

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 Betriebssystem 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 Tren-

nungsgebot 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 Dienstgesetze 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 Hinblick 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 tiefere 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 werden 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 geldwäscherelevante 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 Lösungsverpflichtung 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 Erkenntnisfragen 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, LKA 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 Er richtungsanordnungen 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 Recherche pool 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 geson-

derten 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 Rechts Tatsachen 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-Identifizierungsmustern 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 normklaren 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 vorgesehenen 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 betei-

genden 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 Lösungs- 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 BGS-Gesetz 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 Grenzübergangspapiere 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 zuzuging. Dies erfolgte genau einen Tag vor der abschließenden Beratung eines entsprechenden Gesetzesentwurfs zur Änderung des Ersten Gesetzes zur Änderung des BGS-G.

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 Auskunft- 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. Grunderfassungsmodul 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 BGS-G 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 Grenzollendienst 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 Offenbourg, 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 Petition 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 Regierungsabkommen 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 BGSOG 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 BGSOG) 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 BGSOG 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 erteilt 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 Fol-

ter 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 Dritt- ausländern 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 genügen. 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 Unterrichtspflicht 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 Unterrichtsverpflichtungen 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 ei-

ner 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 Kontrollgremiumsgesetzes 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 BfV 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 Petition 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 ge-

speichert 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 Dienstanzweisung, 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 Petenteingaben 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 Sicherheitsermitt-

lungen 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 Verschlinkung 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 Wirtschaftsunternehmen 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 verschließen, 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 Mehr-

zahl 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 Dienstaussweisen 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 Verzögerung“ 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).