BREMISCHE BÜRGERSCHAFT **Drucksache 16 /980**
Landtag 31. 03. 06
16. Wahlperiode

28. Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2005 den 28. Jahresbericht zum 31. März 2006 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2005.

Sven Holst
Landesbeauftragter für den Datenschutz

Inhaltsverzeichnis

1. Vorwort

Das Grundrecht auf informationelle Selbstbestimmung wurde in den letzten Jahren in Deutschland nicht genügend geachtet. Dabei ist dieses Recht als Konkretisierung u. a. der Menschenwürde und des allgemeinen Persönlichkeitsrechts für personenbezogene Datenverarbeitung nicht disponibel. Es ist auch im Land Bremen mit Verfassungsrang ausgestattet (Art. 12 LV).

1.1 Sicherheit und informationelle Selbstbestimmung

Der 11. September 2001 hat einen Sturmlauf der Innenpolitik in Richtung personenbezogener Datenverarbeitung für Zwecke der inneren Sicherheit entfesselt, der mit seiner Normenflut bei weitem nicht nur auf die Bekämpfung von Terrorismus fokussiert ist. Die dort neu eingeführten Instrumente können weit darüber hinaus Anwendung finden und dabei in erheblichem Maße auch in die Rechte unbescholtener Bürger eingreifen. Aktuellste Beispiele sind die massenhaften und maßlosen Datenerhebungen und Verarbeitungen in Vorbereitung der Fußball-Weltmeisterschaft ohne ausreichende Rechtsschutzgarantien für die Betroffenen und unter nicht zulässiger Einbeziehung der Verfassungsschutzämter (vgl. Ziff. 9.9 und 18.13 dieses Berichts), die gesetzliche Einführung der anlasslosen polizeilichen Kontrollen, die Speicherung aller Telefonverbindungsdaten mit weiteren Bezugsdaten (vgl. Ziff. 3.2 dieses Berichts) und aller Internetaktivitäten für mindestens ein halbes Jahr oder auch die Einführung biometrischer Merkmale in den Reisepass, ohne dass hieraus in Bezug auf den internationalen Terrorismus ein erkennbarer Sicherheitsgewinn zu erzielen ist (vgl. Ziff. 3.3 dieses Berichts).

Trotz Mahnungen der Datenschutzbeauftragten des Bundes und der Länder („Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen“, vgl. 24. JB, Ziff. 15.15) haben Parlamente in Bund und Ländern die Vorlagen aus den Innenministerien weitgehend und unverändert verabschiedet. Dabei wurde der inneren Sicherheit ein fast absoluter Vorrang eingeräumt. Sicherheit und Freiheit bedingen sich gegenseitig. Dies sensible Verhältnis verdeutlicht auch der vom Mitautor der Amerikanischen Verfassung von 1787, Benjamin Franklin, geäußerte Gedanke: „Diejenigen, die bereit sind, ihre Freiheit aufzugeben, um Sicherheit zu gewinnen, werden beides verlieren.“ Für das Anliegen der inneren Sicherheit findet man in der Presse und bei der Exekutive starke Vertreter. Die Freiheitsrechte der Bürger können aber nur in einem abgewogenen Maß verteidigt werden, wenn sich hierfür die Legislative stark macht. Dies hätte man sich in letzter Zeit stärker gewünscht.

Das Bundesverfassungsgericht musste in jüngster Zeit Teile dieser Entwicklung zurücknehmen, in dem es z. B. die gesetzliche Regelung zum Lauschangriff für verfassungswidrig erklärte (1BvR 2378/02 vom 3. März 2004) und mit seiner Entscheidung den „unantastbaren Kernbereich privater Lebensgestaltung“ ausführlich beschrieb. Die Datenschutzbeauftragten des Bundes und der Länder haben seinerzeit in einer Entschließung darauf hingewiesen, dass dieser verfassungsrechtlich geschützte Kernbereich nicht nur für den Wohnraum, sondern auch für andere Bereiche Geltung hat (vgl. Ziff. 19.11 dieses Berichts).

Mitte 2005 folgte das zweite Urteil des Bundesverfassungsgerichts (1BvR 668/04 vom 27. Juli 2005), das Regelungen des niedersächsischen Polizeigesetzes zur präventiven Telefonüberwachung für verfassungswidrig erklärte und mit der Entscheidung verdeutlichte, dass auch im präventiven Bereich das Sicherheitsinteresse keinen absoluten Vorrang vor dem Fernmeldegeheimnis hat. Dessen ungeachtet gingen die Beratungen über die Novellierung des Bremischen Polizeigesetzes und des Bremischen Verfassungsschutzgesetzes zu Ende, ohne dass meinen verfassungsrechtlichen Bedenken zu beiden Gesetzen in Bezug auf die Neuregelung in der Wohnraumüberwachung ausreichend Rechnung getragen wurde (vgl. Ziff. 9.1 und 9.3 dieses Berichts).

Stellt man zu den genannten Entscheidungen des Bundesverfassungsgerichts noch eine dritte ins Verhältnis (2BvR 581/01 vom 12. April 2005), die den Einsatz von GPS-Ortungssystemen bei der Überwachung betrifft, so wird klar, dass selbst bei Fällen schwerwiegender Straftaten präventiven wie strafverfolgenden Handlungen des Staates bei der Überwachung mutmaßlicher Täter verfassungsrechtliche Grenzen gesetzt sind, die von der Gesetzgebung nicht nur zu respektieren, sondern zu gewährleisten sind.

Kaum ist das eine Eingriffsinstrument durch die Innenpolitik erreicht, wird die nächste Idee geboren. Da soll den Geheimdiensten Zugriff auf die Konten- und Bewegungsdaten aller Reisenden bei privaten Reisebüros ermöglicht werden. Oder der noch in der letzten Legislaturperiode vom Parlament verkündete Wille, die Mautdaten nur für Abrechungszwecke zu verwenden, soll plötzlich für die Strafverfolgung wieder aufgehoben werden. Wenn die eben versprochene Zweckbindung der Daten beliebig und willkürlich aufgebrochen werden kann, wie soll da der Bürger noch Vertrauen haben in nutzungsbegrenzende Regelungen für andere neue IuK-Verfahren?

Für einige ist Freiheit ein Sicherheitsrisiko und deshalb unter der Herrschaft der Sicherheitslogik tunlichst zu eliminieren. Die Datenschutzbeauftragten des Bundes und der Länder hingegen versuchen, auch im Sicherheitsbereich die Datenschutzprinzipien der Datenvermeidung und der Datensparsamkeit zu verwirklichen. Nur die notwendigsten Daten sind für den Staat erforderlich. Dies ist ein Konzept, den Staat aus privaten Lebensräumen weitgehend fernzuhalten. Der Datenschutz versucht so, ein Stück Selbstverantwortung in Freiheit zu erhalten.

1.2 Erhalt des informationellen Selbstbestimmungsrechts in anderen Bereichen

Um die Achtung und Gewährleistung des informationellen Selbstbestimmungsrechts geht es aber nicht nur im Bereich der inneren Sicherheit, sondern auch in anderen Bereichen öffentlicher und privater Datenverarbeitung. Zu nennen sind die im Gesetz zur Förderung der Steuerehrlichkeit enthaltenen Regelungen zur Konten-Kontrolle, die zweckgebundene Nutzung der Daten der Autobahnmaut, das Projekt JobCard, das alle Arbeitnehmer in einer Zentraldatei erfasst, oder jetzt in 2006 die datenschutztechnische und -rechtliche Begleitung der Einführung der elektronischen Gesundheitskarte.

Aber auch der ständig sich ausweitende Datenhunger der Privatwirtschaft führt zur Frage, ob in einzelnen Bereichen die rechtlichen Regelungen zum Schutz des informationellen Selbstbestimmungsrechts noch ausreichend sind. Dies betrifft z. B. den Bereich des Arbeitnehmerdatenschutzes inklusive eines Gentest-Gesetzes, insbesondere aber den Bereich der Auskunfteien mit der Nutzung der Daten für ständig sich ausweitende Geschäftsbereiche. Bei meinen Datenschutzkontrollen stoße ich immer häufiger auf Verfahren, bei denen Wohnumfeldanalysen, repräsentative Beobachtungen, statistische Erhebungen oder sonstige Erfahrungswerte genutzt werden, um damit das künftige Kauf- oder Zahlungsverhalten von Personen zu prognostizieren (vgl. Ziff. 18.2 dieses Berichts). Wenn ein Bürger aufgrund eines schlechten Score-Wertes keinen Handy-Vertrag bekommt, mag das noch hinnehmbar sein, schließlich gibt es Prepaid-Karten. Anders sähe es aber aus, wenn Bürger wegen eines schlechten Score-Wertes keine Wohnung bekämen. Die Datenschutzbeauftragten des Bundes und der Länder haben in dem Appell „Eine moderne Informationsgesellschaft braucht mehr Datenschutz“ auf einige legislatorische Bedarfe hingewiesen (vgl. Ziff. 19.3 dieses Berichts).

1.3 Beratung rechtlicher Regelungen zur Datenverarbeitung

Im Berichtsjahr habe ich wiederum zu einer ganzen Reihe von Rechtsvorschriften gegenüber senatorischen Dienststellen eine Stellungnahme abgegeben. Zu nennen sind u. a. die Novellierung des Schuldatenschutzgesetzes (vgl. Ziff. 1.4 und Ziff. 13.3 dieses Berichts), das Umweltinformationsgesetz (vgl. Ziff. 14.1 dieses Berichts), das Krebsregistergesetz (vgl. Ziff. 11.5 dieses Berichts), der Rundfunkgebührenstaatsvertrag, die Entwürfe zum Informationsfreiheitsgesetz (vgl. Ziff. 1.6 dieses Berichts), die Neuregelung eines Bremischen Studienkontengesetzes (BremGBl. 2005, S. 550) sowie ergänzende gesetzliche Regelungen zum Bremischen Polizeigesetz (vgl. Ziff. 9.3 dieses Berichts) wie auch zum Bremischen Verfassungsschutzgesetz (vgl. Ziff. 9.1 dieses Berichts).

1.4 Schuldatenschutzgesetz

Die aus schulischer wie bildungspolitischer Sicht erforderlichen Änderungen des Schuldatenschutzgesetzes sind seit langem durchberaten, eine Befassung mit der Vorlage hat es bereits im Juli 2005 in der Bildungsdeputation gegeben. Die Änderungen müssen dringend verabschiedet werden, um eine rechtmäßige Datenverarbeitung mit dem Informationssystem MAGELLAN herzustellen.

Verlautbarungen nach soll die Vorlage im Senat angehalten worden sein, weil noch Regelungen für die Zusammenarbeit des Lehrpersonals mit der Polizei wie auch Regelungen zur Übermittlung von Schülerdaten an Verfassungsschutz und Staatsschutz fehlen.

Sollten diese Informationen zutreffen, hätte ich für ein Zuwarten kein Verständnis. Solche Regelungen sind äußerst fraglich und bedürften grundsätzlicher Diskussionen. Ich habe daher dem Senator für Bildung, Wissenschaft und Kunst angeraten, die Verabschiedung der von den Schulen und der senatorischen Behörde für ihre Datenverarbeitung dringend benötigten Regelungen voranzutreiben. Parallel dazu können die Beratungen zu den anderen Fragen weitergeführt werden. Sollte sich danach ein weiterer Novellierungsbedarf ergeben, können die Regelungen immer noch ergänzt werden.

1.5 Pilotprojekt „Elektronische Gesundheitskarte“ in Bremen

Bremen hat sich als eine Modellregion für die Einführung der elektronischen Gesundheitskarte (eGK) in einem Pilotprojekt beworben und Ende des Jahres 2005 den Zuschlag bekommen. Da sich meine Dienststelle seit geraumer Zeit mit der Entwicklung der technischen und rechtlichen Rahmenbedingungen der eGK zusammen mit anderen Datenschutzbeauftragten des Bundes und der Länder beschäftigt, ist bekannt, wie vielschichtig und tiefgreifend die IT-Strukturen entwickelt sein müssen, um den gesetzlichen Regelungen zu diesem komplexen Projekt Rechnung tragen zu können. Bei der Bewerbung Bremens als Modellregion habe ich daher deutlich gemacht, dass auch Kosten für die datenschutztechnische und -rechtliche Begleitung berücksichtigt werden müssen. Denn die datenschutzgerechte Ausgestaltung der Infrastruktur für die Datenverarbeitung – das Netz wird später einmal alle Apotheken, alle Krankenkassen, alle Krankenhäuser wie andere Angehörige der Heilberufe verbinden – kann von meiner Dienststelle nicht mit dem ohnehin an der Grenze der Belastbarkeit arbeitenden Personal noch „nebenbei“ mit erledigt werden. Ich habe daher dem zuständigen Ressort mitgeteilt, dass ich sehr daran interessiert bin, das Projekt zu begleiten, dies aber nur kann, wenn für meine Dienststelle gewisse Rahmenbedingungen geschaffen werden, nur dann kann eine verantwortliche Begleitung durch mein Haus sichergestellt werden.

1.6 Informationsfreiheitsgesetz

In der vorherigen und der laufenden Legislaturperiode sind Gesetzentwürfe von Bündnis 90/Die Grünen zum Informationsfreiheitsgesetz (Drs. 16/183 und Drs. 16/772) sowie ein Gesetzentwurf der Koalition (Drs. 16/874) in die Bürgerschaft eingebracht worden. Sie wurden zur weiteren Beratung an den federführenden Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten und an den Rechtsausschuss überwiesen. Die genannten Entwürfe sehen vor, dass dem Landesbeauftragten für den Datenschutz auch die Aufgabe eines Landesbeauftragten für Informationsfreiheit zugewiesen werden soll. Ich werde zu Fragen des Datenschutzes sowie auch zur Ausgestaltung der Rechtsstellung des Landesbeauftragten für Informationsfreiheit Stellung nehmen und zu der damit verbundenen Frage, ob bzw. wie diese zusätzliche Aufgabe durch meine Dienststelle geschultert werden kann (vgl. Ziff. 1.17 dieses Berichts – zur Situation der Dienststelle).

1.7 eGovernment

Das Land Bremen nimmt im Bereich eGovernment häufig eine Vorreiterrolle ein. Vielfältige fachübergreifende Entwicklungen internetgestützter Verwaltungstätigkeiten erfordern auf technischer und organisatorischer Ebene datenschutzkonforme Prozesse. Mit der Gestaltung dieser für eine rechtskonforme Kommunikation zwischen Staat und Bürger, Staat und Wirtschaft und innerhalb der Verwaltung erforderlichen Abläufe beschäftigt sich der Arbeitskreis „Datenschutzgerechtes eGoverment“. In den letzten Jahren habe ich regelmäßig über die Ergebnisse berichtet.

In 2005 hat der Arbeitskreis eine Entschließung zur Sicherheit beim eGovernment durch Nutzung des in Bremen entwickelten Standards OSCI (Online Services Computer Interface) für die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vorbereitet. Mit „OSCI-Transport“ existiert ein geeignetes Standardprotokoll, das Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Da-

ten gewährleistet. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt diese Festlegung, um eine zukünftige Interoperabilität verschiedener eGovernment-Anwendungen, kombiniert mit einer datenschutzkonformen Infrastruktur für den Datenaustausch zwischen diesen Komponenten, zu erreichen.

Der Senator für Finanzen in Bremen plant für 2006 die Fortsetzung der Arbeit des Projektes „Virtuelle Poststelle“ (vgl. 27. JB, Ziff. 3.1, andere Bezeichnung für die über OSCI abgebildete Infrastruktur), verbunden mit der Planung eines flächendeckenden elektronischen Zugangs zu den Behörden des Landes. In Bremen und Bremerhaven gibt es erste bereits laufende und geplante Anwendungen, wie etwa im Bereich der Justiz zur Eröffnung des elektronischen Rechtsverkehrs (vgl. Ziff. 10.1 dieses Berichts). Ich habe mich an der Pilotphase des Projekts beteiligt und unterstütze die Entwicklung eines anwendungsfähigen Datenschutzkonzeptes im Rahmen der Projektgruppe.

1.8 ALG II

In Zeiten leerer öffentlicher Kassen wird genau hingeschaut, ob eine Sozialleistung tatsächlich erbracht werden muss. Dies bekommen insbesondere die Arbeitslosengeld-II-Empfänger stark zu spüren. Gegen eine konkrete Überprüfung ist im Einzelfall sicher nichts einzuwenden. Die Form, in der öffentlich allgemeine Verdächtigungen geäußert werden, und der Umgang mit den Menschen, die zum Teil viele Jahre ihres Lebens gearbeitet haben, verbittert sie und führte zu Beschwerden bei mir. Wenn ständig weitere Datenrasterungen über die Medien angekündigt werden oder Missbrauchsfälle aus der ganzen Republik in Presseberichten so zusammengetragen werden, als seien diese alle in der eigenen Region passiert, entsteht in der Öffentlichkeit leicht ein falscher Eindruck. Denn bisher wurden keine konkreten auf diesen Personenkreis beziehbaren statistischen Zahlen von Missbrauchsfällen bekannt gegeben.

Ich sah mich daher im Berichtszeitraum zwei Mal genötigt, öffentlich klarzustellen, dass auch die ALG-II-Empfänger ihr Datenschutzrecht ungestraft in Anspruch nehmen können, zuletzt, als von der Presse angekündigt wurde, es werde eine telefonische Befragung der ALG-II-Empfänger durch ein beauftragtes Call-Center geben, obwohl die notwendigen datenschutzrechtlichen Vorkehrungen nicht getroffen waren. Hierüber war der Bundesbeauftragte für den Datenschutz (BfD) noch mit der Bundesagentur für Arbeit (BA) in Verhandlungen. So fehlten verbindliche Festlegungen der Aufgaben des Call-Centers. Auch die Zugriffsmöglichkeiten der Mitarbeiter des Call-Centers auf die Daten der Betroffenen, die in den Rechnern der BA gespeichert sind, waren nicht eingeschränkt. Eine hinreichende Information der Arbeitslosen über die Aktion war ebenfalls nicht erfolgt. Auch waren keine verfahrenssichernden Maßnahmen getroffen, die ausschlossen, dass Fremde Missbrauch treiben und gutgläubigen Leistungsempfängern am Telefon persönliche Daten entlocken (vgl. Ziff. 12.1 dieses Berichts). Schon im Herbst hatte sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder zu einer ähnlichen Telefonbefragung kritisch geäußert (vgl. Ziff. 19.5 dieses Berichts).

Aber auch das Verfahren zur Rundfunkgebührenbefreiung brachte die ALG-II-Empfänger auf, werden sie doch dazu verpflichtet, regelmäßig ihren Arbeitslosengeld-Bescheid mit allen darin enthaltenen sozialen und gesundheitlichen Daten im Original oder in beglaubigter Kopie der GEZ vorzulegen. Wenn man nur einmal von 2,5 Millionen Bedarfsgemeinschaften ausgeht, so müssen diese in bestimmten Abständen unter Verstoß gegen den Datenschutz die im Übrigen dem Sozialgeheimnis unterliegenden Daten der GEZ gegenüber preisgeben und dies in einer Zeit von eGovernment, in der es ohne Weiteres möglich wäre, in einem datenschutzgerechten Verfahren die Rundfunkgebührenbefreiung ohne zusätzliche Belastung der Betroffenen in elektronischer Form abzuwickeln.

1.9 Fußball-Weltmeisterschaft 2006 in Deutschland

Wer hätte bei der letzten Fußball-Weltmeisterschaft gedacht, dass sich der Datenschutz mit intensiven Beratungen auf diesem Feld einschalten muss. Aber die Möglichkeiten der modernen Datenverarbeitung haben auch vor diesem Bereich keinen Halt gemacht. Mittlerweile geht es hierbei um die Verarbeitung von Millionen Personendatensätzen aus aller Welt. Es gibt zwei Problemkreise: Einerseits geht es um den Verkauf und die Nutzung der Eintrittskarten (Ticketingverfahren) und andererseits um die Sicherheitsüberprüfung der Menschen, die im Nahbereich der WM-Stadien beschäftigt oder eingesetzt werden (Akkreditierungsverfahren).

Hinsichtlich der datenschutzrechtlichen Problematik des Ticketingverfahrens verweise ich auf die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10./11. März 2005 (vgl. Ziff. 19.2 dieses Berichts) und auf die Veröffentlichung auf meiner Internetseite. Ich bin der Auffassung, dass bei der Bestellung der Eintrittskarten Daten erhoben werden, die für den Kauf nicht erforderlich sind, wie z. B. die Staatsangehörigkeit. Auch werden die Käufer der Eintrittskarten nicht hinreichend über die Verarbeitung ihrer Daten und ihre Rechte aufgeklärt.

Bezüglich der Akkreditierung fehlt es an einer ausreichenden gesetzlichen Grundlage für die Überprüfung dieses umfangreichen Personenkreises (ca. 250.000 Menschen) durch die Polizei und den Verfassungsschutz, ohne dass die Betroffenen selbst hinreichend über die Gründe, die evtl. zu einer Ablehnung ihres Einsatzes bei der WM geführt haben, unterrichtet werden. Diese Ablehnung kann zu weitreichenden arbeitsrechtlichen Konsequenzen führen und auf fehlerhaften Daten beruhen, die durch den Betroffenen nicht richtig gestellt werden können. Weitere Ausführungen zu diesem Thema (vgl. Ziff. 9.9 und Ziff. 18.13 dieses Berichts).

Beide Verfahren werden mit deutscher Gründlichkeit durchgeführt, ein immens großer Datenbestand wird beim Deutschen Fußball-Bund (DFB) aufgebaut und damit der Eindruck erweckt, man habe alles im Griff. Es bestehen aber bei vielen Fachleuten erhebliche Zweifel, ob diese Maßnahmen tatsächlich zu einem Sicherheitsgewinn führen, zumal sich bereits im Vorfeld gezeigt hat, dass viele der auf dem Papier stehenden Maßnahmen sich in der Praxis nicht umsetzen lassen werden.

1.10 Videoüberwachung

Regelmäßig erreichen mich eine Vielzahl von Anfragen und Eingaben zur Videoüberwachung (vgl. Ziff. 18.10 dieses Berichts). Dabei bekomme ich Beschwerden von Bürgern, die mich auf Video-Objektive hinweisen, die viele gar nicht wahrgenommen hätten. Oft handelt es sich um Fälle, die ohne eine Prüfung vor Ort nicht abschließend entschieden werden können. Zu leichtfertig vertrauen die Anwender darauf, dass der Bürger ihre Motive zur Installation einer Videoüberwachungsanlage akzeptiert. Argumente der Anwender, wie „Was ist denn schon dabei?“ oder „Das macht doch heute fast jeder.“, werden von den Betroffenen nicht akzeptiert. Sie fühlen sich als Arbeitnehmer, als Mieter oder als Kunden unwohl, können nicht abschätzen, ob sie permanent beobachtet werden, wer sich die Aufzeichnungen anschaut, usw. Dabei meinen viele Anwender, sie müssten nicht auf die Tatsache der Videoüberwachung hinweisen. Gerade in diesen Fällen reagieren Betroffene besonders verärgert und fühlen sich überrumpelt, eben heimlich beobachtet.

Ein deutlicher Trend geht in letzter Zeit dahin, dass Restaurantbesitzer ihre Lokalitäten per Videoanlage überwachen, angeblich, um Zechpreller zu erkennen. Bei entsprechenden Prüfungen entstand allerdings das Gefühl, dass der hauptsächliche Grund die permanente Überwachung des Personals ist. In den Fällen, in denen sich Gäste über eine Videoüberwachung in einem Restaurant beschweren, sagen sie mir meistens, sie machten das nur für andere, sie selbst gingen nicht mehr in dieses Restaurant. Abgesehen von den datenschutzrechtlichen Belangen meine ich, die Anwender machen sich ihre Entscheidung zu leicht und verkennen oft die Interessen ihrer Kunden.

1.11 Der Verbraucher im Internet

Zahlreiche Verbraucher haben beim Interneteinkauf Angst um die Sicherheit ihrer persönlichen Daten. Das hat zuletzt erneut eine Ende November 2005 vorgestellte Studie des Branchenverbandes Business Software Alliance (BSA) bestätigt. Der Studie liegt die Auswertung von Aussagen von 4.700 Internetnutzern zugrunde. Den Angaben zufolge sind 85 % der befragten Deutschen der Meinung, dass Online-Händler zu wenig für den Schutz ihrer Kunden unternehmen.

Die Untersuchung ergab weiterhin, dass 84 % der befragten deutschen Nutzer auf ihrem Computer Antivirensoftware einsetzen, rund 50 % nutzen E-Mail-Filterprogramme oder Anti-Spam-Software, 43 % verwenden Programme zur Abwehr von Spionagesoftware.

War der Verbraucher mit seinen Sicherheitsbedürfnissen im Internet in der Vergangenheit weitestgehend auf sich allein gestellt, nehmen sich nunmehr auch große Unternehmen der IT-Branche diesem Anliegen an, nachdem die Datenkriminalität,

wie die Entsendung von sensiblen Finanzdaten oder der millionenfache Identitäts-Diebstahl, eine Dimension angenommen hat, die den Internethandel erheblich belastet. Auch ich war im Berichtsjahr erneut bemüht, die Verbraucherrechte im Datenschutz zu stärken (vgl. Ziff. 1.14 und Ziff. 4.1 dieses Berichts).

1.12 Datenschutzkontrolle zusammenhängend organisieren

Auf über 100 Seiten beschreibt die Bundesregierung in ihrem Aktionsprogramm „Informationsgesellschaft Deutschland 2006“ (BR-Drs. 976/03) die nächsten Schritte der elektronischen Datenverarbeitung. Fast alle darin beschriebenen Projekte erfordern die Verarbeitung personenbezogener Daten. Allein im Anhang sind fast 100 Projekte, beginnend mit „Digitale Wirtschaft“ über „Bildung und Qualifizierung“, „Gesundheitswesen und andere Dienste“ bis hin zu „eGovernment“ aufgeführt. Die meisten der angesprochenen Projekte werden Auswirkungen auf die Landesebene haben und verlangen i. d. R. eine Befassung durch meine Dienststelle. An der Aufzählung der Projekte lässt sich leicht verdeutlichen, in welch starkem Maße sich die personenbezogene Datenverarbeitung privater und öffentlicher Stellen immer weiter verzahnt. Auch in diesem Bericht finden sich eine Vielzahl von Beispielen. Sei es das elektronische Gerichtspostfach für Bürger, Anwaltschaft, Gerichte und Staatsanwaltschaft, sei es die JobCard, der elektronische Datenaustausch zwischen Arbeitgeber und Steuerverwaltung oder sei es die elektronische Gesundheitskarte – in allen Bereichen nimmt die Verzahnung zwischen öffentlichem und privatem Bereich zu.

Ich schildere diese Entwicklung, weil ich gefragt worden bin, ob Bremen nicht dem Beispiel Niedersachsen folgen und die Aufgaben des Landesbeauftragten für den Datenschutz und der Datenschutzaufsichtsbehörde für den privaten Bereich trennen sollte. Ich meine, zu den damaligen Überlegungen hier im Lande zur Zusammenlegung der beiden Datenschutzaufsichtsbereiche, die im Wesentlichen auf dem Gesichtspunkt der möglichen Synergieeffekte, sowohl bei der Rechtsanwendung der allgemeinen Datenschutzvorschriften wie auch in der Informations- und Kommunikationstechnikbeurteilung beruhen, sind noch weitere Elemente hinzugekommen.

Eine Datenschutzkontrolle, die nicht in beide Töpfe schauen kann, um zu erkennen, ob die Zutaten stimmen und die Rezepte angewendet werden, bleibt auf halbem Weg stehen. Die Datenschutzkontrolle muss z. B. sehen, wie die Kreditwirtschaft ihre Datenverarbeitung zur Kontenabfrage oder zur Geldwäsche organisiert oder welche Daten an der Schnittstelle zu den Finanzbehörden bzw. der Staatsanwaltschaft zur Verfügung gestellt werden, um die dortige weitere Verarbeitung kompetent kontrollieren zu können. Oder ist es nicht für Beratung und Kontrolle besser, wenn, wie in den Fällen der elektronischen Gesundheitskarte, die Datenschutzbehörde sowohl bei Apotheken, Ärzten und ärztlichen Rechenzentren wie bei der Krankenkasse, Einblick in die Datenverarbeitungsvorgänge nehmen kann? Weitere Argumente ergeben sich aus dem von der EU eingeleiteten Vertragsverletzungsverfahren (vgl. Ziff. 19.6 dieses Berichts). Ich rate daher dringend davon ab, eine Zweiteilung der Datenschutzkontrolle vorzunehmen.

1.13 Bürgeranfragen

In 2005 erhielt ich zahlreiche Eingaben per Post oder E-Mail, durch Anrufe oder Besuche von Bürgern in meiner Sprechstunde, die mich um die Klärung ihrer verschiedenen datenschutzrechtlichen Anliegen baten. Im öffentlichen Bereich ging es am häufigsten um Fragen aus dem Gesundheitsbereich, hier um Fragen der Kranken- und Pflegeversicherung sowie des Datenschutzes in Krankenhäusern. Stark vertreten war auch der Bereich Jugend, Familie und Soziales. Hierbei ging es häufig um Fragen der Sozial- und Jugendhilfe und um Fragen in Bezug auf die Datenverarbeitung der BAgIS. In der Rangliste folgte der Bereich Inneres – hier bezogen sich die meisten Fälle auf Polizei und Verfassungsschutz, gefolgt von melderechtlichen Anliegen.

Im nicht-öffentlichen Bereich waren folgende Branchen besonders häufig vertreten: Gesundheit, hier vor allem in Bezug auf Ärzte und Apotheken, die Videoüberwachung, vornehmlich im Einsatz beim Handel, gefolgt von den Auskunfteien. Erst an vierter Stelle rangierten datenschutzrechtliche Fragen zum Internet, gefolgt von Fragen des Arbeitnehmerdatenschutzes. Auch eine große Zahl der telefonischen Anfragen betrafen die Datenverarbeitung im nicht-öffentlichen Bereich.

Um die Vielfalt der Anfragen aus dem öffentlichen wie nicht-öffentlichen Bereich zu dokumentieren, habe ich auszugsweise einige der Themen aus dem Berichtsjahr in einer Tabelle zusammengestellt (vgl Ziff. 21.2 dieses Berichts). Die dort aufgeführten Fragen konnte ich alle telefonisch beantworten. Ich bin aus Gründen der Effektivität bemüht, möglichst viele Fragen am Telefon zu erledigen, befinden sich die Betroffenen aber in Auseinandersetzung mit Dritten, wird i. d. R. eine schriftliche Bescheidung notwendig.

1.14 Öffentlichkeitsarbeit und Presseberichterstattung

Auch im vergangenen Berichtszeitraum habe ich zu diversen datenschutzrechtlichen Themen Pressemitteilungen herausgegeben, um insbesondere die Bremer Bürgerinnen und Bürger auf neue und teilweise sehr brisante Entwicklungen im Datenschutz aufmerksam zu machen und sie zu motivieren, ihr Recht auf informationelle Selbstbestimmung auch tatsächlich wahrzunehmen. Die Pressemitteilungen können auf meiner Homepage www.datenschutz.bremen.de unter „Pressemitteilungen" abgerufen werden. Ferner bin ich Anfragen der Medien nachgekommen und habe mich im Rahmen von Interviews und Stellungnahmen zu datenschutzrechtlichen Fragestellungen geäußert. Ein Überblick über die in der Presse behandelten Datenschutzthemen ist im Anhang (vgl. Ziff. 21.1 dieses Berichts) zu finden.

Hervorzuheben ist eine Reihe von Beiträgen in den Bremer Tageszeitungen unter dem Titel „Datenklau im Internet", die von meinen Mitarbeitern datenschutzrechtlich beraten wurde. Diese Beiträge befassen sich mit verschiedenen Themen von der Internet-Sicherheit und zielen auf den privaten Nutzer. Themen waren dabei insbesondere:

- Telefonieren per Internet,
- Bankgeschäfte online,
- Schneller DSL-Anschluss,
- Wireless LAN.

Auf meiner Homepage veröffentliche ich neben den Pressemitteilungen unter „Aktuelles" und „Tipps für Bürger" weitere aktuelle Informationen zum Datenschutz, welche eine positive Resonanz in der Öffentlichkeit finden (vgl. Ziff. 1.16 dieses Berichts).

1.15 Durchgeführte Aus- und Fortbildungsmaßnahmen und Vorträge

Wie in den Vorjahren wurden durch Mitarbeiterinnen und Mitarbeiter des Landesbeauftragten für den Datenschutz (LfD) eine Reihe von Aus- und Fortbildungsmaßnahmen durchgeführt sowie Vorträge über verschiedene Datenschutzthemen gehalten. Meine Dienstleistungen in diesem Bereich sind außerhalb der öffentlichen Hand grundsätzlich nicht unentgeltlich.

Um den neu bestellten behördlichen Datenschutzbeauftragten die Aufnahme ihrer Tätigkeit zu erleichtern, bot ich diesen im Berichtsjahr Fortbildungsseminare im Aus- und Fortbildungszentrum der bremischen Verwaltung (AFZ) an, die bei den Datenschutzbeauftragten der Behörden, Kammern und Gesellschaften auf eine gute Resonanz stießen. Langfristig verspreche ich mir davon, dass die Stellen selbst einfache Fragen des Datenschutzes klären. Es wurden drei Seminare „Einführung in die Aufgaben eines behördlichen Datenschutzbeauftragten" durchgeführt, die von insgesamt ca. 60 Teilnehmern besucht wurden. Eine entsprechende Veranstaltung für Bremerhaven wird für Anfang März 2006 angeboten. Daneben wurde ein Einführungsseminar „Bremisches Datenschutzgesetz" für Mitarbeiterinnen und Mitarbeiter der bremischen Verwaltung im AFZ gehalten, das 18 Teilnehmer besuchten.

Erneut hat der LfD ein datenschutzrechtliches Seminar für Studierende des Studiengangs Informatik an der Hochschule Bremerhaven durchgeführt. Für 2006 musste ich die Übernahme eines gleichen Lehrauftrages, insbesondere wegen personeller Engpässe, leider absagen. Sieben Seminare „E-Mail- und Internetnutzung" an der Fortbildungseinrichtung einer Kammer hat eine Mitarbeiterin begleitet und insbesondere die Möglichkeiten und Grenzen des sicheren Umgangs mit dem Internet dargestellt; die Seminare wurden von ca. 150 Teilnehmern besucht. Eine Mitarbeiterin hat im Auftrag und auf Kosten der Europäischen Union durch einen einwöchigen Einsatz den Aufbau der Datenschutzorganisation in dem neuen EU-Mitgliedsland Litauen unterstützt. Es war auch für sie eine besondere Erfahrung, wie ein neues EU-Mitglied die EU-Datenschutzrichtlinien umgesetzt hat.

Des Weiteren wurden von meinen Mitarbeiterinnen und Mitarbeitern Vorträge und Referate anlässlich von Veranstaltungen bremischer Kammern zu Themen wie „Gesundheitskarte“, „JobCard“ und „Sicherer Internetauftritt“ gehalten. Ein Mitarbeiter hat vor dem Erfa-Kreis Bremen/Weser-Ems (Erfahrungskreis der Datenschutzbeauftragten) zu dem Thema: „Arbeitnehmerdatenschutz im Unternehmen“ einen Vortrag gehalten. Auf wichtige Datenschutzaspekte wurde unter meiner Teilnahme auf einer Diskussionsveranstaltung der Deutschen Außenhandels- und Verkehrsakademie über die Nutzung von „RFID“ wie auch auf einer öffentlichen Diskussionsrunde der SPD-Fraktion in der Bremischen Bürgerschaft zur „Videoüberwachung und Sicherheit im öffentlichen Raum“ von meiner Dienststelle hingewiesen.

Wie schon in den Vorjahren konnten bei weitem nicht alle Anfragen zu Fortbildungsmaßnahmen und Vorträgen befriedigt werden. In 2006 verringern sich meine Ressourcen für diese Aufgaben erneut.

1.16 Facelifting der Homepage www.datenschutz.bremen.de

Im Juni 2005 wurde meine überarbeitete Homepage freigeschaltet. Eine Überarbeitung war notwendig geworden aufgrund des Bremischen Gesetzes zur Gleichstellung von Menschen mit Behinderungen in der Fassung vom 18. Dezember 2003 in Verbindung mit der Verordnung für die Gestaltung barrierefreier Informationstechnik nach dem Bremischen Behindertengleichstellungsgesetz (Bremische Barrierefreie Informationstechnik-Verordnung – BremBITV) vom 13. Oktober 2005. Die neue Homepage präsentiert sich seitdem barrierefrei und noch aktueller.

Die Seiten enthalten eine Reihe neuer und interessanter Informationen wie auch interaktive Angebote. Hierzu gehören unter anderem

— Tipps und Hilfestellungen zum Thema Datenschutz in allen Lebenslagen,

— ein Datenschutzscheckheft als Download,

— Informationen zur Selbstverteidigung im Internet,

— ein breites Angebot an technischen Informationen,

— sämtliche Jahresberichte des Landesbeauftragten für den Datenschutz,

— wichtige Gesetzestexte zum Thema Datenschutz,

— Informationen zum Datenschutzaudit,

— ein Link zum Online-Learning-Projekt www.datenschutz4school.de.

Der in die Entwicklung und Erhaltung des Internetangebots investierte Aufwand lohnt sich, weil ich damit von vielen Bürgeranfragen entlastet bin. Die Seiten des Landesbeauftragten für den Datenschutz werden stark frequentiert, oft sind es mehrere Tausend Zugriffe im Monat. Es ist wichtig, dass sich die Bürger auf meiner Homepage über die Entwicklungen des Datenschutzes jederzeit informieren können.

1.17 Zur Situation der Dienststelle

In dem Maße, wie sich die personenbezogene Datenverarbeitung in allen gesellschaftlichen Bereichen ausweitet, steigen auch die Anforderungen an meine Dienststelle. Wie selbstverständlich wird erwartet, dass alle aktuellen Entwicklungen der Informations- und Kommunikationstechniken in Wirtschaft und Verwaltung begleitet und mit Rat und Tat datenschutzrechtlich betreut werden. Selbst Bereiche, in denen vor Jahren noch keiner an personenbezogene Datenverarbeitung dachte, werden davon in immer intensiverem Maße durchdrungen; jüngstes Beispiel ist die Fußball-Weltmeisterschaft. Parallel dazu werden immer mehr bereichsspezifische Datenverarbeitungsregelungen verabschiedet, die Rechtssprechung zu allen Bereichen wächst mit wenig Verzögerung im gleichen Umfang. Diese rasanten Fortschritte müssen ständig aufbereitet werden und parat sein, um rechtsstaatlichen Anforderungen bei meiner Aufgabenerfüllung zu genügen.

Während diese Entwicklung bei allen Datenschutzkontrollinstanzen des Bundes und der Länder zu einer Personal- und Budgetverbesserung geführt haben, ist im Land Bremen die gegenteilige Tendenz auszumachen. Nicht nur, dass seit 1990 beim Landesbeauftragten für den Datenschutz (LfD) ein Stellenabbau stattgefunden hat,

nein, dieser soll weiter fortgesetzt werden. Gleichzeitig sollen neue Aufgaben, zum Beispiel nach dem Informationsfreiheitsgesetz, zusätzlich übernommen werden. Was aber die Lage meiner Dienststelle darüber hinaus noch zusätzlich beeinträchtigt, ist der Wegfall von zwei Stellen Anfang 2006 sowie im laufenden Jahr von einer weiteren halben von zwölf Stellen durch Altersteilzeit ohne absehbar adäquaten Ausgleich.

Ich kann nicht auf Dauer erwarten, dass permanent weit über die reguläre Arbeitszeit hinaus gearbeitet wird, um den vielfältigen Anforderungen des Datenschutzes zu genügen. In der Dienststelle ist ein Klimawechsel zu verspüren, die Rahmenbedingungen haben sich hier mittlerweile dermaßen verschlechtert, dass auch Abgänge aus dem verbleibenden Personalbestand nicht mehr ausgeschlossen werden können.

Den beschriebenen Tendenzen, die bereits in 2005 sichtbar wurden und sich in 2006 fortsetzen, muss dringend entgegengewirkt werden. Ich werde in den anstehenden Haushaltsberatungen hierfür um Unterstützung werben.

1.18 Kooperationen

Das Bremische Datenschutzgesetz verpflichtet in § 27 Abs. 4 zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind. In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im Berichtsjahr unter dem Vorsitz des Landesbeauftragten für den Datenschutz Schleswig-Holstein tagte, wurden eine Reihe von Entschließungen gefasst, welche der Sicherung und Fortentwicklung des Datenschutzes dienen sollen. Die Entschließungen sind im Anhang dieses Berichts zu finden (vgl. Ziff. 19.1 bis 19.12 dieses Berichts).

Im nicht-öffentlichen Bereich findet unter den obersten Aufsichtsbehörden der einzelnen Bundesländer (Düsseldorfer Kreis) ein regelmäßiger Austausch über länderübergreifende Entwicklungen statt, um gemeinsame Positionen verbindlich zu machen. Dadurch soll eine einheitliche Auslegung der Vorschriften des Bundesdatenschutzgesetzes (BDSG) für den privaten Bereich gewährleistet werden. Bremen übernimmt im Jahr 2006 den Vorsitz des Düsseldorfer Kreises für ein Jahr.

Darüber hinaus nehme ich regelmäßig an den Sitzungen des Erfa-Kreises Bremen/Weser-Ems teil. Zum Erfa-Kreis gehören rund 70 Beauftragte für den Datenschutz, die überwiegend aus der Wirtschaft stammen. Schwerpunkt der Erfa-Kreis-Sitzungen ist die gegenseitige Unterstützung sowie Hilfeleistung bei der pragmatischen Umsetzung der Gesetzesanforderungen in die betriebliche Praxis. Da die betrieblichen Datenschutzbeauftragten in ihren Unternehmen oftmals hinsichtlich datenschutzrechtlicher Fragestellungen allein dastehen, ist der Erfa-Kreis ein wichtiges Gremium, um Erfahrungen auszutauschen und Probleme zu diskutieren. Da mir insbesondere auch die Verankerung des Datenschutzes in den Betrieben ein Anliegen ist, begleite ich gern die interessanten Diskussionen und beantworte die an mich als Aufsichtsbehörde gerichteten Fragen. Darüber hinaus informiere ich die Mitglieder des Erfa-Kreises über aktuelle datenschutzrechtliche Entwicklungen.

Seit längerer Zeit ist der Landesbeauftragte für den Datenschutz auch Projektpartner des Virtuellen Datenschutzbüros (www.datenschutz.de) und veröffentlicht über diese Plattform Beiträge. Beim Virtuellen Datenschutzbüro handelt es sich um einen gemeinsamen Service von Datenschutzinstitutionen (u. a. Bundesdatenschutzbeauftragter, Landesdatenschutzbeauftragte, Datenschutzbeauftragte der Kirchen und des Rundfunks sowie europäische und internationale Datenschutzeinrichtungen) im Internet. Die Federführung liegt beim Unabhängigen Landeszentrum für den Datenschutz Schleswig-Holstein (ULD).

2. Behördliche und betriebliche Beauftragte für den Datenschutz

Während es die Funktion der betrieblichen Beauftragten für den Datenschutz seit fast 30 Jahren gibt und diese sich weitgehend in den Betrieben etabliert haben, stehen die behördlichen Beauftragten für den Datenschutz erst ganz am Anfang ihres Wirkens. Ich bin im Rahmen meiner Möglichkeiten bemüht, beide bei ihrer Tätigkeit zu unterstützen und neue Beauftragte durch Schulungen in ihre Aufgaben einzuführen. Am Anfang stehen naturgemäß viele Fragen, die zu einer zusätzlichen Belastung meiner Referate führen. Am Ende – so die Hoffnung – sollen diese Investitionen zu einer Entlastung meines Hauses beitragen.

2.1 Behördliche Datenschutzbeauftragte

Ein wichtiger Teil meiner Arbeit betraf im Berichtszeitraum erneut die Bestellung und das Tätigwerden der behördlichen Datenschutzbeauftragten bei den öffentlichen Stellen in Bremen und Bremerhaven. Zwischenzeitlich haben fast alle Dienststellen der Verwaltung einen behördlichen Datenschutzbeauftragten bestellt und gemeldet. Dabei ging der Ernennung bei einigen Stellen ein langwieriger Prozess voraus, in dem ich die Bestellung des behördlichen Datenschutzbeauftragten wiederholt anmahnen oder gar eine formelle Beanstandung androhen musste. Hierzu zählte das Stadtamt Bremen, das als einer der größten Verarbeiter personenbezogener Daten in der Verwaltung erst am Ende des Berichtsjahres einen behördlichen Datenschutzbeauftragten bestellt hat.

Im November 2005 sind auch für die Ämter des Magistrats der Stadt Bremerhaven die bis dahin fehlenden behördlichen Datenschutzbeauftragten bestellt worden. Die Bestellung erfolgte teilweise dezernats- und ämterübergreifend, auch wurden behördliche Datenschutzbeauftragte bei den Wirtschafts- und Eigenbetrieben der Stadt bestellt und mir gemeldet.

Gem. § 7 a i. V. m. § 1 Abs. 2 Bremisches Datenschutzgesetz (BremDSG) sind behördliche Datenschutzbeauftragte jedoch nicht nur von den Ämtern und Behörden in Bremen und Bremerhaven, sondern u. a. auch von den Kammern und Gesellschaften, denen Aufgaben der öffentlichen Verwaltung übertragen worden sind, zu bestellen und mir zu melden. Eine Mitteilung nach § 7 a Abs. 5 BremDSG hatte ich bislang auch von diesen Stellen fast ausnahmslos nicht erhalten. Mit Rundschreiben wies ich die Stellen auf ihre gesetzliche Verpflichtung hin und stellte ihnen die für die Bestellung und Meldung entwickelten Formulare zur Verfügung. Mehrere Kammern und Gesellschaften bestellten daraufhin behördliche Datenschutzbeauftragte.

Erstmalig wurden im Berichtsjahr zweitägige Fortbildungsveranstaltungen für behördliche Datenschutzbeauftragte der bremischen Verwaltung und der öffentlichrechtlichen Einrichtungen abgehalten. Die Seminare sollen fortgesetzt werden. Meldungen für diese Kurse nimmt das Aus- und Fortbildungszentrum (AFZ) der bremischen Verwaltung entgegen. Auch für die behördlichen Datenschutzbeauftragten des Magistrats der Stadt Bremerhaven wird ein gleichartiges Seminar für Anfang 2006 angeboten. Die Seminare umfassen eine Einführung in das bremische Datenschutzrecht, eine Vertiefung in die gesetzlich konkretisierten Aufgaben eines behördlichen Datenschutzbeauftragten und seine besondere Stellung in der Behörde sowie einen datenverarbeitungstechnischen Teil mit Einblick in die technisch-organisatorischen Maßnahmen. Leider konnten geplante Workshops mit den Teilnehmern der Einführungsseminare, die dem Erfahrungsaustausch dienen sollen, bisher noch nicht durchgeführt werden.

2.2 Gesetzesänderung der Bestellpflicht von betrieblichen Datenschutzbeauftragten

Am 23. September 2005 hat der Bundesrat einen Gesetzesvorschlag der Länder Niedersachsen und Hessen beschlossen (Drs. 599/05), welcher vorsieht, dass die Pflicht zur Bestellung betrieblicher Datenschutzbeauftragter nicht mehr ab einer Mitarbeiterzahl von fünf bestehen soll, sondern erst ab 20 Mitarbeitern. Parallel hierzu soll eine identische Erhöhung der Arbeitnehmeranzahl für das Einsetzen der Meldepflicht erfolgen.

Die vorgeschlagene Gesetzesänderung halte ich für den falschen Ansatz. Eine pauschale Anhebung der Arbeitnehmeranzahl verkennt, dass aufgrund modernster DV-Technik auch Firmen mit nur wenigen Personen in riskanten Bereichen Daten verarbeiten können. Hier bedarf es einer eigenständigen Verantwortung für den Datenschutz. Die Bestellung von betrieblichen Datenschutzbeauftragten soll interaktiv den Datenschutz in allen Verfahren betrieblicher Datenverarbeitung sicherstellen. Daher wird auch von der Europäischen Kommission die Bestellung betrieblicher Datenschutzbeauftragter empfohlen (vgl. erster Bericht der Kommission über die Durchführung der Datenschutzrichtlinie – KOM [2003] 265 endg., Ziff. 4.4.4 und Ziff. 6). Es besteht bei Unternehmen, für die kein betrieblicher Datenschutzbeauftragter bestellt ist, die Gefahr, dass der Datenschutz in Vergessenheit gerät. Absehbar ist, dass es gerade dann in diesem Segment aufgrund von Eingaben vermehrt zu Kontrollen der Aufsichtsbehörden kommen wird, was zu einem Bürokratieaufbau statt des angestrebten Bürokratieabbaus führen würde.

3. Europa und Internationales

Immer mehr Entscheidungen zur personenbezogenen Datenverarbeitung werden auf der europäischen Ebene getroffen (vgl. Ziff. 20 ff dieses Berichts). Diese schlagen teilweise unmittelbar auf die Landesebene durch. Das bedeutet für meine Dienststelle, dass auch diese Entwicklungen beobachtet werden müssen, damit die Vorgaben bei meinen datenschutzrechtlichen Stellungnahmen berücksichtigt werden. Einige will ich nachfolgend kurz darstellen.

In einer globalen Welt nimmt natürlich auch der Datenaustausch mit Staaten außerhalb der EU zu. Die Rahmenbedingungen hierfür regelt das Bundesdatenschutzgesetz (BDSG) nach Maßgabe der EU-Datenschutzrichtlinie. In meiner Rolle als Aufsichts- wie Genehmigungsbehörde wurde ich im Berichtszeitraum aus der Privatwirtschaft des Landes in nicht unerheblichem Maße mit Fragen zu diesem Bereich in Anspruch genommen (vgl. Ziff. 18.13 dieses Berichts).

3.1 Vertragsverletzungsverfahren wegen mangelnder Unabhängigkeit

Die Kommission der Europäischen Gemeinschaften hat am 5. Juli 2005 ein Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland eingeleitet. Sie ist der Auffassung, dass die Bundesrepublik gegen die Verpflichtung aus Art. 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG (EG-Datenschutzrichtlinie) verstößt. Nach dieser Vorschrift haben die Kontrollstellen die ihnen zugewiesenen Aufgaben in „völliger Unabhängigkeit“ wahrzunehmen.

Gemäß § 38 Abs. 6 Bundesdatenschutzgesetz (BDSG) bestimmen die Landesregierungen oder die von ihnen ermächtigten Stellen die für die Kontrolle der Durchführung des Datenschutzes zuständigen Aufsichtsbehörden. Durch die Bekanntmachungen des Senats über Zuständigkeiten nach dem BDSG sind dem Landesbeauftragten für den Datenschutz die Aufgaben der Aufsichtsbehörde übertragen worden. Weder § 38 BDSG noch die Bekanntmachungen treffen eine Aussage bezüglich der Unabhängigkeit der Aufsichtsbehörde. Nur hinsichtlich der Rechtsstellung des Landesbeauftragten für den Datenschutz stellt § 25 Bremisches Datenschutzgesetz (BremDSG) fest: „Der Landesbeauftragte für den Datenschutz ist in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen. Er untersteht der Dienstaufsicht des Senats.“

Die Kommission – wie auch der Senatskommissar für den Datenschutz bisher – gehen davon aus, dass die Aufsichtsbehörde in Bremen sowohl der Fachaufsicht als auch der Dienstaufsicht unterliegt. Die Fachaufsicht solle sich implizit ergeben. Dadurch, dass Bremen keine ausdrückliche Regelung bezüglich der Unabhängigkeit getroffen habe, seien die allgemeinen Regelungen anwendbar, so dass die Aufsichtsbehörde – wie jede andere Behörde – der Fachaufsicht der Landesregierung unterliege. Die Dienstaufsicht wird auf § 25 BremDSG gestützt.

Nach § 226 des Vertrages zur Gründung der Europäischen Gemeinschaften (EGV) muss die Kommission dem von dem Vertragsverletzungsverfahren betroffenen Mitgliedstaat die Gelegenheit zur Äußerung geben. Die Bundesregierung hat mit Schreiben vom 13. September 2005 Stellung genommen. Sie vertritt die Auffassung, dass Art. 28 der EG-Datenschutzrichtlinie lediglich eine funktionale, jedoch keine organisatorische Unabhängigkeit verlange. Eine Einbindung der Kontrollstelle in eine bestehende Aufsichtsstruktur, sei es in der Form der Fachaufsicht, der Rechtsaufsicht oder der Dienstaufsicht, stehe der geforderten Unabhängigkeit nicht entgegen. Die Übertragung der Aufgabe der Datenschutzaufsicht über die Privatwirtschaft auf eine von der Exekutive völlig unabhängige Institution sei mit dem deutschen Verfassungsrecht nicht vereinbar.

Unabhängig von der Frage, ob die Unabhängigkeit funktional oder auch organisatorisch ausgestaltet werden muss, könnte man im Wege der Gesetzesauslegung für Bremen zu dem Ergebnis kommen, dass die Aufsichtsbehörde in Bremen weder einer Fach- noch einer Rechtsaufsicht untersteht. Der Landesbeauftragte für den Datenschutz ist nach § 25 BremDSG in Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen; er untersteht lediglich der Dienstaufsicht des Senats. Man könnte das Gesetz daher dahingehend auslegen, dass dadurch, dass dem Landesbeauftragten auch die Aufgaben der Aufsichtsbehörde übertragen worden sind, seine Unabhängigkeit auf diese Aufgabenerfüllung ausstrahlt. Da die Kommission aber darüber hinaus eine Dienstaufsicht für nicht zulässig erachtet, könnte weiterhin die in § 25 BremDSG geregelte Dienstaufsicht nicht richtlinienkonform sein.

Da die Bundesregierung in ihrer Stellungnahme eine von der Kommission abweichende Auffassung vertritt, ist ein weiteres Betreiben des Klageverfahrens seitens der Kommission vor dem Europäischen Gerichtshofes (EuGH) sehr wahrscheinlich. Wenn der EuGH zu der Feststellung käme, dass die deutsche Umsetzung nicht richtlinienkonform ist, müssten entweder die Regelung des § 38 BDSG oder das bremische Landesrecht angepasst werden.

3.2 Vorratsdatenspeicherung beschlossene Sache

Am 14. Dezember 2005 wurde die obligatorische Speicherung von Telekommunikations-Verkehrsdaten durch das Europäische Parlament beschlossen. Dies ist bedauerlich, weil die Vorratsdatenspeicherung bei der Novellierung des Telekommunikationsgesetzes – nicht zuletzt aufgrund der Proteste der Datenschützer – auf nationaler Ebene erfolgreich verhindert werden konnte. Auch von weiten Teilen des Deutschen Bundestages wurden Bedenken gegen die europäischen Bestrebungen geltend gemacht, flächendeckend eine Verpflichtung zur Speicherung von Telekommunikationsdaten auf Vorrat einzuführen (vgl. hierzu BT-Drs. 16/72, 16/128, 16/142 und 16/237).

Die vom Europäischen Parlament beschlossene Richtlinie verpflichtet die Anbieter von Telekommunikations- und Internetdiensten, umfangreiche Verkehrsdaten auf Vorrat für die Sicherheitsbehörden zu speichern, ohne dass ein konkreter Verdacht der Begehung einer Straftat besteht. Die Richtlinie sieht Speicherungsfristen zwischen sechs und 24 Monaten vor. Erfasst von der Speicherung sind u. a. Daten über die an Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner, Verbindungsdaten jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Bei Internetverbindungen müssen der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet und die dabei zugeteilte IP-Adresse sowie die Verbindungsdaten jeder einzelnen E-Mail gespeichert werden. Lediglich die Speicherung von Inhalten der Kommunikation ist nicht vorgesehen.

Die beschlossene Vorratsdatenspeicherung stellt einen unverhältnismäßigen Eingriff in die Privatsphäre und die Vertraulichkeit der Kommunikation unverdächtiger Bürger dar. Alternative Regelungsansätze, wie das in den USA praktizierte anlassbezogene Vorhalten von Daten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) hätten eine erheblich geringe Eingriffstiefe aufgewiesen, wurden jedoch nicht ernsthaft in Erwägung gezogen.

Von der Entscheidung ist nahezu jeder Bürger betroffen, da die Nutzung des Telefons und Internets ein kaum noch wegzudenkender Gegenstand des Alltags geworden ist. Angesichts der enormen Tragweite für die Grundrechte der Betroffenen kämpften die Datenschützer bis zuletzt vehement gegen die Vorratsdatenspeicherung. Die Konferenz der Landesbeauftragten hatte im Oktober 2005 nochmals ihre bereits seit 2002 geäußerte Kritik an einer Vorratsdatenspeicherung in einer Entschließung (vgl. Ziff. 19.9 dieses Berichts) bekräftigt. In dieser Entschließung appellierte sie an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung nicht zuzustimmen.

Was verbleibt ist, vorbehaltlich einer verfassungsgerichtlichen Klärung, dass der deutsche Gesetzgeber aufgefordert ist, die Richtlinie im Sinne des Datenschutzes möglichst restriktiv – soweit dies überhaupt möglich ist – umzusetzen. Demnach muss zwingend die nach der Richtlinie vorgesehene kürzeste Speicherdauer von sechs Monaten normiert werden. Weiterhin müssen die Daten einer strengen Zweckbindung unterliegen. Langfristig bleibt zu hoffen, dass die Richtlinie durch den Europäischen Gerichtshof beanstandet wird.

3.3 Einführung eines EUROPASSes

Am 14. Dezember 2004 stimmte das Europäische Parlament dem gemeinschaftlichen „Rahmenkonzept zur Förderung der Transparenz von Qualifikationen und Kompetenzen“ (EUROPASS) zu. EUROPASS enthält Informationen über die Schulzeit und die Ausbildung der Bewerber. Damit sollen die Qualifikationen und Kompetenzen von Arbeitgebern in anderen als den ausstellenden europäischen Ländern richtig verstanden und angemessen eingestuft werden. Zu diesem Zweck bietet die Europäische Union (EU) in einem Internet-Portal den Bürgern an, ihren eige-

nen EUROPASS-Lebenslauf und ihr eigenes EUROPASS-Sprachenportfolie online zu erstellen (http://europass.cedefop.eu.int).

Das Internet-Portal bietet keine Verschlüsselungsmöglichkeit der übertragenen Arbeitnehmer- bzw. Bewerberdaten an, dies ist datenschutzrechtlich bedenklich hinsichtlich der Datensicherheit des Verfahrens. Da es sich beim EUROPASS allerdings um ein Angebot der EU handelt, habe ich den zuständigen Europäischen Datenschutzbeauftragten angeschrieben und ihn auf die Problematik hingewiesen. Der Europäische Datenschutzbeauftragte antwortete mir, dass die Website durch Standardsicherheitsmaßnahmen geschützt werde. Eine erneute Überprüfung meinerseits ergab allerdings, dass die Übermittlung der personenbezogenen Daten weder mittels SSL erfolgt noch in das Verfahren integrierte Verschlüsselungsmechanismen bestehen. Zu Standardsicherheitsmaßnahmen gehört zumindest eine SSL-Verschlüsselung.

Parallel hierzu hat sich auch eine Abgeordnete des Europäischen Parlaments an die Europäische Kommission gewandt. Diese teilte ihr mit, dass man an einer sicheren Verbindung durch die Verwendung des http-Protokolls arbeitet. Die EU-Abgeordnete unterrichtete mich hierüber. Bis zum Redaktionsschluss waren diese Pläne jedoch noch nicht umgesetzt.

4. Internet, Telekommunikation, Teledienste

4.1 Internettelefonie – Telekommunikationsgeheimnis nicht gewährleistet

Bis vor kurzem war das Telefonieren über das Internet nicht interessant, weil die Sprachqualität miserabel war und die Übertragung oft zu lange dauerte. Doch in den letzten Jahren ist Bewegung in die Sache gekommen. Zuerst wurde die „Voice-over-IP"-Technologie (VoIP) innerhalb von Telefonanlagen eingeführt. In abgeschlossenen Hausnetzen kann im Gegensatz zum Internet die Sprachqualität gewährleistet werden. Die Infrastruktur des Internet wurde parallel dazu immer leistungsfähiger, sowohl was die großen nationalen und internationalen Datenleitungen betrifft als auch – durch die DSL-Technologien – der letzte Weg bis zum Kunden. Dadurch kann heute das Internet als Transportmedium für Sprachtelefonie genutzt werden. Dabei ist die Qualität oft sogar mit der von ISDN vergleichbar.

So genannte Gateways übernehmen dabei die Kopplung zwischen den herkömmlichen Telefonnetzen und der Internet-Technologie. Sie bilden die Brücke zwischen beiden Welten. Internet-Telefone werden damit vom herkömmlichen Telefon aus erreichbar und umgekehrt. Doch mit der Datensicherheit und mit der Vertraulichkeit des gesprochenen Wortes beim Telefonieren via Internet ist es nicht gut bestellt. Sprachtelefonie ist Echtzeit-Kommunikation, dabei wird im Internet das Realtime Transport Protocol (RTP) genutzt. Es basiert auf dem ungesicherten Datentransportprotokoll UDP (User Datagramm Protocol) des Internet und ermöglicht damit Übertragungen in guter Sprachqualität. Die dadurch zu erreichende Qualität der Sprachübertragung ist aber nachteilig für eine sichere Kommunikation: Gespräche können mit einfachen technischen Mitteln belauscht werden; in den Protokollen UDP bzw. RTP sind keine Sicherungsmechanismen eingebaut. Im Gegensatz zur herkömmlichen Telefonie, bei der das Abhören der Telefongespräche nur mit direktem physikalischen Zugriff auf die Telefonleitungen möglich war, ist zum Abhören von IP-Telefonie nur ein handelsüblicher Computer und entsprechende, frei im Internet verfügbare Software notwendig. Anleitungen dafür, wie solches Abhören durchgeführt werden kann, findet man zuhauf im Internet. Erst eine sichere Ende-zu-Ende-Verschlüsselung der Sprachpakete zwischen den Teilnehmern und deren genutzten Gateways bieten ausreichenden Schutz der Vertraulichkeit von Gesprächen. Diese Technologie existiert, wird aber nicht flächendeckend eingesetzt bzw. unterstützt.

Auch die Sicherheit der alten Telefonwelt, dass die im Telefondisplay des Angerufenen die angezeigte Telefonnummer des Anrufers wirklich zu dem entsprechenden Anschluss gehört, ist nicht mehr gegeben. Mit dem SIP-Protokoll (Session Initiation Protocol) kann eine beliebige Nummer an den Angerufenen übermittelt werden. So kann diesem beispielsweise der Anruf der Hausbank, des Finanzamts oder des Hausarztes vorgespielt werden. Unternehmen, die ihre Kunden über die übermittelte Rufnummer identifizieren, können sich nicht mehr auf die übertragende Rufnummer verlassen. Falschbestellungen oder Ähnliches sind möglich. Zahlreiche Missbrauchsmöglichkeiten erwachsen hieraus.

Die Übermittlung falscher Anschlussdaten kann auch dazu genutzt werden, dass man umsonst auf Kosten anderer telefonieren kann. Werden zum Aufbau des Gesprächs die entsprechenden falschen Daten zur Identifizierung an den Provider übermittelt, laufen die Gesprächskosten auf dem Konto eines anderen Teilnehmers auf. Fazit: Beim Telefonieren über das Internet ist das Telekommunikationsgeheimnis nicht garantiert. Aufgrund der beschriebenen Sicherheitsdefizite und der mangelnden Vertraulichkeit des gesprochenen Wortes ist die Nutzung von Internet-Telefonie aus Sicht des Datenschutzes derzeit nicht zu empfehlen.

Ich habe auf meinen Internet-Seiten einen Artikel mit Hintergrundinformationen zu diesem Thema veröffentlicht und die lokale Presse bei der Informationsrecherche für Beiträge zu diesem Thema beraten. Außerdem arbeite ich in einer Arbeitsgruppe des Arbeitskreises Technik mit, die momentan eine Orientierungshilfe zum Thema „VoIP" erarbeitet.

4.2 Orientierungshilfe „Kommunikation in drahtlosen Netzen"

Die drahtlose Kommunikation zwischen elektronischen Endgeräten setzt sich immer mehr durch. So werden Notebooks und PDA (Persönliche Digitale Assistenten) mittels WLAN in Firmennetze integriert oder Druckdaten mittels Bluetooth vom PC zum Drucker übertragen. Diese schnelle und sehr flexible Methode, Daten per Funk zu übertragen, birgt einige Risiken. Dass in diesen Bereichen dringend Handlungsbedarf besteht, habe ich bereits in meinem 27. Jahresbericht (vgl. Ziff. 3.3) angemerkt. Der Arbeitskreis Technik der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (AK Technik) hat dieses Thema aufgegriffen und unter meiner Mitarbeit die Orientierungshilfe „Datenschutz in drahtlosen Netzen" erarbeitet. Diese bereits in meinem 26. Jahresbericht (vgl. Ziff. 2.2) von mir angekündigte Orientierungshilfe ist im Berichtsjahr endlich fertiggestellt worden. Sie gibt einen Überblick über die „Funkverfahren" WLAN, Bluetooth und Infrarotkommunikation, beschreibt mögliche Gefährdungen und Schutzmaßnahmen, die beim Einsatz mobiler Endgeräte zu berücksichtigen sind und stellt allgemein gültige Schutzmaßnahmen vor, die grundsätzlich in allen Funknetzen umgesetzt werden können. Weiterhin ist auch ein kurzer Abschnitt über die rechtlichen Aspekte des Abhörens von drahtlosen Verbindungen enthalten. Die Orientierungshilfe kann von meinen Internetseiten unter folgendem Link heruntergeladen werden: http://www.datenschutz.bremen.de/pdf/oh_wlan.pdf

5. Medien

5.1 Verfahren der Rundfunkgebührenbefreiung

Der 8. Rundfunkgebührenstaatsvertrag sieht in § 6 Abs. 2 vor, dass der Antragsteller die Voraussetzungen für die Befreiung von der Rundfunkgebührenpflicht durch die Vorlage des Bewilligungsbescheides im Original oder in beglaubigter Kopie belegt. Ich konnte auf die datenschutzrechtliche Schieflage dieser Regelung leider nicht hinweisen, weil ich seitens der Senatskanzlei nicht über die geplante Änderung informiert wurde, obwohl hierzu eine gesetzliche Verpflichtung besteht (vgl. hierzu 27. JB, Ziff. 2.2). In der Praxis führt die Neuregelung zu einem gravierenden Eingriff in das Recht auf informationelle Selbstbestimmung von Arbeitslosengeld-, Sozialhilfe- und BAföG-Empfängern. In den Bewilligungsbescheiden befindet sich eine Vielzahl sensibler besonders schutzwürdiger Daten (z. B. zu einer Schwangerschaft oder Drogenabhängigkeit), die für eine Rundfunkgebührenbefreiung nicht erforderlich sind. Zudem kommt es nicht nur zu einer bloßen Vorlage – wie es das Gesetz vorsieht –, sondern die kompletten Bescheide werden von der GEZ eingescannt und gespeichert.

Da ich eine Vielzahl von Beschwerden betroffener Bremer Bürgerinnen und Bürger erhielt und Radio Bremen (die GEZ verarbeitet die Daten für Radio Bremen im Auftrag) ein von mir vorgeschlagenes datenschutzfreundliches Verfahren in der Praxis nicht umsetzte, berichtete ich in der November-Sitzung des Rechtsausschusses über die Datenschutzmängel beim Gebührenbefreiungsverfahren. In dieser Sitzung wurde angeregt, zügig eine „bremische" Lösung zu finden, die den Belangen des Datenschutzes Rechnung trägt.

Zu diesem Zweck wurde mit Unterstützung des Rechtsausschusses ein „runder Tisch" gebildet, an dem Vertreter von Radio Bremen, des Versorgungsamtes, des Amtes für Soziale Dienste, des BAföG-Amtes, der BAgIS und der Senatskanzlei wie

auch eine Vertreterin des Landesbeauftragten für den Datenschutz (LfD) teilgenommen haben. Die Vertreter des BAföG- und Versorgungsamtes berichteten in dieser Sitzung, dass sie bereits gesonderte Bescheide nur mit den für die GEZ relevanten Daten ausdrucken würden. Die BAgIS sah sich demgegenüber nicht in der Lage, das in Nürnberg gesteuerte System so zu verändern, dass gesonderte Bescheide für die Rundfunkgebührenbefreiung erstellt werden können. Von der Vertreterin des LfD wurde vorgeschlagen, dass die Sozialbehörden den Antrag auf Gebührenbefreiung mit dem Hinweis abstempeln könnten, dass der Originalbescheid, der zur Gebührenbefreiung berechtigt, vorgelegen hat. Mit diesem Verfahren würden dann nur noch die für die Rundfunkgebührenbefreiung erforderlichen Daten an die GEZ übermittelt werden. Die Vertreterin des Amtes für Soziale Dienste erklärte sich zu dieser Praxis bereit; lediglich auf Seiten der BAgIS gab es noch Vorbehalte aufgrund einer befürchteten Mehrbelastung.

In der Dezember-Sitzung des Rechtsausschusses erklärte sich die BAgIS erfreulicherweise bereit, auch auf dem Antragsformular die Voraussetzungen für eine Gebührenbefreiung zu bestätigen. Der Vertreter von Radio Bremen erklärte, dass das Verfahren akzeptiert werden würde, wenn die Bescheinigung die Qualität eines zweiten Originalbescheides aufweise. Nachträglich stellte sich heraus, dass weiterhin von den Betroffenen die Vorlage des Leistungsbewilligungsbescheides (zumindest der ersten Seite) eingefordert wird, da auf dem Befreiungsantrag die Angabe des Befreiungszeitraums nicht vorgesehen sei. Aus datenschutzrechtlicher Sicht enthält selbst die erste Seite des Bewilligungsbescheides mehr Daten (z. B. die namentliche Nennung der Mitglieder der Bedarfsgemeinschaft) als erforderlich. Zu begrüßen ist daher ein Angebot der ARGE Bremerhaven, die der GEZ bzw. Radio Bremen vorgeschlagen hat, dass sie neben der bisher von ihr im Antrag vermerkten Informationen zum ALG-II-Bezug auch die jeweilige Bewilligungsdauer mit angeben würde. Die Anwort der GEZ bzw. von Radio Bremen steht noch aus. Es bleibt zu hoffen, dass das Angebot angenommen und zur allgemeinen Praxis wird.

Da die Rechtslage und die damit verbundenen Probleme nicht nur im Land Bremen, sondern bundesweit existieren, bin ich mit den für den Rundfunkbereich zuständigen Datenschutzbeauftragten anderer Bundesländer bemüht, eine datenschutzfreundliche Regelung im Rundfunkgebührenstaatsvertrag zu erwirken.

6. Datenschutz durch Technikgestaltung und -bewertung

6.1 Verwaltungs-WLAN: BVN-Mobil

In der bremischen Verwaltung ebenso wie in der Privatwirtschaft besteht der Bedarf, immer mehr mobile Endgeräte wie Notebooks und PDA einzusetzen. Diese müssen flexibel in bestehende Infrastrukturen integriert werden, oftmals geschieht dies mit funkbasierten Lösungsmöglichkeiten wie Wireless LAN (WLAN). Die dabei grundsätzlichen Probleme habe ich zuletzt im 27. Jahresbericht (vgl. Ziff. 3.3) dargelegt. Der Senator für Finanzen (SfF), Referat 36, hat aufgrund der beim WLAN-Einsatz bestehenden Risiken das Projekt „BVN-Mobil“ initiiert. Ziel dieses Projektes ist es, ein koordiniertes, sicheres und abgestimmtes Konzept für die Realisierung der WLAN-Infrastruktur für die Behörden und Dienststellen im Land Bremen zu entwickeln. Es soll eine Infrastruktur geschaffen werden, die interessierten Behörden die Möglichkeit gibt, in klar definierter Art und Weise mobile Endgeräte bei unbedingter Einhaltung aller notwendigen Sicherheitsanforderungen für ihre Zwecke einzusetzen. Das mobile Arbeiten soll dabei nicht nur innerhalb der Grenzen der Dienststelle, sondern auch über ihre Grenzen hinaus möglich sein.

Das Projekt „BVN-Mobil“ des SfF soll als Ergebnis die technischen und betrieblichen Rahmenbedingungen für den funkbasierten Zugang zum BVN liefern. Ich berate die Projektgruppe bei der datenschutzkonformen Umsetzung der Lösung.

6.2 Öffnung des BVN: Neue Gefahren für das Bremer Verwaltungsnetz

Die Leistungsfähigkeit von DV-Netzen wird immer größer. Die Ideen zu ihrer Nutzung werden immer vielfältiger, und durch die technisch problemlose Kopplung von DV-Netzen untereinander werden immer mehr elektronische Dienste und Dienstleistungen möglich. So leben z. B. ganze Unternehmen davon, dass sie mehrere Userhelpdesks für verschiedene Kunden rund um die Uhr betreiben oder de-

ren DV-Systeme komplett administrieren und Fehler beseitigen. Die Dienstleister wählen sich im Bedarfsfall in das Netz des Kunden ein oder sind gar permanent mit diesem Netz verbunden oder bilden Brücken zwischen den Netzen ihrer Kunden.

Auch die Entwicklung bei den öffentlichen Stellen im Land wird hiervon gekennzeichnet. Es werden komplexe DV- und Anwendungssysteme betrieben, die allein für Administration und fortlaufendes Customizing, also Anpassung an den Bedarf, ein immenses Spezialwissen erfordern. Spezialwissen, das aus unterschiedlichen Gründen von vielen Dienststellen nicht vorgehalten werden kann. Das ist dann der Ausgangspunkt dafür, entsprechende Dienstleistungen von außen einzukaufen. Dies birgt aber auch Gefahren in sich und muss daher u. a. klar organisiert werden. Im Bremischen Datenschutzgesetz (BremDSG) sind die entsprechenden Anforderungen daran in § 9 (Verarbeitung personenbezogener Daten im Auftrag) explizit geregelt.

Die Öffnung eines DV-Netzes nach außen birgt zusätzliche Gefahren, die sich bei Netzen, die an verschiedenen Stellen gleichzeitig weiterentwickelt werden, nie abschließend beurteilen lassen. Der Personenkreis, der theoretisch mutwillig Daten ausspähen oder manipulieren kann, erweitert sich. Gravierender ist aber, dass ein Betreiber eines DV-Netzes nie zu 100 % sicher sein kann, dass das jeweils andere Netz fehlerlos konfiguriert und betrieben wird. Fehlfunktionen, Fehlkonfigurationen, Fehlbedienungen oder Schadsoftware aus anderen Netzen könnten dann Auswirkungen auf das eigene Netz haben. In den meisten Fällen sind DV-Netze gegenüber dem Internet mittels Firewall-Systemen abgeschottet. Einwahlverbindungen oder direkte Verbindungen (per angemieteter Standleitung oder VPN-Tunnel über das Internet) werden dabei oft nicht berücksichtigt. Sie bilden dann Außenverbindungen ohne jegliche technische Sicherheitsvorkehrung.

Aus diesen Gründen ist auch aus Sicht der einzelnen Dienststellen das BVN als nicht vollständig verlässliches Netz zu betrachten: Das BVN ist gegenüber dem Internet fachgerecht abgeschottet und somit in der Wahrnehmung vertrauenswürdig. Es dient als Verbindung aller teilnehmenden Dienststellen untereinander, mit zentralen Diensten und mit dem Internet. Zwischen den einzelnen Dienststellen ist Datenverkehr prinzipiell in jede Richtung möglich. In Dienststellen sind potenzielle Hintertürchen (ungeschützte Außenverbindungen wie oben beschrieben) aber nicht auszuschließen. Da die Dienststellen-DV-Netze an das BVN angebunden sind, sind diese Hintertürchen auch ungesicherte Außenverbindungen des BVN. Daraus ist nur das Fazit zu ziehen, dass sowohl Außenverbindungen aus DV-Netzen heraus einer genauen Risikoanalyse und Konzeption bedürfen und dass sich jede Dienststelle in ähnlicher Qualität gegen das BVN abschotten muss, wie sie dies bei der Abschottung gegenüber dem Internet oder einem Funk-Netz (vgl. 26. JB, Ziff. 2.2) tut; das BVN-Sicherheitskonzept muss umgesetzt werden (vgl. 26. JB, Ziff. 3.1).

6.3 Offene Netze und USB-Schnittstellen

USB-Schnittstellen (Universal Serial Bus) gehören seit einiger Zeit zur Standardausstattung von PC. Sie ermöglichen den Anschluss einer Vielzahl von Zusatzgeräten wie CD/DVD-Brenner, Festplatten und USB-Sticks. Über diese Schnittstelle können daher USB-Speichermedien unkontrolliert Informationen und Programme im- und exportieren. Darüber hinaus besteht die Möglichkeit, mit nicht zugelassenen Netzwerkadaptern Seiteneingänge in ein lokales Netz zu schaffen und so die zentrale Sicherheitsstruktur zu unterlaufen.

Bleiben USB-Schnittstellen ungeschützt, sind wesentliche durch technische und organisatorische Maßnahmen sicherzustellende Anforderungen des § 7 BremDSG, insbesondere dort die Nummern 3 (Zugriffskontrolle) und 4 (Weitergabekontrolle), nicht erfüllt. Werden sensible personenbezogene Daten verarbeitet, ist es grundsätzlich erforderlich sicherzustellen, dass keine dieser Daten aus dem zugriffsgeschützten Netz entfernt werden, d. h., das Starten der Gerätetreiber für USB-Speichermedien muss deaktiviert werden. Damit würde dem Standardbenutzer die Möglichkeit des Anschlusses von USB-Speichern komplett entzogen.

Häufig ist jedoch aus arbeitsorganisatorischen Gründen die komplette Deaktivierung der Schnittstelle nicht möglich. In diesem Fall ist es erforderlich, die USB-Schnittstelle über Zusatztools konfigurierbar zu machen und damit den Zugriff auf USB-Geräte zu steuern. Der Funktionsumfang des Tools ermöglicht u. a. die dynamische Sperrung und konfigurierbar den Zugriff auf Wechseldatenträger, die Sper-

rung bestimmter Gerätetypen, es protokolliert Gerätekonfigurationsänderungen und ermöglicht die Steuerung des Zugriffs für ausgewählte Benutzer oder Gruppen. Für die Gewährleistung der Datensicherheit der Datenträger ist eine verschlüsselte Speicherung sensibler Daten erforderlich. Auch hier sind Zusatztools verfügbar, die es ermöglichen, einen USB-Datenträger komplett zu verschlüsseln und den Datenzugriff über ein Passwort zu steuern.

Um die bisher in vielen Bereichen erreichte Netz- und Datensicherheit nicht durch ungeschützte Schnittstellen zu gefährden, ist es erforderlich, USB-Schnittstellen zu deaktivieren bzw. datenschutzgerecht zu konfigurieren.

7. Bremische Bürgerschaft – Die Arbeit des Rechtsausschusses

7.1 Ergebnisse der Beratung des 27. Jahresberichts

Bericht und Antrag des Rechtsausschusses zum 27. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2005 (Drucksache 16/578) und zur Stellungnahme des Senats – Mitteilung des Senats vom 30. August 2005 (Drucksache 16/737)

Bericht

Die Bürgerschaft (Landtag) überwies in ihrer Sitzung am 20. April 2005 den 27. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2005 (Drucksache 16/578) und in ihrer Sitzung am 15. September 2005 die dazu erfolgte Stellungnahme des Senats vom 30. August 2005 (Drucksache 16/737) an den Rechtsausschuss zur Beratung und Berichterstattung.

Der Ausschuss nahm seine Beratungen in seiner Sitzung am 5. Oktober 2005 auf und stellte für die Behandlung des 27. Jahresberichtes und für die Stellungnahme des Senats bei den nachfolgend aufgeführten Punkten Beratungs- und Handlungsbedarf fest:

1. Behördliche Datenschutzbeauftragte (Ziffer 1.4),
2. Ergebnisse des 26. Jahresberichts (Ziffer 4.1),
3. Prüfung der Telekommunikationsüberwachung (Ziffer 6.6),
4. ISA-Web statt NIVADIS (Ziffer 6.7),
5. Datenschutz im Notariat (Ziffer 7.2),
6. Stoffwechsel-Screening bei Neugeborenen (Ziffer 8.1),
7. Einführung der elektronischen Arbeitszeiterfassung (Ziffer 1.2),
8. Steuerzahler in der informationellen Zwangsjacke (Ziffer 1.9) und Steuerehrlichkeit – aber mit Datenschutz (Ziffer 12.1),
9. Erlaubnis erweiterter Datenbeschaffung durch die GEZ (Ziffer 2.2).

Der Rechtsausschuss erörterte die genannten Punkte mit dem Landesbeauftragten für den Datenschutz unter Hinzuziehung der Vertreter der betroffenen Ressorts und Institutionen in seinen Sitzungen am 2. November 2005, 7. Dezember 2005 und 15. Februar 2006. Die abschließende Beratung fand in der Sitzung am 15. Februar 2006 statt.

Zu den einzelnen Punkten nimmt der Rechtsausschuss wie folgt Stellung:

Behördliche Datenschutzbeauftragte (Ziffer 1.4): Die vom Landesbeauftragten für den Datenschutz in seinem Bericht monierten fehlenden Bestellungen behördlicher Datenschutzbeauftragter wurden nachgeholt:

Stadtamt: Der Senator für Inneres teilte dem Rechtsausschuss in seiner Sitzung am 15. Februar 2006 mit, dass für das Stadtamt die Bestellung des behördlichen Datenschutzbeauftragten am 22. Dezember 2005 erfolgt sei.

Magistrat der Stadt Bremerhaven: Der Magistrat der Stadt Bremerhaven teilte dem Landesbeauftragten für den Datenschutz am 31. Oktober 2005 mit, dass der Magistrat in seiner Sitzung am 26. Oktober 2005 über die Bestellung behördlicher Datenschutzbeauftragter beschlossen habe.

Ergebnisse des 26. Jahresberichts (Ziffer 4.1) Bürger-Service-Center (BSC – Ziffer 6.3.2 im 26. Jahresbericht): Mit seinem Bericht und Antrag vom 25. Februar 2005 zum 26. Jahresbericht des Landesbeauftragten für den Datenschutz nahm der Rechtsausschuss seinerzeit den vom Senator für Inneres und Sport vorgelegten Zeitplan zur Entwicklung eines Datenschutzkonzeptes zur Kenntnis.

Danach war ein Abschluss der bereits Ende 2004/Anfang 2005 aufgenommenen Arbeiten am Rahmenkonzept einschließlich der einzelnen Module für die Bereiche Kfz-Zulassung, Besuchereinladung, Fischereiangelegenheiten, Antragsannahme für Berechtigungsscheine, Wohngeld und Erziehungsgeld sowie Internet, räumliche Rahmenbedingungen bis Mitte März 2005 angekündigt. Für den Bereich Netzwerk und Zugriffsschutz war der Abschluss bis 30. Juni 2005 geplant. Nach der Einführung neuer Programme sollten die Module Gewerbe bis Herbst 2005 und Meldewesen bis Februar 2006 abgeschlossen sein.

Der Rechtsausschuss stellte bereits in seinem Bericht und Antrag zum 26. Jahresbericht fest, dass die Datenschutzkonzepte dem Grunde nach bereits im Rahmen der Vorbereitung zur Inbetriebnahme der automatisierten Datenverarbeitung – spätestens Ende 2002 – hätten entwickelt werden müssen.

Die datenschutzrechtliche Situation im Stadtamt sowie im BSC wurde aufgrund der immer noch fehlenden Datenschutzkonzepte vom Landesbeauftragten für den Datenschutz im 27. Jahresbericht unverändert beanstandet. Im Rahmen der Beratungen des Ausschusses erläuterte der Senator für Inneres und Sport, dass kurzfristig ein externes Unternehmen mit der Erstellung eines allgemeinen Datenschutzkonzeptes beauftragt werde. Nachdem der Senator für Inneres und Sport dem Rechtsausschuss in seiner Sitzung am 2. November 2005 eine Vorlage des Gesamtkonzeptes für den Beginn des Jahres 2006 in Aussicht gestellt hatte, wurde in der Sitzung am 15. Februar 2006 berichtet, dass die Arbeiten am Gesamtkonzept aufgenommen wurden und einzelne Module wie auch ein Rahmenkonzept bis Mai 2006 abgearbeitet werden sollen.

Einen Zeitplan zum Abschluss der Gesamtkonzepte konnte der Vertreter des Senators für Inneres und Sport nicht benennen.

Der Ausschuss stellt zum Abschluss seiner Beratungen fest, dass die Entwicklung eines Datenschutzkonzeptes für den Bereich des BSC immer noch nicht abgeschlossen wurde.

Waffenrecht (Ziffer 6.3.5 im 26. Jahresbericht): Anlässlich der Beratungen des 26. Jahresberichtes wurde durch den Rechtsausschuss festgestellt, dass ohne ein allgemeines Datenschutzkonzept für das Stadtamt das Datenschutzkonzept „Waffenrecht“ unvollständig sei. Ein Vertreter des Innensenators erklärte auf der Sitzung im Februar 2006, beides soll bis Mai 2006 fertig gestellt werden.

Auch hier stellt der Ausschuss zum Abschluss seiner Beratungen fest, dass die Entwicklung eines Datenschutzkonzeptes für den Bereich des Waffenrechts immer noch nicht abgeschlossen wurde.

Prüfung der Telekommunikationsüberwachung (Ziffer 6.6): Anhand eines Erlasses des Senators für Inneres und Sport zur Telekommunikationsüberwachung aus dem Jahr 2003 nahm der Landesbeauftragte für den Datenschutz eine Prüfung vor und stellte fest, dass technische und organisatorische Fragen offen geblieben und einige Verfahren abweichend vom Erlass durchgeführt worden waren. In Gesprächen mit Ressortvertretern seien Ergänzungsmöglichkeiten erörtert worden. Eine Stellungnahme der Polizei zu den Vorschlägen im Prüfbericht des Landesbeauftragten für den Datenschutz steht noch aus. Eben so wenig wurde eine erweiterte und aktualisierte Verfahrensbeschreibung sowie ein Einsatzkonzept für das Verschriftungsprogramm erstellt. Auch die vom Senat in Aussicht gestellte Beteiligung des Landesbeauftragten für den Datenschutz an einer Arbeitsgruppe zur Behebung der Probleme erfolgte bislang nicht.

Nach Mitteilung des Senators für Inneres und Sport hat sich die eingerichtete Arbeitsgruppe mit inhaltlichen Fragestellungen noch nicht befasst. Die für die entsprechenden Verfahren maßgebliche Arbeitsdatei wurde in Kooperation mit der Polizei in Niedersachsen fortgeschrieben. Sie wird von den Datenschutzbeauftragten der bremischen und niedersächsischen Polizei geprüft.

In der Sitzung am 15. Februar 2006 berichtete der Senator für Inneres und Sport, dass die Verfahrensbeschreibung für die Komponenten des Systems der Telekom-

munikationsüberwachung intern erstellt und innerhalb der Polizei abgestimmt wurden und sodann mit dem Landesbeauftragten für den Datenschutz eine Verständigung herbeigeführt wird.

Der Ausschuss nimmt zur Kenntnis, dass das erforderliche Datenschutzkonzept bis Ende Februar 2006 vorgelegt werden soll.

ISA-Web statt NIVADIS (Ziffer 6.7): Die Bremer Polizei verfolgte die Einführung des Vorgangsbearbeitungssystems NIVADIS nicht weiter, so dass nunmehr ein Datenschutzkonzept für ISA-Web zu erstellen ist. Der Senator für Inneres und Sport teilte dem Ausschuss in seiner Sitzung am 2. November 2005 mit, dass nach Erledigung einiger Restarbeiten bis zum Ende des Jahres 2005 umgehend die Vorlage eines Datenschutzkonzeptes für das InformationsSystemAnzeigen (ISA) erfolgen werde.

Der Rechtsausschuss nimmt Kenntnis.

Datenschutz im Notariat (Ziffer 7.2): Nach dem Bremischen Datenschutzgesetz ist in den Notariaten die Bestellung von Datenschutzbeauftragten verpflichtend. Die Hanseatische Notarkammer wurde vom Landesbeauftragten für den Datenschutz schriftlich gebeten, ihre Mitglieder über die bestehenden datenschutzrechtlichen Pflichten zu unterrichten und auf die Möglichkeiten kompetenter Beratung hinzuweisen. Untersuchungen des Landesbeauftragten für den Datenschutz bei sechs zufällig ausgewählten Notariaten auf freiwilliger Basis ergaben etliche datenschutztechnische Unzulänglichkeiten.

Der Senator für Justiz und Verfassung teilte dem Ausschuss mit, dass mit der Bremer Notarkammer verschiedene Lösungsansätze erörtert wurden. Der von der Notarkammer bestellte behördliche Datenschutzbeauftragte könne von den Notariaten als externer behördlicher Datenschutzbeauftragter bestellt werden und stehe diesen beratend zur Verfügung. Die von der Bundesnotarkammer eigens gegründete GmbH könne ebenfalls die entsprechenden Aufgaben übernehmen. In den einzelnen Notariaten werde entschieden, ob die Angebote der Notarkammer angenommen oder eigene Datenschutzbeauftragte eingesetzt werden. Die Bremer Notarkammer werde die Notariate auf die Notwendigkeit eines behördlichen Datenschutzbeauftragten hinweisen und dabei über die verschiedenen Möglichkeiten informieren.

In seiner Sitzung am 15. Februar 2006 nahm der Rechtsausschuss Kenntnis von einem an den Senator für Justiz und Verfassung gerichteten Schreiben der Bremer Notarkammer vom 8. Februar 2006. Danach wurden die Mitglieder der Notarkammer mit Kammer-Rundschreiben Nr. 01/2006 vom 3. Februar 2006 auf das für die im Land Bremen tätigen Notarinnen und Notare geltende Bremische Datenschutzgesetz (BremDSG) hingewiesen und ein Datenschutzbeauftragter für die Notarkammer gemäß § 7 a Abs. 1 BremDSG bestellt. Die Notarkammer beabsichtigt, neben einer Informationsveranstaltung für die bestellten Datenschutzbeauftragten in einem ausführlichen Rundschreiben die rechtlichen Grundlagen sowie die Anforderungen an die bestellten Datenschutzbeauftragten zu erläutern sowie eine Anleitung zur Unterstützung der Notariate und der Datenschutzbeauftragten vorzubereiten.

Der Rechtsausschuss nimmt Kenntnis.

Stoffwechselscreening bei Neugeborenen (Ziffer 8.1): Im Rahmen des bisherigen Stoffwechselscreening-Verfahrens wurden die Proben aus Bremen zusammen mit den Identitätsdaten des Kindes in das Labor des Universitätsklinikums Hamburg-Eppendorf geschickt, wo die Proben untersucht und die genetischen Ergebnisdaten gespeichert wurden, ohne dass zwischen Bremen und Hamburg eine datenschutzgerechte Regelung vereinbart wurde. Nach den mit Wirkung zum 1. April 2005 in Kraft getretenen Kinderrichtlinien des Gemeinsamen Bundesausschusses sind die beteiligten Krankenhäuser und Institute zur Erstellung eines Datenschutzkonzeptes verpflichtet.

Der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales verwies auf diese Richtlinien, nach denen die Einhaltung der jeweils gültigen Datenschutzbestimmungen zwingend zu gewährleisten sind. Die Richtlinien sehen eine Vernichtung neu eingetroffener Proben binnen drei Monaten vor. Beabsichtigt sei zudem eine schriftliche Vereinbarung mit dem Hamburger Labor gemäß § 9 BremDSG bis zum Beginn des Jahres 2006. Gegenwärtig werden Proben, die länger als fünf Jahre

in Hamburg gelagert wurden, vernichtet. In der Ausschusssitzung am 15. Februar 2006 berichtete der Ressortvertreter, der Vertrag über die Datenverarbeitung habe noch nicht abgeschlossen werden können, dies werde aber bis zum 31. März 2006 nachgeholt.

Der Ausschuss nimmt die Mitteilung des Senators für Arbeit, Frauen, Gesundheit, Jugend und Soziales zur Kenntnis.

Einführung der elektronischen Arbeitszeiterfassung (Ziffer 1.2): Der Landesbeauftragte berichtete dem Ausschuss ergänzend zum Jahresbericht, dass zwischenzeitlich im Rahmen der Einführung der elektronischen Arbeitszeiterfassung in einigen Dienststellen erhebliche Datenschutzmängel im EDV-gestützten Erfassungssystem festgestellt worden seien, die teilweise zum Aussetzen der Anwendung führten. Insbesondere konnte auf Ports an den Arbeitszeiterfassungsgeräten zugegriffen sowie Namen und Passwörter von Nutzern und Administratoren in Erfahrung gebracht werden. Auch die Manipulation der mit dem Gerät erfassten Daten war möglich. Darüber hinaus war entgegen der zwischen Gesamtpersonalrat und Senator für Finanzen abgeschlossenen Dienstvereinbarung konfigurationsbedingt eine Fernadministration möglich.

Nach Mitteilung des Senators für Finanzen ist das zuständige Unternehmen mit der Umsetzung der Vorgaben des Landesbeauftragten beauftragt. Die Arbeiten sollten noch im Laufe des Monats November 2005 abgeschlossen werden. Eine Ausnahme bilde die Möglichkeit des Zugriffs auf einzelne Ports. Für diese Problematik sei erst kürzlich von der BreKom eine Lösungsmöglichkeit vorgeschlagen worden. Die dafür erforderliche Hardware könne innerhalb einer Woche beschafft werden, und er gehe davon aus, dass ein unberechtigter Zugriff auf die Ports bis zum Ende des Jahres 2005 verhindert werden könne.

Der Ausschuss nimmt zur Kenntnis, dass die aufgetretenen datenschutzrechtlichen Probleme bis zum Ende des Jahres 2005 gelöst werden sollten.

Steuerzahler in der informationellen Zwangsjacke (Ziffer 1.9) und Steuerehrlichkeit – aber mit Datenschutz (Ziffer 12.1): Das Gesetz zur Förderung der Steuerehrlichkeit, nach dem Kontoabrufmöglichkeiten vorgesehen sind, verpflichtet die Kreditwirtschaft, Informationen über alle vorhandenen Konten in einem zentralen System vorzuhalten. Bei Anfragen der Finanzbehörden kann unter Eingabe des Namens und des Geburtsdatums eines Betreffenden in Deutschland geführte Konten dieser Person abgefragt werden, womit ein Überwachungsinstrument zur Kontrolle der Steuerehrlichkeit geschaffen wurde.

Aus datenschutzrechtlicher Sicht wurde das Verfahren nicht hinreichend deutlich im Gesetz beschrieben. Zur Frage, ob die Steuerbehörden im Auftrag anderer Behörden – zum Beispiel: Sozialbehörden – Daten abrufen und die Ergebnisse dann an diese weitergeben könnten, ist derzeit ein Verfahren vor dem Bundesverfassungsgericht anhängig. Die im Rahmen des einstweiligen Verfahrens erteilten Auflagen wurden vom Bundesfinanzministerium mittlerweile in einem Erlass umgesetzt. Insbesondere die Beteiligung von Drittbehörden ist weiter verfassungsrechtlich streitig. Die Entscheidung des Bundesverfassungsgerichtes in der Hauptsache wird im Jahr 2006 erwartet.

Die vom Ausschuss an den Senator für Finanzen gerichteten Fragen wurden nach Bekunden des Landesbeauftragten für den Datenschutz ausreichend beantwortet. Der vom Senator für Finanzen herausgegebene Erlass gewährleistet, dass von dem in schriftlicher Form abzuarbeitenden Verfahren nur in dringenden und wirklich eklatanten Fällen Gebrauch gemacht werden soll. Die vorgelegten Zahlen zeigten, dass dieser Maßgabe auch Rechnung getragen werde. Insbesondere sei festgestellt worden, dass kein Abruf von dritten Stellen über dieses System erfolgt sei, so dass dieser bemängelte Punkt bisher in der Praxis noch nicht zum Tragen gekommen sei.

Der Ausschuss nimmt Kenntnis.

Erlaubnis erweiterter Datenbeschaffung durch die GEZ (Ziffer 2.2): Der Rechtsausschuss beschäftigte sich mit der Problematik in seinen Sitzungen am 2. November, 7. Dezember 2005 und 15. Februar 2006.

Aufgrund der Änderungen im Rundfunkgebührenstaatsvertrag (RGbStV) wird der GEZ unter anderem die Beschaffung von Adressen bei kommerziellen Adresshändlern ermöglicht. Nach Auskunft der Senatskanzlei wurde die Möglichkeit der Be-

schaffung von Adressen bei kommerziellen Adresshändlern durch die GEZ im RGbStV rechtlich geregelt, weil in einigen Ländern das Fehlen einer ausdrücklichen gesetzlichen Ermächtigung von den Datenschutzbeauftragten gerügt wurde. Mit der Regelung sollte Rechtssicherheit und Gleichbehandlung aller Landesrundfunkanstalten gewährleistet werden.

Des Weiteren stoßen die Vorschriften zur Gebührenbefreiung gemäß § 6 RGbStV auf datenschutzrechtliche Bedenken. Aus den bei der Antragstellung im Original oder in beglaubigter Abschrift vorzulegenden Bescheiden der Sozialleistungsträger insbesondere beim ALG II sind eine Vielzahl von Daten ersichtlich, die für das Gebührenbefreiungsverfahren bei der GEZ irrelevant sind, dort aber gleichwohl eingescannt und vorgehalten würden.

Der Landesbeauftragte für den Datenschutz rügte das vorgeschriebene Verfahren und dass er vor der durch die Ministerpräsidenten erfolgten Beschlussfassung zum 8. Rundfunkänderungsstaatsvertrag von der Senatskanzlei nicht wie im BremDSG vorgesehenen beteiligt wurde. Er zeigte auch kein Verständnis dafür, dass die Sozialleistungsempfänger in Zeiten von eGovernment noch mit einem derartigen Verfahren belastet würden. Die Senatskanzlei sagte in der Ausschusssitzung zu, ihn im Rahmen der Beratungen zum 9. Rundfunkänderungsstaatsvertrag frühzeitig zu beteiligen.

Die Vorlage von Originalen oder beglaubigten Kopien wird von der GEZ aus Gründen der Fälschungssicherheit verlangt. Die nunmehr in der Praxis deutlich gewordenen Schwierigkeiten im Umgang mit den teilweise sehr umfangreichen Bescheiden waren wiederholt Beratungsgegenstand mit den beteiligten Stellen. So wird die Erstellung von Annexbescheiden, die lediglich die Bestätigung des Vorliegens der Voraussetzungen zur Gebührenbefreiung enthalten, in Bremen vom Studentenwerk, Versorgungsamt und vom Amt für Soziale Dienste zwischenzeitlich sichergestellt. Die Agenturen für Arbeit sehen sich zur Erstellung von Annexbescheiden gegenwärtig nicht in der Lage, so dass die Problematik für ALG-II-Bezieher, die mehr als 60 Prozent der Betroffenen ausmachten, nicht gelöst ist.

Nach Auskunft des Vertreters der BAgIS wird ein bundesweit einheitliches Programm eingesetzt, das von Bremen aus nicht isoliert verändert werden könne. Die BAgIS in Bremen betreue gegenwärtig rund 41.000 Bedarfsgemeinschaften mit Anspruch auf Gebührenbefreiung, so dass bei einer vom Gesetz vorgegebenen maximalen Bewilligungsdauer von sechs Monaten ein erheblicher Verwaltungsaufwand entstehen würde. Bei 200 Sprechtagen pro Jahr werden täglich 410 Anträge in der BAgIS bearbeitet. Der Vertreter der BAgIS unterbreitete folgenden Lösungsweg: Die BAgIS stempelt den Antrag auf Befreiung von der Rundfunkgebührenpflicht mit dem Hinweis ab, der Originalbescheid habe vorgelegen.

Der Datenschutzbeauftragte von Radio Bremen stimmte der Lösung unter dem Vorbehalt zu, dass die Bescheinigung damit die Qualität eines zweiten Originalbescheides erhalte. Auch der Landesbeauftragte erklärte sich mit dem Vorschlag einverstanden.

Die zwischenzeitlich von der GEZ erneut erhobenen Einwände gegen die zuvor dargestellte Lösung bedürfen einer weiteren Klärung zwischen den beteiligten Institutionen.

Der Ausschuss begrüßt, dass die Beteiligten an einer allen Seiten gerecht werdenden Lösung arbeiten.

Antrag

Die Bürgerschaft (Landtag) möge beschließen:

Die Bürgerschaft (Landtag) tritt den Bemerkungen des Rechtsausschusses bei.

7.2 Weitere Themen der Beratungen im Rechtsausschuss

Über die in Ziff. 7.1 dargestellten Ergebnisse hinaus hat sich der für den Datenschutz zuständige Parlamentsausschuss u. a. auch mit nachfolgenden Themen beschäftigt:

— Einführung der elektronischen Gesundheitskarte,

— Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006,

— gravierende Datenschutzmängel bei Hartz IV,

— Entwicklung der datenschutz nord GmbH,

— Vertragsverletzungsverfahren wegen Nichtumsetzung der EU-Datenschutzrichtlinie,

— Dateneinträge im Kraftfahrzeugbrief,

— Elektronisches behördliches Telefonbuch (ETB),

— Veröffentlichung von Insolvenzbekanntmachungen im Internet.

7.3 Einsicht in Unterlagen des Petitionsausschusses

Ein Bürger wandte sich an mich und fragte, ob er einen Anspruch auf Einsicht in die Akten des Petitionsausschusses der Bremischen Bürgerschaft nach Beendigung eines ihn betreffenden Petitionsverfahrens mit dienstrechtlichem Hintergrund habe. Ich habe auf meine fehlende Zuständigkeit hingewiesen, da es sich bei der Arbeit des Petitionsausschusses um eine parlamentarische Aufgabe handelt, die nicht den Bestimmungen des Bremischen Datenschutzgesetzes (BremDSG) unterfällt. Ich habe ihn aber darauf hingewiesen, dass die Datenschutzordnung der Bremischen Bürgerschaft vorsieht, dass Betroffenen auf Antrag Auskunft über die zu ihrer Person gespeicherten Daten zu erteilen ist.

8. Personalwesen

8.1 Technische Mängel bei der Arbeitszeiterfassung (AZE)

Im Laufe des Berichtsjahres habe ich das Verfahren zur elektronischen Arbeitzeiterfassung (AZE) einer technischen Datenschutzprüfung unterzogen. Die Datenschutzprüfung habe ich exemplarisch an mehreren AZE-Terminals beim Senator für Bau, Umwelt und Verkehr (SBUV) und dem in meiner Dienststelle neu installierten System durchgeführt. Dabei habe ich gravierende Mängel festgestellt.

So konnte ich mit einem PC, der mit dem AZE-Terminal vernetzt war, unter Ausnutzung allgemein bekannter, vom Betreiber ignorierter und daher nicht geschlossener Sicherheitslücken problemlos umfangreiche wichtige technische Informationen ermitteln: offene Ports und somit die dahinterliegenden Netzwerkdienste, eine vollständige Liste der freigegebenen Ressourcen der Terminals, wie z. B. Laufwerkfreigaben und auf den Terminals existierenden Benutzergruppen und den ihnen zugeordneten Benutzerkonten. Dazu habe ich keinerlei Zugriffsberechtigung auf das entsprechende Terminal benötigt. An einigen Terminals waren zudem offene physikalische Schnittstellen zu finden. Hier hätten beliebige Externe eine Tastatur an die Terminals anschließen können.

Für potenzielle Hackerangriffe interessant sind immer Benutzerkonten, die der Gruppe „Administratoren“ angehören. Von diesen waren jeweils zwei auf den Terminals zugänglich. Weiterhin konnte ich noch ein Benutzerkonto mit gegenüber den Administratorenkonten eingeschränkten Zugriffsberechtigungen ermitteln. Es gelang, die Passwörter zu den Benutzerkonten zu erraten. Alarmierendes Ergebnis: Das Passwort zu allen ermittelten Benutzerkonten entsprach genau dem jeweiligen Namen des Benutzerkontos! Die Anmeldung als Administrator hätte es daraufhin jedem erlaubt, das komplette System vollständig unter seine Hoheit zu nehmen und z. B. die Konfiguration der Maschine so zu verändern, dass eine Nutzung des Geräts nicht mehr möglich gewesen wäre. Damit hätten auch die Datenbanken, in denen die zur AZE gehörenden Personaldaten der Dienststelle gespeichert und verarbeitet werden, komplett vom Terminal herunterkopiert werden können. Danach wären Offline-Veränderungen der Datenbestände und das Rückspielen falscher Daten möglich geworden. Auf das Kopieren der Datenbanken und deren datenschutzrechtliche Analyse habe ich bei meiner Prüfung verzichtet.

Ich konnte zunächst nicht glauben, dass solche Fehler aus dem kleinen Einmaleins der Datensicherheit gemacht wurden. Nachdem ich die festgestellten Mängel aber bei mehreren der von mir überprüften AZE-Terminals feststellen konnte, war offensichtlich, dass das Konfigurationsproblem bei allen angeschlossenen AZE-Terminals vorhanden war.

Die gefundenen Mängel stellen gravierende Verstöße gegen die in § 7 des Bremischen Datenschutzgesetzes (BremDSG) geforderten Maßnahmen dar, insbesondere sind Zugangskontrolle (BremDSG § 7 Abs. 4 Nr. 2), Zugriffskontrolle (BremDSG

§ 7 Abs. 4 Nr. 3), Eingabekontrolle (BremDSG § 7 Abs. 4 Nr. 5) ebenso wie die Verfügbarkeitskontrolle (BremDSG § 7 Abs. 4 Nr. 7) nicht gewährleistet. Auch stellen die Mängel Verstöße gegen das Datenschutz- und Datensicherungskonzept für die elektronische Arbeitszeiterfassung dar. So hätte mittels der nicht geschlossenen Sicherheitslücken eine Fernwartung mit der Möglichkeit, heimlich auf einzelne Arbeitszeitkonten zu schauen, problemlos durchgeführt werden können, was nach dem Datenschutzkonzept aber nicht zulässig ist.

Ich habe dem Senator für Finanzen (SfF) meinen Prüfbericht zugesandt und ihn aufgefordert, die eklatanten und elementaren Mängel umgehend zu beseitigen. Einige Dienststellen haben daraufhin die elektronische Arbeitszeiterfassung ausgesetzt.

In Abstimmung mit mir wurden die Einstellungen grundlegend verändert und die Sicherheitslücken geschlossen. Mit der Anpassung der sich in Betrieb befindlichen AZE-Terminals wurde begonnen. Die Umstellung aller Dienststellen wird nach Einschätzung des SfF im ersten Quartal 2006 abgeschlossen sein. Ich werde das überwachen.

8.2 Falsche Behandlung von Bewerbungsunterlagen

Im Rahmen einer Bewerbung (Geschäftsführer der Bremer Toto und Lotto GmbH) hatte ein abgewiesener Bewerber die Unterlagen eines anderen Bewerbers vom Innenressort erhalten.

Auf meine Nachfrage hat Herr Bürgermeister Röwekamp in seiner Funktion als Vorsitzender des Aufsichtsrats diesen Sachverhalt bestätigt und bedauert, dass es trotz arbeitsteiliger Organisation und Endkontrolle zu diesem Fehler kommen konnte.

In einem anderen Fall hat der Personalverantwortliche der Industrie- und Handelskammer (IHK) Bremerhaven, der gleichzeitig behördlicher Datenschutzbeauftragter war, Namen und Adressen von Bewerbern zu Werbezwecken ohne deren Einwilligung an die Barmer Ersatzkasse weitergegeben.

Der Hauptgeschäftsführer hat auf meine mehrfachen Nachfragen erklärt, die unzulässigerweise übermittelten Daten seien bei der Krankenkasse vollständig gelöscht worden. Außerdem sei ein anderer zum behördlichen Datenschutzbeauftragten bei der IHK neu bestellt worden.

9. Inneres

9.1 Neues Gesetz über den Verfassungsschutz im Lande Bremen

Nachdem die in den Jahren 2000, 2002 und 2004 vorgesehenen Änderungen des Bremischen Verfassungsschutzgesetzes scheinbar politisch nicht durchsetzbar waren – ich habe jeweils im 25. Jahresbericht und 27. Jahresbericht über meine datenschutzrechtlichen Bedenken berichtet – hat nunmehr das Innenressort einen neuen Anlauf genommen. Grundlage ist die im Koalitionsvertrag getroffene Vereinbarung, die Zusammenarbeit mit dem niedersächsischen Landesamt für Verfassungsschutz zu intensivieren. Obwohl die damit verbundenen Pläne einer Zusammenlegung der Verfassungsschutzämter von Bremen und Niedersachsen nach bisherigem Kenntnisstand nicht mehr weiter verfolgt werden, soll scheinbar an einer Angleichung der Verfassungsschutzgesetze der beiden Länder festgehalten werden.

Für mich ist eine Angleichung kein eigener Wert: Unterschiedliche Länder – unterschiedliche politische Auffassungen von den Aufgaben und Schwerpunkten einer Verfassungsschutzbehörde. Bremen war das erste Land unter den Bundesländern mit datenschutzrechtlichen Regelungen für den Verfassungsschutz. Alle anderen Länder sind nach und nach gefolgt. Eine solche Vorbildrolle sollte Bremen weiter behalten. Auch die Zusammenarbeit der Verfassungsschutzämter von Bremen und Niedersachsen würde durch eine einheitliche Regelung nicht verbessert, denn die Zusammenarbeit unter den Verfassungschutzämtern des Bundes und der Länder ist einheitlich durch Bundesgesetz verpflichtend geregelt. Daraus ergibt sich somit kein Änderungsbedarf.

Im Juli 2005 übersandte mir der Senator für Inneres und Sport einen neuen Entwurf eines Gesetzes über den Verfassungsschutz im Lande Bremen mit Änderungen. Die von mir im vergangenen Berichtsjahr abgegebene Stellungnahme (vgl.

27. JB, Ziff. 6.10) hatte zu mehreren Veränderungen des Entwurfs geführt. Meine verbliebenen, zum Teil gravierenden datenschutzrechtlichen Bedenken führten lediglich zu geringen Änderungen des Entwurfs, bevor im November 2005 der Senat mit dem Gesetzentwurf befasst wurde.

Zum Schutz des Kernbereichs privater Lebensgestaltung bei der Wohnraumüberwachung: Der Gesetzentwurf setzt die Vorgaben des Bundesverfassungsgerichts aus seiner Entscheidung vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 19084/99) nicht vollständig um. Die Wohnraumüberwachung wird bei der Wohnung des Verdächtigen nicht auf ihn beschränkt, so dass andere Personen, die sich dort allein aufhalten, entgegen der Ansicht des Bundesverfassungsgerichts überwacht werden können. Auch können Wohnungen Dritter bereits überwacht werden, wenn die verdächtige Person sich darin aufhält, während das Bundesverfassungsgericht zusätzlich tatsächliche Anhaltspunkte verlangt hat, dass dadurch verfahrensrelevante und verwertbare Gespräche erlangt werden.

Ferner wird die Übermittlung der bei der Wohnraumüberwachung anfallenden Daten an die Strafverfolgungsbehörden in Fällen erlaubt, in denen diese die Daten nicht selbst hätten erheben können. Dies stellt nach der Rechtsprechung des Bundesverfassungsgerichts eine unzulässige Zweckänderung dar.

Schließlich soll die Wohnraumüberwachung nach dem Gesetzentwurf solange und soweit stattfinden, wie neben die Vermutung, dass dort höchstpersönliche Gespräche geführt werden, die Vermutung gesetzt werden kann, dass auch über nicht schutzwürdige strafrechtlich relevante Sachverhalte gesprochen wird. Da ein „großer Lauschangriff“ nur in Betracht gezogen werden darf, wenn vermutet wird, dadurch für die Verhinderung und Aufklärung von Straftaten wichtige Informationen zu erlangen, läuft die Formulierung darauf hinaus, dass die akustische Wohnraumüberwachung immer, d. h., unabhängig von der Art der Räume und der anwesenden Personen, angeordnet wird. Das Bundesverfassungsgericht hat dagegen ein Erhebungs- und Überwachungsverbot gefordert, wenn eine Vorabprognose nach Art der Räume und anwesenden Personen die Vermutung nahe legt, dass das Abhören zu einer Verletzung des Kernbereichs privater Lebensgestaltung führen wird.

Zur Hilfestellung bei der Verwendung von Tarnmitteln: Der Entwurf sieht für alle öffentlichen Stellen die Verpflichtung vor, dem Landesamt für Verfassungsschutz bei der Bereitstellung von Tarnmitteln Unterstützung zu leisten. Aufgrund meiner im vergangenen Berichtsjahr dargestellten Bedenken (vgl. 27. JB, Ziff. 6.10) wurde bedauerlicherweise nur in der amtlichen Begründung festgehalten, dass die Hilfeleistungspflicht lediglich die allgemeine Pflicht zur Amtshilfe ergänzt und bei einer Kollision mit den Aufgaben der verpflichteten Behörde oder Stelle ein Ausgleich gesucht wird. Es wurde ferner in der amtlichen Begründung klargestellt, dass hiermit keine Erweiterung der Kompetenzen des Landesamtes für Verfassungsschutz verbunden ist. Ob diese rechtstheoretischen Ausführungen in der Praxis tragen, erscheint fraglich.

Zu den datenschutzrechtlichen Bestimmungen im Entwurf: Der Gesetzentwurf sieht weiterhin trotz meiner wiederholten Hinweise in einigen Bereichen eigene bereichsspezifische datenschutzrechtliche Bestimmungen vor, obwohl diese bereits ausreichend im Bremischen Datenschutzgesetz (BremDSG) geregelt sind. Betroffen sind der Auskunftsanspruch sowie die Regelungen zur Berichtigung, Löschung und Sperrung personenbezogener Daten.

Zu den Minderjährigenregelungen: Der Entwurf sieht im Anschluss an meine im vergangenen Berichtsjahr geäußerten Bedenken (vgl. 27. JB, Ziff. 6.10) weiterhin eine Regelung zur Speicherung von Daten Minderjähriger vor. Diese weicht von der Regelung des Bundesverfassungsschutzgesetzes insoweit ab, als auch Informationen über verfassungsfeindliche Bestrebungen oder Tätigkeiten vor der Volljährigkeit des Betroffenen die Löschung der über ihn gespeicherten personenbezogenen Daten verhindern können. Der Gesetzentwurf schließt ebenso nur die Übermittlung personenbezogener Daten Minderjähriger vor Vollendung des 14. Lebensjahres an ausländische oder an über- oder zwischenstaatliche Einrichtungen aus, während das Bundesverfassungsschutzgesetz dies für alle Informationen vor Vollendung des 16. Lebensjahres vorsieht. Der Gesetzentwurf erlaubt also abweichend vom Bundesverfassungsschutzgesetz die Übermittlung personenbezogener Daten für das 14. und 15. Lebensjahr. Noch in der Pubertät befindliche Jugendliche können so irreversibel gebrandmarkt werden.

Zur Veröffentlichung von personenbezogenen Daten durch den Verfassungsschutz: Der Gesetzentwurf sieht für Zwecke der Öffentlichkeitsaufklärung, anders als das Bundesverfassungsschutzgesetz, die Veröffentlichung von personenbezogenen Daten durch den Verfassungsschutz vor. Dies kann dazu führen, dass Betroffene gänzlich namentlich im jährlichen Verfassungsschutzbericht genannt werden. Aus datenschutzrechtlicher Sicht bleibt problematisch, dass vor der Veröffentlichung keine Benachrichtigung des Betroffenen vorgesehen ist, die ihn vor Überraschungen schützt oder in die Lage versetzt, auf Irrtümer und Fehler hinzuweisen (vgl. auch 27. JB, Ziff. 6.10).

Zum Schutz von Amts- und Berufsgeheimnis: Der Schutz durch ein Zeugnisverweigerungsrecht geschützter Personen ist aus datenschutzrechtlicher Sicht nicht vollständig. So ist die Informationsbeschaffung nur für bestimmte nachrichtendienstliche Mittel ausgeschlossen, im Übrigen aber im Umkehrschluss zulässig (vgl. § 8 Abs. 3).

9.2 Prüfung beim Landesamt für Verfassungsschutz

Im Berichtsjahr habe ich eine Prüfung beim Landesamt für Verfassungsschutz (LfV) vorgenommen. Schwerpunkte und Ergebnisse dieser Prüfung werden nachfolgend zusammengestellt:

Zum Abruf der Meldedaten: Seit 2002 ist das LfV durch eine entsprechende Änderung in der Meldedatenübermittlungsverordnung befugt, bestimmte Meldedaten aus dem Melderegister abzurufen. § 30 Abs. 3 des bremischen Meldegesetzes bestimmt, dass die Abrufe zu protokollieren und die Aufzeichnungen bis zum Ende des nächsten Jahres, das dem Abruf folgt, aufzubewahren sind. Eine vergleichbare Vorschrift findet sich auch in § 6 Abs. 3 des Bremischen Verfassungsschutzgesetzes. Bei der Prüfung wurde festgestellt, dass die Abrufe zwar festgehalten werden, aber die gesetzliche Frist nicht eingehalten wurde, da die Aufzeichnungen bereits nach einem Monat vernichtet wurden. Es konnten jedenfalls keine weiteren Protokollbögen vorgelegt werden. Durch dieses Vorgehen war es mir nicht möglich, zurückliegende Abrufe zu kontrollieren. Das habe ich beanstandet. Bei der Gelegenheit habe ich das LfV darauf hingewiesen, dass im Rahmen der Neukonzeption des Melderegisterverfahrens (MESO) auch die Protokollierung durch das LfV rechtskonform gestaltet und dafür gesorgt werden muss, dass die Aufzeichnungen, wie in § 30 Abs. 3 des bremischen Meldegesetzes vorgeschrieben, von der abrufenden Stelle vorgenommen werden.

Zu den Zuverlässigkeitsüberprüfungen nach dem Luftsicherheitsgesetz und nach dem Hafensicherheitsgesetz: Zu dem Prüfungszeitpunkt lagen beim LfV keine unerledigten Überprüfungsfälle vor. Auch eine Liste, die der Senator für Wirtschaft und Häfen (SfWuH) mir übersandt hatte, war bereits abgearbeitet. Deshalb konnten nur theoretische Fälle „durchgespielt“ werden (vgl. auch 26. JB, Ziff. 12). Die Überprüfungsfälle werden vom SfWuH über eine sichere E-Mail-Verbindung an das LfV übermittelt und ohne Medienbruch an das Bundesamt für Verfassungsschutz (BfV) zur Prüfung (automatisches Rasterverfahren) weitergeleitet. Das LfV erhält nach wenigen Tagen eine Liste über Negativ- bzw. Positivtreffer. Die „Negativfälle“ werden umgehend freigegeben und die „Positivfälle“ werden eingehend geprüft und bewertet. Anschließend wird der SfWuH im herkömmlichen Verfahren unterrichtet. Eine solche Handhabung ist nicht zu kritisieren.

Zu Datenschutzkonzept und Verfahrensbeschreibung: Für die Hauptanwendungen (z. B. NADIS) und die technische Struktur der DV konnten ausreichende Unterlagen und Festlegungen vorgelegt werden. Allerdings bedarf es hinsichtlich der Sicherheit (fehlende Firewall) gegenüber dem Bremischen Verwaltungsnetz (BVN) Nachbesserungen, die zurzeit vom LfV noch aufgearbeitet werden.

9.3 Änderung des Bremischen Polizeigesetzes

Im Berichtsjahr wurde mir ein neuer Entwurf zur Änderung des Bremischen Polizeigesetzes (BremPolG) zur Stellungnahme übersandt. Meine datenschutzrechtlichen und verfassungsrechtlichen Bedenken im Hinblick auf die Entscheidung des Bundesverfassungsgerichts vom 27. Juli 2005 zur Verfassungswidrigkeit des Niedersächsischen Sicherheits- und Ordnungsgesetzes führten zu verschiedenen Änderungen des Entwurfs, konnten aber in einigen wesentlichen Punkten nicht ausgeräumt wurden:

Zu der überarbeiteten Regelung des Lauschangriffs: Das geltende Bremische Polizeigesetz enthielt Regelungen zur Wohnraumüberwachung, die nach der Rechtsprechung des Bundesverfassungsgerichts vom 3. März 2004 (1 BvR 2378/98 und 1 BvR 19084/99) verfassungswidrig waren. Ich hatte mich mit dem Senator für Inneres und Sport darauf verständigt, dass die verfassungswidrigen Regelungen bis zu einer Neuregelung von der Polizei Bremen nicht angewendet würden. Auch die jetzt vorgeschlagenen Regelungen entsprechen leider nicht in vollem Umfang den vom Verfassungsgericht vorgegebenen Maßgaben.

So hat die Wohnraumüberwachung von vornherein zu unterbleiben, wenn Anhaltspunkte dafür bestehen, dass die Überwachung zu einer Verletzung des Kernbereichs privater Lebensgestaltung führen wird. Ergeben sich Anhaltspunkte dafür, dass Äußerungen erfasst werden, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, so ist die Überwachung unverzüglich abzubrechen. Beides sieht der Gesetzentwurf nicht vor. Darüber hinaus nimmt der Gesetzentwurf Gespräche über Straftaten pauschal vom Kernbereich der privaten Lebensgestaltung aus. Das Bundesverfassungsgericht hingegen hat differenziert: Nicht jedwede Verknüpfung zwischen der Äußerung und dem Verdacht einer Straftat genügt. Auch der Erste Strafsenat des Bundesgerichtshofs hat in einem Urteil vom 10. August 2005 (1 StR 140/05) noch einmal bekräftigt, dass ein Selbstgespräch im Krankenzimmer in den absolut geschützten Kernbereich privater Lebensgestaltung fällt und auch bei überwiegendem allgemeinen Interesse nicht abgehört werden darf.

Bedenklich ist, dass die Gesetzesbegründung die Übertragung der vom Bundesverfassungsgericht aufgestellten Grundsätze zur repressiven Wohnraumüberwachung auf die präventive Wohnraumüberwachung verneint, da hier Zweck der Maßnahme der Schutz einer Person vor Gefahren für Leib, Leben oder Freiheit sei. Soweit ein Verursacher insoweit in Rechte Dritter eingreife, könne er keinen unantastbaren Kernbereich privater Lebensgestaltung beanspruchen. Der Schutz des unantastbaren Kernbereichs privater Lebensgestaltung unterscheidet jedoch nicht zwischen präventiven oder repressiven Maßnahmen der Wohnraumüberwachung. Der Schutz gilt gleichermaßen, wie das Bundesverfassungsgericht auch in seinem Urteil vom 27. Juli 2005 (1 BvR 668/04) deutlich gemacht hat.

Zur Ausweitung der Identitätsfeststellung: Der Entwurf erlaubt die Identitätsfeststellung an von der Polizei festgelegten „Gefahrenorten“, wenn eine Person diesen Ort betritt oder überquert. Bislang war erforderlich, dass die Person sich vor Ort aufhält, d. h. verweilt. Durch die Ausweitung des Anwendungsbereichs werden eine Vielzahl von Personen der Möglichkeit einer Identitätsfeststellung unterworfen, die in ihr Recht auf informationelle Selbstbestimmung eingreift. Für den Bürger ist die polizeiliche Festlegung als „Gefahrenort“ nicht erkennbar. Es ist für ihn nicht überprüfbar, ob die Polizei die Befugnis zur Identitätsfeststellung besitzt. Zur Identitätsfeststellung ist die Polizei zudem zu weiteren Maßnahmen ermächtigt. Sie darf u. a. die Person festhalten und mitgeführte Sachen nach Gegenständen durchsuchen, die der Identitätsfeststellung dienen, sowie sich mitgeführte Ausweispapiere aushändigen lassen oder die Person für erkennungsdienstliche Maßnahmen zur Dienststelle bringen.

Zur Ausweitung von Befragung und Auskunftspflichten: Durch den Gesetzentwurf wird die Befugnis der Polizei eingeführt, zur Verhütung von Straftaten von erheblicher Bedeutung in organisierter Begehungsform auch außerhalb von „Gefahrenorten“ oder Kontrollstellen Personen anzuhalten, zu befragen, mitgeführte Ausweispapiere zu prüfen und Sachen in Augenschein zu nehmen, ohne dass auf die betroffene Person bezogene Anhaltspunkte für die Begehung der Straftat vorliegen müssen. Auch hier geraten viele harmlose Personen in das Visier der Polizei, die Eingriffe in ihr Persönlichkeitsrecht hinnehmen müssen.

Zur Ausweitung von Kontrollstellen: Die Errichtung von Kontrollstellen, die eine Identitätsfeststellung erlauben, wird in dem Gesetzentwurf erheblich erweitert. Kontrollstellen dürfen bei Straftaten von erheblicher Bedeutung errichtet werden. Hierunter fallen alle Verbrechen nach dem Strafgesetzbuch, aber auch eine Reihe von Vergehen. An den Kontrollstellen werden eine Vielzahl von Personen erfasst, die mit der Straftatbegehung in keinerlei Zusammenhang stehen. Datenschutzrechtlich ist problematisch, dass die dabei erhobenen Daten erst spätestens nach einem Monat gelöscht werden sollen und nicht in jedem Fall unverzüglich, wenn keine Anhaltspunkte für die Beteiligung an einer Straftat vorliegen. Die personenbezogenen Daten sollen nach dem Gesetzentwurf zudem auch zur Verfolgung einer nicht

nur geringfügigen Ordnungswidrigkeit genutzt werden. Da eine Kontrollstelle zur Verfolgung von Ordnungswidrigkeiten nicht errichtet werden darf, bestehen Zweifel, ob die erhobenen personenbezogenen Daten nicht über den Zweck hinaus verarbeitet werden, für den sie erhoben werden durften. Das Bundesverfassungsgericht hat festgehalten, dass die Weiterverwendung von Daten nur für Zwecke verfassungsmäßig ist, die auch als Rechtfertigung für die ursprüngliche Erhebung ausgereicht hätten.

Zur Videoaufzeichnung für die Eigensicherung: Der Gesetzentwurf sieht vor, dass Polizeibeamte zu ihrer Eigensicherung bei Verkehrskontrollen offen Bildaufzeichnungen anfertigen dürfen. Ich habe erreicht, dass die Aufzeichnungen nur zur Verfolgung von Straftaten gegen die Polizeibeamten, nicht auch Ordnungswidrigkeiten, verwendet werden dürfen und ansonsten unverzüglich zu löschen sind.

Zum elektronischen Kfz-Kennzeichenabgleich: Der Gesetzentwurf erlaubt der Polizei, bei Verkehrskontrollen Kfz-Kennzeichen elektronisch zu erfassen und mit dem Fahndungsdatenbestand der Polizei abzugleichen. Aufgrund meiner Intervention darf der Abgleich nur sofort erfolgen. Die Kfz-Kennzeichen aller vorbeifahrenden Fahrzeuge dürfen nicht auf Vorrat gespeichert werden.

9.4 Fotos der Polizei in der „Galerie des Verbrechens“

Im November 2004 veröffentlichte eine Boulevardzeitung in Bremen unter der Überschrift „Die Galerie des Verbrechens“ Name und Täter- bzw. Tatverdächtigenbilder, die identisch mit Bildern waren, die im Rahmen erkennungsdienstlicher Maßnahmen durch die Polizei angefertigt worden waren. Die wiedergegebenen Zahlen über Straftaten entsprachen in weiten Teilen kriminalpolizeilichen Unterlagen, die in ExtraPol abrufbar waren. Bei der prangerartigen Veröffentlichung handelt es sich um einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen. Meine auch von Seiten des behördlichen Beauftragten für den Datenschutz der Polizei Bremen unterstützten Nachforschungen, wer für die Indiskretionen verantwortlich ist, waren leider nicht erfolgreich. Die Bilder und zugehörigen personenbezogenen Daten waren auch in ExtraPol gespeichert. Daher konnte der potentielle Kreis der dafür in Frage kommenden Personen nicht eingegrenzt werden. ExtraPol ist eine gemeinsame von der Polizei im Bund und in den Ländern geführte Informationsplattform. Diese enthielt zunächst nur polizeiliche Fachinformationen (Dienstvorschriften, Fachdokumente), nahm jedoch im Jahr 2004 in einem weiteren Schritt auch fallbezogene Fahndungsdaten auf. Aus Sicht des Datenschutzes ist kritisch zu beurteilen, dass ExtraPol keine Zugriffsprotokollierung vorsieht oder in anderer Weise Downloads oder das Ausdrucken von Daten verhindert. Die datenschutzrechtlich geforderte Verantwortung einer Stelle ist damit nicht gewährleistet. Konsequenterweise hat der Polizeipräsident daraufhin eine weitere Einspeicherung von personenbezogenen Daten durch die Polizei Bremen in ExtraPol vorerst gestoppt. Nunmehr besteht die bundesweite Planung, das ExtraPol-Verfahren insgesamt zu prüfen und den datenschutztechnischen Anforderungen anzupassen.

9.5 Errichtungsanordnungen und Verfahrensbeschreibungen

Im Berichtsjahr wurde ich mit einer Reihe von Verfahrensbeschreibungen für automatisierte Verfahren bei der Polizei Bremen konfrontiert, die bereits seit längerer Zeit erlassen worden waren oder sich umgekehrt noch in einem frühen Entwurfsstadium befanden. Darunter waren z. B. die Verfahrensbeschreibungen für die Datenbank „An- und Verkaufsgeschäfte“, die Arbeitsdatei „Vermögensabschöpfung“, die Arbeitsdatei „Fahndung“, das Lagebild „Jugendkriminalität“, die Datenbank „bekannte Täter“, die so genannte Gefährderdatei (Stalker) und die Datenbank „Handyraub“. Die Verfahrensbeschreibungen nahmen zum Teil Bezug auf überholte Rechtsvorschriften im Bremischen Datenschutzgesetz (BremDSG), Bremischen Polizeigesetz (BremPolG) oder Strafgesetzbuch (StGB). Die technischen und organisatorischen Maßnahmen nach § 7 BremDSG waren durchweg unzureichend dargestellt. Auch fehlte teilweise eine Rechtsgrundlage für den Umfang der zu speichernden Daten. Die Zugriffsberechtigten waren oft auch nicht hinreichend genau beschrieben. Ferner standen die Löschfristen nicht immer im Einklang mit den Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (so genannten KpS-Richtlinien). Alle diese Verfahrensbeschreibungen habe ich mit dem behördlichen Datenschutzbeauftragten und z. T. unter Hinzuziehung der zuständi-

gen Fachkräfte erörtert und um Nachbesserung gebeten. Eine erneute Vorlage ist für Anfang 2006 vorgesehen.

Auch auf Bundesebene wurde ich des Öfteren aufgefordert, zu den Errichtungs- und Feststellungsanordnungen neuer personenbezogener Sammlungen des Bundeskriminalamtes, die auch die Polizei im Land Bremen nutzen, gegenüber dem Senator für Inneres und Sport eine Stellungnahme abzugeben. Dies betraf z. B. die Errichtungsanordnungen APOK, Organisierte Kriminalität Osteuropa, Geldwäschedatei, Kinderporno, Dokumente/Menschenhandel/Schleusung, Falschgeld, Waffen, FBK Tötungs- und Sexualdelikte, KAN, Personenfahndung, Sachfahndung, Erkennungsdienst, Haftdatei und Gewalttäter Sport.

9.6 ApolWeb

Bei ApolWeb handelt es sich um eine Anwendung der Ortspolizeibehörde Bremerhaven (OPB), welche ursprünglich als Rückfallebene bei Systemausfällen konzipiert war. Mit diesem System werden einmal täglich Daten aus dem örtlichen Melderegister, dem örtlichen Fahrzeugregister und dem örtlichen Fahrerlaubnisregister in einem Datenbanksystem zusammengeführt und den Beamten zum Abruf im Intranet zur Verfügung gestellt. Der behördliche Datenschutzbeauftragte legte mir die Verfahrensbeschreibung vor. Schon bald wurde der OPB deutlich, dass die Anwendung aufgrund ihrer Bedienerfreundlichkeit erhebliche Vorzüge bietet und daher nicht nur als Rückfallsystem, sondern auch für den Normalbetrieb eingesetzt werden soll. Daraus ergeben sich allerdings einige rechtliche Probleme. So dürfen nur solche Daten eingestellt werden, deren Abruf rechtlich zulässig ist. In der Datenbank sind Datenfelder enthalten, die nach der Meldedatenübermittlungsverordnung (MeldDÜV) nicht hätten zum Abruf bereit gestellt werden dürfen. Grundsätzlich ist aufgrund der Aktualität der Daten immer auf die Originaldaten zuzugreifen und aus der Protokollierung muss klar hervorgehen, welche Personen auf welche Daten zugegriffen haben.

Der Datenschutzbeauftragte der Ortspolizeibehörde Bremerhaven teilte mir zwischenzeitlich mit, dass man an einer anderen technischen Lösung arbeite, bei der die Daten im Hoheitsbereich der Verwaltungspolizei verbleiben und meine Vorgaben zum Zugriff auf die Daten eingehalten werden. Ich werde die weitere Einführung beratend begleiten.

9.7 ISAWeb

Die Polizei Bremen hat sich entschlossen, das bestehende Verfahren ISA (InformationsSystemAnzeigen) auf eine neue technische Basis, nämlich webbasiert, umzustellen (vgl. 27. JB, Ziff. 6.7).

Meine datenschutzrechtlichen Anforderungen an das System habe ich der Polizei Bremen mitgeteilt. Dazu zählen unter anderem die Nachvollziehbarkeit der Datenverarbeitung, Gewährleistung der Zweckbindung, revisionssichere Protokollierung, Sicherstellung der Eindeutigkeit von Personendaten, Gewährleistung von Auskunfts- und Einsichtsrechten sowie die Festlegung der technischen- und organisatorischen Maßnahmen zum Schutz der Daten.

Im Januar 2005 wurde mir ein Prototyp der Anwendung vorgestellt. Dabei wurde mir dargelegt, an welchen Stellen das Programm inhaltlich durch neue Datenfelder ergänzt worden ist, um aus ISA (alt) bekannte Defizite auszugleichen. Ich habe keine grundsätzlichen Einwände geäußert. Weiterhin habe ich gefordert, dass die Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen (so genannte KpS-Richtlinien) zu aktualisieren sind. Die zurzeit gültigen Richtlinien aus dem Jahre 1981 sind veraltet und entsprechen z. B. beim Auskunftsrecht des Betroffenen oder den Aufbewahrungsfristen teilweise nicht mehr den Rechtsvorschriften.

Ich begrüße ausdrücklich, dass bei der Neugestaltung eine Schnittstelle zu der Anwendung der Staatsanwaltschaft Bremen geplant ist, die sicherstellt, dass der „Ausgang des Verfahrens“ zeitlich und rechtlich korrekt in das ISAWeb übernommen wird. Nur so können die Löschfristen exakt berechnet werden.

Im Frühjahr des Berichtsjahres habe ich um weitere Auskünfte gebeten, insbesondere um die Vorlage der Verfahrensbeschreibung mit Angabe der getroffenen technischen und organisatorischen Maßnahmen zum Schutz der Daten sowie eine Beschreibung vorhandener Schnittstellen, eine Darstellung des Zugangs- und Zugriffs-

verfahrens sowie die Ausarbeitung eines Rollenkonzepts, aus dem hervorgeht, in welcher Weise und in welchem Umfang Berechtigungen im ISAWeb vergeben werden.

Die Inbetriebnahme des Programms erfolgte im Juli, ohne dass mir bis dahin die Verfahrensbeschreibung und das Fachdatenschutzkonzept zugegangen sind. Nachdem ich diese Angaben auch bis zum Herbst nicht erhalten habe, wurde das Thema im November im Rechtsausschuss der Bremischen Bürgerschaft behandelt.

Zwischenzeitlich ist die Verfahrensbeschreibung zu ISAWeb eingegangen. Eine Stellungnahme zum rechtlichen Teil ist bereits erfolgt. Es fehlte die zur Bewertung notwendige Beschreibung der Datensatzstruktur, die von der Polizei Bremen noch nachgereicht werden muss. Eine Stellungnahme zu den technischen und organisatorischen Maßnahmen befindet sich in Arbeit. Insgesamt lässt sich bereits feststellen, dass weitere Angaben erforderlich sind, insbesondere zur Softwarearchitektur und den eingesetzten Produkten, zum Beantragungsverfahren für Berechtigungen und zum Berechtigungskonzept, zur Beschreibung der Schnittstellen sowie zur Zugriffskontrolle und Eingabekontrolle. Es wurden keine Aussagen zur Zutritts-, Weitergabe- und Verfügbarkeitskontrolle gemacht, die zu ergänzen sind. Ich erwarte, dass eine baldige Vervollständigung der Unterlagen durch die Polizei Bremen erfolgt.

9.8 Datenschutzkonzepte bei der Ortspolizeibehörde Bremerhaven

Die Ortspolizeibehörde Bremerhaven hat mir im Berichtsjahr mehrere Beschreibungen zu DV-Verfahren vorgelegt. Ingesamt musste ich feststellen, dass insbesondere Maßnahmen mit übergreifendem Charakter sowie die DV-Infrastruktur nicht ausreichend beschrieben waren. Ich habe daher zur weiteren Vorgehensweise den Vorschlag unterbreitet, alle Maßnahmen, die bezogen auf die Behörde für alle Verfahrensbeschreibungen auf technischer Ebene bei der Verwendung gleicher Sicherheitsmechanismen identisch sind, in einem „Allgemeinen Datenschutz- und Sicherheitskonzept“ zusammenzufassen. Die Erstellung dieses übergreifenden Konzeptes hat den Vorteil, dass bei Änderungen der DV-Technik (z. B. bei der Durchführung von Datensicherungen) der Anpassungsaufwand bzgl. der Dokumentation nur an einer Stelle entsteht. Hier erwarte ich insbesondere Aussagen zur Zugangskontrolle wie auch zur Verfügbarkeits- und Weitergabekontrolle (Netzinfrastruktur, Anbindung der Außenstellen).

Der Datenschutzbeauftragte der Ortspolizeibehörde Bremerhaven hat mir bis Ende Januar 2006 eine Darstellung der allgemeinen Datenschutz- und Sicherheitsmaßnahmen der Behörde in Aussicht gestellt.

Aufbauend auf diesem Konzept sollen dann in weiteren Fachdatenschutzkonzepten die Sicherheitsmechanismen dargestellt werden, die sich konkret auf die einzelnen Anwendungen und deren Implementierung beziehen. Zu ergänzen sind im Wesentlichen weitere Angaben zur Softwarearchitektur, zur Zugriffskontrolle (technischer Mechanismus zur Anmeldung und Steuerung der Zugriffe, Berechtigungskonzept, Administrationskonzept) und zur Weitergabekontrolle.

9.9 Fußball-WM 2006: Akkreditierungsverfahren

Für die Fußball-Weltmeisterschaft 2006 werden voraussichtlich mehr als 250.000 Personen, die in den Stadien tätig werden sollen, u. a. Servicebedienstete, Sicherheitskräfte, Mitarbeiter von Hilfsorganisationen und Journalisten, aber auch ehrenamtliche Helfer, Würstchen- und Fanartikel-Verkäufer, in einem Akkreditierungsverfahren durch die Sicherheitsbehörden des Bundes und der Länder auf ihre Zuverlässigkeit überprüft.

Überwiegend übermittelt der Arbeitgeber in Form von Sammelakkreditierungen der Personen, die zum Einsatz kommen sollen, Namen, Vornamen, Straße, Postleitzahl, Ort, Bundesland, Land, Geburtsdatum, -ort, -land, Nationalität, Ausweisart, -nummer und -gültigkeit an das Organisationskomitee der Veranstalter. Das Verfahren und die Kriterien, die zu einer Ablehnung führen, sind Gegenstand einer Datenschutzinformation, die der Betroffene lesen muss, bevor er in die Überprüfung einwilligen kann. Erfolgt die Übermittlung durch den Arbeitgeber, muss dieser gegenüber dem Organisationskomitee der Veranstalter erklären, dass die Arbeitnehmer entsprechend der Datenschutzinformation belehrt wurden.

Das Organisationskomitee übermittelt die für die Überprüfung erforderlichen Daten an das Bundeskriminalamt, das die Daten nach dem Wohnortprinzip in Länderpakete an die Polizei sowie Pakete für das Bundesamt für Verfassungsschutz, die Bundespolizei und das Bundeskriminalamt aufteilt und verteilt. Das Bundesamt für Verfassungsschutz verteilt seinen Datensatz wiederum nach dem Wohnortprinzip an die Landesämter für Verfassungsschutz. Die Sicherheitsbehörden überprüfen die Daten bei der Entgegennahme auf ihre Plausibilität, etwa Schreibfehler und Zahlendreher, und weisen sie ggf. zurück. Die qualifizierten Voten der Sicherheitsbehörden (akkreditiert/nicht akkreditiert) werden nach der Überprüfung ohne Begründung wieder an das Bundeskriminalamt übermittelt, das ein Gesamtvotum erstellt und dem Organisationskomitee mitteilt. Die Ablehnung einer einzelnen Sicherheitsbehörde führt zu einem ablehnenden Gesamtvotum für die betroffene Person. Dem Organisationskomitee werden weder die Gründe noch die ablehnende Sicherheitsbehörde genannt. Das Organisationskomitee teilt das Ergebnis bei Einzelakkreditierungen den Betroffenen persönlich, bei Sammelakkreditierungen hingegen dem Arbeitgeber mit, der seinerseits den betroffenen Arbeitnehmer informiert.

Die Sicherheitsüberprüfung und die vorherige Benachrichtigung des Arbeitgebers bedeuten für die Betroffenen einen erheblichen Eingriff in ihr Grundrecht auf informationelle Selbstbestimmung. Das Negativvotum führt zu einem partiellen Berufsausübungsverbot für die Betroffenen, bei Arbeitnehmern droht der Arbeitsplatzverlust, so dass auch das Grundrecht der Berufsfreiheit und bei Journalisten die Presse- und Rundfunkfreiheit berührt sind. Das Überprüfungsverfahren erweist sich aus datenschutzrechtlicher Sicht in mehrerlei Hinsicht als bedenklich:

Fehlende gesetzliche Eingriffsgrundlage: Die gesetzlichen Voraussetzungen für eine Sicherheitsüberprüfung nach dem Sicherheitsüberprüfungsgesetz (SÜG) liegen nach Auffassung aller Beteiligten nicht vor. Die Einwilligung der Betroffenen stellt keine ausreichende Rechtsgrundlage für eine Überprüfung durch den Verfassungsschutz oder in diesem Ausmaß durch die Polizeibehörden dar. So fehlt es z. B. für die Beteiligung des Verfassungsschutzes an einer Zuverlässigkeitsüberprüfung bereits an einer Aufgabenzuweisung im Bremischen Verfassungsschutzgesetz. Eine Einwilligung kann dies nicht ersetzen. Die allein auf der Einwilligung der Betroffenen beruhende Sicherheitsüberprüfung ist ein Präzedenzfall und umgeht die strenge Zweckbindung der von den beteiligten Verfassungsschutzbehörden mit nachrichtendienstlichen Mitteln erlangten Erkenntnisse, die für die Überprüfung herangezogen werden. Da diese Erkenntnisse den Betroffenen nicht bekannt sind, scheidet auch insoweit eine Einwilligung aus.

Fehlende Authentizität und Wirksamkeit der Einwilligung: Das Akkreditierungsverfahren gewährleistet nicht die Authentizität der Einwilligungserklärung. Die Betroffenen erklären ihre Einwilligung in die Durchführung des Akkreditierungsverfahrens selbst oder über ihren Arbeitgeber mittels eines Online-Antragsformulars gegenüber dem Organisationskomitee. Die Sicherheitsbehörden erhalten damit keinen authentischen Nachweis, der die Urheberschaft des Einwilligenden sicherstellt. Im Prinzip könnte man so Freunde und Bekannte mit überprüfen lassen. Zweifel sind auch an der Freiwilligkeit und damit Wirksamkeit der Einwilligungserklärung angebracht. Eine Vielzahl von Arbeitnehmern wird die Erklärung nur deswegen abgeben, um negative Folgen im Arbeitsverhältnis zu vermeiden, da die fehlende Einwilligung zwingend zur Ablehnung der Akkreditierung führt.

Fehlende Verhältnismäßigkeit: Für die ablehnende Empfehlung der Sicherheitsbehörden des Bundes und der Länder genügt das negative Votum eines einzelnen Landeskriminalamtes oder Landesamtes für den Verfassungsschutz. Berücksichtigt werden auch Erkenntnisse aus eingestellten Ermittlungsverfahren oder Strafverfahren ohne gerichtliche Verurteilung. Bei den Verfassungsschutzbehörden genügt sogar der Verdacht einer Bestrebung gegen die freiheitlich demokratische Grundordnung für eine zwingende Ablehnung. Im Zweifel soll aus Gründen der Sicherheit eine Ablehnung erfolgen. So wurde bei der Endrundenauslosung zur Fußball-Weltmeisterschaft 2006 im Dezember 2005 mehrfach die Akkreditierung verweigert, weil der Personalausweis oder Reisepass des Betroffenen zu einem früheren Zeitpunkt als verloren oder gestohlen gemeldet war. Dies scheint im Hinblick auf die unter Umständen gravierenden Folgen der Nicht-Akkreditierung und dem rechtsstaatlichen Verhältnismäßigkeitsgrundsatz bedenklich.

Defizite beim Rechtsschutz: Die von den Datenschutzbeauftragten des Bundes und der Länder geforderte Rückmeldung der Ergebnisse zunächst an den Betroffenen wurde abgelehnt. Das Organisationskomitee teilt bei Sammelakkreditierungen nur

dem Arbeitgeber ohne Begründung mit, dass die Akkreditierung verweigert wird. Dem betroffenen Arbeitnehmer drohen damit berufliche oder wirtschaftliche Nachteile, bevor er die Möglichkeit erhält, Fehlinformationen zu korrigieren oder Stellung zu nehmen.

Der Rechtsschutz der Betroffenen ist zudem sehr umständlich organisiert. Für den Betroffenen ist nicht erkennbar, welche Stelle für die Nicht-Akkreditierung wegen Sicherheitsbedenken verantwortlich ist. Nach außen tritt das Organisationskomitee in Erscheinung, dass seine Ablehnung nicht begründet. Der Betroffene muss sich an das Landeskriminalamt seines Landes wenden, dass über das Bundeskriminalamt die für die Ablehnung verantwortliche Stelle anschreibt, z. B. das Bundesamt für Verfassungsschutz, das sich seinerseits an das entsprechende Landesamt für Verfassungsschutz wendet. Kritisch zu betrachten ist auch, dass die Polizeibehörden (Bundes-, Landeskriminalamt) auf diese Weise Kenntnis erlangen, dass Informationen über den Betroffenen beim Verfassungsschutz vorliegen.

9.10 Mobile Videoüberwachung durch die Polizei

Es bestehen Planungen bei der Polizei, Videoüberwachung künftig auch mobil einzusetzen. Soweit es sich um die mobile Videoüberwachung zum Zwecke der Eigensicherung der eingesetzten Polizeibeamten handelt, verweise ich auf Ziff. 9.3 dieses Berichts. Daneben bestehen aber auch Überlegungen, vorhandene Videoüberwachungsgeräte, die gemäß § 29 Abs. 3 des BremPolG eingesetzt werden, wahlweise an verschiedenen, festgelegten Orten einzusetzen, ohne dass die begleitenden Maßnahmen, z. B. Hinweisschilder, jeweils konkret auf den Einsatz der Anlage hinweisen. Diese Pläne stehen nicht im Einklang mit § 29 Abs. 3 BremPolG; hierauf habe ich die Polizei Bremen hingewiesen.

9.11 Stalkerdatei

Im August des Berichtsjahres hat die Polizei Bremen in das Polizeiinformationssystem ISA (InformationssystemSachenAnzeigen) die Gefährderdatei „Stalker und Beziehungstäter“ eingeführt. Täter von Stalking oder häuslicher Gewalt werden im Polizeiinformationssystem mit dem personenbezogenen Hinweis „Gefährder“ aufgeführt, so dass Polizeibeamte bei ihren Einsätzen das Gefährdungspotential dieser Personen frühzeitig erkennen und entsprechend reagieren können. Das hierfür erforderliche Datenschutzkonzept wurde mit mir abgestimmt.

9.12 Datenverarbeitung bei der Feuerwehr in Bremen

Der behördliche Datenschutzbeauftragte der Feuerwehr Bremen hat mir aufgrund der Eingabe eines Mitarbeiters eine Dokumentation zur Regelung des Zugriffs auf die Dateien bei der Feuerwehr Bremen (vgl. 27. JB, Ziff. 6.14) vorgelegt. Zu diesem Konzept habe ich Stellung genommen.

Die Dokumentation ist um eine Beschreibung des Beantragungsverfahrens sowie um die Darstellung der Zugriffs- und Verzeichnisstrukturen zu vervollständigen, zur Zugangskontrolle habe ich Empfehlungen abgegeben. Weitere wesentliche Themen sind Probleme bei dezentraler Datenspeicherung (mangelnde Zugriffs- und Verfügbarkeitskontrolle), Fragen zur Vergabe von Gruppenberechtigungen sowie zu benennende Maßnahmen zur Weitergabe-, Verfügbarkeits-, Eingabe- und Auftragskontrolle. Ein Konzept zur Erhöhung der Transparenz der Administratorentätigkeit, welches beispielweise die Festlegung von Verantwortlichkeiten sowie Rechte und Pflichten, Möglichkeiten der Protokollierung und Revision darlegen soll, steht ebenfalls aus.

Zur Auftragskontrolle habe ich dargelegt, dass die Fremdwartung ein Sicherheitskonzept erfordert, durch das geeignete technische und organisatorische Maßnahmen getroffen werden, um personenbezogene Daten vor unberechtigtem Zugriff zu schützen.

Weiterhin habe ich der Bitte des Datenschutzbeauftragten der Feuerwehr Bremen entsprochen und zu Fragen der Netzwerkadministration, der Vergabe von Berechtigungen im Netz (Rollenkonzept, Zugriffskontrolle) und zu einzelnen Positionen des Netzwerksicherheitskonzeptes Stellung genommen. Der behördliche Datenschutzbeauftragte teilte mir mit, dass er voraussichtlich ab Mitte Februar 2006 Ergebnisse zu einzelnen Fragestellungen vorlegen könne.

9.13 Einsatz von Unfalldatenspeichern bei der Feuerwehr Bremen

Die Feuerwehr in Bremen informierte mich über den Einsatz von Unfalldatenspeichern, mit denen Rettungsfahrzeuge, Intensivkrankentransportwagen, Großraumkrankentransportwagen sowie Notarzteinsatzfahrzeuge ausgestattet werden. Ein Unfalldatenspeicher (UDS) ist ein Gerät, welches bei eingeschalteter Zündung permanent und uhrzeitgenau Fahrzeugbewegungen, Stellung bzw. Bedienung angeschlossener Bedienelemente erfasst und interne Vorgänge überwacht. So werden beispielsweise Daten zur Fahrzeugrichtung, Quer- und Längsbeschleunigung, Geschwindigkeit, Fahrtrichtungsanzeiger, Signallicht, Blaulicht, Standlicht, Abblendlicht etc. aufgezeichnet.

Das Datenspeicherprogramm ist sehr komplex. Sobald bestimmte Merkmale erreicht sind, werden die Daten zu einem Ereignis zusammengefasst und in einem von neun Ereignisspeichern gespeichert. So sollen bei einem Unfall die letzten 28 Sekunden vor sowie 15 Sekunden nach dem Ereignis automatisch gespeichert werden. Darüber hinaus besteht die Möglichkeit, dass der Fahrzeuglenker durch Betätigung der UDS-Taste (manuelles Ereignis) die Daten der letzten 43 Sekunden und ca. 100 folgenden Meter speichert (z. B. bei dem Überfahren einer auf Rot stehenden Lichtsignalanlage). Weiterhin werden Daten in einem von drei Stillstandsspeichern gesichert, wenn das Fahrzeug länger als drei Sekunden steht, sowie interne Ereignisse (z. B. Zündung an/aus, UDS-Taste gedrückt, UDS-Speicher ausgelesen) aufgezeichnet.

Mit den UDS-Daten soll der Unfallverlauf rekonstruiert und ggf. das korrekte Verhalten der Fahrzeugführer nachgewiesen werden.

Die Daten sollen mittels eines ausschließlich hierfür vorgehaltenen Notebooks aus dem UDS heruntergeladen werden. Dieser Vorgang geschieht mit einer hierfür vorgesehenen und durch einen Hardlock gesicherten Software. Zusätzlicher Schutz des Notebooks vor missbräuchlicher Nutzung wird durch weitere technische und organisatorische Maßnahmen geschaffen. Die heruntergeladenen Daten werden auf einem kennwortgeschützten USB-Stick gespeichert und an einen vom Hersteller autorisierten und von der Feuerwehr schriftlich beauftragten Sachverständigen weitergegeben, dem die Auswertung der Daten obliegt. Die Feuerwehr Bremen besitzt keine weiterführende Software, die eine Auswertung der Daten ermöglicht.

Der Datenschutzbeauftragte der Feuerwehr Bremen legte mir die nach dem Bremischen Datenschutzgesetz (BremDSG) erforderliche Verfahrensbeschreibung sowie die Dienstanweisung und Bekanntmachung vor. Hierzu habe ich im Berichtsjahr Stellung genommen und Vorschläge und Anforderungen zur Gestaltung der Dienstvereinbarung sowie insbesondere zur Speicherung und zu den technischen und organisatorischen Maßnahmen gemacht.

Ich habe darauf hingewiesen, dass der betroffene Fahrzeugführer in jedem Fall über das Auslesen des UDS zu benachrichtigen ist. Klärungsbedarf gibt es derzeit noch zum Umfang der aufgezeichneten Betriebsdaten des Fahrzeugs wie auch zur tatsächlichen Speicherdauer und zur Löschung hoher Bewertungen. Die Messdaten werden mit einer bestimmten Bewertung durch den UDS gespeichert. Die Löschung der Daten soll durch Überschreiben der Ereignisspeicher mit einer höheren Bewertung erfolgen. Eine abschließende Stellungnahme der Feuerwehr Bremen liegt noch nicht vor.

9.14 Internetnutzung bei der Feuerwehr Bremen

Ich habe die Feuerwehr in Bremen zur Nutzung von E-Mail und Internet am Arbeitsplatz beraten. Die mir hierzu vorgelegten Dienstvereinbarungen und Dokumente bezogen sich auf veraltete Regelwerke, was formale und inhaltliche Anpassungen erfordert hätte. Ich begrüße daher die Entscheidung der Feuerwehr Bremen, stattdessen die Richtlinie für die Nutzung der Elektronischen Post vom 7. März 2002 sowie die Richtlinie für die Bereitstellung und Nutzung von Internet-/Intranet-Zugängen vom 10. Februar 2004 einzuführen, nach dessen Vorgaben die Protokollierung ausgerichtet wird.

Hinsichtlich der Aufstellung zusätzlicher PC zur ausschließlichen privaten Nutzung des Internets habe ich auf die Einhaltung der Vorgaben zum Datenschutz und zur Protokollierung (z. B. Untersagung dezentraler Protokollierung bei privaten Zugriffen) gedrungen. So ist zu gewährleisten, dass der für die private Nutzung bereitgestellte Proxy-Server genutzt wird, ebenso müssen geeignete technische und or-

ganisatorische Maßnahmen (u. a. Firewall, Virenschutz, DMZ, logische Trennung, Deaktivierung externer Medien) getroffen werden, um das Netzwerk der Feuerwehr gegen die Internet-PC abzuschotten und vor Angriffen aus dem Internet zu schützen.

Der Datenschutzbeauftragte der Feuerwehr Bremen teilte mir mit, dass meine Vorschläge zum Datenschutz bei der Umsetzung des Vorhabens berücksichtigt werden.

9.15 Zentrales Datenschutzkonzept und Verfahrensbeschreibungen beim Stadtamt Bremen

Im Berichtsjahr wurden mir vom Stadtamt Bremen scheibchenweise mehrere unzureichende Verfahrensbeschreibungen zur Stellungnahme übergeben. Zum einen handelte es sich hier um die seit 2002 von mir geforderte Verfahrensbeschreibung zur Waffenverwaltung, zum anderen um Angaben zu Verfahren, die beim Bürger-Service-Center (BSC) genutzt werden.

Insgesamt musste ich feststellen, dass es keine übergreifende Dokumentation gibt, in der die allgemeinen Sicherheits- und Datenschutzmaßnahmen des Stadtamtes beschrieben sind. Hierzu zähle ich auch das BSC, da es technisch mit den Fachverfahren für das Meldewesen (MESO), Gewerbe (GewNeu/MIGEWA), Kfz-Zulassung (eKol/Ikol), Führerschein, Fischereiangelegenheiten, Ausländer/Verpflichtungserklärungen und weiteren Anwendungen an das Stadtamt gebunden ist. Inhalt einer solchen Dokumentation sollten unter anderem die internen IT-Sicherheitsziele und Maßnahmen zu ihrer Umsetzung, die Beschreibung der Sicherheitsaspekte der Netzinfrastruktur sowie auch Sicherheitsmechanismen zur Zutritts-, Zugangs-, Verfügbarkeits- und Weitergabekontrolle sein.

Neben der Erstellung des allgemeinen Sicherheits- und Datenschutzkonzepts ist eine Anpassung der einzelnen Fachdatenschutzkonzepte für die Waffenverwaltung und die vom BSC genutzten Anwendungen erforderlich. Hier fehlt es beispielweise an der durchgängigen und vollständigen Beschreibung der Prozesse sowie an Angaben zur Zugriffskontrolle, zur Protokollierung und zur Administration.

Mehrfach habe ich die Erstellung der erforderlichen Datenschutzkonzepte für Stadtamt und BSC gefordert. Erst in der Sitzung des Rechtsausschusses im November des Berichtsjahres wurde von einem Vertreter des Innenressorts und vom Leiter des Stadtamts zugesagt, die spätestens seit 2003 überfällige Bestellung eines behördlichen Datenschutzbeauftragten vorzunehmen, wie aber auch mit Hilfe eines externen Unternehmens die Erstellung des Datenschutzkonzeptes zu beauftragen. Kurz vor Weihnachten 2005 ging bei mir eine Vorstudie „Unterstützung Datenschutzkonzeptorganisation Stadtamt“ ein. Hierzu habe ich Stellung genommen.

Im Februar fand die Kick-Off-Veranstaltung für die Erstellung der genannten Datenschutzkonzepte statt. Die Terminplanung sieht vor, dass die ersten Fachdatenschutzkonzepte sowie das allgemeine Rahmendatenschutzkonzept bis Ende April 2006 abgeschlossen sein sollen. Es bleibt zu hoffen, dass der zähe Fortgang der Erstellung der Datenschutzkonzepte und des Verfahrensverzeichnisses in 2006 ein Ende finden wird.

9.16 Einführung eines neuen DV-Verfahrens bei der Meldebehörde Bremen

Da das bisherige DV-Verfahren den melderechtlichen Anforderungen nicht mehr gerecht wurde, gelangt seit Ende des Berichtsjahres – wie bei zahlreichen anderen Meldebehörden in Deutschland – auch in Bremen das DV-Verfahren MESO (Meldebehördensoftware) zum Einsatz. Die Einführung des neuen Verfahrens erfolgt schrittweise, wobei die Verfahrensteile „Personalausweis- und Passregister“, „Lohnsteuer“ und „Wahlen“ erst bei weiteren Schritten implementiert werden sollen. Die Software enthält umfangreiche Programmkomponenten, deren Nutzung die Bearbeitung von Vorgängen im Bereich des Meldewesens erheblich vereinfachen soll.

Verbunden mit der Einführung sind jedoch auch erhebliche datenschutzrechtliche Fragestellungen, die vor der Inbetriebnahme eines derartigen Verfahrens geklärt werden müssen. Nachdem ich von der Meldebehörde über ihre Absicht, ein neues DV-Verfahren zu implementieren, unterrichtet und um eine datenschutzrechtliche Beratung gebeten worden war, hatte ich sie bereits im Frühjahr des vergangenen Jahres auf die zu klärenden Punkte aufmerksam gemacht. Um das vorgesehene DV-Verfahren beurteilen zu können, bat ich die Meldebehörde u. a., mir eine Verfah-

rensbeschreibung zum neuen Verfahren einschließlich Datensatz- und Datenbankbeschreibungen, Auflistungen von Mitteilungs- und Übermittlungsdiensten, Informationen zu eGovernment-Anwendungen, Informationen über die Berücksichtigung von Auskunfts- und Übermittlungssperren sowie ein Datenschutzkonzept mit den vorgesehenen technischen und organisatorischen Sicherungsmaßnahmen (insbesondere im Hinblick auf die vorhandenen Zugriffsmöglichkeiten, die vorgesehenen Datenübermittlungen und Protokollierungen) zukommen zu lassen. Zu meinem Bedauern habe ich hiervon bislang erst einen sehr kleinen Teil der Unterlagen erhalten, die ihrerseits dann wieder zahlreiche Fragen hinsichtlich der Datenverarbeitung mit dem Verfahren MESO aufwerfen. Eine Beurteilung des Verfahrens war mir somit bislang nicht möglich. Trotzdem wird MESO von der Meldebehörde eingesetzt. Möglicherweise bestehende datenschutzrechtliche Mängel konnten vor der Inbetriebnahme des Verfahrens nicht mehr behoben werden, was zu erheblichen Datenschutzverletzungen im laufenden Betrieb führen kann.

Ich habe der Meldebehörde noch einmal mitgeteilt, welche Informationen und Unterlagen von mir benötigt werden. Für den Fall, dass mir diese auch weiterhin nicht zur Verfügung gestellt werden, behalte ich mir eine formelle Beanstandung gegenüber dem Senator für Inneres und Sport ausdrücklich vor.

9.17 FundInfo über das Internet

Im September des Berichtsjahres hat das Fundamt des Stadtamtes die Internet-Anwendung FundInfo eingeführt. Dabei sind die Datenbestände bestehender Fundbüros im Land Bremen und zahlreicher Umlandgemeinden vernetzt und in einer zentralen Datenbank zusammengeführt worden. Der Bürger kann nun jederzeit von zu Hause über das Internet nach verlorenen Gegenständen suchen. Die Suche wird durch Angabe eines Suchgebietes, Kategorien von Gegenständen (z. B. Schlüssel, Ausweis, Fahrrad) und den Tag, seit dem der Gegenstand vermisst wird, eingegrenzt. Anschließend zeigt FundInfo eine Liste der Sucheinträge mit einer kurzen Beschreibung des Gegenstandes, dem Funddatum und -ort sowie das zuständige Fundbüro an. Wie bisher bleibt darüber hinaus die telefonische Auskunft oder das persönliche Aufsuchen des Fundbüros möglich.

Fundsachen wie Brieftaschen oder Mobiltelefone enthalten oft personenbezogene Daten bis hin zu sensiblen Daten des Betroffenen, z. B. einen Schwerbehindertenausweis, Rechnungen oder Fotos. Auch bei der Fundsachenverwaltung fallen personenbezogene Daten des Finders z. B. für Finderlohnansprüche und des Eigentümers der verlorenen Sachen an. Ich habe mich dafür eingesetzt, dass der Schutz der personenbezogenen Daten innerhalb der Datenbank und beim Zugriff über das Internet technisch und organisatorisch sichergestellt wird. Auch dürfen nicht mehr personenbezogene Daten als für die Fundsachenverwaltung erforderlich aufgenommen oder über FundInfo im Internet zugänglich sein. Die Einführung von FundInfo wurde von mir aus datenschutzrechtlicher Sicht begleitet. Zurzeit steht noch die Erstellung einer Verfahrensbeschreibung nach § 8 Bremisches Datenschutzgesetz (BremDSG) aus.

9.18 Eingaben betreffend die Meldebehörde

Wiederholt erhielt ich im Berichtsjahr Eingaben von Bürgern, die die unzulässige Verarbeitung ihrer Daten durch die Einwohnermeldebehörde betrafen. Ein Bürger beklagte sich, dass die Meldebehörde Bremen für ihn eine Abmeldung von seinem Wohnsitz vollzogen habe, obgleich sich dieser nicht verändert hätte. Der Petent erklärte, dass die Abmeldung von Amts wegen vorgenommen worden sei, nachdem Nachbarn von ihm der Behörde mitgeteilt hätten, dass mein Petent verzogen sei. Gemäß § 21 Satz 1 Bremisches Meldegesetz (BremMeldG) hat die Meldebehörde das Melderegister von Amts wegen fortzuschreiben, wenn sich gespeicherte Daten geändert haben oder wenn neue oder weitere Daten zu speichern sind. Wie die Meldebehörde bei meiner Prüfung bestätigte, war jedoch die notwendige Überprüfung der Angaben bedauerlicherweise unterblieben. Die Meldebehörde hätte die ihr zugeleiteten Informationen z. B. durch eine Befragung des Wohnungsgebers überprüfen müssen. Der festgestellte Sachverhalt wurde zum Anlass genommen, die zuständigen Mitarbeiter der Meldebehörde für die Problemlage zu sensibilisieren. Das Melderegister wurde nach § 10 BremMeldG korrigiert, wonach unrichtig gespeicherte Daten zu berichtigen sind.

In einem anderen Fall beklagte sich ein Bürger über die Erteilung von nicht zulässigen Auskünften zu seiner Person an Unternehmen der Privatwirtschaft. Die Aus-

künfte seien an die Firmen erteilt worden, obwohl die Meldebehörde Bremen nicht nach ihm, sondern nach einer anderen Person mit gleichem Namen gefragt worden sei. Um die Verwechselung zu vermeiden, hätte die Meldebehörde nur weitere Angaben zum Betroffenen, u. a. die ihr genannte frühere Anschrift, präziser berücksichtigen müssen, was nicht geschehen sei. Durch die Verwechselung wurden dem Petenten durch das Unternehmen der Privatwirtschaft äußerst sensible Daten bekannt, die für ihn sonst nicht zugänglich gewesen wären. Er erhielt u. a. Kenntnis von nicht bezahlten Rechnungen und laufenden Mahnverfahren. Gemäß § 32 Abs. 1 und 2 BremMeldG darf die Meldebehörde Auskünfte nur über einzelne bestimmte Einwohner erteilen. Dies bedeutet u. a., dass der Einwohner, zu dem eine Auskunft verlangt wird, vom Auskunftsuchenden so zu bestimmen ist, dass eine eindeutige Identifikation möglich wird. Eine Verwechselung der Person, zu der Auskunft erteilt wird, darf nicht vorkommen. Auf mein Anschreiben bestritt die Meldebehörde Bremen, bei der Erteilung der Auskünfte über den Petenten einen Fehler gemacht zu haben. Da der Straßenname bei der Selektion der Person, über die beauskunftet wurde, Berücksichtigung fand und unter dem Straßennamen keine weitere Person gemeldet war, sei die bei der Erteilung solcher Auskünfte gebotene Sorgfalt berücksichtigt worden. Im Übrigen weise die Meldebehörde bei der Erteilung von Melderegisterauskünften die Auskunftsuchenden ausdrücklich darauf hin, dass keine Gewähr dafür übernommen werden kann, dass die ermittelte mit der tatsächlich gesuchten Person übereinstimmt.

Zu den Ausführungen der Meldebehörde Bremen wies ich darauf hin, dass gemäß § 7 BremMeldG die schutzwürdigen Belange der Betroffenen zu wahren sind. Übermittelt werden dürfen Daten nur zu der Person, zu der angefragt wurde; anderenfalls ist die Übermittlung unzulässig. Bestehen Zweifel, ob die aus dem Melderegister selektierten Daten der Person zuzuordnen sind, zu der angefragt wurde, ist die Übermittlung zu unterlassen. Der Hinweis an die Auskunftsuchenden, dass keine Gewähr dafür übernommen werden kann, dass die ermittelte Person mit der tatsächlich gesuchten Person übereinstimmt, reicht zur Wahrung der schutzwürdigen Belange der Betroffenen nicht aus. Ich halte an meiner Auffassung fest, dass die Meldebehörde bei der Übermittlung der den Petenten betreffenden Daten die gebotene Sorgfalt unbeachtet ließ, und forderte diese nochmals auf, bei der Erteilung von Auskünften nach § 32 BremMeldG künftig sorgfältiger vorzugehen, ihr Verfahren bei der Auskunftserteilung im Hinblick auf die Wahrung der schutzwürdigen Belange der Betroffenen ggf. zu verbessern und mir dies entsprechend zu bestätigen. Die Bestätigung steht noch aus.

9.19 Einführung des ePasses

Seit dem 1. November 2005 wird in Deutschland der so genannte ePass ausgegeben. Der neue Reisepass ist mit einem elektronischen Speicherchip versehen, der ein Gesichtsbild des Passinhabers enthält. Von März 2007 an sollen auf dem Chip auch Fingerabdrücke gespeichert werden. Grundlage hierfür ist eine EU-Verordnung aus dem Jahr 2004, die nicht zuletzt nach den Anschlägen des 11. September 2001 auf Druck der USA verabschiedet worden ist. Interessant ist dies deshalb, weil in den USA bislang nicht einmal ein bundesweit einheitlicher Personalausweis existiert, den die Bürger mit sich führen müssen.

Für die Bremer Bürgerinnen und Bürger wird sich bei der Beantragung eines solchen Biometriepasses zunächst nichts ändern. Lediglich an das vorzulegende Lichtbild werden andere Anforderungen gestellt als bisher. Außerdem wird die Gebühr für das Dokument erhöht. Für einen normalen Reisepass zahlt man nun 59 € statt bisher 26 €.

Ich halte die Einführung biometrischer Pässe aus datenschutzrechtlicher Sicht für bedenklich. Die Speicherung biometrischer Merkmale in Ausweisdokumenten führt nicht automatisch auch zur Verbesserung der Sicherheit. Denn nicht die deutschen Bürgerinnen und Bürger sind vornehmlich das Sicherheitsrisiko. Solange daher nicht weltweit einheitliche Verfahren bei der Passvergabe gewährleistet sind, wird es keinen gravierenden Sicherheitszuwachs geben. Das gilt umso mehr, als in einigen Staaten bislang nicht einmal fälschungssichere Ausweispapiere ausgegeben werden. Außerdem existieren bisher keine international gültigen Regelungen, die gewährleisten, dass biometrische Daten deutscher Staatsbürger nicht in anderen Staaten in externen Datenbanken gespeichert werden. Ich bezweifle aus diesen Gründen die Geeignetheit und Erforderlichkeit der Einführung biometrischer Pässe.

Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder beurteilt die Einführung biometrischer Ausweisdokumente kritisch. In ihrer Entschließung vom 1. Juni 2005 (vgl. Ziff. 19.11 dieses Berichts) fordert die Konferenz, dass mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten erst begonnen wird, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Bis heute liegt jedoch ein umfassendes Sicherheitskonzept nicht vor. Außerdem fehlen im Passgesetz Regelungen zur strikten Zweckbindung der Daten.

9.20 Veröffentlichung von Daten von Beiratsmitgliedern und „Fachberatern" im Internet

In einem Ortsamtsbereich wurden in Form einer „Stadtteilbroschüre" im Internet personenbezogene Daten, unter anderem der Mitglieder der Beiräte und der Fachausschüsse, veröffentlicht. Die Veröffentlichung betraf dabei nicht nur die regulären Beiratsmitglieder, sondern auch die so genannten sachkundigen Bürger, die nur in nicht-öffentlichen Sitzungen der Fachausschüsse in Erscheinung treten. Einer dieser Bürger wandte sich an mich, da er mit der Veröffentlichung in dieser Form nicht einverstanden war.

Bei der Veröffentlichung im Internet handelt es sich rechtstechnisch um eine Übermittlung personenbezogener Daten, die nur zulässig ist, soweit der Betroffene eingewilligt hat oder Rechtsvorschriften die Veröffentlichung erlauben oder voraussetzen. Vorliegend fehlte es sowohl an einer Einwilligung der Betroffenen als auch an einer Rechtsvorschrift. Auf meinen Hinweis gegenüber dem Ortsamtsleiter werden die personenbezogenen Daten nunmehr nur mit Einwilligung der Betroffenen veröffentlicht. Bei den sachkundigen Bürgern werden selbst dann nur die Namen, nicht jedoch die Adresse und Telefonnummer oder E-Mail-Adresse wiedergegeben.

10. Justiz

10.1 Eröffnung des elektronischen Rechtsverkehrs

Am 1. Dezember 2005 wurde in Bremen als erstem Bundesland flächendeckend die Möglichkeit des elektronischen Rechtsverkehrs mit der Justiz eröffnet. Bei allen Gerichten und Staatsanwaltschaften Bremens – mit Ausnahme des gemeinsamen Landessozialgerichts Bremen/Niedersachsen – können nun Klageschriften und andere Dokumente in elektronischer Form eingereicht werden. Durch das Justizkommunikationsgesetz wurden in den einzelnen Verfahrensordnungen Rechtsgrundlagen für den elektronischen Rechtsverkehr geschaffen. Diese sehen für die Eröffnung des elektronischen Rechtsverkehrs ihrerseits den Erlass einer Rechtsverordnung voraus. Diese trat am 26. November 2005 in Bremen in Kraft.

Der Senator für Justiz und Verfassung (SfJuV) informierte mich im Juni 2005 über das geplante Vorhaben. Die Basiskomponenten für den elektronischen Rechtsverkehr sind das „elektronische Gerichts- und Verwaltungspostfach (EGVP) – Produktname Govello" sowie die „Virtuelle Poststelle – Produktname Governikus". Bei „EGVP" handelt es sich um Clientsoftware, die Funktionalitäten zur Verfügung stellt, um unstrukturierte Textkommunikation mit Anlagen zu ermöglichen (vergleichbar mit der herkömmlichen E-Mail, aber erweitert um Signatur- und Verschlüsselungsverfahren). „Governikus" bezeichnet die technologische Plattform, die erst die einzelnen spezifischen Verfahren ermöglicht.

In Gesprächen mit dem SfJuV wurden die datenschutzrechtlichen Anforderungen für den elektronischen Rechtsverkehr erörtert. Dabei wurde ein Schwerpunkt auf die Verteilung der elektronischen Dokumente an die entsprechenden Bearbeiter gelegt. Die Dokumente, die elektronisch die Gerichte und Staatsanwaltschaften erreichen, werden dort entschlüsselt und sind an die jeweiligen Bearbeiter zu verteilen. Die unverschlüsselte Weiterverteilung der eingereichten Dokumente per E-Mail ist – auch hausintern – gemäß E-Mail-Richtlinie (Richtlinie für die Nutzung der Elektronischen Post [E-Mail] vom 7. März 2002) nicht zulässig. Ich habe ein Abrufverfahren vorgeschlagen, bei dem die zuständigen Bearbeiter von der Eingangsstelle die elektronischen Dokumente zur Bearbeitung anfordern können.

Weiteres Augenmerk habe ich auf die fristgerechte Löschung der Daten nach deren Weiterleitung gelegt. Hierzu habe ich ein Verfahren aufgezeigt, wie die Daten halb-automatisiert gelöscht werden können. Der manuelle Aufwand würde sich auf

das absolut notwendige Minimum beschränken. Der SfJuV hat mir daraufhin am 21. Dezember 2005 mitgeteilt, dass er dieses Verfahren gerne aufgreifen würde, mit einer Umsetzung innerhalb von sechs Monaten aber nicht zu rechnen sei und daher zunächst längere Löschfristen in Kauf genommen werden müssten.

Zur Verfahrensumsetzung gehört, dass sowohl für den Einsatz der zentralen Komponente „Governikus" ein Datenschutzkonzept anzufertigen ist als auch für die jeweils an dem Verfahren teilnehmenden Geschäftsstellen dezentrale und auf den betreffenden Anwendungsfall bezogene Verfahrensbeschreibungen zu erstellen sind. Am 21. Dezember 2005 wurden mir vom SfJuV hierzu verschiedene Dokumente, u. a. die Verfahrensbeschreibung „Elektronischer Rechtsverkehr mit den Gerichten und Staatsanwaltschaften im Land Bremen" zugesandt. Eine datenschutzrechtliche Bewertung der Dokumente war bis zum Redaktionsschluss nicht mehr möglich.

10.2 Neuregelung der forensischen DNA-Analyse

Am 1. November 2005 traten die Neuregelungen der forensischen DNA-Analyse in Kraft. Aus datenschutzrechtlicher Sicht möchte ich auf eine Änderung besonders eingehen, nämlich die der DNA-Reihenuntersuchung in § 81 h Strafprozessordnung (StPO). Schon im letzten Jahr habe ich die Schaffung einer ausdrücklichen Rechtsgrundlage mit präzisen und engen Anforderungen gefordert (vgl. 27. JB, Ziff. 6.3). Diese Forderung resultierte nicht zuletzt aus der während der DNA-Reihenuntersuchung in Bremerhaven entstandenen Rechtsunsicherheit. Da es bislang keine gesetzliche Grundlage für die DNA-Reihentests gab, waren erhebliche Unsicherheiten aufgetreten, unter welchen Voraussetzungen ein Reihentest durchgeführt werden darf (z. B. ob eine richterliche Anordnung erforderlich ist).

Wesentliche Punkte der Neuregelung des § 81 h StPO sind:

— Reihengentests sind nur zulässig bei Verbrechen gegen Leben, Leib, Freiheit und sexuelle Selbstbestimmung.

— Nur ein Richter darf den Reihengentest anordnen (Richtervorbehalt).

— In der richterlichen Anordnung müssen die betroffenen Personen anhand bestimmter Prüfungsmerkmale bezeichnet werden (z. B. alle Männer einer bestimmten Altersklasse, die in einer bestimmten Umgebung wohnen).

— Die Tests dürfen nur auf freiwilliger Basis erfolgen; die schriftliche Einwilligung der Betroffenen ist erforderlich.

— Die Betroffenen sind über die Freiwilligkeit ihrer Mitwirkung zu belehren.

— Die erhobenen Daten dürfen nicht in der DNA-Analysedatei gespeichert werden.

— Die entnommenen Körperzellen sind unverzüglich zu vernichten, sobald sie nicht mehr erforderlich sind.

— Die Aufzeichnungen über die Auswertungen der DNA-Analyse sind zu löschen, wenn sie zur Aufklärung des Verbrechens nicht mehr erforderlich sind. Die Löschung muss dokumentiert werden.

— Die Untersuchung des DNA-Materials wird in anonymisierter Form durch Sachverständige durchgeführt.

Damit wurde wesentlichen, auch von mir erhobenen datenschutzrechtlichen Anforderungen bei der Novellierung von § 81 h StPO weitgehend entsprochen.

Weiterhin war es aus datenschutzrechtlicher Sicht wichtig, dass der Richtervorbehalt generell für die Entnahme und die molekulargenetische Untersuchung bestehen blieb. Es gab Initiativen zur Streichung des Richtervorbehalts. Dagegen hat sich auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder mit einer Entschließung vom 11. März 2005 (vgl. Ziff. 19.10 dieses Berichts) gewandt. Die jetzt in der StPO getroffene Neuregelung stellt die DNA-Analyse auch weiterhin unter Richtervorbehalt. Allerdings ist eine richterliche Anordnung entbehrlich, wenn der Betroffene eingewilligt hat und darüber belehrt worden ist, für welchen Zweck die zu erhebenden Daten verwendet werden. Darüber hinaus kann auch bei Gefahr im Verzug die Staatsanwaltschaft oder Polizei entscheiden. Diese Aufweichungen des Richtervorbehalts sind datenschutzrechtlich nicht unbedenklich.

Als Anlasstat ist nach der Neuregelung auch die wiederholte Begehung sonstiger Straftaten ausreichend. Da die DNA-Analyse einen erheblichen Eingriff in das Recht auf informationelle Selbstbestimmung darstellt, ist diese Absenkung der Anforderungen bedenklich. Hiergegen haben sich die Datenschutzbeauftragten des Bundes und der Länder ausgesprochen.

10.3 Akustische Wohnraumüberwachung

Die akustische Wohnraumüberwachung (Großer Lauschangriff) wurde in weiten Teilen vom Bundesverfassungsgericht für verfassungswidrig erklärt (vgl. 27. JB, Ziff. 7.1). Das Gericht verpflichtete den Gesetzgeber, einen verfassungsmäßigen Zustand bis spätestens zum 30. Juni 2005 herzustellen. Der Bundestag hat die Neuregelungen im Juni 2005 verabschiedet. Unter anderem sind jetzt Abhörmaßnahmen unverzüglich zu unterbrechen, soweit sich während der Überwachung Anhaltspunkte dafür ergeben, dass Äußerungen, die dem Kernbereich privater Lebensgestaltung zuzurechnen sind, erfasst werden. Darüber hinaus ist der Straftatenkatalog unter dem Gesichtspunkt der Erheblichkeit der Strafandrohung reduziert worden.

Daneben hat ein vom Bundesministerium der Justiz an das Max-Planck-Institut in Auftrag gegebenes Gutachten die akustische Wohnraumüberwachung im strafprozessualen Bereich evaluiert. Das Gutachten kommt zu dem Ergebnis, dass häufig keine ausreichende Dokumentation der Maßnahme erfolgte. Eine Dokumentation hat aus Gründen der sicheren Erfüllung der Benachrichtigungspflicht, der damit verbundenen Ermöglichung eines effektiven Rechtsschutzes sowie der Nachvollziehbarkeit von Löschungs- und Vernichtungspflichten zu erfolgen. Aufgrund der Defizite in der Praxis sollte die Dokumentationspflicht gesetzlich umfassender vorgeschrieben werden.

Die Anforderungen des Bundesverfassungsgerichts lassen sich nicht nur auf die akustische Wohnraumüberwachung beschränken. Die Gesetzgeber in Bund und Ländern sind aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden den Vorgaben des Verfassungsgerichts entsprechend auszugestalten. Diese Verpflichtung lässt sich zum einen aus den allgemein verbindlichen Vorgaben der Entscheidung des Bundesverfassungsgerichts zum Großen Lauschangriff und zum anderen aus der erneuten Bestätigung der hohen Anforderungen an Eingriffe in den Kernbereich der privaten Lebensgestaltung im Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung herleiten, in welcher eine entsprechende Regelung im niedersächsischen Polizeigesetz für verfassungswidrig erklärt wurde. Das Bundesverfassungsgericht stellte in dieser Entscheidung fest, dass der durch die Menschenwürde garantierte, unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist.

10.4 Prüfung der DV-Verfahren bei Vaterschaftstests

Die Zulässigkeit von so genannten heimlichen Vaterschaftstests stellt ein sehr kontrovers diskutiertes Thema dar. Im Januar 2005 wurden Pläne des Bundesministeriums der Justiz bekannt, heimlich veranlasste Vaterschaftstests generell zu verbieten und unter Strafe zu stellen. Dieses Gesetzesvorhaben wurde jedoch nicht weiter betrieben. Auch der Bundesgerichtshof befasste sich Anfang des Jahres 2005 mit den heimlichen Labortests zur Feststellung der Vaterschaft (vgl. Urteile vom 12. Januar 2005 – XII ZR 60/03 und XII ZR 227/03). Er hatte darüber zu entscheiden, ob ohne die Zustimmung des Kindes bzw. dessen allein sorgeberechtigter Mutter eingeholte DNA-Vaterschaftsanalysen im Rahmen einer Vaterschaftsanfechtungsklage verwertet werden können. Der Bundesgerichtshof kam zu dem Ergebnis, dass eine Anfechtung der Vaterschaft nicht auf heimlich eingeholte DNA-Vaterschaftstests gestützt werden kann. Die Entscheidung wurde damit begründet, dass die Untersuchung des genetischen Materials eines anderen Menschen ohne dessen ausdrückliche Zustimmung gegen das Recht auf informationelle Selbstbestimmung verstößt und damit rechtswidrig ist. Das Selbstbestimmungsrecht des Kindes brauche nicht hinter dem Interesse des als Vater geltenden Mannes zurückzustehen, der sich Gewissheit über seine biologische Vaterschaft verschaffen wolle.

Die Entscheidungen des Bundesgerichtshofs stellen eine Entwicklung im Sinne des Datenschutzes dar. Bereits im Jahr 2001 forderte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Gendiagnostikgesetz, mit dem die

heimliche Durchführung von Gentests gesetzlich untersagt wird (vgl. hierzu 24. JB, Ziff. 15.11). Diese Forderung gilt nicht nur für heimliche Vaterschaftstests, sondern für alle Gentests, die ohne Wissen des Betroffenen durchgeführt werden. Aus diesem Grund habe ich mich zur Bestärkung dieser Forderung mit einer Pressemitteilung „Genetische Daten wirksam schützen" nochmals an die Öffentlichkeit gewandt. Um Missbrauch entgegen zu wirken, sollten Gentests nur durchgeführt werden, wenn die Betroffenen wirksam eingewilligt haben oder wenn eine gesetzliche Ermächtigungsgrundlage dies erlaubt.

Da auch in Bremen durch zwei Institute Vaterschaftstests auf der Grundlage vergleichender DNA-Analysen erstellt werden, habe ich diese hinsichtlich der Beachtung von datenschutzrechtlichen Grundsätzen bei privaten wie auch durch Gericht beschlossenen Vaterschaftstests einer Prüfung unterzogen.

Soweit ein gerichtlich beauftragtes Abstammungsgutachten erstellt wird, ersetzt die gerichtliche Entscheidung die Einwilligung. Bei privat initiierten Gutachten erfolgt die Probenentnahme i. d. R. beim Hausarzt oder beim Gesundheitsamt. Das Einverständnis der sorgeberechtigten Elternteile mit der Durchführung der Untersuchung ist auf einem Antragsformular dokumentiert bzw. es erfolgt vor der Untersuchung eine Identitätsfeststellung der betroffenen Personen. Hinsichtlich der informationstechnischen Verarbeitung der Stamm- und Analysedaten hatte ich qualitative Verbesserungen zur Passwortgestaltung, zum Einsatz von Verschlüsselungsverfahren für die Speichermedien und zum Einsatz sicherer Löschfunktionen gefordert. Gefährdungen der Datensicherheit durch externe Angriffe waren in beiden Instituten nicht gegeben, da keine der dafür erforderlichen Schnittstellen zur Verfügung stand.

10.5 Zugriff der Strafverfolgung auf E-Mail

Am 17. Januar 2005 hat das Amtsgericht Bremen (Az. 92 Gs 54/2005) entschieden, dass eine Durchsuchung von privaten Dateien auf einem Dienstrechner eines Polizeibeamten rechtswidrig gewesen ist. Dieses Verfahren habe ich im Hinblick auf Auswirkungen auf die für die bremische Verwaltung geltende E-Mail-Richtlinie (Richtlinie für die Nutzung der Elektronischen Post [E-Mail] vom 7. März 2002) besonders interessiert verfolgt. Der einer Unterschlagung Beschuldigte hatte die Durchsuchung einer passwortgeschützten Datei im Bereich ODDSET-Wetten erlaubt, um seine Spielsucht in dem Strafverfahren zu dokumentieren. Im Rahmen der Durchsuchung war der System-Administrator auf weitere private passwortgeschützte Dateien mit pornografischen Inhalten gestoßen und hatte diese sichergestellt. Der Beschuldigte legte Beschwerde gegen die Beschlagnahme und Einsicht seiner privaten E-Mail-Verläufe und E-Mail-Inhalte ein und begehrte eine richterliche Entscheidung. Das Amtsgericht stellte fest, dass die Durchsicht der Dateien nur durch die Staatsanwaltschaft bzw. auf deren Anordnung durch ihre Ermittlungspersonen hätte erfolgen dürfen. Das Landgericht Bremen (Az. 11 Qs 112/2005) bestätigte die Entscheidung des Amtsgerichts und stellte darüber hinaus fest, dass gemäß § 105 Abs. 1 Strafprozessordnung (StPO) eine richterliche Anordnung für die Sichtung der privaten Dateien notwendig gewesen wäre, da der Beschuldigte lediglich in die Sichtung „ODDSET" eingewilligt hatte. Eine richterliche Anordnung sei auch dann nicht entbehrlich, wenn die private Nutzung des Rechners und E-Mail-Anschlusses vom Dienstherrn untersagt ist. Eine dienstanweisungswidrige Nutzung soll den besonderen strafprozessualen Schutz vor Zugriffen ohne vorherige richterliche Anordnung nicht aufheben.

11. Gesundheit und Krankenversicherung

11.1 Überprüfung des Hilfesystems für psychisch Kranke

Im 27. Jahresbericht berichtete ich unter Ziff. 8.4 über das Vorhaben des Senators für Arbeit, Frauen, Gesundheit, Jugend und Soziales, das Hilfesystem für psychisch Kranke evaluieren zu lassen. Diese Untersuchung steht veranlasst im Zusammenhang mit bei einem Tötungsdelikt vermuteten organisatorischen Mängeln im Hilfesystem.

Nach ersten Gesprächen ruhte das Vorhaben, da man sich nicht auf den in Aussicht genommenen Gutachter einigen konnte. Ende Juli des Berichtsjahres wurde ich darauf aufmerksam, dass nunmehr mit der Datenübermittlung von den Kliniken an ein

privates Unternehmen aus Göttingen, worauf man sich offenbar inzwischen geeinigt hatte, begonnen werden sollte. Ich drang darauf, die Datenübermittlung bis zur Klärung der datenschutzrechtlichen Voraussetzungen auszusetzen. Im Raum standen Fragen des Arbeitnehmer- und Patientendatenschutzes, da zunächst nicht bekannt war, ob die Daten personenbezogen übermittelt werden sollten. Ich bat um die Vorlage des zwischen dem Gesundheitsressort und dem privaten Unternehmen geschlossenen Vertrages, da es sich um einen Fall der Auftragsdatenverarbeitung handelte, bei dem der Auftraggeber für die Einhaltung der datenschutzrechtlichen Bestimmungen verantwortlich ist. Der mir vorgelegte Vertrag enthielt zunächst keine ausreichenden Bestimmungen zum Datenschutz.

Im weiteren Verlauf wurde deutlich, dass es für die Untersuchung ausreichen würde, nur anonymisierte Datensätze zu übermitteln. Die zur Übermittlung vorgesehen Datenkategorien wurden mir zur Verfügung gestellt. Nach einigen kleineren Änderungen konnte verifiziert werden, dass sich die Daten nicht auf die betreffenden Personen beziehen ließen, sie also tatsächlich anonymisiert waren. Damit war meinem Anliegen Genüge getan.

11.2 Neues zur elektronischen Gesundheitskarte

Seit März 2005 liegt die durch das Fraunhofer-Institut für Software- und Systemtechnik (ISST) für die elektronische Gesundheitskarte (eGK) entwickelte „Spezifikation der Lösungsarchitektur zur Umsetzung der Anwendungen der eGK“ vor. Dahinter verbirgt sich die technische Beschreibung des gesamten Projekts in allen Ebenen. Nun sind die Selbstverwaltung (Spitzenverbände der Krankenkassen, Kassenärztliche Bundesvereinigung, Bundesärztekammer, Deutsche Krankenhausgesellschaft und Spitzenorganisation der Apotheker) und deren Betreibergesellschaft Gematik GmbH (Gesellschaft für Telematik) gefordert, über die Vorschläge zur Lösungsarchitektur zu entscheiden.

Da Bremen frühzeitig sein Interesse bekundet hat, im Rahmen eines Modellprojekts die Karte zu testen, habe ich dem Rechtsausschuss der Bürgerschaft (Landtag) im Herbst des Berichtsjahres die verschiedenen Phasen der Einführung der Anwendungen der eGK vorgestellt und insbesondere die gesetzlichen Vorgaben hinsichtlich der verpflichtenden und der freiwilligen Anwendungen erläutert. Als Pflichtanwendungen sind nur das elektronische Rezept und der europäische Versichertennachweis vorgesehen; alle anderen Anwendungen werden freiwillig und auf Einwilligungsbasis zur Verfügung stehen (vgl. 27. JB, Ziff. 8.7). Wie auch immer die technische Umsetzung im Einzelnen ausgestaltet sein wird, wichtig ist, dass sich die Verfügungsbefugnisse der Versicherten über ihre Gesundheitsdaten durch die Einführung der eGK nicht verschlechtern. Außerdem muss gewährleistet sein, dass die Vorgaben des § 6 c Bundesdatenschutzgesetz (BDSG) gewahrt werden, der ausdrücklich auf die eGK anwendbar ist; d. h., die Versicherten sind spätestens mit der Aushändigung der neuen Karte über die Funktionsweise des Mediums und über das Verfahren zu informieren, auch darüber, wie sie erfahren können, bei welcher Stelle welche Daten gespeichert und verarbeitet werden, welche sonstigen Rechte sie haben und über die zu treffenden Maßnahmen bei Verlust oder Zerstörung der Karte. Es müssen also ein Höchstmaß an Transparenz geschaffen und die Versicherten in die Lage versetzt werden, die ihnen gesetzlich garantierten Rechte auch tatsächlich in der Praxis wahrnehmen zu können.

Im vierten Quartal 2005 sollten Kartenanwendungen in ausgewählten Modellregionen getestet werden. Die unterschiedlichen Auffassungen zwischen der Gematik GmbH und der Selbstverwaltung über die Umsetzung der datenschutzkonformen vorgenannten Spezifikation führte zu einer erheblichen zeitlichen Verzögerung. Weil der Zeitplan zur Fertigstellung des Kriterienkatalogs für die Testphase und die Vorstellung der Auswahlkriterien für Testregionen nicht eingehalten wurde, hat das damalige Bundesministerium für Gesundheit und Soziale Sicherung (BMGS) der Gematik GmbH eine Vielzahl von Weisungen erteilt, deren Gesamtanforderungen die gesetzlichen Vorgaben zum Funktionsumfang der Karte und insbesondere zum Datenschutz berücksichtigen müssen. Dies hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder in ihrer Entschließung ausdrücklich begrüßt (vgl. Ziff. 19.1 dieses Berichts).

Darüber hinaus hat das damalige BMGS anstelle der notwendigen Beschlüsse der Gesellschaft Mitte Oktober 2005 den Entwurf einer Rechtsverordnung (VO-E) über Testmaßnahmen für die Einführung der eGK nach § 291 b Abs. 4 Satz 4 SGB V vorgelegt. Leider sieht der VO-E keine Tests datenschutzrechtlicher Aspekte vor.

In § 2 Satz 2 VO-E wird die Sicherstellung des Datenschutzes lediglich als allgemeines Ziel angegeben. Nur in der Begründung zu § 3 des VO-E wird auf allgemeine Dienste zur Gewährleistung von Datensicherheit, Datenschutz und Rechtemanagement hingewiesen und nur allgemein erwähnt, dass die Komponenten und Dienste der Telematikinfrastruktur auch in einer Konfiguration nutzbar sein sollen, in der der Versicherte sein informationelles Selbstbestimmungsrecht wahrnehmen kann.

Aufgrund dessen habe ich die senatorische Behörde unter Hinweis auf die konkreten Vorgaben des § 291 a SGB V gebeten, sich auf Bundesebene für die zwingende Einbeziehung insbesondere folgender Testgegenstände in die Verordnung einzusetzen:

— Einwilligung der versicherten Person und ihre Dokumentation auf der Karte, ihre Widerruflichkeit und ihre Beschränkung auf einzelne Anwendungen,

— technische Vorkehrungen zur Zugriffs-Autorisierung durch die versicherte Person,

— Einbeziehung des elektronischen Arztbriefes, der elektronischen Patientenakte und des Patientenfaches.

Ohne Berücksichtigung dieser konkreten Vorschläge ist die Verordnung über Testmaßnahmen für die Einführung der elektronischen Gesundheitskarte (VOeGK) vom 2. November 2005 (BGBl. I S. 2128) in Kraft getreten.

Ende des Jahres 2005 hat das Bundesgesundheitsministerium (BGM) u. a. Bremen zur Testregion erklärt. Integraler Bestandteil der seinerzeitigen Bewerbung Bremens ist nach Aussage des Gesundheitsressorts eine datenschutzrechtliche und -technische Begleitung. Ich habe meine generelle Bereitschaft erklärt, die Testphase in Bremen zu begleiten, gleichzeitig aber darauf hingewiesen, dass meine derzeitigen personellen Ressourcen nicht ausreichen, um eine verantwortliche und angemessene Begleitung sicherzustellen und gebeten, dafür eine Unterstützung aus Projektmitteln einzuplanen.

11.3 Mammographie-Screening

Mit dem Übergang des Bremer Modellprojektes zur Brustkrebsfrüherkennung (Mammographie-Screening) in die Regelversorgung der Gesetzlichen Krankenkassen (vgl. 27. JB, Ziff. 8.5) wird die für das Modellprojekt entwickelte Software abgelöst. Die neue Software „MaSc“ wurde in Bremen im Dezember 2005 in der Zentralen Stelle beim Gesundheitsamt Bremen, das für das Einladungswesen für die Länder Bremen und Niedersachsen zuständig ist, als Pilotbetrieb mit Echtdaten in Betrieb genommen. Bei der Umstellung auf die neue Software bin ich bestrebt, das damals erreichte Datenschutzniveau aus dem Modellprojekt zu erhalten (vgl. insb. 24. JB, Ziff. 8.3).

Um dies bewerten zu können, habe ich im Rahmen der Verfahrensbeschreibung nach § 8 Abs. 1 Nr. 7 Bremisches Datenschutzgesetz (BremDSG) ein Sicherheitskonzept gefordert. Darin soll insbesondere deutlich werden, wie die Anwendung mit den sicherheitskritischen Daten gegenüber anderen Komponenten (beispielsweise zentrale Komponenten auf der Ebene der Infrastruktur des Netzes des Gesundheitsamtes) geschützt wird und wie die Daten innerhalb der Anwendungssoftware selbst (beispielsweise durch die Zugriffslogik) abgesichert werden. Dieses Sicherheitskonzept soll konkret die Implementierung entsprechender Sicherheitsdienste beschreiben. Darüber hinaus muss die Verantwortlichkeit für den Betrieb des Systems und insbesondere der Sicherheitskomponenten (Funktionsprüfung, Fehlerbehandlung, Aktualisierung etc.) definiert werden (Sicherheitsmanagement). Hierzu gehört auch der Aufbau einer Revision, deren Voraussetzung eine Protokollierung sensibler Aktionen innerhalb der Anwendung ist. Auch die Migration der Altdaten in das neue System muss nach datenschutzrechtlichen Vorgaben erfolgen.

Eine wesentliche Datenschutzanforderung aus dem Modellprojekt ist die Anonymisierung der Daten der Frauen gewesen, die auch nach einer Nacheinladung zum Screening nicht teilgenommen oder der Speicherung der Daten widersprochen haben. Die Identitätsdaten dieser Personengruppen müssen nach erfolglosem Einladungsverfahren anonymisiert werden.

Auch die Datenverarbeitung im Rahmen des Mammographieprojektes verlangt die Anonymisierung von Daten. Sensible medizinische Daten frühzeitig zu anonymi-

sieren und damit verbunden der Schutz der Identitätsdaten, ist für die Nutzung zu Forschungszwecken unabdingbar (z. B. §§ 6 Abs. 2, 7 Abs. 3 - 5 bremisches Krebsregistergesetz – BremKRG). Hierfür ist die Bildung einer eindeutigen, lebenslang geltenden „Screening-ID“ vorgesehen, die nach einem bestimmten Hash-Algorithmus (ein Programm, das einen Wert berechnet, der ein Objekt eindeutig charakterisieren kann) gebildet wird. Der berechnete Wert (ein Code) lässt sich nicht auf die Ursprungsdaten zurückrechnen. Allerdings ergibt sich aus den gleichen Grunddaten (Vornamen, Familienname, frühere Familiennamen einschließlich Geburtsname, Geburtsdatum, Geburtsort und Anschrift) immer der gleiche Hashwert. Das bedeutet, dass bei erneuter Berechnung des Wertes aus den Grunddaten durch Vergleich eines berechneten neuen Wertes mit einem vorhandenen alten Wert die Identifizierung der einzelnen betroffenen Frauen möglich ist.

Dieses Problem verschärft sich durch die Zusammenlegung des epidemiologischen Bremer Krebsregisters mit dem klinischen Register (vgl. Ziff 11.4 dieses Berichts) und dem geplanten anonymisierten Abgleich im Rahmen des neuen Verfahrens mit dem Bremer Krebsregister. In den mir bereits zur Verfügung gestellten Unterlagen sind Datensätze beschrieben, in denen die im Rahmen der Anonymisierung beim Krebsregister vergebene Kontrollnummer zusammen mit der korrespondierenden Screening-Nummer verarbeitet werden soll. Das hätte zur Folge, dass auch die als sicherer geltende Kontrollnummer wieder mit den dahinterstehenden Identitätsdaten verbunden werden kann, wofür insbesondere nach § 4 Abs. 4 BremKRG hohe Hürden vorgesehen sind. Die Zentrale Stelle des Gesundheitsamtes hat deshalb Bereitschaft signalisiert, in den bundesweiten Gremien auf eine Änderung des Aufbaus der Screening-ID hinzuwirken, um eine Re-Identifizierung auszuschließen.

Insgesamt werden die durch die Vernetzung der unterschiedlichen Institutionen und damit verbunden die wachsende Komplexität der Systeme immer höhere Anforderungen an die technischen Maßnahmen, Anforderungen zur Anonymisierung der Daten und die Abbildung des Willens der Betroffenen (Einwilligung, Widerspruch, Ablehnung des gesamten Verfahrens aus frauen- und gesundheitspolitischen oder anderen Gründen) gestellt. Es wird zunehmend schwieriger, die dafür erforderliche Transparenz herzustellen, da die einzelnen Verfahren nicht mehr nur getrennt, sondern auch in ihren vielfältigen Verknüpfungen betrachtet werden müssen.

11.4 Tumordokumentationszentrum

Die Ärztekammer Bremen hat mir ein Konzept für die Errichtung eines Tumordokumentationszentrums Bremen (TDZB) vorgestellt. Danach sollen die Aufgaben des epidemiologischen Krebsregisters mit denen des klinischen Krebsregisters zusammengefasst und eine gemeinsame Datenannahmestelle geschaffen werden. Wesentliche Ziele sind die Abbildung des gesamten Behandlungsverlaufs zu einem Patienten, Rückmeldungen über den Krankheitsverlauf an den betreuenden Arzt und Zusammenarbeit mit wissenschaftlichen Einrichtungen, die Forschung über die Verursachung von Krebserkrankungen sowie Diagnostik und Therapie betreiben.

Vorgesehen ist, dass der erste betreuende Arzt einer Krebserkrankung einen so genannten Nachsorgekalender mit einer Nummer an den Patienten ausgibt. Diese Kalendernummer soll als Zuordnungskriterium für die Meldungen an die Datenannahmestelle dienen; daneben sollen Name und Geburtsdatum des Patienten an das TDBZ übermittelt werden.

Bei der Aushändigung des Nachsorgekalenders soll der Arzt den Patienten über die Meldung an das dann gemeinsame Register informieren und ihn nun auf sein Widerspruchsrecht hinweisen. Nach dem Konzept gilt ein nicht erfolgter Widerspruch als (mündliche) Einwilligung.

Ob die im Konzept nicht näher erläuterte Überschaubarkeit des Datenschutzes für den Patienten tatsächlich eine Verbesserung oder Verschlechterung des Datenschutzes darstellt, bedarf einer gründlichen Prüfung. Insbesondere hätte ich erhebliche Bedenken, wenn sich die jeweils unterschiedlichen Zwecke des Krebsregisters und des epidemiologischen Registers vermischten und insoweit dem Grundsatz der Zweckbindung widersprächen.

Es bedarf noch weiterer Überlegungen, weil das derzeit vorgesehene Verfahren (Widerspruchslösung) zur Übermittlung der Gesundheitsdaten an das TDZB nicht den Anforderungen an eine wirksame Einwilligung in die Übermittlung besonderer Arten von Daten nach § 3 Abs. 3 und 4 i. V. m. § 3 Abs. 2 Nr. 2 Bremisches Da-

tenschutzgesetz (BremDSG) erfüllt. Nach diesen Vorschriften muss sich die Einwilligung ausdrücklich auf die Gesundheitsdaten beziehen und sie muss schriftlich erfolgen. Die noch vorgesehene Widerspruchslösung beinhaltet nicht gleichzeitig eine Einwilligung; diese setzt insbesondere das positive Einverständnis voraus.

Aus technischer Sicht ist eine Konzentration von in der Vergangenheit getrennt verarbeiteten Daten zu beobachten. Ursprüngliches Ziel war sicherzustellen, dass in die Persönlichkeitsrechte der Betroffenen durch die Einrichtung eines Bremer Krebsregisters nur soweit unbedingt erforderlich eingegriffen wird.

Die im Rahmen des bremischen Krebsregisters (BremKRG) erhobenen und verarbeiteten Daten wurden deshalb bisher streng getrennt in voneinander abgeschotteten Netzen der Registerstelle und der Vertrauensstelle verarbeitet (vgl. 20. JB, Ziff. 14.1 und 21. JB, Ziff. 8.1). Es wurde neben der edv-technischen Abschottung zunächst darauf geachtet, dass beide Stellen des Bremer Krebsregisters auch organisatorisch und personell voneinander getrennt waren. Die Kommunikation zwischen beiden Netzen erfolgte unter hohen Sicherheitsanforderungen und unter besonderem Schutz der Identitätsdaten bei der Vertrauensstelle. Die strikte Trennung dieser beiden Stellen wurde in der Zwischenzeit aufgehoben. Vertrauens- und Registerstelle stehen nunmehr unter einer Leitung (vgl. Ziff. 11.5 dieses Berichts) und befinden sich beide in den Räumlichkeiten des Bremer Instituts für Präventionsforschung und Sozialmedizin (BIPS). Für die Trennung der elektronischen Verarbeitung der Daten wurden besondere Bedingungen ausgehandelt (vgl. 27. JB, Ziff. 8.6)

Eine weitere strenge Trennung bestand zunächst zwischen den Daten der Vertrauensstelle des Bremer Krebsregisters (epidemiologisches Register) und der Nachsorgeleitstelle (klinisches Register). Dadurch konnte auf technischer Ebene garantiert werden, dass die unterschiedlichen Meldevoraussetzungen berücksichtigt wurden.

Es wurde jedoch in der Praxis sehr schnell deutlich, dass sich die in die Systeme einzugebenden Daten häufig überschnitten haben. Aus Effektivitätsgründen wurde daher von beiden Stellen ein Konzept für eine zentrale Eingabestelle entwickelt. Auf der Ebene der elektronischen Verarbeitung der eingegebenen Daten wurde in Absprache mit mir sichergestellt, dass die rechtlich gebotene Trennung der Datenbestände auf logischer Ebene abgebildet wurde (vgl. 26. JB, Ziff. 8.2.1).

Die neuerlich geplante Zusammenfassung des epidemiologischen und klinischen Krebsregisters zu einem Tumordokumentationszentrum stellt die EDV-Technik erneut vor die Aufgabe, auf logischer Ebene weiterhin die rechtlich zwingend gebotenen Trennungen der Datenbestände zu garantieren.

Ich habe daher zunächst ein Sicherheitskonzept (Verfahrensbeschreibung nach § 8 BremDSG) angefordert, in dem detailliert die technischen und organisatorischen Maßnahmen (§ 7 BremDSG) beschrieben werden. Hier müssen auf verschiedenen Systemebenen über die Zugriffslogik und die Sicherheitsfunktionen (Verschlüsselung, Authentifizierung etc.) angemessene Sicherheitsmaßnahmen beschrieben werden.

Im Wesentlichen werden diese Maßnahmen davon abhängen, an welcher Stelle und wie sicher die zu verarbeitenden sensiblen personenbezogenen Daten anonymisiert bzw. pseudonymisiert werden. Von besonderer Bedeutung sind die geplanten, für die Identifizierung einzelner Datensätze zu vergebenden Nummern. Hier ist genau zu definieren, ob und mit welchen Funktionen diese Nummern in den jeweiligen Organisationseinheiten Verknüpfungen mit Identitätsdaten ermöglichen.

Grundsätzlich ist es datenschutzrechtlich immer schwieriger und weniger wirkungsvoll, auf ein zentrales System die rechtlich gebotenen Einschränkungen abzubilden, als mit getrennten Netzen zu arbeiten. Die Gespräche über die Lösungsarchitektur sollen in 2006 fortgesetzt werden.

11.5 Änderung des Krebsregistergesetzes

Ich berichtete über den Umzug der Vertrauensstelle des Bremer Krebsregisters in das Gebäude des Bremer Instituts für Präventionsforschung und Sozialmedizin (BIPS), wo das epidemiologische Krebsregister Bremens geführt wird (vgl. 27. JB, Ziff 8.6). Dabei war wichtig, durch technische Maßnahmen sicherzustellen, dass die im bremischen Krebsregistergesetz (BremKRG) vorgeschriebene räumliche, personelle und organisatorische Trennung beider Stellen gewahrt bleibt.

In der Folgezeit wurde die Leitung der Vertrauensstelle vakant. In Ermangelung einer anderweitigen Lösungsmöglichkeit wurde zunächst der Leiter der Registerstelle als kommissarischer Leiter der Vertrauensstelle eingesetzt. Dabei machte ich deutlich, dass dies nur eine vorübergehende Lösung sein könne und drang darauf, baldmöglichst einen Zustand herzustellen, der mit der Regelung im Krebsregistergesetz in Einklang steht, denn das Gesetz sieht die personelle Trennung vor, die durch die Doppelbesetzung der Leitung von Vertrauens- und Registerstelle nicht mehr gegeben war.

Da anscheinend keine andere Leitung für die Vertrauensstelle gefunden werden konnte, suchte der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales die Lösung des Problems in der Änderung des bremischen Krebsregistergesetzes. Es sollte die aus Sicht des Datenschutzes wichtige personelle Trennung aufgegeben werden. Bedeutsam war die Festschreibung der Trennung deshalb, weil sie gewährleistete, dass keine Verbindung zwischen der Stelle bestand, die mit den pseudonymisierten, epidemiologischen Daten forschte und derjenigen, die die personenbezogenen Daten vorhielt. Obschon ich meine grundsätzlichen Bedenken hinsichtlich der Aufgabe der Trennung vortrug, wurde an der Gesetzesänderung gearbeitet. Ich versuchte daher, auf den Gesetzeswortlaut Einfluss zu nehmen.

Leider konnte ich nicht erreichen, dass in § 1 Abs. 3 Satz 2 BremKRG, mit dem die gemeinsame Leitung von Vertrauens- und Registerstelle von der Trennung ausgenommen wird, folgender neuer Satz 3 angefügt wird: „Grundsätzlich hat die gemeinsame Leitung kein Recht auf Einsicht in personenbezogene Daten." Immerhin gelang es mir, dass dies Eingang in die Gesetzesbegründung fand und dort verdeutlicht wurde, dass nur ausnahmsweise in rechtlich begründeten Einzelfällen, wie etwa Patientenbeschwerden, die Einsichtnahme durch die Leitung möglich sein soll. Die Gesetzesänderung ist durch Gesetz vom 28. Juni 2005 (Brem.GBl. S. 306, 307) in Kraft getreten.

11.6 Rechtswidrige Datenübermittlung durch zwei Krankenkassen

Die AOK Bremen/Bremerhaven und die Handelskrankenkasse (HKK) haben unzulässigerweise sensible Gesundheitsdaten an das damalige Bundesministerium für Wirtschaft und Arbeit (BMWA) und die Bremer Sozialzentren übermittelt.

Hintergrund ist die schwierige Einordnung Hilfebedürftiger in das System des 2. Buchs Sozialgesetzbuch (SGB II Arbeitslosengeld II) oder das des 12. Buchs Sozialgesetzbuch (SGB XII Sozialhilfe). Diejenigen, die Arbeitslosengeld II erhalten, also mindestens vier Stunden täglich arbeitsfähig sind, werden in der Gesetzlichen Krankenversicherung nach § 5 Abs. 1 Nr. 2 a 5. Buch Sozialgesetzbuch (SGB V) pflichtversichert. Für Menschen, die nicht arbeitsfähig sind, wird die Krankenbehandlung nach § 264 SGB V im Bedarfsfall von den Krankenkassen übernommen, denen die dafür entstandenen Aufwendungen von den Trägern der Sozialhilfe erstattet werden.

Die Krankenkassen haben ein wirtschaftliches Interesse daran, dass nur diejenigen pflichtversichert werden, die tatsächlich in das System des SGB II einzuordnen sind, um die Belastung der Versichertengemeinschaft gering zu halten. Dieses Problem haben die Kassen offenbar dem BMWA vorgetragen, denn von dort wurden die Kassen gebeten, Zweifelsfälle bei der Einordnung Versicherter aufzuzeigen.

Dieser Aufforderung sind die AOK Bremen/Bremerhaven und die HKK in der Weise nachgekommen, dass sie Listen mit Namen, Anschriften, Geburtsdaten und kasseneigenen Kurzdiagnosen bzw. Kurzbegründungen, aus denen Diagnosen abgeleitet werden können, an das Ministerium und an die Bremer Sozialzentren versandten. In den Listen waren Angaben wie „ist Alkoholiker", „Methadon-Substitution", „bösartiger Tumor", „psychische Verhaltensstörung", „Hepatitis C", „Schlaganfall", „Multimorbidität", „schwerwiegende chronische Erkrankung" enthalten. Sie sollten Aufschluss über die aus Sicht der Kasse mangelnde Arbeitsfähigkeit geben.

In Bezug auf die Datenübermittlung an die Sozialzentren beruft sich die AOK darauf, die Übermittlung von Zweifelsfällen an die zuständigen Sozialzentren sei nach § 69 Abs. 1 Nr. 1 SGB X erforderlich gewesen.

Das ist jedoch nicht zutreffend. Es hätten nur Namen und Anschriften der Personen an die Sozialzentren übermittelt werden dürfen. Die Sozialbehörden hätten

dann im Rahmen ihrer gesetzlichen Aufgaben nach § 44 a SGB II feststellen können, ob die benannten Personen als arbeitsfähig einzustufen sind oder nicht. Die Angabe von einzelnen Diagnosen war dagegen regelmäßig nicht zur Klärung von Zweifeln über die Zuordnung der Einzelfälle erforderlich.

Die Datenübermittlung an das BMWA hat die AOK auf meine kritischen Nachfragen als unzulässig bewertet. Ihr gegenüber hatte sich das BMWA auf seine gesetzliche Aufsicht über die Bundesagentur für Arbeit (BA) nach § 47 Abs. 1 SGB II und Verwaltungsvereinbarungen mit den zugelassenen kommunalen Trägern gestützt. Danach sei die AOK verpflichtet, dem BMWA auf Anforderung zeitnah Auskünfte zu erteilen und Unterlagen vorzulegen, die eine Beurteilung ermöglichen, ob Aufwendungen des Bundes zu tragen sind.

Auch diese Auffassung ist nicht zutreffend. Da die Krankenkassen sämtliche Einzelfälle bilateral mit den örtlich zuständigen Sozialbehörden abarbeiten, halte ich es für höchst unwahrscheinlich, dass alle Einzelfälle im Bundesgebiet auch noch durch das BMWA parallel dazu überprüft werden. Nach allem wäre es völlig ausreichend gewesen, wenn das BMWA lediglich anonyme bzw. aggregierte Daten über die seiner Aufsicht unterliegende BA bei den Verbänden der Krankenkassen angefordert hätte. Die Übermittlung von personenbezogenen Einzeldaten war dagegen nicht erforderlich.

Den Bundesbeauftragten für den Datenschutz habe ich gebeten, diese Haltung dem nunmehr zuständigen Bundesministerium für Arbeit und Soziales darzulegen und mich über das Ergebnis seiner Bemühungen zu unterrichten.

Inzwischen hat mich der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales um Stellungnahme gebeten, weil er eine aufsichtsbehördliche Bewertung vornehmen möchte. Ich habe auch ihm meine Auffassung hierzu dargelegt und ihn gebeten, die Rechtslage in seiner Bewertung zu berücksichtigen.

12. Arbeit und Soziales

12.1 Datenerhebung bei Arbeitslosengeld-II-Empfängern durch Call-Center

Ein Bürger wandte sich an mich, der in Bremen Arbeitslosengeld II (ALG II) bezieht und von einem Call-Center in Rostock angerufen und um die Angabe von Sozialdaten gebeten wurde. Erst auf Nachfrage sei ihm erklärt worden, dass der Anruf im Auftrag der Bundesagentur für Arbeit (BA) erfolge und man sich durch die Nennung der Bedarfsgemeinschaftsnummer legitimieren könne. Der Betroffene war erstaunt, dass das Call-Center tatsächlich über seine Bedarfsgemeinschaftsnummer verfügte. Seine Sozialdaten wollte er aber nicht am Telefon preisgeben. Ein Hinweis darauf, dass die Angabe von Daten freiwillig sei, erfolgte nicht, vielmehr wurde ihm gegenüber auf etwaige Nachteile bei der Antragsbearbeitung hingewiesen, wenn die Angaben nicht gemacht würden.

Meine Nachforschungen ergaben, dass die BA einen Auftrag über eine telefonische Outbound-Aktion zur Erhebung von ALG-II-Daten an die T-Systems International GmbH vergeben hatte. Den Mitarbeitern in den Call-Centern stehe ein Gesprächsleitfaden zur Verfügung, dem zu entnehmen sei, dass zu Anfang des Gesprächs auf die Freiwilligkeit hinzuweisen sei. Da dies offenbar auf diese Weise nicht gewährleistet werden kann, forderte der zuständige Bundesbeauftragte für den Datenschutz (BfD) die BA auf, die telefonische Datenerhebung auszusetzen, bis die Betroffenen eine schriftliche Information über das Vorhaben erhalten haben. Die Arbeitsgemeinschaften im Land Bremen beteiligen sich ebenfalls an der Call-Center-Aktion auf der Basis des Gesprächsleitfadens.

Neben grundsätzlichen Bedenken, die ich nachfolgend schildere, ist es dringend erforderlich, dass bei solchen Unternehmungen sichergestellt ist, dass die Betroffenen tatsächlich darüber informiert sind, dass es ihnen überlassen ist, ob sie am Telefon Angaben machen oder diese Angaben lieber gegenüber der BAgIS machen, und dass ihnen keinerlei Nachteile daraus entstehen, wenn sie dies nicht tun (vgl. dazu auch die Entschließung der 70. Konferenz zu „Telefonbefragungen von Leistungsbezieherinnen und Leistungsbeziehern von Arbeitslosengeld II datenschutzgerecht gestalten“ unter Ziff. 19.5 dieses Berichts).

Ende November 2005 hat der BfD den Datenschutzbeauftragten der Länder ein „Konzept zur Einrichtung eines Contact Centers SGB II“ der BA zugesandt; zu dem Stellung genommen wurde.

Nach dem Konzept ist zwar vorgesehen, dass Telefonanrufe durch das Contact Center (CC) vorher schriftlich angekündigt werden sollen. Gleichwohl bestehen erhebliche Zweifel, ob der Angerufene zweifelsfrei erkennen kann, dass der Anrufer tatsächlich im Auftrag der BA anruft. Daher sollte sich der Angerufene regelmäßig die entsprechende Gewissheit verschaffen, z. B. durch Ankündigung und Anzeige der zur Befragung genutzten Telefonnummer oder Mitteilung eines Codewortes.

Eine Verbesserung dürfte sein, dass dem Betroffenen nunmehr schriftlich erklärt wird, dass die telefonische Datenerhebung freiwillig ist. Es ist vorgesehen, dass der Betroffene bei einer Nichtteilnahme eine Einladung von der zuständigen Sozialbehörde erhält. Zumindest sollte in dem Ankündigungsschreiben auf diese Möglichkeit hingewiesen werden und ihm die Wahl eingeräumt werden, die entsprechenden Fragen der zuständigen Behörde gegenüber schriftlich zu beantworten, damit dem Grundsatz der Freiwilligkeit der Einwilligung Rechnung getragen wird.

Allerdings ist auf Bundesebene nach Ziffer 2.6 des Koalitionsvertrages zwischen CDU/CSU und SPD vorgesehen, eine gesetzliche Grundlage dafür zu schaffen, dass Leistungsempfänger zur Teilnahme an einer Telefonabfrage verpflichtet werden, in der die aktuellen Lebenssituationen überprüft werden sollen. Dies würde eine neue Qualität der Kontrolle, ggf. sogar eine Rufbereitschaft beinhalten, die aufgrund des Misstrauens gegenüber Telefonbefragungen aller Art einen tiefen Eingriff in das informationelle Selbstbestimmungsrecht des Betroffenen bedeuten würde. Ich bin nicht dagegen, auch der Sachbearbeiterin/dem Sachbearbeiter der BAgIS gegenüber am Telefon einmal Auskünfte zu erteilen. Ich habe aber generelle Vorbehalte gegen eine Auslagerung der Aufgaben zur Erhebung von Sozialdaten durch beauftragte Call-Center. Es darf jedenfalls nicht passieren, dass ein und derselbe Mitarbeiter in einem x-beliebigen Call-Center z. B. Geräteservice macht, Handyverträge verkauft, Kreditauskünfte erteilt und darüber hinaus dem Sozialgeheimnis unterliegende Daten bei ALG-II-Empfängern abfragt.

Ein wesentliches Problem besteht nach wie vor darin, dass alle Mitarbeiter des Call-Centers unmittelbaren Zugriff auf alle Daten aller Fachverfahren haben, weil die Mitarbeiter im Rahmen so genannter telefonischer Sachbearbeitung und „fallabschließend“ Eintragungen vornehmen sollen. Damit würde ein Stand verfestigt, der vom BfD im Jahre 2004 beanstandet worden ist. Der Grundsatz der Erforderlichkeit bei den Zugriffen auch der Call-Center-Mitarbeiter muss genauso gelten wie für die Mitarbeiter der örtlich zuständigen Sozialbehörden, so dass ein datenschutzkonformes Zugriffsberechtigungskonzept umgesetzt werden muss.

Es besteht eindeutig die Gefahr, dass durch die Einschaltung anonymer Call-Center und deren Mitarbeiter ein Stück Entmenschlichung des Verfahrens eintritt, was der Datenschutz allerdings nicht verhindern kann.

12.2 Einsatz des A2LL-Verfahrens bei der BAgIS

Seit dem Beginn des Berichtsjahres besteht die Bremer Arbeitsgemeinschaft für Integration und soziale Sicherung (BAgIS), ein Zusammenschluss der Sozialämter mit der Agentur für Arbeit auf der Grundlage des § 44 b Sozialgesetzbuch (SGB) II. Die BAgIS ist zuständig für die Auszahlung des Arbeitslosengeldes II, zu dessen Berechnung die von der Bundesagentur für Arbeit (BA) bereitgestellte Software A2LL eingesetzt wird (vgl. 27. JB, Ziff. 9.2).

Zwar wurde das Verfahren A2LL von der BA zur Verfügung gestellt, so dass für die Beurteilung grundsätzlicher Datenschutzfragen das Verfahren betreffend der Bundesbeauftragte für den Datenschutz (BfD) zuständig ist; gleichwohl besteht unter den Datenschutzbeauftragten des Bundes und der Länder Einigkeit, dass für den Einsatz des Verfahrens in den Arbeitsgemeinschaften vor Ort den Landesbeauftragten eine Prüfkompetenz zusteht.

Daher habe ich bei der BAgIS (Abteilung Ost II) die örtlichen Gegebenheiten sowie insbesondere die sich aus dem Einsatz der neuen Software ergebenden Datenschutzfragen geprüft.

Zu den örtlichen Gegebenheiten in dem neu bezogenen Gebäude, in dem die BAgIS in Bremen untergebracht ist, war festzustellen, dass zwischen den einzelnen Anmeldebereichen genügend Abstand besteht, um die Wahrung des Sozialgeheimnisses zu gewährleisten; darüber hinaus finden weitergehende Datenerhebungen im Rahmen der Fallberatung in den Räumen der jeweiligen Sachbearbeiter statt.

Zum Zeitpunkt meines Besuchs bei der BAgIS waren die Umbauarbeiten noch nicht abgeschlossen. So war ein Registraturraum, in dem sich die Akten befinden, noch nicht mit abschließbaren Türen versehen, dies ist aber inzwischen geschehen.

Da die von der BA konzipierten Antragsvordrucke für die Erhebung der für die Gewährung des Arbeitslosengeldes II erforderlichen Daten zunächst mangelhaft waren und daher mehr Daten erhoben wurden als erforderlich, stellte sich nun die Frage, wie mit diesen Überschussinformationen umgegangen wird. Denn nach § 84 Abs. 2, 10. Buch Sozialgesetzbuch (SGB X) sind Sozialdaten zu löschen, wenn ihre Speicherung unzulässig ist. Nach Auskunft der BAgIS verbleiben jedoch die zuviel erhobenen Daten in den Akten, da eine nachträgliche Löschung zu aufwändig sei. Selbst wenn man zugesteht, dass ein generelles Durchsuchen der Akten auf Überschussinformationen die Kapazitäten sprengt und die Erhebung dieser Daten letztlich auf den Antragsbogen der BA zurückzuführen ist, so muss doch gefordert werden, dass zuviel – und damit unrechtmäßig – erhobene Daten aus der Akte wenigstens dann entfernt werden, wenn die betreffende Akte wieder bearbeitet wird.

Ein Kritikpunkt an dem Verfahren A2LL war von Beginn an die bundesweite Zugriffsmöglichkeit auf die Daten aller Arbeitsgemeinschaften mit der Funktion „Personensuche bundesweit". Diese Zugriffsmöglichkeit steht auch den Mitarbeitern der BAgIS zur Verfügung und wird laut BAgIS grundsätzlich zur Vermeidung von Doppelmeldungen genutzt. Problematisch daran ist, dass dabei nicht nur der Stammdatensatz der gesuchten Person angezeigt wird, sondern die Anzeige des gesamten Falls möglich ist. Eine Rechtsgrundlage besteht dafür nicht. Daher muss der Zugriff auf die Stammdaten beschränkt werden.

Die BA und das damalige Bundesministerium für Wirtschaft und Arbeit (BMWA) haben zugesagt, die seitens der Datenschutzbeauftragen vorgetragenen Mängel zu beseitigen und somit einen datenschutzkonformen Einsatz des Verfahrens A2LL in den einzelnen Arbeitsgemeinschaften zu ermöglichen.

Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch immer noch keine erkennbaren Fortschritte. Weder ist ein klar definiertes Zugriffskonzept umgesetzt noch erfolgt eine Protokollierung der lesenden Zugriffe. Dies gilt ebenso für das elektronische Vermittlungsverfahren coArb, das auch einen bundesweiten Lesezugriff für die über 40.000 Mitarbeiter der BA und der Arbeitsgemeinschaften nach § 44 b SGB II (ARGE) erlaubt. Dies haben die Datenschutzbeauftragten des Bundes und der Länder beanstandet (vgl. Entschließung der 70. Konferenz zu „Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen" unter Ziff. 19.4 dieses Berichts). Insgesamt bleibt abzuwarten, wie die BA auf die seitens der Datenschutzbeauftragten vorgetragenen Mängel reagiert und somit einen datenschutzkonformen Einsatz des Verfahrens A2LL in den einzelnen Arbeitsgemeinschaften ermöglicht.

12.3 JobCard – der Weg zum „gläsernen Arbeitnehmer"?

Im 27. Jahresbericht (Ziff. 1.10) habe ich die mit der Einführung der JobCard geplanten Ziele und Geschäftsprozesse beschrieben. Die Einführung einer zentralen Speicherstelle (ZSS), in der Arbeits- und Einkommensdaten der abhängig beschäftigten Bevölkerung Deutschlands gespeichert werden sollen, ist auf verfassungsrechtliche Bedenken der Datenschutzbeauftragten der Länder gestoßen. Insbesondere wegen der in diesem Verfahren verbundenen Gefahren einer verfassungsrechtlich unzulässigen Datenvorratsspeicherung, des Missbrauchspotentials und der völlig ungeklärten Zweckbestimmung dieser Datenverarbeitung hat die 70. Konferenz der Datenschutzbeauftragten im Oktober 2005 in seinem Beschluss zum JobCard-Verfahren die Bundesregierung aufgefordert, die verfassungsrechtliche Zulässigkeit der JobCard zu prüfen und das Ergebnis vorzulegen.

Wie bei allen Verfahren, die eine bundesweite zentrale Speicherung von sensiblen personenbezogenen Daten verlangen, muss das Aufsetzen einer logischen technischen Infrastruktur umgesetzt werden. Das bedeutet, dass diese Infrastruktur je nach angestrebtem Verwendungszweck an Erweiterungen jederzeit angepasst werden kann. Darüber hinaus ist ein Missbrauch der zentral gespeicherten Leistungsberechtigungsdaten (trotz Verschlüsselung der Daten auf dem Transportweg und in der zentralen Speicherstelle) technisch nicht auszuschließen.

Anders gesagt: Ohne die zentrale Speicherung der Entgelt- und Beschäftigtendaten wäre der Aufbau dieser komplexen Sicherheitsarchitektur gar nicht erforder-

lich. Dezentrale Systeme könnten für bestimmte Verwendungszwecke zur Verfügung gestellt werden, die Kommunikation mit anderen Systemen müsste explizit definiert und aufgebaut werden.

Ein anderer Vorschlag von der AG JobCard der Datenschutzbeauftragten zur Minimierung der Risiken wäre durch eine Ende-zu-Ende-Verschlüsselung der Beschäftigtendaten im JobCard-Verfahren mit dem Schlüssel der Beschäftigten zu erreichen gewesen. Die Verfügbarkeit der Daten durch Dritte wäre dann direkt an deren Entschlüsselung durch die Betroffenen gekoppelt gewesen. Die Konferenz der Datenschutzbeauftragten hat diesen Vorschlag ihrer Arbeitsgruppe aufgegriffen und das Bundeswirtschaftsministerium gebeten, die Realisierung dieses Konzepts durch einen neutralen Gutachter überprüfen zu lassen.

Das Bundesamt für Sicherheitstechnik (BSI) hat hierzu ein Gutachten erstellt und diese Lösungsvariante als technisch möglich bewertet. Es wird vom BSI jedoch bezweifelt, ob die hohen technischen Anforderungen bei so einem großen Projekt wie der JobCard erfüllbar sind. Als Alternative hierzu soll nun die Ver- und Entschlüsselung der Daten durch eine unabhängige Vertrauensstelle (Teilung der Verantwortlichkeit) erfolgen – sicherlich eine qualitative Verbesserung gegenüber dem bisherigen Weg. Der Nachteil dieser Lösung ist, dass die Betroffenen ihre Verfügungsgewalt über ihre Daten verlieren und die technischen Möglichkeiten eines zentralen Zugriffs bestehen bleiben.

13. Bildung und Wissenschaft

13.1 Datenschutz im Hochschulbereich

Gemäß § 11 Abs. 1 Bremisches Hochschulgesetz (BremHG) dürfen die Hochschulen von Studienbewerbern, Studierenden und weiteren Personen diejenigen personenbezogenen Daten verarbeiten, die u. a. für die Zulassung, Immatrikulation und Teilnahme an Lehrveranstaltungen und Prüfungen erforderlich sind. Die von den Betroffenen anzugebenden Daten und die Zwecke, für die sie verwendet werden dürfen, sind nach dem Bremischen Hochschulgesetz durch Rechtsverordnung zu bestimmen. Seit dem 1. September 1992 sind diese Festlegungen in der „Verordnung über die Verarbeitung von Studentendaten im Hochschulbereich“ getroffen.

Im Jahr 2003 wurde § 11 Abs. 1 BremHG dahingehend geändert, dass nunmehr Studierendendaten auch zum Zwecke der Berechnung des Studienguthabens nach § 109 a BremHG verarbeitet werden dürfen. Die näheren Einzelheiten sind auch insoweit durch Rechtsverordnung zu regeln. Aus diesem Grund ist eine Änderung der bestehenden Verordnung erforderlich.

Die Rechtsverordnung wurde seit ihrem In-Kraft-Treten nicht geändert. Eine Anpassung an die im Laufe der Zeit veränderten tatsächlichen und rechtlichen Verhältnisse ist somit über einen langen Zeitraum unterblieben. Die für die Arbeit der Hochschulen unbestritten notwendige Verarbeitung personenbezogener Daten erfolgt aus diesem Grund z. T. seit langer Zeit ohne hinreichend klare rechtliche Grundlage. Deshalb hat der Senator für Bildung und Wissenschaft (SfBuW) die zur Einführung von Studiengebühren erforderliche Änderung der Verordnung zum Anlass genommen, einen Entwurf für ihre grundlegende Novellierung zu erarbeiten. Es fehlte jedoch die nötige Zeit, um den umfangreichen Entwurf bis zum geplanten In-Kraft-Treten in der gebotenen Ausführlichkeit zu diskutieren und abzustimmen. Außerdem hat sich gezeigt, dass viele der Regelungen in dem Verordnungsentwurf nicht mit § 11 BremHG im Einklang stehen, der seinerseits demnächst im Zuge der anstehenden Novellierung des Bremischen Hochschulgesetzes geändert werden soll. Das Wissenschaftsressort ist daher meiner Empfehlung gefolgt, die Neufassung der Verordnung zunächst zurückzustellen und eine grundlegende Überarbeitung zusammen mit der Änderung des Bremischen Hochschulgesetzes vorzunehmen. Allerdings ist entscheidend, dass dies bald in Angriff genommen wird, um schnellstmöglich alle notwendigen Datenverarbeitungsprozesse an den Hochschulen auf eine hinreichende rechtliche Grundlage zu stellen.

13.2 Stipendienprogramm „Start“

Die Gemeinnützige Hertie-Stiftung hat in verschiedenen Bundesländern, so auch in Bremen, ein Stipendienprogramm für begabte und engagierte Zuwandererkinder aufgelegt. Im Rahmen des Bewerbungsverfahrens sollte u. a. ein Formular vom Be-

werber ausgefüllt werden zur Prüfung, ob der ökonomische Familienhintergrund es nicht erlaubt, die mit dem Stipendium verbundenen Leistungen der Förderung selbst zu finanzieren. Hierzu wurde eine Vielzahl von Daten verlangt. So hielt ich es u. a. nicht für erforderlich, dezidiert die Geburtstage und ggf. den Todestag eines Elternteils zu erheben. Es reicht aus, wenn – wie bei den Geschwistern – nur nach dem Alter des Vaters und der Mutter und ggf. nach dem Todesjahr gefragt wird. Nach Rücksprache mit dem zuständigen Vertreter der Gemeinnützigen Hertie-Stiftung sind meine Änderungsvorschläge vollständig übernommen worden.

13.3 Novellierung des bremischen Schuldatenschutzgesetzes

In meinem 27. Jahresbericht habe ich unter Ziffer 10.3 die wesentlichen Neuerungen im Arbeitsentwurf zur Novellierung des bremischen Schuldatenschutzgesetzes (BremSchulDSG) dargelegt, und zwar die Einbeziehung der Privatschulen, die automatisierte Verarbeitung von Schülerdaten, die Datenverarbeitungsregelung im Gesetz und zum Datenkatalog per Rechtsverordnung, die Datenverarbeitung durch Lehrkräfte außerhalb der Schule sowie die Durchführung von Untersuchungen und wissenschaftlicher Forschung mit pseudonymisierten Daten.

Die neuen Regelungen sind aufgrund der Entwicklungen der automatisierten Datenverarbeitung dringend erforderlich, zumal das Gesetz seit 1987 unverändert gilt und bereits seit zwei Jahren die Schulverwaltungssoftware MAGELLAN eingesetzt wird, obwohl die Datenverarbeitung nicht in vollem Umfang vom geltenden Schuldatenschutzgesetzes abgedeckt ist (vgl. Ziff. 13.4 dieses Berichts).

Meine Bedenken gegen eine Regelung zur Übermittlung von Schülerdaten an die Polizei bleiben bestehen. Die Polizei ist einerseits Gehilfin der Staatsanwaltschaft, andererseits obliegen ihr Aufgaben der vorbeugenden Verbrechensbekämpfung und Gefahrenabwehr, so dass die Erhebungsbefugnisse nach dem Bremischen Polizeigesetz (BremPolG) gegenüber anderen öffentlichen Stellen (auch Schulen) ausreichen. Bei einer verpflichtenden Regelung ist eine Beeinträchtigung der pädagogischen Arbeit der Lehrkraft nicht ausgeschlossen. Es spricht nichts gegen eine übergreifende Kooperation, aber die Übermittlung von Schülerdaten in konkreten Fällen an die Polizei, die nach der Gesetzesbegründung der Kooperation zwischen Polizei und Schule, pädagogischer Einflussnahme und regionaler Prävention dienen soll, halte ich für bedenklich und bedarf daher noch vertiefter Beratung.

Hiervon unberührt bleibt der Datenaustausch in Schulverweigerer-/Präventionsausschüssen (SCHUPS). Auf diese Problematik bin ich erst im Sommer 2005 vom Beratungsdienst Schulvermeidung, dem Amt für Soziale Dienste und der Polizei aufmerksam gemacht worden. Bei einer Besprechung mit Vertretern dieser Einrichtungen wurde deutlich, dass der Austausch u. a. von besonderen Arten von Daten (Gesundheitsdaten, ethnische Herkunft) und weiteren sensiblen Daten, z. B. die Gesamtheit der familiären Situation, zwischen den einzelnen Institutionen (Beratungsdienst Schulvermeidung, Schulärztlicher und Schulpsychologischer Dienst, Kontaktpolizist u. a.) zur Erarbeitung eines fallbezogenen Maßnahmenkatalogs regelmäßig erforderlich ist.

Für diesen Datenaustausch besteht allerdings keine gesetzliche Erlaubnis (auch nicht im Novellierungs-Entwurf), so dass es nach Auffassung aller Gesprächsteilnehmer im überwiegenden Allgemeininteresse für erforderlich angesehen wird, hier eine angemessene Rechtsgrundlage zu schaffen. Beispielsweise böte sich eine Regelung zur Erstellung eines einzelfallbezogenen Maßnahmenkatalogs im schweren Falle einer Schulvermeidung an; orientiert an dem Hilfeplan nach § 36 Sozialgesetzbuch zur Kinder- und Jugendhilfe (SGB VIII). Einbezogen werden sollte auch die Weitergabe erforderlicher Schülerdaten an freie Träger, soweit eine von SCHUPS entschiedene Maßnahme den Einsatz einer besonderen Einrichtung eines freien Trägers vorsieht.

Zuletzt habe ich allerdings im Herbst 2005 vernommen, die Senatsvorlage zum Schuldatenschutzgesetz sei auf Wunsch des Senators für Inneres und Sport zurückgezogen worden, weil der Gesetzentwurf keine Regelung zur Übermittlung von Schülerdaten an den Verfassungsschutz und den Staatsschutz vorsehe. Nähere Auskünfte hierzu erhielt ich bisher nicht.

13.4 Prüfung des Schuldatenverwaltungsverfahrens MAGELLAN

Im Juni 2005 habe ich beim Senator für Bildung und Wissenschaft die Schulverwaltungssoftware MAGELLAN geprüft. Es handelt sich um eine als Client-Server-

Applikation konzipierte Datenbankanwendung. Die Software wird in allen öffentlichen Schulen und bei der senatorischen Dienststelle eingesetzt. Zum Zeitpunkt der Prüfung wurden Stammdaten von Lehrern und Schülern der öffentlichen Schulen der Stadtgemeinde Bremen und alle Schülerdaten der privaten Schulen erfasst. Teil dieser Stammdaten sind auch sensible Informationen wie beispielsweise solche über Behinderungen, Förderbedarfe und Herkunft. Zukünftig geplant ist darüber hinaus die Erfassung von Leistungsdaten. Das System muss daher besonderen Anforderungen des Datenschutzes gerecht werden.

Ich habe bei meiner Prüfung zu folgenden Bereichen Mängel festgestellt und entsprechende Anforderungen für einen datenschutzgerechten Betrieb des Systems formuliert:

Eingabekontrolle: Die Eingabekontrolle (§ 7 Abs. 4 Nr. 5 Bremisches Datenschutzgesetz – BremDSG) soll gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Zum Zeitpunkt der Prüfung gab es keine auf einzelne Nutzer beziehbare Eingabekontrolle. Die senatorische Dienststelle hält momentan die Zugriffs- und Eingabekontrolle für jeden einzelnen Nutzer (momentan: Schulleiterin/Schulleiter, Vertreterin/Vertreter, Sekretärin/Sekretär) nicht für realisierbar, da sie zu aufwändig sei. Zur Gewährleistung der Eingabekontrolle ist jedoch festzulegen, welche Ereignisse zu protokollieren und welche Informationen dabei zu erfassen sind. Wie viele Ereignisse zu erfassen sind, hängt vom Schutzbedarf des jeweiligen Systems und der verarbeiteten Daten ab.

Die Protokollierung muss sich auf die Benutzeraktivitäten (Verfahrensüberwachung) und auf die Administrationstätigkeiten (i. d. R. Systemüberwachung) beziehen. Modifikationen von Systemparametern müssen zumindest über manuelle Aufzeichnungen nachvollziehbar sein. Systemzustände, wie beispielsweise die Dokumentation der Zugriffsrechte, sind ebenfalls aufzuzeichnen. Meine Forderungen sind allgemeine Standards. Gleiches gilt für die nachfolgenden Punkte.

Revision: Zum Zeitpunkt der Prüfung gab es keine Revision des Systems. Hierzu ist festzulegen, welche Benutzer unter welchen Rahmenbedingungen auf die protokollierten Informationen zugreifen dürfen und wann und nach welchen Kriterien die Protokolldaten ausgewertet werden sollen. Auch Löschfristen sind zu definieren (§ 12 Abs. 4 BremDSG – enge Zweckbindung der Protokolldaten).

Organisation der Administration: Zum Zeitpunkt der Prüfung lagen keine organisatorischen Regelungen über die Befugnisse der Administratoren vor. Eine schriftliche Fixierung der Aufgabenbereiche ist aufgrund der umfassenden Zugriffsmöglichkeiten erforderlich.

Pseudonymisierte Datenbank: In dieser für statistische Zwecke benötigten Datenbank werden die Daten nicht unter dem Namen der Schülerin bzw. des Schülers gespeichert, sondern unter einem Pseudonym. Es handelt sich hierbei um eine zweite Datenbank, die aufgrund des Primärdatensatzes erstellt wird. Das Pseudonym sollte so gestaltet werden, dass die Identifikation eines Schülers ausgeschlossen ist (so genannte Einweg-Pseudonyme), um eine nicht personenbezogene Datenverarbeitung zu ermöglichen. Zum Zeitpunkt der Prüfung wurden lediglich Identifikationsnummern als Namensersatz verwendet, die zusammen mit den entsprechenden inhaltlichen Aussagen direkte Rückschlüsse auf Einzelpersonen zuließen. Die senatorische Dienststelle hat hierzu einen Lösungsvorschlag erarbeitet. Dieser sieht die inzwischen erfolgte Löschung des Geburtsortes als mögliches Identifikationsmerkmal vor. Für die Umsetzung der Pseudonymisierung wurde ein Algorithmus entwickelt. Da es sich hierbei um eine Eigenentwicklung handelt, muss dessen Funktionssicherheit, Unumkehrbarkeit und Stabilität gegenüber Angriffen noch zusätzlich getestet werden. Ich habe daher den Einsatz eines Standardproduktes (SHA-1, Secure Hash Algorithm), das vom National Institute of Standards and Technology (NIST) empfohlen wird, nahe gelegt.

Verfahrensbeschreibung: Obwohl sich das Verfahren bereits im Echtbetrieb befand, war keine Verfahrensbeschreibung nach § 8 BremDSG vorhanden. Inzwischen ist eine Verfahrensbeschreibung vorgelegt worden. Diese entspricht lediglich den formalen Kriterien, enthält jedoch keine ausreichenden Informationen, um eine datenschutzrechtliche Bewertung vornehmen zu können.

Ich habe daher die senatorische Dienststelle im November 2005 aufgefordert, das aktuelle Datenschutzkonzept gemäß § 8 Abs. 1 Nr. 7 BremDSG vorzulegen, in dem die vorgenannten Anforderungen aufgenommen werden. Dies ist bis zum Redaktionsschluss nicht erfolgt.

14. Umwelt

14.1 Schaffung eines Bremischen Umweltinformationsgesetzes

Nach Art. 11 EU-Richtlinie 2003/4EG über den Zugang der Öffentlichkeit zu Umweltinformationen (UI-RI) vom 28. Januar 2003 ist die Umweltinformationsrichtlinie 90/131/EWG aus dem Jahr 1990 zum 14. Februar 2005 aufgehoben worden. Dafür sind die Mitgliedstaaten nach Art. 10 UI-RI verpflichtet, die neue Richtlinie bis zu diesem Zeitpunkt umzusetzen.

Aus datenschutzrechtlicher Sicht ist bedeutsam, dass nach Art. 4 Abs. 2 f UI-RI Ausnahmen vom Informationszugangsrecht gemacht werden können, wenn die Bekanntgabe negative Auswirkungen hätte auf die Vertraulichkeit personenbezogener Daten und/oder Akten über eine natürliche Person, sofern diese der Bekanntgabe dieser Informationen an die Öffentlichkeit nicht zugestimmt hat und sofern eine derartige Vertraulichkeit nach innerstaatlichem oder gemeinschaftlichem Recht vorgesehen ist. Insoweit hat sich nichts Wesentliches zur bisherigen Umweltinformationsrichtlinie geändert.

Weil die Länder auf ihrer Gesetzgebungskompetenz bestanden haben, hat der Bund nur für Stellen seines Bereichs ein Umweltinformationsgesetz (UIG) in Kraft gesetzt (vgl. BGBl. I S. 3704). Auf meine diesbezügliche Anfrage im Februar 2005 hat mir der Senator für Bau, Umwelt und Verkehr den Entwurf eines Bremischen Umweltinformationsgesetzes (BremUIG) vorgelegt, den ich mit beraten habe. Das Gesetz ist inzwischen in Kraft getreten (BremUIG vom 15. November 2005; Brem.GBl. S. 573).

Besonders beachtlich ist, dass § 4 BremUIG die Einrichtung eines internet-unterstützten Umweltinformationssystems mit einer Servicestelle beim für den Umweltschutz zuständigen Mitglied des Senats vorsieht. Nach § 2 Abs. 2 BremUIG gelten für den Zugang zu Umweltinformationen die Vorschriften des Umweltinformationsgesetzes des Bundes. Da das BremUIG Ausnahmen vom Zugang zu Umweltinformationen nicht enthält, wird insoweit auf die Regelungen des UIG verwiesen. Die Vorschrift des § 9 Abs. 1 Nr. 1 UIG regelt die Ausnahme vom Informationszugangsrecht, wenn es sich dabei um die Bekanntgabe personenbezogener Daten handelt und dadurch Interessen der Betroffenen erheblich beeinträchtigt werden. Vor der Entscheidung über die Offenbarung dieser Daten sind die Betroffenen anzuhören.

14.2 Erhebung von Hochwasserschutzbeiträgen

Der Senator für Bau, Umwelt und Verkehr hat mir eine Änderung des § 120 Abs. 5 Bremisches Wassergesetz vorgelegt. Damit sollte eine Rechtsgrundlage für die Einführung zur Erhebung von Hochwasserschutzbeiträgen in Bremerhaven nach Maßgabe einer zu erlassenden Rechtsverordnung geschaffen werden.

Da in dem Verordnungsentwurf der Umfang der Verarbeitung personenbezogener Daten über Beitragspflichtige festgelegt werden sollte, habe ich vorgeschlagen, die Ermächtigungsnorm zum Erlass einer Rechtsverordnung entsprechend zu erweitern. Mein Vorschlag wurde übernommen. Die Gesetzesänderung vom 14. Dezember 2004 (Brem.GBl. S. 595) ist in Kraft getreten.

15. Finanzen

15.1 Kontodatenabrufe nach § 24 c KWG und §§ 93, 93 b AO

Bereits seit April 2003 müssen Kreditinstitute nach § 24 c Kreditwesengesetz (KWG) zur Aufdeckung illegaler Finanztransaktionen die Kontostammdaten ihrer Kunden zum Abruf durch staatliche Stellen bereithalten. Hierzu zählen Kontonummer, Name und Geburtsdatum des Inhabers und eventueller Verfügungsberechtigter sowie Name und Anschrift von abweichend wirtschaftlich Berechtigten. Seit April 2005 können diese Daten nach §§ 93, 93 b Abgabenordnung (AO) nunmehr auch von den Finanzbehörden abgefragt werden, wenn dies zur Festsetzung oder Erhebung von Steuern dient. Aber auch viele andere Behörden, z. B. die zahlreichen Stellen

der Sozialleistungsträger, und Gerichte haben Zugriff, wenn diese ein Gesetz anwenden, das „an Begriffe des Einkommensteuerrechts“ anknüpft. Diese Regelungen wurden durch das Gesetz zur Förderung der Steuerehrlichkeit vom 23. Dezember 2003 (BGBl. I 2003, S. 2928) geschaffen (vgl. 27. JB, Ziff. 12.1).

Insbesondere um der Kritik der Datenschutzbeauftragten des Bundes und der Länder entgegenzukommen, hat das Bundesfinanzministerium in seinem Anwendungserlass zur Abgabenordnung vom 10. März 2005 einengende Voraussetzungen für die Kontodatenabrufe formuliert. Diese Einschränkungen bestehen v. a. in der Pflicht zur Benachrichtigung des Betroffenen nach Durchführung einer Abfrage sowie darin, dass Abrufe nur anlassbezogen und zielgerichtet und unter Bezugnahme auf eindeutig bestimmte Personen zulässig sind. Außerdem sieht der Erlass vor, dass Betroffenen zunächst Gelegenheit gegeben werden soll, selbst Auskunft über ihre Konten und Depots zu erteilen und auf diese Weise den Datenzugriff beim Kreditinstitut zu vermeiden. Auch werden die Fälle abschließend benannt, in denen sonstige Behörden und Gerichte von der Abrufmöglichkeit Gebrauch machen dürfen. All dies ist in den Gesetzesbestimmungen selbst nicht klar geregelt.

a) Verfassungsbeschwerden gegen die Kontodatenabrufe

Betroffene haben Verfassungsbeschwerde gegen die gesetzlichen Regelungen im KWG und in der AO eingelegt und z. T. versucht, im Rahmen eines Eilverfahrens vor dem Bundesverfassungsgericht das In-Kraft-Treten der neuen Vorschriften in der Abgabenordnung zu verhindern. Den Erlass einer entsprechenden einstweiligen Anordnung hat das Gericht abgelehnt, eine Entscheidung im Hauptsacheverfahren ist aber noch zu treffen.

Zur Begründung für die Ablehnung des Erlasses einer einstweiligen Anordnung hat das Bundesverfassungsgericht u. a. ausgeführt, dass die Nachteile für die Betroffenen nicht so schwer wiegen, dass die Aussetzung des Vollzugs des Gesetzes zu verfügen ist. Dies gelte jedenfalls, solange die in dem Anwendungserlass zur Abgabenordnung verfügten Einschränkungen der Kontenabfrage beachtet werden.

Für die Frage, über die das Bundesverfassungsgericht im Hauptsacheverfahren noch zu entscheiden hat, nämlich ob die gerügten Normen verfassungsgemäß sind oder nicht, ist aber entscheidend, ob im Gesetz selbst hinreichende Beschränkungen der Abrufbefugnisse zum Schutz des Rechts auf informationelle Selbstbestimmung enthalten sind. Ein Anwendungserlass mit bloß verwaltungsinterner Wirkung kann die Mängel eines Gesetzes nicht beheben. Aus diesem Grund habe ich in meiner Stellungnahme, zu deren Abgabe mir das Bundesverfassungsgericht im Rahmen des Hauptsacheverfahrens Gelegenheit gegeben hat, auch die Verfassungsmäßigkeit der Vorschriften über den Kontodatenabruf in Frage gestellt. Ganz wesentlich ist dabei die fehlende Transparenz für die Betroffenen, die fehlende Zweckbestimmung für Zugriffe durch andere Behörden und Gerichte sowie die fehlende Bestimmbarkeit dieser Stellen.

Es bleibt abzuwarten, wie das Bundesverfassungsgericht entscheiden wird. Im Interesse des Datenschutzes wäre eine Klarstellung, dass die geänderten Bestimmungen in ihrer derzeitigen Form das Grundrecht auf informationelle Selbstbestimmung unzulässig einschränken, zu begrüßen.

b) Nutzung der Kontenabfragemöglichkeit nach §§ 93, 93 b AO in Bremen

Ich hatte im Rechtsausschuss der Bremischen Bürgerschaft vorgeschlagen, sich mit der bremischen Praxis zu befassen.

In einem Zeitraum von drei Monaten (August bis Oktober 2005) haben die Finanzämter zehn Abrufersuchen an das Bundesamt für Finanzen gerichtet. Ersuchen anderer öffentlicher Stellen gab es nicht. In fünf Fällen wurde zunächst von einer Benachrichtigung der Betroffenen abgesehen, um den Ermittlungszweck nicht zu gefährden. Ich begrüße den zurückhaltenden Einsatz der Abfragemöglichkeit. Allerdings hängt dieser möglicherweise auch damit zusammen, dass die Abrufersuchen zurzeit noch nicht – wie für die Zukunft geplant – vollelektronisch, sondern in einem manuellen Verfahren gestellt und beantwortet werden. Dementsprechend hat der SfF die Finanzämter gebeten, bei der Auswahl der in Frage kommenden Fälle Prioritäten zu setzen und bis auf Weiteres nur in ausgewählten Einzelfällen von der Möglichkeit des Kontenabrufs Gebrauch zu machen.

Aus datenschutzrechtlicher Sicht ist entscheidend, dass auch nach Einführung eines vollelektronischen Verfahrens die gesetzlichen Voraussetzungen für den Ab-

ruf in jedem Einzelfall sorgfältig geprüft werden. Auf keinen Fall darf die Abfragemöglichkeit zu einem unreflektiert eingesetzten Routineinstrument werden.

15.2 DATA-Port

Mit Gesetz vom 20. Dezember 2005 ist das Land Bremen dem Länderstaatsvertrag zur Errichtung der Anstalt des öffentlichen Rechts DATA-Port beigetreten (Brem.GBl. 2005, S. 615). DATA-Port unterstützt die IT-Steuerverwaltung der Länder Schleswig-Holstein, Hamburg, Mecklenburg-Vorpommern und Bremen. Bestandteil ist die Weiterentwicklung von EOSS (Evolutionär Orientierte Steuer Software) als Zwischenschritt zu einem bundesweiten, einheitlichen Besteuerungsverfahren. Ob auch weitere IT-Verfahren des Landes – wie bisher für Schleswig Holstein und Hamburg – von DATA-Port betreut werden sollen, wird erst in 2006 entschieden werden. Der Entwurf des Staatsvertrags ist unter datenschutzrechtlichen Gesichtspunkten von mir beraten worden. Soweit DATA-Port personenbezogene Daten für bremische öffentliche Stellen verarbeitet, gelten das Bremische Datenschutzgesetz (BremDSG) und die sonstigen für bremische öffentliche Stellen geltenden Vorschriften über den Datenschutz. Nach § 15 des Staatsvertrages obliegt dem Landesbeauftragten für den Datenschutz die Überwachung der Einhaltung dieser Vorschriften. Zudem berate ich insoweit DATA-Port in Fragen des Datenschutzes und nehme das Anhörungsrecht gegenüber dem Datenschutzbeauftragten von DATA-Port wahr. Ende 2005 wurde eine ressortübergreifende Arbeitsgruppe beim Senator für Finanzen eingerichtet, die ein umfassendes Konzept zur Weiterentwicklung des IT-Bereichs im Land Bremen entwickelt und dabei prüft, welche Aufgaben sich für eine auszugründende und auf DATA-Port zu übertragende Einheit eignen.

16 Häfen

16.1 Zuverlässigkeitsüberprüfung nach dem Hafensicherheitsgesetz

Seit Juli 2004 ist das Hafensicherheitsgesetz in Kraft. Das Hafensicherheitsgesetz sieht eine Verordnungsermächtigung vor, nach der der Senator für Wirtschaft und Häfen (SfWuH) das Verfahren der Zuverlässigkeitsüberprüfung konkret zu regeln hat, da das Gesetz nur den Rahmen vorgibt. Diese Verordnung ist bisher nicht erlassen worden. Eine Nachfrage im September 2005 nach dem Stand des Entwurfs der Verordnung ergab, dass vor Januar 2006 nicht mit einer Fertigstellung zu rechnen ist, da noch eine Abstimmung unter den norddeutschen Küstenländern erfolgen soll. Dieser verspätete Erlass ist aus datenschutzrechtlicher Sicht zu kritisieren.

17. Bremerhaven

Da es sich anbietet, viele Themen in einem Sachzusammenhang darzustellen, soll an dieser Stelle die Auffindbarkeit von Beiträgen erleichtert werden, die Themen aus Bremerhaven betreffen. Sie finden sich unter Ziff. 1.7 (eGovernment), Ziff. 1.15 (Durchgeführte Aus- und Fortbildungsmaßnahmen und Vorträge), Ziff. 2.1 (Behördliche Datenschutzbeauftragte), Ziff. 5.1 Verfahren der Rundfunkgebührenbefreiung, Ziff. 7.1 (Bremische Bürgerschaft – Ergebnisse der Beratung des 27. Jahresberichts), Ziff. 8.2 (Falsche Behandlung von Bewerbungsunterlagen), Ziff. 9.6 (ApolWeb), Ziff. 9.8 (Datenschutzkonzepte bei der Ortspolizeibehörde Bremerhaven), Ziff. 10.2 (Neuregelung der forensischen DNA-Analyse), Ziff. 12.3 (Rechtswidrige Datenübermittlung durch zwei Krankenkassen), Ziff. 14.2 (Erhebung von Hochwasserschutzbeiträgen), Ziff. 18.12 (Verarbeitung personenbezogener Daten von Fahrgästen durch Kontrolleure, Ziff. 18.18 (Vergabe von Ausbildungsplätzen nach einem öffentlichen Lauf-Casting).

18. Datenschutz in der Privatwirtschaft

18.1 Geldwäschebekämpfung durch den Einsatz von Research-Systemen

Das Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (GwG) stellt für Kreditinstitute und weitere private Stellen zur Bekämpfung von Geldwäsche und der Finanzierung einer terroristischen Vereinigung besondere Identifizierungs-, Aufzeichnungs- und Aufbewahrungspflichten auf und verpflichtet zur Anzeige von Verdachtsfällen. Außerdem müssen interne Maßnahmen zum Schutz gegen Geldwä-

sche getroffen werden. § 25 a des Gesetzes über das Kreditwesen schreibt den Kreditinstituten darüber hinaus vor, Sicherungssysteme gegen Geldwäsche und betrügerische Handlungen zu implementieren. Als Folge dessen setzen die Banken so genannte Research-Systeme ein. Es handelt sich dabei um eine EDV-gestützte Durchleuchtung aller Kontobewegungen sämtlicher Kunden mit dem Ziel, mögliche Anhaltspunkte für einen Geldwäscheverdacht festzustellen. Das System durchsucht alle Transaktionen nach bestimmten Kriterien, die von den Kreditinstituten in eigener Verantwortung vorgegeben werden.

Bei zwei Bremer Kreditinstituten habe ich mich darüber informiert, welche Rasterkriterien dort eingesetzt werden. Beispielsweise sucht das System nach Überweisungen in Länder, die den international festgesetzten Standards in Bezug auf Geldwäschepräventionsmaßnahmen nicht entsprechen. Aber etwa auch eine hohe Zahl Verfügungsberechtigter, eine vorfristige Darlehensrückzahlung in großem Umfang, eine fehlende Benennung des Buchungszwecks oder eine hohe Anzahl von Einzahlungen am Bareinzahlungsautomaten stellen nach den Einstellungen des Systems ein Indiz für einen Geldwäscheverdacht dar. Die Indizien werden nach einem von der Bank vorgegebenen Punkteschema bewertet, und erst bei Erreichen eines bestimmten Gesamtpunktewertes schlägt das System Alarm mit der Folge, dass der betreffende Kunde vom Geldwäschebeauftragten des Instituts näher unter die Lupe genommen wird. Dabei existieren Indizien, die für sich genommen schon den maßgeblichen Gesamtpunktewert erreichen. Ergeben sich für den Geldwäschebeauftragten nach seiner Prüfung tatsächlich Anhaltspunkte für einen Geldwäscheverdacht, unterrichtet er die zuständige Strafverfolgungsbehörde.

Aus datenschutzrechtlicher Sicht ist der Einsatz solcher Research-Systeme problematisch, weil von nichtstaatlichen Stellen Nachforschungen zur Ermittlung eines eventuellen Anfangsverdachts angestellt werden. Außerdem zeigen die oben genannten Beispiele, wie leicht es ist, als unbescholtener Bürger in das Visier des Geldwäschebeauftragten und damit in den „Vorhof“ des Verdachts zu geraten.

Aus diesem Grund befasst sich eine Unterarbeitsgruppe der Arbeitsgruppe Kreditwirtschaft des Düsseldorfer Kreises, an der ich mich beteilige, mit der Frage, welche datenschutzrechtlichen Anforderungen an Research-Systeme zu stellen sind. Eine abschließende rechtliche Bewertung ist zurzeit nicht möglich, da mir und den anderen Aufsichtsbehörden dazu einige Informationen noch nicht vorliegen. Ich halte es jedoch für erforderlich, dass die Bankkunden über die flächendeckende Rasterung aller Kontobewegungen informiert werden. Außerdem ist bei der Frage, wie alt der für das Research-System verwendete Datenbestand sein darf, § 35 Abs. 2 Satz 2 Nr. 3 Bundesdatenschutzgesetz (BDSG) zu beachten. Danach sind personenbezogene Daten zu löschen, sobald sie für die Erfüllung des Zwecks ihrer Speicherung nicht mehr erforderlich sind. Die Banken dürfen zudem nur solche Suchkriterien in die Research-Systeme einstellen, die in sachlich nachvollziehbarer Weise auf einen Geldwäscheverdacht hindeuten. Für unbefriedigend halte ich es, dass die Kreditinstitute nach Angaben von Banken- und Bankenverbandsvertretern bei der Definition der Suchkriterien von Strafverfolgungsbehörden und der Bundesanstalt für Finanzdienstleistungsaufsicht weitgehend allein gelassen werden. Verbindliche Vorgaben existieren nicht. Jedenfalls unzulässig ist aber die Rasterung von besonderen Arten personenbezogener Daten im Sinne von § 3 Abs. 9 BDSG, insbesondere von rassischer und ethnischer Herkunft, poliltischer Meinung sowie religiöser Überzeugung.

Da derzeit verschiedene Research-Systeme im Einsatz sind, müssen für eine detaillierte Bewertung die Prüfergebnisse der Aufsichtsbehörden abgewartet werden. Wegen des mit ihrem Einsatz verbundenen weitreichenden Eingriffs in das Grundrecht auf informationelle Selbstbestimmung ist eine vertiefte Diskussion über dieses Instrument aber dringend angezeigt.

18.2 Credit-Scoring als Folge von Basel II

Im September 2005 hat das Europäische Parlament die Richtlinien zur Schaffung von neuen Eigenkapitalregelungen für Banken verabschiedet und damit die Rahmenvereinbarung des Baseler Ausschusses für Bankensicherheit über die neue Eigenkapitalempfehlung für Kreditinstitute (Basel II) umgesetzt. Bis zum 1. Januar 2007 sollen die EU-Richtlinien in nationales Recht transformiert werden. Durch Basel II soll v. a. die Sicherheit und Solidität der Banken gewährleistet und die Stabilität der Finanzbranche insgesamt verbessert werden. Wesentlicher Bestandteil sind dabei

neue Mindestanforderungen an die Eigenkapitalausstattung von Kreditinstituten, die sich künftig mehr nach den tatsächlichen Risiken einer Bank richten sollen. Für die Kreditvergabe bedeutet das, dass für jedes Darlehen das Ausfallrisiko zu bestimmen ist. Je nach Ausfallwahrscheinlichkeit schwanken dann die Höhe des zu hinterlegenden Eigenkapitals und damit auch die zu zahlenden Kreditzinsen.

Zur Risikoklassifizierung nutzen die Banken zum Großteil schon heute das so genannte Credit-Scoring. Dabei werden bestimmte Daten von Kreditnehmern mit statistischen Auswertungen über vertragsgemäß oder nicht vertragsgemäß zurückgezahlte Kredite verglichen und an Hand dieses Vergleichs bewertet. Ist es beispielsweise statistisch erwiesen, dass junge Menschen zwischen 18 und 21 Jahren einen Kredit besonders häufig nicht zurückzahlen, wirkt sich dieses Merkmal bei der Stellung eines Kreditantrages für einen 20-jährigen potentiellen Kreditnehmer negativ aus. In einem automatisierten Verfahren wird auf diese Weise eine Vielzahl von personenbezogenen Daten des Antragstellers nach statistisch-mathematischen Verfahren bewertet und so ein statistisches Ausfallrisiko ermittelt. Das kann mit Hilfe eines institutsinternen Scoring-Verfahrens (internes Scoring) oder durch einen Dritten (externes Scoring) erfolgen. Einbezogen werden dabei Angaben wie Familienstand, Alter, Einkommen, Vermögensverhältnisse, aber auch – soweit bekannt – Informationen zum Zahlungsverhalten des Betroffenen.

Aus datenschutzrechtlicher Sicht problematisch ist dabei der Umstand, dass in einer für den Kreditnehmer nicht nachvollziehbaren Art und Weise aus der Gesamtheit seiner personenbezogenen Daten ein Wert ermittelt wird, der vermeintlich Auskunft über das Risiko seines Ausfalls gibt. Vermeintlich deshalb, weil es sich hierbei allein um eine statistische Aussage handelt. Ob aber – um beim obigen Beispiel zu bleiben – der 20-jährige Kreditnehmer im konkreten Fall tatsächlich seine Darlehensverbindlichkeiten unzuverlässig erfüllt, steht gar nicht fest. Damit stellt sich v. a. die Frage, wie eine ausreichende Transparenz für die Betroffenen hergestellt werden kann und welche personenbezogenen Daten unter Berücksichtigung berechtigter Interessen der Banken und schutzwürdiger Interessen der Kunden im Rahmen von Scoring-Verfahren verwendet werden dürfen.

Vor diesem Hintergrund hat sich der Düsseldorfer Kreis, der Zusammenschluss aller obersten Datenschutzaufsichtsbehörden für den nicht-öffentlichen Bereich, mit den datenschutzrechtlichen Anforderungen, die an Scoring-Systeme zu stellen sind, befasst. Zusammen mit meinen Kollegen aus den anderen Bundesländern bin ich der Auffassung, dass beim Credit-Scoring jedenfalls nur solche Parameter verwendet werden dürfen, deren Bonitätsrelevanz mittels mathematisch-statistischer Verfahren nachgewiesen ist. Zusätzlich sind bei der Beurteilung der Zulässigkeit der Nutzung von personenbezogenen Daten nach § 28 Abs. 1 Satz 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) die berechtigten Interessen der Bank und die schutzwürdigen Interessen der Bankkunden gegeneinander abzuwägen. Danach dürfen Daten, die lediglich einen statistischen Indizcharakter für die Bonitätsbeurteilung haben (z. B. das Alter, die Zahl der Wohnsitzwechsel in einem bestimmten Zeitraum), etwa dann nicht verwendet werden, wenn der Bank hinreichende Informationen über die Einkommens- und Vermögensverhältnisse sowie über vorangegangene Geschäftsbeziehungen mit dem Kreditnehmer vorliegen.

Hinsichtlich der Anforderungen an die Transparenz von Scoring-Verfahren gilt, dass für die Betroffenen erkennbar sein muss, welche personenbezogenen Merkmale allgemein in die Berechnung des Score-Wertes einfließen und welche ihrer Daten dafür konkret genutzt werden. Außerdem müssen die Betroffenen darüber aufgeklärt werden, welche Daten den Score-Wert maßgeblich negativ beeinflusst haben. Dabei sind mindestens die vier entscheidensten Merkmale zu benennen. Nur so ist der Betroffene selbst in der Lage zu prüfen, ob die der Berechnung zugrunde liegenden Daten richtig sind.

18.3 Probleme bei der Entsorgung von Bankunterlagen

Im Herbst 2005 wurde ich von einem Zeitungsredakteur darüber informiert, dass ein Bürger vor einem Kreditinstitut in Bremen-Rablinghausen in einem offen zugänglichen Altpapiercontainer Ausdrucke der Bank gefunden hat. Die entdeckten Unterlagen enthielten in Tabellen aufgelistete Kundendatensätze mit Vor- und Nachnamen, Anschriften, Geburtsdaten, Telefon- und Kontonummern. Zu jedem Konto waren minuziös die dazugehörigen Kontostände vermerkt. Da es sich ganz überwiegend um Kunden aus der näheren Umgebung des Kreditinstituts handelte,

hätte jeder, der dort wohnt, Kenntnis von den finanziellen Verhältnissen seiner Nachbarn bekommen können.

Die Ausdrucke wurden mir zur Verfügung gestellt. Ich habe die Angelegenheit zum Anlass für eine Prüfung des Entsorgungskonzepts bei der betreffenden Bank genommen. Dabei habe ich zunächst festgestellt, dass die gefundenen Unterlagen tatsächlich von dort stammten. Die Bank erklärte nach Befragung des Filialleiters und der verantwortlichen Bankangestellten, der Vorfall könne möglicherweise durch ein Versehen des Reinigungspersonals einer Fremdfirma zu erklären sein, das auch mit der Entsorgung von Bankunterlagen betraut ist. Es ließ sich jedoch nicht mit Sicherheit feststellen, wie die mir übersandten Unterlagen dorthin gelangt waren.

Meine weitere Untersuchung ergab Folgendes: In den Filialen der Bank gab es bisher an den Arbeitsplätzen zwei verschiedene Müllgefäße, eines für Datenmüll, das andere für sonstigen Papiermüll. Meine Prüfung ergab, dass die externe Reinigungsfirma vertraglich zu einer besonderen Behandlung der Bankunterlagen verpflichtet war. Gleichwohl war festzustellen, dass das bislang praktizierte Verfahren, bei dem Reinigungskräfte einer Fremdfirma beteiligt waren, mit dem Risiko der unbefugten Kenntnisnahme einer Vielzahl von personenbezogenen Daten, die dem Bankgeheimnis unterliegen, behaftet war und daher verbessert werden musste. Auch konnte die bisher bei dem Kreditinstitut vorgeschriebene Mülltrennung leicht einmal zu Fehlern führen.

Es ist festzuhalten, dass die dem Bankgeheimnis unterliegenden Daten besonders sensibel sind und die Verantwortlichen eine besondere Sorgfalt bei allen Phasen der Datenverarbeitung – auch bei der Vernichtung – walten lassen müssen. Ich habe die Bank deshalb aufgefordert, ein umfassendes Entsorgungskonzept zu erarbeiten, bei dem die Verantwortung für eine ordnungsgemäße Entsorgung – wie auch in anderen Bereichen der Wirtschaft und Verwaltung – regelmäßig bei den Beschäftigten selbst liegt. Die Bank hat diesen Vorgaben entsprechend ein neues Entsorgungskonzept erstellt. Künftig sind die Mitarbeiter verpflichtet, ihren Datenmüll selbst zu entsorgen. Dafür werden verschlossene Papiercontainer an zentralen Stellen innerhalb der Filialen aufgestellt bzw., soweit schon vorhanden, Aktenvernichtungsgeräte genutzt. Sämtliche Papierkörbe für „Datenmüll“ werden abgeschafft, um eine Verwechselung von Datenmüll und aus datenschutzrechtlicher Sicht unproblematischem Altpapier auszuschließen. Das neue Entsorgungskonzept soll bis Ende Februar 2006 umgesetzt sein.

18.4 Neuere Entwicklungen im Bereich Auskunfteien

Der Handel mit Bonitätsdaten ist nach wie vor ein einträgliches Geschäft. Deshalb verwundert es nicht, dass neue Auskunfteien gegründet werden und existierende Auskunfteien ihr Geschäftsfeld zu erweitern suchen.

Besonders kritisch sind dabei neuere Tendenzen bei der SCHUFA zu sehen. Die Zielsetzung der SCHUFA besteht bislang darin, die an ihr System angeschlossenen Unternehmen vor Verlusten im Kreditgeschäft zu schützen. Damit ist die Absicht, zukünftig Versicherungen als Abrufberechtigte in das so genannte B-Verfahren aufzunehmen, aus meiner Sicht nicht vereinbar, da Versicherungen i. d. R. aufgrund der gesetzlichen Vorschriften im Versicherungsvertragsgesetz und wegen bestehender Aufrechnungsmöglichkeiten kein kreditorisches Risiko tragen. Außerdem beabsichtigt die SCHUFA, Inkassounternehmen als B-Vertragspartner aufzunehmen, was das Risiko birgt, dass über diesen Weg alltägliche Streitigkeiten, wie z. B. von Bürgern mit Handwerksbetrieben, zu einem SCHUFA-Eintrag mit den damit verbundenen negativen Folgen bei einem Kreditantrag oder einer Bestellung im Versandhandel führen können. Ferner übermittelt die SCHUFA zurzeit ihre Score-Werte an B-Vertragspartner. Das halte ich für unzulässig, weil die Score-Werte auch auf so genannten Positivdaten (d. h. Informationen, die eben nicht die Mitteilung von vertragswidrigem Verhalten beinhalten) beruhen. B-Vertragspartner haben aber keinen Anspruch auf diese Daten als solche. In all diesen Fragen finden Gespräche zwischen der SCHUFA und der zuständigen Aufsichtsbehörde in Hessen sowie der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises statt. Bei den aufgrund der unterschiedlichen Interessenlage natürlicherweise bestehenden Meinungsverschiedenheiten treten die Vertreter der SCHUFA allerdings zunehmend in einer Art und Weise auf, die nicht mehr länger hinnehmbar ist.

Über die Frage der Zulässigkeit von Mieterwarndateien bei Auskunfteien habe ich bereits in meinem 27. Jahresbericht (vgl. Ziff. 14.8.1) berichtet. Ich teile insoweit

die Auffassung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, dass Auskunfteien nur Daten aus öffentlichen Schuldnerverzeichnissen sowie harte Negativdaten aus dem Mietbereich an Vermieter übermitteln dürfen.

18.5 Kreditauskünfte an Mitglieder einer Wohnungseigentümergemeinschaft

Ein Bürger beklagte sich bei mir im Berichtsjahr darüber, dass seine bei Creditreform Bremen gespeicherten Daten an zwei Mitglieder einer Wohnungseigentümergemeinschaft übermittelt worden wären, ohne dass es hierfür einen Grund gegeben hätte. Die beiden Empfänger der übermittelten Daten hatten sich unabhängig voneinander mit der Bitte an Creditreform Bremen gewandt, ihnen die für eine Bonitätsüberprüfung benötigten Angaben mitzuteilen. Die Anfrage bei Creditreform Bremen war vor dem Hintergrund erfolgt, dass der sich an mich wendende Petent zuvor zum Verwalter der Wohnungseigentümergesellschaft bestellt worden war und einige Mitglieder dessen Abberufung wegen fehlender wirtschaftlicher Zuverlässigkeit und Seriosität bei der nächsten Mitgliederversammlung erwogen.

Gem. § 29 Abs. 2 Satz 1 Bundesdatenschutzgesetz (BDSG) hätte die Auskunftei in diesem Fall Daten über den Betroffenen nur übermitteln dürfen, wenn der Empfänger der Daten ein berechtigtes Interesse an deren Kenntnis glaubhaft dargelegt hätte und kein Grund zu der Annahme bestehen würde, dass der Betroffene ein schutzwürdiges Interesse am Ausschluss der Übermittlung hat. Nach der Rechtsprechung des Bundesgerichtshofs kann ein berechtigtes Interesse nur dann und insoweit vorliegen, als die Kenntnis der Daten für die vom Datenempfänger beabsichtigten Ziele und Zwecke erforderlich ist. Bei einer Auskunftsanfrage im Zusammenhang mit der Aufnahme oder Fortführung einer Geschäftsbeziehung besteht ein berechtigtes Interesse an der Datenübermittlung, soweit ein konkretes Risiko für den Empfänger vorliegt, das durch die Informationen der Auskunftei verringert oder beseitigt werden kann.

Eine Geschäftsbeziehung zwischen dem Petenten und den Empfängern der Auskunft bestand in diesem Fall nicht und war auch nicht beabsichtigt. Verträge über die Verwaltung einer Wohnungseigentümergemeinschaft mit den damit verbundenen Risiken werden nicht von den einzelnen Mitgliedern, sondern von der Gemeinschaft selbst geschlossen und auch gekündigt. Die Mitglieder, die die Daten von Creditreform Bremen erhalten hatten, waren überdies für die Gemeinschaft nicht vertretungsberechtigt. Gleichwohl bejahte ich das Vorliegen eines berechtigten Interesses in diesem Fall schließlich, da die Tätigkeit des Verwalters auch unmittelbar Einfluss auf das Wohneigentum des Einzelnen hat. Eine unzuverlässige oder unseriöse Verwaltung des gemeinschaftlichen Eigentums kann den Wert des Einzelwohneigentums erheblich verringern und zu erheblichen Nachteilen für den Betroffenen führen. Die Bestellung des Verwalters einer Wohnungseigentümergemeinschaft ist daher auch für jedes einzelne Mitglied mit erheblichen Risiken behaftet, so dass dennoch ein berechtigtes Interesse an den von meinem Petenten kritisierten Datenübermittlungen festzustellen war.

18.6 Unzulässige Datenerhebung durch Creditreform Bremen für die Inkassotätigkeit

Creditreform Bremen hat im Berichtsjahr einen Bürger angeschrieben mit der Bitte, dem Unternehmen im Rahmen seiner Inkassotätigkeit die Verzugsadresse eines früheren Mieters mitzuteilen. Die genannte Person war dem Bürger, der sich an mich wandte, vollkommen unbekannt. Er war auch nicht früherer Vermieter des Betroffenen. Einziger Verbindungspunkt zwischen den beiden war, dass die Person, nach der gefragt wurde, vor ihrem Umzug zwar in derselben Straße, allerdings in einem ganz anderen Haus gewohnt hatte. Das Schreiben von Creditreform Bremen enthielt neben der Bitte um Mitteilung der Verzugsanschrift auch eine ausführliche Aufstellung der gegenüber dem Betroffenen geltend gemachten finanziellen Forderungen mit dem Namen des betreffenden Gläubigers.

Die Übersendung des Anschreibens an den Bürger mit den darin enthaltenen Informationen stellt eine gravierende Verletzung der Bestimmungen des Bundesdatenschutzgesetzes (BDSG) dar. Im Rahmen seiner Inkassotätigkeit darf Creditreform Bremen personenbezogene Daten über einen Betroffenen u. a. unter Beachtung von § 28 Abs. 1 BDSG erheben. Im Hinblick auf die Feststellung einer Verzugsanschrift erfolgt daher i. d. R. zunächst eine Anfrage bei der Einwohnermeldebehörde.

Hat sich der Betroffene korrekt um- oder abgemeldet, so darf die Meldebehörde dem Unternehmen nach § 32 Meldegesetz (BremMeldG) die benötigte Anschrift mitteilen. Die Übermittlung von Angaben zu der Forderung an die Meldebehörde ist allerdings auch im Hinblick auf die Auskunft nicht erforderlich. Dass die Übersendung einer Forderungsaufstellung mit sehr sensiblen, personenbezogenen Daten des Betroffenen an einen Dritten wie im vorliegenden Fall unzulässig ist, muss darüber hinaus den für das Unternehmen tätigen Mitarbeitern stets bewusst sein und bei der Inkassotätigkeit auch beachtet werden.

Creditreform Bremen räumte den Verstoß gegen die Bestimmungen des BDSG ein und sicherte zu, dass sich ein solcher Fall nicht wiederholen werde.

Gleichwohl verhängte ich wegen des festgestellten eklatanten Verstoßes, der nach § 43 Abs. 2 Nr. 1 BDSG eine Ordnungswidrigkeit darstellt, noch ein Bußgeld in angemessener Höhe, das von dem Unternehmen umgehend bezahlt wurde.

18.7 Bestellung von externen Datenschutzbeauftragten für Berufsgeheimnisträger

In meiner Beratungs- und Prüfpraxis wurde in letzter Zeit häufig die Frage an mich herangetragen, ob und unter welchen Voraussetzungen Berufsgeheimnisträger (z. B. Rechtsanwälte, Steuerberater, Apotheker oder Ärzte mit entsprechend großen Büros oder Praxen) externe betriebliche Datenschutzbeauftragte bestellen dürfen. Nach dem Bundesdatenschutzgesetz (BDSG) ist ein betrieblicher Datenschutzbeauftragter zu bestellen, wenn mindestens fünf Mitarbeiter mit der automatisierten Verarbeitung, Nutzung oder Erhebung personenbezogener Daten beschäftigt sind. Oftmals ist es – insbesondere für kleinere bis mittlere Kanzleien oder Praxen – wegen der fehlenden fachlichen Eignung der eigenen Mitarbeiter nicht ausreichend oder nicht praktikabel, diese zum betrieblichen Datenschutzbeauftragten zu bestellen.

Fraglich ist allerdings, ob mit der Bestellung eines externen betrieblichen Datenschutzbeauftragten eine unbefugte Offenbarung von Berufgeheimnissen verbunden sein kann und damit eine Strafbarkeit nach § 203 Abs. 1 Nr. 1 Strafgesetzbuch (StGB) begründet wird. Um den anfragenden Stellen eine rechtsverbindliche Antwort geben zu können, habe ich die Generalstaatsanwältin um ihre rechtliche Einschätzung gebeten. Diese teilte mir mit, dass einem externen betrieblichen Datenschutzbeauftragten eines Berufsgeheimnisträgers ohne Verstoß gegen § 203 Abs. 1 Nr. 1 StGB die vom Bundesdatenschutzgesetz erfassten personenbezogenen Daten offenbart werden dürften, weil sie ihm gegenüber keine Geheimnisse darstellen würden. Allerdings lässt sich aus der Antwort der Generalstaatsanwältin keine eindeutige Schlussfolgerung herleiten, da sie weiter ausführt, dass alle Informationen über den Gegenstand des anwaltlichen Mandats für die Aufgabenerfüllung keine Bedeutung hätten und daher Geheimnisse seien, die einem Externen nicht zugänglich gemacht werden dürften. In der Praxis wird man eine Kenntnisnahme dieser Informationen nicht ausschließen können.

Daneben wurde die Problematik im Düsseldorfer Kreis (Datenschutzgremium der Obersten Aufsichtsbehörden) erörtert. Es wurde einstimmig die Auffassung vertreten, dass die Bestellung eines externen Datenschutzbeauftragten bei Berufsgeheimnisträgern zulässig sei. Unterschiedliche Auffassungen bestanden jedoch hinsichtlich der Frage, ob sich die Kontrollkompetenz eines externen Datenschutzbeauftragten auch auf die dem Berufsgeheimnis unterliegenden Daten bezieht.

Darüber hinaus hat sich auch der Bundesbeauftragte für den Datenschutz (BfD) an das Bundesministerium der Justiz gewandt. Dieses soll die Auffassung vertreten haben, dass ein Arzt sich durch die Bestellung eines externen betrieblichen Datenschutzbeauftragten auch dann nicht strafbar macht, wenn dieser im Rahmen seiner Tätigkeit Kenntnis von Daten erlange, die durch § 203 Abs. 1 Nr. 1 StGB geschützt seien. Die Bestellung eines externen betrieblichen Datenschutzbeauftragten sei in § 4 f Abs. 2 Satz 2 BDSG ausdrücklich vorgesehen. Insoweit bestehe eine Befugnis zur Offenbarung der durch § 203 Abs. 1 Nr. 1 StGB geschützten Privatgeheimnisse in dem zur Aufgabenerfüllung durch den Datenschutzbeauftragten erforderlichen Ausmaß. Dies folge aus dem Grundsatz der Einheit der Rechtsordnung.

Zur abschließenden Klärung der Frage und Rechtssicherheit für die Betroffenen wäre eine gesetzgeberische Klarstellung wünschenswert. Diesbezüglich könnte ein Gesetzesvorschlag der Länder Niedersachsen und Hessen, die Bestellung von Da-

tenschutzbeauftragten betreffend, Klarheit schaffen (Bundesrat Drs. 599/05). Darin wird folgende Regelung vorgeschlagen: „Ein nach § 4 f Abs. 2 Satz 2 BDSG bestellter Beauftragter für den Datenschutz hat dieselben Aufgaben, Rechte und Pflichten wie ein Beauftragter für den Datenschutz innerhalb der verantwortlichen Stelle. Die verantwortliche Stelle und die bei ihr tätigen Personen können sich gegenüber dem Beauftragten für den Datenschutz, soweit er seine Aufgaben wahrnimmt, nicht auf die in § 1 Abs. 3 Satz 2 BDSG genannten Geheimhaltungspflichten berufen."

18.8 Veröffentlichung von personenbezogenen Daten im Internet

Auf der Homepage eines Vereins wurden Namen und Anschrift von Mitgliedern veröffentlicht, die ihren Mitgliedsbeitrag nicht gezahlt hatten. Ich habe die Verantwortlichen darauf hingewiesen, dass die Veröffentlichung von personenbezogenen Daten der genannten Personen unzulässig ist. Die „Prangerwirkung" der namentlichen Nennung lässt die schutzwürdigen Interessen der Betroffenen eindeutig gegenüber den Interessen des Vereins überwiegen. Ich habe den Verein aufgefordert, die personenbezogenen Daten unverzüglich zu löschen. Dieser Aufforderung wurde nachgekommen.

Das war nicht der einzige Fall. In der letzten Zeit erhielt ich mehrere Eingaben, welche die Veröffentlichung von personenbezogenen Daten im Internet zum Inhalt hatten. Es wurde z. B. beanstandet, dass sensible Informationen (Gesundheitsdaten), die ein Mitglied nur innerhalb einer geschlossenen Nutzergruppe offenbart hatte, durch einen Mitnutzer der Allgemeinheit zugänglich gemacht wurde. In der Veröffentlichung von personenbezogenen Daten kann ein erheblicher Eingriff in das Recht auf informationelle Selbstbestimmung des Betroffenen liegen, da das Internet ein sehr einfach recherchierbares, weltweit verfügbares Medium ist.

Die Problematik von Internetveröffentlichungen habe ich auch auf dem Workshop der Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich angesprochen. Es bestand die einhellige Auffassung, dass eine Veröffentlichung von personenbezogenen Daten grundsätzlich nur mit Einwilligung der Betroffenen zulässig ist. Auch im Rahmen einer Interessenabwägung sind die schutzwürdigen Belange der Betroffenen an dem Ausschluss der Nutzung ihrer Daten regelmäßig höher zu bewerten als das Interesse der verantwortlichen Personen an der Veröffentlichung.

Weiterhin ist mir aufgefallen, dass viele Internetangebote kein oder nur ein unvollständiges Impressum haben. Die Impressumspflicht ergibt sich aus § 6 Teledienstegesetz bzw. § 10 Mediendienstestaatsvertrag. Hiernach ist der Betreiber der Homepage verpflichtet, die in diesen Vorschriften genannten Informationen (wie z. B. seinen Namen und Anschrift, die E-Mail-Adresse) leicht erkennbar zu veröffentlichen. Diese Angaben sollen ermöglichen, schnell mit dem Diensteanbieter Kontakt aufzunehmen und unmittelbar und effizient, etwa wegen eines Datenschutzanliegens, mit ihm zu kommunizieren. Die Möglichkeit der Kontaktaufnahme wird beispielsweise dann relevant, wenn sich Betroffene durch Angaben auf der Homepage des Verantwortlichen in ihren Rechten verletzt fühlen und ihn darauf hinweisen möchten. Darüber hinaus stellt ein fehlendes Impressum eine Ordnungswidrigkeit dar.

18.9 Einführung eines Kundenbindungssystems bei zwei Zeitungsverlagen

Ein in Bremen und ein in Bremerhaven ansässiger Zeitungsverlag haben ein neues, in der Ausgestaltung annähernd gleiches Kundenbindungssystem eingeführt. Beide Unternehmen haben mich um eine datenschutzrechtliche Beratung gebeten; ihrer Bitte bin ich gern nachgekommen.

Den Abonnenten der Verlage wird die Ausstellung einer Kundenkarte angeboten. Wollen sie an dem neuen System teilnehmen, müssen sie ein unterschriebenes Antragsformular an den Verlag senden. Unter Vorlage der Kundenkarte bekommen die Abonnenten dann beim Kauf von Ware oder Dienstleistungen bei einem der beteiligten Partnerfirmen einen Bonus, d. h. eine Gutschrift auf einem vom Verlag geführten Konto. Die Boni werden ab einer bestimmten Höhe oder spätestens am Ende eines Kalenderjahres ausgezahlt. Dabei werden die Umsätze bei den Partnerfirmen und die daraus resultierenden Boni von einem externen Dienstleister erfasst. Außerdem erhalten Karteninhaber Vergünstigungen für Angebote und Leistungen des Verlages.

Im Rahmen dieses Systems wird eine Reihe von personenbezogenen Kundendaten in verschiedenen Schritten verarbeitet. Zu den Abonnenten-Stammdaten (Name und Anschrift) werden in dem Antragsformular weitere Daten wie Geburtsdatum, Telefon- und Faxnummer sowie E-Mail-Adresse abgefragt. Da es sich bei diesen Daten um solche handelt, die für die Durchführung des Bonusprogramms nicht erforderlich sind, bedarf es insoweit der Einwilligung des Betroffenen, die jederzeit widerrufen werden kann. Aus datenschutzrechtlicher Sicht positiv ist der deutliche Hinweis auf dem Antragsformular, dass die Daten auf freiwilliger Basis erhoben werden.

Setzt ein Abonnent die Karte bei einem beteiligten Partnerunternehmen ein, erfährt dieses nach Angaben der Verlage allenfalls den auf der Karte abgedruckten Namen des Kunden. Im Übrigen erfasst das Unternehmen lediglich die Kundennummer, den jeweiligen Umsatz, das Datum sowie ggf. eine so genannte Bonusklasse, die der Unterscheidung der Bonushöhe nach Waren- bzw. Dienstleistungsart dient, und übermittelt diese auf elektronischem Wege an einen Dienstleister der Verlage. Das Konzept sieht vor, dass die Partnerunternehmen diese Daten nicht selbst speichern. Detaillierte Informationen über gekaufte Waren oder Leistungen werden nicht erhoben. Die Erstellung von Kundenprofilen, die Auskunft über Konsumverhalten geben, ist aus diesem Grund nicht möglich. Der derart gestaltete Umgang mit personenbezogenen Daten ist nach § 28 Abs. 1 Satz 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) zulässig.

Der Dienstleister der Verlage verwaltet im Rahmen eines Auftrags zur Datenverarbeitung nach § 11 BDSG die eingehenden Informationen, führt für die teilnehmenden Abonnenten ein Bonuskonto und veranlasst die Überweisung von auszuzahlenden Boni durch die Verlage. Außerdem führt er in anonymisierter Form Auswertungen durch, die den Partnerfirmen für Marketingzwecke zur Verfügung gestellt werden. Einzelne personenbezogene Daten werden dabei nicht übermittelt. Der Dienstleister hat sich gegenüber den Verlagen dazu verpflichtet, die eingehenden personenbezogenen Daten nur nach Vorgabe der Verlage für die Durchführung des Bonussystems und für anonymisierte Auswertungen zu verwenden. Die Weitergabe von Daten an Dritte ist nicht vorgesehen. Sie werden gelöscht, sobald die steuerrechtlichen Aufbewahrungsfristen abgelaufen sind. Die Teilnehmer an dem System werden über die verantwortliche Stelle, die einzelnen Datenverarbeitungsschritte sowie den Zweck der Datenerhebung in den allgemeinen Teilnahmebedingungen auf der Rückseite des Antragsformulars unterrichtet.

Insgesamt lässt sich feststellen, dass das Konzept des eingeführten Kundenbindungssystems im Vergleich mit anderen im Einzelhandel eingesetzten Systemen relativ datenschutzfreundlich ausgestaltet ist. Bisher gab es außer einigen Nachfragen über die Funktionsweise keine Beschwerden von Bürgerinnen oder Bürgern.

18.10 Videoüberwachung in Umkleidekabinen und im Kunden-WC

Regelmäßig erreichen mich eine Vielzahl von Anfragen und Eingaben zur Videoüberwachung. Da die Darstellung aller Anfragen den Rahmen dieses Berichts sprengen würde, berichte ich nur über zwei ungewöhnliche Eingaben.

In dem einen Fall wurde moniert, dass die Umkleidekabinen in einem Sportstudio videoüberwacht würden, wobei die Kameras per Bewegungsmelder aktiviert würden. Auf Anfrage erklärte der Betreiber des Sportstudios, aufgrund vermehrter Diebstähle sei dort eine nur kurzzeitige Videoüberwachung vorgenommen worden. Die Bilder aus den betroffenen Räumen seien rund um die Uhr aufgezeichnet und auf einem speziellen Speichersystem gesichert worden. Nur die Polizei hätte im Fall einer Diebstahlsanzeige die Bilddaten aus dem Aufzeichnungsgerät ausgelesen und ausgewertet. Das Studiopersonal hätte zu keiner Zeit Zugriff auf die Filmaufzeichnungen und Bilder der Kamera. Die Kameras seien inzwischen abgeschaltet worden.

Ich habe dem Betreiber unter Hinweis auf § 6 b Bundesdatenschutzgesetz (BDSG) dargelegt, dass Umkleidekabinen den Intimbereich tangieren und von Videoüberwachung generell auszuschließen und Alternativen zu prüfen sind, die weniger in das Persönlichkeitsrecht der Betroffenen eingreifen. Außerdem reicht es nicht aus, die Videokameras abzuschalten; sie müssen abmontiert werden.

Daraufhin hat der Betreiber erklärt, nunmehr hätten die Kunden die Gelegenheit, Wertsachen an der Theke im Eingangsbereich abzugeben, und die Kameras seien abmontiert worden.

Der andere Fall betraf eine Videoüberwachung in dem Kunden-WC eines großen Kaufhauses. Der Organisationsleiter des Kaufhauses begründete die Videoüberwachung damit, häufig würden Kunden Kleidungsstücke (z. B. Hosen), ohne zu bezahlen, mitnehmen und in der Kundentoilette anziehen, um dann unbemerkt das Kaufhaus zu verlassen.

Obwohl den Angaben zufolge lediglich die Waschräume überwacht worden seien, habe ich darauf hingewiesen, dass auch dieser Bereich die Privat- bzw. Intimsphäre der Betroffenen berührt, wenn beobachtet werden kann, wer wann die Kundentoilette aufsucht, so dass aus diesen Gründen die schutzwürdigen Interessen der Betroffenen überwiegen. Daraufhin erklärte das Kaufhaus, die Anlage sei abmontiert worden.

18.11 Angabe der Adressen auf Fototüten

Eine Beschwerdeführerin wandte sich dagegen, dass in der Filiale einer Drogeriemarktkette eingereichte Filme nicht entwickelt bzw. von Negativen keine Abzüge gemacht würden, wenn die Fototüten keine Anschrift enthielten. Hierauf würde in der Filiale mit einem Schild hingewiesen. Diese Fototüten lägen in dem Geschäft in offenen Behältern, so dass jeder Kunde mühelos und ohne Aufwand die Adressen und Namen der Kunden einsehen könne. Es werde nicht überprüft, ob es sich bei der Ausgabe um richtige oder falsche Adressen handele.

Eine solche Angabe mag Verwechselungen vermeiden oder eine Benachrichtigung des Betroffenen ermöglichen, aber auch zu Missbrauch einladen, dies muss aber jeweils der Betroffene selbst entscheiden können.

Auf meine Anfrage bei der Filiale hat die Zentrale der Drogeriekette daraufhin erklärt, die unselbstständige Verkaufsstelle habe eigenmächtig gehandelt. Das Schild sei inzwischen entfernt worden. Es würde allen Kunden in allen unselbstständigen Verkaufsstellen freistehen, Personen- und Adressenangaben oder Telefonnummern auf der Fototüte zu vermerken, um sodann den Kontroll- und Rückgabeabschnitt von der Fototüte zu entfernen. Dies werde nunmehr auch in der betreffenden Verkaufsstelle beachtet.

18.12 Verarbeitung personenbezogener Daten von Fahrgästen durch Kontrolleure

Im Rahmen einer Eingabe wurde mir im Jahre 2004 bekannt, dass der von der Verkehrsgesellschaft Bremerhaven AG mit Fahrausweisüberprüfungen beauftragte Sicherheitsdienst zur Überprüfung der Identität der Betroffenen über die polizeiliche Personalienfeststellung hinaus weitere Kontrollen vornimmt. In dem mir vorliegenden Beschwerdeverfahren begleitete der Kontrolleur die betroffene Schülerin zu ihrer Schule und ließ sich die Personenangaben unter Offenlegung des Sachverhaltes von der Leiterin der Oberstufe bestätigen.

Dieses Vorgehen habe ich aus datenschutzrechtlicher Sicht als unzulässig bemängelt. Die Kontrollbefugnisse des privaten Sicherheitsdienstes enden an dem Fahrzeug des öffentlichen Personennahverkehrs. Es war auch weder erforderlich noch angemessen, die Schule einzuschalten, weil dadurch Dritte Kenntnis von den Problemen bei der Fahrausweisüberprüfung erhalten haben. Ich habe die Verkehrsgesellschaft Bremerhaven AG auf die von mir geprüfte Praxis der Bremer Straßenbahn AG hingewiesen. Danach ist bei einer Fahrausweisüberprüfung, sofern sich der Betroffene nicht ausweisen kann, aber sonstige Bedenken an der Richtigkeit der Angaben bestehen, kurzfristig die Polizei zur Identitätsfeststellung beizuziehen. In Bremen ruft der Kontrolleur fernmündlich die Polizei an, identifiziert sich durch seine Rufnummer und ein Passwort und lässt sich die Angaben des Betroffenen bestätigen. Ein entsprechendes Verfahren zur Personalienüberprüfung bei Ticketkontrollen wurde daraufhin zum 1. Januar 2005 zwischen der Verkehrsgesellschaft Bremerhaven, dem von ihr beauftragten Sicherheitsdienst und der Ortspolizeibehörde Bremerhaven vereinbart.

18.13 Fußball-WM 2006: Ticketingverfahren

Mit dem 1. Februar des Berichtsjahres begann die erste von fünf Verkaufsphasen für die Tickets zur Fußball-Weltmeisterschaft 2006 in Deutschland. Während der Verkaufsphasen konnte online über das Internet, postalisch oder per Fax auf dem offiziellen Bestellformular der FIFA eine Kartenbestellung abgegeben werden. Im

Bestellformular mussten Name, Vorname, Straße, Postleitzahl, Stadt, Land, Nationalität, Geschlecht, Geburtsdatum, Ausweisnummer und bei Online-Bestellungen eine E-Mail-Adresse angegeben werden, daneben Angaben zu dem gewünschten Ticket und der Zahlungsweise. Da die Nachfrage die Anzahl der vorhandenen Tickets überstieg, erfolgte anschließend eine Zuordnung nach dem Zufallsprinzip durch Auslosung. Die erfolgreichen Besteller erhielten eine Bestätigung.

Mit den Datenschutzbeauftragten des Bundes und anderer Länder wie auch den Datenschutzaufsichtsbehörden anderer Länder betrachte ich das personalisierte Ticket-Konzept unter Einsatz von RFID-Technologie mit großer Sorge. Es ist aus datenschutzrechtlicher Sicht grundsätzlich abzulehnen, dass Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen dürfen. Im Rahmen des Bestellvorgangs wurden entgegen dem Gebot der Datenvermeidung und -sparsamkeit mehr Daten erhoben als für den Erwerb des Tickets erforderlich, unter anderem die vollständige Angabe des Geburtsdatums und die komplette Pass- oder Ausweisnummer. Die von den Käufern beim Ticketerwerb abzugebende Einwilligungserklärung für die Nutzung ihrer personenbezogenen Daten war unzureichend. Der Erklärung ließen sich die einzelnen Werbepartner nicht entnehmen. Auch wurde auf eine weitere Datenübermittlung durch die Werbepartner an Dritte nicht hingewiesen. Schließlich erweckte die Einwilligungserklärung in ihrer ursprünglichen Ausgestaltung den Anschein, eine Zustimmung sei für die Teilnahme am Auslosungsverfahren zwingend. Es ist ferner zweifelhaft, ob die mit der Personalisierung der Tickets verfolgten Ziele, die Unterbindung des „Schwarzmarkthandels“ und die größtmögliche Sicherheit in den Stadien, erreicht werden können. Angesichts des Massenandrangs bei Stadioneinlass werden in der Praxis an den Stadieneingängen aus Zeitgründen kaum mehr als Stichproben durchgeführt werden können. Die umfangreiche Erhebung personenbezogener Daten von weltweit mehreren Millionen Personen im Rahmen des Ticket-Auslosungsverfahrens wurde von den Veranstaltern allein auf die Einwilligung der Betroffenen gestützt. Die Abstimmung des Inhalts der Datenschutzinformation erfolgte nur schleppend und in unbefriedigender Weise, auch wenn eine Reihe von datenschutzrechtlichen Verbesserungen bei den Verhandlungen erreicht werden konnte. Hinsichtlich der Akkreditierung von Beschäftigten bei der Fußball-WM vgl. Ziff. 9.9 dieses Berichts.

18.14 Datenübermittlungen in Drittstaaten

In letzter Zeit sind vermehrt Unternehmen an mich herangetreten, die Daten in Drittstaaten übermitteln wollen, die ich umfassend berate; in einem Fall wurde bei mir ein Genehmigungsverfahren eingeleitet. Aus diesem Grund stelle ich im Folgenden dar, was hierbei zu beachten ist.

Bevor die Zulässigkeit einer Datenübermittlung in Drittstaaten geprüft werden kann, ist zu klären, ob die der Übermittlung zu Grunde liegenden Daten nach deutschem Datenschutzrecht in zulässiger Weise verarbeitet werden. Eine Datenverarbeitung, die gegen die Bestimmungen des Bundesdatenschutzgesetzes (BDSG) verstößt, kann nicht Grundlage für eine Datenübermittlung in Drittstaaten sein.

Innerhalb der Europäischen Union (EU) und für Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum (EWR) gilt der Grundsatz des freien Datenverkehrs. Für die Beurteilung der Zulässigkeit von Übermittlungen personenbezogener Daten an Stellen außerhalb der EU und des EWR ist eine dreistufige Prüfung vorzunehmen (§ 4 b und c BDSG):

— Besteht ein angemessenes Datenschutzniveau? Nach § 4 b Abs. 2 Satz 2 BDSG hat eine Datenübermittlung in Drittstaaten zu unterbleiben, wenn schutzwürdige Interessen der Betroffenen entgegenstehen. Ein schutzwürdiges Interesse liegt vor, wenn beim Datenempfänger kein angemessenes Datenschutzniveau gegeben ist. Ein angemessenes Datenschutzniveau wurde u. a. durch die Europäische Kommission aufgrund der dortigen Rechtslage für Argentinien, Guernsey, Isle of Man, Kanada und die Schweiz festgestellt. Außerdem gibt es für die USA die so genannte Safe-Harbor-Liste. Das zwischen der EU und dem US-Handelsministerium ausgehandelte Safe-Harbor-Verfahren soll ein angemessenes Datenschutzniveau gewährleisten. Voraussetzung ist, dass das US-Unternehmen sich durch Erklärung gegenüber der zuständigen US-Behörde zur Einhaltung bestimmter Datenschutzprinzipien verpflichtet. Die Liste der Unternehmen ist unter http://www.export.gov/safeharbor abrufbar.

— Greift trotz mangelhaftem Datenschutzniveau einer der Erlaubnistatbestände in § 4 c Abs. 1 BDSG? Eine Erlaubnis kann sich z. B. aus der Einwilligung der Betroffenen in die Datenübermittlung oder aufgrund eines wichtigen öffentlichen Interesses ergeben.

— Können angemessene Garantien durch zu genehmigende Vertragsklauseln oder verbindliche Unternehmensregelungen nach § 4 c Abs. 2 BDSG geschaffen werden? Es besteht die Möglichkeit nach § 4 c Abs. 2 BDSG, dass die zuständige Aufsichtsbehörde (in Bremen ist das der Landesbeauftragte für den Datenschutz) einzelne Übermittlungen oder bestimmte Arten von Übermittlungen genehmigen kann, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte aufweist. Diese Garantien können sich insbesondere aus Vertragsklauseln und verbindlichen Unternehmensregelungen ergeben.

Vertragsklauseln können u. a. verwendet werden, wenn ein oder mehrere Unternehmen in Europa Daten zu einem Unternehmen in einen Drittstaat übermitteln wollen. Hierfür muss ein Vertrag zwischen dem Datenübermittler und -empfänger geschlossen werden. Dies gilt auch für Niederlassungen und Mutterkonzerne, da es im Datenschutz kein Privileg für Konzerne gibt. Ich empfehle den Unternehmen, die von der Europäischen Kommission genehmigten Standardvertragsklauseln zu verwenden. Wenn die EU-Standardvertragsklauseln wörtlich übernommen werden, besteht keine Genehmigungspflicht seitens der Aufsichtsbehörden. Darüber hinaus sind sie für alle Mitgliedstaaten verbindlich. Es gibt zum einen die von der Europäischen Kommission entwickelten Standardvertragsklauseln aus dem Jahr 2001 und zum anderen die von mehreren Wirtschaftsverbänden unter der Federführung der Internationalen Handelskammer (ICC) der Europäischen Kommission vorgelegten alternativen Standardvertragsklauseln von Ende 2004. Die Entscheidung der Kommission zu den Standardvertragsklauseln ist unter folgender Internetadresse zu finden: http://europa.eu.int/comm/justice_home/fsj/privacy/modelcontracts/index_de.htm

Will ein Unternehmen die internationalen Datenflüsse allgemein regeln, so sollte dies durch verbindliche Unternehmensregelungen erfolgen. Diese muss das Unternehmen der zuständigen Aufsichtsbehörde vorlegen (hinsichtlich einer Genehmigungspflicht bestehen abweichende Auffassungen zwischen den Aufsichtsbehörden). Zunächst ist aber seitens des Unternehmens zu prüfen, wo es tatsächlich seinen europäischen Hauptsitz hat (vgl. hierzu WP 108 der Artikel-29-Datenschutzgruppe „Muster-Checkliste für Anträge auf Genehmigungen verbindlicher unternehmensinterner Datenschutzregelungen“). Zuständig für die Antragsbearbeitung ist nämlich die Aufsichtsbehörde des Hauptsitzlandes.

18.15 Telefonische Mahnungen durch Computer-Anruf

Wem ist es noch nicht passiert? Eine nette Stimme mit leichtem Akzent ruft an und zunächst denkt man, es solle sich ein Gespräch entwickeln. Aber schon bald merkt man, die andere Seite reagiert gar nicht auf eigene Einwendungen, sondern predigt ihren Text weiter herunter. Wenige Augenblicke später hat sich die Situation so verfremdet, dass einem klar wird, es handelt sich nicht um einen leibhaftigen Menschen am anderen Ende der Leitung, sondern um einen Computer-Anruf.

Um wie viel überraschter würde man sein, wenn der Computeranruf für die Lieferung einer bestimmten Ware die Zahlung einer überfälligen Rechnung anmahnen würde. Zu dieser Methode gehen aber zunehmend große Unternehmen, speziell Versandhäuser über. Offene Rechnungen per Computer-Anruf telefonisch anzumahnen, sei nach Aussage der Unternehmen kostengünstiger als schriftliche Mahnungen.

Aus Sicht des Datenschutzes ergeben sich bei einer telefonischen Mahnung per Computer-Anruf dann Bedenken, wenn nicht sichergestellt ist, dass der Kunde selbst das Gespräch entgegennimmt, sondern z. B. ein anderes Familienmitglied, im Haushalt Beschäftigte oder andere, und so Informationen über eine Bestellung und eine nicht bezahlte Rechnung Dritten bekannt werden.

Telefonische Mahnungen durch Computer-Anruf dürfen nur mit Einwilligung des Kunden und unter bestimmten vorher festgelegten Verfahrensregularien, wie die Bekanntgabe einer vom Kunden bestimmten Telefonnummer, durchgeführt werden. Die Beratungen hierzu sind unter den Aufsichtsbehörden noch nicht abgeschlossen.

18.16 Umfang der Daten auf einem Online-Bewerberformular

Eine Firma suchte über das Internet Personen, die in Bereichen wie Marketing, Meinungsumfragen etc. eingesetzt werden sollten. Hierzu wurde ein Online-Bewerberformular für potentielle Bewerber bereitgehalten, auf dem eine Vielzahl von Angaben verlangt werden.

Ich habe der Firma mitgeteilt, dass die Erhebung von Religionszugehörigkeit, Nationalität, Sozialversicherungsdaten, Angaben über Kinder und Steuerklasse zumindest in diesem ersten Stadium des Bewerbungsverfahrens nicht erforderlich und demzufolge unzulässig ist. Angaben über Religionszugehörigkeit und Nationalität sind besondere Arten von Daten und unterliegen besonderen Erhebungsbefugnissen. Angaben über Konfektionsgröße, sonstige Fähigkeiten und Hobbys sind überhaupt nicht erforderlich.

Das Unternehmen hat daraufhin die vorgenannten Daten aus dem Online-Bewerberformular entfernt.

18.17 Fotos von Beschäftigten in einer Werkszeitung und im Internet

Der Betriebsrat eines Unternehmens hat mich gefragt, ob und ggf. unter welchen Voraussetzungen die Veröffentlichung von für Werksausweise angefertigten Fotos Beschäftigter einschließlich der damit zusammenhängenden Personalangaben in der Werkszeitung oder auf der Internetseite des Unternehmens zulässig ist.

Eine betriebsinterne wie auch eine weltweite Veröffentlichung personenbezogener Daten via Internet stellt eine Verarbeitung dar, die ohne Einwilligung des Betroffenen nur unter den Voraussetzungen des § 28 Bundesdatenschutzgesetz (BDSG) zulässig ist.

Insoweit war zu prüfen, ob die Veröffentlichung dieser (Bild-)Daten zur Wahrung der berechtigten Interessen des Unternehmens erforderlich ist und schutzwürdige Interessen des Betroffenen an dem Ausschluss dieser Verarbeitung nicht überwiegen (§ 28 Abs. 1 Nr. 2 BDSG).

Der Arbeitgeber kann es durchaus für erforderlich halten, das besondere Jubiläum eines Beschäftigten einschließlich des Werdegangs in der Werkszeitung zu erwähnen. Gleichwohl hat er vorher zu klären, ob der Betroffene schutzwürdige Interessen hat, die gegen die Veröffentlichung in dieser Weise sprechen. Besonders beachtlich ist hierbei, dass insoweit auch vertraulich zu behandelnde Personaldaten Dritten zugänglich gemacht werden, obwohl diese Daten regelmäßig nur zu Personalverwaltungszwecken verwendet werden und nur Berechtigte Zugang dazu haben dürfen.

Soweit Fotos veröffentlicht werden sollen, die eigens für die im Betrieb vorgeschriebenen Werksausweise angefertigt wurden, stellt dies eine Nutzungsänderung dar. Da eine Veröffentlichung dieser Bilder im Internet ein „Verbreiten“ im Sinne des Kunsturhebergesetzes (KUrhG) darstellt, sind die Regelungen zum Recht am eigenen Bild anwendbar.

Als einzige rechtmäßige Maßnahme kommt die vorherige Einwilligung des Beschäftigten nach § 4 a Abs. 1 BDSG in Frage. Willigt der Betroffene nicht ein, ist eine derartige Veröffentlichung nicht zulässig.

18.18 Vergabe von Ausbildungsplätzen nach einem öffentlichen Lauf-Casting

Nach einem Zeitungsartikel sollte im Rahmen des 1. City-Marathons in Bremerhaven ein Lauf-Casting für junge Leute ausgerichtet werden, die einen Ausbildungsplatz suchen. Da dem Zeitungsartikel zufolge die Industrie- und Handelskammer (IHK) dieses Casting unterstützen wollte, habe ich zunächst dort nachgefragt. Diese hat jede Unterstützung bestritten, allerdings mir Name und Anschrift des Veranstalters des 1. City-Marathons mitgeteilt.

Ich habe den Veranstalter vorsorglich darauf hingewiesen, dass vor der Besetzung von Ausbildungsplätzen regelmäßig Bewerbungsverfahren durchgeführt werden und dass auch bei einem Lauf-Casting die Bewerberdaten vertraulich zu behandeln sind.

Außerdem bleibt ein ungutes Gefühl, wenn Ausbildungsplatz suchende Jugendliche aufgrund der Ausbildungsnot mehr oder weniger gezwungen werden, sich öffentlich zur Schau zu stellen, weil sie existentiell auf einen Ausbildungsplatz an-

gewiesen sind. Daraufhin hat der Veranstalter mitgeteilt, auf das Lauf-Casting zu verzichten.

18.19 Verfahrensregister

Nach § 4 d Abs. 1 Bundesdatenschutzgesetz (BDSG) haben nicht-öffentliche Stellen der zuständigen Aufsichtsbehörde Verfahren automatisierter Verarbeitungen zu melden. Ohne Ausnahme von dieser Meldepflicht betroffen sind nach § 4 d BDSG automatisierte Verarbeitungen, in denen geschäftsmäßig personenbezogene Daten von der nicht-öffentlichen Stelle zum Zweck der Übermittlung (z. B. von Auskunfteien und Adresshandelsunternehmen) oder zum Zweck der anonymisierten Übermittlung (z. B. von Markt- und Meinungsforschungsinstituten) gespeichert werden. Ich schrieb daher im Berichtsjahr wiederholt Unternehmen der Privatwirtschaft an, bei denen ich vermutete, dass sie der Meldepflicht unterliegen, und bat sie, mir ggf. die erforderliche Registermeldung zukommen zu lassen. In dem von meiner Behörde geführten Verfahrensregister werden nunmehr acht Stellen geführt, wobei es sich um drei Auskunfteien, drei Markt- und Meinungsforschungsinstitute, ein Adresshandelsunternehmen und eine Detektei/Auskunftei handelt.

19. Die Entschließungen der Datenschutzkonferenzen im Jahr 2005

19.1 Einführung der elektronischen Gesundheitskarte

(Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10./11. März 2005)

Die Datenschutzbeauftragten des Bundes und der Länder begleiten aufmerksam die Einführung der elektronischen Gesundheitskarte. Sie weisen darauf hin, dass die über die Karte erfolgende Datenverarbeitung nach den gesetzlichen Vorgaben weitgehend aufgrund der Einwilligung der Versicherten erfolgen muss. Um die hierfür nötige Akzeptanz bei den Versicherten zu erlangen, sind neben den rechtlichen auch die tatsächlichen – technischen wie organisatorischen – Voraussetzungen zu schaffen, dass sowohl das Patientengeheimnis als auch die Wahlfreiheit bei der Datenspeicherung und -übermittlung gewahrt sind.

Die Versicherten müssen darüber informiert werden, welche Datenverarbeitungsprozesse mit der Karte durchgeführt werden können, wer hierfür verantwortlich ist und welche Bestimmungsmöglichkeiten sie hierbei haben. Das Zugriffskonzept auf medizinische Daten muss technisch so realisiert werden, dass in der Grundeinstellung das Patientengeheimnis auch gegenüber und zwischen Angehörigen der Heilberufe umfassend gewahrt bleibt. Die Verfügungsbefugnis der Versicherten über ihre Daten, wie sie bereits in den Entschließungen zur 47. und 50. Datenschutzkonferenz gefordert wurde, muss durch geeignete Maßnahmen sichergestellt werden, um die Vertraulichkeit der konkreten elektronischen Kommunikationsbeziehungen unter Kontrolle der Betroffenen entsprechend dem gegenwärtigen technischen Stand zu gewährleisten.

Vor der obligatorischen flächendeckenden Einführung der elektronischen Gesundheitskarte sind die Verfahren und Komponenten auf ihre Funktionalität, ihre Patientenfreundlichkeit und ihre Datenschutzkonformität hin zu erproben und zu prüfen. Die Tests und Pilotversuche müssen ergebnisoffen ausgestaltet werden, damit die datenschutzfreundlichste Lösung gefunden werden kann. Eine vorzeitige Festlegung auf bestimmte Verfahren sollte deshalb unterbleiben.

Für die Bewertung der Gesundheitskarte und der neuen Telematikinfrastruktur können unabhängige Gutachten und Zertifizierungen förderlich sein, wie sie ein Datenschutz-Gütesiegel und ein Datenschutz-Audit vorsehen. Vorgesehene Einführungstermine dürfen kein Anlass dafür sein, dass von den bestehenden Datenschutzanforderungen Abstriche gemacht werden.

19.2 Datenschutzbeauftragte plädieren für Eingrenzung der Datenverarbeitung bei der Fußball-Weltmeisterschaft 2006

(Entschließung der 69. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 10./11. März 2005)

Die Datenschutzbeauftragten des Bundes und der Länder betrachten das Vergabeverfahren für die Eintrittskarten zur Fußball-Weltmeisterschaft 2006 mit großer

Sorge. Bei der Bestellung von Tickets müssen die Karteninteressentinnen und -interessenten ihre persönlichen Daten wie Name, Geburtsdatum, Adresse, Nationalität sowie ihre Ausweisdaten angeben, um bei der Ticketvergabe berücksichtigt zu werden. Die Datenschutzbeauftragten befürchten, dass mit der Personalisierung der Eintrittskarten eine Entwicklung angestoßen wird, in deren Folge die Bürgerinnen und Bürger nur nach Preisgabe ihrer persönlichen Daten an Veranstaltungen teilnehmen können.

Es wird deshalb gefordert, dass nur die personenbezogenen Daten erhoben werden, die für die Vergabe unbedingt erforderlich sind. Rechtlich problematisch ist insbesondere die vorgesehene Erhebung und Verarbeitung der Pass- bzw. Personalausweisnummer der Karteninteressentinnen und -interessenten. Der Gesetzgeber wollte die Gefahr einer Nutzung der Ausweis-Seriennummer als eindeutige Personenkennziffer ausschließen. Die Seriennummer darf damit beim Ticketverkauf nicht als Ordnungsmerkmal gespeichert werden. Zur Legitimation der Ticketinhaberin bzw. -inhabers beim Zutritt zu den Stadien ist sie nicht erforderlich. Das Konzept der Ticketvergabe sollte daher überarbeitet werden. Eine solche Vergabepraxis darf nicht zum Vorbild für den Ticketverkauf auf Großveranstaltungen werden. Solche Veranstaltungen müssen grundsätzlich ohne Identifizierungszwang besucht werden können.

19.3 Eine moderne Informationsgesellschaft braucht mehr Datenschutz

(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht für die 16. Legislaturperiode des Deutschen Bundestags großen Handlungsbedarf im Bereich des Datenschutzes. Der Weg in eine freiheitliche und demokratische Informationsgesellschaft unter Einsatz modernster Technologie zwingt alle Beteiligten, ein verstärktes Augenmerk auf den Schutz des Rechts auf informationelle Selbstbestimmung zu legen. Ohne wirksameren Datenschutz werden die Fortschritte vor allem in der Informations- und der Biotechnik nicht die für Wirtschaft und Verwaltung notwendige gesellschaftliche Akzeptanz finden.

Es bedarf einer grundlegenden Modernisierung des Datenschutzrechtes. Hierzu gehört eine Ergänzung des bisher auf Kontrolle und Beratung basierenden Datenschutzrechtes um Instrumente des wirtschaftlichen Anreizes, des Selbstdatenschutzes und der technischen Prävention. Es ist daher höchste Zeit, dass in dieser Legislaturperiode vom Deutschen Bundestag ein Datenschutz-Audit-Gesetz erarbeitet wird. Datenschutzkonforme Technikgestaltung als Wettbewerbsanreiz liegt im Interesse von Wirtschaft, Verwaltung und Bevölkerung. Zugleich ist die ins Stocken geratene umfassende Novellierung des Bundesdatenschutzgesetzes mit Nachdruck voranzutreiben. Eine Vereinfachung und Konzentration der rechtlichen Regelungen kann Bürokratie abbauen und zugleich den Grundrechtsschutz stärken.

Die Bürgerinnen und Bürger müssen auch in Zukunft frei von Überwachung sich informieren und miteinander kommunizieren können. Nur so können sie in der Informationsgesellschaft ihre Grundrechte selbstbestimmt in Anspruch nehmen. Dem laufen Bestrebungen zuwider, mit dem Argument einer vermeintlich höheren Sicherheit immer mehr alltägliche Aktivitäten der Menschen elektronisch zu registrieren und für Sicherheitszwecke auszuwerten. Die längerfristige Speicherung auf Vorrat von Verkehrsdaten bei der Telekommunikation, die zunehmende Videoüberwachung im öffentlichen Raum, die anlasslose elektronische Erfassung des Straßenverkehrs durch Kfz-Kennzeichenabgleich, die Erfassung biometrischer Merkmale der Bevölkerung oder Bestrebungen zur Ausdehnung der Rasterfahndung betreffen ganz überwiegend völlig unverdächtige Bürgerinnen und Bürger und setzen diese der Gefahr der Ausforschung ihrer Lebensgewohnheiten und einem ständig wachsenden Anpassungsdruck aus, ohne dass dem immer ein adäquater Sicherheitsgewinn gegenübersteht. Freiheit und Sicherheit bedingen sich wechselseitig Angesichts zunehmender Überwachungsmöglichkeiten kommt der Freiheit vor staatlicher Beobachtung und Ausforschung sowie dem Grundsatz der Datensparsamkeit und Datenvermeidung eine zentrale Bedeutung zu.

Den Sicherheitsbehörden steht bereits ein breites Arsenal an gesetzlichen Eingriffsbefugnissen zur Verfügung, das teilweise überstürzt nach spektakulären Verbrechen geschaffen worden ist. Diese Eingriffsbefugnisse der Sicherheitsbehörden müs-

sen einer umfassenden systematischen Evaluierung durch unabhängige Stellen unterworfen und öffentlich zur Diskussion gestellt werden. Unangemessene Eingriffsbefugnisse, also solche, die mehr schaden als nützen, sind wieder zurückzunehmen.

Die Kontrolle der Bürgerinnen und Bürger wird auch mit den Argumenten der Verhinderung des Missbrauchs staatlicher Leistungen und der Erhöhung der Steuerehrlichkeit vorangetrieben. So richtig es ist, in jedem Einzelfall die Voraussetzungen für staatliche Hilfen zu prüfen und bei hinreichenden Anhaltspunkten Steuerhinterziehungen nachzugehen, so überflüssig und rechtsstaatlich problematisch ist es, alle Menschen mit einem Pauschalverdacht zu überziehen und Sozial- und Steuerverwaltung mit dem Recht auszustatten, verdachtsunabhängig Datenabgleiche mit privaten und öffentlichen Datenbeständen vorzunehmen. Es muss verhindert werden, dass mit dem Argument der Leistungs- und Finanzkontrolle die Datenschutzgrundsätze der Zweckbindung und der informationellen Gewaltenteilung auf der Strecke bleiben.

Die Entwicklung in Medizin und Biotechnik macht eine Verbesserung des Schutzes des Patientengeheimnisses notwendig. Telemedizin, der Einsatz von High-Tech im Gesundheitswesen, gentechnische Verfahren und eine intensivierte Vernetzung der im Gesundheitsbereich Tätigen können zu einer Verbesserung der Qualität der Gesundheitsversorgung und zugleich zur Kosteneinsparung beitragen. Zugleich drohen die Vertraulichkeit der Gesundheitsdaten und die Wahlfreiheit der Patientinnen und Patienten verloren zu gehen. Diese bedürfen dringend des gesetzlichen Schutzes, u. a. durch ein modernes Gendiagnostikgesetz und durch datenschutz- und patientenfreundliche Regulierung der Computermedizin.

Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, insbesondere durch neue Möglichkeiten der Kontrolle bei der Nutzung elektronischer Kommunikationsdienste, Videotechnik, Funksysteme und neue biotechnische Verfahren. Schranken werden bisher nur im Einzelfall durch Arbeitsgerichte gesetzt. Das seit vielen Jahren vom Deutschen Bundestag geforderte Arbeitnehmerdatenschutzgesetz muss endlich für beide Seiten im Arbeitsleben Rechtsklarheit und Sicherheit schaffen.

Die Datenschutzkontrolle hat mit der sich fast explosionsartig entwickelnden Informationstechnik nicht Schritt gehalten. Immer noch findet die Datenschutzkontrolle in manchen Ländern durch nachgeordnete Stellen statt. Generell sind Personalkapazität und technische Ausstattung unzureichend. Dem steht die europarechtliche Anforderung entgegen, die Datenschutzaufsicht in völliger Unabhängigkeit auszuüben und diese adäquat personell und technisch auszustatten.

Die Europäische Union soll ein „Raum der Freiheit, der Sicherheit und des Rechts“ werden. Die Datenschutzbeauftragten des Bundes und der Länder sind sich bewusst, dass dies zu einer verstärkten Zusammenarbeit der Strafverfolgungsbehörden bei der Verbrechensbekämpfung in der Europäischen Union führen wird.

Die grenzüberschreitende Zusammenarbeit von Polizei- und Justizbehörden darf jedoch nicht zur Schwächung von Grundrechtspositionen der Betroffenen führen. Der vermehrte Austausch personenbezogener Daten setzt deshalb ein hohes und gleichwertiges Datenschutzniveau in allen EU-Mitgliedstaaten voraus. Dabei ist von besonderer Bedeutung, dass die Regelungen in enger Anlehnung an die Datenschutzrichtlinie 95/46/EG erfolgen, damit ein möglichst einheitlicher Datenschutz in der Europäischen Union gilt, der nicht zuletzt dem Ausgleich zwischen Freiheitsrechten und Sicherheitsbelangen dienen soll.

Die Datenschutzbeauftragten des Bundes und der genannten Länder appellieren an die Fraktionen im Bundestag und an die künftige Bundesregierung, sich verstärkt für den Grundrechtsschutz in der Informationsgesellschaft einzusetzen.

19.4 Gravierende Datenschutzmängel beim Arbeitslosengeld II endlich beseitigen

(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass bei der Umsetzung der Zusammenlegung von Arbeitslosenhilfe und Sozialhilfe weiterhin erhebliche datenschutzrechtliche Mängel bestehen. Die Rechte der Betroffenen werden dadurch stark beeinträchtigt. Zwar ist das Verfahren der Daten-

erhebung durch die unter Beteiligung der Datenschutzbeauftragten des Bundes und der Länder überarbeiteten Antragsvordrucke auf dem Weg, datenschutzkonform ausgestaltet zu werden. Bei der Leistungs- und Berechnungssoftware A2LL gibt es jedoch entgegen den Zusagen des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und der Bundesagentur für Arbeit (BA) immer noch keine erkennbaren Fortschritte.

Weder ist ein klar definiertes Zugriffsberechtigungskonzept umgesetzt, noch erfolgt eine Protokollierung der lesenden Zugriffe. Damit ist es über 40.000 Mitarbeiterinnen und Mitarbeitern in der BA und den Arbeitsgemeinschaften nach SGB II (ARGEn) nach wie vor möglich, voraussetzungslos auf die Daten aller Leistungsempfänger und -empfängerinnen zuzugreifen, ohne dass eine Kontrolle möglich wäre.

Dies gilt auch für das elektronische Vermittlungsverfahren coArb, das ebenfalls einen bundesweiten lesenden Zugriff erlaubt. Äußerst sensible Daten, wie z. B. Vermerke über Schulden-, Ehe- oder Suchtprobleme, können so eingesehen werden. Den Datenschutzbeauftragten sind bereits Missbrauchsfälle bekannt geworden. Einzelne ARGEn reagieren auf die Probleme und speichern ihre Unterlagen wieder in Papierform. Es muss sichergestellt sein, dass das Nachfolgesystem VerBIS, das Mitte 2006 einsatzbereit sein soll, grundsätzlich nur noch einen engen, regionalen Zugriff zulässt und ein detailliertes Berechtigungs- und Löschungskonzept beinhaltet. Der Datenschutz muss auch bei der Migration der Daten aus coArb in VerBIS beachtet werden.

Mit Unterstützung der Datenschutzbeauftragten des Bundes und der Länder hat die BA den Antragsvordruck und die Zusatzblätter überarbeitet. Soweit die Betroffenen auch die ergänzenden neuen Ausfüllhinweise erhalten, wird ihnen ein datenschutzgerechtes Ausfüllen der Unterlagen ermöglicht und damit eine Erhebung von nicht erforderlichen Daten vermieden. Doch ist immer noch festzustellen, dass die bisherigen Ausfüllhinweise nicht überall verfügbar sind. Es ist daher zu gewährleisten, dass allen Betroffenen nicht nur baldmöglichst die neuen Antragsvordrucke, sondern diese gemeinsam mit den Ausfüllhinweisen ausgehändigt werden („Paketlösung“).

Es handelt sich bei den ARGEn um eigenverantwortliche Daten verarbeitende Stellen, die uneingeschränkt der Kontrolle der Landesbeauftragten für Datenschutz unterliegen. Dies haben die Bundesanstalt und die ARGEn zu akzeptieren. Es ist nicht hinnehmbar, dass über die Verweigerung einer Datenschutzkontrolle rechtsfreie Räume entstehen und damit in unzumutbarer Weise in die Rechte der Betroffenen eingegriffen wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die BA und die sonstigen verantwortlichen Stellen auf Bundes- und Länderebene auf, selbst und im Rahmen ihrer Rechtsaufsicht die Datenschutzmissstände beim Arbeitslosengeld II zu beseitigen. Für den Fall einer völligen Neugestaltung des Systems A2LL wegen der offenbar nicht zu beseitigenden Defizite erwarten die Datenschutzbeauftragten ihre zeitnahe Beteiligung. Es ist sicherzustellen, dass die datenschutzrechtlichen Vorgaben, wie die Protokollierung der lesenden Zugriffe und ein klar definiertes Zugriffsberechtigungs- und Löschungskonzept, ausreichend berücksichtigt werden, um den Schutz des informationellen Selbstbestimmungsrechts zu gewährleisten.

19.5 Telefonbefragungen von Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II datenschutzgerecht gestalten

(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist anlässlich von durch die Bundesanstalt mit Hilfe privaten Callcentern durchgeführten Telefonbefragungen bei Leistungsbeziehern und Leistungsbezieherinnen von Arbeitslosengeld II darauf hin, dass es den Betroffenen unbenommen ist, sich auf ihr Grundrecht auf informationelle Selbstbestimmung zu berufen. Da die Befragung freiwillig war, hatten sie das Recht, die Beantwortung von Fragen am Telefon zu verweigern.

Die Ablehnung der Teilnahme an einer solchen Befragung rechtfertigt nicht den Verdacht auf Leistungsmissbrauch. Wer seine Datenschutzrechte in Anspruch nimmt, darf nicht deshalb des Leistungsmissbrauchs bezichtigt werden.

Die Konferenz fordert daher das Bundesministerium für Wirtschaft und Arbeit und die Bundesanstalt für Arbeit dazu auf, die Sach- und Rechtslage klarzustellen und bei der bereits angekündigten neuen Telefonaktion eine rechtzeitige Beteiligung der Datenschutzbeauftragten sicherzustellen.

19.6 Unabhängige Datenschutzkontrolle in Deutschland gewährleisten

(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005)

Anlässlich eines von der Europäischen Kommission am 5. Juli 2005 eingeleiteten Vertragsverletzungsverfahrens gegen die Bundesrepublik Deutschland zur Unabhängigkeit der Datenschutzkontrolle fordert die Konferenz erneut eine völlig unabhängige Datenschutzkontrolle.

Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (EG-Datenschutzrichtlinie) verlangt, dass die Einhaltung datenschutzrechtlicher Vorschriften in den Mitgliedstaaten von Stellen überwacht wird, die die ihnen zugewiesenen Aufgaben in völliger Unabhängigkeit wahrnehmen. In Deutschland ist indessen die Datenschutzkontrolle der Privatwirtschaft überwiegend in den Weisungsstrang der jeweiligen Innenverwaltung eingebunden. Diese Aufsichtsstruktur bei der Datenschutzkontrolle der Privatwirtschaft verstößt nach Ansicht der Europäischen Kommission gegen Europarecht.

Die Datenschutzbeauftragten des Bundes und der Länder können eine einheitliche Datenschutzkontrolle des öffentlichen und privaten Bereichs in völliger Unabhängigkeit sicherstellen. Sie sollten dazu in allen Ländern und im Bund als eigenständige Oberste Behörden eingerichtet werden, die keinen Weisungen anderer administrativer Organe unterliegen.

Demgegenüber ist die in Niedersachsen beabsichtigte Rückübertragung der Datenschutzkontrolle des privatwirtschaftlichen Bereichs vom Landesdatenschutzbeauftragten auf das Innenministerium ein Schritt in die falsche Richtung. Die Konferenz wendet sich entschieden gegen diese Planung und fordert den Bund sowie alle Länder auf, zügig europarechtskonforme Aufsichtsstrukturen im deutschen Datenschutz zu schaffen.

19.7 Schutz des Kernbereichs privater Lebensgestaltung bei verdeckten Datenerhebungen der Sicherheitsbehörden

(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005)

Aus dem Urteil des Bundesverfassungsgerichts vom 27. Juli 2005 zur präventiven Telekommunikationsüberwachung nach dem niedersächsischen Polizeigesetz folgt, dass der durch die Menschenwürde garantierte unantastbare Kernbereich privater Lebensgestaltung im Rahmen aller verdeckten Datenerhebungen der Sicherheitsbehörden uneingeschränkt zu gewährleisten ist. Bestehen im konkreten Fall Anhaltspunkte für die Annahme, dass eine Überwachungsmaßnahme Inhalte erfasst, die zu diesem Kernbereich zählen, ist sie nicht zu rechtfertigen und muss unterbleiben (Erhebungsverbot). Für solche Fälle reichen bloße Verwertungsverbote nicht aus.

Die Gesetzgeber in Bund und Ländern sind daher aufgerufen, alle Regelungen über verdeckte Ermittlungsmethoden diesen gerichtlichen Vorgaben entsprechend auszugestalten.

Diese Verpflichtung erstreckt sich auch auf die Umsetzung der gerichtlichen Vorgabe zur Wahrung des rechtsstaatlichen Gebots der Normenbestimmtheit und Normenklarheit. Insbesondere im Bereich der Vorfeldermittlungen verpflichtet dieses Gebot die Gesetzgeber aufgrund des hier besonders hohen Risikos einer Fehlprognose, handlungsbegrenzende Tatbestandselemente für die Tätigkeit der Sicherheitsbehörden zu normieren.

Im Rahmen der verfassungskonformen Ausgestaltung der Vorschriften sind die Gesetzgeber darüber hinaus verpflichtet, die gerichtlichen Vorgaben im Hinblick auf die Wahrung des Verhältnismäßigkeitsgrundsatzes – insbesondere die Angemessenheit der Datenerhebung – und eine strikte Zweckbindung umzusetzen.

In der Entscheidung vom 27. Juli 2005 hat das Gericht erneut die Bedeutung der – zuletzt auch in seinen Entscheidungen zum Großen Lauschangriff und zum Außenwirtschaftsgesetz vom 3. März 2004 dargelegten – Verfahrenssicherungen zur Gewährleistung der Rechte der Betroffenen hervorgehoben. So verpflichtet beispielsweise das Gebot der effektiven Rechtsschutzgewährung die Sicherheitsbehörden, Betroffene über die verdeckte Datenerhebung zu informieren.

Diese Grundsätze sind sowohl im Bereich der Gefahrenabwehr als auch im Bereich der Strafverfolgung, u. a. bei der Novellierung der §§ 100 a und 100 b StPO, zu beachten.

Die Konferenz der DSB erwartet, dass nunmehr zügig die erforderlichen Gesetzgebungsarbeiten in Bund und Ländern zum Schutz des Kernbereichs privater Lebensgestaltung bei allen verdeckten Ermittlungsmaßnahmen aufgenommen und die Vorgaben des Bundesverfassungsgerichts ohne Abstriche umgesetzt werden.

19.8 Telefonieren mit Internettechnologie (Voice over IP – VoIP)

(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005)

Die Internet-Telefonie verbreitet sich rasant. Mittlerweile bieten alle großen Provider in Deutschland das Telefonieren über das Internet an. Dabei ist den Kunden und Kundinnen oft nicht bekannt, dass diese Verbindungen in den meisten Fällen noch wesentlich unsicherer sind als ein Telefongespräch über das herkömmliche Festnetz.

Bei Telefongesprächen über das Internet kommt die Internet-Technologie Voice over IP (VoIP) zum Einsatz. In zunehmendem Maße wird angeboten, Telefongespräche mit Hilfe der Internet-Technologie VoIP zu führen. Das Fernmeldegeheimnis ist auch für die Internet-Telefonie zu gewährleisten. Während jedoch bei separaten, leitungsvermittelten Telekommunikationsnetzen Sicherheitskonzepte vorzulegen sind, ist dies bei VoIP bisher nicht die Praxis. Vielmehr werden diese Daten mit Hilfe des aus der Internetkommunikation bekannten Internet-Protokolls (IP) in Datenpakete unterteilt und paketweise über bestehende lokale Computernetze und/oder das offene Internet übermittelt.

Eine derartige Integration von Sprache und Daten in ein gemeinsames Netzwerk stellt den Datenschutz vor neue Herausforderungen. Die aus der Internetnutzung und dem Mail-Verkehr bekannten Unzulänglichkeiten und Sicherheitsprobleme können sich bei der Integration der Telefonie in die Datennetze auch auf die Inhalte und näheren Umstände der VoIP-Kommunikation auswirken und den Schutz des Fernmeldegeheimnisses beeinträchtigen. Beispielsweise können VoIP-Netzwerke durch automatisierte Versendung von Klingelrundrufen oder Überflutung mit Sprachpaketen blockiert, Inhalte und nähere Umstände der VoIP-Kommunikation mangels Verschlüsselung ausgespäht, kostenlose Anrufe durch Erschleichen von Authentifizierungsdaten geführt oder Schadsoftware wie Viren oder Trojaner aktiv werden. Darüber hinaus ist nicht auszuschließen, dass das Sicherheitsniveau der vorhandenen Datennetze negativ beeinflusst wird, wenn sie auch für den VoIP-Sprachdaten-Verkehr genutzt werden. Personenbezogene Daten der VoIP-Nutzenden können außerdem dadurch gefährdet sein, dass Anbieter von VoIP-Diensten ihren Sitz mitunter im außereuropäischen Ausland haben und dort möglicherweise weniger strengen Datenschutzanforderungen unterliegen als Anbieter mit Sitz in der Europäischen Union (EU).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert deshalb Hersteller und Herstellerinnen, Anbieter und Anbieterinnen sowie Anwender und Anwenderinnen von VoIP-Lösungen auf, das grundgesetzlich geschützte Fernmeldegeheimnis auch bei VoIP zu wahren und hierfür

— angemessene technische und organisatorische Maßnahmen zu treffen, um eine sichere und datenschutzgerechte Nutzung von VoIP in einem Netzwerk zu ermöglichen,

— Verschlüsselungsverfahren für VoIP anzubieten bzw. angebotene Verschlüsselungsmöglichkeiten zu nutzen,

— Sicherheits- und Datenschutzmängel, die die verwendeten Protokolle oder die genutzte Software bisher mit sich bringen, durch Mitarbeit an der Entwicklung möglichst schnell zu beseitigen,

— auf die Verwendung von offenen, standardisierten Lösungen zu achten beziehungsweise die verwendeten Protokolle und Algorithmen offenzulegen,

— VoIP-Kunden über die Gefahren und Einschränkungen gegenüber dem klassischen, leitungsvermittelten Telefondienst zu informieren und

— bei VoIP alle datenschutzrechtlichen Vorschriften genauso wie bei der klassischen Telefonie zu beachten.

In den benutzten Netzen, auf den beteiligten Servern und an den eingesetzten Endgeräten müssen angemessene Sicherheitsmaßnahmen umgesetzt werden, um die Verfügbarkeit, die Vertraulichkeit, die Integrität und die Authentizität der übertragenen Daten zu gewährleisten.

19.9 Vorratsdatenspeicherung in der Telekommunikation

(Entschließung der 70. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. Oktober 2005)

Die Europäische Kommission hat den Entwurf einer Richtlinie über die Vorratsspeicherung von Daten über die elektronische Kommunikation vorgelegt. Danach sollen alle Telekommunikationsanbieter und Internet-Provider verpflichtet werden, systematisch eine Vielzahl von Daten über jeden einzelnen Kommunikationsvorgang über einen längeren Zeitraum (ein Jahr bei Telefonaten, sechs Monate bei Internet-Nutzung) für mögliche Abrufe von Sicherheitsbehörden selbst dann zu speichern, wenn sie diese Daten für betriebliche Zwecke (z. B. zur Abrechnung) gar nicht benötigen. Die Annahme dieses Vorschlags oder des gleichzeitig im Ministerrat beratenen, weiter gehenden Entwurfs eines Rahmenbeschlusses und ihre Umsetzung in nationales Recht würde einen Dammbruch zulasten des Datenschutzes unverdächtiger Bürgerinnen und Bürger bedeuten. Sowohl das grundgesetzlich geschützte Fernmeldegeheimnis als auch der durch die Europäische Menschenrechtskonvention garantierte Schutz der Privatsphäre drohen unverhältnismäßig eingeschränkt und in ihrem Wesensgehalt verletzt zu werden.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre bereits seit 2002 geäußerte grundsätzliche Kritik an jeder Pflicht zur anlassunabhängigen Vorratsdatenspeicherung. Die damit verbundenen Eingriffe in das Fernmeldegeheimnis und das informationelle Selbstbestimmungsrecht lassen sich auch nicht durch die Bekämpfung des Terrorismus rechtfertigen, weil sie unverhältnismäßig sind. Insbesondere gibt es keine überzeugende Begründung dafür, dass eine solche Maßnahme in einer demokratischen Gesellschaft zwingend notwendig wäre.

Die anlassunabhängige Vorratsdatenspeicherung aller Telefon- und Internetdaten ist von großer praktischer Tragweite und widerspricht den Grundregeln unserer demokratischen Gesellschaft. Erfasst würden nicht nur die Daten über die an sämtlichen Telefongesprächen und Telefax-Sendungen beteiligten Kommunikationspartner und -partnerinnen, sondern auch der jeweilige Zeitpunkt und die Dauer der Einwahl ins Internet, die dabei zugeteilte IP-Adresse, ferner die Verbindungsdaten jeder einzelnen E-Mail und jeder einzelnen SMS sowie die Standorte jeder Mobilkommunikation. Damit ließen sich europaweite Bewegungsprofile für einen Großteil der Bevölkerung für einen längeren Zeitraum erstellen.

Die von einigen Regierungen (z. B. der britischen Regierung nach den Terroranschlägen in London) gemachten Rechtfertigungsversuche lassen keinen eindeutigen Zweck einer solchen Maßnahme erkennen, sondern reichen von den Zwecken der Terrorismusbekämpfung und der Bekämpfung des organisierten Verbrechens bis hin zur allgemeinen Straftatenverfolgung. Alternative Regelungsansätze wie das in den USA praktizierte anlassbezogene Vorhalten („Einfrieren“ auf Anordnung der Strafverfolgungsbehörden und „Auftauen“ auf richterlichen Beschluss) sind bisher nicht ernsthaft erwogen worden.

Mit einem Quick-freeze-Verfahren könnte man dem Interesse einer effektiven Strafverfolgung wirksam und zielgerichtet nachkommen.

Der Kommissionsvorschlag würde zu einer personenbezogenen Datensammlung von beispiellosem Ausmaß und zweifelhafter Eignung führen. Eine freie und unbefangene Telekommunikation wäre nicht mehr möglich. Jede Person, die in Zukunft solche Netze nutzt, würde unter Generalverdacht gestellt. Jeder Versuch, die zweckgebundene oder befristete Verwendung dieser Datensammlung auf Dauer sichern zu wollen, wäre zum Scheitern verurteilt. Derartige Datenbestände würden Begehr-

lichkeiten wecken, aufgrund derer die Hürde für einen Zugriff auf diese Daten immer weiter abgesenkt werden könnten. Auch aus diesem Grund muss bereits den ersten Versuchen, eine solche Vorratsdatenspeicherung einzuführen, entschieden entgegengetreten werden. Zudem ist eine Ausweitung der Vorratsdatenspeicherung auch auf Inhaltsdaten zu befürchten. Schon jetzt ist die Trennlinie zwischen Verkehrs- und Inhaltsdaten gerade bei der Internetnutzung nicht mehr zuverlässig zu ziehen. Dieselben – unzutreffenden – Argumente, die jetzt für eine flächendeckende Speicherung von Verkehrsdaten angeführt werden, würden bei einer Annahme des Kommissionsvorschlags alsbald auch für die anlassfreie Speicherung von Kommunikationsinhalten auf Vorrat ins Feld geführt werden.

Die Konferenz appelliert an die Bundesregierung, den Bundestag und das Europäische Parlament, einer Verpflichtung zur systematischen und anlasslosen Vorratsdatenspeicherung auf europäischer Ebene nicht zuzustimmen. Auf der Grundlage des Grundgesetzes wäre eine anlasslose Vorratsdatenspeicherung verfassungswidrig.

19.10 Gleichsetzung der DNA-Analyse mit dem Fingerabdruck

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Bundesratsinitiative mehrerer Länder zur Ausweitung der DNA-Analyse im Umlaufverfahren/17. Februar 2005)

Die strafprozessuale DNA-Analyse ist – insbesondere in Fällen der Schwerstkriminalität wie bei Tötungsdelikten – ein effektives Fahndungsmittel. Dies hat zu Forderungen nach der Ausweitung ihres Anwendungsbereichs zur Identitätsfeststellung in künftigen Strafverfahren geführt. So sieht ein Gesetzesantrag mehrerer Bundesländer zum Bundesratsplenum vom 18. Februar 2005 die Streichung des Richtervorbehalts und der materiellen Erfordernisse einer Anlasstat von erheblicher Bedeutung sowie der Prognose weiterer schwerer Straftaten vor.

Das zur Begründung derartiger Vorschläge herangezogene Argument, die DNA-Analyse könne mit dem herkömmlichen Fingerabdruck gleichgesetzt werden, trifft jedoch nicht zu:

Zum einen hinterlässt jeder Mensch permanent Spurenmaterial z. B. in Form von Hautschuppen oder Haaren. Dies ist ein Grund für den Erfolg des Fahndungsinstruments „DNA-Analyse“, weil sich Täter vor dem Hinterlassen von Spuren nicht so einfach schützen können, wie dies bei Fingerabdrücken möglich ist. Es birgt aber – auch unter Berücksichtigung der gebotenen vorsichtigen Beweiswürdigung – in erhöhtem Maße die Gefahr, dass Unbeteiligte aufgrund zufällig hinterlassener Spuren am Tatort unberechtigten Verdächtigungen ausgesetzt werden oder dass sogar bewusst DNA-Material Dritter am Tatort ausgestreut wird.

Zum anderen lassen sich bereits nach dem derzeitigen Stand der Technik aus den so genannten nicht-codierenden Abschnitten der DNA über die Identitätsfeststellung hinaus Zusatzinformationen entnehmen (Verwandtschaftsbeziehungen, wahrscheinliche Zugehörigkeit zu ethnischen Gruppen, aufgrund der räumlichen Nähe einzelner nicht-codierender Abschnitte zu codierenden Abschnitten möglicherweise Hinweise auf bestimmte Krankheiten). Die Feststellung des Geschlechts ist bereits nach geltendem Recht zugelassen. Nicht absehbar ist schließlich, welche zusätzlichen Erkenntnisse aufgrund des zu erwartenden Fortschritts der Analysetechniken zukünftig möglich sein werden.

Mit gutem Grund hat daher das Bundesverfassungsgericht in zwei Entscheidungen aus den Jahren 2000 und 2001 die Verfassungsmäßigkeit der DNA-Analyse zu Zwecken der Strafverfolgung nur im Hinblick auf die derzeitigen Voraussetzungen einer vorangegangenen Straftat von erheblicher Bedeutung, einer Prognose weiterer schwerer Straftaten und einer richterlichen Anordnung bejaht. Es hat besonders gefordert, dass diese Voraussetzungen auch nach den Umständen des Einzelfalls gegeben sein müssen und von der Richterin oder dem Richter genau zu prüfen sind.

Eine Prognose schwerer Straftaten und eine richterliche Anordnung müssen im Hinblick auf diese Rechtsprechung und den schwerwiegenden Eingriff in das Recht auf informationelle Selbstbestimmung, den die DNA-Analyse darstellt, auch zukünftig Voraussetzung einer derartigen Maßnahme bleiben.

Die besondere Qualität dieses Grundrechtseingriffs muss auch im Übrigen bei allen Überlegungen, die derzeit zu einer möglichen Erweiterung des Anwendungs-

bereichs der DNA-Analyse angestellt werden, den Maßstab bilden; dies schließt eine Gleichsetzung in der Anwendung dieses besonderen Ermittlungswerkzeugs mit dem klassischen Fingerabdruckverfahren aus.

19.11 Einführung biometrischer Ausweisdokumente

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Umlaufverfahren vom 1. Juni 2005)

Obwohl die Verordnung Nr. 2252/2004 des Europäischen Rates vom 13. Dezember 2004 die Mitgliedstaaten verpflichtet, bis Mitte 2006 mit der Ausgabe biometriegestützer Pässe für die Bürgerinnen und Bürger der Europäischen Union zu beginnen, sollen in Deutschland noch im laufenden Jahr die ersten Pässe ausgegeben werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist der Auffassung, dass mit der Ausgabe von elektronisch lesbaren biometrischen Ausweisdokumenten erst begonnen werden kann, wenn die technische Reife, der Datenschutz und die technische und organisatorische Sicherheit der vorgesehenen Verfahren gewährleistet sind. Diese Voraussetzungen sind bisher jedoch noch nicht in ausreichendem Maße gegeben.

Daher sind in einem umfassenden Datenschutz- und IT-Sicherheitskonzept zunächst technische und organisatorische Maßnahmen zur Wahrung des Rechts auf informationelle Selbstbestimmung festzulegen. Darüber hinaus sind im Passgesetz Regelungen zur strikten Zweckbindung der Daten erforderlich.

Die Konferenz begrüßt das Eintreten des Europäischen Parlaments für verbindliche Mindestanforderungen biometriegestützter Pässe zur Verhinderung des Missbrauchs, insbesondere des heimlichen Auslesens und der Manipulation der Daten. Die Konferenz bedauert es jedoch, dass die Einführung dieser Pässe beschlossen wurde, ohne dass die Chancen und Risiken der Technik ausreichend diskutiert wurden. Besonders problematisch ist es, dass die Entscheidung durch den Europäischen Rat der Regierungsvertreter entgegen der entsprechenden Stellungnahme des Europäischen Parlaments und der nationalen Gesetzgeber der EU-Mitgliedstaaten getroffen wurde.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Einführung biometrischer Merkmale nicht automatisch zur Verbesserung der Sicherheit führt. Noch immer weisen manche biometrische Identifikationsverfahren hohe Falscherkennungsraten auf und sind oft mit einfachsten Mitteln zu überwinden. Scheinbar besonders sichere Ausweisdokumente werden durch den Einsatz unsicherer biometrischer Verfahren somit plötzlich zu einem Risikofaktor. Fehler bei der Erkennung von Personen haben zudem erhebliche Konsequenzen für die Betroffenen, weil sie einem besonderen Rechtfertigungsdruck und zusätzlichen Kontrollmaßnahmen ausgesetzt werden.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine objektive Bewertung von biometrischen Verfahren und tritt dafür ein, die Ergebnisse entsprechender Untersuchungen und Pilotprojekte zu veröffentlichen und die Erkenntnisse mit der Wissenschaft und der breiten Öffentlichkeit zu diskutieren. Mit der Ausgabe von elektronisch lesbaren, biometrischen Ausweisdokumenten darf erst begonnen werden, wenn durch rechtliche, organisatorische und technische Maßnahmen gewährleistet wird,

— dass die biometrischen Merkmale ausschließlich von den für die Passkontrollen zuständigen Behörden für hoheitliche Zwecke genutzt werden,

— dass die in Ausweisen gespeicherten Daten mit den biometrischen Merkmalen nicht als Referenzdaten genutzt werden, um Daten aus unterschiedlichen Systemen und Kontexten zusammenzuführen,

— dass die für die Ausstellung und das Auslesen verwendeten Geräte nach internationalen Standards von einer unabhängigen Stelle zertifiziert werden,

— dass die verwendeten Lesegeräte in regelmäßigen zeitlichen Intervallen durch eine zentrale Einrichtung authentisiert werden,

— dass eine verbindliche Festlegung der zur Ausgabe oder Verifikation von Dokumenten zugriffsberechtigten Stellen erfolgt,

— dass vor der Einführung biometrischer Ausweise Verfahren festgelegt werden, die einen Datenmissbrauch beim Erfassen der Referenzdaten (sicheres Enrollment), beim weiteren Verfahren und bei der Kartennutzung verhindern,

— dass diese Verfahrensfestlegungen durch eine unabhängige Stelle evaluiert werden.

Darüber hinaus muss sichergestellt sein, dass keine zentralen oder vernetzten Biometriedatenbanken geschaffen werden. Die biometrischen Identifizierungsdaten dürfen ausschließlich auf dem jeweiligen Ausweisdokument gespeichert werden. Durch international festzulegende Standards sowie Vorschriften und Vereinbarungen ist anzustreben, dass die bei Grenzkontrollen erhobenen Ausweisdaten weltweit nur gemäß eines noch festzulegenden einheitlichen hohen Datenschutz- und IT-Sicherheitsstandards verarbeitet werden.

19.12 Sicherheit bei eGovernment durch Nutzung des Standards OSCI

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Umlaufverfahren vom 15. Dezember 2005)

In modernen eGovernment-Verfahren werden personenbezogene Daten zahlreicher Fachverfahren zwischen unterschiedlichen Verwaltungsträgern in Bund, Ländern und Kommunen übertragen. Die Vertraulichkeit, Integrität und Zurechenbarkeit der übertragenen Daten kann nur gewährleistet werden, wenn dem Stand der Technik entsprechende Verschlüsselungs- und Signaturverfahren genutzt werden.

Mit dem Online Services Computer Interface (OSCI) steht bereits ein bewährter Sicherheitsstandard für eGovernment-Anwendungen zur Verfügung. Verfahren, die diese Standards berücksichtigen, bieten die Gewähr für eine durchgehende Sicherheit bei der Datenübermittlung vom Versand bis zum Empfang (Ende-zu-Ende-Sicherheit) und erlauben somit auch rechtsverbindliche Transaktionen zwischen den beteiligten Kommunikationspartnerinnen und -partnern.

Die durchgehende Sicherheit darf nicht dauerhaft durch Vermittlungs- und Übersetzungsdienste, die nicht der OSCI-Spezifikation entsprechen, beeinträchtigt werden. Werden solche Dienste zusätzlich in die behördlichen Kommunikationsströme eingeschaltet, wird das mit OSCI-Transport erreichbare Sicherheitsniveau abgesenkt. Der Einsatz von so genannten Clearingstellen, wie sie zunächst für das automatisierte Meldeverfahren vorgesehen sind, kann daher nur eine Übergangslösung sein.

Werden Programme und Schnittstellen auf der Basis derartiger Standards entwickelt, ist sichergestellt, dass die Produkte verschiedener Anbieterinnen und Anbieter im Wettbewerb grundlegende Anforderungen des Datenschutzes und der Datensicherheit in vergleichbar hoher Qualität erfüllen. Gleichzeitig erleichtern definierte Standards den öffentlichen Verwaltungen die Auswahl datenschutzkonformer, interoperabler Produkte.

Vor diesem Hintergrund begrüßt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder die vom Koordinierungsausschuss Automatisierte Datenverarbeitung (KoopA ADV), dem gemeinsamen Gremium von Bund, Ländern und Kommunalen Spitzenverbänden, getroffene Festlegung, in eGovernment-Projekten den Standard OSCI-Transport für die Übermittlung von personenbezogenen Daten einzusetzen. Um die angestrebte Ende-zu-Ende-Sicherheit überall zu erreichen, empfiehlt sie einen flächendeckenden Aufbau einer OSCI-basierten Infrastruktur.

20. Die Entschließungen der Internationalen Konferenz der Datenschutzbeauftragten

20.1 Erklärung von Montreux: „Ein universelles Recht auf den Schutz personenbezogener Daten und der Privatsphäre unter Beachtung der Vielfalt in einer globalisierten Welt“

(Entschließung der 27. Internationalen Konferenz der Datenschutzbeauftragten in Montreux [Schweiz] vom 16. September 2005)

Die Beauftragten für Datenschutz und den Schutz der Privatsphäre sind auf ihrer 27. Internationalen Konferenz in Montreux (14. bis 16. September 2005) übereingekommen, die Anerkennung des universellen Charakters der Datenschutzgrundsätze zu fördern, und haben folgende Schlusserklärung angenommen:

Die Datenschutzbeauftragten

1. entsprechen der bei der 22. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Venedig verabschiedeten Erklärung,

2. erinnern an die auf der 25. Internationalen Konferenz der Beauftragten für Datenschutz und den Schutz der Privatsphäre in Sydney angenommene Entschließung über den Datenschutz und die internationalen Organisationen,

3. stellen fest, dass die Entwicklung der Informationsgesellschaft durch die Globalisierung des Informationsaustausches, den Einsatz zunehmend invasiver Datenverarbeitungstechnologien und verstärkte Sicherheitsmaßnahmen beherrscht wird,

4. sind besorgt angesichts der wachsenden Risiken einer allgegenwärtigen Personenüberwachung auf der ganzen Welt,

5. verweisen auf die Vorteile und potentiellen Risiken der neuen Informationstechnologien,

6. sind besorgt über die weiterhin bestehenden Abweichungen zwischen den Rechtssystemen in verschiedenen Teilen der Welt und insbesondere über den mancherorts herrschenden Mangel an Datenschutzgarantien, der einen effektiven und globalen Datenschutz untergräbt,

7. sind sich bewusst, dass aufgrund des rasch wachsenden Kenntnisstandes im Bereich der Genetik Daten über die menschliche DNA zu den sensibelsten überhaupt werden können und dass die Gewährleistung eines angemessenen rechtlichen Schutzes dieser Daten angesichts der beschleunigten Wissensentwicklung wachsende Bedeutung erlangt,

8. erinnern daran, dass die Erhebung personenbezogener Daten und ihre spätere Verarbeitung im Einklang mit den Erfordernissen des Datenschutzes und des Schutzes der Privatsphäre erfolgen müssen,

9. anerkennen die in einer demokratischen Gesellschaft bestehende Notwendigkeit einer wirksamen Bekämpfung des Terrorismus und des organisierten Verbrechens, wobei jedoch daran zu erinnern ist, dass dieses Ziel unter Achtung der Menschenrechte und insbesondere der menschlichen Würde besser erreicht werden kann,

10. sind der Überzeugung, dass das Recht auf Datenschutz und den Schutz der Privatsphäre in einer demokratischen Gesellschaft unabdingbare Voraussetzung für die Gewährleistung der Rechte der Personen, des freien Informationsverkehr und einer offenen Marktwirtschaft ist,

11. sind überzeugt, dass das Recht auf Datenschutz und den Schutz der Privatsphäre ein grundlegendes Menschenrecht ist,

12. sind überzeugt, dass die universelle Geltung dieses Rechts verstärkt werden muss, um eine weltweite Anerkennung der Grundsatzregeln für die Verarbeitung personenbezogener Daten unter gleichzeitiger Beachtung der rechtlichen, politischen, wirtschaftlichen und kulturellen Vielfalt durchzusetzen,

13. sind überzeugt, dass allen Bürgern und Bürgerinnen der Welt bei der Verarbeitung sie betreffender personenbezogener Daten ohne jegliche Diskriminierung individuelle Rechte zugesichert werden müssen,

14. erinnern daran, dass der Weltgipfel zur Informationsgesellschaft (Genf 2003) in seiner Grundsatzerklärung und seinem Aktionsplan die Bedeutung des Datenschutzes und des Schutzes der Privatsphäre für die Entwicklung der Informationsgesellschaft hervorgehoben hat,

15. erinnern daran, dass die internationale Arbeitsgruppe für den Datenschutz in der Telekommunikation empfiehlt, im Rahmen multilateraler Abkommen den von ihr im Jahre 2000 erarbeiteten zehn Geboten zum Schutz der Privatheit Rechnung zu tragen,

16. anerkennen, dass die Datenschutzprinzipien auf verbindlichen und nicht verbindlichen internationalen Rechtsurkunden beruhen, namentlich den Leitlinien der OECD für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten, dem Übereinkommen des

Europarates zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, den Richtlinien der Vereinten Nationen betreffend personenbezogene Daten in automatisierten Dateien, der europäischen Richtlinie 95/46 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr und den Datenschutz-Leitsätzen der Asian Pacific Economic Cooperation (APEC),

17. erinnern daran, dass es sich dabei insbesondere um folgende Prinzipien handelt:

— Prinzip der Zulässigkeit und Rechtmäßigkeit der Erhebung und Verarbeitung der Daten,

— Prinzip der Richtigkeit,

— Prinzip der Zweckgebundenheit,

— Prinzip der Verhältnismäßigkeit,

— Prinzip der Transparenz,

— Prinzip der individuellen Mitsprache und namentlich der Garantie des Zugriffsrechts für die betroffenen Personen,

— Prinzip der Nicht-Diskriminierung,

— Prinzip der Sicherheit,

— Prinzip der Haftung,

— Prinzip einer unabhängigen Überwachung und gesetzlicher Sanktionen,

— Prinzip des angemessenen Schutzniveaus bei grenzüberschreitendem Datenverkehr.

In Anbetracht dieser Erwägungen

bekunden die Datenschutzbeauftragten ihren Willen, den universellen Charakter dieser Grundsätze zu stärken. Sie vereinbaren eine Zusammenarbeit insbesondere mit den Regierungen und den internationalen und supranationalen Organisationen bei der Ausarbeitung eines universellen Übereinkommens zum Schutz des Menschen bei der Verarbeitung personenbezogener Daten.

Zu diesem Zweck ersuchen die Datenschutzbeauftragten

a. die Organisation der Vereinten Nationen um Vorbereitung einer verbindlichen Rechtsurkunde, in der das Recht auf Datenschutz und Schutz der Privatsphäre als vollstreckbare Menschenrechte im Einzelnen aufgeführt werden;

b. sämtliche Regierungen der Welt, sich für die Annahme von Rechtsurkunden zum Datenschutz und zur Wahrung der Privatsphäre gemäß den Grundprinzipien des Datenschutzes einzusetzen, auch in ihren gegenseitigen Beziehungen;

c. den Europarat, gemäß Artikel 23 des Übereinkommens zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten die Nichtmitgliedstaaten des Europarates, die über eine Datenschutzgesetzgebung verfügen, zum Beitritt zu dem Übereinkommen und seinem Zusatzprotokoll aufzufordern.

Zudem ermutigen die Datenschutzbeauftragten

die Staats- und Regierungschefs, die sich im Rahmen des Weltgipfels zur Informationsgesellschaft in Tunis (16. bis 18. November 2005) versammeln, in ihre Schlusserklärung die Verpflichtung aufzunehmen, einen Rechtsrahmen zu entwickeln oder zu verstärken, der das Recht auf Privatsphäre und den Schutz der Personendaten aller Bürgerinnen und Bürger der Informationsgesellschaft gewährleistet, im Einklang mit der Verpflichtung, die die iberoamerikanischen Staats- und Regierungschefs im November 2003 in Santa Cruz (Bolivien) sowie die Staats- und Regierungschefs der frankophonen Länder am Gipfel in Ouagadougou (November 2004) eingegangen sind.

Die Datenschutzbeauftragten richten im Weiteren eine Aufforderung an

a. die internationalen und supranationalen Organisationen, damit diese sich verpflichten, mit den wichtigsten internationalen Urkunden betreffend den Datenschutz und den Schutz der Privatsphäre vereinbare Grundsätze einzu-

halten und insbesondere unabhängige und mit Kontrollbefugnissen ausgestattete Aufsichtsbehörden einzurichten;

b. die internationalen nichtstaatlichen Organisationen wie Wirtschafts- und Handelsverbände oder Verbraucherorganisationen zur Ausarbeitung von Normen, die auf den Grundprinzipien des Datenschutzes beruhen oder mit diesen Prinzipien im Einklang sind;

c. die Hersteller von Informatikmaterial und Software zur Entwicklung von Produkten und Systemen, deren integrierte Technologien den Schutz der Privatsphäre gewährleisten.

Die Datenschutzbeauftragten kommen außerdem überein,

a. namentlich den Informationsaustausch, die Koordinierung ihrer Überwachungstätigkeiten, die Entwicklung gemeinsamer Standards, die Förderung der Information über die Aktivitäten und die Entschließungen der Konferenz zu verstärken;

b. die Zusammenarbeit mit den Staaten zu fördern, die noch nicht über unabhängige Datenschutz-Aufsichtsbehörden verfügen;

c. den Informationsaustausch mit den im Bereich des Datenschutzes und des Schutzes der Privatsphäre tätigen nichtstaatlichen internationalen Organisationen zu fördern;

d. mit den Datenschutzberatern von Organisationen zusammenzuarbeiten;

e. eine ständige Website einzurichten, die insbesondere als gemeinsame Informations- und Ressourcenverwaltungsdatenbank dienen soll.

Die Beauftragen für den Datenschutz und den Schutz der Privatsphäre vereinbaren, die Zielvorgaben der vorliegenden Erklärung regelmäßig auf ihre Verwirklichung zu überprüfen. Eine erste Beurteilung wird anlässlich der 28. Internationalen Konferenz im Jahre 2006 erfolgen.

20.2 Resolution zur Verwendung der Biometrie in Pässen, Identitätskarten und Reisedokumenten

(Entschließung der 27. Internationalen Konferenz der Datenschutzbeauftragten in Montreux [Schweiz] vom 16. September 2005)

Die 27. Internationale Konferenz der Datenschutzbeauftragten beschließt:

In Anbetracht der Tatsache, dass Regierungen und internationale Organisationen, namentlich die Internationale Zivilluftfahrtorganisation (ICAO), sich zurzeit anschicken, Vorschriften und technische Normen zur Integration biometrischer Daten (Fingerabdrücke, Gesichtserkennung) in Pässe und Reisedokumente zu beschließen, um zum einen den Terrorismus bekämpfen und zum anderen Grenzkontrollen und Check-in-Verfahren beschleunigen zu können;

wissend, dass auch im Privatsektor zunehmend biometrische Daten verarbeitet werden, meistens auf freiwilliger Basis;

unter Berücksichtigung des Umstandes, dass biometrische Daten gesammelt werden können, ohne dass die betroffene Person Kenntnis davon erhält, da sie biometrische Spuren unbewusst hinterlassen kann;

im Hinblick darauf, dass die Biometrie den menschlichen Körper „maschinenlesbar“ machen wird und dass biometrische Daten als weltweit einheitlicher Identifikator benutzt werden könnten;

unter Hinweis darauf, dass die verbreitete Verwendung der Biometrie weitreichende Folgen für die Weltgesellschaft haben wird und deshalb Gegenstand einer offen geführten weltweiten Diskussion bilden sollte;

fordert die Konferenz

1. wirksame Schutzmaßnahmen, die zu einem möglichst frühen Zeitpunkt Anwendung finden sollen, damit die der Biometrie inhärenten Risiken vermindert werden können,

2. die strikte Trennung zwischen biometrischen Daten, die auf der Grundlage gesetzlicher Verpflichtungen zu öffentlichen Zwecken (z. B. Grenzkontrollen) ge-

sammelt und gespeichert werden, und solchen, die mit Einwilligung zu Vertragszwecken gesammelt und gespeichert werden,

3. die technischen Beschränkungen der Verwendung biometrischer Daten in Pässen und Identitätskarten auf den Zweck der Identifizierung durch Vergleich der Daten des Dokuments mit Daten des Dokumenteninhabers im Moment der Dokumentvorlage.

20.3 Resolution zur Verwendung von Personendaten für die politische Kommunikation

(Entschließung der 27. Internationalen Konferenz der Datenschutzbeauftragten in Montreux [Schweiz] vom 16. September 2005)

In Erwägung, dass politische Kommunikation ein grundlegendes Instrument für die Beteiligung der Bürgerinnen und Bürger, der politischen Kräfte und der Kandidatinnen und Kandidaten am Leben einer Demokratie ist, und in Anerkennung der Wichtigkeit der Freiheit der politischen Meinungsäußerung als ein Grundrecht;

in Erwägung, dass gelebte Staatsbürgerschaft das Recht der Bürgerinnen und Bürger voraussetzt, im Rahmen von Wahlkampagnen von Politik und Verwaltung Informationen zu erhalten und angemessen informiert zu werden; in Erwägung, dass diese Rechte auch geeignet sind, um bei weiteren Themen, Ereignissen und politischen Positionen in Kenntnis der Sachlage seine Wahl zu anderen Themen des politischen Lebens treffen zu können, sei es bei Referenden, bei der Wahl von Kandidatinnen und Kandidaten oder beim Zugang zu Informationen innerhalb politischer Organisationen oder von gewählten Amtsträgern;

in Erwägung, dass die politischen Kräfte und politischen Organisationen im Allgemeinen sowie gewählte Abgeordnete sich verschiedener Formen der Kommunikation und der Geldmittelbeschaffung bedienen und Informationsquellen und neue Technologien nutzen, um direkte und persönliche Kontakte mit verschiedensten Kategorien von betroffenen Personen zu knüpfen;

in Erwägung, dass in einer wachsenden Zahl von Ländern ein Trend hin zu immer stärkerer institutioneller Kommunikation gewählter Kandidatinnen und Kandidaten und Körperschaften zu beobachten ist, ebenfalls auf lokaler Ebene und mittels eGovernment; in der Erwägung, dass diese Aktivitäten, die die Verarbeitung von Personendaten voraussetzen können, in Einklang stehen mit dem Recht der Staatsbürgerinnen und -bürger, über die Tätigkeiten der gewählten Kandidatinnen und Kandidaten und Körperschaften informiert zu werden;

in Erwägung, dass in diesem Rahmen von politischen Organisationen fortlaufend eine große Menge von Personendaten gesammelt und manchmal in aggressiver Art und Weise verwendet werden, unter Anwendung verschiedener Techniken wie Umfragen, Sammlung von E-Mail-Adressen mittels geeigneter Software oder Suchmaschinen, flächendeckender Stimmenwerbung in Städten oder Formen politischer Entscheidbildung durch interaktives Fernsehen oder Computerdateien, die die Herausfilterung einzelner Stimmenden erlauben; in Erwägung, dass in diesen Daten – zusätzlich zu elektronischen Adressen, Telefonnummern, E-Mail-Konten, Informationen über berufliche Tätigkeiten und familiäre Verhältnisse – zuweilen unrechtmäßig auch sensible Daten enthalten sein können wie Informationen über – tatsächliche oder bloß vermutete – ethische oder politische Überzeugungen oder Aktivitäten oder über das Wahlverhalten;

in Erwägung, dass von verschiedenen Personen invasive Profile erstellt und sie klassifiziert werden – manchmal unzutreffenderweise oder auf der Grundlage eines flüchtigen Kontakts – als solche, die mit einer bestimmten politischen Strömung sympathisieren, sie unterstützen, ihr angehören oder gar Parteimitglieder sind, um so mit bestimmten Gruppen von Bürgerinnen und Bürgern vermehrt persönlich kommunizieren zu können;

in Erwägung, dass diese Aktivitäten gesetzeskonform und ordnungsgemäß ausgeübt werden müssen;

in Erwägung, dass es nötig ist, die Grundrechte und Grundfreiheiten der betroffenen Personen zu schützen und mit geeigneten Maßnahmen zu verhindern, dass diese Personen ungerechtfertigtes Eindringen in ihre Privatsphäre erfahren, Schaden erleiden oder ihnen Kosten entstehen, dass sie namentlich negative Auswirkungen und mögliche Diskriminierungen erleiden oder auf die Ausübung bestimmter Formen der politischen Beteiligung verzichten müssen;

in Erwägung, dass es möglich sein sollte, das Schutzziel zu erreichen, indem sowohl die Interessen der Öffentlichkeit an bestimmten Formen politischer Kommunikation als auch angemessene Modalitäten und Garantien in Bezug auf die Kommunikation mit Parteimitgliedern und mit anderen Bürgerinnen und Bürgern in Betracht gezogen werden;

in Erwägung, dass in diesem Sinne ein verantwortungsbewusstes Marketing gefördert werden kann, ohne dass der Austausch politischer Ideen und Vorschläge behindert zu werden braucht, und dass die politische Kommunikation, auch wenn sie gelegentlich Elemente typischer Werbetätigkeiten aufweist, doch Eigenheiten hat, die sie vom kommerziellen Marketing unterscheiden;

in Erwägung, dass Datenschutzgesetze bereits in vielen Gerichtsbarkeiten auf politische Kommunikation anwendbar sind;

in Erwägung, dass es nötig ist, die Einhaltung der Datenschutzgrundsätze zu garantieren und dazu einen weltweiten Minimalstandard zu schaffen, der dazu beitragen könnte, dass das Schutzniveau für Personen, von denen Daten gesammelt werden können, zu harmonisieren, indem zum einen nationale und internationale Verhaltensregeln zur Grundlage genommen und zum anderen spezifische Lösungen und Regelungen einzelner Länder berücksichtigt werden;

in Erwägung, dass die Datenschutzbeauftragten künftig eine stärkere Rolle in der Planung koordinierter Aktionen spielen könnten, auch in Zusammenarbeit mit anderen Aufsichtsbehörden in den Bereichen der Telekommunikation, Information, Meinungsumfragen oder Wahlverfahren;

verabschiedet die Konferenz folgende Resolution:

Jede Aktivität politischer Kommunikation, die die Verarbeitung von Personendaten voraussetzt – auch diejenige, die nicht im Zusammenhang mit Wahlkampagnen steht –, muss die Grundrechte und Grundfreiheiten der von der Datenverarbeitung betroffenen Personen respektieren, einschließlich des Rechts auf Schutz der persönlichen Daten, und muss im Einklang stehen mit den anerkannten Grundsätzen des Datenschutzes, namentlich:

Datenminimierung

Personendaten sollen nur so weit verarbeitet werden, als es zur Erreichung des spezifischen Zwecks, zu welchem sie gesammelt werden, erforderlich ist.

Erhebung auf rechmäßige Weise und nach Treu und Glauben

Personendaten sollen aus erkennbaren Quellen rechtmäßig erhoben werden, und sie sollen nach Treu und Glauben verarbeitet werden. Es soll sichergestellt werden, dass die Quellen, im Einklang mit dem Gesetz, entweder öffentlich zugänglich sind oder dass andernfalls respektiert wird, dass sie nur zu bestimmten Zwecken, unter bestimmten Modalitäten, für einen begrenzten Anlass oder Zeitraum genutzt werden dürfen.

Besondere Aufmerksamkeit soll jenen Fällen geschenkt werden, in denen aggressive Methoden für die Kontaktaufnahme mit den betroffenen Personen gewählt werden.

Datenqualität

Bei der Verarbeitung sollen die anderen Grundsätze zur Sicherung der Datenqualität beachtet werden. Die Daten müssen insbesondere richtig, relevant und auf das notwendige Minimum beschränkt sein und à jour gehalten werden im Hinblick auf den bestimmten Zweck, zu dem sie erhoben wurden, besonders wenn sich die Informationen auf gesellschaftliche oder politische Anschauungen oder ethische Überzeugungen der betroffenen Person beziehen.

Zweckmäßigkeit

Personendaten aus privaten oder öffentlichen Informationsquellen, Institutionen oder Organisationen dürfen für die politische Kommunikation verwendet werden, wenn ihre Weiterverarbeitung im Einklang steht mit dem Zweck, zu dem sie ursprünglich erhoben wurden, und den betroffenen Personen zur Kenntnis gebracht werden; dies gilt insbesondere für sensible Daten. Gewählte Abgeordnete müssen diese Grundsätze beachten, wenn sie Daten, die zur Ausübung der amtlichen Funktionen gesammelt wurden, für die politische Kommunikation benutzen wollen.

Personendaten, die ursprünglich mit aufgeklärter Einwilligung der betroffenen Person zu Marketingzwecken erhoben wurden, dürfen für die politische Kommunikation verwendet werden, wenn der Zweck der politischen Kommunikation in der Zustimmungserklärung ausdrücklich genannt wird.

Verhältnismäßigkeit

Personendaten dürfen nur auf die Art und Weise verarbeitet werden, die dem Zweck der Datensammlung entspricht, insbesondere wenn es um Daten zu potenziellen Wählerinnen und Wählern oder um den Vergleich von Daten geht, die aus verschiedenen Archiven oder Datenbanken stammen.

Personendaten, insbesondere solche, die über den Anlass hinaus, zu dem sie erhoben wurden, aufbewahrt werden, dürfen weiter verwendet werden, bis die Ziele der politischen Kommunikation erreicht sind.

Information der betroffenen Person

Der betroffenen Person muss eine dem gewählten Kommunikationsmittel entsprechende Informationsnotiz zugestellt werden, bevor von ihr Daten gesammelt werden; die Notiz hat den für die Datensammlung Verantwortlichen zu bezeichnen (die einzelne kandidierende Person, den externen Kampagnenleiter, die lokale Unterstützungsgruppe, lokale oder assoziierte Vereinigungen, die Partei insgesamt) sowie den zu erwartenden Datenaustausch zwischen diesen Instanzen.

Die Person, von der Daten gesammelt werden, muss informiert werden, wenn diese Daten ohne ihr Zutun gesammelt werden, zumindest wenn die Daten nicht nur vorübergehend aufbewahrt werden.

Einwilligung

Es muss sichergestellt sein, dass die Verarbeitung von Personendaten auf der Einwilligung der betroffenen Person oder auf einem anderen gesetzlich vorgesehenen Grund beruht. Die Verarbeitung muss die im jeweiligen Staat geltenden, den spezifischen Informationsquellen und -mitteln entsprechenden Regelungen beachten, namentlich im Falle von E-Mail-Adressen, Faxnummern, SMS oder anderen Text/Bild/Video-Mitteilungen oder von aufgezeichneten Telefonkontakten.

Datenaufbewahrung und Datensicherheitsmaßnahmen

Jede für eine Datensammlung verantwortliche Person, sei es eine politische Gruppierung oder eine einzelne kandidierende Person, muss alle technischen und organisatorischen Maßnahmen treffen, die nötig sind, um die Integrität der Daten zu schützen und um zu verhindern, dass die Daten verloren gehen oder von unbefugten Personen oder Stellen benutzt werden.

Rechte der betroffenen Person

Die betroffene Person hat das Recht auf Zugang, Berichtigung, Sperrung und Löschung ihrer Daten; sie hat das Recht, sich gegen unerwünschte Kommunikation zu wehren und – kostenlos sowie auf einfache Weise – zu verlangen, keine neuen Mitteilungen mehr zu erhalten. Diese Rechte müssen in der an sie gerichteten Informationsnotiz ausdrücklich genannt werden.

Für den Fall, dass diese Rechte verletzt werden, sind angemessene Maßnahmen und Sanktionen vorzusehen.

21. Anhang

21.1 Pressespiegel

Datum	Zeitung	Titel/Inhalt
09.01.2005	Weser-Report	**Neu in Bremen und gleich die GEZ im Nacken** Studentin über Datenabgleich verwundert
11.01.2005	Bremer Nachrichten/Weser-Kurier	**SPD gegen heimliche Vaterschaftstests**
18.01.2005	Delmenhorster Kreisblatt	**„Zögerliche Haltung ist unverständlich“** DNA-Analyse: CDU-Bürgerschaftsfraktion fordert schnelle Gesetzesänderung
18.01.2005	Bremer Nachrichten/Weser-Kurier	**Neuer Umgang mit DNA-Daten** Scherf und Röwekamp: Mehr Rechte für den Staat
18.01.2005	Nordsee-Zeitung	**„DNA-Probe muss Standard werden“**
18.01.2005	Bremer Nachrichten/Weser-Kurier	**Bremer wollen gerne testen** Umfrage zur elektronischen Gesundheitskarte zeigt positive Grundeinstellung
22.01.2005	Nordsee-Zeitung	**Datenschützer schreiben Erfolgsstory** Bremerhavener Datenschutz Nord setzt sich durch
23.01.2005	Weser-Report	**Die GEZ will wieder zuschlagen** Ab 2007 wird für Internet-PC abkassiert/Stimmt Bürgerschaft heiklem Staatsvertrag zur?
26.01.2005	taz-nord-bremen	**Finger-fertig** Polizei in Bremerhaven testet neues Verfahren zur schnellen Identifizierung von Fingerabdrücken
26.01.2005	Nordsee-Zeitung	**Fingerabdruck wird binnen Sekunden erkannt** Regionale Datenbank liefert Ergebnisse binnen Sekunden – Polizeichef: Entscheidender Schritt im Kampf gegen Verbrechen
26.01.2005	Kreiszeitung Syke	**Spurensuche per Computer**
26.01.2005	Frankfurter Allgemeine	**Die GEZ darf jetzt fast alles** GEZ soll Leserdaten anfordern dürfen – Warum die Gebührenerheber vom 1. April an sämtliche Daten von Zeitschriftenlesern kriegen
03.02.2005	Bremer Nachrichten/Weser-Kurier	**Gewaltexpress kündigt sich oft an** Freie Universität Berlin will mit Bremer Polizei Warnsignale für Lehrer erforschen
10.02.2005	Bremer Nachrichten/Weser-Kurier	**Effektivere Behandlung dank Chipkarte** „Ibon“ speichert elektronisch die Daten von Krebspatienten/Bundesweit einmaliges Projekt
13.02.2005	taz-nord-bremen	**Deutschland freundlichster Geheimdienst** Das „Bundesamt für Sicherheit in der Informationstechnik“ in Bonn gibt gern den harmlosen deutschen Hausmeister im Internet. Tatsächlich spähen in seiner Werkstatt Meister-Hacker unser digitales Leben aus
15.02.2005	taz-nord-bremen	**Ärger mit dem Glückspenis** Ein Netz von Polizisten, die sich Pornografisches, Schlüpfriges und einfach nur Blödes per Mail auf den Dienstcomputer schickten, kundschafteten Ermittler im Sommer aus. „Hysterie“, heißt es nun. Dem Chef fehle das Fingerspitzengefühl.

Datum	Zeitung	Titel/Inhalt
18.02.2005	Kreiszeitung Syke	**„DNA nicht als Standard“**
18.02.2005	Bremer Nachrichten/Weser-Kurier	**„Eingriff in Grundrechte“** Datenschützer warnen vor routinemäßigen DNA-Analysen
18.02.2005	taz-nord-bremen	**Warnung vom Datenschützer**
19.02.2005	Bremer Nachrichten/Weser-Kurier	**Abschied von der Lohnsteuerkarte**
21.02.2005	RB „buten un binnen“	**CDU will mehr Video**
22.02.2005	taz-nord-bremen	**Video I: CDU will mehr big brother**
22.02.2005	taz-nord-bremen	**Video II: SPD will mehr Prüfung**
22.02.2005	Bild-Bremen	**Mehr Videoüberwachung**
26.02.2005	Bremer Nachrichten/Weser-Kurier	**„Es gibt nicht nur den einen „Big Brother“** Vortragsreihe in der Villa Ichon. Überwachung der Telekommunikation greift immer weiter um sich
14.03.2005	Bremer Nachrichten/Weser-Kurier	**Staat will an die Handy-Daten** Telefon- und Internet-Verbindungen sollen bis zu zwölf Monate gespeichert werden
14.03.2005	Bremer Nachrichten/Weser-Kurier	**Hunger auf Daten** Kommentar zur Speicherung von Handy- und Internet-Verbindungen
18.03.2005	Bremer Nachrichten/Weser-Kurier	**Weber: Rechnungshof soll im Parlament mitreden** Präsident will Geschäftsordnung ändern/Kritik am Prüfbericht Rechnungshof, Datenschützer und Frauenbeauftragte sollen ihre Jahresberichte künftig im Parlament vorstellen
30.03.2005	Weser-Report	**Pro & Contra** Verbindungsdaten länger speichern?
01.04.2005	taz-nord-bremen	**Keine Angst vorm Datenschutz** Bremer Behörden lassen sich meist vorab beraten, lobt der Datenschutzbeauftragte
01.04.2005	Kreiszeitung Syke	**„Sachbericht statt Mängelliste“** Landesbeauftragter für den Datenschutz: Gute Konzepte der bremischen Verwaltung/Kritik am Bund
01.04.2005	Bremer Nachrichten/Weser-Kurier	**Datenschützer ziehen positive Bilanz** Bericht 2004 vorgelegt/Kritik an Agentur für Arbeit
01.04.2005	Delmenhorster Kreisblatt	**Datenschützer mit Bremen zufrieden**
01.04.2005	Nordsee-Zeitung	**Bund entwickelt Daten-Sammelwut** Datenschützer Holst kritisiert „gesetzgeberischen Aktionismus“ – Verwaltung und Wirtschaft im Land Bremen gelobt
05.04.2005	Handelsblatt	**Europa vernetzt seine Strafdatenbanken** Abfrage innerhalb eines Tages statt mehrerer Wochen

Datum	Zeitung	Titel/Inhalt
06.04.2005	Weser-Report	**Kampf dem Kartenbetrug** Hkk übernimmt bundesweit Vorreiterrolle/Software schlägt Alarm
14.04.2005	Bremer Nachrichten/ Weser-Kurier	**Fußball-WM sorgt weiter für Kritik** Datenschützer erheben neue rechtliche Einwände
14.04.2005	Nordsee-Zeitung	**Datenhunger zur Fußball-WM** Datenschützer des Landes kritisiert den Deutschen Fußballbund für mangelnden Datenschutz bei der Ticket-Lotterie
18.04.2005	Nordsee-Zeitung	**„Vorbildlicher Datenschutz“** Zertifizierung der SWB durch datenschutz nord GmbH
02.05.2005	Bremborium	**Übergabe des Jahresberichts des LfD an den Bürggerschaftspräsidenten**
04.05.2005	Bremer Nachrichten/Weser-Kurier	**Datenschützer warnt vor zu großer Eile** Kritische Fragen zur elektronischen Gesundheitskarte
21.05.2005	Bremer Nachrichten/Weser-Kurier	**SPD will keine weitere Video-Überwachung**
24.05.2005	Bremer Nachrichten/Weser-Kurier	**Eine große Gefahr liegt in der schleichenden Aushöhlung der Grundrechte** Schwere Verstöße im Brechmitteleinsatz und der auszuferenden Telekommunikationsüberwachung
09.06.2005	Bremer Nachrichten/Weser-Kurier	**Gebührenfahndung auf Parzellen** Kleingärtner fühlen sich von der GEZ ausspioniert/ Zum Teil saftige Nachzahlungen
11.06.2005	Bremer Nachrichten/Weser-Kurier	**Akteneinsicht nur ohne Fotokopien?** Grüne: Klärung durch die Bürgerschaft ist nötig/Senat: Rechte privater Dritter gefährdet
11.06.2005	Norddeutsche	**Lieber Mützen statt Linsen** Polizisten bevorzugt: Beirat skeptisch gegenüber Videoüberwachung am Bahnhof
13.06.2005	Bremer Nachrichten/Weser-Kurier	**Tagen Deputationen künftig öffentlich?** Weber schlägt Belebung des Parlamentarismus vor
14.06.2005	Bremer Nachrichten/Weser-Kurier	**Böhrnsen auch für öffentliche Sitzungen**
14.06.2005	taz-nord-bremen	**Deputationen für alle offen?**
14.06.2005	Nordsee-Zeitung	**Öffentlichkeit in Deputationen**
15.06.2005	Burg-Lesumer-Vereinsblatt	**Keine Videokamera am Bahnhof** Beiratsmehrheit plädierte für Abstimmungsverschiebung/„Kontakt zum Bürger verloren“
22.06.2005	taz-nord-bremen	**Bankgeheimnis weniger geheim** Am 1. Juli tritt die EU-Zinsrichtlinie in Kraft. Konten im Ausland werden heimischen Finanzämtern gemeldet. Ausnahmen gelten ausgerechnet in den Steuerparadiesen
08.07.2005	Bremer Nachrichten/Weser-Kurier	**Videokamera am Bahnhof: Polizei zieht positives Fazit** Zahlen gehen teils deutlich zurück/Weitere Standorte im Gespräch

Datum	Zeitung	Titel/Inhalt
09.07.2005	Frankfurter Rundschau	**Ungewisse Wirkung von Videoüberwachung**
09.07.2005	taz-nord-bremen	**Details unbekannt** Polizeiliche Kriminologen sehen Forschungsbedarf: Nicht alles, was die Polizei tut, macht nachweislich Sinn. Skepsis gegenüber der Videoüberwachung.
10.07.2005	Kurier am Sonntag	**FDP gegen Kameras an Sielwallkreuzung**
15.07.2005	Nordsee-Zeitung	**Videoüberwachung soll ausgeweitet werden** Pläne in Niedersachsen und im Land Bremen
15.07.2005	Bremer Nachrichten/Weser-Kurier	**Videokameras nach Gefühl eingesetzt** Fachtagung: Polizeimaßnahmen werden nicht überprüft
16.07.2005	Bremer Nachrichten/Weser-Kurier	**Kameras täuschen Sicherheit nur vor** SPD-Kritik an CDU-Forderung
20.07.2005	Bremer Anzeiger	**Koalition streitet um die Videoüberwachung** Röwekamp: „Am Bahnhof erfolgreich“
24.07.2005	Bremer Anzeiger	**Liberale gegen Videoüberwachung** FDP will am Sielwalleck nicht filmen
26.07.2005	taz-nord-bremen	**Schünemanns Scheune zu** Vorbeugende Telefonüberwachung: Niedersachsens Innenminister dürfte vom BVF eine Niederlage einfahren
26.07.2005	Bremer Nachrichten/Weser-Kurier	**„Privatheit kein Luxusartikel“** Karlsruhe urteilt über das Abhören von Telefongesprächen
27.07.2005	Der Spiegel online	**Bundesverfassungsgericht: Präventiver Lauschangriff verstößt gegen Grundgesetz**
27.07.2005	Weser-Report	**Pro & Contra: Videoüberwachung ausweiten?**
28.07.2005	taz	**Urteil gegen Regelungswut** Kommentar zum Urteil des Bundesverfassungsgerichts gegen eine vorbeugende Telefonüberwachung
28.07.2005	taz-nord-bremen	**Gegen Überwachung** Datenschützer will Verfassungsschutz-Pläne prüfen
28.07.2005	Bremer Nachrichten/Weser-Kurier	**Karlsruhe bremst Hannover** Niedersachsens Regierung muss ihr Polizeigesetz wieder entschärfen
28.07.2005	Bremer Nachrichten/Weser-Kurier	**Ein Lehrstück in Sachen Demokratie** Verfassungsgericht: Über Grenzen der Freiheit entscheidet nicht die Verwaltung
28.07.2005	Bremer Nachrichten/Weser-Kurier	**Weniger ist mehr** Kommentar zum Karlsruher Urteil zur Telefonüberwachung
09.08.2005	Nordsee-Zeitung	**Datenschützer kritisiert Befragung** Telefonbefragung von Beziehern des Arbeitslosengeldes II im Auftrag der Bundesagentur für Arbeit ist in die Kritik geraten
09.08.2005	Süddeutsche Zeitung	**Datenschützer kritisieren Telefonaktion** Telefonische Überprüfung der Daten von Hunderttausenden Arbeitslosengeld-II-Empfängern durch die Bundesagentur für Arbeit hat scharfen Protest der Datenschützer ausgelöst.

Datum	Zeitung	Titel/Inhalt
25.08.2005	Bremer Nachrichten/Weser-Kurier	**Digitale Tarnkappen im Internet** Wie man unbemerkt durch das World Wide Web surfen kann
26.08.2005	taz-nord-bremen	**Datei für Stalker** Die Polizei speichert Stalker künftig in einer „Gefährder-Datei". Anlass: Der Auftakt eines Mordprozesses
26.08.2005	Bremer Nachrichten/Weser-Kurier	**Stalker werden als „Gefährder" gespeichert** Polizei führt neuen Hinweis in ihrem Anzeigensystem ein/Schnellerer Überblick für Beamte
26.08.2005	Nordsee-Zeitung	**Stalker für Polizei schneller erkennbar** „Gefährder"-Datei beim Landeskriminalamt
03.09.2005	Bremer Nachrichten/Weser-Kurier	**Blick in die Akten genehmigt** Behörde gibt Hotel-Unterlagen frei
11.09.2005	Kurier am Sonntag	**Zwischen Schweigepflicht und Aufklärung** Notfallmediziner informierten sich im Krankenhaus Links der Weser über das Vorgehen nach Straftaten
16.09.2005	Bremer Nachrichten/Weser-Kurier	**Sensible Daten im Altpapier** Gesamtübersicht über die Konten von Sparkassen-Kunden aufgetaucht/Datenschutzbeauftragter eingeschaltet
15.10.2005	taz-nord-bremen	**Neue Software, andere Öffnung**
19.10.2005	Bremer Nachrichten/Weser-Kurier	**Wo hängt die nächste Kamera?** Innenressort legt Bericht vor/Polizei bringt mobile Videoüberwachung ins Spiel
25.10.2005	Bremer Nachrichten/Weser-Kurier	**Schöne neue Telefonie-Welt** Wie Gespräche via Internet funktionieren und warum man sie leicht belauschen kann
25.10.2005	Bremer Nachrichten/Weser-Kurier	**„Internet-Telefonie ist riskant"** Datenschützer warnt vor erheblichen Sicherheitslücken der neuen Technologie
01.11.2005	Nordsee-Zeitung	**Datenschützer gegen Reisepass**
03.11.2005	Nordsee-Zeitung	**Datenschützer kritisieren GEZ-Verfahren**
03.11.2005	Nordsee-Zeitung	**Datenschützer sind als Hacker aktiv** Fehler in Arbeitszeit-Erfassung aufgedeckt
10.11.2005	Bremer Nachrichten/Weser-Kurier	**Serie: Datenklau im Internet, Teil 1** **Privat bleibt bei Funknetzen auf WLAN-Basis oft nicht mehr** Dritte können ohne großen Aufwand mithören/Unbemerkter Zugriff auf persönliche Daten
17.11.2005	Bremer Nachrichten/Weser-Kurier	**Serie: Datenklau im Internet, Teil 2** **Späher haben leichtes Spiel** Schwachstellen in der DSL-Technologie/Wie sich Internetnutzer besser abschotten können
24.11.2005	Bremer Nachrichten/Weser-Kurier	**Serie: Datenklau im Internet, Teil 3** **Mit Tricks auf gefälschte Internetseiten gelockt** Betrüger verleiten Online-Bankkunden dazu, ihre persönlichen Daten anzugeben/Auf Abweichungen bei der Adresse achten

Datum	Zeitung	Titel/Inhalt
24.11.2005	Bremer Nachrichten/Weser-Kurier	**Wieviel darf der Staat wissen?** BVG prüft Schutz von E-Mails und Handys
01.12.2005	Bremer Nachrichten/Weser-Kurier	**Serie: Datenklau im Internet, Teil 4 Technologie mit erheblichen Sicherheitslücken** Beim Telefonieren per Internet ist die Vertraulichkeit nicht gesichert
02.12.2005	Nordsee-Zeitung	**Firmendaten im Internet abrufbar** Elektronisches Handelsregister erstellt
08.12.2005	Nordsee-Zeitung	**Ein Stempel gegen den Daten-Striptease** Langzeitarbeitslose sollen für Rundfunkgebühren-Befreiung nicht mehr den Bescheid vorlegen
12.12.2005	Bremer Nachrichten/Weser-Kurier	**„Videokamera kein Allheilmittel“** Innenbehörde zieht jedoch positives Fazit der Überwachung des Bahnhofsplatzes/Verdrängungseffekt
16.12.2005	Bremer Nachrichten/Weser-Kurier	**Durfte die Kripo Telefone anzapfen?** Torso-Prozess: Streit um Beweismittel
17.12.2005	Bremer Nachrichten/Weser-Kurier	**Gesundheitskarte: Bremen Testregion**
17.12.2005	Kreiszeitung Syke	**Bremen wird Testregion** Schneller Zugriff auf Daten durch elektronische Gesundheitskarte
18.12.2005	Bremer Anzeiger	**„Bremen ist in Sachen Terror kein weißer Fleck“** Bremens Innensenator Thomas Röwekamp (CDU) erläutert im Bremer Anzeiger das neue Sicherheitspaket
19.12.2005	taz-nord-bremen	**Bremen testet Gesundheitskarte**
21.12.2005	taz-nord-bremen	**Schon GEZahlt? Oder nicht gestempelt?**
28.12.2005	taz-nord-bremen	**GEZ-Befreiung: Hinweis genügt**

21.2 Auswahl telefonisch beantworteter Anfragen

Thema	Anfragesteller/-in
Löschfristen für Sozialdaten	Bürgerbeauftragte
Erhebung von Daten durch einen Internetanbieter	Bürger
Auskunfts- und Berichtigungsanspruch nach dem SGB	Bürgerin
Bestellung des betrieblichen Datenschutzbeauftragten	Firma
Weitergabe von Mietverträgen durch das Sozialamt an die GEZ	Bürgerin
Umfang der Offenbarungsbefugnis einer Klinik gegenüber der Presse, wenn ein Patient an diese wegen schlechter Behandlung herangetreten ist	betrieblicher DSB
Friendfinder, Ortung von anderen Personen über Handy	Journalist
Weitergabe einer Adresse durch O2	Bürger aus Bremerhaven
Bestellung des betrieblichen Datenschutzbeauftragten	Firma

Thema	Anfragesteller/-in
Vom Patienten wurde beim Zahnarzt vor der Behandlung ein Passfoto aufgenommen. Zulässig?	Bürger
Speicherdauer von Daten aus dem Antrag einer privaten Krankenversicherung und Austausch von Informationen der Versicherungen untereinander	Bürger
Gesetzliche Bestimmungen im Gesundheitsdatenschutz	Schüler
Bestellung des betrieblichen Datenschutzbeauftragten	Firma
Missbrauch von Handyortungssystemen unter privaten Benutzern	Journalist
Bürgerin erhielt Post von der Agentur für Arbeit Bremen zusammen mit einem Schreiben, das an eine andere arbeitslose Person gerichtet war	Ehemann der Bürgerin
Berichtigung, Sperrung, Löschung von Sozialdaten	Bürger
Betrieblicher Datenschutzbeauftragter in Arztpraxen	Arzt
Datenweitergabe von der Meldebehörde an die GEZ	Bürger
Vorlage der Einkommensteuer-Erklärung bei der Gesetzlichen Krankenversicherung	Bürger
Bestellung des betrieblichen Datenschutzbeauftragten	Arbeitgeber
Erteilung von Auskünften durch Auskunfteien an den Betroffenen	Bürger
Hat ein betrieblicher Datenschutzbeauftragter auch Ermittlungskompetenzen bei pornographischen Inhalten auf der Festplatte?	betrieblicher DSB
Verarbeiten Hotels personenbezogene Daten, wenn sie Namen und Anschrift der Gäste speichern? Verpflichtung zur Bestellung eines betrieblichen Datenschutzbeauftragten?	Hotel-/Gaststättenverband
Fragen zum Kontodatenabruf	Bürger
Fragen zum Audit	behördlicher DSB
Datenerhebung beim Schrotthändler	Bürger
Gewährung von Schadensersatz nach dem BDSG	Versicherungsmakler
Auskunft aus Daten der Polizei	Bürger
Bestellung des betrieblichen Datenschutzbeauftragten	betrieblicher DSB
Weitergabe von Mitarbeiterdaten durch die Personalstelle an die GEZ	betrieblicher DSB
Datenschutz und Privatisierung öffentlicher Aufgaben	Studentin
Verbreitung ehrverletzender Behauptungen im Internet	Bürger
Speicherung von Telekommunikationsdaten	Bürgerin
Auskunftsersuchen von Behörden	Bürgerin
Fragebogen von Adresshändlern; Auskunftsverpflichtung	Bürger
Nennung des vollständigen Namens eines Amtsträgers durch die Presse	Dienststelle
Erhebung von Daten durch einen Online-Learning-Anbieter	Anbieter
Datenschutzgerechte Gestaltung einer Homepage	betrieblicher DSB

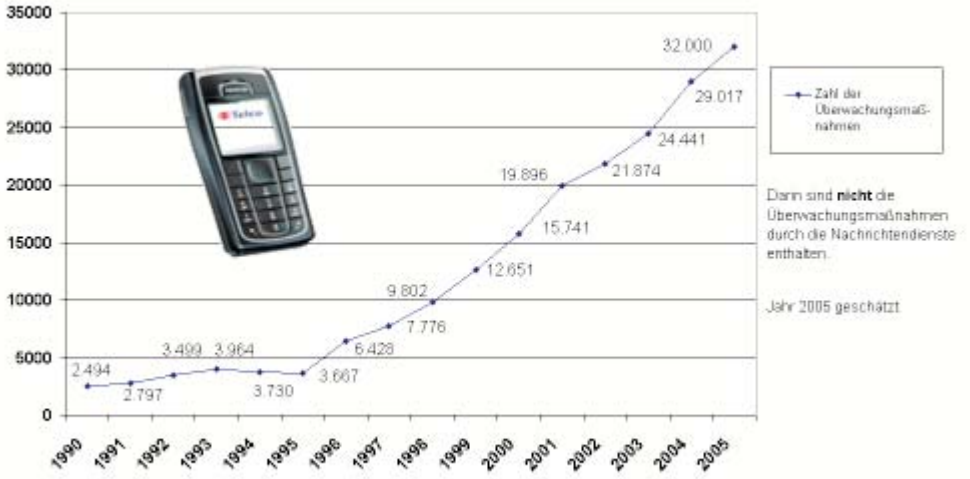
Thema	Anfragesteller/-in
Zulässigkeit der Weitergabe von Mitgliederdaten durch eine Kirchengemeinde	Vorstand
Weitergabe von Daten durch Meldebehörde an GEZ trotz Sperrvermerk	Bürger
Fragen betr. Marktforschungsinstituten	Bürgerin
Weitergabe von Sozialdaten bei GEZ-Befreiung von Jugendlichen in Hilfemaßnahmen	Sozialarbeiter
GEZ schreibt Bf. 3 Jahre nach Firmenaufgabe immer noch als Firmeninhaber an und fordert zur Anmeldung auf	Bürger
Anrufer möchte gern in die Personalakte seines verstorbenen Vaters schauen, der entlassen wurde, weil er seinerzeit nicht an S-Veranstaltungen teilgenommen hatte	Bürger
Speicherung von Daten bei der Deutschen Bank ohne Einverständnis (Werbebrief, Anrufer kein Bankkunde)	Bürger
Wie kann man sich gegen die Veröffentlichung seiner personenbezogenen Daten im Internet wehren?	Bürger
Fragen bzgl. Inkasso	Bürger
Fragen bzgl. Creditreform	Bürger
Frage, wer verantwortliche Stelle ist	betrieblicher DSB
Datenspeicherung der SCHUFA	Bürger
Einwilligung in Übergabegespräch am Patientenbett zwecks Pflegeüberleitung	Krankenhausmitarbeiterin
Dürfen Programmtestläufe mit Personaldaten (Echtdaten) durchgeführt werden?	Personalrat
Fragen zu Happy Digits	Bürger
Frage zur Zulässigkeit der Herausgabe von Programm-Quellcodes einer Versicherung an die Außendienstmitarbeiter	betrieblicher DSB
Löschung von Daten bei der Polizei	Bürger
Sorgen über Biometrie	Bürgerin
Fragen zu maschinenlesbaren Ausweisen	Bürger
Einbeziehung von Eltern/behandelndem Kinderarzt bei Fördergutachten	Arzt
Aufforderung der BAGIS, einen Lebenslauf mitzubringen	Bürgerin
Fragen bzgl. Datenschutz in der Uni-Verwaltung	Studentin
Zulässigkeit der Weitergabe von Mitgliederdaten eines Freizeitvereins für Kinder zum Zwecke der Durchführung einer Reise an den Beirat wg. finanzieller Förderung	Mitarbeiter des Vereins
TELE 2 bewirbt Telekom-Kunden telefonisch und verwendet personenbezogene Daten, obwohl einer Weitergabe von Daten gegenüber der Telekom ausdrücklich widersprochen wurde	Bürger
Beauftragung von Arbeitsvermittlungsagenturen durch die BAGIS	Bürger
Werden Telefongespräche mit Strafgefangenen von der JVA abgehört?	Sozialarbeiterin

Thema	Anfragesteller/-in
Telefonische Ansprache älterer Menschen zwecks Werbung für ein Hausrufsystem durch den Malteser Hilfsdienst	Bürger
BAföG-Zahlungen wurden plötzlich eingestellt; möchte der Sache nach Jahren auf den Grund gehen und Nachforschungen anstellen. Gibt es noch Akten dazu, oder ist bereits alles vernichtet?	Bürger
Fragen zum Verfahrenverzeichnis	behördlicher DSB
Fragen zum Bundeszentralregister	Bürger
Auskunftsanspruch des Betroffenen gegenüber einer Versicherung	Bürger
Datenlöschung bei der SCHUFA	Bürger
Unvereinbarkeit von Betriebsratstätigkeit und Administratorentätigkeit	betrieblicher DSB
Vorgehen bei Einführung neuer Verfahrenssoftware	Projektverantwortlicher
Datenschutz im Verein, Anforderungen an eine Einwilligung, Internetauftritt	Vereinsmitglied
Datenspeicherung durch Auskunfteien	Bürger
Vorlage einer Verdienstbescheinigung des Mitbewohners bei der BAGIS	Bürger
Vorlage des Einkommensteuerbescheids bei einer Krankenkasse	Bürgerin
Gesetzessystematik des Datenschutzes in Krankenhäusern	Rechtsreferendar
Diagnoseschlüssel in Krankenhausrechnungen	Bürgerin
Konzerninterne Weitergabe von Daten einer minderjährigen Begünstigten eines Lebensversicherungs vertrags	Bürger
Personalausweiskopien zur Internetbenutzung beim Arbeitsamt	Bürgerin
Datenübermittlungen in Drittstaaten, Verwendung von Standardvertragsklauseln	betrieblicher DSB
Datenschutz im Justizbereich	Bürger
Welche Standardvertragsklauseln sollte man für die Übermittlung in Drittstaaten verwenden?	betrieblicher DSB
Anwendungsbereich des BremDSG bzgl. gGmbH	behördlicher DSB
Beschwerde bezüglich neuer Praxis der Gebührenbefreiung bei der GEZ	Bürger
Werbebeilagen in Gehaltsabrechnungen	Bürger
Betriebsvereinbarung – Internetnutzung für Administratoren	Administrator
Löschungsfristen der Auskunfteien	Bürger
Fragen zu Einsichtsrecht beim Gesundheits- und Sozialamt, Häusliche Pflege u. Mitwirkungspflicht	Bürger
Internet-Abzocke durch Schweizer Produktforschungsfirma und Bankeinzug ohne Vollmacht durch Online-Inkassobüro	Bürger
Namentliches Aufrufen im Jobcenter	Solidarische Hilfe
Bestellung des betrieblichen Datenschutzbeauftragten	Call-Center

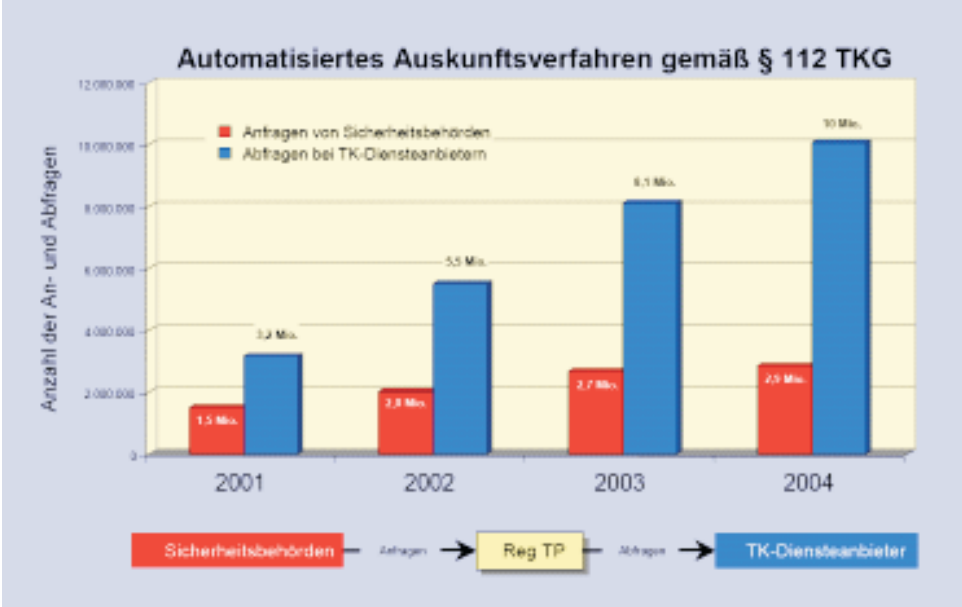
Thema	Anfragesteller/-in
Speicherung von Daten auf einer Internetseite	Bürger
Wieso erscheint u. a. bei Polizei und Arbeitsamt Absender-Telefonnummer? (Handel mit Telefonnummern durch angerufene Behörde etc. möglich!)	Bürger
Datenerhebung durch Krankenkasse wg. Erstattung von Zuzahlungen	Bürger
Bestellung des betrieblichen Datenschutzbeauftragten	Unternehmen
Übermittlung von Personaldaten an Betriebsärztin	betrieblicher DSB
Gesundheitsdaten eines Verwandten in Arztbericht	Bürger
Praxisübernahme, ärztliche Dokumentationspflicht und Einsichtsrecht	Bürgerin
Anforderung an Datenschutzerklärung für Homepage, Impressumspflicht	betrieblicher DSB
Verlust von Dokumenten bei Versand an Gericht	Bürgerin
Vorlagepflicht von Standardvertragsklauseln	Rechtsanwaltsbüro
Besteht für Kreditinstitute die Verpflichtung zur Videoüberwachung an Geldausgabeautomaten? (BAFin verwies an LfD)	Bürger
Identitätsfeststellung bei einem Telekommunikationsunternehmen zum Zwecke der Änderung des Vertrages	Bürger
Durchführung und Zweckmäßigkeit eines Datenschutzaudits	behördlicher DSB
Zuständigkeit für private Postdienstleistungen, Meldepflicht, etc.	betrieblicher DSB
In welchem Umfang dürfen Gutachter psychiatrische Daten an Leistungsträger übermitteln?	Bürger
Strafantragsrecht bei Weitergabe der Information über ein laufendes Sorgerechtsverfahren	Bürger
Wann ist ein betrieblicher Datenschutzbeauftragter zu bestellen?	Unternehmen
Kann der Bürger der Weitergabe seiner Daten durch Adresshändler widersprechen?	Bürgerin
Unrichtigkeit durch Auskunfteien gespeicherter Daten	Bürger
Verstößt die Weitergabe von Daten an einen externen Dienstleister gegen § 203 StGB	Bürger
Beschwerde bezüglich neuer Praxis der Gebührenbefreiung bei der GEZ wegen des Umfangs der preiszugebenden Daten	Bürgerin
Meldepflicht nach § 4 d BDSG	Unternehmen
Löschung eines SCHUFA-Eintrags	Bürger
Frage zum Adresshandel	Bürgerin
Adressankauf der GEZ, Fragen zum Adresshandel	Bürgerin
Weitergabe von Daten durch Adresshändler	Bürger
Löschung einer Eintragung bei Creditreform	Bürger
Bestellung des betrieblichen Datenschutzbeauftragten	Unternehmen
Neues Gebührenbefreiungsverfahren, Befreiung auch bei Radio Bremen möglich?	Bürger
Bestellung des betrieblichen Datenschutzbeauftragten	Unternehmen

Thema	Anfragesteller/-in
Veröffentlichung von Namen im Internet bei Zwangsversteigerungen	Bürger
Weitergabe von Daten an Versicherung durch Kreditinstitut	Bürger
Datenübermittlungen in Drittstaaten: Ist die Übermittlung aufgrund einer Einwilligung zulässig? Fragen zu Standardverträgen	Unternehmen
Anwendbarkeit des BremDSG	Gesellschaft
Auskunftspflicht beim Mikrozensus	Bürger
Fragen zu Kundenkarten und Werbesendungen	Bürger
Woher hat die GEZ Daten, habe ich Anspruch auf Löschung?	Bürgerin
Auskunft einer Bank an einen Rechtsanwalt	Bürgerin
Datenschutz bei Auftraggebern	DV-Dienstleister
Auskunftsrecht Betroffener nach dem BremVerfSchG	Behörde
Fragen zum Impressum und Datenschutzerklärung im Internet	Unternehmen
Auskunftsrecht von Adoptivkindern bzgl. weiterer leiblicher Geschwister	behördlicher DSB
Einsicht von Logbüchern nach dem Bremischen Archivgesetz	Bürger
Mitlesen von SMS durch Support-Mitarbeiter eines Mobilfunkanbieters	Bürger
Namentliches Aufrufen im Jobcenter	Bürger
Auskunft zu Gesetzentwurf zur Änderung des BDSG	externer DSB
Fragen zur Bestellung betrieblicher DSB	Bürger
Anschriftwiedergabe im Telefonbuch trotz Widerspruch	Bürger
Fragen zum Entwurf IFG (Anwendungsbereich, Ausnahmeregelungen etc.)	behördlicher DSB
Nichteinhaltung des vereinbarten Verfahrens hinsichtlich der Gebührenbefreiung bei der Arge Bremerhaven	Bürger
Probleme bei der Rundfunkgebührenbefreiung	Bürger
Probleme mit einer Auskunftei	Bürger
Personenbeziehbare Kosten- und Leistungsrechnung	behördlicher DSB
Ebay-Verkäufer verwendet E-Mailadresse des Bf	Bürger
Beteiligung des Verfassungsschutzes im Einbürgerungsverfahren	Rechtsanwalt
Pflicht zur Bestellung eines betrieblichen Datenschutzbeauftragten	Firma
Beschwerde über GEZ, abgestempelte Anträge des Amts für wirtschaftliche Hilfen werden nicht anerkannt	Bürger
Fragen zur Telekommunikationsüberwachung: Richtervorbehalt etc.	Bürgerin
Fragen zur Vorratsdatenspeicherung: Speicherfristen etc.	Bürger

21.3 Anstieg der Telefonüberwachung



Die aktuellen Zahlen der tatsächlich in 2005 durchgeführten Maßnahmen der Telefonüberwachung liegen noch nicht vor. Meine im letzten Jahresbericht abgegebene Schätzung von 27.500 (vgl. 27. JB, Ziff. 16.3) wurde noch übertroffen.



Sicherheitsbehörden erhalten gemäß § 112 Telekommunikationsgesetz (TKG) über die Regulierungsbehörde für Telekommunikation und Post (Reg TP), jetzt Bundesnetzagentur, von Telekommunikationsdiensteanbietern Auskünfte aus deren Kundendateien (Namen und Anschrift der Inhaber von Rufnummern). Der Kreis der ins automatisierte Verfahren eingebundenen Behörden und verpflichteten Unternehmen wurde im Laufe der Jahre stetig vergrößert. Nach dem Jahresbericht der Reg TP zu 2004 können ca. 1.000 bei der Reg TP registrierte Sicherheitsbehörden bei insgesamt 71 Telekommunikationsdiensteanbietern entsprechende Bestandsdaten abfragen. Im abgebildeten Diagramm ist die Entwicklung beim automatisierten Auskunftsverfahren gemäß § 112 TKG im Zeitraum 2001 bis 2004 dargestellt.

21.4 Liste des verfügbaren Informationsmaterials

Informationen zu verschiedenen Bereichen können im Internet unter www.datenschutz.bremen.de abgerufen werden; hier gibt es auch Downloads für Formulare.

Folgende Informationsmaterialien können beim

Landesbeauftragten für den Datenschutz der Freien Hansestadt Bremen
Postfach 10 03 80 27503 Bremerhaven
Telefon: 04 71 / 9 24 61-0 Telefax: 04 71 / 9 24 61-31
E-mail: office@datenschutz.bremen.de

angefordert werden:

25. Jahresbericht 2002, Bürgerschafts-Drs. 15/1418 (Restexemplare)
26. Jahresbericht 2003, Bürgerschafts-Drs. 16/189 (Restexemplare)
27. Jahresbericht 2004, Bürgerschaffs-Drs. 16/578 (Restexemplare)

Broschüre	„Mobilfunk und Datenschutz“
Broschüre	„Datenschutz bei WindowsNT“
Faltblatt	„Das Informationsfreiheitsgesetz des Bundes“
Faltblatt	„Datenschutz im Verein“
Faltblatt	„Adressenhandel und unerwünschte Werbung“
Faltblatt	„Handels- und Wirtschaftsauskunfteien“
Faltblatt	„Hinweise zum Antrag Arbeitslosengeld II“
Faltblatt	„Meine Datenschutzrechte als Telefonkunde“
Faltblatt	„Keine Spione auf der Festplatte“
Faltblatt	„Verräterische Spuren auf Festplatten“
Faltblatt	„Videoüberwachung durch private Stellen“
Faltblatt	„Surfen am Arbeitsplatz – Datenschutz-Wegweiser“
BfD–Info 1	Bundesdatenschutzgesetz – Text und Erläuterungen –
BfD–Info 2	Der Bürger und seine Daten
BfD–Info 3	Schutz der Sozialdaten (zurzeit nicht verfügbar)
BfD–Info 4	Die Datenschutzbeauftragten in Behörde und Betrieb
BfD–Info 5	Datenschutz in der Telekommunikation (zurzeit nicht verfügbar)

21.5 Glossar

Abkürzung	Erklärung
A2LL	Verfahren zur Berechnung des Arbeitslosengeldes II
AFZ	Ausbildungsförderungszentrum im Land Bremen GmbH
ALG II	Arbeitslosengeld II
AO	Abgabenordnung
ARGE	Arbeitsgemeinschaft
Auditing	Gutachterliche Untersuchung eines DV-Verfahrens
Authentifizierung	Ausweisen für einen berechtigten Zugriff
AZE	Arbeitszeiterfassung
BA	Bundesagentur für Arbeit
BAföG	Bundesausbildungsförderungsgesetz
BDSG	Bundesdatenschutzgesetz
BfD	Bundesbeauftragter für den Datenschutz
BfV	Bundesamt für Verfassungsschutz
BIPS	Bremer Institut für Präventionsforschung und Sozialmedizin
BKA	Bundeskriminalamt
BMWA	Bundesministerium für Wirtschaft und Arbeit (ehemaliges)
BreKom	Bremer Kommunikationstechnik
BremDSG	Bremisches Datenschutzgesetz
BremHG	Bremisches Hochschulgesetz
BremKRG	Bremisches Krebsregistergesetz
BremMeldG	Bremisches Meldegesetz
BremPolG	Bremisches Polizeigesetz
BremSchulDSG	Bremisches Schuldatenschutzgesetz
BremUIG	Bremisches Umweltinformationsgesetz
BSC	Bürger-Service-Center
BSI	Bundesamt für die Sicherheitstechnik
BVerfG	Bundesverfassungsgericht
BVN	Bremer Verwaltungsnetz
BZRG	Bundeszentralregistergesetz

Abkürzung	Erklärung
Client	Beteiligung eines PC (Kunde) in einem Netzwerk
DFB	Deutscher Fußball-Bund
DMZ	Demilitarisierte Zone
DNA	Träger der Erbinformationen („Genetischer Code“) in Lebewesen
DSL	Digital Subscriber Line, breitbandige digitale Verbindung über Telefonnetze
DV	Datenverarbeitung
EG	Europäische Gemeinschaft
eGK	elektronische Gesundheitskarte
eGovernment	elektronische Verwaltung
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
Erfa-Kreis	Erfahrungskreis der Datenschutzbeauftragten
ETB	Elektronisches behördliches Telefonbuch
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EVGP	Elektronisches Verwaltungs- und Gerichtspostfach
EWR	Europäischer Wirtschaftsraum
Firewall	Programm zum Schutz von Angriffen aus dem Internet
GDD	Gesellschaft für Datenschutz und Datensicherung e. V.
GEZ	Gebühreneinzugszentrale
GPS	Global Positioning System
GwG	Gesetz über das Aufspüren von Gewinnen aus schweren Straftaten (Geldwäsche)
Homepage	Eingangs- und Eröffnungsseite einer Internetadresse
http	Hypertext Transfer Protocol, Protokoll zur Übertragung von Daten in einem Netzwerk
iBON	integratives Bremer Onkologie- und Hämatologie Netzwerk
IHK	Industrie- und Handelskammer
IP	Internet Protocol
ISA	Informationssystem Sachen und Anzeigen
ISDN	Integrated Services Digital Network (das digitale Telefonnetz)
IT	Informationstechnologie
IuK	Informations- und Kommunikationstechnologien
KpS	Richtlinien für die Führung kriminalpolizeilicher personenbezogener Sammlungen
KUrhG	Kunsturhebergesetz
KWG	Kreditwesengesetz
LAN	Local Area Network (lokales Netzwerk)
LfD	Landesbeauftragter für den Datenschutz
LfV	Landesamt für Verfassungsschutz
MAGELLAN	Schulverwaltungssoftware
MeldDÜV	Meldedatenübermittlungsverordnung
MESO	Meldebehördensoftware
Monitoring	Überwachung während des laufenden Betriebs
NADIS	Nachrichtendienstliches Informationssystem
NIVADIS	Niedersächsisches Vorgangs-, Analyse-, Dokumentations- und Informations-System
OECD	Organisation für wirtschaftliche Zusammenarbeit und Entwicklung
OSCI	Online Services Computer Interface, sichere und vertrauliche Übertragung digital signierter Dokumente über das Internet

Abkürzung	Erklärung
PDA	Personal Digital Assistant (elektronisches Notizbuch)
PuMa	Personalverwaltung und -management
RFID	Radio Frequency Idendification, Funk-Erkennung
RGbStV	Rundfunkgebührenstaatsvertrag
Router	Gerät zum Steuern von Datenpaketen im Netz
RTP	Real Time Transport Protocol, Protokoll zur kontinuierlichen Übertragung von audiovisuellen Daten über IP-basierte Netzwerke
SCHUFA	Schutzgemeinschaft des kreditgewährenden Gewerbes
SCHUPS	Schulverweiger-Präventionsausschuss
Scoring	Bewertung
Security-Gateway	Rechner, der Daten- bzw.Rechnernetze sicher verbindet
Server	ist ein Computer in einem Netzwerk, der andere Computer bedient
SGB	Sozialgesetzbuch
SHA	Secure Hash Algorithm
Signatur	elektronische Unterschrift
SIP	Session Initiation Protocol, Protokoll zum Aufbau einer Kommunikationssitzung zwischen mindestens zwei Teilnehmern
SMS	Short Message Service, Kurznachrichten via Mobiltelefon
SSL	Security Socket Layer (Internet-Protokoll zur sicheren Datenübertragung
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
SÜG	Sicherheitsüberprüfungsgesetz
TDZB	Tumordokumentationszentrum Bremen
TKG	Telekommunikationsgesetz
TKÜ	Telekommunikationsüberwachung
UDP	User Dataprogramm Protocol, Netzprotokoll zur Übertragung von Daten in IP-Netzen ohne Schwerpunkt auf die zuverlässige Übertragung von Daten
UDS	Unfalldatenspeicher
UIG	Umweltinformationsgesetz
ULD	Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
USB	Universal Serial Bus, standartisierte Steckverbindung
VoIP	Voice over Internet Protocol, Telefonieren über Computernetzwerke auf der Basis des IP-Protokolls
VPN	Virtual Private Network
VPN-Tunnel	Virtual Privat Networking, abgesicherter Datenstrom
VPS	Virtuelle Poststelle
WLAN	Wireless Local Area Network (Funknetz)
ZSS	Zentrale Speicherstelle

21.6 Index

Druck: Anker-Druck Bremen