem auf Besorgnisse aus Verbraucherkreisen ein, die im Zusammenhang mit dem Problem des „identity theft“ vorgebracht werden. Den Betroffenen soll künftig einmal im Jahr ein kostenfreier Zugang zu ihren Kreditdaten möglich sein, um diese im Hinblick auf Richtigkeit und Vollständigkeit überprüfen zu können. Unabhängig von der Jahresfrist ist unter bestimmten Umständen (z. B. im Fall von Rechtsstreitigkeiten) ein weiterer Datenzugang möglich, der ansonsten gebührenpflichtig ist. Darüber hinaus ist die Schaffung eines landesweiten Alarmsystems zur Meldung von Identity-Theft-Fällen geplant sowie eine umfassendere Unterrichtung der Betroffenen über die Zusammensetzung ihrer Kredit-Scorewerte.

Im August 2003 verabschiedete das Parlament des US-Staates **Kalifornien** den Financial Information Privacy Act, der Banken und andere Finanzdienstleister zur Einholung der Einwilligung ihrer Kunden vor der Weitergabe von deren Daten an andere Unternehmen verpflichtet. Außerdem können die Kunden für ein opting-out votieren, wenn sie nicht mit der Weitergabe ihrer Daten innerhalb des Unternehmens einverstanden sind. Zum 1. Juli 2004 ist der kalifornische Online Privacy Protection Act in Kraft getreten, der allen online datenverarbeitenden Unternehmen – soweit noch nicht geschehen – die Einführung einer privacy policy vorschreibt. Diese muss über Einzelheiten der praktizierten und beabsichtigten Datenverarbeitungen sowie über die Datenempfänger Auskunft geben und die Betroffenen auf ihre Zugangsmöglichkeiten zu den über sie gespeicherten Daten und ihre Berichtigungsmöglichkeiten hinweisen.

27.3 Die Internationale Datenschutzkonferenz

Die 25. und die 26. Internationale Datenschutzkonferenz in Sydney bzw. Wroclaw befassten sich mit einer Reihe von staatenübergreifenden Themenschwerpunkten und verabschiedeten so viele Entschließungen wie nie zuvor in einem Berichtszeitraum.

Die 25. und die 26. Internationale Datenschutzkonferenz fanden vom 10. bis 12. September 2003 in Sydney und vom 14. bis 16. September 2004 in Wroclaw statt. Wie in den vergangenen Jahren (vgl. zuletzt 19. TB Nr. 32.5) führten die Tagungen die Vertreter von Datenschutzbehörden aus aller Welt mit Repräsentanten von internationalen Organisationen und Vertretern aus Wissenschaft, Wirtschaft und Verwaltungen zu einem umfassenden Gedankenaustausch zusammen.

Die 25. Internationale Datenschutzkonferenz von Sydney stand unter dem Leitthema „Practical Privacy for People, Government and Business“ und verabschiedete fünf Entschließungen zu den Themen

- Automatische Software-Aktualisierungen (vgl. Anlage 4)
- Transfer von Passagierdaten (vgl. Anlage 5)
- Datenschutz und internationale Organisationen (vgl. Anlage 6)
- Verbesserung der Bekanntmachung von Praktiken zum Datenschutz (vgl. Anlage 7)
- Radio Frequency Identification (vgl. Anlage 8).

Die Nutzung der Radio Frequency Identification Technologie, ihre Auswirkungen auf die Privatsphäre der Bürger und die daraus resultierenden Herausforderungen für den Datenschutz bildete auch einen der Themenschwerpunkte der 26. Internationalen Konferenz von Wroclaw (vgl. auch Nr. 4.2.1). Daneben ist aus der Vielfalt der behandelten Themen das Problem der Abwägung zwischen den Erfordernissen der öffentlichen Sicherheit und den Grundrechtspositionen der Betroffenen – in diesem Zusammenhang referierte eine Vertreterin des US-Heimatschutzministeriums aus erster Hand über die Vorgaben des US Patriot Act – hervorzuheben sowie die Erörterung aktueller Fragen zu den Gefahren für die Privatsphäre durch die Printmedien und das Internet sowie durch das politische Marketing.

Die Internationale Konferenz von Wroclaw verabschiedete Resolutionen

- zum Entwurf eines ISO-Rahmenstandards zum Datenschutz (vgl. Anlage 9)
- zur Änderung der Entschließung der Konferenz 2003 zur automatischen Software-Aktualisierung (vgl. Anlage 10)
- zur Zulassung weiterer Teilnehmer zur Internationalen Datenschutzkonferenz (Accreditation Resolution, vgl. Anlage 11).

Ein wichtiges Thema war der Globalisierung der Datenverarbeitung und deren Konsequenzen für den Datenschutz gewidmet. Angesichts aller bisherigen, regional begrenzt gebliebenen Ansätze habe ich die Notwendigkeit eines wirksamen globalen Datenschutzes dargestellt und ausgeführt, dass sich nach dem großen Erfolg des europäischen Datenschutzes die Frage nach einem völkerrechtlich verbindlichen globalen Datenschutz stelle.

Die nächste Internationale Konferenz, die im September 2005 in Montreux/Schweiz unter dem Motto „The protection of personal data and privacy in a globalised world: A universal right respecting the diversities“ stattfinden soll, wird dazu Gelegenheit geben.

27.4 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Die OECD zeigt ein großes Interesse an der Zusammenarbeit mit der Art. 29-Gruppe und den nationalen Kontrollstellen. Bei Fragen der Biometrie in Reisedokumenten unterstützt die OECD die europäische Datenschutzposition.

Anlässlich meines Treffens mit Vertretern der OECD im Juni 2004 in Paris stieß ich auf ein erfreulich großes Interesse an einer Vertiefung der Beziehungen mit den nationalen Datenschutzkontrollinstanzen sowie der Brüsseler Art. 29-Gruppe (vgl. Nr. 3.2.1). Als Vorsitzender der Art. 29-Gruppe habe ich mich insbesondere über den Vorschlag gefreut, informelle Konsultationen oder Zusammenkünfte etwa in Form von Workshops abzuhalten, wenn Themen von gemeinsamen Interesse berührt sind. Aus dem Berichtszeitraum hervorzuheben sind die gemeinsamen Arbeiten der OECD und der International Civil Aviation Organization (Internationale Zivilluftfahrt-Organisation – ICAO) an Richtlinienentwürfen über die Nutzung von Biometrie in internationalen Reisedokumenten (vgl. auch Nr. 6.2 zur Biometrie in Pässen und Visen). Das Bestreben der OECD ist dabei vor allem darauf gerichtet, die Ziele und Ergebnisse der zahlreichen internationalen Arbeitsprojekte zur Biometrie zu harmonisieren. Großen Wert legt die OECD in diesem Zusammenhang auf eine Übereinstimmung mit den von der Art. 29-Gruppe in ihrer Stellungnahme 07/2004 vom 11. August 2004 gefundenen Ergebnissen (WP 96, vgl. Anlage 12).

28 Aus meiner Dienststelle

28.1 Umzug des BfD im Jahr 2003

Umzug des BfD und Büros in Berlin

Seit ihrer Errichtung im Jahr 1977 war meine Dienststelle in verschiedenen angemieteten Gebäuden in Bonn untergebracht. Im November 2003 konnte sie in ein bundeseigenes Gebäude in der Husarenstraße 30 in 53117 Bonn, das als Folge des Umzugs von Parlament und Teilen der Bundesregierung freigeworden war, umziehen.

In Berlin stehen meinen Mitarbeitern, die sich als Dienstreisende dort aufhalten, und mir im Dienstgebäude des Bundesministeriums des Innern seit Oktober 2004 Arbeitsplätze in zwei Büroräumen zur Verfügung. Durch Inanspruchnahme dieser Räume sollen zeitliche und personelle Ressourcen besser genutzt werden. Ob die Räume bzw. der Standort den Anforderungen im vollem Umfang gerecht wird, bleibt abzuwarten.

28.2 Der Datenschutzbeauftragte im Internet

Das Informationsangebot des BfD im Internet wird von einer großen Anzahl von Nutzern in Anspruch genommen. Die Homepage meiner Dienststelle ist unter der Adresse http://www.bfd.bund.de oder http://www.datenschutz.bund.de erreichbar.

Neben der konventionellen Öffentlichkeitsarbeit gewinnt das Internet als allgemeine Informations- und Kommunikationsplattform ständig an Bedeutung. Aus diesem Grund hat der Ausbau des Internetangebots meiner Dienststelle für mich eine hohe Priorität.

Bereits jetzt werden in dem Internetangebot des BfD eine Vielzahl aktueller Informationen (insbesondere Pressemitteilungen, Redetexte, Entschließungen der Datenschutzkonferenzen und Veranstaltungshinweise) und vielfältige Grundlagentexte (z. B. Gesetze, Orientierungshilfen zur Datensicherheit, Tätigkeitsberichte des BfD und von europäischen Datenschutzkontrollinstitutionen) bereit gehalten.

Im Berichtszeitraum waren ca. 7,9 Millionen Seitenanfragen zu verzeichnen. Das entspricht im Durchschnitt etwa 10 800 Seitenanfragen pro Tag.

Die meisten Zugriffe entfielen mit ca. 75 Prozent auf die Rubrik Materialien zum Datenschutz, die unter anderem Tätigkeitsberichte, Informationsbroschüren BfD-Info 1 bis 5 wie auch Entschließungen der Datenschutzkonferenzen und einschlägige Gesetze und Verordnungen enthält.

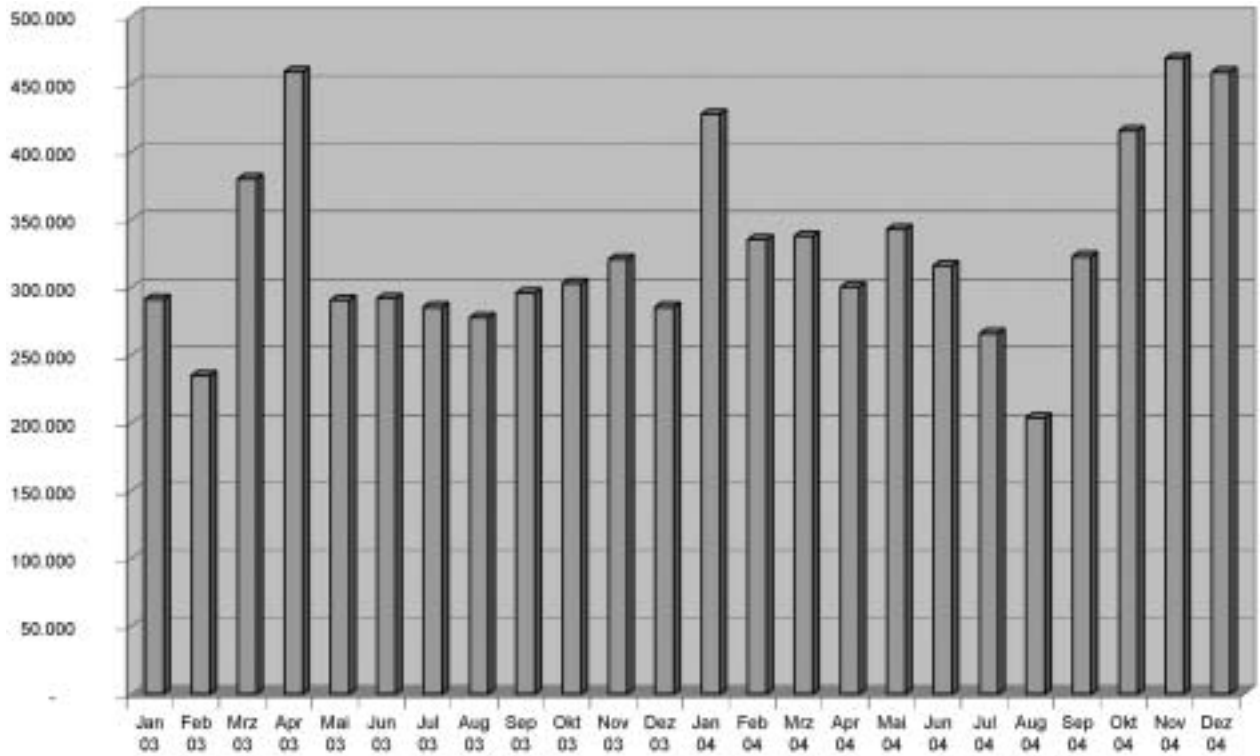
Die Website des BfD unterliegt einer ständigen Weiterentwicklung. Dabei geht es zum einen um die Erweiterung des Informationsangebots, zum anderen um die Verbesserung der Nutzbarkeit durch neue Funktionen, die die vielfältigen Informationen besser erschließbar machen. So wurde im Dezember 2003 eine Suchmaschine in Betrieb genommen, die das Auffinden bestimmter Informationstexte erleichtert.

Seit Oktober 2004 wird ein interaktives Formular bereitgestellt, mit dem Bürgerinnen und Bürger ihre Eingaben in geschützter Form über das Internet an mich senden können. Die Anwendung wurde in Zusammenarbeit mit der Fachhochschule des Bundes entwickelt. Es ist sichergestellt, dass die in Eingaben enthaltenen sensiblen Daten kryptographisch verschlüsselt und damit gegen unbefugte Kenntnisnahme und Veränderung geschützt übertragen werden.

Diese Maßnahmen sowie weitere geplante Verbesserungen sind mit dem eGovernment-Projekt der Bundesregierung, BundOnline 2005, abgestimmt. Mitte 2004 habe ich eine Projektgruppe eingesetzt, die mein Internetangebot weiter ausbauen und optimieren soll. Dabei wird besonderer Wert auf die einfache Erschließbarkeit der Informationen gelegt.

Abbildung 10 (zu Nr. 28.2)

Internetzugriffe im Berichtszeitraum



Von zunehmender Bedeutung für die Wahrnehmung des Datenschutzes in der Öffentlichkeit ist auch das „Virtuelle Datenschutzbüro“, das von dem ehemaligen schleswig-holsteinischen Datenschutzbeauftragten Helmut Bäumler initiiert wurde und unter meiner Mitwirkung weiterhin vom ULD Schleswig-Holstein betrieben wird (www.datenschutz.de). Es dient der besseren Zusammenarbeit der Datenschutzbehörden und bietet zudem einen guten Startpunkt für Internetnutzer, die sich für Datenschutzfragen interessieren.

28.3 Erfolgreicher Auftritt bei der CeBIT 2004

Erstmals konnten Datenschutzthemen auf einer internationalen Messe einem interessierten Publikum unter dem Motto „Erfolg mit Datenschutz“ näher gebracht werden – Fortsetzung folgt ...

Unter dem Leitthema „Deutschland Online – eGovernment in Stadt, Land, Bund“ präsentierten sowohl öffentliche Stellen wie auch Wirtschaftsunternehmen im Ausstellungsbereich „PublicSectorParc“ ihre eGovernment-Projekte. Dabei standen Themen wie elektronische Gesundheitskarte, JobCard, Biometrie und Internetnutzung ganz weit oben auf der Interessenskala der Besucher. Die Besucher begrüßten insbesondere, dass im Ausstellungsbereich neben den doch sehr technischen Projektpräsentationen, noch ergänzende, für die Umsetzung von Projekten sehr hilfreiche Informationen zum Datenschutz und zur Datensicherheit angeboten wurden.

Das enorme Interesse an Themen des Datenschutzes – allein über sechshundert registrierte Besucher am Stand – sprechen dafür, auch künftig auf der CeBIT präsent zu sein, also: Fortsetzung folgt!

28.4 Ein sicherer Dienst: Erfahrungen mit dem mobilen Zugang

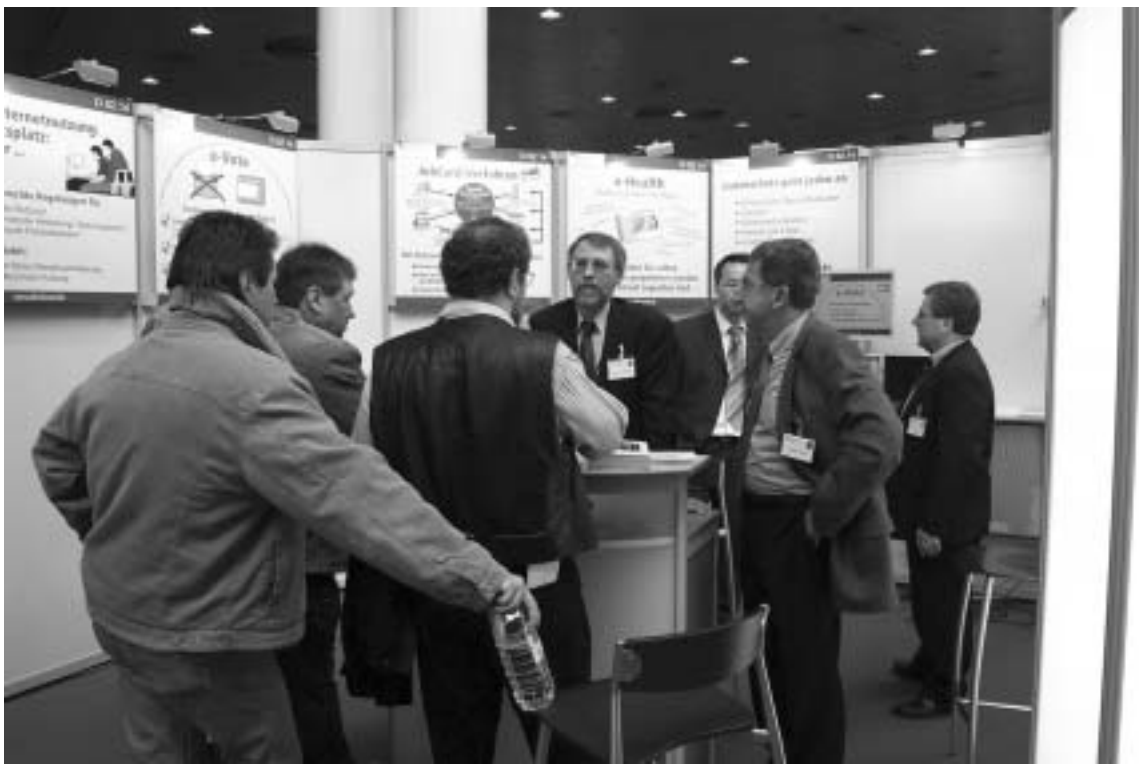
Auch wenn Mitarbeiter auf Dienstreisen sind, muss eine reibungslose Zusammenarbeit untereinander sichergestellt sein. Gleiches gilt für Telearbeitsplätze.

Meine Mitarbeiter und ich sind häufig auf Dienstreisen. Auch hier besteht die Notwendigkeit, auf aktuelle Dokumente meines Hauses zugreifen zu können oder beispielsweise E-Mails direkt aus meiner Dienststelle abrufen zu können. Dabei müssen allerdings Datenschutz, Datensicherheit und IT-Sicherheit gewahrt bleiben.

Schon seit einiger Zeit hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit der Telekom Systems International, die den Informationsverbund Berlin/Bonn (IVBB) betreibt, ein System in Betrieb, das dieses Problem zu lösen hilft. In meinem Haus wurde dazu ein sog. Gateway–Rechner installiert, der das Hausnetz mit dem Gateway–Rechner im IVBB verbindet. Dieser wiederum kann getunnelte und verschlüsselte Verbindungen ins Internet herstellen. Mit einem entsprechenden Client ausgestattet, kann man sich mit dem Gateway-Rechner im IVBB verbinden und dann gesichert Daten mit dem eigenen Hausnetz austauschen.

Abbildung 11 (zu Nr. 28.3)

CeBIT 2004



Mit Hilfe der vom BSI vorgegebenen Software ergeben sich nun eine ganze Reihe von sicheren Kommunikationsmöglichkeiten. Der Zugriff in das Hausnetz ist über verschiedene Telekommunikationstechniken möglich. Die Verbindung kommt dabei immer verschlüsselt und getunnelt zustande. Ich habe mit derselben Technik in meiner Dienststelle auch Telearbeitsplätze angeschlossen, für die ebenfalls ein hoher Sicherheitsstandard gewährleistet ist.

28.5 Referendare und Praktikanten beim BfD

BfD als Ausbildungsbehörde

Im Berichtszeitraum war eine weiter steigende Zahl von Anfragen nach Praktika in meiner Dienststelle zu verzeichnen. Vor allem interessierten sich Studenten der Rechtswissenschaft und Rechtsreferendare für Themen des Datenschutzes. Gerne haben meine Mitarbeiter und ich diesen Wünschen entsprochen. So konnten in den Jahren 2003 und 2004 mehr als 20 Studenten und Referendare Teile ihrer Ausbildung in meinem Hause absolvieren. Die uneingeschränkt positiven Erfahrungen auf beiden Seiten sind Anlass, auch künftig alle Möglichkeiten zu nutzen, um an der Ausbildung junger Menschen mitzuwirken.

29 Wichtiges aus zurückliegenden Tätigkeitsberichten

1. In meinem 19. TB (Nr. 7.10) hatte ich über die datenschutzrechtliche Begleitung verschiedener Projekte und Verfahren im Zusammenhang mit der **Wiedergutmachung für NS-Opfer** berichtet. Diese sind im Berichtszeitraum fortgeführt und weitgehend zum Abschluss gebracht worden. Bei der Tätigkeit der Stiftung „Erinnerung, Verantwortung und Zukunft“ (19. TB Nr. 7.10.1) und in Verbindung damit beim Projekt zur Nachweisbeschaffung für ehemalige NS-Zwangsarbeiter (19. TB Nr. 7.10.2) haben sich bislang keine weiteren datenschutzrechtlichen Probleme ergeben. Hier wird in Zukunft nach endgültigem Abschluss der Projekte die Frage zu klären sein, wie mit den entstandenen Datenbeständen zu verfahren ist.

   Auch das Projekt zur Entschädigung von Holocaust-Opfern durch die Versicherungswirtschaft (19. TB Nr. 7.10.3) konnte erfolgreich vorangetrieben werden. Die Bundesanstalt für Finanzdienstleistungsaufsicht erstellte – von mir datenschutzrechtlich begleitet – eine Gesamtliste von deutschen Lebensversicherungspoliceninhabern der Jahre 1920 bis 1945 und glich diese im Wege der Auftragsdatenverarbeitung entsprechend einem Abkommen zwischen der International Commission on Holocaust Era Insurance Claims (ICHEIC), der Stiftung „Erinnerung, Verantwortung und Zukunft“ und dem Gesamtverband der Deutschen Versicherungswirtschaft e.V. mit einer Liste jüdischer Einwohner der Jahre 1933 bis 1945 (Residentenliste) ab. Das Ergebnis dieses Abgleichs wurde von der ICHEIC im Internet veröffentlicht. Um die Persönlichkeitsrechte der Betroffenen zu wahren, wurden diese in einem vorangestellten besonders hervorgehobenen Text auf die Möglichkeit hingewiesen, einer Veröffentlichung in der Liste zu widersprechen. Dieses Verfahren war mit mir und der AG Versicherungswirtschaft des Düsseldorfer Kreises abgesprochen.

2. Bereits in der Vergangenheit hatte ich ausführlich über die Maßnahmen des Deutschen Presserates berichtet, mit denen die gesetzlichen Ausnahmen beim **Datenschutz in den Redaktionen von Zeitungen und Zeitschriften** durch Selbstregulierung und Selbstkontrolle ausgeglichen werden sollen (18. TB Nr. 31.5; 19. TB Nr. 34, dort Nr. 15). Hierbei wurden im Berichtszeitraum weitere Fortschritte erzielt, über die der Deutsche Presserat in seinem im Jahre 2004 vorgelegten ersten Bericht zum Redaktionsdatenschutz und auf einem Symposium „Pressefreiheit und Datenschutz“ am 24. November 2004 informiert hat. Zwar weist dieses System der freiwilligen Selbstkontrolle immer noch Lücken auf, weil bislang nicht alle Zeitungs- und Zeitschriftenverlage die erforderlichen Selbstverpflichtungserklärungen abgegeben haben, mittlerweile nimmt aber die ganz überwiegende Zahl der betroffenen Verlage am Kontrollsystem teil, insbesondere auch im Bereich der Anzeigenblätter, die im übrigen dem Deutschen Presserat nicht angehören. Dieser hat versichert, in seinen Anstrengungen nicht nachzulassen, die datenschutzrechtliche Selbstkontrolle flächendeckend zu etablieren. Die bisherige Spruchpraxis des Beschwerdeausschusses zum Redaktionsdatenschutz lässt erkennen, dass dieser die Belange des Datenschutzes ernsthaft verfolgt und in ein ausgewogenes Verhältnis zum Informationsauftrag der Printmedien zu bringen versucht. Nach einer ersten Zwischenbilanz kann ich daher feststellen, dass sich Selbstregulierung und Selbstkontrolle in diesem speziellen Bereich grundsätzlich bewährt haben.

3. Gemäß § 14 Abs. 4 Umsatzsteuergesetz – eingeführt durch das Steuerverkürzungsbekämpfungsgesetz (StVBG) vom 19. Dezember 2001 – muss eine **Rechnung,** deren Gesamtbetrag 100 Euro übersteigt, seit dem 1. Juli 2002 u. a. die dem leistenden Unternehmer vom Finanzamt erteilte **Steuernummer** oder die ihm vom Bundesamt für Finanzen erteilte Umsatzsteuer-Identifikationsnummer enthalten (vgl. 19. TB Nr. 9.2.2).

   Hier hat sich herausgestellt, dass die in Eingaben formulierten Bedenken, die Steuernummer könnte zum Erfragen von Steuerdaten bei den Finanzämtern durch Unbefugte genutzt werden, nach Aussage der für den Datenschutz bei den Finanzämtern zuständigen LfD unbegründet sind. Demnach existieren ausführliche Weisungen an die Finanzämter zur Auskunftserteilung und die Finanzämter werden laufend über stattgefundene fingierte Anfragen informiert. Dementsprechend liegen dort auch keine Fälle vor, in denen Unbefugten Steuerdaten mitgeteilt wurden.

   Deshalb hatte ich bislang keine grundsätzlichen datenschutzrechtlichen Bedenken mehr gegen die

Pflicht zur Angabe der Steuernummer auf Rechnungen. Jedoch hat dieses Thema vor dem Hintergrund bestehender Missbrauchsmöglichkeit im Verfahren ELSTER erneut an Bedeutung und Aktualität gewonnen (vgl. Nr. 8.6).

4. Die **fiscus GmbH** wurde vom Bund und 15 Ländern als privatrechtlich organisierte Gesellschaft mit der Aufgabe, steuerliche Software für die Finanzverwaltung zu entwickeln und zu pflegen, gegründet. Sie ist ausschließlich im Auftrag ihrer Gesellschafter als deren Dienstleister tätig.

   Mit den Datenschutzbeauftragten der Länder habe ich von Anfang an eine enge datenschutzrechtliche Betreuung des Projekts angestrebt.

   Dem steht jedoch die Auffassung des BMF entgegen, das keine Veranlassung für eine unmittelbare Kontaktaufnahme der Datenschutzbeauftragten mit der fiscus GmbH sieht, da die fachlichen Vorgaben nicht von der GmbH verantwortet würden. Ich teile diese Auffassung nicht und werde gemeinsam mit den Datenschutzbeauftragten der Länder das Projekt fiscus GmbH auch weiterhin beobachten, um bereits frühzeitig bei der Entwicklung steuerlicher Software datenschutzrechtliche Anforderungen bei der weiteren Automatisierung der Finanzverwaltung durchzusetzen (vgl. auch Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom Oktober 2004, Kasten zu Nr. 29.4).

5. Im Jahre 2004 habe ich die Verarbeitung personenbezogener Daten im Verfahren **Steuerlicher Internetabgleich – STINA –** beim Bundesamt für Finanzen (BfF) in Bonn kontrolliert. In diesem Verfahren findet ein automatisierter Abgleich der Daten im Internet tätiger deutscher Unternehmer mit der beim BfF geführten Unternehmerdatenbank statt. Die dabei ermittelten Daten nicht steuerlich registrierter Unternehmer werden anschließend automatisiert an die zuständigen Landesfinanzbehörden weitergegeben.

   Gem. § 5 Abs. 1 Nr. 17 Finanzverwaltungsgesetz ist das BfF für die Beobachtung von elektronisch angebotenen Dienstleistungen zur Unterstützung der Landesfinanzverwaltungen bei der Umsatzbesteuerung des elektronischen Handels zuständig. Die Internetrecherche (Beobachtung) sowie Anfertigung und Übermittlung von Kontrollmaterial für bzw. an die Landesfinanzbehörden (Unterstützung) entsprechen dieser Aufgabe. Jedoch umfasst diese Vorschrift nach meiner Auffassung nicht den automatisierten Abgleich.

   Entgegen der Auffassung des BMF sehe ich auch in § 30 Abs. 4 Nr. 1 AO keine Ermächtigung für die Finanzverwaltung zu einem automatisierten Abgleich, da hier lediglich von der „Offenbarung“ der erlangten Kenntnisse die Rede ist. Die diesbezüglichen Gespräche mit dem BMF waren bei Redaktionsschluss noch nicht abgeschlossen.

6. In meinem 18. TB (Nr. 20.4) hatte ich darüber berichtet, dass für die Beurteilung von Leistung und Verhalten Arbeitsloser bei der Durchführung von Fortbildungs- und Trainingsmaßnahmen, die die Agentur für Arbeit angeordnet hat, keine Rechtsgrundlage besteht. In dem Gesetz zur Reform der arbeitsmarktpolitischen Instrumente vom 10. Dezember 2001 (Job-AQTIV-Gesetz, BGBl. I S. 3443) hat der Gesetzgeber meine Hinweise zum Teil aufgegriffen und für die Teilnehmer an einer beruflichen Aus- oder Weiterbildung geregelt, dass diese verpflichtet sind, „eine Beurteilung ihrer Leistung und ihres Verhaltens durch den Träger zuzulassen“ (§ 318 Abs. 2 Satz 1 Nr. 2 SGB III – vgl. 19. TB Nr. 23.3).

Kasten zu Nr. 29.4

Entschließung der 68. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 28. und 29. Oktober 2004

Datensparsamkeit bei der Verwaltungsmodernisierung

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Bemühungen, Dienstleistungen der öffentlichen Verwaltung bürgernäher und effizienter zu erbringen. Sie fordern, dass im Zug von Maßnahmen der Verwaltungsreform die sich dadurch bietenden Möglichkeiten genutzt werden, um das Datenschutzniveau zu verbessern. Verwaltungsvereinfachung muss auch dazu genutzt werden, weniger personenbezogene Daten zu verarbeiten. Künftig müssen Verfahren und Datenflüsse wesentlich besser überschaubar und nachvollziehbar sein. Besonders sollen die Möglichkeiten der Technik genutzt werden, Risiken zu minimieren, die mit der Zentralisierung von Datenbeständen verbunden sind.

Werden Rechtsvorschriften, etwa im Steuerrecht oder im Arbeits- und Sozialrecht und hier insbesondere bei Änderungen in den Systemen der sozialen Sicherung, mit dem Ziel der Verwaltungsvereinfachung erlassen, sind die Auswirkungen auf den Datenschutz frühzeitig zu prüfen. Im Ergebnis müssen die Normen den gesetzlich verankerten Grundsatz der Datenvermeidung umsetzen und somit das Recht auf informationelle Selbstbestimmung gewährleisten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deswegen, bei Vorschlägen zur Verwaltungsvereinfachung und darüber hinaus bei allen Regelungsvorhaben darauf zu achten, dass das damit verbundene Potential an Datensparsamkeit und Transparenz ausgeschöpft wird.

Hierzu ist eine Folgenabschätzung auf mögliche Beeinträchtigung der informationellen Selbstbestimmung vorzunehmen. Die Ergebnisse sind in geeigneter Form zu dokumentieren.

Nicht geregelt wurde jedoch die **Beurteilung von Teilnehmern an Maßnahmen nach den §§ 48 ff. SGB III.** Es handelt sich hierbei vor allem um Maßnahmen, die zur Verbesserung der Eingliederungsaussichten von Arbeitslosen oder von Arbeitslosigkeit bedrohten Arbeitssuchenden beitragen sollen (Maßnahmen der Eignungsfeststellung, Trainingsmaßnahmen). Dies führte vor allem im Bereich der Trainingsmaßnahmen zu einer Reihe von Eingaben, in denen sich Arbeitssuchende darüber beklagten, dass ihre Leistung und ihr Verhalten von Maßnahmeträgern beurteilt und diese Beurteilungen der Agentur für Arbeit übermittelt wurden (vgl. 19. TB Nr. 23.3).

Das BMWA hat meinen Vorschlag zur Schaffung einer Ermächtigungsgrundlage für die Beurteilung der Leistung und des Verhaltens einer nach § 48 SGB III geförderten Person durch den Träger der Maßnahme aufgegriffen. Durch das Dritte Gesetz für moderne Dienstleistungen am Arbeitsmarkt vom 23. Dezember 2003 (BGBl. I S. 2848) wurde § 318 Abs. 2 Satz 1 Nr. 2 SGB III um die Verpflichtung der Betroffenen erweitert, solche Beurteilungen zuzulassen.

7. Im 19. Tätigkeitsbericht habe ich unter Nr. 21.2.3.1 über den Umgang mit sensiblen medizinischen Daten von Beschäftigten bei der Deutschen Post AG berichtet. Zwischenzeitlich hat mir die **Deutsche Post AG** Entwürfe verschiedener Anweisungen zum Umgang mit Daten zum Gesundheitszustand von Beschäftigten mit der Bitte um datenschutzrechtliche Prüfung und Bewertung vorgelegt, die im Zusammenhang mit der Einführung eines **„Gesundheitsmanagements“** stehen. Ich habe zu diesen Entwürfen umfangreiche Hinweise zur datenschutzgerechten Ausgestaltung gegeben. Da die Deutsche Post AG meinen Vorschlägen entsprochen hat, gehe ich davon aus, dass die klaren Vorgaben, insbesondere zum Umgang mit ärztlichen Bescheinigungen, Befunden und Diagnosen, zu einer datenschutzgerechten Verfahrensweise führen. Zur konkreten Umsetzung hat die Deutsche Post AG zudem zugesagt, die entsprechenden Anweisungen zum Umgang mit Gesundheitsdaten von Beschäftigten durch gezielte Schulungsveranstaltungen vor Ort bekannt und transparent zu machen. Wichtig für die Wahrung der Datenschutzrechte der Mitarbeiterinnen und Mitarbeiter wird darüber hinaus auch eine interne stichprobenartige Kontrolle der praktischen Umsetzung sein.

8. Im 19. Tätigkeitsbericht (Nr. 26.5) hatte ich darüber berichtet, dass verschiedene **Staatsanwaltschaften** von den technischen Aufsichtsdiensten der Unfallversicherungsträger **Untersuchungsberichte** anforderten. Dabei hatten die Staatsanwaltschaften in § 69 Abs. 1 SGB X eine ausreichende Übermittlungsnorm gesehen und auf die in der tatsächlich anwendbaren Spezialregelung des § 73 SGB X vorgesehene richterliche Anordnung verzichtet. Das BMGS teilt meine rechtliche Bewertung, sieht jedoch keinen Handlungsbedarf, da eine eindeutige gesetzliche Regelung bestehe. Deswegen haben sich einige Unfallversicherungsträger an das Bayerische Staatsministerium der Justiz gewandt. Die dargestellte Problematik des Sozialdatenschutzes soll nun mit den Leitern der bayerischen Staatsanwaltschaften erörtert werden. Ich hoffe, durch ein solches Gespräch wird sich die Sensibilität in Fragen des Sozialdatenschutzes erhöhen.

9. In meinem 19. TB hatte ich über einen Einzelfall berichtet, der sich mit einem **Verwertungsverbot** bei unzulässiger Erhebung und Nutzung eines Obduktionsergebnisses befasste. Das Landessozialgericht Nordrhein-Westfalen hatte im Berufungsverfahren ein Verwertungsverbot bei der Verletzung datenschutzrechtlicher Vorschriften generell abgelehnt. Nunmehr liegt der Rechtsstreit dem Bundessozialgericht zur Entscheidung vor. Über den Ausgang dieses Verfahrens und die Bedeutung der datenschutzrechtlichen Regelungen werde ich weiter berichten.

10. In meinem letzten Tätigkeitsbericht (19. TB Nr. 12.7) habe ich über das neue Verfahren der Deutschen Post AG bei der Paketzustellung informiert. Da das System der **Packstationen** von den Kunden gut angenommen wurde, baute die Deutsche Post AG das Netz der Packstationen bis Ende 2004 um rund 500 weitere Packstationen aus. Erfreulich: Im Berichtszeitraum gab es kaum Beschwerden hierzu.

11. Dagegen führte die Handhabung bei der **Paketabholung** insbesondere in den Filialen der Deutschen Post AG zu vielen Nachfragen. In meinem 19. Tätigkeitsbericht (Nr. 12.3) habe ich auf die rechtmäßige Möglichkeit aller Postdienstunternehmen hingewiesen, bei Abholung eines Pakets in ihrer Niederlassung die (**Personal-**) **Ausweisdaten** zu erfassen und zu speichern, um die ordnungsgemäße Ausführung ihrer Dienstleistung nachweisen zu können. Aus datenschutzrechtlicher Sicht ist dieses Verfahren nicht zu beanstanden. Es entspricht der Regelung in § 8 Postdienste-Datenschutzverordnung, die das Interesse des Bürgers an einem maßvollen Umgang mit seinen persönlichen Daten als auch das Interesse der Postdienstunternehmen, Postdienstleistungen ordnungsgemäß zu erbringen, ausgewogen berücksichtigt. In bilateralen Gesprächen mit den Postdienstunternehmen habe ich darauf hingewirkt, die Mitarbeiterinnen und Mitarbeiter in den Filialen und Agenturen besser zu schulen, damit sie den Kunden entsprechend kompetent Auskunft geben können.

12. Bereits in meinen beiden letzten Tätigkeitsberichten habe ich über die nicht zum Ziel geführten Versuche des Gesetzgebers berichtet, Regelungen für ein **Register unzuverlässiger Unternehmer** zu schaffen. In dieser Legislaturperiode soll nun eine Neuordnung des gesamten Vergaberechts erfolgen, in deren Zusammenhang auch dieser Themenkomplex behandelt werden wird.

13. Durch die Regelungen des Terrorismusbekämpfungsgesetzes und des Zuwanderungsgesetzes hat sich die Einführung einer **Smartcard im Asylverfahren** erledigt. Diese Karte sollte ursprünglich nach dem Wunsch der Ständigen Konferenz der Innenminister und -senatoren der Länder die Angaben zur Aufenthaltsgestattung und Duldung von Asylbewerbern dokumentieren (vgl. zuletzt 18. TB Nr. 34, dort Nr. 2). Die Überlegungen des BMI gehen nunmehr auch hinsichtlich des Einsatzes biometrischer Daten in eine andere Richtung (vgl. Nr. 6.2). Die Ergebnisse der 1998 erstellten Machbarkeitsstudie zum Einsatz einer Smartcard im Asylverfahren spielen dabei keine Rolle mehr.

14. Gemäß § 22 AZRG i.V.m § 10 AZRG-Durchführungsverordnung sind Polizeibehörden berechtigt, nach entsprechender Zulassung durch das Bundesverwaltungsamt Daten des Ausländerzentralregisters (AZR) im automatisierten Verfahren abzurufen. In meinem 18. Tätigkeitsbericht (Nr. 5.1.4) hatte ich die Praxis sog. **Stellvertreterabfragen durch die Polizeibehörden beim AZR** kritisiert. Dabei rufen Polizeistellen stellvertretend für benachbarte Polizeistellen Daten im automatisierten Verfahren ab, während die ursprünglich anfragende Stelle entgegen den Protokollierungsvorschriften des AZRG über die Protokolldatei nicht ausgewertet werden kann. Um sicherzustellen, dass auch bei Stellvertreterabfragen zu erkennen ist, für welche Behörde der Abruf erfolgt ist, hatte das BMI 2003 einen Regelungsvorschlag erarbeitet, dem seinerzeit alle Länder mit Ausnahme Bayerns zustimmten. Da ich mich den Einwänden Bayerns zu diesem ersten Vorschlag – statt des Namens sollte auch die Funkrufbezeichnung des Veranlassenden protokolliert und an das AZR übermittelt werden – nicht verschließen konnte, hat das BMI ihn in Absprache mit mir modifiziert. Eine Identifikation des datenschutzrechtlich Verantwortlichen ist somit sichergestellt. Ich gehe davon aus, dass die Innenminister und -senatoren – soweit noch nicht geschehen – ihre Polizeibehörden veranlassen, künftig bei Stellvertreterabfragen entsprechend dieser Vereinbarung zu verfahren.

15. Das **Suchdienstedatenschutzgesetz** ist wohl doch keine endliche Geschichte, wie ich noch in meinem 19. Tätigkeitsbericht (Nr. 7.4) gehofft hatte. Zwar arbeitet das BMI an einem Entwurf für eine gesetzliche Regelung der Aufgabenwahrnehmung durch den DRK-Suchdienst und den Kirchlichen Suchdienst, wie ich es erstmals in meinem 13. Tätigkeitsbericht (Nr. 5.11) gefordert hatte. Allerdings lag mir bei Redaktionsschluss immer noch kein Referentenentwurf vor. In dem Entwurf sollten insbesondere die Beschreibung der Aufgaben der Suchdienste konkretisiert und der Bestand von Daten sowie die Erhebung und Verarbeitung von Daten durch die Suchdienste genauestens (ggf. mittels eines Rasters) ermittelt werden. Ich hoffe, dass das Gesetzesvorhaben nunmehr bald verwirklicht wird.

16. Was lange währt, wird endlich gut – so könnte die Überschrift für den Bericht über die Praxis der Datenerhebung und Recherche im Zusammenhang mit der **Verleihung des Verdienstordens der Bundesrepublik Deutschland** lauten. In meinem 15. Tätigkeitsbericht (Nr. 3.7) hatte ich erstmals beschrieben, welche Fragen zum Schutz des Persönlichkeitsrechts sich bei der Erhebung von Daten des für eine Ehrung Vorgeschlagenen im Rahmen der Prüfung der Ordenswürdigkeit stellen können. Das in der Folge entwickelte so genannte Zwei-Stufen-Modell, das eine Datenbeschaffung auf Vorrat durch die parallele Prüfung von „Verdiensten“ und „Würdigkeit“ unterbindet, hat sich in der Praxis bewährt und wird nunmehr von allen Ländern umgesetzt. Danach werden grundsätzlich zunächst die Verdienste des Betroffenen geprüft und in einem zweiten Schritt wird die Prüfung der Ordenswürdigkeit eingeleitet. Dabei gehe ich davon aus, dass sich die Anzahl der Prüfungsanfragen sowohl hinsichtlich der Verdienste als auch der Ordenswürdigkeit im Rahmen der Verhältnismäßigkeit bewegt.

17. In der Zentrale der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR (BStU) habe ich mir die Verwendung der sog. **„Rosenholz-Unterlagen“** erläutern lassen. Ihre Nutzung hat immer wieder zur Enttarnung – auch prominenter – informeller Mitarbeiter (IM) des ehemaligen Ministeriums für Staatssicherheit der DDR geführt. Bei den unter dem Namen „Rosenholz“ bekannt gewordenen Unterlagen handelt es sich um Mikrofilme von Karteien der Stasi-Hauptverwaltung Aufklärung, die Aufschluss über deren Netz von IM sowohl im Ausland wie auch in der DDR geben (vgl. 18. TB Nr. 5.8.2; 19. TB Nr. 34, dort Nr. 7). Die Mikrofilme waren nach der Wende auf unbekannte Weise in die USA gelangt. Kopien der Mikrofilme auf CD wurden von 1999 bis Anfang 2003 an die BStU übergeben. Bedingung der Übergabe war zunächst die Einstufung als Verschlusssache, die im Juni 2003 aufgehoben wurde, was in einer Vielzahl von Fällen zu einer erneuten Überprüfung auf Stasi-Mitarbeit führte.

Anlage 1

Hinweis für die Ausschüsse des Deutschen Bundestages

Nachfolgend habe ich dargestellt, welche Beiträge dieses Berichtes für welchen Ausschuss von *besonderem Interesse* sein könnten:

Ausschuss für Wahlprüfung, Immunität und Geschäftsordnung	9; 13.10
Auswärtiger Ausschuss	3.1 bis 3.2.6; 5.8.4; 13.10; 22.1; 22.2; 23: 27
Innenausschuss	2.1 bis 2.5; 2.7; 3.1 bis 3.3; 5; 4.2.2; 4.3.1; 4.3.2; 6.1 bis 6.12; 8.2; 8.4; 8.7; 10.2.1; 11.4 bis 11.5.1; 11.5.3; 11.6; 11.7; 11.8; 13.1.1; 13.5; 13.10; 22.1; 27; 28.3; 29.1; 29.13 bis 29.17
Rechtsausschuss	2.1; 2.2; 2.7; 3.1 bis 3.2.7; 3.3.4; 4.1; 4.2.2; 5.4.3; 6.9; 7; 13.1.1; 13.10; 22.1; 27; 29.1
Rechtsausschuss – Unterausschuss Europarecht –	3.1, 3.2, 22.2
Finanzausschuss	3.3.3; 5.4; 8; 11.1; 11.3; 11.5.3; 13.10; 29.3 bis 29.5
Haushaltsausschuss	13.10; 29.4
Rechnungsprüfungsausschuss	6.9
Ausschuss für Wirtschaft und Arbeit	2.2; 2.5; 3.2.5; 4.1; 4.2.2; 4.2.4; 5.8.2; 10.1; 11.1; 11.2; 11.4 bis 11.5.1; 11.5.3; 11.6; 11.7; 11.8; 13.1.3; 13.2; 13.4; 13.10; 13.13; 14; 15.2; 16; 17.1.9; 21.3
Ausschuss für Verbraucherschutz, Ernährung und Landwirtschaft	4.2.1; 4.2.2; 4.3.3; 4.3.4; 7.15; 8.6; 8.10; 13.8; 13.10; 29.3
Verteidigungsausschuss	5.6; 5.8.3; 13.10; 25
Ausschuss für Familie, Senioren, Frauen und Jugend	13.10; 17.1.8; 26
Ausschuss für Gesundheit und Soziale Sicherung	2.5; 2.6; 4.1.1.2; 13.10; 15.1.4; 17.1.1; 17.1.3; 17.1.8; 17.1.9; 17.2.1; 19.1.1;; 21.1; 21.2; 21.3
Ausschuss für Verkehr, Bau- und Wohnungswesen	8.12.1; 13.10; 22
Ausschuss für Umwelt, Naturschutz und Reaktorsicherheit	12; 13.10
Ausschuss für Menschenrechte und Humanitäre Hilfe	3.2; 22.2
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung	2.5; 4; 13.10; 24.1 bis 24.3; 28.2; 28.4
Ausschuss für Wirtschaftliche Zusammenarbeit und Entwicklung	27.4
Ausschuss für Tourismus	22.2
Ausschuss für die Angelegenheiten der Europäischen Union	3.1; 3.2; 3.3.1 bis 3.3.4; 8.9; 13.10; 22.2
Ausschuss für Kultur und Medien	4; 6.3; 7.12; 13.7; 13.10; 28.4; 29.2; 29.17
Ausschuss für Kultur und Medien – Unterausschuss „Neue Medien“ –	8.6

Anlage 2

Übersicht über die durchgeführten Kontrollen, Beratungen und Informationsbesuche

Bundeskanzleramt

- Bundesnachrichtendienst

Auswärtiges Amt

- Zentrale
- eine Deutsche Botschaft

Bundesministerium des Innern

- Ministerium
- Bundesakademie für öffentliche Verwaltung
- Bundeskriminalamt
- Bundesgrenzschutz mit Grenzschutzdirektion und einer BGS-Inspektion
- Bundesamt für Verfassungsschutz
- Bundesamt für Sicherheit in der Informationstechnik
- Statistisches Bundesamt
- Bundesverwaltungsamt
- Bundesamt für Migration und Flüchtlinge (Zentrale und drei Außenstellen)
- Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR: Zentrale und eine Außenstelle
- Technisches Hilfswerk

Bundesministerium der Justiz

- Ministerium
- Generalbundesanwalt beim Bundesgerichtshof
- sowie dessen Dienststelle Bundeszentralregister
- Deutsches Patent- und Markenamt, Zentrale und Außenstelle Jena

Bundesministerium der Finanzen

- Ministerium
- Bundesamt für Finanzen
- ein Bundesvermögensamt
- Bundesanstalt für Finanzdienstleistungsaufsicht
- Bundesteuerberaterkammer
- drei Oberfinanzdirektionen
- zwei Hauptzollämter
- ein Flughafenzollamt
- Zollkriminalamt
- Zollfahndungsamt

Bundesministerium für Wirtschaft und Arbeit

- Ministerium
- drei Agenturen für Arbeit
- Regulierungsbehörde für Telekommunikation und Post
- Wirtschaftsprüferkammer

Bundesministerium der Verteidigung

- Militärischer Abschirmdienst
- eine Wehrbereichsverwaltung
- eine Panzerdivision
- ein Bundeswehrkrankenhaus

Bundesministerium für Familie, Senioren, Frauen und Jugend

- eine Zivildienstgruppe
- eine Verwaltungsstelle eines Wohlfahrtsverbandes

Bundesministerium für Gesundheit und Soziale Sicherung

- Berufsgenossenschaft für den Einzelhandel
- Berufsgenossenschaft der Feinmechanik und Elektrotechnik
- Berufsgenossenschaft der chemischen Industrie
- Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege
- Verwaltungs-Berufsgenossenschaft
- Großhandels- und Lagerei-Berufsgenossenschaft
- Bergbau-Berufsgenossenschaft

Bundesministerium für Verbraucherschutz, Ernährung und Landwirtschaft

- Absatzförderungsfonds der deutschen Land- und Ernährungswirtschaft

Bundesministerium für Bildung und Forschung

- Internetpräsenz

Bundesministerium für Verkehr, Bau- und Wohnungswesen

- Ministerium
- Internetpräsenz
- Kraftfahrt-Bundesamt
- Wasser- und Schifffahrtsdirektion Südwest

noch Anlage 2

– Bundesamt für Güterverkehr
– Fa. Toll Collect GmbH
– Bundesanstalt für Straßenwesen
– Zentrale Militärkraftfahrstelle

Bundesministerium für Umwelt, Naturschutz und Reaktorsicherheit

– Ministerium
– Internetpräsenz
– Bundesamt für Strahlenschutz

Deutsche Post AG

– Zentrale
– Niederlassung Dortmund
– Paketfrachtzentrum Köln
– Niederlassung Paket Bonn

Neue Postdienstunternehmen

– German Logistic Sercice GLS, Bad Hersfeld
– Hermes Versand Service, Hamburg
– Deutscher Paketdienst DPD, Aschaffenburg
– General Overnight GO!, Bonn
– PIN intelligente Dienstleistungen AG, Berlin
– Blitz Kurier, Rathenow
– Maximail Briefservice, Darmstadt

Telekommunikationsunternehmen

– OneTel Telecommunication GmbH
– T-Mobile Deutschland GmbH
– Debitel AG
– Die Dresdner Telekommunikationsgesellschaft mbH (ddkom)
– TELE2 Telecommunication Services GmbH
– Talkline ID GmbH
– Operator Telekommunikation International AG
– Vodafone D2 GmbH
– WEB.DE AG

Bundesversicherungsanstalt für Angestellte

– Hauptstelle
– eine Nebenstelle in Berlin
– eine Rehabilitationsklinik

Kranken- und Pflegekassen

– Deutsche Angestellten Krankenkasse
– Barmer Ersatzkasse
– Techniker Krankenkasse
– Kaufmännische Krankenkasse

Sonstige

– Wirtschaftsunternehmen wegen Verfahren zur Sicherheitsüberprüfung
– Bundesdruckerei GmbH
– GDV Dienstleistungs-GmbH & Co. KG, Hamburg – Zentralruf der Autoversicherer

Anlage 3

Übersicht über Beanstandungen nach § 25 BDSG

Bundesministerium des Innern

- Verstoß der Grenzschutzdirektion gegen Art. 96 Abs. 2 des Schengener Durchführungsübereinkommens (s. Nr. 5.3.8)
- Verstoß gegen die Regelungen der §§ 90 ff. Bundesbeamtengesetz zur Personalaktenführung (s. Nr. 10.4.6)

Bundesministerium der Finanzen

- Verstoß einer Oberfinanzdirektion gegen § 20 Abs. 2 Nr. 2 BDSG wegen mangelhafter technischer und organisatorischer Überwachung von Löschungsfristen in der zentralen Datenbank BillBAO II (s. Nr. 8.4)
- Verstoß einer Oberfinanzdirektion gegen die Regelungen der §§ 90 ff. Bundesbeamtengesetz und des § 28 Abs. 1 i. V. m § 12 Abs. 4 BDSG beim Umgang mit sensiblen Personal-/Personalaktendaten (s. Nr. 10.4.4)

Bundesministerium für Gesundheit und Soziale Sicherung

- Verstoß der Berufsgenossenschaft Nahrungsmittel und Gaststätten gegen das Sozialgeheimnis nach § 35 Abs. 1 SGB I durch die Übermittlung personenbezogener Daten an den Arbeitgeber, ohne dass eine Übermittlungsbefugnis vorlag (vgl. Nr. 19.1)
- Verstoß der Großhandels- und Lagerei-Berufsgenossenschaft gegen §§ 200 Abs. 2 SGB VII, 200 Abs. 2, 2. Halbs. SGB VII i. V. m. § 76 Abs. 2 SGB X, weil eine beratende Ärztin mit einem Gutachten beauftragt wurde, ohne dem Versicherten die in diesen Vorschriften genannten Rechte zu gewähren (s. Nr. 19.1)
- Verstoß der Tiefbau-Berufsgenossenschaft gegen §§ 200 Abs. 2 SGB VII, 200 Abs. 2, 2. Halbs. SGB VII i. V. m. § 76 Abs. 2 SGB X, weil ein beratender Arzt mit einem Gutachten beauftragt wurde, ohne dem Versicherten die in diesen Vorschriften genannten Rechte zu gewähren und dieses Gutachten zunächst verwertet werden sollte (s. Nr. 19.1)
- Verstoß der Verwaltungs-Berufsgenossenschaft gegen §§ 200 Abs. 2 SGB VII, 200 Abs. 2, 2. Halbs. SGB VII i. V. m. § 76 Abs. 2 SGB X, weil ein Gutachter unter Verwendung „anonymisierter“ Daten einer Versicherten in Auftrag gegeben werden sollte, um ihr nicht die in den Vorschriften genannten Rechte gewähren zu müssen, und die Anonymisierung misslang (s. Nr. 19.1)
- Verstoß der Holz-Berufsgenossenschaft und der Berufsgenossenschaft für Gesundheitsdienst und Wohlfahrtspflege gegen §§ 200 Abs. 2 SGB VII, 200 Abs. 2, 2. Halbs. SGB VII i. V. m. § 76 Abs. 2 SGB X, weil während eines anhängigen Gerichtsverfahrens ein Gutachten eines beratenden Arztes eingeholt wurde, ohne dem Versicherten die in diesen Vorschriften genannten Rechte zu gewähren (s. Nr. 19.1.3)

Bundesministerium der Justiz

- Zwei Beanstandungen wegen Verstößen des Deutschen Patent- und Markenamtes gegen die Regelungen der §§ 90 ff. Bundesbeamtengesetz beim Umgang mit Personalaktendaten (automatisiert und manuell) sowie hierbei gegen § 9 BDSG sowie Anlage zu § 9 Satz 1 BDSG wegen erheblicher technisch-organisatorischer Mängel bei der Verarbeitung von Personal-/Personalaktendaten (s. Nr. 10.4.3)

Bundesministerium der Verteidigung

- Verstöße des MAD gegen § 11 Abs. 1 Nr. 1 des Sicherheitsüberprüfungsgesetzes (s. Nr. 5.8.3)
- Verstoß eines Bundeswehrkrankenhauses gegen die §§ 9 und 18 Abs. 2 BDSG wegen nicht ordnungsgemäßer Führung des Verfahrensverzeichnisses DATAV (s. Nr. 25.2)

Bundesagentur für Arbeit

- Verstoß der Bundesagentur für Arbeit gegen § 35 SGB I i. V. m. § 78a SGB X wegen eines fehlenden differenzierten Zugriffsberechtigungskonzeptes sowie fehlender Protokollierung beim Programm A2LL (s. Nr. 16.1.3)
- Verstoß einer Agentur für Arbeit gegen § 35 SGB I i. V. m. § 78a SGB X wegen rechtswidriger Entsorgung von Sozialdaten im Hausmüll (s. Nr. 16.1.3)

Anlage 4 (zu Nr. 27.3)

25. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 10. bis 12. September 2003

Entschließung zur Automatischen Software-Aktualisierung

Auf Vorschlag der Datenschutzbeauftragten Deutschlands, der Tschechischen Republik, der Republik Litauen, der Informations- und Datenschutzbeauftragten von Ontario und des Eidgenössischen Datenschutzbeauftragten fasst die Internationale Konferenz folgende Entschließung:

1. Die Konferenz stellt mit Besorgnis fest, dass Software-Unternehmen weltweit zunehmend dazu übergehen, nicht-transparente Techniken für die Übertragung von Software-Aktualisierungen auf die Computer der Nutzer zu verwenden.

   Dadurch sind sie in der Lage,

   - personenbezogene Daten, die auf dem Computer des Nutzers gespeichert sind (z. B. Browser-Einstellungen oder Informationen über das Nutzungsverhalten) auszulesen, ohne dass der Nutzer dies bemerken, beeinflussen oder verhindern kann,
   - zumindest die teilweise Kontrolle über den Zielcomputer zu gewinnen und damit die Möglichkeit des Nutzers einzuschränken, seinen rechtlichen Verpflichtungen zur Gewährleistung der Datensicherheit und des Schutzes der personenbezogenen Daten auf seinem Computer zu genügen,
   - die auf dem Computer installierten Programme zu verändern, die ohne vorgeschriebene Tests oder Freigabeverfahren eingesetzt werden und Fehlfunktionen verursachen können, ohne dass das Update als Ursache erkannt wird.

   Dies kann besondere Probleme bei Behörden und Unternehmen verursachen, soweit diese speziellen rechtlichen Verpflichtungen beim Umgang mit personenbezogenen Daten unterliegen.

2. Die Konferenz fordert deshalb die Software-Hersteller dazu auf,

   - Verfahren für Programm-Updates nur auf die Initiative oder den Wunsch des Nutzers hin, auf transparente Weise und nur so anzubieten, dass kein unkontrollierter Zugang zum Computer des Nutzers eröffnet wird;
   - die Offenbarung von personenbezogenen Daten nur mit der informierten Einwilligung des Nutzers zu verlangen und nur, soweit es zur Durchführung der Aktualisierung erforderlich ist;
   - Wahlfreiheit vorzusehen durch das Angebot von Online Updates nur als eine Alternative zu anderen (Offline-) Formen der Software-Distribution wie z. B. auf CD-ROM.

3. Die Konferenz ruft zur Entwicklung und Umsetzung von solchen Techniken der Aktualisierung von Software auf, die die Privatsphäre und Selbstbestimmung der Computernutzer respektieren.

Anlage 5 (zu Nr. 27.3)

25. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 10. bis 12. September 2003

Entschließung über den Transfer von Passagierdaten

Die 25. Internationale Konferenz der Datenschutzbeauftragten beschließt folgendes:

A. Die Konferenz stellt fest, dass

1. Im Zuge des legitimen Kampfes gegen den Terrorismus und das organisierte Verbrechen in einigen Ländern Maßnahmen in Betracht gezogen werden, die die Grundrechte und Freiheiten, insbesondere das Recht auf den Schutz der Privatsphäre, gefährden könnten.

2. Ein Risiko besteht, Demokratie und Freiheit zu gefährden, unter der Vorgabe diese Werte zu verteidigen.

3. Gesetzliche Anforderungen an Fluggesellschaften oder andere Transportanbieter den Zugriff auf Gesamtdaten von Passagieren, die in Reservationssystemen gespeichert werden, zu gewährleisten oder diese zu übertragen, mit den internationalen Datenschutzgrundsätzen oder den Verpflichtungen der Transportanbieter, die sich auf den nationalen Datenschutzgesetzen stützen, im Konflikt stehen könnten.

B. Die Konferenz bekräftigt infolgedessen, dass

1. In der Bekämpfung des internationalen Terrorismus und des organisierten Verbrechens die Staaten unter vollständiger Achtung der Grundprinzipien des Datenschutzes reagieren sollten, denn diese Werte stellen einen integralen Bestandteil der Werte dar, die sie verteidigen.

2. Regelmäßige internationale Transfers von Personendaten, soweit nötig, nur innerhalb eines bestimmten Datenschutzesrahmens erfolgen dürfen, z. B. auf Basis eines internationalen Abkommens, welches den datenschutzrechtlichen Anforderungen wie einem klar definierten Zweck, der verhältnismäßigen Datenerhebung, einer zeitlichen Begrenzung der Datenspeicherung, der Benachrichtigung der betroffenen Personen, der Gewährleistung der Rechte der betroffenen Personen, sowie einer unabhängigen Aufsicht gerecht wird.

Anlage 6 (zu Nr. 27.3)

25. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 10. bis 12. September 2003

Entschließung über Datenschutz und internationale Organisationen

Die Konferenz ruft dazu auf, dass:

(a) internationale und übernationale Institutionen sich formell zu den Prinzipien bekennen, die mit den wichtigsten internationalen Bestimmungen über den Datenschutz übereinstimmen;

(b) internationale und übernationale Institutionen, welche persönliche Daten verwenden oder verwalten, im Einklang mit den betreffenden Datenschutzrichtlinien Maßnahmen zum Schutz dieser Daten ergreifen (z. B. mit Kontrollbefugnis);

(c) international und übernationale Institutionen, welche sich mit der Verkündung von Normen, Satzungen oder Maßnahmen beschäftigen, die die Behandlung von persönlichen Daten innerhalb des Zuständigkeitsbereiches ihrer jeweiligen Institutionen betreffen, geeignete Maßnahmen ergreifen um sicherzustellen, dass bei ihrer Arbeit die Belange des Datenschutzes hinreichend berücksichtigt werden wie z. B. Rücksprache mit [//] Datenschutzbehörden.

Hinweis zur Erläuterung:

Die Internationale Konferenz, nunmehr in ihrem 25. Jahr, besteht hauptsächlich aus nationalen Datenschutzbehörden, sowie im Falle von Ländern mit dezentraler oder föderaler Verwaltung aus ihren regionalen Gegenstücken.

Aufbauend auf Vorarbeiten der 21. und 22. Internationalen Konferenz, hat die 23. Internationale Konferenz den Beschluss gefasst, ein Verfahren und geeignete Kriterien zur Akkreditierung von Datenschutzbehörden einzurichten.

Die Pariser Entschließung hat ausdrücklich die Existenz solcher Behörden innerhalb von internationalen und übernationalen Institutionen vorweggenommen.

Die Internationale Konferenz wird in diesem Jahr zum ersten Mal dazu aufgerufen, Behörden auf internationaler und übernationaler Ebene zu akkreditieren.

Zwar bestehen Datenschutzbestimmungen für einige Schlüsselinstitutionen, Übereinkommen und Datenbanken auf internationaler und übernationaler Ebene, aber eine Reihe von Übereinkommen zur Mitbenutzung von Daten sind von internationalen Institutionen auf den Weg gebracht worden.

Nicht alle dieser Institutionen zeichneten sich in der Vergangenheit durch ein übermäßiges Engagement für den Datenschutz und dessen Berücksichtigung bei der Festlegung internationaler Normen aus.

Dies betrifft insbesondere eine Reihe von Exekutivorgane. Ebenso gibt es momentan Initiativen von besonderen Organisationen, die weitreichende Auswirkungen auf den Datenschutz haben.

- verschiedene Initiativen mit dem Ziel biometrische Daten in Pässen zu verankern, bedingt durch die Vorgaben der Internationalen Zivilluftfahrt-Organisation (www.icao.int);
- die Dopingtest-Richtlinie, welche kürzlich von der World Anti-Doping Agency (www.wada-ama.org) erlassen wurde, schließt unter anderem die Weitergabe von Information über den Aufenthaltsort von Athleten ein;
- der ENUM-Vorschlag (www.enum-forum.org) betreffend der Kombination von Telefonnummern und E-Mail-Adressen.

Selbst internationale Organisationen, welche sich zu den Prinzipien des Datenschutzes bekennen, laufen Gefahr, ihr Bewusstsein für diese Problematik zu verlieren, sofern sie kein institutionelles Organ mit Kontrollfunktion besitzen.

Die Datenschutzerklärung der UNO enthält z. B. keinen Hinweis auf die eigenen Richtlinien für den Umgang mit computergestützten Daten, welche von der UN-Generalversammlung 1990 verabschiedet wurden.

Angemessener Umgang von internationalen und übernationalen Organisationen mit Daten und Informationen kann nicht allein durch nationale Gesetze und Datenschutzbeauftragte erreicht werden. Vielmehr müssen die internationalen Organisationen selbst ausreichende Normen und Vorschriften erlassen und dafür sorgen, dass diese auch durchgesetzt werden.

Diese Entschließung unterstützt solche Bestrebungen, soweit sie im Einklang mit international anerkannten Regeln erfolgen.

Darüber hinaus sind internationale Institutionen immer mehr für die Verkündung von Vorschriften und Richtlinien auf internationaler Ebene, die dann auf nationale Ebene übertragen werden müssen.

Obwohl solche die Festlegung internationaler Normen generell zu begrüßen ist, kann es zu bestimmten Problemfällen auf nationaler Ebene führen. Dies ist dann der Fall, wenn die Reichweite nationaler Datenschutzbestimmungen bei der Festlegung der internationalen Normen nicht in Betracht gezogen wurde.

noch Anlage 6 (zu Nr. 27.3)

Durch die Annahme dieser Entschließung soll das Bewusstsein und die Einhaltung von Datenschutzbestimmungen innerhalb internationaler Institutionen gestärkt werden. Ein zu erhoffender Nebeneffekt besteht zugleich in der verbesserten Information über Datenschutz in Bezug auf die Festlegung internationaler Standards (inklusive der Errichtung von geeigneten Mechanismen, um existierende Datenschutzbehörden bei Themen, die ihre Kompetenzen berühren, zu konsultieren).

Der Ausrichter der 25. Internationalen Konferenz wird aufgerufen, die Aufmerksamkeit relevanter internationaler Institutionen auf diese Entschließung zu lenken. Die Urheber dieser Entschließung sichern ihm dabei ihre Unterstützung zu.

Es ist zu erwarten, dass ein kurzer Bericht über den Ausgang dieses Unterfangens auf der 26. Internationalen Konferenz vorgelegt wird.

Anlage 7 (zu Nr. 27.3)

25. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 10. bis 12. September 2003

Entschließung über die Verbesserung der Bekanntmachung von Praktiken zum Datenschutz

Die 25. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre beschließt folgendes:

1. Die Konferenz fordert Organisationen sowohl im öffentlichen als auch privaten Sektor auf, ihr Augenmerk auf folgende Notwendigkeiten zu richten:

   - Deutliche Verbesserung der Bekanntmachung, wie persönliche Daten von der jeweiligen Organisation behandelt werden.
   - Globale Standardisierung bezüglich der Art und Weise, wie diese Informationen bekannt gemacht werden.

   Und dadurch

   - das individuelle Verständnis und Bewusstsein für die eigenen Rechte und die Möglichkeiten, die sich daraus für den Einzelnen ergeben, zu verbessern; sowie
   - einen Anreiz durch dieses gesteigerte Bewusstsein für Organisationen zu schaffen, die eigenen Methoden zur Behandlung von persönlichen Daten zu verbessern und noch transparenter zu gestalten.

2. Die Internationale Konferenz befürwortet die folgenden Maßnahmen, um die oben beschriebenen Ziele zu erreichen:

   - Die Entwicklung und Verwendung eines zusammenfassenden Standardformates für eine Übersicht über Informationen zum Datenschutz, welches von Organisationen weltweit verwendet werden kann. Dieses Standardformat sollte folgende Informationen beinhalten:
     - jene Informationen, die für die einzelne Person am wichtigsten sind; und
     - jene Informationen, an denen die Mehrzahl der betroffenen Personen interessiert sein könnte; sowie
   - den Gebrauch von einfacher, klarer und direkter Sprache;
   - den Gebrauch der Sprache, die auf der Website oder dem Formular verwendet wird, um die jeweiligen Informationen zu erheben;
   - die Beschränkung des Formats auf eine begrenzte Anzahl von Elementen, die in Übereinstimmung mit dem oben Gesagten, die wichtigsten Grundsätze zum Datenschutz beinhalten:
     - Wer die persönlichen Informationen sammelt und wie dieser Jemand zu erreichen ist (mindestens der offizielle Name und die postale Anschrift der Organisation).
     - Welche persönlichen Informationen diese Organisation erhebt und wie dies geschieht.
     - Warum diese Daten erhoben werden und welchem Zweck dies dient.
     - Ob diese Informationen Dritten zugänglich gemacht werden und wenn, ja, wem (Name und Tätigkeit des Dritten) und zu welchem Zweck.
     - Die Möglichkeiten, die der einzelnen Person durch Datenschutzbestimmungen gewährt werden und wie diese einfach anzuwenden sind. Dies betrifft insbesondere Informationen, die unbeteiligten Dritten zu legalen Zwecken zugänglich gemacht werden und die vom Verbraucher offen gelegt werden müssen, um die jeweilige Dienstleistung in Anspruch nehmen zu können.
     - Eine Zusammenfassung der individuellen Rechte auf Einsicht, Korrektur, Zurückhaltung sowie Löschung von persönlichen Daten.
     - Welche unabhängige Aufsichtsbehörde Individuen kontaktieren können, wenn sie der Ansicht sind, dass ihre Rechte verletzt wurden.
   - Geeignete Maßnahmen, die das Auffinden von zusätzlichen Informationen wie den folgenden einfacher machen:
     - Alle Informationen, die Organisationen von Rechts wegen machen müssen, z. B. Rechte auf Einsicht, Korrektur, Zurückhaltung sowie Löschung von persönlichen Daten, und wie lange diese Daten gespeichert werden dürfen; und
     - eine komplette Erklärung der in der gekürzten Übersicht enthaltenen Informationen; und
     - die kompletten Datenschutzerklärungen der jeweiligen Organisation im Bezug auf Behandlung und Verwertung von Daten.

3. Die Konferenz ist sich darüber einig, dass ein solch standardisiertes und zusammenfassendes Format nur in Übereinstimmung mit allen entsprechenden nationalen Gesetzen und wo nötig, mit allen Anzeigen, die eine Organisation einem Individuum gegenüber verpflichtet ist zu machen, sinnvoll ist.

noch Anlage 7 (zu Nr. 27.3)

4. Die Konferenz ist sich der Tatsache bewusst, dass der Zeitpunkt bei der Darbietung von Informationen zum Umgang und Schutz von Daten eine wichtige Rolle spielt. So wäre es z. B. besonders hilfreich, wenn diese Informationen automatisch zu dem Zeitpunkt präsentiert werden, an dem die Person wählen kann, welche Informationen sie (an Dritte) weitergeben will und welche nicht. In anderen Fällen kann es ausreichend sein, zusätzliche Informationen über Verweise auf die entsprechenden Links bereitzustellen. Die Konferenz erkennt die wichtige Arbeit der EU-Art. 29 Datenschutz-Arbeitsgruppe an, die diese zum Thema „Automatisierte Präsentation von Informationen zum Datenschutz“ in Empfehlung 2/2001 *Empfehlung zu einigen Mindestanforderungen für die Online-Erhebung personenbezogener Daten in der Europäischen Union* geleistet hat.

5. Die Konferenz ist der Ansicht, dass der Zeitpunkt für die Darbietung der zusammengefassten Version (mit Bezügen zum On- und Offline-Bereich) ein angemessenes zukünftiges Betätigungsfeld für Datenschutzbeauftragte ist.

6. Die Konferenz ist sich auch der Tatsache bewusst, dass es in diesem Bereich andere Aktivitäten gibt, so z. B. die Entwicklung von Computersprachen, welche in der Lage sind, Datenschutzrichtlinien zu beschreiben. Sie ermutigt zur weiteren Entwicklung von Wegen, diese Richtlinien in das standardisierte und zusammenfassende Format zu übersetzen.

7. Die Konferenz sieht diese Aktivitäten als erste Schritte in Richtung einer Verbesserung der Art und Weise an, in der Organisationen mit persönlichen Daten umgehen und sie verarbeiten. Die Konferenz ist sich dem Vorhandensein diverser Initiativen in diesem Bereich bewusst und ermutigt zu derartigen Initiativen, die die Kommunikation zwischen Organisationen und Individuen verbessern. Die Konferenz ist bereit, mit Organisationen und Interessengruppen, die sich in diesem Bereich betätigen, zusammenzuarbeiten und weitergehende Schritte in dieser Richtung auf zukünftigen Konferenzen zu unternehmen.

Anlage 8 (zu Nr. 27.3)

25. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 10. bis 12. September 2003

Entschließung zu Radio-Frequency Identification

Auf Vorschlag des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg, des Unabhängigen Zentrums für Datenschutz Schleswig-Holstein, Deutschland, der Spanischen Datenschutzbehörde und des Datenschutzbeauftragten des Kantons Zug, Schweiz, hat die Internationale Konferenz folgende Entschließung gefasst:

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für die Privatsphäre möglich. RFID-Etiketten (RFID tags) werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle der Logistik oder zum Schutz der Authentizität einer Produktmarke (Warenzeichen) verwendet; sie könnten aber auch mit personenbezogenen Informationen wie Kreditkartendaten verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

a) sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpft sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

b) wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

c) dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zur Erreichung dieses Zwecks erforderlich ist und

d) soweit RFID-Etiketten im Besitz von Personen sind, sollten diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detailliert verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

Anlage 9 (zu Nr. 27.3)

26. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 14. bis 16. September 2004

Resolution zum Entwurf eines ISO-Rahmenstandards zum Datenschutz

Die Internationale Standardisierungsorganisation (ISO) hat eine Arbeitsgruppe zu Datenschutztechnologien (PTSG) im Rahmen des Gemeinsamen Technischen Ausschusses (JTC 1) eingerichtet, um die Notwendigkeit der Entwicklung eines Standards für Datenschutztechnologien und gegebenenfalls das Verfahren zur Formulierung und den Geltungsbereich eines solchen Standards zu prüfen und bis zum November 2004 zu berichten;

der Gemeinsame Technische Ausschuss (JTC 1) der ISO leitet dem Unterausschuss 27 (Sicherheit der Informationstechnik) Vorschläge für einen Datenschutz-Rahmenstandard zur Entscheidung in einem beschleunigten Verfahren zu;

die Internationale Allianz für Sicherheit, Vertrauen und Datenschutz (International Security, Trust and Privacy Alliance – ISTPA –) ist eine weltweite Vereinigung von Unternehmen, Institutionen und Technologie-Anbietern, die zusammenarbeiten, um gegenwärtige und entstehende Probleme in Bezug auf Sicherheit, Vertrauen und Datenschutz zu klären und zu lösen;

die ISO hat den Entwurf eines Internationalen Standards (ISO/IEC (PAS) DIS 20886) für einen Datenschutzrahmen erhalten, den ISTPA[1] in einem beschleunigten Verfahren eingebracht hat und über den durch schriftliche Abstimmung bis zum 11. Dezember 2004 abgestimmt werden soll;

das Projekt zum Test und zur Bewertung von Datenschutz fördernden Technologien (Privacy Enhancing Technology Testing & Evaluation Project – PETTEP –)[2] ist eine weltweite Gruppe von Datenschutzbeauftragten, Wissenschaftlern, öffentlichen und nicht-öffentlichen Stellen und Datenschutzexperten, denen es um die Entwicklung international anerkannter Test- und Evaluationskriterien für die Datenschutzkonformität von Informationstechnologien und -systemen geht;

die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation hat bei ihrer 35. Sitzung in Buenos Aires am 14./15. April 2004 ein Arbeitspapier zu einem zukünftigen ISO-Datenschutzstandard angenommen[3];

die Internationale Konferenz der Datenschutzbeauftragten (im Folgenden die „Konferenz“) möchte die Entwicklung eines effektiven und universell akzeptierten Internationalen Standards über Datenschutztechnologien unterstützen und der ISO ihren Sachverstand für die Entwicklung eines solchen Standards zur Verfügung stellen;

die Konferenz erkennt an, dass die Befolgung jedes gegenwärtigen oder zukünftigen ISO-Standards nicht notwendigerweise die Befolgung von rechtlichen Bestimmungen impliziert oder ersetzt. Die Konferenz sieht aber in der Entwicklung solcher Standards der Informationstechnologie ein Mittel, um die Beteiligten bei der Befolgung rechtlicher Regelungen zum Datenschutz zu unterstützen. Die Konferenz erkennt an, dass trotz der Tatsache, dass jedes Mitgliedsland gegenwärtig und in Zukunft eigene, in bestimmter Hinsicht von anderen verschiedene Datenschutzgesetze hat, insgesamt ein hohes Maß an Übereinstimmung zwischen diesen rechtlichen Anforderungen besteht, denen am Besten zu entsprechen wäre, wenn sie durch die Entwicklung eines Internationalen Standards zur datenschutzrechtlichen Informationstechnik unterstützt würden.

Die Konferenz nimmt die folgenden Resolutionen an:

1. Die Konferenz empfiehlt, dass ein weltweiter Datenschutzstandard und insbesondere ein Standard für Datenschutztechnologien von der ISO formuliert wird, der die Umsetzung bestehender rechtlicher Bestimmungen zum Datenschutz und die Formulierung solcher Bestimmungen – wo sie noch fehlen – unterstützt.
2. Die Konferenz ist der Auffassung, dass die Entwicklung eines Internationalen Datenschutzstandards sowohl auf gerechte Informationspraktiken als auch auf die Begriffe der Datensparsamkeit, Datenminimierung und Anonymität gestützt sein muss. Um effektiv zu sein, muss ein Standard für Informationstechnologie:
   - Evaluierungs- und Testkriterien bereitstellen, die es erlauben, die Datenschutzfunktionalität jedes Systems oder jeder Technologie zu bewerten, um auf diese Weise die Daten verarbeitenden Stellen bei der Befolgung nationaler und internationaler Vorschriften zum Datenschutz zu unterstützen;
   - einen Grad an Vertrauenswürdigkeit hinsichtlich der Technologien und Systeme zur Verarbeitung personenbezogener Daten gewährleisten, die den Anspruch erheben, datenschutzgerecht zu sein;
   - in der Lage sein, Datenschutzerfordernisse bezüglich personenbezogener Daten zu erfüllen, unabhängig von der Kombination und Zahl von Organisationen, die an der Verwendung und am Austausch dieser personenbezogenen Daten beteiligt sein mögen.

[1] vgl. http://www.istpa.org

[2] PETTEP ist ein Projekt, das von der Informations- und Datenschutzbeauftragten von Ontario geleitet wird und das Test- und Bewertungskriterien für datenschutzfreundliche Informationstechnik untersucht.

[3] http://datenschutz-berlin.de/doc/int/iwgdpt/index.htm

noch Anlage 9 (zu Nr. 27.3)

3. Die Konferenz unterstützt die jüngst erfolgte Einrichtung einer vorläufigen Arbeitsgruppe zu Datenschutztechnologien (Privacy Technology Study Group – PTSG), um die Notwendigkeit eines Standards wie auch seinen Geltungsbereich und die Methode für die Entwicklung eines solchen Standards innerhalb der Internationalen Standardisierungsorganisation zu untersuchen.

4. Die Konferenz unterstützt nachhaltig die Beschleunigung und unverzügliche Einrichtung eines neuen, ständigen Unterausschusses der ISO für die Entwicklung von Standards zu Informationstechnologien mit Bezug zum Datenschutz. Der neue Unterausschuss soll die Arbeit an bestimmten Datenschutzfragen, die zurzeit in den bestehenden Unterausschüssen geführt wird, berücksichtigen.

5. Die Konferenz unterstützt entschieden die Aufnahme des Projektes zum Test und zur Bewertung von datenschutzfördernden Technologien (PETTEP) als eine offizielle Verbindungsorganisation zur ISO JTC1 Arbeitsgruppe zu Datenschutztechnologien (PTSG). Dies gibt den Datenschutzbeauftragten die Möglichkeit, direkt innerhalb der ISO-Arbeitsgruppe (PTSG) zu arbeiten, zudem eröffnet es den Mitgliedern von PETTEP die offizielle Möglichkeit, der Datenschutzarbeitsgruppe Vorschläge zu machen und zu ihrer Arbeit und ihren Diskussionen beizutragen.

6. Die Konferenz unterstützt und ermutigt interessierte Datenschutzbeauftragte, PETTEP beizutreten, was sie in die Lage versetzen würde, als PETTEP-Mitglieder eine unmittelbare Stimme bei den Diskussionen zur Entwicklung eines ISO-Datenschutztechnologie-Standards zu haben.

7. Die Konferenz erkennt an, dass PETTEP bereits in die PTSG aufgenommen worden ist und bittet PETTEP darum, die Entschließungen der Konferenz aufzugreifen und sie der PTSG zum frühestmöglichen Zeitpunkt vorzulegen.

8. Auch wenn die Konferenz die Zielrichtungen und das Engagement der ISTPA im Bereich des Datenschutzes anerkennt, bittet sie darum, den ISTPA-Rahmenentwurf als eine öffentlich erhältliche Spezifikation zurückzuziehen, bis die folgenden Punkte aufgegriffen worden sind:

   – Der Begriff des Datenschutzes, auf den der Entwurf eines Datenschutzrahmenstandards sich stützt, und die Anerkennung der Grenzen der Datenerhebung. Der Entwurf definiert „Datenschutz“ als „den korrekten Umgang und die Nutzung personenbezogener Information während ihrer Lebensdauer, in Übereinstimmung mit den Datenschutzprinzipien und den Festlegungen des Betroffenen“[4]. Die Verfasser des Entwurfs meinen, dass die Erhebung und Verarbeitung personenbezogener Daten wesentlich für das reibungslose Funktionieren einer modernen Gesellschaft und des Handels ist[5]. Diese Aussage beruht auf der Annahme, dass es keine Grenzen für die Erhebung von personenbezogenen Daten gibt. Es kann Situationen geben, in denen die Erhebung und Verarbeitung personenbezogener Daten in diesem Sinne wesentlich ist. Dies sollte aber nicht als Regel zu Grunde gelegt werden.

9. Die Konferenz bittet die ISO, alle gegenwärtig vorliegenden Anträge für die Behandlung von öffentlich zugänglichen Spezifikationen im Bereich des Datenschutzes zur Annahme in einem Schnellverfahren (oder die Einführung neuer Anträge mit öffentlich zugänglichen Spezifikationen bezüglich des Datenschutzes) zurückzustellen, da die Entwicklung eines Datenschutzstandards gründlicher Erörterung bedarf.

10. Die Konferenz bittet darum, dass die ISO Anträge für öffentlich zugängliche Spezifikationen und andere Anträge mit Bezug auf den Datenschutz als Beiträge und Bausteine für die Entwicklung eines Gesamtrahmens und die mögliche Entwicklung zukünftiger Standards innerhalb dieses Rahmens betrachtet.

[4] ebenda S. 13
[5] ebenda S. 10

Anlage 10 (zu Nr. 27.3)

26. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 14. bis 16. September 2004

Änderung der Entschließung der Konferenz 2003 zur Automatischen Software-Aktualisierung

1. Die Konferenz stellt mit Besorgnis fest, dass Software-Unternehmen weltweit immer häufiger nicht-transparente Techniken benutzen, um die Software-Aktualisierung auf die Computer der Nutzer zu übertragen.

   Dadurch sind sie in der Lage:

   - die personenbezogenen Daten, die auf dem Computer des Nutzers gespeichert sind (z. B. Browser-Einstellungen oder Informationen über das Nutzungsverhalten) auszulesen und zu sammeln, ohne dass der Nutzer dies bemerken, beeinflussen oder verhindern kann,
   - zumindest die teilweise Kontrolle über den Zielcomputer zu gewinnen und damit die Möglichkeit des Nutzers einzuschränken, seinen rechtlichen Verpflichtungen zur Gewährleistung der Datensicherheit und des Schutzes der personenbezogenen Daten auf seinem Computer zu genügen,
   - die auf dem Computer installierten Programme zu verändern, die ohne vorgeschriebene Tests oder Freigabeverfahren eingesetzt werden und
   - Fehlfunktionen verursachen können, ohne dass das Update als Ursache erkannt wird.

   Dies kann besondere Probleme bei Behörden und Unternehmen in diesem Bereich verursachen, soweit dies speziellen rechtlichen Verpflichtungen beim Umgang mit personenbezogenen Daten unterliegt.

2. Die Konferenz fordert deshalb die Software-Hersteller dazu auf:

   a. Verfahren für Online-Programm-Updates nur mit der Benachrichtigung und der Update-Ausübung nach dem Erlangen der Nutzereinwilligung, ohne diese Einwilligung zu übertreten oder verletzen, auf transparente Weise und nur so anzubieten, dass kein unkontrollierter Zugang zum Computer des Nutzers eröffnet wird;

   b. die Offenbarung von personenbezogenen Daten nur mit der informierten Einwilligung des Nutzers zu verlangen und nur, soweit es zur Durchführung der Aktualisierung erforderlich ist. Die Nutzer dürfen nicht gezwungen werden, ihre Identität zu bestimmen (im Gegensatz zur Authentisierung) bevor sie das Update herunterladen;

   c. nur solche Update-Leistungen anzubieten, die die Möglichkeit der vorherigen Prüfung auf einem separaten Server vor der Installierung vorsehen.

3. Die Konferenz ruft zur Entwicklung und Umsetzung von solchen Techniken der Aktualisierung von Software auf, die die Privatsphärve und Selbstbestimmung der Computernutzer respektieren.

Anlage 11 (zu Nr. 27.3)

26. Internationale Konferenz der Beauftragten für den Datenschutz und den Schutz der Privatsphäre vom 14. bis 16. September 2004

Zulassung weiterer Teilnehmer zur Internationalen Datenschutzkonferenz

Die folgenden Behörden sind gemäß den Kriterien und Prinzipien des Mandatausschusses akkreditiert worden

A Nationale Behörden für den Datenschutz

Korea

- Korean Information Security Agency

B Behörden für den Datenschutz mit der regionalen Zuständigkeit

Spanien

- Katalonien: Katalonische Agentur für den Datenschutz (Agéncia Catalana des Protecció de Dades)

C Behörden für den Datenschutz, die in den internationalen und supranationalen Organen zusammenschgeschlossen sind

Europäische Union

- Der Europäische Beauftragte für den Datenschutz (Contrôleur européen de la protection des données)

Erklärungsnote

Gemäß den Prinzipien des Mandatausschusses und gemäß der Ergänzung der Richtlinien und Prozeduren betreffend der Konferenzentschließungen („Ergänzung“) bestimmt folgende Entschließung die Empfehlungen im Bereich der Akkreditierung der Behörden für den Datenschutz zu der Teilnahme an der internationalen Konferenz gemäß der richtigen Klassifikation. Wenn die Behörde den Namen in einer anderen als Englische Sprache besitzt, ist der in den Klammern gegeben.

Abs. 2 der Ergänzung sieht vor, das die im Rahmen der internationalen oder supranationalen Organen akkreditierten Behörden kein Stimmrecht haben, soweit die Konferenz entscheidet, ihnen nicht das Stimmrecht während der Akkreditierung zu geben. Mandatausschuss empfiehlt, das Stimmrecht dem Europäischen Beauftragten für den Datenschutz zu geben.

Anlage 12 (zu Nr. 3.2.1)

Von der Art. 29-Gruppe im Berichtszeitraum verabschiedete Dokumente

Von der Gruppe im Berichtszeitraum verabschiedete Dokumente

WP 68 (10054/03)	Leitlinien für Online-Authentifizierungssysteme – Pressemitteilung der Artikel 29-Datenschutzgruppe – Arbeitspapier zu Online-Authentifizierungsdienste Angenommen am 29. Januar 2003
WP 69 (12054/02)	Stellungnahme 1/2003 zur Speicherung von Kommunikationsdaten zu Zwecken der Gebührenabrechnung Angenommen am 29. Januar 2003
WP 71 (12054/02)	Arbeitsprogramm 2003 der Artikel 29-Datenschutzgruppe Angenommen am 29. März 2003
WP 73 (10593/02)	Stellungnahme zu eGovernment Angenommen am 8. Mai 2003
WP 74 (11639/02)	Stellungnahme zu verbindlichen unternehmensinternen Vorschriften für den internationalen Datentransfer (so genannte Binding Corporate Rules) Angenommen am 3. Juni 2003
WP 76 (10972/03)	Stellungnahme 2/2003 zur Anwendung der Datenschutzprinzipien auf die „Whois“ Verzeichnisse Angenommen am 13. Juni 2003
WP 77 (10066/03)	Europäischer Ehrenkodex für die Verwendung personenbezogener Daten in der Direktwerbung – Pressemitteilung der Artikel 29-Datenschutzgruppe – Stellungnahme 3/2003 der Artikel 29-Datenschutzgruppe – Anhang: FEDMA Code Angenommen am 13. Juni 2003
WP 78 (11070/03)	Stellungnahme 3/2003 zum Schutzniveau in den Vereinigten Staaten für die Übermittlung von Passagierdaten – Pressemitteilung der Artikel 29-Datenschutzgruppe – Verpflichtungserklärung der US Zoll- und Grenzschutzbehörden sowie der US Transportation Security Administration Angenommen am 13. Juni 2003
WP 79 (10595/03)	Stellungnahme 5/2003 zum Schutzniveau personenbezogener Daten in Guernsey Angenommen am 13. Juni 2003
WP 80 (10595/03)	Stellungnahme zur Verarbeitung von biometrischen Merkmalen Angenommen am 1. August 2003
WP 82 (11580/03)	Stellungnahme 6/2003 zum Schutzniveau personenbezogener Daten auf der Isle of Man Angenommen am 21. November 2003
WP 83 (10936/03)	Stellungnahme 7/2003 zur Weiterverwendung von Informationen des öffentlichen Sektors und dem Schutz personenbezogener Daten Angenommen am 12. Dezember 2003

noch Anlage 12 (zu Nr. 3.2.1)

(12065/03)	Sechster Jahrsbericht über den Stand des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten und des Schutzes der Privatsphäre in der Europäischen Union und in Drittländern – Berichtsjahr 2001 Angenommen am 16. Dezember 2003
WP 84 (11754/03)	Stellungnahme 8/2003 zu dem von mehreren Wirtschaftsverbänden eingereichten Entwurf von Standardvertragsklauseln Angenommen am 17. Dezember 2003
WP 85 (10031/03)	Stellungnahme 1/2004 zum Datenschutzniveau in Australien bei der Übermittlung von Passagierdaten Angenommen am 16. Januar 2004
WP 86 (11816/03)	Stellungnahme zu vertrauenswürdigen Rechnerplattformen und insbesondere zur Tätigkeit der Trusted Computing Group TCG Angenommen am 23. Januar 2004
WP 87 (10019/04)	Stellungnahme 2/2004 zur Angemessenheit des Schutzes der Passagierdaten, (Passenger Name Records – PNR), die den Zoll- und Grenzschutzbehörden der Vereinigten Staaten übermittelt werden Angenommen am 29. Januar 2004
WP 88 (10037/04)	Stellungnahme 3/2004 zum Datenschutzniveau in Kanada bei der Übermittlung von Passagierdaten (PNR) und erweiterten Passagierdaten (API) Angenommen am 11. Februar 2004
WP 89 (11750/02)	Stellungnahme 4/2004 zur Verarbeitung personenbezogener Daten aus der Videoüberwachung Angenommen am 11. Februar 2004
WP 90 (11601/03)	Stellungnahme 5/2004 zu unerbetenen Werbenachrichten (Spam) im Sinne von Artikel 13 der Richtlinie 2002/58/EG Angenommen am 27. Februar 2004
WP 91 (12178/03)	Stellungnahme zu genetischen Daten Angenommen am 17. März 2004
WP 92 (10650/04)	Arbeitsprogramm 2004 Angenommen am 17. März 2004
WP 93 (10649/04)	Gemeinsame Erklärung zu den Terroranschlägen in Madrid am 11. März 2004 Angenommen am 17. März 2004
WP 95 (11221/04)	Stellungnahme 6/2004 zur Kommissionsentscheidung vom 14. Mai 2004 über die Angemessenheit des Schutzes der Passagierdaten, die den Zoll- und Grenzschutzbehörden der USA übermittelt werden, und zum Abkommen zwischen der EU und den USA über die Verarbeitung von Passagierdaten und deren Übermittlung durch die Fluggesellschaften an das US-Ministerium für Heimatschutz Angenommen am 22. Juni 2004

noch Anlage 12 (zu Nr. 3.2.1)

WP 96 (11487/04)	Stellungnahme 7/2004 zur Verarbeitung biometrischer Merkmale in Visen und Aufenthaltstiteln im Visa-Informationssystem (VIS) Angenommen am 11. August 2004
WP 97 (11733/04)	Stellungnahme 8/2004 zur Unterrichtung von Passagieren bei Flügen zwischen der EU und den USA Angenommen am 30. September 2004
WP 98	Strategiepapier Angenommen am 29. September 2004
WP 99	Stellungnahme 9/2004 zur Speicherung von Kommunikationsdaten zur Prävention, Ermittlung und Verfolgung von kriminellen Handlungen, auch von Terrorismus Angenommen am 9. November 2004
WP 100	Stellungnahme zu den Informationspflichten der Datenverarbeiter – Anhänge Angenommen am 25. November 2004
WP 101	Stellungnahme zur Umsetzung der EU-Datenschutzrichtlinie Angenommen am 25. November 2004

Anlage 13 (zu Nr. 2 und Nr. 8.1)

65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März 2003

Entschließung:
Forderungen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder an Bundesgesetzgeber und Bundesregierung

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

- Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes
  - Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.
  - Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.
  - Die Freiwilligkeit der Einwilligung muss gewährleistet sein.
  - Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in“ statt „opt out“).
- Technischer Datenschutz

  Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.
- Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

  Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen. Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.
- Förderung von datenschutzgerechter Technik

  Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind. Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

  Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

noch Anlage 13 (zu Nr. 2 und Nr. 8.1)

- Anonyme Internetnutzung

  Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von e-Mails sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

  Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

- Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

  Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten: Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

  Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

  Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

  Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung – für geboten.

  Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung – als grundrechtssicherndes Verfahrenselement ergreifen muss.

- Stärkung des Schutzes von Gesundheitsdaten

  Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung“ einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

  Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu

beachten und zwar auch für deren Verwendung im Einzelfall. Der Gesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese z.B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

- Datenschutz und Gentechnik

  Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen – dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

  Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

  In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes“ vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

- Datenschutz im Steuerrecht

  Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

  Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit. Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

- Arbeitnehmerdatenschutz

  Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

  – die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

  – die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,

  – die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

  – die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

  Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

  Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

- Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

  Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Artikel 28 der EG-Datenschutzrichtlinie gebietet.

  Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist

noch Anlage 13 (zu Nr. 2 und Nr. 8.1)

in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

- Stellung des Bundesdatenschutzbeauftragten

  Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

- Verbesserung der Informationsrechte

  Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

Anlage 14 (zu Nr. 7.2.1)

66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25. und 26. September 2003

Entschließung:
Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai dieses Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen“ vorgelegt. Darin hat es festgestellt, dass

- die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 Prozent erhöht (1996: 2 149; 2001; 3 868) hat,
- die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2 494 um das Sechsfache auf 15 741 gestiegen ist,
- sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3 730 auf 9 122 fast verdreifacht hat,
- in 21 Prozent der Anordnungen zwischen 1 000 und 5 000 Gespräche, in 8 Prozent der Anordnungen mehr als 5 000 Gespräche abgehört worden sind,
- der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 Prozent auf ca. 14 Prozent angestiegen ist,
- die Beschlüsse in ca. ¾ aller Fälle das gesetzliche Maximum von drei Monaten umfassen, ¾ aller Maßnahmen tatsächlicher aber nur bis zu zwei Monaten andauern,
- lediglich 24 Prozent der Beschlüsse substanziell begründet werden,
- es nur in 17 Prozent der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,
- 73 Prozent der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrechts der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung – nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

- Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.
- Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100b StPO dahingehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).
- Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.
- Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100 a StPO muss reduziert werden.
- Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschafft werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.
- Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Gesprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

noch Anlage 14 (zu Nr. 7.2.1)

- Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.
- Zur Sicherung der Zweckbindung nach § 100b Abs. 5 StPO und § 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.
- Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.
- Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

Anlage 15 (zu Nr. 17.1.1)

65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 27. und 28. März 2003 in Dresden

Entschließung:
Datenschutzrechtliche Rahmenbedingungen zur Modernisierung des Systems der gesetzlichen Krankenversicherung

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen die Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u. a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

- den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,
- das Prinzip der Stichprobe zugrunde legen,
- eine strikte Einhaltung der Zweckbindung gewährleisten und
- die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

noch Anlage 15 (zu Nr. 17.1.1)

Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grds. selbst zu entscheiden,

- ob sie überhaupt verwendet wird,
- welche Daten darauf gespeichert werden oder über sie abgerufen werden können,
- welche Daten zu löschen sind und wann das zu geschehen hat,
- ob sie im Einzelfall vorgelegt wird und
- welche Daten im Einzelfall ausgelesen werden sollen.

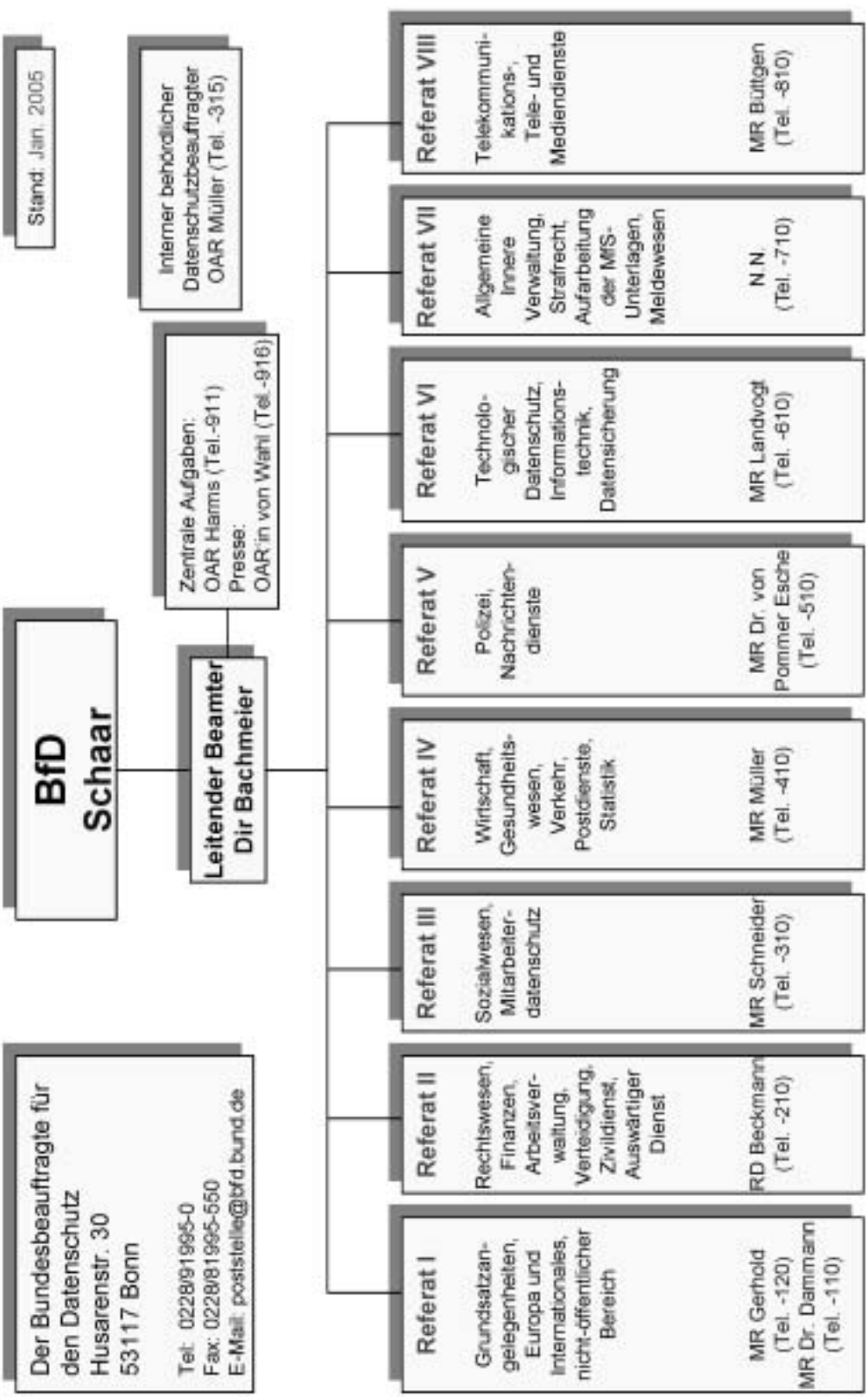
Sicherzustellen ist weiterhin

- ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,
- die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und
- die Strafbarkeit des Datenmissbrauchs.

Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26. Oktober 2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen“ vom 3. Mai 2002, wonach „der Patient Herr seiner Daten“ sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski“, „raucht“, „trinkt zwei Biere pro Tag“), diese überwachen und so zur „Gesundheitspolizei“ werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.


Stand: Jan. 2005
Interner behördlicher Datenschutzbeauftragter OAR Müller (Tel. -315)
Zentrale Aufgaben: OAR Harms (Tel.-911) Presse: OAR'in von Wahl (Tel.-916)
BfD Schaar
Leitender Beamter Dir Bachmeier
Der Bundesbeauftragte für den Datenschutz Husarenstr. 30 53117 Bonn
Tel: 0228/81995-0 Fax: 0228/81995-550 E-Mail: poststelle@bfd.bund.de
Referat I
Grundsatzangelegenheiten, Europa und internationales, nicht-öffentlicher Bereich
MR Gerhold (Tel. -120) MR Dr. Dammann (Tel. -110)
Referat II
Rechtswesen, Finanzen, Arbeitsverwaltung, Verteidigung, Zivildienst, Auswärtiger Dienst
RD Beckmann (Tel. -210)
Referat III
Sozialwesen, Mitarbeiterdatenschutz
MR Schneider (Tel. -310)
Referat IV
Wirtschaft, Gesundheitswesen, Verkehr, Postdienste, Statistik
MR Müller (Tel. -410)
Referat V
Polizei, Nachrichtendienste
MR Dr. von Pommer Esche (Tel. -510)
Referat VI
Technologischer Datenschutz, Informationstechnik, Datensicherung
MR Landvogt (Tel. -610)
Referat VII
Allgemeine Innere Verwaltung, Strafrecht, Aufarbeitung der MfS-Unterlagen, Meldewesen
N N (Tel. -710)
Referat VIII
Telekommunikations-, Tele- und Mediendienste
MR Büttgen (Tel. -810)

Sachregister

Als Fundstelle ist die Nummer des Abschnitts oder des Beitrages angegeben, in dem der Begriff verwendet wird.

Abkürzungsverzeichnis/Begriffe

AA	Auswärtiges Amt
ABBA	Automatisiertes Beihilfeabrechnungssystem
ABl.	Amtsblatt der Europäischen Gemeinschaften
ABMG	Autobahnmautgesetz
Abs.	Absatz
AG	Aktiengesellschaft: aber auch: Arbeitsgruppe
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AIS	Arbeitgeber-Informations-Service
Alt.	Alternative
AO	Abgabenordnung
Art.	Artikel
ATLAS	Internes Informatikverfahren der deutschen Zollverwaltung
AufenthG	Aufenthaltsgesetz
AufenthV	Aufenthaltsverordnung
AuslG	Ausländergesetz
AWG	Außenwirtschaftsgesetz
AZR	Ausländerzentralregister
AZRG	Gesetz über das Ausländerzentralregister
BA	Bundesagentur für Arbeit
BaFin	Bundesanstalt für Finanzdienstleistungen
BAFl	Bundesamt für die Anerkennung ausländischer Flüchtlinge
BAföG	Bundesausbildungsförderungsgesetz
BAG	Bundesamt für Güterverkehr
BAköV	Bundesakademie für öffentliche Verwaltung
BAMF	Bundesamt für Migration und Flüchtlinge
BAN	Bundesgrenzschutzaktennachweis
BArchG	Bundesarchivgesetz
BAZ	Bundesamt für den Zivildienst
BBG	Bundesbeamtengesetz
bDSB	behördlicher Datenschutzbeauftragter
BDSG	Bundesdatenschutzgesetz
BfA	Bundesversicherungsanstalt für Angestellte
BfD	Bundesbeauftragter für den Datenschutz
BfD/BA	Beauftragter für den Datenschutz der Bundesanstalt für Arbeit
BfF	Bundesamt für Finanzen
BfV	Bundesamt für Verfassungsschutz

BGBl.	Bundesgesetzblatt
BGS	Bundesgrenzschutz
BGSG	Bundesgrenzschutzgesetz
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
Bluetooth	Standard für die drahtlose Übermitlung von Sprache und Daten im Nahbereich
BMF	Bundesministerium der Finanzen
BMGS	Bundesministerium für Gesundheit und Soziale Sicherung
BMI	Bundesministerium des Innern
BMJ	Bundesministerium der Justiz
BMVBW	Bundesministerium für Verkehr, Bau- und Wohnungswesen
BMVg	Bundesministerium der Verteidigung
BMWA	Bundesministerium für Wirtschaft und Arbeit
BND	Bundesnachrichtendienst
BNDG	Gesetz über den Bundesnachrichtendienst
BR	Bundesrat
BSI	Bundesamt für Sicherheit in der Informationstechnik
BStU	Bundesbeauftragte für die Unterlagen des Staatssicherheitsdienstes der ehemaligen DDR
BT	Bundestag
BVA	Bundesverwaltungsamt, aber auch: Bundesversicherungsamt
BVerfG	Bundesverfassungsgericht
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfSchG	Bundesverfassungsschutzgesetz
BVerwG	Bundesverwaltungsgericht
BVV	Bundesvermögensverwaltung
BZR	Bundeszentralregister
BZRG	Bundeszentralregistergesetz
bzw.	beziehungsweise
ca.	circa
CD / CD-ROM	Compact Disc - Read Only Memory
COSINUS	Personalinformationssystem der Bundesfinanzverwaltung
d. h.	das heißt
DDR	Deutsche Demokratische Republik
DMP	Disease-Management-Programme
DNA	Desoxyribonoclein acid (acid=Säure)
DPMA	Deutsches Patent- und Markenamt
Drs.	Drucksache

Düsseldorfer Kreis	oberstes Koordinierungsgremium der obersten Aufsichtsbehörden für den Datenschutz
DV/dv	Datenverarbeitung
e.V.	eingetragener Verein
E-Commerce	Elektronic Commerce/Elektronischer Handel
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft(en)
EG-ZIS	Europäisches Zollinformationssystem
EIS	Europäisches Informationssystem
EJG	Eurojust-Gesetz
ELSTER	Elektronische Steuererklärung
E-Mail	Electronic Mail
EMF	Elektromagnetische Felder
EP	Europäisches Parlament
EPC	Electronic Product Code – Der EPC besteht aus vier Datenblöcken zur Identifizierung der Version, des Herstellers, der Produktkategorie und des individuellen Gegenstands
EPCglobal	EPCglobal Inc. ist ein Joint Venture zwischen EAN International und dem Uniform Code Council (UCC). Die Aufgabe des Nonprofit-Unternehmens liegt in der kommerziellen Vermarktung sowie der Administration des EPC
EPOS	Elektronisches Personal-, Organisations- und Stellenmanagement-System
EStG	Einkommensteuergesetz
ETB	Elektronisches Tagebuch
etc.	ecetra
eTIN	Lohnsteuerliches Ordnungsmerkmal
EU	Europäische Union
Eurodac	Europäisches daktyloskopisches Fingerabdrucksystem zur Identifizierung von Asylbewerbern
Europol	Europäisches Polizeiamt
EVN	Einzelverbindungsnachweis
EWG	Europäische Wirtschaftsgemeinschaft
EWR	Europäischer Wirtschaftsraum
f.	folgend
FDZ	Forschungsdatenzentrum
ff.	folgende
FH Bund	Fachhochschule des Bundes für öffentliche Verwaltung
FIDE	automatisiertes Aktennachweissystem im Zollbereich
FIU	Financial Intelligence Unit
FKS	Finazkontrolle Schwarzarbeit
FVG	Finanzverwaltungsgesetz

G10	Artikel 10 Ggesetz
GBA	Generalbundesanwalt beim Bundesgerichtshof
gem.	gemäß
GFG	Gemeinsame Finanzermittlungsgruppe
GG	Grundgesetz
ggf.	gegebenenfalls
GGO	Gemeinsame Geschäftsordnung der Bundesministerien
GJVollz-E	Gesetzentwurf zur Regelung des Jugendstrafvollzugs
GKI	Gemeinsame Kontrollinstanz
GKV	Gesetzliche Krankenversicherung
GmbH	Gesellschaft mit beschränkter Haftung
GMBl	Gemeinsames Ministerialblatt
GMG	Gesetz zur Modernisierung der gesetzlichen Krankenversicherung
GwG	Geldwäschegesetz
Hartz-Kommission	Kommission „Moderne Dienstleistungen am Arbeitsmarkt“
HKP	häusliche Krankenpflege
HPC	Health Professional Card
HTML	Hypertext Markup Language-Standardisierte Seitenbeschreibungssprache für Seiten im Internet/ Intranet
HVBG	Hauptverband der gewerblichen Berufsgenossenschaften
i. d. F.	in der Fassung
i. S. d.	im Sinne des (der)
i. S. v.	im Sinne von
i. V. m.	in Verbindung mit
ICAO	International Civil Aviation Organization
ICHEIC	International Commission on Holocaust Era Insurance Claims
IFOS-Bund	Interaktives Fortbildungssystem für die Bundesverwaltung
IKPO	Internationale Kriminalpolizeiliche Organisation
ILO	International Labour Organization
IMK	Ständige Konferenz der Innenminister und -senatoren der Länder
IMSI	International Mobile Subscriber Identity
INPOL	Informationssystem der Polizei
IP	Internet Protocol
IPSec	Internet Protocol Security
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Informationstechnik
IVBB	Informationsverbund Berlin-Bonn

KBA	Kraftfahrt-Bundesamt
Kfz	Kraftfahrzeug
KOM	Europäische Kommission
KWG	Kreditwesengesetz
LAN	Local Area Network
LfD	Landesbeauftragter für den Datenschutz
lit.	litera (=Buchstabe)
LKA	Landeskriminalamt
LuftSiG	Gesetz zur Neuregelung von Luftsicherheitsaufgaben (Luftsicherheitsgesetz)
m. E.	meines Erachtens
MAD	Militärischer Abschirmdienst
MADG	Gesetz über den MAD
MAK	Mindestanforderungen an das Kreditgeschäft der Kreditinstitute
MDK	Medizinischer Dienst der Krankenversicherung
MRRG	Melderechtsrahmengesetz
MZG	Mikrozensusgesetz
NADIS	Nachrichtendienstliches Informationssystem
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NSDAP	Nationalsozialistische Deutsche Arbeiterpartei
NTS	Nato-Truppenstatut
o. a.	oben aufgeführt
o. g.	oben genannt
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OFD	Oberfinanzdirektion
OK	Organisierte Kriminalität
PassG	Passgesetz
PAVOS	Polizeiliches Auskunfts- und Vorgangsbearbeitungssystem (beim BGS)
PC	Personalcomputer
PEPSY	Personalverwaltungssystem des Auswärtigen Amtes
PERFIS	Personalführungs- und Informationssystem der Bundeswehr
PersauswG	Personalausweisgesetz
PKGr	Parlamentarisches Kontrollgremium
PKV	Private Krankenversicherung
PNR	Passenger Name Record
Protection Profile	Schutzprofil

Ratsdok.	Ratskokument (EU)
RatSWD	Rat für Sozial- und Wirtschaftsdaten
RegTP	Regulierungsbehörde für Telekommunikation und Post
Reha	Rehabilitation
Retaxation	Hat die Apotheke beim Verkauf einer Ware nicht ihre Auflage befolgt, bei fehlender Größenangabe des verschriebenen Medikaments auf dem Rezept immer die kleinstmögliche Packung abzugeben, bekommt sie von der entsprechenden Versicherung nur die für die kleinste Packung anfallenden Kosten erstattet. Diese Zahlungsverweigerung bezeichnet man als Retaxation.
RFID	Radio Frequency Identification – Transpondertechnik für die berührungslose Erkennung von Objekten
RFID-Chip	Radio Frequency Identification-Chip (Funkchip)
RSAV	Risikostrukturausgleichsverordnung
RVOrgG	Gesetz zur Organisationsreform in der gesetzlichen Rentenversicherung
S.	Seite
s.	siehe
SAP R/3HR	Datenbanksystem der Fa. SAP (Personalinformationssystem)
SCHUFA	Schutzgemeinschaft für allgemeine Kreditsicherung
SchwarzArbG	Schwarzarbeiterbekämpfungsgesetz
SDÜ	Schengener Durchführungsübereinkommen
SGB	Sozialgesetzbuch
SGB I	Sozialgesetzbuch Erstes Buch (Allgemeiner Teil)
SGB II	Sozialgesetzbuch Zweites Buch (Grundsicherung für Arbeitssuchende)
SGB III	Sozialgesetzbuch Drittes Buch (Arbeitsförderung)
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 (Rehabilitation und Teilhabe behinderter Menschen)
SGB X	Sozialgesetzbuch Zehntes Buch (Sozialverwaltungsverfahren und Sozialdatenschutz)
SGB XI	Sozialgesetzbuch Elftes Buch (soziale Pflegeversicherung)
SGB XII	Sozialgesetzbuch Zwölftes Buch (Sozialhilfe)
SigG	Signaturgesetz
SIS	Schengener Informationssystem
SMS	Short Message Service
sog.	so genannt
STADA	Staatsangehörigkeitsdatei
Stasi	Staatssicherheitsdienst der ehemaligen DDR
StDAV	Steuerdaten-Abruf-Verordnung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung

StUG	Gesetz über die Unterlagen des Staatssicherheitsdienstes der ehemaligen Deutschen Demokratischen Republik (Stasi-Unterlagen-Gesetz)
StVBG	Steuerverkürzungsbekämfpungsgesetz
StVergAbG	Steuervergünstigungsabbaugesetz
StVollzG	Strafvollzugsgesetz
SÜG	Sicherheitsüberprüfungsgesetz
TAB	Büro für Technikfolgenabschätzung beim Deutschen Bundestag
TB	Tätigkeitsbericht
TBG	Terrorismusbekämpfungsgesetz
TK	Telekommunikation
TKG	Telekommunikationsgesetz
TOP	Tagesordnungspunkt
u. a.	unter anderem
u. ä.	und ähnliches
u. U.	unter Umständen
UIG	Umweltinformationsgesetz
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus – eine Schnittstelle am PC
UStG	Umsatzsteuergesetz
usw.	und so weiter
VDR	Verband Deutscher Rentenversicherungsträger
VG	Verwaltungsgericht
vgl.	vergleiche
VIS	Visa Information System
vpS	vorbeugender personeller Sabotageschutz
WiMax	Wordwide Interoperability for Microwave Access Standard gemäß IEEE 802.16a für lokale Funknetze
WP	Working Paper
WPK	Wirtschaftsprüferkammer
WPO	Wirtschaftsprüferordnung
WPV	Versorgungswerk der Wirtschaftsprüfer
www	world wide web
z. B.	zum Beispiel
z. T.	zum Teil
ZAUBER	Abrufverfahren
ZDG	Zivildienstgesetz
ZFdG	Zollfahndungsdienstgesetz

ZIS	Zollinformationssystem
ZIV	Zinsinformationsverordnung
ZKA	Zollkriminalamt
ZORA	Zentralstelle für Risikoanalyse (Zoll)
ZPO	Zivilprozessordnung
ZSS	Zentrale Speicherstelle
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister

Tätigkeitsbericht	Berichtszeitraum	Bundestagsdrucksachennummer
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
15.	1993–1994	13/1150
16.	1995–1996	13/7500
17.	1997–1998	14/850
18.	1999–2000	14/5555
19.	2001–2002	15/888

Der Bundesbeauftragte für den Datenschutz
Husarenstraße 30
53117 Bonn

Tel.: (0 22 8) 8 19 95-0
Tel. IVBB: (0 18 88) 77 99-0
Fax: (0 22 8) 8 19 95-5 50
E-Mail: poststelle@bfd.bund.de
Internet: http://www.bfd.bund.de

Bonn 2005

Dieser Bericht ist als Bundestagsdrucksache 15/5252 erschienen

Druck: Buch- und Offsetdruckerei
H. Heenemann GmbH & Co
Bessemerstraße 83–91
12103 Berlin