Deutscher Bundestag **Drucksache 14/1527**

14. Wahlperiode 01. 09. 99

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Petra Pau und der Fraktion der PDS – Drucksache 14/1447 –

Die neue Bundesregierung und der Datenschutz

In ihrer Koalitionsvereinbarung hatten die Regierungsparteien geschrieben: „Effektiver Datenschutz im öffentlichen und privaten Bereich gehört zu den unverzichtbaren Voraussetzungen für eine demokratische und verantwortbare Informationsgesellschaft. Die notwendige Anpassung des deutschen Datenschutzrechts an die Richtlinie der Europäischen Union soll kurzfristig umgesetzt werden. Durch ein Informationsfreiheitsgesetz wollen wir unter Berücksichtigung des Datenschutzes den Bürgerinnen und Bürgern Informationszugangsrechte verschaffen.“ (Koalitionsvereinbarung zwischen der SPD und Fraktion BÜNDNIS 90/DIE GRÜNEN vom 20. Oktober 1998, Satz 38)

Im Januar 1999 schrieb die „Deutsche Vereinigung für Datenschutz e.V.“ über ihre datenschutzrechtlichen Erwartungen an die rot-grüne Bundesregierung:

„Die Koalitionsvereinbarung zwischen SPD und Fraktion BÜNDNIS 90/DIE GRÜNEN, die Grundlage für die Regierungspolitik einer rot-grünen Bundesregierung für die nächste Legislaturperiode sein soll, läßt nicht ansatzweise erkennen, dass sich die Bundesrepublik Deutschland an der technologisch bedingten Schwelle zur Informationsgesellschaft befindet, die neue Antworten zur wirksamen Verteidigung der Bürgerrechte notwendig macht. Sie gibt auch nicht zu erkennen, dass nach 16 Jahren einer autoritär-konservativen Politik eine Trendwende im Bereich des Datenschutzes beabsichtigt sei.

Die Politikerinnen und Politiker müssen zur Kenntnis nehmen, dass sich die Bedrohungslagen für die Freiheitsrechte und die Menschenwürde an der Schwelle zum 21. Jahrhundert von denen unterscheiden, die uns in den letzten 150 bis 200 Jahren seit den bürgerlichen Revolutionen in Europa bekannt wurden. Drohte den Menschen bisher vor allem Gefahr durch ungezügelte Ausbeutung als Arbeitnehmerinnen bzw. Arbeitnehmer und durch exekutive staatliche Übergriffe, so verschieben sich die Risiken in den informationellen Bereich; neue Gefahren sind die schamlose Klassifikation und Manipulation der Menschen als Konsumentinnen und Konsumenten und die informationelle staatliche Kontrolle im Alltag. Persönliche Selbstbestimmung ist weniger durch privaten und staatlichen Zwang bedroht als durch die lautlose Kontrolle mit Hilfe informationstechnischer Instrumente.

Informationstechnik eröffnet aber auch völlig neue positive Möglichkeiten; sie ist in der Lage, den Menschen ihr Leben und Arbeiten einfacher und angeneh-

---

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 26. August 1999 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schriftype – den Fragetext.

mer zu machen. Sie kann dazu benutzt werden, im Interesse von demokratischer Transparenz und Selbstbestimmung Informationen zu vermitteln und diese breit zu diskutieren. Sie dient nicht zuletzt als Hilfsmittel zum Schutz des Menschen, seiner Kommunikationsfreiheit und seiner Privatsphäre. Auch diese Chancen scheinen bisher kein Anliegen der rot-grünen Koalitionspartner zu sein.

Mit dem Argument der gerechten Verteilung gesellschaftlicher Ressourcen und der vorbeugenden Bekämpfung von Straftaten werden die Menschen derzeit schon in einem Maße erfaßt und kontrolliert, wie es früher, schon allein mangels technischer Möglichkeiten, nicht vorstellbar war. Der Erhalt der sozialen Leistungen wird von der totalen Offenlegung der persönlichen Verhältnisse abhängig gemacht. Durch Audio- und Videoüberwachung sowie anlaßunabhängige polizeiliche Kontrollmöglichkeiten schwinden die Unbefangenheit im öffentlichen Leben, Meinungsfreiheit und ziviles Engagement. Mit dem Lauschangriff wird selbst in den intimsten persönlichen Raum eingegriffen. Mit dem Abbau von Zeugnisverweigerungsrechten und Berufsgeheimnissen wird die personelle Geheimsphäre eingeschränkt. Mit Konsum- und Kommunikationsprofilen sowie sozialen und ökonomischen Rastern, erstellt und zusammengefügt in privaten und öffentlichen Datenbanken – unter Auswertung von bei immer mehr alltäglichen Verrichtungen anfallenden Datenschatten und von immer raffinierter erhobenen Datenbeständen – werden die Menschen zu Informationsmustern reduziert, deren Verhalten nicht durch gesellschaftlich demokratisch ausdiskutierte Ge- und Verbote festgelegt wird, sondern durch soziale Ein- und Ausgrenzung, durch gezieltes Verteilen bzw. Vorenthalten von Informationen und von materiellen Ressourcen. Beschäftigte in multinationalen Konzernen müssen erleben, dass ihre Leistungs- und Verhaltensdaten weltweit abrufbar sind und rücksichtslos ausgewertet werden. Die Spitze der informationellen Ausbeutung der Menschen droht durch die Analyse des menschlichen Genoms und durch die Auswertung dieser Informationen. Die als ‚Informationsvorsorge' oder ‚informationelle Fürsorge' präsentierten Maßnahmen haben gravierende Auswirkungen auf die betroffenen Menschen. Sie werden zu reinen Objekten staatlicher und privatwirtschaftlicher Planungen. Die zumeist anonymen Planungen sind für die Betroffenen weder transparent, geschweige denn beeinflussbar.

Das Grundgesetz basiert auf einem positiven Menschenbild. Die letzten 16 unionsgeführten Regierungsjahre waren dagegen geprägt von einer Kontrollkultur. Basis der Erfassung war institutionelles Mißtrauen. Jede Form der Überwachung läßt sich dadurch scheinbar rational begründen, dass man unterstellt, Menschen mißbrauchen ihre Freiräume und Rechte. Mit der Unterstellung von Mißbrauch (z. B. des Asyl- oder des Demonstrationsrechts, von Versicherungs- und Sozialleistungen) läßt sich die Durchleuchtung auch noch des letzten Winkels in unserem Leben rechtfertigen. Die Überwachung verhindert jedoch nicht den Mißbrauch; oft wird das Gegenteil erreicht. Überzogene Kontrolle ermuntert zum Umgehen der Überwachung; das institutionelle Mißtrauen verringert die Bereitschaft zur freiwilligen Ehrlichkeit. Sicherlich bedarf es in einer hochtechnischen Risikogesellschaft an vielen Stellen der Kontrolle. Diese muss sich aber immer im Rahmen der Verhältnismäßigkeit bewegen. Vor einer personenbezogenen Überwachung sind zunächst Verfahren zu prüfen, bei denen nur eine sach- bzw. technikbezogene oder nur eine anonyme Kontrolle erfolgt.

Sah man in der Vergangenheit die größte Gefahr für das Persönlichkeitsrecht der Menschen im Staat als ‚Big Brother' oder als ‚Leviathan', so hat sich die Bedrohung erweitert: Zunehmend sammeln private Wirtschaftsunternehmen, insbesondere im Elektronik- und Medienbereich, persönliche Daten für Zwecke der Kontrolle und Manipulation und nutzen diese Mittel zum Zweck der Machtausübung und aus Profitinteresse. Big Brother hat Geschwister bekommen, die ihn hinsichtlich der Verweigerung informationeller Selbstbestimmung oft schon weit übertreffen.

Um dem Trend zunehmender Überwachung mit Hilfe moderner Informationstechnik entgegenzuwirken, hat das Bundesverfassungsgericht 1983 aus der Menschenwürde (Artikel 1 Absatz 1 GG) und dem allgemeinen Freiheitsgrundrecht (Artikel 2 Absatz 1 GG) ein ‚Grundrecht auf informationelle Selbstbe-

stimmung‘ abgeleitet. Dieses Grundrecht, kurz ‚Recht auf Datenschutz‘ genannt, ist Grundbedingung für eine menschen- und bürgerrechtskonforme demokratische Informationsgesellschaft.

Verfassungsrechtlich versuchte man nun das Grundrecht auf informationelle Selbstbestimmung sowie die sonstigen Freiheitsgrundrechte (Unverletzlichkeit der Wohnung, Unschuldsvermutung, Meinungs- und Versammlungsfreiheit usw.) durch ein ‚Grundrecht auf Sicherheit‘ zu relativieren. Damit wurde auf der Basis berechtigter Sicherheitsinteressen und dem kollektiven Schüren von Angst ein rechtliches Konstrukt aufgebaut, mit dem jegliche verfassungsrechtliche Freiheitsgewährleistung beschnitten werden kann. Damit geriet auch aus dem Blick, dass ‚öffentliche Sicherheit‘ ein gesellschaftliches Gut ist, das nicht rechtlich erzwungen und eingeklagt werden kann, sondern politisch gestaltet werden muss.

Das Defizit der rot-grünen Koalitionsvereinbarung besteht darin, dass sie die Problematik informationstechnischer Überwachung nicht zur Kenntnis nimmt. Eine in der Vereinbarung liegende Chance besteht aber darin, dass sie – ungeachtet der technischen Gegebenheiten – dennoch Rahmenbedingungen benennt, die eine bürgerrechtskonforme Informationstechnikpolitik ermöglichen. Dieses Potential gilt es auszuschöpfen. Die Deutsche Vereinigung für Datenschutz sieht ihre Aufgabe darin, gemeinsam mit anderen Bürgerrechtsorganisationen durch kritische Politikbegleitung informationelle Selbstbestimmung in allen Lebensbereichen einzufordern und für deren Realisierung zu kämpfen.

Im Datenschutzrecht müssen alte Zöpfe geköpft werden. Statt der abwehrenden, muss diesem Recht eine gestaltende Funktion gegeben werden für eine moderne bürgerrechtskonforme Informationsgesellschaft. Entfielen bisher gesellschaftliche Gefahren, so wurden die Instrumente zu deren Bekämpfung nicht wieder abgeschafft, sondern beibehalten für evtl. neue, noch nicht bekannte Anwendungsfelder (Gefahr des ‚Kommunismus‘, dann Terrorismus, jetzt ‚Organisierte Kriminalität‘). Zugleich wurden privaten Überwachungspraktiken keine wirksamen Grenzen gesetzt. Diese Altlasten müssen aufgearbeitet und bereinigt werden. Das Rad staatlicher Überwachung ist zurückzudrehen. Es sind Evalutionsinstrumente zu schaffen, mit denen die Wirkungen und die Wirksamkeit staatlicher Kontrolle untersucht werden (können). Durch verfahrensrechtliche Sicherungen ist zu verhindern, dass Kontrollmonopole missbraucht werden. Neue Formen des Grundrechtsschutzes sind zu installieren. Gegenüber privaten wie öffentlichen Stellen sind den Betroffenen Abwehrrechte zur Verfügung zu stellen. Ihnen muss das rechtliche und technische Knowhow vermittelt werden, sich der Risiken der Informationstechnik bewußt zu werden und sich selbst zu schützen.“

(Deutsche Vereinigung für Datenschutz, Datenschutzrechtliche Erwartungen an die rot-grüne Bundesregierung, Januar 1999, S. 1 bis 2)

Die Deutsche Vereinigung für Datenschutz fordert von der Bundesregierung u. a.:

„Noch im Jahr 1999 muss ein Bundesdatenschutzgesetz verabschiedet werden, das nicht nur den Vorgaben der europäischen Datenschutzrichtlinie, sondern auch den neuen technischen Herausforderungen und Möglichkeiten gerecht wird.

– Ein modernes Datenschutzrecht hat die Grundsätze der Datenvermeidung und Datensparsamkeit (...), des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

– Den Betroffenen sind vertrauenswürdige Verschlüsselungsverfahren zum Schutz ihrer elektronischen Kommunikation anzubieten. Die Vorstellung, jede elektronische Kommunikation müsse staatlich beobachtbar sein, muss aufgegeben werden. (...)

– Dem klassischen Datenschutz ist ein Recht auf Informationsfreiheit an die S. zu stellen.

- Informationsfreiheit und informationelle Selbstbestimmung gehören als verfassungsrechtliche Rahmenbedingungen einer demokratischen Informationsgesellschaft ins Grundgesetz. (...)
- Die Datenschutzkontrolle im öffentlichen und nicht-öffentlichen Bereich ist institutionell zusammenzufassen und organisationsrechtlich völlig unabhängig auszugestalten.
- Die Datenschutzbehörden sind endlich angemessen personell und materiell auszustatten und neben ihren traditionellen Kontrollaufgaben mit neuen Aufgaben im Bereich der Beratung und der Dienstleistung für Betroffene und Anwender zu betrauen.
- Datenschutzorganisationen wie die Deutsche Vereinigung für Datenschutz genießen zwar öffentliche Aufmerksamkeit, sind aber nicht formell in Entscheidungsprozesse eingebunden. Nach dem Vorbild des Umweltrechts ist die Beteiligung von Verbänden im Bereich des Datenschutzes zu verbessern.
- Datenschutzrecht wird immer vorrangig als Sicherheitsrecht verstanden, nicht als Grundrechtsschutz. Organisationsrechtlich gehört dieser Bereich zum Verfassungs-, also zum Justiz-, nicht zum Innenressort.
- Das seit 15 Jahren fällige Arbeitnehmerdatenschutzgesetz ist endlich zu schaffen. Hierbei sind die Arbeitnehmer-Vertretungen einzubeziehen. Die Rechte der Betroffenen sind zu stärken, insbesondere auch gegenüber multinationaler Konzerndatenverarbeitung.
- In vielen Bereichen, z. B. beim Adressenhandel oder bei Finanzdienstleistern, sind die bestehenden Widerspruchs- durch Einwilligungsregelungen zu ersetzen.
- Verbraucherschutzvorschriften im Rahmen der Datenverarbeitung der Versicherungs- und Finanzwirtschaft sind überfällig.
- Die Datenschutzbestimmungen im Multimediarecht sind fortzuschreiben. (...)
- Die Befugnisse zum informationellen Eindringen in die privaten Wohnungen (Lauschangriff) sind zurückzunehmen.
- Das Telekommunikationsrecht muss derart überarbeitet werden, dass das Recht auf telekommunikative Selbstbestimmung nicht durch sicherheitsbehördliche Zugriffsrechte ad absurdum geführt wird.
- Zur informationellen Gewaltenteilung gehört die organisatorische Trennung von Innen- und Justizressorts.
- Die deutschen Geheimdienste BND, BfV und MAD sind tendenziell aufzulösen. Zunächst sind diese aus der Zeit des Kalten Krieges stammenden Institutionen personell und bez. ihrer Befugnisse zu reduzieren. Kurzfristig sollten deren geheimdienstliche Aufgaben durch öffentliche Bildungsaufgaben abgelöst werden.
- Das Bundeskriminalamt (BKA) ist bez. Personal und Befugnissen zugunsten der Länderpolizeien zu reduzieren.
- Die Befugnisse zur anlaßunabhängigen Personenkontrolle des Bundesgrenzschutzes (BGS) sind zurückzunehmen.
- Die Datenspeicherung in der Gen-Datei ist zu beschränken auf klar gesetzlich definierte schwere Straftaten und einer engeren Zweckbindung zu unterwerfen.
- Das Ausländerzentralregister ist von seiner sicherheitsbehördlichen Funktion zu befreien und auf rein ausländerrechtliche Zwecke zu beschränken.
- Maßnahmen verdeckter polizeilicher Datenverarbeitung sind in Rechtstatsachenstellen auf ihre Wirkungen und Notwendigkeit hin zu evaluieren.
- Die Datenerhebungsbefugnisse nach dem Anti-Terrorismusrecht sind zu überprüfen und zurückzunehmen.

– Technische Maßnahmen, die eine Totalkontrolle von Menschen erlauben (z. B. elektronischer Hausarrest, AsylCard) sind nicht weiterzuverfolgen. (...)

– Die Datenverarbeitungsregelungen im Sozialrecht (SGB) sind umfassend zu überarbeiten. Hierbei muss die ursprüngliche Idee des SGB, Berufsgeheimnisse und das Sozialgeheimnis normativ abzusichern, wieder zum Tragen gebracht zu werden.

– Das medizinische Datenschutzrecht entspricht in keiner Weise mehr den technischen Gegebenheiten der Diagnostik, der medizinischen Kommunikation und den organisatorischen und ökonomischen Verhältnissen. Dem kann durch ein bereichsspezifisches übergreifendes Medizindatenschutzrecht in Form eines Rahmengesetzes abgeholfen werden. Hierbei ist, v. a. für den Bereich der Gentechnik, ein ‚Recht auf Nichtwissen' vorzusehen. Medizinische Forschungsdaten müssen beschlagnahmefest gemacht werden.

– Im Melderecht sind Übermittlungen an Parteien, Adreßbuchverlage u. ä. Nutzungen unter Einwilligungsvorbehalt zu stellen.

– Planungen für eine Volkszählung als eine Voll-Zwangserhebung sollten zugunsten einfacherer und weniger belastender statistischer Methoden aufgegeben werden. (...)

– Die Schaffung eines Datenschutzrechtes auf europäischer Ebene und einer unabhängigen Kontrollinstanz sind voranzutreiben.

– Bei der Verhandlung mit Drittstaaten, namentlich den USA, über angemessene Datenschutzstandards beim Datenexport sind unabhängige Kontrollen, die Beachtung des Zweckbindungsgrundsatzes und der Betroffenenrechte unabdingbare Voraussetzungen.

– Europol muss so umgestaltet werden, dass nur klar definierte, engbegrenzte Befugnisse übertragen werden und eine parlamentarische und rechtliche Kontrolle ermöglicht wird.

– Vor der Einführung neuer europäischer Datenbanken ist eine umfassende Erforderlichkeits- und Subsidiaritätsprüfung im Rahmen einer öffentlichen Debatte vorzunehmen." (Deutsche Vereinigung für Datenschutz, a. a. O., S. 3 bis 5)

Vorbemerkung

Die Bundesregierung weist darauf hin, dass es sich mit Blick auf den Umfang des Fragenkatalogs (17 Einzelfragen mit bis zu jeweils 14 Unterfragen) nicht um eine „Kleine Anfrage" im Sinne der Gemeinsamen Geschäftsordnung (GGO) handelt; deren Rahmen wird hier deutlich gesprengt.

1. Welche allgemeinen und besonderen Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um den Datenschutz in der Bundesrepublik Deutschland zu verbessern?

Die Bundesregierung betreibt mit Nachdruck die Umsetzung der EG-Datenschutzrichtlinie in nationales Recht. Die Arbeiten an dem Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze kommen gut voran. Mit einer parlamentarischen Befassung ist noch in diesem Jahr zu rechnen.

Im Übrigen wird auf die nachfolgenden Ausführungen verwiesen.

2. Welche Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um

   a. Datenschutz durch Technik, Zweckbindung der Daten und ihres Verwendungszusammenhanges in den Mittelpunkt zu stellen;

Sowohl der Zweckbindungsgrundsatz als auch die Maßgeblichkeit des Verwendungszusammenhangs beim Umgang mit personenbezogenen Daten sind seit dem sog. Volkszählungsurteil des Bundesverfassungsgerichts aus dem Jahre 1983 wichtige Kriterien im Rahmen jeder Maßnahme der Bundesregierung auf dem Gebiet des Datenschutzes. Eine Notwendigkeit für gesonderte Maßnahmen der Bundesregierung, die Zweckbindung der Daten und ihren Verwendungszusammenhang in den Mittelpunkt zu stellen, ist daher nicht erkennbar.

Soweit die Frage auf Datenschutz durch Technik abstellt, ist darauf hinzuweisen, dass der Entwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze seit Oktober 1998 um mehrere einschlägige Vorschriften ergänzt wurde. An erster Stelle ist hier die Aufnahme des Prinzips der Datenvermeidung und -sparsamkeit in den Entwurf zu nennen. Der Durchsetzung dieses Prinzips dient die gleichfalls in den Entwurf aufgenommene Verpflichtung zum vorrangigen Gebrauch anonymer und pseudonymer Formen der Datenverarbeitung. Datenschutz durch Technik wird auch durch die Aufnahme eines grundsätzlichen Gebotes der Trennung von zu unterschiedlichen Zwecken erhobenen Daten in den o.g. Entwurf gefördert.

   b. Grundsätze der Datenvermeidung und Datensparsamkeit durchzusetzen;

Auf die Antwort zu Frage 2.a) wird verwiesen.

   c. den Betroffenen vertrauenswürdige Verschlüsselungsverfahren zum Schutz ihrer elektronischen Kommunikation anzubieten;

Die Bundesregierung hat mit den „Eckpunkten der deutschen Kryptopolitik“ vom 2. Juni 1999 beschlossen, die Verbreitung sicherer Verschlüsselung in Deutschland aktiv zu unterstützen. Gegenwärtig wird auf der Basis dieser Eckpunkte ein Konzept zur Ausgestaltung der deutschen Kryptopolitik entwickelt, um dadurch die Sicherheit von Staat, Wirtschaft und Gesellschaft in den weltweiten Informationsnetzen zu verbessern. Das Bundesamt für Sicherheit in der Informationstechnik wurde angewiesen, künftig auch die Sicherheit und Vertrauenswürdigkeit von Verschlüsselungsprodukten zu prüfen, zu bewerten und zu zertifizieren.

   d. dem Datenschutzrecht ein Recht auf Informationsfreiheit an die Seite zu stellen;

Zur Verbesserung der Transparenz und zur Förderung der Beteiligung der Bürger wird zur Zeit ein Entwurf für ein Akteneinsichts- und Informationszugangsgesetz erstellt, das auch den teilweise gegenläufigen Belangen des Datenschutzrechts Rechnung tragen wird.

e. die Informationsfreiheit und das informationelle Selbstbestimmungsrecht als verfassungsrechtliche Rahmenbedingungen in das Grundgesetz aufzunehmen;

Vorschläge zur ausdrücklichen Verankerung des in Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG enthaltenen Rechts auf informationelle Selbstbestimmung sowie eines allgemeinen Informationszugangsrechts im Grundgesetz haben bei den Beratungen über eine Verfassungsreform in der 12. Legislaturperiode des Deutschen Bundestages keine Mehrheit gefunden. Die Bundesregierung sieht keine Anhaltspunkte dafür, dass sich heute für entsprechende Vorschläge eine verfassungsändernde Mehrheit finden würde. Sie hat daher davon abgesehen, dieses Thema erneut zum Gegenstand verfassungspolitischer Initiativen zu machen.

f. die Datenschutzkontrolle im öffentlichen und nichtöffentlichen Bereich institutionell zusammenzufassen und organisationsrechtlich völlig unabhängig auszugestalten;

Die Frage nach einer institutionellen Zusammenfassung der Datenschutzkontrolle im öffentlichen und nichtöffentlichen Bereich sowie ihrer Ausgestaltung als völlig unabhängig stellt sich nur im Bereich der Länder, da nur diese über datenschutzrechtliche Kontrollkompetenzen sowohl im öffentlichen Bereich (s. die jeweiligen Landesdatenschutzgesetze) als auch im nichtöffentlichen Bereich (s. hierzu das BDSG) verfügen. Das BDSG sieht für den nichtöffentlichen Bereich insoweit vor, dass die Landesregierungen oder die von ihnen ermächtigten Stellen die für die Überwachung der Durchführung des Datenschutzes zuständigen Aufsichtsbehörden bestimmen.

Die EG-Datenschutzrichtlinie wiederum enthält eine Vorschrift, wonach die Kontrollstellen die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. Dieser Vorgabe der Richtlinie entsprechend wurde in den Entwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze eine Vorschrift aufgenommen, derzufolge die Aufsichtsbehörden der Länder für den Datenschutz im nichtöffentlichen Bereich in Ausübung ihrer Rechte unabhängig und nur dem Gesetz unterworfen sind und der Rechtsaufsicht der Landesregierung oder der zuständigen obersten Landesbehörde unterstehen.

g. die Datenschutzbehörden personell und materiell angemessen auszustatten;

Nach Auffassung der Bundesregierung ist die Dienststelle des Bundesbeauftragten für den Datenschutz (BfD) personell und materiell angemessen ausgestattet, so dass es keine Veranlassung für weitere Aufstockungen gibt. Dies wird schon dadurch deutlich, dass sich der Stellenbestand des BfD von insgesamt 19 im Jahre 1978 auf 57 im Haushaltsjahr 1999 erhöht hat. Davon wurden allein 4 im Haushaltsjahr 1999 – trotz der insgesamt äußerst restriktiven Haushaltspolitik – neu bewilligt.

h. die Datenschutzbehörden neben ihren traditionellen Kontrollaufgaben mit neuen Aufgaben im Bereich der Beratung und der Dienstleistung für Betroffene und Anwender zu betrauen;

In den Entwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze ist eine ausdrückliche Befugnis des Bundesbeauftragten für den Datenschutz aufgenommen worden, sich jederzeit an Parlament und Öffentlichkeit wenden zu dürfen, um diese über wichtige Entwicklungen des Datenschutzes sowohl im öffentlichen als auch im nichtöffentlichen Bereich zu unterrichten.

Der BfD hat zur Frage wie folgt Stellung genommen: „Der BfD hat den Bereich der Beratung und Dienstleistung für die Bürgerinnen und Bürger sowie für die datenverarbeitenden Stellen ständig ausgebaut. Er steht gemessen am Arbeitseinsatz deutlich vor den Kontrollaktivitäten.

Seit Februar 1999 ist der BfD im Internet mit einer eigenen Website vertreten (http://www.bfd.bund.de). Auf diesem Weg wird schneller Rat vor allem zu den modernen Techniken erwartet, etwa zur Frage, wie Kreditkartendaten im Web sicher weitergegeben werden können. Die Website wird weiter ausgebaut, damit auch speziellere und vertiefte Informationen schnell und rationell bereitgestellt werden können.

Für spezielle Anwendergruppen, insbesondere für Telekommunikationsdiensteanbieter, hat der BfD einen ‚runden Tisch' eingerichtet, wo regelmäßig allgemein interessierende datenschutzrelevante Fragen diskutiert werden."

i. Datenschutzorganisationen in Entscheidungsprozesse – nach dem Vorbild des Umweltschutzes – einzubinden;

Die GGO der Bundesministerien sieht eine Unterrichtung der maßgeblichen Fachkreise und Verbände sowie deren Möglichkeit zur Stellungnahme im Rahmen der Vorbereitung von Gesetzen vor. Die Bundesregierung ist der Auffassung, dass diese Einbindung sachgerecht, aber auch ausreichend ist.

j. Datenschutz statt dem Innenressort endlich dem Justizressort zuzuordnen;

Die Zuordnung des Datenschutzes zum Innenressort ist nach Auffassung der Bundesregierung sachgerecht, da es sich beim Datenschutz um eine Aufgabe der allgemeinen inneren Verwaltung handelt.

k. ein Arbeitnehmerdatenschutzgesetz zu schaffen und die Rechte der Betroffenen gegenüber multinationaler Konzerndatenverarbeitung zu stärken;

Die Bundesregierung sieht die Schaffung eines Arbeitnehmerdatenschutzgesetzes als dringlich an. Das Bundesministerium für Arbeit und Sozialordnung wird deshalb noch in dieser Legislaturperiode im Anschluß an die Novellierung des BDSG den Entwurf für ein Arbeitnehmerdatenschutzgesetz vorlegen.

Das BDSG enthält keine Bestimmungen, die den Umgang mit Arbeitnehmerdaten zwischen konzernangehörigen, aber rechtlich selbständigen Unternehmen im Vergleich zum Datenverkehr mit Dritten begünstigen. Es ist nicht vorgesehen, dies zu ändern. Da künftig Arbeitnehmerdaten gegenüber Dritten verbesserten

Schutz erfahren, wird sich daraus auch eine Stärkung der Rechte des Arbeitnehmers gegenüber der Konzerndatenverarbeitung ergeben.

l. im Adressenhandel oder bei Finanzdienstleistern die bestehenden Widerspruchs- durch Einwilligungsregelungen zu ersetzen;

Im Entwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze ist eine Verbesserung der geltenden Rechtslage für Betroffene insoweit vorgesehen, als diese nunmehr bei der Ansprache zum Zwecke der Werbung oder der Markt- oder Meinungsforschung über die verantwortliche Stelle, die Herkunft der Daten sowie über ihr Widerspruchsrecht gegen die Nutzung oder Übermittlung personenbezogener Daten zu den o. g. Zwecken zu unterrichten sind. Diese Regelung gilt auch für Finanzdienstleister, soweit diese Werbung betreiben.

m. Verbraucherschutzvorschriften im Rahmen der Datenverarbeitung der Versicherungs- und Finanzwirtschaft zu schaffen;

Die Bundesregierung hat keine spezifischen dahin gehenden Maßnahmen über die allgemein geltenden Regelungen hinaus ergriffen.

n. Datenschutzbestimmungen im Multimediarecht fortzuschreiben?

Am 1. August 1997 ist in Deutschland das Informations- und Kommunikationsdienstegesetz (IuKDG) in Kraft getreten, dessen Artikel 2 das Gesetz über den Datenschutz bei Telediensten (TDDSG) enthält. Aufgrund eines Evaluierungsauftrages des Deutschen Bundestages (Drucksache 13/7935 vom 11. Juni 1997) hat das Bundesministerium für Wirtschaft und Technologie mit Schreiben vom 17. Juni 1999 den Bericht der Bundesregierung über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten im Zusammenhang mit der Umsetzung des IuKDG dem Deutschen Bundestag zugeleitet (Drucksache 14/1191 vom 18. Juni 1999, S. 13 bis 16, 33). Darin werden auch die Erfahrungen mit dem TDDSG sowie der weitere Handlungsbedarf dargestellt. Auf den Regierungsbericht wird verwiesen.

3. Welche Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um im Bereich der Inneren Sicherheit

a. die Befugnisse zum informationellen Eindringen in die private Wohnung (Lauschangriff) zurückzunehmen;

Im Frühjahr 1998 sind die Gesetze in Kraft getreten, die zur verbesserten Bekämpfung insbesondere schwerwiegender Formen der organisierten Kriminalität die akustische Wohnraumüberwachung zu Zwecken der Strafverfolgung ermöglichen. Vorausgegangen waren intensive Erörterungen in den parlamentarischen Gremien. Die nach dem Vermittlungsverfahren verabschiedeten Änderungen der Strafprozessordnung tragen sowohl den Belangen der Strafverfolgung als auch dem Schutz des Persönlichkeitsrechts der Betroffenen Rechnung. Ob und welche Änderungen ggf. vorzunehmen sind, wird nach Vorliegen aussagekräftiger Erfahrungen mit den gesetzlichen Regelungen, insbesondere aufgrund des von der Bundesregierung bis zum 31. Januar 2002 zu erstattenden Erfahrungsberichts an den Deutschen Bundestag zu beurteilen sein.

b. das Telekommunikationsrecht derart zu überarbeiten, dass das Recht auf telekommunikative Selbstbestimmung nicht durch sicherheitsbehördliche Zugriffsrechte ad absurdum geführt wird;

Eingriffe in das Fernmeldegeheimnis richten sich nach den strengen Voraussetzungen des Gesetzes zu Artikel 10 Grundgesetz (G 10), der Strafprozeßordnung und des Außenwirtschaftsgesetzes. Die Bundesregierung teilt die in der Frage zum Ausdruck gebrachte Bewertung, dass ein „Recht auf telekommunikative Selbstbestimmung“ durch „sicherheitsbehördliche Zugriffrechte“ ad absurdum geführt werde, nicht.

c. die nachrichtendienstliche Tätigkeit des BfV, BND und MAD und deren Befugnisse zur Erhebung, Speicherung, Aufbewahrung und Weitergabe von Daten einzuschränken;

Die Voraussetzungen, unter denen das BfV, der BND und der MAD Daten erheben, speichern, aufbewahren und weitergeben dürfen, sind im Bundesverfassungsschutzgesetz (BVerfSchG), im BND-Gesetz und im MAD-Gesetz geregelt. Für die betroffenen Vorschriften besteht derzeit kein Änderungsbedarf.

d. die Möglichkeit der Weitergabe von Daten durch das BfV an Private abzuschaffen;

Die Bundesregierung hat keine Maßnahmen im Sinne der Fragestellung ergriffen und beabsichtigt keine Änderung von § 19 Abs. 4 BVerfSchG, der Datenübermittlungen an Private nur unter engen Voraussetzungen, nur in zwingenden Ausnahmefällen und nur mit Zustimmung des Bundesministers des Innern zulässt. Darüber hinaus schreibt diese Bestimmung weitere datenschutzrechtliche Sicherungen vor, insbesondere gesonderte Nachweise über diese Übermittlungen zur Ermöglichung effektiver datenschutzrechtlicher Kontrollen.

e. Personal und Befugnisse des BKA zugunsten der Länderpolizeien zu reduzieren;

f. die Befugnisse des BKA zur Erhebung, Speicherung, Aufbewahrung und Weitergabe nach und nach einzuschränken;

Am 1. August 1997 ist das Bundeskriminalamtgesetz (BKAG) in Kraft getreten. Ziel dieses Gesetzes war die bereichsspezifische Umsetzung des Volkszählungsurteils (BVerfGE 65, 1) bei der Kriminalpolizei des Bundes. Das BKAG enthält ausgewogene Regelungen für die Datenverarbeitung im BKA sowie die Zusammenarbeit des Bundes mit den Ländern in kriminalpolizeilichen Angelegenheiten.

Nach nunmehr zwei Jahren seit Inkrafttreten des Gesetzes kann festgestellt werden, dass sich das BKAG bewährt hat. Es besteht ebensowenig Anlaß, die getroffene Kompetenzverteilung zwischen BKA und Länderpolizeien zu ändern, wie ein Grund ersichtlich ist, die Befugnisse des BKA zur Erhebung und Verwendung personenbezogener Daten einzuschränken. Das BKA muss, um die ihm übertragenen Aufgaben (§§ 2 bis 6 BKAG) erfüllen zu können, mit den entsprechenden Kompetenzen und Befugnissen ausgestattet sein; dies ist im BKAG erfolgt.

g. den Betroffenen zu garantieren, dass durch das BKA aus seinen Dateien gelöschte Daten auch tatsächlich gelöscht werden und später nicht wieder abrufbar sind;

Die Löschung von personenbezogenen Daten richtet sich nach § 32 BKAG (zum Begriff des Löschens s. § 3 Abs. 5 Nr. 5 BDSG). Die Löschung erfolgt beim BKA als physikalische Löschung, so dass die Daten auch tatsächlich nicht mehr abrufbar sind. Natürlich findet auch eine Kontrolle der informationellen Tätigkeit des BKA statt. Hier ist zum einen auf die Kontrolle durch den Bundesbeauftragten für den Datenschutz hinzuweisen. Darüber hinaus ist besonders darauf hinzuweisen, dass es bereits seit 1978 im BKA einen behördlichen Datenschutzbeauftragten gibt, der mit inzwischen fünf Mitarbeitern die Kontrollaufgaben wahrnimmt.

h. die Befugnisse des BGS zur anlaßunabhängigen Personenkontrolle des BGS zurückzunehmen;

Die in einem breiten politischen Konsens beschlossene Befugniserweiterung zu lageabhängigen Personenkontrollen des BGS ist durch Artikel 2 Abs. 2 des Ersten Gesetzes zur Änderung des Bundesgrenzschutzgesetzes vom 25. August 1998 (BGBl. I S. 2486) bis zum 31. Dezember 2003 befristet. Bis zu diesem Zeitpunkt wird entschieden, ob die Regelungen auslaufen oder unbefristet weitergelten sollen.

i. die Datenerhebungsbefugnisse nach dem Anti-Terrorismusrecht zurückzunehmen;

Strafprozessuale Ermittlungsbefugnisse in diesem Bereich sind zur Verfolgung schwerwiegender Kriminalitätsformen auch weiterhin erforderlich.

j. auf die Einführung von technischen Maßnahmen, die eine Totalkontrolle von Menschen erlauben, zu verzichten;

Technische Maßnahmen, die eine Totalkontrolle von Menschen erlauben, sind der Bundesregierung nicht bekannt.

k. Datenschutzregelungen für das Zollkriminalamt und den Zollfahndungsdienst zu erarbeiten bzw. zu erlassen;

Ein Arbeitsentwurf für ein Gesetz über das Zollkriminalamt wird derzeit intensiv durch das Bundesministerium der Finanzen (BMF) mit dem Zollkriminalamt abgestimmt und soll danach unverzüglich den Ressorts zur Stellungnahme übersandt werden. Aufgrund der Komplexität des Regelungsbedarfs ist der benötigte Zeitaufwand beträchtlich. Es ist jedoch geplant, die Abstimmung im BMF im zweiten Halbjahr 1999 durchzuführen, so dass der Entwurf spätestens im Frühjahr 2000 mit den Ressorts abgestimmt werden kann. Für den Datenschutz bei den Zollfahndungsämtern gelten – ebenso wie bei den Dienststellen der Steuerfahndung – die Bestimmungen der Abgabenordnung.

l. die Genomanalyse im Strafverfahren zurückzuführen;

Die in den §§ 81a, 81e und 81f der Strafprozeßordnung geregelte molekulargenetische Untersuchung ist ein für die Strafverfolgung unverzichtbares Hilfsmittel, nicht zuletzt bei der Aufklärung schwerer Sexualdelikte. Die gesetzlichen Regelungen tragen sowohl den Erfordernissen der Strafverfolgung als auch dem Schutz des Persönlichkeitsrechts der Betroffenen Rechnung.

m. datenschutzrechtliche Bestimmungen für den Vollzug der Untersuchungshaft und den Jugendvollzug zu erlassen?

Die Bundesregierung hat am 28. April 1999 den Entwurf eines Gesetzes zur Regelung des Vollzuges der Untersuchungshaft beschlossen und in das Gesetzgebungsverfahren eingebracht (BR-Drucksache 249/99). Artikel 1 des Entwurfs überträgt die durch das Vierte Gesetz zur Änderung des Strafvollzugsgesetzes (4. StVollzGÄndG) eingeführten datenschutzrechtlichen Ergänzungen auf den Vollzug der Untersuchungshaft, indem er die §§ 179 bis 187 StVollzG mit bereichsspezifischen Maßgaben für entsprechend anwendbar erklärt (§ 36). Junge Untersuchungsgefangene sind in den Anwendungsbereich des Entwurfs einbezogen. Damit erstrecken sich die datenschutzrechtlichen Regelungen für den Vollzug der Untersuchungshaft auch auf diese Gruppe von Inhaftierten.

4. Welche allgemeinen Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um die Datenschutzbestimmungen im Sozialrecht neu zu regeln?

Die Bundesregierung wird durch den von ihr vorbereiteten Entwurf eines Gesetzes zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze auch das Sozialgesetzbuch so ändern, dass es der EG-Datenschutzrichtlinie entspricht und die im Bundesdatenschutzgesetz künftig enthaltenen modernen datenschutzrechtlichen Grundsätze wiedergibt.

Datenschutzrechtliche Regelungen enthält auch der Gesetzentwurf der Bundesregierung zur Reform der gesetzlichen Krankenversicherung ab dem Jahr 2000 – GKV-Gesundheitsreform 2000 – (BR-Drucksache 454/99).

5. Welche allgemeinen Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um die Datenschutzbestimmungen im Finanzwesen neu zu regeln und die Vorschläge des Bundesbeauftragten für den Datenschutz aus seinem 17. Tätigkeitsbericht (Drucksache 14/850) aufzugreifen?

Die datenschutzrechtlichen Empfehlungen des Bundesbeauftragten für den Datenschutz (BfD) wurden im Gesetzgebungsverfahren zum Steuerentlastungsgesetz 1999/2000/2002 vom 24. März 1999 berücksichtigt. So sind die Änderungen des § 45d EStG in datenschutzrechtlicher Hinsicht mit dem BfD abgestimmt. Auch außerhalb von Gesetzgebungsverfahren werden datenschutzrechtliche Empfehlungen zu steuerlichen Vorschriften sorgfältig geprüft und erforderliche Änderungen aufgegriffen.

Die im 17. Tätigkeitsbericht des Bundesbeauftragten für den Datenschutz enthaltenen Vorschläge sind von der Bundesregierung wie folgt aufgegriffen worden:

Freistellungsaufträge:

Mit Erlaß vom 5. Januar 1999 hat das Bundesministerium der Finanzen das Bundesamt für Finanzen angewiesen, nach pflichtgemäßem Ermessen einem Freistellungsauftraggeber Auskunft über die im Rahmen des Kontrollverfahrens nach § 45d EStG über ihn gespeicherten Daten zu erteilen, soweit der Freistellungsauftraggeber hierfür ein berechtigtes Interesse darlegt oder dies ohne weitere Ermittlungen ersichtlich ist und keine Versagungsgründe vorliegen. Die Bundesregierung hat dem Anliegen des Bundesbeauftragten für den Datenschutz damit im Wesentlichen kurzfristig im Wege einer pragmatischen Lösung entsprochen. Entgegen den geäußerten Befürchtungen des Bundesbeauftragten für den Datenschutz hat das Bundesamt für Finanzen seit Januar 1999 von 1163 schriftlichen Auskunftsersuchen lediglich in einem Fall eine Auskunft wegen der fehlenden Darlegung eines berechtigten Interesses versagen müssen (Stand: 2. August 1999).

Steuerliche Fahrtenbücher:

Mit Schreiben vom 23. Juli 1999 an den Bundesbeauftragten für den Datenschutz hat das Bundesministerium der Finanzen, unter Berücksichtigung datenschutzrechtlicher Belange, im Wesentlichen Folgendes klargestellt:
Zur ordnungsgemäßen Führung eines Fahrtenbuchs im Sinne des § 6 Abs. 1 Nr. 4 Satz 3 EStG ist es nicht erforderlich, den aufgesuchten Patienten im Fahrtenbuch namentlich zu benennen, wenn dessen Name und Anschrift vom Arzt in einem vom Fahrtenbuch getrennt zu führenden Verzeichnis festgehalten werden und sichergestellt ist, dass die Zusammenführung von Fahrtenbuch und Patientenverzeichnis leicht und einwandfrei möglich ist und keinen erheblichen Aufwand verursacht. Die Finanzbehörden sollen die Vorlage des Fahrtenbuchs bzw. des Verzeichnisses nicht regelmäßig verlangen, sondern nur, wenn – vornehmlich anlässlich einer Außenprüfung – festgestellt wird, dass tatsächliche Anhaltspunkte bestehen, die Zweifel an der Richtigkeit oder Vollständigkeit der Eintragungen im Fahrtenbuch begründen und die Zweifel nicht anders auszuräumen sind. Die Finanzbehörden reagieren auf die Nichtvorlage des Fahrtenbuchs/Verzeichnisses erfahrungsgemäß nicht mit Zwangsmitteln, sondern mit der Pauschalbesteuerung nach § 6 Abs. 1 Nr. 4 Satz 2 EStG.

Nach Auffassung der Bundesregierung sind damit die datenschutzrechtlichen Bedenken des Bundesbeauftragten für den Datenschutz ausgeräumt.

Abgabenordnung:

Die Vorschriften der Abgabenordnung (AO) sind auch unter datenschutzrechtlichen Gesichtspunkten verfassungskonform. Dies bestätigt die Rechtsprechung des Bundesverfassungsgerichts und des Bundesfinanzhofs. Beide Gerichte haben sich bereits mehrfach in datenschutzrechtlicher Hinsicht mit Vorschriften der Abgabenordnung befasst (§§ 30, 30a, 93 Abs. 1 Satz 1, § 194 Abs. 3, § 208 Abs. 1 AO) und diese ausdrücklich oder inzident für verfassungsgemäß angesehen. Aufgrund neuerer Entwicklungen (z. B. im Bereich neuer Informations- und Kommunikationstechniken) wird das Bundesministerium der Finanzen voraussichtlich noch in diesem Jahr erneut Gespräche mit dem Bundesbeauftragten für den Datenschutz zur Berücksichtigung datenschutzrechtlicher Belange in der Abgabenordnung aufnehmen.

Automatisiertes Abrufverfahren für Steuerdaten:

Die Sachverhaltsdarstellung des Bundesbeauftragten für den Datenschutz ist zutreffend. Das BMF arbeitet derzeit am Entwurf einer Steuerdaten-Abruf-Verordnung, die unter Einbeziehung der Gemeinden die in der Steuerdaten-Abruf-Verwaltungsregelung getroffenen Regelungen übernehmen wird. Ergänzend ist beabsichtigt, in Fällen der Nutzung eines öffentlich zugänglichen Übertragungsnetzes mit Wählverbindung eine Verschlüsselung der Daten vorzuschreiben. Ein Referentenentwurf wird voraussichtlich im Herbst vorgelegt.

Mitteilungsverordnung:

Die Zweite Verordnung zur Änderung der Verordnung über die Mitteilungen an die Finanzbehörden durch andere Behörden und öffentlich-rechtliche Rundfunkanstalten (Mitteilungsverordnung) vom 26. Mai 1999 (BStBl Teil I S. 524) hält die vom Gesetzgeber gezogenen Grenzen der Mitteilungspflicht ein.

6. Welche allgemeinen Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um die Datenschutzbestimmungen bei der Datenverarbeitung bei Familienkassen (Kindergeld) zu reformieren und die Vorschläge des Bundesbeauftragten für den Datenschutz aus seinem 17. Tätigkeitsbericht (Drucksache 14/850) aufzugreifen?

Unter Nummer 7.7.1 des 17. Tätigkeitsberichts hat der BfD in einem konkreten Fall die „Mißverständliche Anforderung von (Ausbildungs-)Nachweisen durch Familienkassen“ beschrieben. Auf Anregung des BfD wurde durch eine Änderung des Kindergeld-Merkblattes sichergestellt, dass künftig keine Zweifel über den Umfang des Nachweises eines Ausbildungsabschlusses mehr bestehen.

7. Welche Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um Daten von Kundinnen und Kunden vor Unternehmen zu schützen?

Auf die Antwort zu Frage 2l) wird verwiesen.

8. Welche Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um das medizinische Datenschutzrecht neu zu regeln?

Die Bundesregierung sieht keine Veranlassung, ein übergreifendes Medizindatenschutzrecht in Form eines Rahmengesetzes vorzuschlagen. Bereichsspezifische Datenschutzvorschriften können den jeweiligen Anforderungen der einzelnen Fachbereiche in geeigneter Weise angepaßt werden, um damit gleichzeitig konkret auf das für den Fachbereich erforderliche Ausmaß ausgestaltet zu werden.

9. Welche Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um im Melderecht den Datenschutz zu verbessern?

Die Umsetzung des 1994 novellierten Melderechtsrahmengesetzes in Landesrecht ist weitgehend abgeschlossen. Ungeachtet dessen prüft die Bundesregierung derzeit, ob u. a. im Hinblick auf die sich rasant entwickelnde Nutzung behördlicher Dienstleistungen mittels Internet (z. B. Internet-Zugang zu den kommunalen Melderegistern) weitere Änderungen im Melderecht veranlasst sind. Bei der Schaffung der hierzu möglicherweise erforderlichen Rechtsgrundlagen wird den datenschutzrechtlichen Belangen der betroffenen Bürger Priorität einzuräumen sein.

10. Welche Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um

    a. den Datenschutz von hier lebenden Ausländerinnen und Ausländern im Rahmen von Gesetzen und Verwaltungsvorschriften zu verbessern;

Vergleiche Antwort zu Frage 1. Bezüglich der hier lebenden Ausländer bestehen zusätzliche ausreichende Regelungen in bereichsspezifischen Vorschriften, z. B. im AZR-Gesetz. Der Entwurf der Verwaltungsvorschriften zum Ausländergesetz enthält Regelungen, die die datenschutzrechtlichen Bestimmungen des Ausländergesetzes präzisieren.

    b. die Möglichkeiten von staatlichen Stellen einzuschränken und zurückzuführen, Daten von Ausländerinnen und Ausländern zu erheben, zu speichern, aufzubewahren und weiterzuleiten;

Die Verarbeitung von Daten (§ 3 Abs. 5 BDSG) erfolgt auf Grund der in der Verwaltungspraxis festgestellten Notwendigkeiten unter Beachtung der gesetzlichen Vorgaben. Für die Förderung nach Einschränkungen gibt es keine überzeugenden Begründungen.

    c. alle Planungen bez. der Einführung einer Asyl-Card einzustellen;

Es gibt keine diesbezüglichen Planungen, sondern lediglich eine wissenschaftliche Studie mit Vorstellungen der Verfasser, zu denen die Bundesländer, deren Verwaltungspraxis im Sinne einer Harmonisierung der Verfahrensabläufe und Verwaltungsvereinfachung berührt würde, um Stellungnahme gebeten sind.

    d. erkennungsdienstliche Maßnahmen gegen Asylsuchende einzuschränken und zurückzuführen und die Weitergabe an nicht EU-Staaten sofort einzustellen;

Erkennungsdienstliche Maßnahmen bei Asylbewerbern werden im Rahmen der gesetzlichen Bestimmungen des AsylVfG durchgeführt. Sie sind notwendig, um ggf. Mehrfachanträge zu erkennen und die Verfahren ordnungsgemäß durchzuführen. Einschränkungen kommen daher nicht in Betracht. Das gilt im Wesentlichen auch für die in Absprache mit dem BfD vereinbarte Weitergabe von Daten aus ASYLON an einzelne Staaten, die nicht der EU angehören, wobei unverzichtbare Bedingung ist, dass sie ein dem deutschen Recht vergleichbares Datenschutzrecht haben.

    e. die gesetzlich ungeregelte Weitergabe von Daten aus ASYLON und dem AZR an das Liaisonpersonal sofort einzustellen;

Die Übermittlung von Daten aus ASYLON und dem AZR an Liaisonpersonal im BAFI erfolgt im erforderlichen Umfang, soweit das Liaisonpersonal Aufgaben des BAFI wahrnimmt und damit den für Bedienstete des BAFI geltenden datenschutzrechtlichen Regelungen sowie den Weisungen des BAFI unterliegt.

f. den Zugriff des Liaisonpersonals auf die Datenbanken des Bundesamtes für die Anerkennung ausländischer Flüchtlinge (BAFI) zu untersagen;

Auf die Antwort zu Frage 10e) wird verwiesen.

g. alle Planungen über die Einrichtung einer Warndatei einzustellen und die Praxis der Erhebung von Daten über Gastgeber von Flüchtlingen sofort einzustellen;

Die in der 13. Legislaturperiode durchgeführten Vorarbeiten für einen entsprechenden Referentenentwurf sind nicht weiterverfolgt worden.

Die Erhebung von Daten über Gastgeber von Flüchtlingen erfolgt im Zusammenhang mit der Abgabe von Verpflichtungserklärungen nach § 84 Abs. 1 AuslG. Sie soll die Beantwortung der Frage ermöglichen, ob der Gastgeber die von ihm zu übernehmenden Verpflichtungen tatsächlich erfüllen kann, um zu verhindern, dass letztlich die Allgemeinheit durch Inanspruchnahme von Sozialleistungen finanziell belastet wird.

h. die Praxis der Erhebung von Daten von Flüchtlingen, analog wie 1996 an den Flüchtlingen aus Bosnien-Herzegowina auf Anweisung des Bundesministeriums des Innern erstmals durchgeführt, sofort einzustellen?

Die Erhebung der Daten von Flüchtlingen analog der 1996 bei Flüchtlingen aus Bosnien und Herzegowina erfolgten Datenerhebung ist unverzichtbar, um die Durchführung einer geordneten Rückkehr zu gewährleisten.

11. Welche Maßnahme hat die Bundesregierung ergriffen, um

a. die Staatsangehörigkeitsdatei beim Bundesverwaltungsamt sofort zu schließen;

b. gegebenenfalls hierfür eine gesetzliche Regelung herbeizuführen?

Die beim Bundesverwaltungsamt geführte Staatsangehörigkeitsdatei dient insbesondere der oftmals schwierigen Nachweisführung hinsichtlich des Erwerbs der deutschen Staatsangehörigkeit sowie in Verfahren zur Feststellung der Spätaussiedlereigenschaft. Auskünfte über Staatsangehörigkeitsverhältnisse und Volkszugehörigkeit sind auch in Renten-, Lastenausgleichs- oder Erbschaftsangelegenheiten für die Betroffenen nicht selten von entscheidungserheblicher Bedeutung.

Welche Datenbestände künftig in der Staatsangehörigkeitsdatei gespeichert werden, soll im Rahmen der Neuregelung (Gesamtreform) des Staatsangehörigkeitsrechts festgelegt werden.

12. Welche Maßnahmen hat die Bundesregierung ergriffen, um den Einsatz der Chipkarten besser gesetzlich zu regeln?

In den Entwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) und anderer Gesetze wurde eine Vorschrift aufgenommen, die (auch) die Verwendung von Chipkarten regelt.

13. Welche Maßnahmen hat die Bundesregierung seit Oktober 1998 ergriffen, um den Datenschutz in der Europäischen Union und die Schaffung einer unabhängigen Kontrollinstanz voranzutreiben?

Der Erlaß einer Datenschutzregelung für die Organe und Einrichtungen der EU und die Schaffung einer unabhängigen Kontrollinstanz (Artikel 286 EG-Vertrag) obliegen dem Rat auf Vorschlag der Kommission (Artikel 251 EG-Vertrag). Im Juli 1999 hat die Kommission den Mitgliedstaaten den ersten Entwurf eines Vorschlags für eine solche Datenschutzregelung bekannt gemacht, der in den zuständigen Arbeitsgremien beraten werden wird. Die Bundesregierung begrüßt die Initiative der Kommission und wird den Rechtsetzungsakt – im Rahmen der ihr nach dem EG-Vertrag offen stehenden Möglichkeiten – konstruktiv unterstützen.

a. Wieso wurden die europäischen Datenschutzrichtlinien (95/46/EG) vom 24. Oktober 1995 nicht innerhalb der vorgeschriebenen dreijährigen Umsetzungsfrist in deutsches Recht umgesetzt?

Das deutsche Datenschutzrecht ist komplex strukturiert und vielgestaltig. Das Bundesdatenschutzgesetz selbst ist als Querschnittsregelung konzipiert, die – wenngleich auch nur subsidiär – in allen Rechtsbereichen zur Anwendung gelangt. Da die Umsetzung der Richtlinie schwerpunktmäßig durch die Änderung des Bundesdatenschutzgesetzes erfolgt, erstrecken sich die Auswirkungen der Novellierung zumindest mittelbar auch auf alle Rechtsbereiche. Dass der hieraus resultierende Abstimmungsbedarf erheblich ist, bedarf keiner näheren Darlegung. Erschwert wurde die Abstimmung zusätzlich durch die Existenz zahlreicher sogenannter bereichsspezifischer Datenschutzregelungen. Auch hier waren die Auswirkungen der Umsetzung flächendeckend zu prüfen, um widersprüchliche oder sachwidrige Regelungen zu vermeiden.

b. Wieso wurde die dreijährige Frist – trotz wiederholter Mahnungen durch den Bundesbeauftragten für den Datenschutz – nicht eingehalten?

Auf die Antwort zu Frage 13a) wird verwiesen.

c. Wie bewertet die Bundesregierung die Tatsache, dass Deutschland zu einem der vier Länder zählt, die diese Richtlinien nicht umgesetzt haben?

Deutschland verfügt bereits über ein anerkannt hohes Datenschutzniveau, das durch einen überaus hohen Normierungsgrad gekennzeichnet ist. So kennt das deutsche Datenschutzrecht – anders als das der meisten übrigen Mitgliedstaaten der Europäischen Union – nicht nur ein allgemeines Datenschutzgesetz, sondern

eine Vielzahl bereichsspezifischer Regelungen. Hinzu kommen auf Grund der föderativen Struktur Deutschlands in jedem Bundesland weitere Datenschutzgesetze sowohl allgemeiner als auch bereichsspezifischer Art. Nach Auffassung der Bundesregierung ist daher Zurückhaltung bei einem wertenden Vergleich mit dem Stand der Umsetzung der Richtlinie in anderen Mitgliedstaaten der Europäischen Union geboten.

d. Welche Probleme haben sich daraus – nach Kenntnis der Bundesregierung – für den Datenschutz und die Landesgesetzgebung in den einzelnen Bundesländern ergeben?

Nach Kenntnis der Bundesregierung haben sich aus der nicht fristgerechten Umsetzung der Richtlinie bislang weder Probleme für den Datenschutz noch für die Landesgesetzgebung in den einzelnen Bundesländern ergeben.

e. Welche Probleme ergeben sich hieraus bez. eines angestrebten harmonisierten Datenverkehrs innerhalb des europäischen Binnenmarktes?

Datenflüsse von Stellen in Deutschland zu Empfängern in anderen Staaten der EU sind schon heute vielfach bereichsspezifisch und richtlinienkonform geregelt. Der Rückgriff auf allgemeine Regelungen wie § 17 BDSG ist daher meist gar nicht erforderlich. Zudem stellt § 17 BDSG keine mit der EG-Datenschutzrichtlinie unvereinbaren Anforderungen an Übermittlungen zu Empfängern in anderen Staaten der EU.

f. Welche Schadensersatzforderungen hat die Bundesrepublik Deutschland aus der nicht fristgemäßen Umsetzung der europäischen Datenschutzrichtlinien bisher erhalten bzw. zu erwarten; und wer haftet dafür?

Der Bundesregierung sind keine Schadensersatzforderungen im Zusammenhang mit der nicht fristgerechten Umsetzung der Richtlinie bekannt. Angesichts der Ausgestaltung der Regelungen der Richtlinie ist die Wahrscheinlichkeit entsprechender Schadensersatzforderungen als eher gering einzuschätzen. Haften würde dafür die Bundesrepublik Deutschland.

g. Welche personellen und politischen Konsequenzen zieht die Bundesregierung aus diesem Verhalten in bezug auf die nicht fristgerechte Umsetzung der europäischen Datenschutzrichtlinien?

Die Bundesregierung sieht keine Veranlassung, in dieser Richtung Überlegungen anzustellen.

h. Wann wird mit der Umsetzung der europäischen Datenschutzrichtlinien durch die Bundesregierung zu rechnen sein?

Auf die Antwort zu Frage 1 wird verwiesen.

14. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Befugnisse von Europol einzuschränken und statt dessen eine parlamentarische und rechtliche Kontrolle über Europol zu ermöglichen?

Zunächst ist festzuhalten, dass Europol nach der derzeitigen Rechtslage keine strafprozessualen Ermittlungszuständigkeiten mit Eingriffscharakter besitzt, sondern die Aufgabe hat, durch Sammlung und Analyse von Daten die nationalen Behörden in ihrer Tätigkeit zu unterstützen. Die Frage nach einer Einschränkung der Befugnisse von Europol stellt sich daher nicht.

Bei der Forderung nach einer (verbesserten) parlamentarischen Kontrolle von Europol ist zunächst zu berücksichtigen, dass es sich um eine Einrichtung der Regierungszusammenarbeit im Rahmen der Europäischen Union handelt, bei der eine parlamentarische Kontrolle der Regierungsvertreter im Rat durch die nationalen Parlamente stattfindet. Diese Kontrolle erfolgt – bereits seit Beginn der Aufbauphase von Europol – insbesondere durch laufende Berichterstattung durch die Bundesregierung an die Ausschüsse des Deutschen Bundestages. Ferner schreibt Artikel 39 des Vertrags über die EU (Fassung von Amsterdam) eine Beteiligung des Europäischen Parlaments an der Zusammenarbeit im Bereich Justiz und Inneres, zu der Europol gehört, vor: Der Rat muss das Europäische Parlament über die durchgeführten Arbeiten regelmäßig unterrichten; er hat das Europäische Parlament zu Ratsbeschlüssen, Änderungen des Europol-Übereinkommens und Durchführungsmaßnahmen anzuhören, bevor sie verabschiedet werden; das Europäische Parlament hat das Recht, Anfragen oder Empfehlungen an den Rat zu richten. Außerdem wird dem Parlament nach dem Europol-Übereinkommen jährlich ein Sonderbericht über Europol vorgelegt.

Europol führt keine eigenständigen Ermittlungen, sondern unterstützt lediglich nationale Ermittlungsverfahren. Damit liegt die Sachherrschaft bei deutschen Ermittlungsverfahren weiterhin bei der deutschen Staatsanwaltschaft. Entsprechendes gilt für andere Mitgliedstaaten.

Zur Frage der Stellung und Rolle der Justiz im Verhältnis zu Europol hat das Bundesministerium der Justiz eine rechtsvergleichende Studie bei den Max-Planck-Instituten Freiburg und Heidelberg in Auftrag gegeben.

a. Welche Maßnahmen hat die Bundesregierung ergriffen, um die Möglichkeiten des Schengener Informationssystems (SIS) zurückzufahren?

Das Schengener Informationssystem (SIS) ist das Herzstück der Ausgleichsmaßnahmen für den Wegfall der Binnengrenzkontrollen zwischen den Schengen-Staaten. Das SIS wird auf der Grundlage des Titels IV des Schengener Durchführungsübereinkommens (SDÜ) betrieben. Das SDÜ als zwischen den Schengen-Staaten ausgehandeltes und ratifiziertes Übereinkommen bestimmt die Möglichkeiten des SIS, insbesondere dessen Betrieb. Insofern können nicht einseitig Maßnahmen getroffen werden, die in diese verbindlichen Festlegungen eingreifen.

Das SIS hat sich seit seiner Inbetriebnahme als wirkungsvolles Instrument der polizeilichen Fahndung erwiesen und ist somit geeignet, einen signifikanten Beitrag zur öffentlichen Ordnung und inneren Sicherheit in den Schengen-Staaten zu leisten. Insofern wäre ein Zurückfahren des SIS mit spürbaren Sicherheitseinbußen für den Bürger verbunden.

b. Welche Maßnahmen hat die Bundesregierung ergriffen, um das SIS datenschutzrechtlich zu regeln, und welche Kontrollmöglichkeiten haben gegenwärtig die nationalen Parlamente und das Europäische Parlament?

Im Titel IV des SDÜ ist der Datenschutz im SIS bereits geregelt. Für die Kontrolle des Datenschutzes im nationalen Teil des SIS (N.SIS) ist der Bundesbeauftragte für den Datenschutz (BfD) bzw. der Datenschutzbeauftragte im Bundeskriminalamt (BKA) zuständig. Entsprechende gesetzliche Regelungen sind bereits vorhanden.

Die Kontrolle des Datenschutzes in der technischen Unterstützungseinheit in Straßburg (C.SIS) obliegt der Schengener Gemeinsamen Kontrollinstanz nach Artikel 115 SDÜ. In diese Kontrollinstanz werden jeweils Vertreter der nationalen Kontrollinstanzen entsandt. In Deutschland wird ein Vertreter durch den BfD bestimmt; ein weiterer Vertreter wird aus dem Kreis der Landesbeauftragten für den Datenschutz entsandt.

Die nationalen Kontrollinstanzen berichten jeweils den Parlamenten. Die Schengener Gemeinsame Kontrollinstanz veröffentlicht Tätigkeitsberichte, die über die nationalen Kontrollinstanzen ebenfalls den Parlamenten zugesandt werden.

Mit dem Inkrafttreten des Amsterdamer Vertrages wurde die Einbeziehung des Europäischen Parlaments in die Arbeit der dritten Säule verbessert. Der Artikel 39 EUV bietet dem Europäischen Parlament entsprechende Möglichkeiten, auch im Bereich des Datenschutzes aktiv zu werden.

c. Wie viele Datensätze werden – nach Kenntnis der Bundesregierung – monatlich im Rahmen des SIS ausgetauscht?

Der Bestand an Datensätzen im SIS steigt sowohl in Deutschland als auch in den anderen Schengen-Staaten tendenziell an. Im Bereich der Personenfahndung sind insgesamt ca. 1,3 Millionen Datensätze vorhanden. Der weit überwiegende Teil dient der Fahndung nach Sachen, z. B. Kraftfahrzeugen, Identitätsdokumenten, Schußwaffen. Die Gesamtzahl der Datensätze lag Ende Juni 1999 bei ca. 9,3 Millionen, wobei Deutschland ca. 3 Millionen Datensätze zu verzeichnen hatte.

Der Bestand an Datensätzen ist im gesamten Schengener Raum (derzeit 10 Staaten) einheitlich vorhanden und jederzeit abrufbar. Allein in Deutschland wurde das SIS im Jahre 1998 ca. 65 Millionen mal abgefragt, was über 100 000 Abfragen pro Tag bedeutet. Neue Datensätze eines Schengen-Staates werden mittels der technischen Unterstützungseinheit (C.SIS) in alle anderen Schengen-Staaten verteilt. Datensätze, die im Nachgang eines Treffers oder infolge des Endes der Speicherungsdauer gelöscht werden, werden in allen Schengen-Staaten gelöscht.

Es werden keine Statistiken über Bewegungen von Datensätzen innerhalb des SIS geführt.

d. Wie bewertet die Bundesregierung die Tatsache, dass die Betroffenen keine Schutzrechte haben?

Die in der Fragestellung enthaltene Annahme nicht vorhandener datenschutzrechtlicher Schutzrechte trifft nicht zu.
Grundsätzlich findet das nationale Recht auf die betreffende Ausschreibung im SIS Anwendung, sofern das SDÜ nicht engere Bestimmungen enthält. Insofern gelten alle Regelungen, die auf Ausschreibungen im nationalen Polizei-Informationssystem INPOL Anwendung finden, auch für durch Deutschland in das SIS

übernommene Ausschreibungen. Dies gilt insbesondere auch für die Wahrung der Rechte der ausgeschriebenen Person.

Das SDÜ nimmt darüber hinaus speziell Bezug auf

- die Bedeutung des Falles, die die Ausschreibung rechtfertigen muss,
- die Zweckbindung der im SIS vorhandenen Daten,
- die Protokollierung der Abrufe zum Zwecke der Prüfung der Zulässigkeit des Abrufs,
- die Notwendigkeit der Richtigkeit und Aktualität der Ausschreibungen sowie die Löschung, sofern unrichtige oder unrechtmäßig gespeicherte Daten vorhanden sind,
- das Auskunftsrecht,
- die Speicherungsdauer,
- die Haftung des ausschreibenden Schengen-Staates und
- die technischen und organisatorischen Maßnahmen zum Schutz des SIS vor unberechtigtem Zugriff.

e. Wieso beabsichtigt die Bundesregierung nicht, Rechtsschutzregelungen für das Schengener Durchführungsübereinkommen (SDÜ) vom 19. Juni 1990 vorzulegen und umzusetzen?

Die allgemeinen Rechtsschutzregelungen, die auch für die Anwendung des Schengener Durchführungsübereinkommens (SDÜ) gelten, sind ausreichend. Nach Artikel 111 SDÜ hat jeder das Recht, im Hoheitsgebiet jeder Vertragspartei eine Klage wegen einer seine Person betreffenden Ausschreibung insbesondere auf Berichtigung, Löschung, Auskunftserteilung oder Schadensersatz vor dem nach nationalem Recht zuständigen Gericht oder der zuständigen Behörde zu erheben.

f. Welche Maßnahmen hat die Bundesregierung ergriffen, um beim Datenexport in Drittstaaten angemessene Datenschutzbestimmungen einzuführen?

Die Fragestellung geht offenbar davon aus, dass für die Datenübermittlung ins Ausland keine hinreichenden gesetzlichen Vorschriften vorhanden seien. Dies trifft nicht zu: In § 17 Bundesdatenschutzgesetz ist eine Querschnittsregelung getroffen, die in verschiedenen Fachgesetzen (z. B. § 14 BKAG, § 19 Abs. 3 BVerfSchG, § 30 Abs. 7 Straßenverkehrsgesetz) bereichsspezifisch modifiziert wird.

Für das neue Bundesdatenschutzgesetz sind in Umsetzung der EG-Datenschutzrichtlinie Bestimmungen vorgesehen, die den Grundsatz der Erforderlichkeit eines angemessenen Datenschutzniveaus normieren und entsprechend der Richtlinie hiervon Abweichungen insbesondere auch für die Wahrung eines wichtigen öffentlichen Interesses zulassen.

Im übrigen entspricht es der deutschen Staatspraxis, gerade bei Staaten mit nicht angemessenem Datenschutzniveau die Verwendung der Daten durch entsprechende Klauseln völkervertraglich zu regeln.

g. Welche Maßnahmen hat die Bundesregierung ergriffen, um das europäische daktyloskopische Fingerabdrucksystem zur Identifizierung von Asylbewerbern (EURODAC) zurückzufahren und sofort umfassende Schutzregelungen für die Betroffenen herzustellen?

Das Fingerabdruckvergleichssystem EURODAC soll eine effizientere Anwendung des Übereinkommens vom 15. Juni 1990 über die Bestimmung des zuständigen Staates für die Prüfung eines in einem Mitgliedstaat der Europäischen Gemeinschaften gestellten Asylantrags (Dubliner Übereinkommen) gewährleisten.

Die Bundesregierung ist in den Verhandlungen zu EURODAC aktiv dafür eingetreten, dass ausreichende datenschutzrechtliche Bestimmungen Bestandteil der einschlägigen Entwurfstexte sind. Durch das Inkrafttreten des Amsterdamer Vertrages am 1. Mai 1999 ist es notwendig geworden, die bisherigen EURODAC-Entwürfe in einen Gemeinschaftsrechtsakt zu überführen. Der von der Europäischen Kommission vorgelegte Entwurf einer EURODAC-EG-Verordnung enthält umfangreiche Datenschutzbestimmungen, die sich an der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr orientieren. Darüber wird derzeit in den zuständigen Gremien der Europäischen Union beraten.

h. Welche Maßnahmen hat die Bundesregierung ergriffen, um die EURODAC durch nationale Parlamente und das Europäische Parlament kontrollieren zu können?

Das EURODAC-System wird im Rahmen von Titel IV EG-Vertrag eingeführt werden. Bei der zu erlassenden EURODAC-Verordnung wird es sich also um ein Gemeinschaftsrechtsinstrument im ersten Pfeiler der Europäischen Union handeln. Daher werden dem Europäischen Parlament die im Rahmen des ersten Pfeilers üblichen Befugnisse zustehen. Eine Kontrolle wird außerdem durch die gemäß Artikel 286 EG-Vertrag einzurichtende Kontrollinstanz sowie – im Rahmen ihrer Zuständigkeit – durch die nationalen Datenschutzkontrollinstanzen stattfinden.

i. Welche Maßnahmen hat die Bundesregierung ergriffen, um zu garantieren, dass zuerst die Möglichkeiten eines Datenschutzes der Betroffenen und die Kontrollmöglichkeiten der Parlamente hergestellt sind, bevor die Erhebung, Speicherung und Weitergabe von EURODAC-Daten erfolgt?

Die Erhebung, Speicherung und Weitergabe von Daten im Rahmen von EURODAC dürfen des vorherigen Inkrafttretens eines Gemeinschaftsrechtsinstruments als Rechtsgrundlage. Der Entwurf der Europäischen Kommission für eine EURODAC-EG-Verordnung enthält umfassende Datenschutzbestimmungen. Hierüber wird derzeit in den zuständigen Gremien der Europäischen Union beraten.

j. Welche datenschutzrechtlichen Regelungen gelten gegenwärtig für das Zollinformationssystem (ZIS)?

Zwei Zollinformationssysteme mit dem Namen „ZIS“ sind zur Zeit geplant.

Rechtsgrundlage für das ZIS der *Gemeinschaft* (I. Säule der Union; „ZIS-EG“) ist die VO (EG) Nr. 515/97.

Rechtsgrundlage für das ZIS der *Mitgliedstaaten* (III. Säule der Union; „ZIS-MS“) ist das noch zu ratifizierende Übereinkommen über die Nutzung der Informationstechnologie im Zollbereich. Ein Gesetzentwurf befindet sich zur Zeit in der Ressortabstimmung.

Gegenwärtig gelten für das ZIS der Gemeinschaft die bereichsspezifischen Datenschutzregelungen nach der VO (EG) Nr. 515/97 unmittelbar. Darüber hinaus gilt das ZIS der Gemeinschaft in jedem Mitgliedstaat aus Datenschutzgründen als eine nationale Datenbank. Damit gelten nationale Datenschutzregelungen, soweit die VO Nr. 515/97 im Einzelfall nichts anderes bestimmt.

Der zur Zeit in der Ressortabstimmung befindliche Gesetzentwurf zur innerstaatlichen Umsetzung des ZIS-Übereinkommens der Mitgliedstaaten sieht bereichsspezifische Datenschutzregelungen für den Informationsfluss zwischen den nationalen Behörden vor.

k. Wie viele Datensätze werden gegenwärtig monatlich im Rahmen des ZIS unter den EU-Mitgliedstaaten ausgetauscht, und wie werden die Belange der Betroffenen geschützt?

Das ZIS-EG wird zur Zeit noch technisch ohne Verwendung von Echtdaten erprobt. Der Betrieb mit Echtdaten soll zu Beginn des Jahres 2000 aufgenommen werden.

Das ZIS-MS muss noch entwickelt werden. Es ist vorgesehen, hierfür das ZIS-EG zu kopieren und die Kopie in dem erforderlichen Umfang an das ZIS-Übereinkommen anzupassen.

l. Wie kann der Datentransfer des ZIS von den nationalen Parlamenten und dem Europäischen Parlament kontrolliert werden?

Sowohl die VO (EG) Nr. 515/97 als auch das ZIS-Übereinkommen sehen keine direkten Kontrollrechte nationaler Parlamente oder des Europäischen Parlaments vor.

Mittelbar ergeben sich die Rechte in Bezug auf das ZIS-EG jedoch zum einen aus den allgemeinen Kontrollrechten des Europäischen Parlaments bez. der Kommission und zum anderen aus der Zusammenarbeit mit dem Bürgerbeauftragten nach Artikel 195 EUV, der bis zur Schaffung einer unabhängigen EU-Datenschutzbehörde Kontrollaufgaben wahrnehmen soll. Nationale Parlamente werden durch die Berichte der unabhängigen nationalen Datenschutzbehörden unterrichtet.

m. Welche Anstrengungen hat die Bundesregierung unternommen, um die erforderlichen bereichsspezifischen Datenschutzregelungen für das ZIS innerhalb der EU herzustellen, und wann kann mit der Verabschiedung gesetzlicher Regelungen gerechnet werden?

Auf die Antwort zu Frage 14 j) wird verwiesen.

15. Was hat die Bundesregierung während der Zeit ihrer EU-Präsidentschaft unternommen, um den Datenschutz zu verbessern oder den Zugriff auf Daten von Betroffenen neu zu regeln (bitte die Maßnahmen mit Datum einzeln auflisten)?

Im Zuge der deutschen Ratspräsidentschaft ist die Koordinierung des Standpunktes der Gemeinschaft zu wichtigen geplanten Rechtsakten des Europarates vorangebracht worden. Die Koordinierung zu der für den Verbraucher wesentlichen Empfehlung für den Schutz von für Versicherungszwecke erhobenen und verarbeiteten Daten steht kurz vor dem Abschluß. In einem Zusatzprotokoll zur Datenschutzkonvention des Europarates aus dem Jahre 1981 sollen Grundsätze über nationale Datenschutzkontrollinstanzen und grenzüberschreitende Datenflüsse aufgenommen werden. Die Koordinierung des Gemeinschaftsstandpunktes zum Text dieses Zusatzprotokolls wurde unter deutscher Ratspräsidentschaft abgeschlossen. Schließlich wurden die rechtlichen Voraussetzungen für einen Beitritt der EU zur Datenschutzkonvention des Europarates geschaffen. Hinsichtlich der Schengener Gemeinsamen Kontrollinstanz wurde auf Initiative und Betreiben der Bundesregierung ein Ratsbeschluss erarbeitet und angenommen, der die Arbeitsfähigkeit und Unabhängigkeit der Schengener Gemeinsamen Kontrollinstanz nach Artikel 115 SDÜ auch nach dem Inkrafttreten des Amsterdamer Vertrages sicherstellt (Dok. 8060/99 SCHENGEN 45 vom 12. Mai 1999, angenommen am 20. Mai 1999). Herauszustellen ist dabei die Möglichkeit der Gemeinsamen Kontrollinstanz, unter Wahrung ihrer Unabhängigkeit auf die komplette Infrastruktur des Generalsekretariats des Rates zurückgreifen zu können (Sitzungssäle, Übersetzungsdienst usw.). In der Frage der Reisekosten wurde eine Verbesserung gegenüber dem Schengener Regime dahin gehend erreicht, dass künftig auch für Kontrollen der technischen Unterstützungseinheit (C.SIS) Reisekosten erstattet werden.

16. Nach welchem Aktions- und Zeitplan will die Bundesregierung zukünftig in der Bundesrepublik Deutschland und in der EU datenschutzrechtliche Bestimmungen reformieren (bitte genau auflisten nach Vorhaben, Ziel des Vorhabens und dem zu erwartenden Zeitpunkt)?

Die Bundesregierung beabsichtigt, noch in dieser Legislaturperiode eine umfassende Neukonzeption des BDSG zu verabschieden, die das Gesetz modernisiert, vereinfacht und seine Lesbarkeit erhöht. Darüber hinaus wird im Laufe dieser Legislaturperiode das gesamte bereichsspezifische Datenschutzrecht daraufhin zu überprüfen sein, ob über die bereits vorgenommenen Änderungen hinaus weitere Anpassungen an die Richtlinie geboten sind.

Die Reform datenschutzrechtlicher Bestimmungen der EU obliegt ausschließlich den Organen der EU.

17. In welchen Bereichen hat die Bundesregierung seit Oktober 1998 die Zugriffsmöglichkeiten – bezogen auf die Erhebung, Speicherung, Aufbewahrung, Weitergabe – staatlicher, behördlicher und privater Stellen auf Daten der Bürgerinnen und Bürger erweitert und erleichtert – wie beispielsweise bei der Reform des Staatsangehörigkeitsrechtes (bitte genau die Maßnahmen auflisten)?

Im staatsangehörigkeitsrechtlichen Bereich haben der mit dem Gesetz zur Reform des Staatsangehörigkeitsrechts vom 15. Juli 1999 (BGBl. I S. 1618) neu eingeführte Erwerb der deutschen Staatsangehörigkeit für Kinder ausländischer Eltern durch Geburt im Inland (§ 4 Abs. 3 Staatsangehörigkeitsgesetz – StAG) und das damit zusammenhängende Optionsverfahren (§ 29 StAG) weitere Maß-

nahmen für die Speicherung und Weitergabe von personenbezogenen Daten erforderlich gemacht.

Im Einzelnen:

– Der Erwerb der deutschen Staatsangehörigkeit wird durch den für die Beurkundung der Geburt des Kindes zuständigen Standesbeamten eingetragen (§ 4 Abs. 3 Satz 2 StAG). Das Nähere wird in der Personenstandsverordnung sowie in der Dienstanweisung für die Standesbeamten und ihre Aufsichtsbehörden geregelt (§ 70 Nr. 5 Personenstandsgesetz).

– Die Tatsache, dass nach § 29 StAG ein Verlust der deutschen Staatsangehörigkeit eintreten kann, wird ins Melderegister eingetragen, § 2 Abs. 2 Nr. 3 Melderechtsrahmengesetz.

– Angaben zur Erklärungspflicht des Ausweisinhabers nach § 29 des Staatsangehörigkeitsgesetzes werden in das Personalausweisregister bzw. in das Passregister eingetragen, § 2a Abs. 1 Satz 2 Nr. 5 des Gesetzes über Personalausweise bzw. § 21 Abs. 2 Nr. 16 Passgesetz.

Gesamtherstellung: H. Heenemann GmbH & Co., Buch- und Offsetdruckerei, Bessemerstraße 83–91, 12103 Berlin
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333