BREMISCHE BÜRGERSCHAFT
Landtag
16. Wahlperiode

Drucksache 16/189
19. 03. 04

26. Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2003 den 26. Jahresbericht zum 31. März 2004 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2003.

Sven Holst
Landesbeauftragter für den Datenschutz

Inhaltsverzeichnis

1. Vorwort

Es ist jedes Jahr wieder spannend, wie der Jahresbericht wohl tatsächlich ausfallen wird. Allein die Auflistung der in der Betreff-Zeile genannten Themen, die jedes Jahr mit der Post in die Dienststelle schwemmen, würden aneinandergereiht wohl leicht fünfzehn bis zwanzig engbedruckte Seiten füllen. Hinzu käme im Jahr ein fast gleichgroßer Anteil an neuen Themen, die per E-Mail bei der Dienststelle eingehen, gefolgt von dem nicht unwesentlichen Anteil an telefonischen Anfragen und Eingaben. Am Jahresende wird dann von den Referaten die Auswahl getroffen: Welche Themen stellen einen Schwerpunkt der Arbeit dar, von welchen Themen können auch andere Stellen lernen, welche Entwicklungen werden uns auch die kommenden Jahre noch beschäftigen und bei welchen Themen sollte eine öffentliche Diskussion stattfinden. Diese Themenauswahl schreiben wir dann in eine Liste, die i. d. R. immer noch viel zu lang ist. Jetzt beginnt die interne vergleichende Diskussion über die Relevanz von einzelnen Themen. Ist die Auswahl getroffen, werden die Beiträge erstellt. Dabei müssen die von den Referaten gefertigten Artikel regelmäßig in einem zweiten Arbeitsschritt gekürzt werden, um möglichst das selbst gesteckte Ziel zu erreichen, den Bericht in seinem Umfang unter einhundert Seiten zu halten. Am Ende dieses Prozesses steht dann das, was der Leser jetzt in den Händen hält oder in einem Download-Verzeichnis auf seinem PC hat. Im Inhaltsverzeichnis zum Jahresbericht findet er die so ausgewählten Bereiche im Überblick wieder. In diesem Jahr sind es mehr als 150 verschiedene Themen, die der Bericht enthält. Ein Beweis für die außergewöhnliche Leistungsfähigkeit und die hohe Motivation der in der Dienststelle Beschäftigten.

Auch wenn der Schwerpunkt des Augenmerks im Land Bremen liegt, ist doch immer auch der Blick nach Europa und den anderen führenden Industrienationen notwendig, insbesondere, um die technologischen und gesellschaftlichen Entwicklungen zu erkennen und datenschutzrechtlich und -technisch einordnen zu können. Die Vorbemerkungen zu meinem Bericht sind daher in besonderem Maße geeignet, schlaglichtartig auf besondere Entwicklungen einzugehen und die mit den Entwicklungen einhergehenden Gefahren für das informationelle Selbstbestimmungsrecht darzustellen, was in den folgenden 25 Punkten zum Teil deutlich werden dürfte. Die Zusammenarbeit unter den Datenschutzbeauftragten und den Datenschutzaufsichtsbehörden auf nationaler wie auch auf europäischer und internationaler Ebene ist dabei mittlerweile so gut ausgebaut, dass man von einem funktionierenden Frühwarnsystem sprechen kann.

1.1 25 Jahre Datenschutz im Land Bremen

In 2003 gab es „25 Jahre Datenschutz in der Freien Hansestadt Bremen" zu feiern. Ich habe dieses Jubiläum zum Anlass genommen, eine Festausgabe auf einer multimedialen CD herauszugeben. Die CD spiegelt die wechselvollen Themen und Entwicklungen der Vergangenheit wider, enthält aktuelle Sammlungen und Übersichten und wirft interessante Blicke in die Zukunft. Auszugsweise zu nennen sind: Die Bürger werden über ihre aktuellen Datenschutzrechte aufgeklärt, ein chronologischer Überblick und eine Zeitleiste zur Datenschutzgesetzgebung im Land, verbunden mit den Plenarprotokollen aus der Bremischen Bürgerschaft zur Datenschutzgesetzgebung, wie auch eine umfassende Sammlung des Landesrechts zum Datenschutz sind auf der CD zu finden. Die Landesbeauftragten für den Datenschutz in Bremen, die Senatskommissare sowie die acht Vorsitzenden des Datenschutzausschusses in den einzelnen Legislaturperioden kommen zu Wort. Alle 25 Jahresberichte liegen auf der CD komplett in elektronischer Form vor, was mich darüber hinaus erstmalig in den Stand versetzt, Bestellungen alter Jahresberichte nachzukommen. Wer einmal versucht hat, ein Werk mit einer Vielzahl von Autoren herauszubringen, wird erahnen können, wie viel Mühe es bereitet hat, alle Beiträge zusammenzustellen. Gleichwohl hat sich der Aufwand gelohnt, die Beschäftigung mit der Vergangenheit hat auch Freude bereitet und das vielseitige Lob für die CD waren Dank genug. Gleichzeitig wurde mit ihr ein Grundstock gelegt, der sich jederzeit aktualisieren lässt, denn die Navigationsinstrumente auf der CD lassen sich auch bei Erweiterungen nutzen. Die erste Auflage von 1.000 CD war schnell vergriffen, lediglich einige wenige Stücke wurden für besondere Anlässe zurückgehalten.

1.2 Zwanzig Jahre Volkszählungsurteil

Ein weiteres Jubiläum war 2003 zu feiern: Vor zwanzig Jahren, am 15. Dezember 1983, hatte das Bundesverfassungsgericht mit dem Volkszählungsurteil das

Grundrecht auf informationelle Selbstbestimmung anerkannt und damit eine grundlegende Änderung des gesamten Datenschutzes in Gesetzgebung, Rechtsprechung und Praxis bewirkt. Das Bundesverfassungsgericht hat in den Leitsätzen zum Volkszählungsurteil festgehalten: „Das Grundrecht gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen. Einschränkungen dieses Rechts auf informationelle Selbstbestimmung sind nur im überwiegenden Allgemeininteresse zulässig."

Das in dem Urteil zum Ausdruck kommende Grundrechtsverständnis, das die Selbstbestimmung des Bürgers als Regelfall und ihre Einschränkung als Ausnahme feststellt, ist bis heute keineswegs durchgängig akzeptiert. Statt Verfahren ohne personenbezogene Daten einzusetzen, zeichnet sich ab, dass verstärkt Identifikationsnummern und solche Systeme eingeführt werden, die das Verhalten des Einzelnen kontrollierbar machen. Beispiele dafür sind die elektronische Kontrolle mit den neuen Ortungstechniken, Videoüberwachung und die geplante Vorratsspeicherung von Kommunikationsdaten durch Telefonanbieter sowie der Einsatz von RFID-Mikrochips. Diese und andere Entwicklungen gefährden das Recht auf informationelle Selbstbestimmung in immer stärkerem Maße. Das Bundesverfassungsgericht hat im Volkszählungsurteil ausdrücklich vor den Gefahren der unbegrenzten Erhebung und Verwendung persönlicher Daten durch den flächendeckenden Einsatz von Informations- und Kommunikationstechnik gewarnt.

Insbesondere wird die weitere Aussage des Bundesverfassungsgerichts häufig übergangen, dass die Einschränkungen zu Lasten des Bürgers nicht weitergehen dürfen, „als es zum Schutze öffentlicher Interessen unerlässlich ist". Gerade in jüngster Zeit sind wieder Tendenzen festzustellen, dieses Verhältnis umzudrehen, was zum Beispiel in dem Schlagwort zum Ausdruck kommt, der rechtstreue Bürger brauche sich vor staatlicher Datenverarbeitung nicht zu fürchten. Dabei wird vergessen, dass nicht der Bürger sich dafür rechtfertigen muss, dass er einen Eingriff in sein informationelles Selbstbestimmungsrecht nicht hinnehmen will, vielmehr ist der Staat dafür beweispflichtig, dass die geplante Datenverarbeitung mit personenbezogenen Daten zwingend erforderlich ist.

Auf der anderen Seite hat das Urteil des Bundesverfassungsgerichts eine Reihe positiver Datenschutzregelungen in Gesetzen und Verordnungen des Bundes und des Landes hervorgerufen. Die Änderung der bremischen Landesverfassung in Art. 12 wäre ohne das Volkszählungsurteil nicht zu denken. Exemplarisch sei hier weiter an die Datenschutzordnung der Bremischen Bürgerschaft, das Bremische Krankenhausdatenschutzgesetz oder das Bremische Schuldatenschutzgesetz, auch wenn dieses demnächst novelliert werden soll, erinnert.

1.3 Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

Immer mehr Beschäftigte in Wirtschaft und Verwaltung erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner sowie bei der technischen Abwicklung sind bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Beschäftigten neben der beruflichen auch eine private Nutzung des Internets am Arbeitsplatz gestattet wird.

In dem Maße aber, in dem der Einsatz moderner Telekommunikationstechnik im Arbeitsumfeld zunimmt, wachsen auch die Gefahren für die informationelle Selbstbestimmung der Beschäftigten. Das Surfen im Internet oder das Versenden von E-Mails hinterlässt Datenspuren auf dem Arbeitsplatzrechner, auf dem Internetserver und in den Netzen. In wachsendem Maße sind die Beschäftigten auf die Nutzung von E-Mail und Internet bei ihrer Arbeit angewiesen. Es wird für Vorgesetzte und Arbeitgeber daher leichter, durch die Auswertung und die Kenntnisnahme von protokollierten Verbindungs-, Nutzungs- oder sogar Inhaltsdaten, umfassend die Leistung und das Verhalten ihrer Mitarbeiter zu kontrollieren. Datenschutz- und Arbeitsrecht müssen daher für einen Ausgleich zwischen den Direktions- und Kontrollrechten der Arbeitgeber auf der einen Seite und dem Schutz der informationellen Selbstbestimmung der Beschäftigten auf der anderen Seite sorgen.

Bei der beruflichen Nutzung ist eine Kontrolle bei konkretem Missbrauchsverdacht im Einzelfall zulässig, auch hat der Arbeitgeber grundsätzlich das Recht, stichprobenartig zu prüfen, ob das Surfen oder das Versenden von E-Mails dienstlicher Natur ist. Eine umfassende automatisierte Vollprotokollierung aller Aktivitäten hingegen ist untersagt. Wird eine private Nutzung erlaubt, so ist es grundsätzlich möglich, diese Erlaubnis an einschränkende Voraussetzungen zu knüpfen. Beschäftigte, die jedoch solche Voraussetzungen nicht erfüllen wollen, müssen ihre Einwilligung ohne berufliche Nachteile verweigern können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits in einer Entschließung der 63. Konferenz (vgl. 25. JB, Ziff. 15.3) wesentliche dabei zu beachtende Grundsätze formuliert.

Im vergangenen Jahr bin ich häufig mit Fragen aus diesem Bereich konfrontiert worden (vgl. z. B. Ziff. 16.3.1 dieses Berichts), wobei mich sowohl Beschäftigte wie auch betriebliche Datenschutzbeauftragte um Rat gebeten haben. In einem Fall hatte der Arbeitgeber sämtliche private E-Mails einer Beschäftigten während ihres Urlaubs gelesen und darauf gestützt, eine Kündigung ausgesprochen. Auch das TuI-Referat des Senators für Finanzen hat mich bei der Entwicklung einer Internetnutzungsrichtlinie intensiv beteiligt; es konnte auch die Abstimmung mit dem Gesamtpersonalrat noch im letzten Jahr erreicht werden, so dass einer Umsetzung in 2004 nichts mehr im Wege steht (vgl. Ziff. 5.4 dieses Berichts). Zu begrüßen ist insbesondere, dass durch die Verwendung des so genannten P-Switch eine klare Trennung zwischen dienstlicher und privater Nutzung möglich wird, so dass auch bei einer Kontrolle durch den Arbeitgeber keine Vermischung dieser beiden Sphären auftreten kann.

1.4 Behördliche Datenschutzbeauftragte

Durch die Novelle des Bremischen Datenschutzgesetzes (BremDSG) sind dem behördlichen Datenschutzbeauftragten wichtige Aufgaben zugewachsen. Der mit der Modernisierung der Verwaltung einhergehende verstärkte Einsatz automatisierter Verfahren und fachspezifischer eGovernment-Anwendungen stellt erhöhte Anforderungen an die Kompetenz und Sachkunde der behördlichen Datenschutzbeauftragten, sowohl im Bereich des Datenschutzrechts wie auch im Bereich des technischen Datenschutzes. Darüber hinaus haben die behördlichen Datenschutzbeauftragten nunmehr bereits im Vorfeld neue Aufgaben, wenn wegen der Art der zu verarbeitenden Daten oder der Verwendung neuer Technologien besondere Risiken damit verbunden sind. Mit der Novellierung hat der Landesgesetzgeber sich dazu entschlossen, den öffentlichen Stellen beim Einsatz automatisierter Verfahren für die Verarbeitung personenbezogener Daten verbindlich die Bestellung eines Beauftragten für den Datenschutz vorzuschreiben, § 7 a BremDSG. Damit folgt er dem auch im Bundesdatenschutzgesetz für öffentliche und private Stellen verankerten Gedanken, zur Gewährleistung des Datenschutzes die Selbstkontrolle in den öffentlichen Stellen der Fremdkontrolle durch den Landesbeauftragten vorzuschalten.

Die Bestellung eines behördlichen Datenschutzbeauftragten ist mir anzuzeigen. Im Laufe des Jahres sind eine ganze Reihe von Meldungen bei mir eingegangen, allerdings muss ich ein Jahr nach In-Kraft-Treten dieser Bestimmung noch davon ausgehen, dass viele öffentliche Stellen ihrer gesetzlichen Verpflichtung zur Bestellung eines behördlichen Datenschutzbeauftragten immer noch nicht nachgekommen sind. Ich habe mich daher entschlossen, in 2004 noch einmal alle Stellen auf die gesetzliche Regelung hinzuweisen. Auf meiner Internetseite habe ich ausführlich die Aufgaben der behördlichen Datenschutzbeauftragten und die Verfahren zur Bestellung beschrieben. Im Intranet der öffentlichen Verwaltung in Bremen habe ich in den öffentlichen Ordnern auf dem Formularserver Bestellungsvordrucke zum Abruf bereitgestellt. Darüber hinaus biete ich für behördliche Datenschutzbeauftragte Schulungen an.

1.5 Tod in der Neustadt

Im Sommer des Berichtsjahres wurde in der Stadtgemeinde Bremen eine psychisch kranke Frau beschuldigt, eine Nachbarin getötet zu haben. Bei mir schrillten deshalb die Alarmglocken, weil in einem Pressebericht am 18. Juli 2003 behauptet wurde, der Datenschutz sei an einer nicht ausreichenden Information der beteiligten Stellen schuld. Ich habe daher umgehend den Vorgang bei den betei-

ligten Stellen prüfen lassen, denn hätte eine Vorschrift bestanden, die eine hinreichende Information der beteiligten Stellen verhindert hätte, so hätte diese umgehend geändert werden müssen. Die datenschutzrechtlichen Nachforschungen haben aber ergeben, dass ein umfassender Datenaustausch zwischen der Psychiatrie, dem Stadtamt, der Polizei und dem Vormundschaftsgericht in solchen Fällen möglich ist. Bereits wenige Tage später titelte die Presse dann auch mit: „Die 41-jährige Täterin . . . war der Polizei einschlägig bekannt – doch angeblich ist diese Information nicht weitergereicht worden."

Der Datenschutz Mitschuld an einem Tötungsdelikt? Indirekt verbunden sah ich damit wieder einmal den platten Vorwurf, der Datenschutz sei Täterschutz. Ich habe nicht mehr aufklären können, wie diese Pressemeldung zu Stande gekommen ist, aber manche interessierte Kreise können den Versuch nicht lassen, den Datenschutz an den Pranger zu stellen. Unabhängig von meinem Prüfergebnis in der Sache kommt auch die vom Senat eingesetzte interne Untersuchungsgruppe in ihrem Prüfbericht zu dem Ergebnis, dass nicht der Datenschutz eine Mitschuld trägt, sondern ausschlaggebend waren andere Umstände, die dazu führten, dass die Tat nicht verhindert wurde. Damit wird der Datenschutz auch von neutraler Seite von dem Vorwurf, er trage eine Mitschuld an dem Tod der Frau, entlastet (vgl. Ziff. 8.2.5 dieses Berichts).

1.6 Zum Ausgang der Rasterfahndung

Zu den datenschutzrechtlich umstrittensten Themen der letzten beiden Jahre gehört die Rasterfahndung. Viele Fragen sind dabei offen geblieben, eine Evaluation dieses Instruments erscheint nach wie vor erforderlich. Ich habe die damit im Zusammenhang stehende Datenverarbeitung in Bremen bis zum Abschluss der Rasterfahndung verfolgt und in einer Stichprobe die rund 20 Personendatensätze einer letzten Prüfung unterzogen, die dem Staatsschutz bei der Polizei Bremen zur weiteren Abklärung übergeben wurden (vgl. Ziff. 6.1.3 dieses Berichts). Hervorheben möchte ich an dieser Stelle, dass das Bundeskriminalamt (BKA) bestätigt hat, dass aus Bremen stammende Datensätze, die beim BKA in die bundesweite Rasterfahndung mit einbezogen wurden, nicht an Nachrichtendienste und auch nicht an ausländische Polizeidienststellen weitergegeben wurden. Die an das BKA übermittelten Daten der Rasterfahndung durch die Polizei Bremen wurden im April 2003 dort gelöscht. In Bremen wurden die Daten der Rasterfahndung im September 2003 gelöscht und die zugehörige Arbeitsdatei aufgelöst.

1.7 Datenabgleich

Öffentliche Kritik gab es in 2003 sowohl in Bremen wie in Bremerhaven an der Durchführung eines Datenabgleichs von Sozialhilfeempfängern mit der Kfz-Zulassungsstelle. Dieser Abgleich ist aber im Bundessozialhilfegesetz geregelt (§ 117 BSHG). Ich hatte daher nur die rechtmäßige Verarbeitung der Daten zu kontrollieren.

Auch die Bremer Entsorgungsbetriebe (BEB) wollten im vergangenen Jahr einen Datenabgleich vorbereiten, um zu überprüfen, ob die Bremer Haushalte entsprechend der Anzahl der Bewohner eines Grundstücks auch genügend Müllgebühren bezahlen. Hierzu war ein Onlinezugriff auf das Melderegister geplant. Die Vertragspartner der BEB sind die Hauseigentümer, nicht etwa die Mieter. Es hätte daher für die Fragestellung der BEB ausgereicht, wenn die Anzahl der Haushalte und Bewohner bekannt gegeben worden wäre. Ein Zugriff auf die Namen der Bewohner war dafür nicht erforderlich. Am Ende hat das Bauressort die Planungen zum Datenabgleich abgebrochen, laut Presseberichten, „weil sich der Aufwand nicht lohne und es Probleme mit dem Datenschutz gebe". Auch wenn das Ziel des Datenabgleichs ohne die Verarbeitung personenbezogener Daten hätte erreicht werden können, freut es mich, wenn so viel Rücksicht auf den Datenschutz genommen wird.

1.8 Vom Big Brother am Straßenrand und anderen Überwachungstechniken

Nach dem Motto „steter Tropfen höhlt den Stein" werden immer neue Ansprüche zur Verwendung von Video- und anderen Überwachungstechniken formuliert. Hierzu zähle ich die Vorschläge aus einem benachbarten Land, nachdem dort ein

Schüler gequält worden ist, die Schulhöfe videoüberwachen zu lassen, ebenso wie den Vorschlag, an belebten Straßen Videokameras zu installieren, die die Nummernschilder vorbeifahrender Fahrzeuge registrieren sollen, um diese Daten dann mit in polizeilichen Systemen gespeicherten Daten abzugleichen. Schließlich wurden nicht umsonst die neuen Nummernschilder mit maschinenlesbaren Kennzeichen eingeführt. Die Datenschutzbeauftragten müssen sich daher auch mit diesen Vorhaben datenschutzrechtlich beschäftigen. Mit der polizeilichen Videoüberwachung auf dem Bahnhofsvorplatz in Bremen, wie auch in Firmen und Betrieben, habe ich mich im letzten Jahresbericht hinreichend auseinandergesetzt. Im Berichtsjahr konnte ich vermehrt Eingaben zum Einsatz von Videokameras vermerken, die zum Objektschutz montiert waren, aber zugleich den öffentlichen Raum überwachten (vgl. Ziff. 16.4.1 dieses Berichts). Seit Einführung der Überwachungskameras in öffentlichen Verkehrsmitteln in Bremen reißt der Strom der Beschwerden nicht ab, dabei ist bisher nur ein Teil der Fahrzeuge mit Videotechnik ausgestattet (vgl. Ziff. 16.4.2 dieses Berichts). Auch die so genannten Webcams, die Bildsequenzen ins Internet stellen, können zur Beobachtung menschlichen Verhaltens genutzt werden. Wegen grundsätzlicher Fragestellungen zum Einsatz solcher Kameras habe ich den Düsseldorfer Kreis mit dieser Thematik befasst (vgl. Ziff. 16.4.3 dieses Berichts). Durch die geplante Einführung des Maut-Systems hätten sich weitere Überwachungsmöglichkeiten geboten, zumal bei der Durchfahrt an den Maut-Kontrollbrücken alle Fahrzeuge, Lkw wie Pkw, erfasst werden sollten. Bei der automatischen Einbuchung durch die so genannte On-Board-Unit (OBU) sollte jede Autobahnbenutzung eines Lkw per Satellitennavigation mit Positions- und Fahrzeugdaten registriert und über GSM-Mobilfunk an die Betreibergesellschaft übermittelt werden. Die Begehrlichkeiten anderer Stellen an diesen Daten sind abzusehen, ebenso wie beim Handy, das zunächst ausschließlich zum Telefonieren konzipiert, mehr und mehr zum Überwachungsinstrument umfunktioniert wird (vgl. Ziff. 1.21 dieses Berichts).

1.9 eGovernment

Durch die Einführung von eGovernment begibt sich die Verwaltung auf lange Sicht in zunehmendem Maße in die Abhängigkeit von elektronischen Datenverarbeitungssystemen. Damit entstehen neue Gefahren für das informationelle Selbstbestimmungsrecht. Netzsicherheit, Nutzungsprofile, die Verantwortlichkeit für elektronisch getroffene Entscheidungen oder Fragen zur Sicherstellung der eindeutigen Identität der Nutzer sind in diesem Zusammenhang zu nennen. Die Datenschutzbeauftragten des Bundes und der Länder haben Empfehlungen zum Datenschutz einer serviceorientierten Verwaltung erarbeitet. Sie wurden dabei durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Professoren Lenk und Rossnagel unterstützt. Auch ich habe an dieser Arbeitsgruppe mitgewirkt, die Arbeiten konnten im Frühjahr 2003 abgeschlossen werden. Produkt ist eine auch bei mir erhältliche Broschüre, in der neben der Darstellung rechtlicher Rahmenbedingungen viele praktische Handlungsempfehlungen enthalten sind. Umfangreich und interessant ist auch die Sammlung ausgewählter eGovernment-Anwendungen (vgl. Ziff. 3.2 dieses Berichts). Adressaten dieser Veröffentlichung sind in erster Linie Verwaltungschefs, Organisatoren, Verfahrensentwickler, IT-Verantwortliche, behördliche Datenschutzbeauftragte und Personalräte, eben alle, die Anwendungen von eGovernment vorzubereiten oder umzusetzen haben. Daneben kommen aber auch die privaten Anwender und Bürger, die eGovernment nutzen wollen, nicht zu kurz. Für sie finden sich Hinweise und Empfehlungen zum Selbstschutz, denn ein wesentlicher Teil der Verantwortung für Sicherheit und Vertraulichkeit ihrer Daten verbleibt bei ihnen selbst.

1.10 Lauschangriff

Zur Reihe der grausamen Angriffe wider den Datenschutz zählt auch der Vorschlag, für den sich die Justizminister und -ministerinnen der Bundesländer im Sommer 2003 mehrheitlich ausgesprochen haben sollen. Ihr Vorschlag war laut Presseberichten, eine gesetzliche Grundlage dafür zu schaffen, dass Hausverwalter, Schlüsseldienste, Angestellte der Stadtwerke oder Schornsteinfeger künftig aushelfen sollen, wenn Kriminalpolizei oder Verfassungsschutz „Wanzen“ in Wohnungen oder Geschäftsräumen platzieren wollen. Der Nachbar als Schnüffler und verlängerter Arm der Staatsmacht?

In 2003 habe ich zusammen mit anderen Datenschutzbeauftragten der Länder eine Stellungnahme gegenüber dem Bundesverfassungsgericht (BVerfG) in der Verfassungsbeschwerde zu Art. 13 Abs. 3 bis 6 GG (BvR 2378/98 u. BvR 1084/99) im Verfahren gegen den so genannten Großen Lauschangriff abgegeben und darin meine verfassungsrechtlichen Bedenken zum Ausdruck gebracht. Die mit Spannung erwartete Verkündung einer Entscheidung in dieser Sache ist vom Gericht für das Frühjahr 2004 terminiert. Ich hoffe, dass das Gericht die Gelegenheit nutzt, auch zu der genannten, von den Justizministern und -ministerinnen mehrheitlich getragenen Initiative, deutliche Worte zu finden.

Für das Land nachzutragen bleibt: Ergebnis der Parlamentarischen Kontrollkommission ist, dass im Land Bremen im Jahr 2002 keine Maßnahme nach § 100 c Abs. 1 Nr. 3 der Strafprozessordnung durchgeführt wurde, die von einem bremischen Gericht angeordnet wurde (Bremische Bürgerschaft Drs. 16/20).

1.11 Beratung neuer Datenschutzvorschriften im Land

Im April 2003 traten Änderungen des Bremischen Verwaltungsverfahrensgesetzes in Kraft (Brem.GBl. 2003, S. 147 ff.). Mit den Änderungen soll die elektronische Kommunikation im Verwaltungsverfahren ermöglicht werden. Ebenfalls im Frühjahr beriet ich einen Arbeitsentwurf des Senators für Inneres, Kultur und Sport zur Änderung des bremischen Verfassungsschutzgesetzes. Die Formulierungen waren schon sehr weit gediehen, einige wenige Punkte waren aus datenschutzrechtlicher Sicht noch kontrovers und hätten der politischen Meinungsbildung zugeführt werden können. Wohl auch wegen der bevorstehenden Bürgerschaftswahl wurde das Gesetz nicht mehr in die Bremische Bürgerschaft eingebracht.

Die Beratungen zur Änderung des Bremischen Krankenhausdatenschutzgesetzes (Brem.GBl. 2003, S. 47) hingegen wurden noch zum Ende der Legislaturperiode abgeschlossen. Wesentliches Anliegen dieser Gesetzesnovelle war, die Datenschutzbestimmungen den veränderten technischen Bedingungen und praktischen Behandlungsbedürfnissen in den Krankenhäusern anzupassen, ohne das im Bremischen Krankenhausdatenschutzgesetz verankerte Datenschutzniveau zu verschlechtern (vgl. Ziff. 8.1.1 dieses Berichts).

Seit Ende 2002 befasst sich eine Arbeitsgruppe mit der Überarbeitung der Aktenordnung für die Behörden der Freien Hansestadt Bremen und der Stadtgemeinde Bremen. Die jetzt noch gültige Fassung stammt aus dem Jahr 1958 und ist dringend überarbeitungsbedürftig. Sie genügt weder den Anforderungen des Datenschutzes noch berücksichtigt sie die neuen technischen Anforderungen, die sich aus einer modernen Bürokommunikation ergeben. Die neue Aktenordnung soll die Rahmenvorgaben für den Umgang mit und die Organisation von Schriftgut geben, dessen nähere Ausgestaltung den senatorischen Bereichen überlassen werden soll. Ich habe in der Arbeitsgruppe mitgewirkt, die Arbeiten stehen kurz vor dem Abschluss.

Durch die Mithilfe des Rechtsausschusses konnte darüber hinaus im vergangenen Jahr erreicht werden, das Einvernehmen über den Inhalt einer Internet-Nutzungsrichtlinie zwischen den beteiligten Stellen herzustellen. Der Senator für Finanzen hat die I.8 Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet Zugängen in Kraft gesetzt und Anfang 2004 im Amtsblatt (Brem.ABl. 2004, S. 77 ff.) veröffentlicht. Auch die Arbeiten an einer Verordnung zum Datenschutzaudit von öffentlichen Stellen (vgl. Ziff. 3.4 dieses Berichts) sind weitestgehend abgeschlossen, ich rechne mit einer baldigen Veröffentlichung. Die Richtlinien für die E-Mail-Nutzung in der Seestadt Bremerhaven, die für den Magistrat und die Vollzugspolizei unterschiedlich ausfallen werden, stehen kurz vor dem in Kraft setzen.

In Kraft getreten ist zwischenzeitlich auch die Änderung der bremischen Meldedatenübermittlungsverordnung (§ 5 Abs. 18 MeldDÜV), die die Einrichtung von Online-Zugriffen auf das Einwohnermelderegister durch die Amtsgerichte Bremen, Bremen-Blumenthal und Bremerhaven sowie das Landgericht Bremen ermöglicht (Brem.GBl. 2004, S. 37).

1.12 Internetauftritt: www.datenschutz.bremen.de

Der im Jahr 2001 begonnene Internetauftritt des Landesbeauftragten für den Datenschutz hat sich mittlerweile etabliert. Allerdings muss immer wieder Arbeit hi-

neingesteckt werden, um die vorhandenen Seiten à jour zu halten. Der Aktualisierungsaufwand wird vom Besucher nicht gesehen, aktuelle Seiten werden einfach erwartet, eine nicht aktuelle Homepage wird binnen kurzer Zeit mit Nichtbeachtung gestraft. Der flüchtige Besucher ist häufig nur an Neuem interessiert. Ich habe daher auch im vergangenen Jahr das Angebot weiterentwickelt, wenn auch in 2003 ein Schwerpunkt in der Erstellung der CD „25 Jahre Datenschutz in der Freien Hansestadt Bremen“ lag.

Natürlich kann ich mich mit dem umfassenden Angebot des Virtuellen Datenschutzbüros unter www.datenschutz.de nicht messen, sehe aber das Angebot auch nicht als Konkurrenz. Auf meiner Homepage liegen in erster Linie Seiten, die die Bürger im Land erreichen sollen; soweit darüber hinaus ein gutes bundesweit interessierendes Angebot auf meiner Internetseite besteht, wird dieses mit dem Virtuellen Datenschutzbüro verlinkt.

Eine projektbezogene Arbeitsgemeinschaft der Deutschen Hochschule für Verwaltungswissenschaften Speyer hat im Rahmen des Themas eGovernment „Datenschutz im Internet – Internet im Datenschutz" die Internetauftritte der Datenschutzbeauftragten des Bundes und der Länder auf den Prüfstand gestellt. Wesentliche Kriterien waren hierbei der Inhalt und die Aufbereitung der Informationen, Benutzerfreundlichkeit, angebotene Kommunikation und Transaktion.

Dabei hat der Bremer Internetauftritt die bestmögliche Bewertung „außerordentlich erfreulich" erhalten.

In dem Speyerer Arbeitsheft 2003, Nr. 153, werden die Homepages der Datenschutzbeauftragten in Bund und Ländern auf 60 Seiten genauestens untersucht. Für die Homepage des LfD Bremen wird besonders hervorgehoben, dass das Datenschutzscheckheft des Landesbeauftragten für den Datenschutz „eine sehr gute Übersicht von Downloadmöglichkeiten standardisierter Formulare zur Wahrung von Auskunftsrechten enthält".

Die Anzahl der Aufrufe meiner Homepage ist auch immer ein Gradmesser für das Interesse der Internetgemeinde am Datenschutz. Ende 2002 landete ich mit dem Thema „Selbstverteidigung im Internet“ einen Volltreffer, die Zugriffe auf die Homepage nahmen im Dezember rapide zu. Dies hielt auch noch im Januar 2003 an, danach gingen die Zugriffe um rund 20 Prozent zurück, stabilisierten sich aber auf einem höheren Niveau gegenüber dem Vorjahr. Besonders berichtenswert erscheint mir aber die Zahl der Downloads des letzten Jahresberichts. Der 25. Jahresbericht, der zum 31. März 2003 eingestellt wurde, ist bis Ende Dezember, also im letzten dreiviertel Jahr, 927 mal abgerufen worden, d. h. pro Monat werden über 100 Jahresberichte aus Bremen über das Internet nachgefragt. Allein die Gesamtzahl der Abrufe des Jahresberichts in elektronischer Form bis Dezember ist doppelt so hoch wie die Anzahl der für die Bürger in Papierform vorgehaltenen Jahresberichte. Drucklegung und Versandporto eingerechnet, rechtfertigt allein dieser eingesparte Posten die Kosten für meinen Internetauftritt.

1.13 Öffentlichkeitsarbeit und Presseresonanz

Auch im vergangenen Jahr habe ich wieder zu aktuellen Themen der Informationsverarbeitung Stellung genommen und in Pressemitteilungen und Interviews auf neue Entwicklungen im Datenschutz aufmerksam gemacht. Meine Pressemitteilungen sind jeweils aktuell auf meiner Homepage www.datenschutz.bremen.de abrufbar. Dass Datenschutzthemen auch im vergangenen Jahr einen breiten Raum in der Presseberichterstattung eingenommen haben, ist dem im Anhang beigefügten Pressespiegel (vgl. Ziff. 20.1 dieses Berichts) zu entnehmen.

1.14 Fortbildung durch den LfD

Im Berichtszeitraum haben Mitarbeiter des Landesbeauftragten für den Datenschutz verschiedene Fortbildungsveranstaltungen abgehalten oder mitgestaltet. Dies waren z. B. Veranstaltungen beim Aus- und Fortbildungszentrum der Bremischen Verwaltung (AFZ), an der Wirtschafts- und Sozialakademie der Arbeitnehmerkammer, bei Radio Bremen sowie Fortbildungen für Personalräte und für betriebliche Datenschutzbeauftragte zu speziellen, insbesondere technischen Themen. Weiter habe ich mich an der Schulung von Administratoren und Webmastern

zur Internetnutzung in Schulen beteiligt. Eine gleiche Schulungsveranstaltung habe ich im Ökumenischen Gymnasium in der Stadt Bremen durchgeführt.

Auf Bitten der Dienstleistungsgewerkschaft „ver.di" habe ich im Rahmen des Projektes Call-Center in Niedersachsen/Bremen auf einem Seminar und auf dem 21. Treffen des Netzwerkes von Call-Center-Beschäftigten auf einer Abendveranstaltung zum Thema „Arbeitnehmerdatenschutz in Call-Centern" über die besonderen Datenschutzprobleme beim Arbeiten in Call-Centern referiert.

Im nächsten Jahr sehe ich insbesondere Fortbildungsbedarf für neu bestellte behördliche Datenschutzbeauftragte nach § 7 a des BremDSG. Es ist beabsichtigt, für diesen Personenkreis in Zusammenarbeit mit dem AFZ und der datenschutz nord GmbH Fortbildungsveranstaltungen anzubieten.

1.15 Zur Situation der Dienststelle

Personelle Abgänge konnten durch personelle Neuzugänge aufgefangen werden, auch wenn dies nicht lückenlos gelang. Dabei gilt ein besonderer Dank dem Senator für Finanzen, der für ein Jahr einen Juristen aus seinem Einstellungspool an meine Dienststelle abgeordnet hat. Ohne diese Hilfe hätte ich meinen gesetzlichen Aufgaben nicht im erforderlichen Umfang nachkommen können. Die Lage wird im nächsten Jahr erneut prekär werden, weil durch den Abgang eines erfahrenen und bewährten Kollegen ohne erneute fremde Hilfe aus personalwirtschaftlichen Gründen kein Ersatz zur Verfügung stehen wird. Diese Situation wird sich in den nächsten Jahren noch erheblich verschärfen, wenn weitere Beschäftigte vorzeitig ausscheiden werden. Ich bin um Lösungen bemüht und benötige für die Überbrückung dieser Zeit gegebenenfalls auch politische Unterstützung.

Eine weitere Entwicklung ist berichtenswert: Im vergangenen Jahr ist es endlich gelungen, ein elektronisches Dokumentenmanagementsystem nach dem DOMEA-Prinzip in meiner Dienststelle einzuführen. Dazu mussten von allen Beschäftigten in der Dienststelle erhebliche Vorarbeiten geleistet werden, denn das System musste auf die Struktur und die Bedingungen der Dienststelle voreingestellt werden. In Schulungen waren dann vor Einführung alle Beschäftigten der Dienststelle mit den Funktionen und dem Aufbau des Systems vertraut zu machen, denn ab dem Zeitpunkt der Einführung musste jeder die Anwendung beherrschen. So muss jetzt jeder selbst seine E-Mails und andere elektronische Dokumente den entsprechenden Vorgängen zuordnen oder auch durch Recherche elektronisch abgespeicherte Dokumente im System auffinden. Auch die Ausgangsschreiben werden mit Hilfe des Systems erstellt.

Nicht leistbar wäre es gewesen, auch den gesamten alten Aktenbestand in das neue System zu integrieren. Ich habe mich dazu entschlossen, die alten Akten über einen Zeitraum von fünf Jahren auszusondern. Nur soweit nach dem Stichtag der Einführung des Systems Themen aus dem alten Aktenbestand aufgegriffen werden, werden diese in das neue System überführt. Dies wird dann im alten Aktenplan vermerkt. Auch das Scannen der gesamten eingehenden Post ist personell nicht leistbar, so dass es weiterhin neben der elektronischen Akte eine papierene Akte geben kann. In der elektronischen Akte ist aber erkennbar, welche weiteren Dokumente außerhalb des Aktenverwaltungssystems zu dem jeweiligen Vorgang bestehen. Eine über 25 Jahre eingefahrene Aktenverwaltung auf einen Stichtag hin umzustellen, ist kein leichtes Unterfangen und bedurfte der Anstrengung aller. Durch ihre Beteiligung bei der Auswahl und der Umsetzung des Systems ist eine hohe Akzeptanz in der Dienststelle erreicht worden. Auch wenn die Umstellung mit erheblichen Strapazen verbunden war und noch ist, zeichnet sich doch schon jetzt ab, dass sich der Schritt gelohnt hat und in vielen Bereichen zu erheblichen Arbeitserleichterungen führt. Selbstverständlich wurden für die Einführung des Systems Regelungen zur Aktenverwaltung getroffen und ein Datenschutzkonzept in Kraft gesetzt.

1.16 Kooperationen

Das Datenschutzgesetz verpflichtet zur Zusammenarbeit mit allen Stellen, die mit Kontrollaufgaben des Datenschutzes betraut sind (§ 27 Abs. 5 BremDSG). In der Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr unter dem Vorsitz des Sächsischen Datenschutzbeauftragten

tagte, wurden erneut eine Reihe von Entschließungen gefasst, die die Fortentwicklung des Datenschutzes fördern sollen. Sie sind im Anhang zu diesem Bericht zu finden. Im Jahr 2004 geht der Vorsitz auf den Saarländischen Datenschutzbeauftragten über.

Angesichts der weiterhin rasanten technischen Entwicklung auf allen Gebieten der Informationsverarbeitung und unter engen personellen Ressourcen bei fast allen für den Datenschutz zuständigen Kontrollstellen, ist die Zusammenarbeit in den Arbeitskreisen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder ein Gebot der Vernunft. Ich versuche im Rahmen der Möglichkeiten meines Reisekostenbudgets eine Teilnahme Bremens sicherzustellen.

Im Laufe des Jahres hat es wieder Wechsel unter den Datenschutzbeauftragten gegeben, so in Hessen und in Sachsen. Hervorheben möchte ich an dieser Stelle die Neuwahl von Peter Schaar zum Bundesbeauftragten für den Datenschutz (Plenarprotokoll 15/76, 14.11.2003, S. 6572 und S. 6584) und das Ausscheiden von Dr. Joachim Jacob nach Ablauf seiner zweiten Amtsperiode. Der Bundesbeauftragte für den Datenschutz wird auf fünf Jahre gewählt.

Weiter unterstütze ich das „Virtuelle Datenschutzbüro“, dies ist der gemeinsame Internetauftritt der Datenschutzbeauftragten aus Deutschland, der Schweiz, den Niederlanden und Kanada. Das Virtuelle Datenschutzbüro hat sein Angebot erneut erweitert und verbessert. Es ist unter www.datenschutz.de zu erreichen.

Im Berichtszeitraum hat auch wieder ein Meinungsaustausch mit dem Datenschutzbeauftragten von Radio Bremen stattgefunden. Die Erörterung von Fragen gemeinsamen Interesses soll im kommenden Jahr fortgesetzt werden.

Auch mit der landeseigenen „datenschutz nord GmbH“ hat es wieder eine Zusammenarbeit in verschiedenen Projekten, die nicht meiner Datenschutzkontrolle unterliegen, gegeben. Die GmbH hat mittlerweile in verschiedenen Projekten im Land Bremen zur Verbesserung des Datenschutzniveaus beigetragen. Ihre Unterstützung wird mittlerweile auch von Datenschutzkontrollinstanzen anderer Länder nachgefragt. Ich pflege mit der GmbH einen regelmäßigen Gedankenaustausch.

Was im öffentlichen Bereich durch die Konferenz der Datenschutzbeauftragten u. a. erreicht wird, nämlich die Findung gemeinsamer Positionen zu Themen mit länderübergreifenden Inhalten, wird im nicht öffentlichen Bereich durch den „Düsseldorfer Kreis“ sichergestellt. Der „Düsseldorfer Kreis” ist das Abstimmungsgremium unter den Datenschutzaufsichtsbehörden, um eine einheitliche Auslegung der Vorschriften des Bundesdatenschutzgesetzes für den privaten Bereich zu gewährleisten. Einige Ergebnisse finden sich im Abschnitt Ziff. 16. dieses Berichtes wieder.

Abgerundet werden soll der Bericht über die Kooperationen mit dem Hinweis, dass ich in der Funktion der Datenschutzaufsichtsbehörde für den nicht öffentlichen Bereich auch in 2003 wieder mit dem GDD Erfakreis Bremen/Weser-Ems, ein Kreis, in dem sich die betrieblichen Datenschutzbeauftragten der Region zusammengeschlossen haben und einen Meinungs- und Erfahrungsaustausch pflegen, zusammengearbeitet habe. Die Datenschutzaufsichtsbehörde informiert den Erfakreis oder seine Unterarbeitskreise gelegentlich in Vorträgen über neuere Entwicklungen. Wesentlicher Bestandteil der Zusammenarbeit sind technische und rechtliche Fragen, hier insbesondere Fragen der Auslegung des Bundesdatenschutzgesetzes und anderer spezialrechtlicher Regelungen des Datenschutzes, wie zum Beispiel des Teledienstedatenschutzgesetzes (TDDSG).

1.17 Entwicklungen in der Informationsgesellschaft

Im Dezember 2003 kam die internationale Staatengemeinschaft erstmals im Rahmen eines Weltgipfels der Vereinten Nationen zusammen, um Fragen der globalen Informationsgesellschaft zu erörtern. In diesem Zusammenhang hat die Bundesregierung den Deutschen Bundestag mit einem „Aktionsprogramm Informationsgesellschaft Deutschland 2006” über Stand und Perspektiven unterrichtet. Dem Bericht zufolge soll der Anteil der Internetnutzerinnen und -nutzer an der Bevölkerung ab 14 Jahren bis 2005 auf 75 Prozent steigen. Der Bericht enthält eine Vielzahl von interessanten Entwicklungen, zum Teil vergleichend in Diagrammen

dargestellt und gibt am Ende eine Übersicht über die verschiedenen auf Bundesebene laufenden IT-Projekte (BT-Drs. 510/2315 vom 23.12.2003). Leider kommt der Datenschutz in dem Bericht entschieden zu kurz. Es wurde wieder einmal nicht erkannt, dass nicht nur Datensicherheit, sondern gerade auch der Datenschutz ein wichtiger Faktor für die Akzeptanz neuer Datenverarbeitungssysteme ist.

1.18 Schutz der Intimsphäre

Es treten immer wieder Fälle auf, in denen in Hotelzimmern, Toiletten, Dusch- und Umkleidekabinen oder gar im Badezimmer einer gemieteten Wohnung mit einer an einem versteckten Ort installierten Linse (Kamera) elektronisch beobachtet oder aufgezeichnet wird. Es kommt auch vor, dass heimlich in fremde Wohnungen oder andere gegen Einblick geschützte Bereiche hinein gefilmt oder fotografiert wird. Es ist unstreitig, dass die so traktierten Personen dagegen unzureichend geschützt sind.

Gegenwärtig besteht eine strafrechtliche Lücke im Bereich der Verletzung des höchstpersönlichen Lebens- und Geheimbereichs durch Bildaufnahmen. Während die Verletzung der Vertraulichkeit des Wortes (§ 201 Strafgesetzbuch [StGB]), die Verletzung des Briefgeheimnisses (§ 202 StGB), das unbefugte Ausspähen von Daten (§ 202 a StGB) oder die Verletzung von Privatgeheimnissen (§ 203 StGB) strafbar sind, ist der Schutz der Intimsphäre vor unbefugten Bildaufnahmen nicht ausreichend strafrechtlich geschützt. Der Bundesrat hat daher am 26. September 2003 einen Gesetzesentwurf „zum verbesserten Schutz der Intimsphäre“ verabschiedet und beschlossen, diesen beim Deutschen Bundestag einzubringen (BR-Drs. 164/03). Diese Gesetzesinitiative ist zu begrüßen. Der Gesetzentwurf stellt dabei nur den höchstpersönlichen Lebensbereich in Wohnungen und geschützten Räumen unter einen besonderen strafrechtlichen Schutz.

Derzeit häufen sich die Klagen von Personen über mittels Multimedia-Handys mit eingebauter Kamera im öffentlichen Raum gemachte Bilder, die unbemerkt aufgenommen und weitergeleitet werden, ohne dass die Bürger dies unmittelbar wahrnehmen. Die so belästigten Personen würden wegen des von der Gesetzesinitiative gezogenen Schutzbereichs nicht daran teilhaben. Sie sind weiterhin auf den Schutz durch die Vorschriften des Kunsturhebergesetzes (Recht am eigenen Bild) angewiesen.

1.19 Ausweisdokumente und Biometrie

Es ist beschlossene Sache, dass auch die Personalausweise und Pässe der Bundesbürger mit einem Chip ausgestattet werden, auf dem biometrische Merkmale gespeichert werden sollen. Der Druck auf die EU wächst, insbesondere, weil die USA angekündigt haben, auch allen Europäern bei der Einreise Fingerabdrücke abzunehmen, wenn nicht bis Ende 2004 die Einreisedokumente eindeutig überprüfbare biometrische Merkmale enthalten. Bei der EU-Kommission und bei den G-8-Staaten wird über gemeinsame Lösungen beraten. Derzeit ist nicht abzusehen, ob noch im Jahr 2004 eine Entscheidung getroffen wird.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat schon im März 2002 (vgl. 25. JB, Ziff. 15.1) hierzu eine Entschließung gefasst und darauf hingewiesen, dass die biometrischen Merkmale nur auf dem Chip im Ausweis und nicht in zentralen Datenbanken (Referenzdateien) hinterlegt werden sollen, damit der Bürger selbst die Verwendung seiner biometrischen Merkmale in den Händen behält. Gleiches gilt, denke ich, für die Auswahl zwischen den verschiedenen möglichen biometrischen Merkmalen (genauer vgl. 25. JB, Ziff. 3.3), die zur Verfügung stehen. Neben der Sicherheit muss ein zentrales Kriterium sein, dass der Bürger nur bewusst dieses Merkmal einem Prüfcomputer zur Verfügung stellt. Deshalb hielte ich einen Gesichtsscanner, der auch im Vorbeigehen unbemerkt per Gesichtserkennung einen Abgleich vornehmen kann, aus Sicht des Datenschutzes für nicht wünschenswert.

1.20 Auf dem Weg zum gläsernen Steuerbürger

Hatte die Gesetzgebung der letzten Jahre die Steuerflüchtlinge und die organisierte Kriminalität ins Auge gefasst, erinnert sei an das Gesetz zur Bekämpfung der Geldwäsche, das u. a. beim Bundeskriminalamt eine „Zentralstelle für Ver-

dachtsanzeigen“ geschaffen hat, das vierte Finanzmarktförderungsgesetz, das der Bundesanstalt für Finanzdienstleistungsaufsicht einen automatisierten Abruf von Kontoinformationen ermöglicht und eine Regelung zum so genannten Konto-Screening enthält, so hat die jetzige Gesetzgebung den normalen Steuerbürger im Visier. Erkennbar wird, dass über die Kontrollmitteilungen der Banken an die Finanzbehörden hinaus der Steuerstaat sich immer stärker hin zu einer vorbeugenden Überwachung entwickelt. Vorsorgliche Ausforschung tritt an die Stelle anlassbezogener Ermittlungen und die Erhebung von Daten beim Betroffenen selbst. Die klassische Lohnsteuerkarte soll fortfallen, an ihre Stelle tritt die unmittelbare Übermittlung des Einkommens und der Steuerdaten durch den Arbeitgeber an das Finanzamt. Verbunden sind diese Änderungen mit der Einführung einer eindeutigen lebenslang geltenden Identifikationsnummer für Privatpersonen beziehungsweise eine Wirtschaftsidentifikationsnummer für wirtschaftlich arbeitende Betriebe und Personen, die vom Bundesamt für Finanzen vergeben wird.

Die datenschutzrechtlichen und tatsächlichen Auswirkungen der Einführung dieses Identifikationsmerkmals sind nicht einmal ansatzweise abzuschätzen, die Zweckbindung dieses Merkmals wird kaum sicherzustellen sein, die Verwendung wird erodieren (vgl. Ziff. 13.1 f. dieses Berichts). Die mit dem Steueränderungsgesetz 2003 vorgesehene Regelung sieht vor, unter einer „Electronic Taxpayer Identification Number“ personenbezogene Daten der Meldeämter und Daten zu sämtlichen Steuerbereichen bundesweit zu speichern. Hinzutreten soll die Verpflichtung aller Kreditinstitute, alle Zinseinkünfte von Bürgern und Betrieben elektronisch an das Bundesamt für Finanzen zu melden. Damit ist der Grundstein für den Beginn einer lückenlosen Kontrolle der Steuerzahler gelegt. Da diese Entwicklung auf bundesgesetzlichen Ermächtigungen beruht, ist der Einfluss, den der einzelne Landesdatenschutzbeauftragte nehmen kann, begrenzt.

1.21 Erweiterung der Überwachung von Telekommunikationsverkehr und der Internetnutzung

Die Zahl der Telefonüberwachungen steigt seit Jahren ständig an. So haben die Telekommunikationsunternehmen der Regulierungsbehörde für Telekommunikation und Post für das Jahr 2001 19.896 Anordnungen und für das Jahr 2002 21.874 Anordnungen gemeldet, also ein deutlicher Anstieg binnen eines Jahres um über zehn Prozent. Die Zahl der Anordnungen steigt von Jahr zu Jahr beachtlich und hat sich seit 1995 bereits verfünffacht. Eine nachvollziehbare befriedigende Erklärung gibt es hierfür nach wie vor nicht. Auch das beim Max-Planck-Institut in Auftrag gegebene und von der Universität Münster durchgeführte Forschungsprojekt gibt hierzu keine hinreichenden Antworten. Die Datenschutzbeauftragten des Bundes und der Länder haben die Ergebnisse zum Anlass genommen und dem Gesetzgeber Vorschläge zur Verbesserung des Datenschutzes unterbreitet (vgl. Ziff. 18.14 dieses Berichts).

Über den Umfang, in dem der IMSI-Catcher (International Mobile Subscriber Identity) von Polizei und Geheimdiensten eingesetzt wird, gibt es keine publizierten Zahlen. Gleichwohl bedürfte auch der Einsatz dieses Instruments politischer Kontrolle. Der IMSI-Catcher simuliert eine Basisstation eines Mobilfunknetzes, bei der sich Handys in einem bestimmten Umkreis aus technischen Gründen anmelden. Durch den Einsatz des Gerätes können aber nicht nur die Karten- und Gerätedaten eines konkret gesuchten Handys zur Identifizierung des Anschlussinhabers genutzt werden, sondern auch alle anderen aktiven Mobiltelefone in seinem räumlichen Umfeld werden erfasst. Die Datenschutzbedenken bestehen darin, dass in die Überwachung mit dem IMSI-Catcher wegen der Umfelderfassung zwangsläufig eine Vielzahl unverdächtiger Personen einbezogen werden. Darüber hinaus sind die in § 100 i Strafprozessordnung (StPO) genannten Anordnungsvoraussetzungen zu weit gefasst.

In eine ähnliche Richtung geht der Einsatz der so genannten stillen SMS. Dabei kann ein bestimmtes Handy gezielt angesprochen werden, ohne dass der Handybesitzer Kenntnis davon erlangt. Beim Handy-Provider werden daraufhin Nutzungsdaten erzeugt, die problemlos zur Standortbestimmung des Handys genutzt werden können. Weiterhin besteht die Möglichkeit, die Anfrage bei vorübergehend nicht erreichbaren Mobiltelefonen in eine Warteschleife zu stellen, so dass diese sofort, nachdem sie eingeschaltet wurden, antworten. Die genaue Wir-

kungsweise und die damit verbundenen Datenspeicherungen sind noch mit den Providern zu klären, Gleiches gilt für die rechtlichen Rahmenbedingungen.

Auch die Initiative des Bundesministeriums für Wirtschaft und Technologie, im Telekommunikationsgesetz (TKG) die Anbieter von Telekommunikationsdienstleistungen zu verpflichten, vor Herausgabe von Prepaid-Cards die Kundendaten zu erheben, und zwar unabhängig davon, ob sie die Daten für die Vertragsabwicklung benötigen, zielt darauf ab, die Bürger zu deanonymisieren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist mit einer Entschließung (vgl. 25. JB, Ziff. 15.5) diesem Gesetzesvorhaben entgegengetreten.

In die Reihe technischer Unzulänglichkeiten hingegen gehört das Telefonieren im Internet. Hintergrund ist, dass beim Transport von Datenpaketen zeitliche Verzögerungen eintreten können und dadurch keine unterbrechungsfreie Kommunikation zustande käme. Deshalb wurde für Internet-Telefonie, die so genannte Voice over IP, ein „Real Time Transport Protocol (RTP)" entwickelt, das aber ein unsicheres Datentransportprotokoll nutzt, so dass Gespräche mit einfachen technischen Mitteln mitgehört werden können. Hier sind neue, sicherere technische Lösungen gefordert.

Während sich in den vergangenen Jahren die Bemühungen der Sicherheitsbehörden auf den Zugriff der bei den Anbietern von Telekommunikations- und Internetdienstleistungen bereits gespeicherten Daten konzentrierten, richten sich nunmehr die Bestrebungen der Politik, angetrieben durch die Sicherheitsbehörden, darauf, die Anbieter dazu zu verpflichten, insbesondere Bestands-, Verbindungs- und Nutzungsdaten ihrer Kunden „vorbeugend" für einen längeren Zeitraum für Zwecke der Strafverfolgung und der Nachrichtendienste zu speichern. Diese Speicherung soll unabhängig davon erfolgen, ob die Anbieter diese Daten selbst für die Abrechnung in Anspruch genommener Dienstleistungen mit ihren Kunden benötigen. Derartige Vorschläge stellen den Grundrechtsschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnisses prinzipiell in Frage. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in mehreren Entschließungen auf die Gefahren hingewiesen, die mit einer derartigen Entwicklung verbunden wären (vgl. Ziffern 18.6, 18.13 und 18.14 dieses Berichts).

Im Bereich der Telekommunikationsüberwachung bis hin zur Erstellung von Bewegungsbildern sind die Aktivitäten, Eingriffe in die Rechte der Bürger vorzubereiten, besonders stark ausgeprägt. Ständig werden neue Initiativen gestartet; dies macht auch die Vielzahl der Entschließungen deutlich, die die Konferenz der Datenschutzbeauftragten des Bundes und der Länder allein in den letzten zwei Jahren verabschiedet haben. Es ist Aufgabe aller demokratischen Kräfte, darüber zu wachen, dass das grundrechtlich garantierte Fernmeldegeheimnis nicht Stück für Stück ausgehöhlt wird und sich in Deutschland schleichend und fast unbemerkt eine Überwachungskultur entwickelt, deren tatsächliche Notwendigkeit und Effizienz nicht nachweisbar ist. Dies gilt auch im Hinblick auf die in den Koalitionsverhandlungen in Bremen getroffene Vereinbarung, die Telefonüberwachung zu präventiven Zwecken zuzulassen.

1.22 Keine Sicherheit im Haifischbecken Internet

So geht es vielen Internetsurfern: Das Netz spült ihnen Viren, Bugs und Würmer auf den Rechner, Programme installieren sich selbst und verändern den Rechner, Spyware und andere Programme saugen Daten vom Rechner an unbekannte Orte.

Einige empfinden die Unsicherheit der digitalen Medien, insbesondere des Internets, gerade als deren ungeheuren Reiz. Der Rechner nimmt insofern nur an ständigen Veränderungen teil. Während man mit dem Rechner arbeitet, holt er sich selbstständig etwas aus dem Netz und verändert sich, man partizipiert sozusagen an den ständigen Wandlungen im Netz. Dadurch entsteht für sie die besondere Faszination an dem Medium.

Andere hingegen wollen ein verlässliches Medium, sie wollen sich nicht fremdbestimmt mit ständigen Änderungen auseinander setzen. Vielleicht benötigen sie die Leistung ihres Rechners für den Beruf, jedenfalls möchten sie selbst entscheiden, wann und was sich auf ihrem Rechner verändert.

Nun ist allenthalben klar, dass das Internet ein unsicheres Medium ist. Dafür ist es auch überhaupt nicht konzipiert. Im Gegenteil, vielen Surfern wird allmählich klar, dass sie die vielen schönen, kostenlosen Internetangebote häufig in Wahrheit mit ihren personenbezogenen Daten bezahlen müssen. Das Internet sicher zu machen, ist also ein zu großes, ja sogar unmögliches Unterfangen. Jeder ist, wie ich mit meiner Kampagne „Selbstverteidigung im Internet“ im letzten Jahr deutlich gemacht habe, zunächst einmal selbst aufgefordert, für seine Rechnersicherheit zu sorgen und die jeweilige Defence-Software zu installieren und dann auch zu aktualisieren.

Darüber hinaus hält das Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Plattform bereit, auf der weitere Sicherheitsinformationen zur Verfügung stehen. Auch große Industrieunternehmen haben bereits vor einigen Jahren einen eigenen Arbeitskreis zur Internetsicherheit (Arbeitskreis Schutz von Infrastrukturen/Aksis) gegründet. In ähnliche Richtung geht eine von der Bundesregierung eingesetzte Arbeitsgruppe „Kritische Infrastrukturen (Kritis)“, die Abwehrstrategien für Risikoszenarien entwickelt.

Dass PC sicherer werden müssen, darüber sind sich ausnahmsweise einmal alle Experten einig. Sobald es aber um das konkrete „Wie“ geht, scheiden sich die Geister. Führende Hard- und Softwarehersteller versuchen, mit Palladium und TCPA (Trusted Computing Platform Alliance) den PC zu „versiegeln“. Sie haben sich in einem Firmenkonsortium zusammengeschlossen, um eine neue, sicherere Hardwareplattform für PC und andere vernetzte Geräte zu schaffen. Deren Kernstück ist das „Trusted Platform Module (TMP)“, in dem sich ein eigener Prozessor und ein gesicherter Speicher befinden. In dem TPM werden Prüfsummen von BIOS, Bootsektor und anderen Hardwarekomponenten gespeichert, um ein sicheres Betriebssystem zu booten. Dieses identifiziert den Rechner über den TPM bei einem Server oder Diensteanbieter im Internet. Und hier setzen nun die Forderungen der Datenschutzbeauftragten an: Wäre der TPM nicht ein fest installierter Chip, dessen Funktionen für den Benutzer nicht klar erkennbar sind, insbesondere nicht, ob er Informationen über das Netz an die Hersteller weitergibt, sondern könnte der Benutzer frei darüber entscheiden, wann er mit dem Chip die Sicherheit aktiviert und nutzt und wann nicht, wäre sicherlich vielen wohler (zu den Gefahren vgl. Ziff. 18.2, zu automatischen Software-Updates Ziff. 18.11 dieses Berichts).

Vielen Anwendern, die Sicherheit haben wollen und die erwarten, dass ihre persönlichen und personenbezogenen Daten nur für bestimmte Zwecke genutzt werden, vertraulich bleiben und nicht unautorisiert verändert werden können, fehlt das notwendige Wissen, um beurteilen zu können, ob die eingesetzten Systeme vertrauenswürdig sind. Auf Marketingaussagen und Versicherungen der Softwarehersteller möchte sich niemand wirklich abschließend verlassen. Auch ist für den Verbraucher nicht zu erkennen, ob ein Datenverarbeitungssystem nur das Allernötigste für den Datenschutz tut, ob Lücken vorhanden sind oder ob ein hoher Datenschutzstandard implementiert ist. Und gerade hier setzt der Gedanke der Auditierung an (vgl. auch Ziffern 3.4 und 18.3 dieses Berichts). Ein von Sachverständigen untersuchtes System wird nach festgelegten Datenschutzkriterien bewertet und erhält, wenn es alle Datenschutzanforderungen erfüllt, ein Gütesiegel verliehen.

1.23 Weitere Folgen der Anschläge vom 11. September 2001

Dass die Folgen des 11. September 2001 noch lange wirken würden, habe ich bereits in meinem 24. Jahresbericht (dort Ziff. 1.1) prognostiziert. Dabei meinte ich nicht die kriegerischen Aktionen in Afghanistan oder im Irak, sondern die tiefen Eingriffe in das informationelle Selbstbestimmungsrecht. In einer ersten Reaktion wurden in der Bundesrepublik, insbesondere den Nachrichtendiensten im Terrorismusbekämpfungsgesetz vom 9. Januar 2002, weiterreichende zusätzliche Befugnisse eingeräumt.

Eine weitere tiefgreifende Maßnahme war die jetzt abgeschlossene Rasterfahndung, in die Datensätze von mehreren hunderttausend Bürgern einflossen; ein damit verbundener Fahndungserfolg wurde bisher nicht publik.

Die Einführung von biometrischen Merkmalen in Visa bei der Einreise in die Bundesrepublik ist in 2003 vollzogen, am 28. November 2003 haben sich die In-

nen- und Justizminister/-innen der EU in Brüssel über die Einführung biometrischer Merkmale in Visa und Aufenthaltstiteln für Drittstaatenangehörige geeinigt. Die geplante Einführung von biometrischen Merkmalen in Pass und Personalausweis gegen die eigene Bevölkerung werden folgen. Einreisende in die USA aus Nicht-EU-Ländern dürfen sich jetzt schon wie Schwerkriminelle fühlen, müssen sie doch seit Anfang des Jahres ihre Fingerabdrücke nehmen lassen. Darüber hinaus wird weltweit ein kostenintensiver Kontroll- und Überwachungsapparat zur maritimen und zur Luftsicherheit aufgebaut (vgl. Ziffern 12.1 und 12.2 dieses Berichts).

Im „Kampf gegen die Achse des Bösen" versuchte die US-Bundesregierung auch bei den Flugdaten, unter Hintanstellung europäischen und nationalen Rechts eine Vorrangstellung zu erzwingen. Den Rahmen hierfür bilden folgende Zahlen: Allein rund 100.000 Menschen arbeiten für die CIA (Central Intelligence Agency), weitere US-Geheimdienste sind die NSA (National Security Agency), die die weltweiten Abhörtätigkeiten steuern, die NRO (National Reconnaissance Office), die sich mit der Auswertung von Satellitenbildern befasst, die DIA (Defence Intelligence Agency), die Spionageabteilung der Armee sowie Teile des FBI (Federal Bureau of Investigation) und Abteilungen des Außen-, Energie- und des Finanzministeriums. Mehr als 170.000 Menschen sollen in Zukunft dem Department of Homeland Security (DHS) dienen, einem Superministerium, das nur die Aufgabe hat, die Vereinigten Staaten vor terroristischen Angriffen zu schützen. Sicherheitsspezialisten aus 22 US-Behörden haben in den vier Hauptabteilungen des DHS künftig ein neues Aufgabenfeld.

Und nun greift das von den USA neu gegründete DHS auf europäische Flugreservierungssysteme zu. Darin können in weit mehr als einhundert Datenfeldern besondere Daten zu jedem einzelnen Fluggast gespeichert werden (vgl. Ziff. 17.3 dieses Berichts). Die USA dürfen sich derzeit uneingeschränkt bedienen. Hier sind nicht nur die Flüge in die USA, sondern auch alle anderen, z. B. innereuropäischen Flüge gespeichert. Die USA interessieren sich dabei nicht nur für die Identität der einzelnen Flugpassagiere, sondern auch, z. B., wer neben wem im Flugzeug gesessen hat und mit welchen Kreditkarten und -nummern bezahlt wurde. Die Anträge der DHS, auf Banken- und Kreditkartensysteme in den USA Zugriff nehmen zu können, sollen schon gestellt sein. Das Szenario wird deutlicher, wenn man die Leistungsfähigkeit modernster Data-Mining-Produkte hinzu denkt. Diese Software kann in beliebig vielen Schichten in hoch komplexen Informationssystemen Daten auffinden und korrelieren.

Hat das DHS den Zugriff auf Banken- und die Kreditkartensysteme, kann man in den USA, wo fast ausschließlich bargeldlos bezahlt wird, jederzeit feststellen, z. B. wann und wo der Fluggast einen Hamburger gegessen oder ein Hotel bezahlt hat. Und bei manchen Kreditkartensystemen wird sich das sicherlich nicht nur auf die USA beschränken. Damit wird deutlich: Das ganze System verdächtigt prinzipiell alle und stellt damit einen Ansatz dar, der in krassem Widerspruch zum europäischen Datenschutzgedanken steht, der sich in der Europäischen Datenschutzrichtlinie manifestiert. Viele der grundlegenden Prinzipien, wie die Erforderlichkeit, die Zweckbindung, die vorrangige Erhebung der Daten beim Betroffenen etc. werden außer Kraft gesetzt. Es besteht damit die Gefahr, dass unter der Vorgabe, Demokratie und Freiheit zu schützen, diese Werte gefährdet werden.

1.24 Die neue elektronische Gesundheit (eGesundheit)

Einen weiteren Schwerpunkt meiner Beratungen stellte in den letzten Jahren und stellt auch in der Zukunft die Gesundheitsreform dar. Der Umbau des Gesundheitssystems bringt radikale Einschnitte mit sich, die mehr Kontrolle der Leistungen und Kosten beinhalten und daher auf völlig neue Datenbasen gestellt werden sollen (vgl. Ziff. 8.8.3 dieses Berichts). Damit einher geht die zunehmende elektronische Erfassung und Übermittlung von Gesundheits- und Abrechnungsdaten, die u. a. eine verbesserte Datenbasis für die Behandlung bringen sollen (Lipobay-Skandal), die Leistungsabwicklung transparenter und kontrollierbarer machen sowie die Kostenkontrolle vereinfachen soll. Dabei bedient man sich umfassender elektronischer Datenverarbeitung in der Hoffnung, die Verwaltungs- und Abrechnungsabläufe zu effektivieren. Da an allen Ecken des Gesundheitssystems zugleich verändert wird, ist im Moment schwer einzuschätzen, welche DV-Verfahren sich durchsetzen oder Bestand haben werden. Hinzu kommt, dass viele neue

Projekte mit unterschiedlichsten Ansätzen zur Datenverarbeitung entwickelt werden, wobei teilweise Pilotprojekte nicht einmal zu Ende geführt sind, geschweige denn deren Ergebnisse evaluiert sind, da werden sie schon bundesweit eingeführt. Neue chipkartenbasierte Projekte, die mit Piloten in verschiedenen Teilen Deutschlands durchgeführt werden, treten hinzu. Da ist es angesichts der geringen personellen Kapazitäten bei den Datenschutzbeauftragten kaum mehr leistbar, eine solide Datenschutzberatung durchzuführen. Gelegentlich könnte auch der Eindruck entstehen, dieser Rat werde gar nicht verlangt. Während die gesetzlichen Krankenkassen mit erheblichem finanziellen und technischen Aufwand versuchen, das Gesundheitssystem grundlegend zu verändern, ist bei den privaten Krankenversicherungen eher eine gewisse Zurückhaltung festzustellen. Die Hoffnung, mit großen Datenmengen und komplexen Datenverarbeitungssystemen zum Erfolg zu gelangen, hat sich schon in anderen Bereichen als Holzweg erwiesen. Je mehr Beraterverträge man vergibt, desto mehr Ratschläge hat man im nachhinein zu koordinieren. Im Moment scheint nicht hektischer Aktionismus gefragt, sondern ein wenig Besinnung auf das Wesentliche.

1.25 Mikrochips zum Aufbügeln

Warenhersteller und Handel setzen zunehmend weltweit Radio-frequenz-gestützte Mikrochips (RFID-tags) zur Kennzeichnung von Warenbeständen wie auch zur Preisauszeichnung ein. Diese im Mikrobereich weniger als Millimeter großen Chips sollen als „schlaue Etiketten" den bisherigen Strichcode (Barcode) ersetzen. Darüber hinaus sind Verfahren angedacht, die Verfolgung von Gegenständen mit den RFID-tags zu ermöglichen. Die RFID-tags sind miniaturisierte IT-Systeme, die über eine Antenne Funksignale empfangen oder abgeben können. Die dafür erforderliche elektrische Energie wird über das Funksignal eines RFID-Lesegerätes bereit gestellt, so dass das RFID-tag ohne eigene Energiequelle funktionieren kann. Die Entfernung, auf die diese RFID-tags angesprochen werden können, kann im Zentimeterbereich liegen, es gibt aber auch Reichweiten bis zu 30 Metern. Die RFID-Technologie wird sich aufgrund geringer Herstellungskosten in naher Zukunft weltweit ausbreiten. Der Anwendungsbereich liegt bei der Kennzeichnung von Waren, der Markierung von Gegenständen, um sie auf diese Weise vor Diebstahl zu sichern, bis hin zur Verfolgung von Gegenständen in der Produktion und im Vertrieb. Damit könnte das verloren gegangene Hemd in der Reinigung bald der Vergangenheit angehören, ein im Kragen mit eingewebtes RFID-tag könnte jederzeit darüber Auskunft geben, wo sich das Hemd gerade befindet. Die Europäische Zentralbank hat zudem bereits angekündigt, Eurobanknoten mit entsprechenden Mikrochips auszustatten.

Die neue Technologie ist Teil der globalen Entwicklung hin zu einer „intelligenten Umgebung" und zur allgegenwärtigen Datenverarbeitung. Diese Entwicklung fordert aber auch neue Antworten durch den Datenschutz. Hierauf hat die Internationale Konferenz der Datenschutzbeauftragten in einer Entschließung hingewiesen (vgl. Ziff. 19.2 dieses Berichts).

Bei einer weiten Verbreitung der RFID-tags ist auch daran gedacht, das diese untereinander kommunizieren können. Auf diese Weise könnte eine neue Dimension von Bewegungsprofilen entstehen. Um bei dem vorgenannten Beispiel zu bleiben: Genauso wie der Weg des Hemdes in der Reinigung verfolgbar ist, wäre auch der Weg des Trägers eines solchen Hemdes verfolgbar. Würde darüber hinaus noch der Käufer bei Zahlung mit Kreditkarte festgehalten, wäre die Personenbeziehbarkeit hergestellt. Sollten die Banknoten, wie angekündigt, mit entsprechenden RFID-tags ausgestattet werden, würde damit auch das Geld seine Anonymität verlieren, würde bei der Auszahlung am Geldautomaten festgehalten, an wen ein bestimmter Geldschein ausgegeben wurde, ließe sich auch der Weg des Geldes weiter verfolgen. Wichtig wird also sein, sicher zu stellen, dass der Eigentümer selbst darüber entscheiden kann, ob bzw. in welchem Umfang Funktionen eines RFID-tags aktiviert sind.

2. Telekommunikation

2.1 Neue Telekommunikationsanlage für Bremen

Für die bremische Verwaltung soll im Jahr 2004 mit der Installation einer neuen TK-Anlage begonnen werden. Dazu wurde frühzeitig vom Referat 36 des Senators

für Finanzen (SfF) eine dienststellenübergreifende „Arbeitsgruppe Telekommunikation" („ATK") einberufen, um die Anforderungen an die neu zu beschaffende TK-Anlage zu definieren. Von Anfang an war neben dem Gesamtpersonalrat (GPR) auch meine Dienststelle an der Arbeit in dieser Arbeitsgruppe beteiligt.

Moderne Telefonanlagen bieten neben den vielen verschiedenen Möglichkeiten der Kommunikationsunterstützung auch zahlreiche Möglichkeiten, die über sie transportierten Kommunikationsflüsse zu steuern und auch auszuwerten. Die Auswertungen können dabei nicht nur global geführt werden, sondern bis herunter auf einzelne Arbeitsplätze und somit auch auf einzelne Mitarbeiter. Aufgrund dieser komplexen Auswertungs- und Kontrollmöglichkeiten ist es wichtig, die datenschutzrechtlichen Anforderungen zu beachten. Während für Personen, die telefonisch in Kontakt mit der Bremer Verwaltung treten, vornehmlich die Bestimmungen des Telekommunikationsgesetzes einschlägig sind, sind bezüglich der Arbeitnehmer in der Bremer Verwaltung auch für den Arbeitnehmerdatenschutz relevante Regelungen zu beachten. Innerhalb der Bremer Verwaltung gilt derzeit die mit dem GPR abgestimmte "Dienstvereinbarung über den Betrieb und die Nutzung von Telekommunikationsanlagen (Fernsprechanlagen)" vom 7. Juni 1991, die die Belange der Telefonie in der öffentlichen Verwaltung in Bremen regelt. Zuständig für den Bereich der Sprachtelefonie ist der Senator für Finanzen, Referat 36. Es besteht unter den Beteiligten Einigkeit, dass die bestehende Dienstvereinbarung nicht mehr den modernen Anforderungen an ein Regelwerk für Sprachtelefonie genügt und sie zu überarbeiten ist. In ersten informellen Gesprächen, denen ein von der Arbeitsgruppe „ATK" in Zusammenarbeit mit externen Dienstleistern erarbeiteter Anforderungskatalog an die zukünftige TK-Anlage zugrunde lag, habe ich bereits den SfF über die Anforderungen, z. B. an ein verwaltungsweites elektronisches Telefonbuch, an die Protokollierung von dienstlichen und privaten Telefonaten zu Abrechnungszwecken und die damit verbundene notwendige Anpassung der bestehenden Dienstvereinbarung informiert. Die wesentlichen Entwicklungen werden aber erst 2004 anstehen.

2.2 Gefahren von Funknetzen

Die 1996 von Bob Allen (damals CEO von AT&T) geäußerte Vision „Anytime, Anywhere" zu kommunizieren und Zugriff auf benötigte Informationen zu erhalten, ist mittlerweile Realität geworden. Die mobilen Kommunikationsmöglichkeiten gehen dabei weit über das simple Telefonieren hinaus. Mobiles E-Mailing und andere komplexe Dienste sind problemlos nutzbar geworden.

Notwendige Basis für alle mobilen Dienste ist eine Vernetzung der mobilen Kommunikationsgeräte. Dafür existieren neben den Mobilfunknetzen zunehmend andere Technologien. Für die Kommunikation über kurze Distanzen mit Peripheriegeräten, z. B. Bluetooth, und für die drahtlose Vernetzung von Computern untereinander die WLAN-Technik. Gerade die WLAN-Technik wird sehr gern genutzt, wenn es darum geht, „mal eben schnell" Rechner zu verbinden, um Daten auszutauschen, oder kostengünstig neue DV-Arbeitsplätze in alten Gebäuden zu schaffen, in denen keine ausreichende Verkabelung vorhanden ist. Denkmalschützer sind froh über solche Technik, aber aus Sicht des Datenschutzes bereitet sie doch einige Kopfschmerzen. Denn gerade die einfache und flexible Möglichkeit einer schnellen Verbindung von mehreren Rechnern bringt auch viele Gefahren für die in den Rechnern gespeicherten und zwischen diesen Computern übertragenen Daten mit sich. So sind Funknetze räumlich nicht auf Gebäude begrenzt, sie sind ein offenes Medium. Außerhalb von Gebäuden, in denen Funknetze installiert werden, sind deren Funkwolken zu orten und die übertragenen Daten aufzufangen. Wenn nicht entsprechende Vorkehrungen getroffen werden, kann man sich darüber hinaus nicht sicher sein, dass nur autorisierte Teilnehmer im Funknetz sind und somit Zugriff auf die entsprechenden Daten und Anwendungen haben. Diese Gefahren werden oft bei Funknetz-Installationen vernachlässigt. Oft wird auch vergessen, dass durch eine unbedachte Anbindung von Rechnern via Funk an bestehende, drahtgebundene Unternehmensnetzwerke schwach oder gar nicht gesicherte Hintertüren in eben diesen Unternehmensnetzwerken geöffnet werden: Die Absicherung der Netzwerke gegen das Internet wird gelegentlich, z. B. mittels teurer Firewall-Lösungen, realisiert, aber das Funknetz ist „offen wie ein Scheunentor".

Ich arbeite im Rahmen des „Arbeitskreises Technik" an einer Orientierungshilfe „Datenschutz in drahtlosen Netzen" mit, die Mitte 2004 veröffentlicht werden soll.

Neben der Beschreibung allgemeiner Gefahren von Funknetzen soll darin auf die Themen WLAN, Bluetooth, Infrarot-Kommunikation, Funkmäuse und Funktastaturen sowie Personal Digital Assistant (PDA) eingegangen werden.

2.3 Orientierungshilfe Kryptografie

Das Bundesdatenschutzgesetz (BDSG) und auch alle Landesdatenschutzgesetze schreiben verschiedene technische und organisatorische Maßnahmen vor, die von den verantwortlichen Stellen zu treffen sind. Im Bremischen Datenschutzgesetz (BremDSG) sind diese Regelungen in § 7 „Datenvermeidung, Vorabkontrolle, technische und organisatorische Maßnahmen" festgeschrieben. Neben anderen Punkten wird hier die Kontrolle des Zugriffs (Zugriffskontrolle, BremDSG § 7 Satz 4 Nr. 3) und der Weitergabe (Weitergabekontrolle, BremDSG § 7 Satz 4 Nr. 4) personenbezogener Daten verlangt. Diese Anforderungen können mit dem Hilfsmittel der Kryptografie erfüllt werden. Kryptografie ist die Wissenschaft, die sich damit befasst, wie Daten vor den Augen unbefugter Dritter verborgen werden. So können mit ihrer Hilfe Daten auf Datenträgern verschlüsselt werden ebenso wie Daten, die von einem Punkt zu einem anderen übertragen werden müssen, auf der Strecke verschlüsselt werden können. Dabei sind, je nach Sensibilität der Daten, geeignete Ver- und Entschlüsselungsverfahren zu wählen, damit gewährleistet ist, dass Unbefugte keinen Zugriff auf die Daten erhalten können oder um sicherzustellen, dass Daten wirklich von einem bestimmten Absender kommen und dass sie zwischen Versand und Empfang nicht verfälscht worden sind. Da es im Bereich der Verschlüsselung sehr viele verschiedene geeignete und weniger geeignete Methoden gibt, hat der „Arbeitskreis Technik" (AK Technik) der Datenschutzbeauftragten des Bundes und der Länder eine Orientierungshilfe erarbeitet. Neben der Beschreibung der technischen Grundlagen und ihrer Bedeutungen bzw. Auswirkungen (Algorithmen, Schlüssellängen im Zusammenhang mit symmetrischen und asymmetrischen Verschlüsselungsverfahren, Angreifbarkeit der Verschlüsselung durch Wahl „schlechter" Methoden oder fehlerhaft implementierter Algorithmen, etc.) ist es notwendig, zuerst eine Kategorisierung der Daten vorzunehmen, die einer besonders gesicherten Behandlung bedürfen, also höchst sensibel sind. Es sind dies Daten über die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit, Sexualleben, Dienst- und Arbeitsverhältnisse sowie steuerliche und soziale Verhältnisse (vgl. § 3 g BDSG, § 2 b BremDSG). Damit ist der Rahmen für den höchsten Schutzbedarf abgesteckt, der den Einsatz kryptografischer Methoden erfordert. In der von den Datenschutzbeauftragten erarbeiteten Broschüre werden Grundszenarien (Zugriffskontrolle, Weitergabekontrolle) dabei ebenso diskutiert wie allgemeine Lösungsansätze, wie z. B. das Tunneln unsicherer Netze oder der Einsatz digitaler Signaturen. Zum Schluss der Orientierungshilfe wird auf in verschiedenen Szenarien auftretende IT-Sicherheitsprobleme und mögliche Lösungswege unter Anwendung kryptografischer Verfahren, sowohl bezogen auf die eingesetzten bzw. einzusetzenden Infrastrukturen (z. B. Internet, Virtual Private Networks) als auch bestimmte Anwendungsfälle eingegangen. Die Orientierungshilfe kann von meiner Internetseite unter www.datenschutz.bremen.de heruntergeladen werden.

2.4 Erhebliche datenschutzrechtliche Defizite bei der Novellierung des Telekommunikationsgesetzes

Am 15. Oktober 2003 wurde von der Bundesregierung ein Entwurf für ein neues Telekommunikationsgesetz (TKG) beschlossen. Dieser Entwurf beinhaltet wesentliche Verschlechterungen für den Datenschutz:

Der Gesetzesentwurf berechtigt die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (Angaben, die beim Aufbau und bei der Abwicklung von Telekommunikationsverbindungen anfallen, also etwa eine angerufene Telefonnummer oder den Zeitpunkt des Anrufs) ungekürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern, wobei auch alle Zielrufnummern enthalten sind. Der Innenausschuss des Bundesrates geht noch einen Schritt weiter in seinen Forderungen. Er will aus Gründen der inneren Sicherheit sogar eine zwölfmonatige Speicherungsfrist vorsehen. Ich habe zu diesen Bestrebungen schon in meiner Pressemitteilung vom 21. November 2003 erklärt: "Das Recht, mit seiner Umwelt unbeobachtet und frei zu kommunizieren, gehört zu den entschei-

denden Grundrechten in der Informationsgesellschaft. Eine umfassende Speicherung von Verkehrsdaten auf Vorrat ist damit unvereinbar".

Weiterhin sollen sich in Zukunft die Käufer auch beim Erwerb eines vertragslosen Prepaid-Handys ausweisen und registrieren lassen. Schon seit längerem kritisieren die Datenschutzbeauftragten eine Zwangsidentifizierung beim Erwerb von Prepaid-Handys als gesetzeswidrig. Durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 2302) sehen sich die Datenschutzbeauftragten nunmehr in dieser Auffassung bestätigt. In diesem Urteil betont das Gericht, dass eine Pflicht eines Prepaid-Anbieters, personenbezogene Kundendaten zu erheben, einen staatlichen Eingriff in das verfassungsrechtlich gewährleistete Recht der Kunden auf informationelle Selbstbestimmung darstellt, der nicht erforderlich ist.

Schließlich können nach der Novellierung des TKG die Strafverfolgungsbehörden und die Nachrichtendienste bei der Verfolgung jedweder Strafdaten ohne richterliche Anordnung von den Diensteanbietern Passwörter und Geheimzahlen anfordern, mit denen die Inhalte oder näheren Umstände einer Telekommunikation geschützt werden.

Aufgrund der erheblichen verfassungsrechtlichen Bedenken hinsichtlich dieser gesetzgeberischen Vorhaben hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Frühjahr die Entschließung „Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation" (Ziff. 18.8 dieses Berichts) und im Herbst die Entschließung „Gravierende Verschlechterung des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes" (Ziff. 18.14 dieses Berichts) gefasst. Hierin habe ich mit den anderen Datenschutzbeauftragten gefordert, die datenschutzrechtlichen Defizite zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

2.5 Wissenschaftliche Untersuchung der Telefonüberwachung

Im Mai dieses Jahres hat das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg ein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten zur „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach §§ 100 a, 100 b der Strafprozessordnung (StPO) und anderer verdeckter Ermittlungsmaßnahmen" vorgelegt. Es handelt sich bei diesem Projekt um eine Studie, die aus einer empirischen Perspektive Fragestellungen des strafprozessualen Instruments der Überwachung der Telekommunikation aufgreift. Die Untersuchung basiert auf Strafaktenanalysen, schriftlichen Befragungen und Expertengesprächen mit Polizisten, Staatsanwälten und Richtern. Da durch die Aktenanalyse aber auch in den Befragungen und Gesprächen personenbezogene Daten erhoben und verarbeitet wurden, war für das Forschungsvorhaben ein abgestimmtes Datenschutzkonzept unerlässlich. Dieses Datenschutzkonzept enthält u. a. Festlegungen zu den Fragen des Zugangs von Mitarbeitern, Mitarbeiterverpflichtungen, der Anonymisierung, der Aktenentnahme zur Bearbeitung und zu Kopierbeschränkungen.

Das Gutachten des Max-Planck-Institutes dokumentiert, dass die Zahl der Ermittlungsverfahren, in denen Telekommunikationsüberwachungen angeordnet wurden, sich in dem Zeitraum von 1996 bis 2001 um 80 % erhöht hat. Auch die Anzahl der staatsanwaltschaftlichen Eilanordnungen (welche anstelle des Richtervorbehaltes nur als absolute Ausnahme vorgesehen sind) ist deutlich angestiegen. Weiterhin werden erhebliche Defizite in der Praxis aufgezeigt. Als ein großes Manko der Telekommunikationsüberwachung wird in dem Gutachten die Umsetzung des Richtervorbehaltes im Zusammenhang mit der damit verbundenen Begründungsanforderung beschrieben. Lediglich 24 % der Beschlüsse waren substanziell begründet. Das führt zu einem Mangel an Transparenz, Nachvollziehbarkeit und Kontrolle. Aus diesem Grund wird in dem Gutachten auch eine Verbesserung der richterlichen Kontrolle gefordert. Daneben wird die Einrichtung externer Kontrollsysteme und der Ausbau der Rechtsschutzmöglichkeiten vorgeschlagen. Weiterhin wird festgestellt, dass in den wenigsten Fällen die Anschlussinhaber über die Maßnahme benachrichtigt wurden. Nach § 101 StPO sind die Beteiligten von der getroffenen Maßnahme des § 100 a StPO jedoch zu unterrichten. Zu teilweise vergleichbaren Ergebnissen kommt auch ein Forschungsprojekt der Universität Bielefeld.

Angesichts des gravierenden Eingriffes in das Telekommunikationsgeheimnis durch die Telekommunikationsüberwachung können derartige Defizite nicht einfach hingenommen werden. Die 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat die Konsequenzen aus der Untersuchung des Max-Planck-Institutes in eine Entschließung gefasst (Ziff. 18.13 dieses Berichts). Die Datenschutzbeauftragten machen darauf aufmerksam, dass die Telefonüberwachung im Ermittlungsverfahren ultima ratio bleiben muss. Ein Eingriff in das Recht auf unbeobachtete Kommunikation kann nur bei Verfolgung schwerwiegender Straftaten gerechtfertigt sein. Der gesetzliche Richtervorbehalt darf nicht gelockert werden. Vielmehr muss die Qualität der Entscheidung verbessert werden. Erhebliche Verstöße gegen das Begründungserfordernis können nicht ungeahndet bleiben, sondern müssen ein Beweisverwertungsverbot nach sich ziehen. Die Strafverfolgungsbehörden sollten durch Berichtspflichten dazu angehalten werden, ihren gesetzlich festgeschriebenen Pflichten, wie z. B. der Benachrichtigungspflicht, nachzukommen.

Weiterhin hat die 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder im März 2003 eine Entschließung zur Transparenz der Telefonüberwachung gefasst (Ziff. 18.6 dieses Berichts). Hierin hat sie die Beibehaltung der Jahresstatistik über zu Strafverfolgungszwecken durchgeführte Überwachungsmaßnahmen, die von den Betreibern der Telekommunikationsanlagen zu führen ist, gefordert. Die Jahresstatistik dient der Information der Allgemeinheit über Ausmaß und Entwicklung der Telekommunikation. Nur so kann die Transparenz der Überwachungsmaßnahmen ermöglicht werden. In dem Entwurf des Telekommunikationsgesetzes hat dieses Anliegen Berücksichtigung gefunden.

2.6 Gesetz zur Bekämpfung des Missbrauchs von 0190er-/0900er-Nummern in Kraft

Immer wieder werde ich von Bürgern mit Fragen zum Missbrauch von 0190er- und 0900er-Nummern konfrontiert. Auch der Datenschutzausschuss der 15. Legislaturperiode hat sich mit diesem Thema beschäftigt und mich aufgefordert, dieses Thema weiterhin zu verfolgen. Deshalb berichte ich an dieser Stelle über den Fortgang.

Das Gesetz gegen den Missbrauch von 0190er-/0900er-Nummern ist am 15. August 2003 in Kraft getreten (BGBl. I 2003, S. 1590 f). Durch das Gesetz soll insbesondere vor Dialern geschützt werden, die in der Vergangenheit erheblichen Missbrauch erzeugt haben. Dialer sind kleine Anwählprogramme, die einen Rechner über eine bestimmte Telefonnummer mit einem Internetserver verbinden. Das Heimtückische hieran: Viele der Dialer installieren sich unbemerkt und bauen eine Standardverbindung ins Internet auf. Dabei nutzen sie regelmäßig eine teure 0190er- oder 0900er-Nummer, was sich meist erst mit der nächsten Telefonrechnung beim Betroffenen schmerzlich bemerkbar macht. Diesem Missbrauch soll durch das neue Gesetz nun ein Riegel vorgeschoben werden: Entgelte, die für 0190er- und 0900er-Nummern erhoben werden dürfen, sind mit 30 € pro Einwahl und 2 € pro Minute begrenzt. 0190er- und 0900er-Verbindungen müssen nach spätestens einer Stunde automatisch getrennt werden (es sei denn, es wurde ausdrücklich ein längerer Zeitraum vereinbart). Außerdem dürfen Dialer nur eingesetzt werden, wenn diese vor Inbetriebnahme bei der Regulierungsbehörde für Telekommunikation und Post registriert worden sind. Die Registrierung erfolgt, wenn das Anwählprogramm bestimmte Mindestvoraussetzungen erfüllt und der Registrierungsverpflichtete schriftlich versichert, dass eine rechtswidrige Nutzung ausgeschlossen ist. Nicht registrierte oder die Mindestanforderungen nicht erfüllende Dialer dürfen nicht mehr eingesetzt werden. Die Regulierungsbehörde hat eine Datenbank zu den registrierten Dialern ins Internet gestellt, um dem Verbraucher eine Prüfungsmöglichkeit zu geben, ob der Dialer auch tatsächlich registriert ist. Ein nicht registrierter Dialer ist rechtswidrig und es erwächst damit für den Nutzer keine Zahlungspflicht. Zudem können rechtswidrig genutzte 0190er- und 0900er-Nummern von der Regulierungsbehörde entzogen und Geldbußen von bis zu 100.000 € verhängt werden.

Darüber hinaus kann man sich durch Software gegen Dialer schützen. Es besteht auch die Möglichkeit eine 0190er/0900er-Anschlusssperre bei seinem Anbieter einrichten zu lassen, bei der sämtliche dieser Rufnummern gesperrt werden.

3. Datenschutz durch Technikgestaltung und -bewertung

3.1 Restrukturierung BVN

1998 wurden per Senatsbeschluss die grundlegenden Strukturen und Aufgaben im Bremischen Verwaltungsnetz (BVN) festgelegt. In diesem Dokument ist der Grundsatz formuliert, dass keinerlei Zugriff auf die lokalen Netze der Dienststellen von außen erfolgen darf. Das BVN war aus Sicherheitsgründen bisher sternförmig aufgebaut. Die sternförmige Struktur sollte gewährleisten, dass der Anschluss an das BVN und die Nutzung der darin zur Verfügung gestellten Dienste, wie Internet oder E-Mail, für eine Dienststelle einfach und weitgehend ohne zusätzliche eigene Sicherheitsmaßnahmen erfolgen konnte. Es war nicht möglich, von außen in das BVN bzw. auf die daran angeschlossenen Hausnetze einzelner Dienststellen zuzugreifen. Auch der gegenseitige Zugriff von Dienststellen untereinander war bisher nicht möglich. Für Projekte wie Telearbeit, Fernwartung bzw. Fernadministration und einige Client-Server-Anwendungen, die auf Server bzw. Daten innerhalb des BVN zugreifen müssen, waren zusätzliche spezielle Sicherheitsregelungen erforderlich. Mit den Jahren ist aber der Bedarf an die flexible Möglichkeit des Datenaustausches gewachsen. Wesentliche Forderung der Teilnehmer am BVN war (und ist) dabei, sicher und flexibel mit anderen Teilnehmern oder mit externen Stellen direkt zu kommunizieren bzw. Daten auszutauschen.

Da das bisherige Sicherheitskonzept für das BVN diesen Anforderungen im Wege stand, bedurfte es der Erarbeitung eines neuen Sicherheitskonzeptes, das ermöglichen soll, bisher nicht mögliche Verbindungen innerhalb des BVN zu realisieren, ohne die Sicherheit des BVN selbst zu gefährden. Die datenschutz nord GmbH hat im Auftrag des Senators für Finanzen (Betreiber des BVN) ein solches Sicherheitskonzept erarbeitet.

Das Konzept sieht vor, dass innerhalb des BVN verschiedene Zonen mit unterschiedlich hohem Schutzbedarf existieren. Diese Zonen werden mit entsprechenden Grenznetzen, früher auch als DMZ („Demilitarisierte Zone") bezeichnet, ausgerüstet. In den verschiedenen Grenznetzen werden dabei jeweils die Server platziert, die Kontakt nach „außen" (bezieht sich hier auf außerhalb der Hausnetze der Dienststellen und Behörden) haben müssen. Somit werden alle Server, die Verbindungen zu BVN-Externen benötigen, in ein zu diesem Zweck konfiguriertes Grenznetz, bezeichnet als GN-E, deponiert. Server, die ausschließlich Verbindungen zu anderen BVN-Teilnehmern haben, jedoch nicht oder nicht direkt für BVN-Externe erreichbar sein sollen, werden in einem internen Grenznetz (GN-I) untergebracht. Weiterhin kann es Server geben, die in Grenznetzen der einzelnen Behörden oder Dienststellen aufgestellt werden müssen. Dies darf nur geschehen, wenn das entsprechende Netz alle Sicherheitsrichtlinien des BVN erfüllt und somit zu GN-E bzw. GN-I äquivalent gesicherte Netze, bezeichnet als GN-T_E bzw. GN-T_I, besitzt.

Die einzelnen Grenznetzbereiche werden durch Firewalls voneinander abgeschottet. Die gegenüber der jeweils vorigen Stufe realisierten Sicherheitsniveaus ergeben sich aus der nachfolgenden Tabelle:

Stufe	Sicherheitsniveau	Grenznetz
1	Niedrig	GN-E
2	Mittel	GN-I
3	Hoch	GN-T_E bzw. GN- T_I

Gewährleistet werden die Sicherheitsniveaus durch unterschiedlich komplexe Filterregelungen. Durch das vorgesehene Sicherheitskonzept erreicht der SfF als Betreiber nach dessen Umsetzung ein Verwaltungsnetz, das den Anforderungen an ein modernes Verwaltungsnetz erfüllt. Die im Sicherheitskonzept entworfene Struktur des Netzes ermöglicht es, das BVN im notwendigen Maße zu öffnen, bei maximaler Sicherheit für die Daten und Netze der angeschlossenen Dienststellen und die innerhalb des BVN zwischen verschiedenen Stellen übertragenen Daten. Das Sicherheitskonzept wurde bereits frühzeitig während seiner Entwicklung mit mir abgestimmt.

3.2 MEDIA@Komm und bremen online services

Das MEDIA@Komm-Projekt ist 2003 beendet worden. In weitgehender Zusammenarbeit der bremischen Verwaltung mit der bremen online services GmbH & Co. KG (bos KG) sind seit Projektbeginn ca. 130 Anwendungen für den Bereich des eGovernment entwickelt worden. Damit ist das Projekt zu einer Erfolgsgeschichte für den Bereich der elektronischen Verwaltung geworden, was so nicht erwartet werden konnte. Durch die Tätigkeit der bos KG ist sichergestellt, dass das Projekt auch weiterhin Früchte trägt. Der besondere Erfolg zeigt sich u. a. darin, dass sich die bos KG abermals als Sieger in einem internationalen Wettbewerb durchsetzen konnte und im Juli 2003 den „eGovernment-Award", die höchste eGovernment-Auszeichnung Europas, erhalten hat. Mit dem Preis ist zugleich die Freie Hansestadt Bremen für den Nachweis ausgezeichnet worden, dass bereits heute erhebliche Einsparungen durch effektive eGovernment-Anwendungen erzielt werden können.

Herausragende Bedeutung hat aus der Sicht des Datenschutzes, dass die von der bos GK entwickelte Software GOVERNIKUS besonders hohen Sicherheitsstandards genügt. Durch diese Middleware-Software wird der Einsatz von Signaturkarten für eine Vielzahl von Verwaltungsleistungen ermöglicht. Auch der Bund hat nun die besondere Wichtigkeit dieser Sicherheitssoftware erkannt und wird sie als Basiskomponente und Kernbestandteil für die „Virtuelle Poststelle" des Bundes einsetzen (vgl. Ziff. 3.3 dieses Berichts). Es bleibt zu hoffen, dass auch die Gründung des „Bündnisses für elektronische Signaturen" von Staat und Wirtschaft im April 2003, an der auch Bremen im Rahmen des MEDIA@Komm-Wettbewerbs beteiligt ist, dem Markt für elektronische Signaturen einen starken Schub für ihre weitere Verbreitung geben wird. Hierzu mag die Auszeichnung beitragen, die der bos KG vom europäischen Städtenetzwerk „Telecities" zum Thema „Sicherheit bei der Datenübertragung" für GOVERNIKUS verliehen wurde.

Als Landesbeauftragter für den Datenschutz werde ich die Tätigkeit von bremen online services wegen der hervorragenden Bedeutung, insbesondere für die Datensicherheit, weiterhin mit besonderer Aufmerksamkeit begleiten.

3.3 Virtuelle Poststelle

Der Senator für Finanzen hat ein Pilotprojekt gestartet, bei dem mehrere bremische Behörden mit der so genannten Virtuellen Poststelle einen neuen Kom-munikationsweg erproben werden. Über das Internet können dabei unter Verwendung einer Signaturkarte Nachrichten und eventuelle Anhänge an die Behörde verschlüsselt gesendet werden. Wichtige Kommunikations- und Sicherheitsfunktionen werden damit zentralisiert und unter Gewährleistung der erforderlichen Daten- und Rechtssicherheit wird Bürgerinnen und Bürgern sowie Unternehmen und anderen Behörden ein zusätzlicher Weg der Informationsübermittlung zur Verfügung gestellt.

Vereinfacht dargestellt ist die Virtuelle Poststelle einem Postfach vergleichbar. Der Kunde der Verwaltung lädt auf seinem PC die entsprechende Anwendung vom Webserver, füllt das Formular mit seiner Nachricht aus und sendet es anschließend signiert und verschlüsselt an das Postfach. Die Behörde wird bei Eingang einer solchen Nachricht automatisch per E-Mail benachrichtigt und kann die Nachricht sodann aus dem virtuellen Postfach abrufen. Rückantworten durch die Behörde können in entsprechender Weise über das Postfach abgewickelt werden.

Der Einsatz der Virtuellen Poststelle wird von mir wegen der damit verbundenen besonderen Datensicherheit begrüßt und unterstützt. Ihre Einführung in der bremischen Verwaltung wird daher auch von meiner Dienststelle begleitet. Am Pilotprojekt wird meine Dienststelle selbst teilnehmen.

3.4 Bremische Datenschutzauditverordnung

Das bremische Datenschutzrecht hat mit der letzten Novelle die Möglichkeit geschaffen, für öffentliche Stellen ein so genanntes Datenschutzaudit vorzusehen. Ziel des Datenschutzaudits ist es, öffentlichen Stellen die Möglichkeit einzuräumen, auf freiwilliger Basis durch ein vom Landesbeauftragten für den Datenschutz zugelassenes Gutachter-Verfahren die Datenverarbeitung auf ihre Datenschutz-

konformität überprüfen zu lassen und dabei besonderen Anforderungen zu genügen. Als Ausweis dieser besonderen Datenschutzqualität des Verfahrens wird ein bremisches Datenschutzaudit-Gütesiegel eingeführt, das die geprüften Verfahren auszeichnen soll. Bisher haben nur wenige andere Länder eine vergleichbare Regelung geschaffen. Auch die Umsetzung eines Datenschutzaudits auf Bundesebene lässt trotz einer entsprechenden Vorschrift im Bundesdatenschutzgesetz noch auf sich warten. Die in Bremen für das Audit erforderliche Rechtsverordnung ist zum Ende des Jahres zwischen den Behörden abgestimmt worden und wird voraussichtlich Anfang 2004 in Kraft treten. Das Gütesiegel darf dann für zwei Jahre verwendet werden, danach bedarf es einer erneuten Auditierung. Durch diese Regelung wird zum einen den sich schnell wandelnden technischen Bedingungen Rechnung getragen und zum anderen ein Ansporn geschaffen, den Datenschutz auf dem aktuellen Stand der Technik zu halten. Es handelt sich daher beim Datenschutzaudit auch nicht um eine ausschließlich stichtagsbezogene Überprüfung. Vielmehr ergibt sich die Zukunft des Audits bereits aus seinen inhaltlichen Anforderungen. Danach sind unter anderem die geplanten Datenschutz-Ziele festzulegen und anzugeben, mit welchen Mitteln diese Ziele erreicht werden sollen.

4. Bremische Bürgerschaft – Die Arbeit des Datenschutz- und Rechtsausschusses

4.1 Vom Datenschutz- zum Rechtsausschuss

Das Bremische Datenschutzgesetz bestimmt, dass zur Durchführung der parlamentarischen Kontrolle des Datenschutzes ein ständiger Parlamentsausschuss zu wählen ist, der die Jahresberichte des Landesbeauftragten für den Datenschutz und den jeweiligen Entwurf des Haushaltskapitels berät (§ 35 BremDSG). Diese Aufgabe hat in den vergangenen sieben Legislaturperioden der vom Parlament gebildete „Datenschutzausschuss“ wahrgenommen. In der im letzten Jahr begonnenen 16. Legislaturperiode wurde die Anzahl der Sitze im Parlament reduziert, dies wurde vom Parlament zum Anlass genommen, die Aufgaben nach § 35 BremDSG dem Rechtsausschuss zu übertragen (Bürgerschafts-Drs. 16/17 vom 02.07.2003).

In dem Rechtsausschuss bestand zunächst die Idee, einen Unterausschuss einzusetzen, der sich mit den Angelegenheiten des Datenschutzes befassen sollte. Bei näherer Befassung, insbesondere einer gutachterlichen Stellungnahme der Ausschussassistenz, stellte man fest, dass einem solchen Unterausschuss nur sehr eingeschränkte Kompetenzen zur Verfügung stehen würden. Deshalb wurde dieser Gedanke nach Beratung in den Fraktionen nicht weiter verfolgt. Zwischenzeitlich hat sich eine gute Übung eingespielt, sowohl Themen der Justiz wie des Datenschutzes in den Sitzungen des Rechtsausschusses zu behandeln. Allerdings führt dies trotz einer straffen Führung teilweise zu sehr langen Sitzungen und einer erheblichen Mehrbelastung der im Ausschuss vertretenen Mitglieder.

4.2 Ergebnisse der Beratung des 25. Jahresberichts

Bericht und Antrag des Rechtsausschusses vom 11. Februar 2004 zum 25. Jahresbericht des Landesbeauftragten für den Datenschutz vom 21. März 2003 (Drs. 15/1418) und zur Stellungnahme des Senats vom 26. August 2003 (Drs. 16/25)

Bericht

Die Bürgerschaft (Landtag) hat in ihrer Sitzung am 3. Juli 2003 den 25. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung am 11. September 2003 die Stellungnahme des Senats zur Beratung und Berichterstattung an den Rechtsausschuss überwiesen.

Der Ausschuss hat sich in mehreren Sitzungen mit dem Jahresbericht und der Stellungnahme befasst. Den Schwerpunkt der Beratungen bildeten diejenigen Punkte, über die auch in dem Zeitraum zwischen der Veröffentlichung des 25. Jahresberichts im März 2003 und der Übermittlung der Stellungnahme des Senats an die Bremische Bürgerschaft im August 2003 kein Einvernehmen zwischen dem Landesbeauftragten für den Datenschutz und den betroffenen Ressorts erzielt oder in denen trotz eines grundsätzlich bestehenden Einvernehmens eine zufrieden stellende Regelung noch nicht getroffen werden konnte. Bei den Beratungen hat der Ausschuss den Landesbeauftragten für den Datenschutz, Vertreter der betroffe-

nen Ressorts sowie einen Vertreter des Gesamtpersonalrats angehört. Die wesentlichen Beratungsergebnisse sind nachfolgend aufgeführt. Die Textziffern in den Überschriften entsprechen denen des 25. Jahresberichtes.

Software P-Switch (Tz. 3.2): Innerhalb des bremischen Verwaltungsnetzes (BVN) soll Mitarbeiterinnen und Mitarbeitern neben der dienstlichen Nutzung des Internetzugangs auch die private Nutzung erlaubt sein. Abhängig von der Art der Nutzung gelten für die dabei zulässige Protokollierung unterschiedliche rechtliche Anforderungen. Der Senator für Finanzen hat daher den Vorschlag des Landesbeauftragten für den Datenschutz aufgegriffen, den Nutzerinnen und Nutzern das aktive Umschalten zwischen dienstlicher und privater Internetnutzung zu ermöglichen. Im Auftrag des Senators für Finanzen hat die datenschutz nord GmbH eine Software mit dem Namen „P-Switch" entwickelt, die die Trennung privater und dienstlicher Zugriffe ermöglicht. Das Programm P-Switch verändert die Systemeinstellungen des Internet-Explorers von Microsoft. Je nach Art der Nutzung wird zwischen den zwei vom Internet-Explorer zu nutzenden zentralen Proxy-Servern, die entsprechend den rechtlichen Regelungen unterschiedliche Konfigurationen zur Protokollierung der Internetnutzung haben, umgeschaltet. Die aktuell eingestellte Nutzungsart wird für den Nutzer erkennbar auf dem Desktop durch die Buchstaben „D" für die dienstliche Nutzung sowie „P" für die private Nutzung dargestellt. Das Programm P-Switch stellt ein einfaches Werkzeug dar, das es ermöglicht, auf für den Nutzer unkomplizierte Weise die datenschutzrechtlichen Anforderungen der dienstlichen und privaten Internetnutzung am Arbeitsplatz zu erfüllen. Die Protokollierung auf den Proxy-Servern im BVN wird standardmäßig nicht personenbezogen erfolgen, bei konkretem Verdacht auf missbräuchliche Nutzung kann jedoch eine anlassbezogene zeitlich begrenzte Vollprotokollierung durchgeführt werden.

Der Einsatz des Programms und der Umfang der Protokollierung auf den beiden im BVN befindlichen Proxy-Servern ist Gegenstand einer neuen Internetrichtlinie. Diese wurde vom Senator für Finanzen mit dem Gesamtpersonalrat und dem Landesbeauftragten für den Datenschutz abgestimmt. Sie wird in Kürze in Kraft treten.

Der Rechtsausschuss begrüßt die Einführung der Software, die eine Trennung zwischen dienstlicher und privater Internetnutzung ermöglicht und so die Einhaltung der datenschutzrechtlichen Vorgaben gewährleistet.

Videoüberwachung Bahnhofsvorplatz (Tz. 6.1): Seit Anfang Oktober 2002 ist auf dem Bahnhofsvorplatz in Bremen eine polizeiliche Videoüberwachungsanlage in Betrieb. Sie kann vom Polizeipräsidium aus gesteuert werden und ermöglicht aufgrund einer Zoomfunktion bis ins Detail gehende Vergrößerungen.

Der Landesbeauftragte für den Datenschutz hat kritisiert, dass bei der Inbetriebnahme der Anlage den datenschutzrechtlichen Anforderungen nicht in ausreichendem Maße Rechnung getragen worden sei. Insbesondere sei er nicht rechtzeitig gemäß der seinerzeit geltenden Fassung des § 27 Abs. 4 Bremisches Datenschutzgesetz (BremDSG) über die Planungen zum Aufbau der Videoüberwachungsanlage unterrichtet worden. Er habe keine Möglichkeit gehabt, auf die Auswahl von Hard- und Software, die Installation oder die Datenübertragungswege Einfluss zu nehmen.

Der Senat hat dazu in seiner Stellungnahme ausgeführt, er habe entgegen der Darstellung des Landesbeauftragten für den Datenschutz diesen über die Planungen zum Aufbau einer Videoüberwachung frühzeitig unterrichtet. Eine darüber hinausgehende Einbeziehung des Landesbeauftragten in konkrete Beschaffungsmaßnahmen sei gesetzlich nicht vorgesehen.

Im Laufe der Beratungen des Rechtsausschusses sind der Landesbeauftragte für den Datenschutz und das Innenressort übereingekommen, zukünftig bei bevorstehenden ähnlichen Maßnahmen bereits im Vorfeld kooperativ zusammenzuarbeiten.

Der Landesbeauftragte für den Datenschutz hat außerdem die aufgestellten Hinweisschilder bemängelt, die Straftäter abschrecken und die Bevölkerung über eine mögliche Beobachtung informieren sollen. Sie genügten nicht den Anforderungen des § 29 Abs. 3 Bremisches Polizeigesetz (BremPolG), wonach polizeiliche Be-

obachtungen mittels Bildübertragung und Aufzeichnung nur offen und erkennbar durchgeführt werden dürfen. Die Schilder seien zu unauffällig und zu klein und schlecht zu lesen. Außerdem stünden sie zum Teil zu weit innerhalb des überwachten Bereichs.

Die Polizei Bremen hat die diesbezügliche Kritik des Landesbeauftragten für den Datenschutz zum Anlass genommen, die Schilder und ihre Standorte im Einvernehmen mit dem Landesbeauftragten zu modifizieren. Die neuen Schilder sind noch im Dezember 2003 aufgestellt worden.

Schließlich hat sich der Ausschuss mit dem Vorschlag des Landesbeauftragten für den Datenschutz befasst, eine so genannte Verschleierungssoftware einzusetzen, die die Gesichter der Passanten auf dem Bahnhofsvorplatz unkenntlich macht. Der Senator für Inneres und Sport hält den Einsatz einer Verschleierungssoftware für nicht zweckmäßig, da die Videoüberwachung eine Maßnahme zur Prävention von Straftaten sei. Die Nutzung einer solchen Software berge die Gefahr, dass Straftäter erst identifiziert werden könnten, wenn sie bereits eine Straftat begangen hätten. Aus diesem Grunde halten die Vertreter von SPD und CDU die Verwendung einer Software, mit deren Hilfe Gesichter von Passanten unkenntlich gemacht werden können, ebenfalls für nicht sachgerecht. Die Vertreter von Bündnis 90/Die Grünen haben in diesem Zusammenhang klargestellt, sie lehnten die Videoüberwachung am Bahnhofsvorplatz grundsätzlich ab, befürworteten aber, soweit sie dennoch zum Einsatz komme, den Einsatz einer Verschleierungssoftware.

Der Rechtsausschuss kritisiert, dass der Landesbeauftragte für den Datenschutz nicht früher von der geplanten Videoüberwachung am Bahnhofsvorplatz unterrichtet wurde, und erwartet für die Zukunft bei beabsichtigten Maßnahmen nach § 29 Abs. 3 BremPolG eine schnellere und engere Beteiligung des Landesbeauftragten.

Der Ausschuss begrüßt, dass am Bahnhofsvorplatz nunmehr größere und besser sichtbare Schilder auf die Videoüberwachung hinweisen.

Gegen die Stimmen der Ausschussmitglieder der Fraktion Bündnis 90/Die Grünen spricht sich der Ausschuss dafür aus, auf den Einsatz einer Verschleierungssoftware zu verzichten.

Rasterfahndung (Tz. 6.2): Nach den Anschlägen vom 11. September 2001 in den USA wurde auch in Deutschland nach Hintermännern und so genannten Schläfern gefahndet. In diesem Zusammenhang beschloss die Innenministerkonferenz, in den Bundesländern einen Datenabgleich mit anderen Daten, die so genannte Rasterfahndung, nach weitgehend einheitlichen Vorgaben durchzuführen. Die dazu erforderliche Änderung des Bremischen Polizeigesetzes erfolgte im Oktober 2001.

Auf der Grundlage des neu eingefügten § 36 i BremPolG ordneten die Polizei Bremen und die Ortspolizeibehörde Bremerhaven mit Zustimmung des Senators Inneres, Kultur und Sport gegenüber zahlreichen öffentlichen Stellen an, bestimmte Datensätze an die Polizei zu übermitteln. Der Innensenator gab seine Zustimmung in allen Fällen spätestens drei Tage nach Erlass der einzelnen Anordnungen durch die Polizei. Der Zeitraum zwischen Anordnungserlass und der gesetzlich vorgeschriebenen Unterrichtung des Landesbeauftragten für den Datenschutz betrug in aller Regel mindestens sieben Tage, in einigen Fällen war er deutlich länger.

Das Rasterprofil lautete für alle Stellen gleich und enthielt u. a. das Merkmal „Religionszugehörigkeit Islam". Die betroffenen Stellen selektierten ihre Datenbestände überwiegend selbst. In den Datenabgleich wurden rund 90.000 Datensätze aus dem Ausländerzentralregister und 10.000 Datensätze aus den Bereichen der übrigen Stellen einbezogen. Nach Abschluss des Datenabgleichs werden bei der Polizei 21 Verdachtsfälle bearbeitet. Alle nicht mehr benötigten Datensätze sind inzwischen gelöscht worden.

Der Landesbeauftragte für den Datenschutz hat die Durchführung der Rasterfahndung aus datenschutzrechtlicher Sicht bewertet und in einigen Punkten kritisiert. Der Rechtsausschuss hat sich insbesondere mit der Frage befasst, ob die polizeilichen Begründungen zu den Anordnungen in ausreichender Form die vom Gesetz geforderten Erwägungen wiedergeben und ob die Unterrichtung des Landesbeauftragten für den Datenschutz rechtzeitig erfolgte.

Der Landesbeauftragte für den Datenschutz hält die Begründung der Anordnungen der Rasterfahndung für unzureichend, da das Vorliegen der gesetzlich vorgeschriebenen Voraussetzungen für die Maßnahme nicht hinreichend dokumentiert worden sei. Das Innenressort ist dieser Ansicht entgegengetreten, hat jedoch inzwischen die Polizei Bremen und die Ortspolizeibehörde Bremerhaven gebeten, bei der Durchführung zukünftiger Datenabgleiche in der Begründung auf alle gesetzlichen Erfordernisse einzugehen. Der Rechtsausschuss geht insoweit davon aus, dass insbesondere das Rastermerkmal „Islam" bei der Anordnung eines Datenabgleichs mit anderen Daten einer besonderen Begründung bedarf, da es sich hierbei um eine besondere Kategorie personenbezogener Daten im Sinne der EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) handelt. Diese dürfen nach Art. 8 der Richtlinie, dessen Vorgaben inzwischen in § 3 Abs. 2 BremDSG umgesetzt worden sind, nur unter besonderen Voraussetzungen verarbeitet werden.

Ferner hat der Landesbeauftragte für den Datenschutz den Zeitpunkt seiner Unterrichtung moniert. Gemäß § 36 i Abs. 3 Satz 1 BremPolG darf die Rasterfahndung nur durch die Behördenleitung mit Zustimmung des Senators für Inneres und Sport angeordnet werden. Nach § 36 i Abs. 3 Satz 2 BremPolG ist der Landesbeauftragte für den Datenschutz unverzüglich zu unterrichten. Das Ressort hat die Auffassung vertreten, die Unterrichtung des Landesbeauftragten für den Datenschutz müsse erst erfolgen, sobald die Anordnung durch die erlassende Behörde gegenüber den Stellen wirksam ist, die die Daten übermitteln sollen. Der Rechtsausschuss ist jedoch mit dem Landesbeauftragten der Ansicht, dass dieser gemäß § 36 i Abs. 3 BremPolG spätestens unverzüglich nach Zustimmung durch den Innensenator über die Anordnung zu informieren ist. Der Senator für Inneres und Sport und der Landesbeauftragte haben sich inzwischen darauf verständigt, dass die Unterrichtung in Zukunft unverzüglich erfolgen soll, nachdem die Bestätigung der Anordnung durch den Innensenator den Polizeibehörden zugegangen ist. Die Polizeibehörden sollen sich dabei moderner Kommunikationsmittel bedienen, um Verzögerungen zu vermeiden.

Hinsichtlich der Durchführung der Rasterfahndung ist das Innenressort inzwischen einer Reihe von Vorschlägen des Landesbeauftragten für den Datenschutz gefolgt. So sollen die Polizeibehörden darauf achten, dass alle Daten übermittelnden Stellen selbst eine Auswahl nach den vorgegebenen Kriterien vornehmen und dies nicht der Polizei überlassen. Außerdem ist bei Beteiligung dritter Stellen, die eine Datenaufbereitung durchführen, ein eindeutiger schriftlicher Auftrag gemäß § BremDSG zu erteilen.

Der Rechtsausschuss erwartet, dass der Landesbeauftragte gemäß § 36 i Abs. 3 BremPolG zukünftig unverzüglich nach Zustimmung zur Rasterfahndung durch den Senator für Inneres unterrichtet wird und dass bei der Begründung der Anordnung die datenschutzrechtlichen Bestimmungen berücksichtigt werden.

City-Server (Tz. 6.7): In der Stadtgemeinde ist ein so genannter City-Server eingerichtet worden. Hierbei handelt es sich um eine Datenbank, die digitale Aufnahmen von allen Straßenzügen in Bremen mit den darin befindlichen Häusern enthält. Auf den Aufnahmen sind gelegentlich auch einzelne Personen zu erkennen. Der City-Server soll eine Besichtigung vor Ort entbehrlich machen.

Der Landesbeauftragte für den Datenschutz hat kritisiert, die nach §§ 7 und 8 BremDSG erforderlichen organisatorischen und technischen Maßnahmen seien nicht getroffen worden. Außerdem bestünden erhebliche Bedenken, wenn nichtöffentliche Stellen oder Privatpersonen beliebig auf die Bilddaten zugreifen könnten.

Im Gegensatz dazu meint das Innenressort, bei den Bilddokumenten der City-Server-Technologie handele es sich nicht um personenbezogene Daten, so dass die Vorgaben des Bremischen Datenschutzgesetzes nicht einschlägig seien. Dennoch hat das Ressort in Abstimmung mit dem Landesbeauftragten für den Datenschutz ein Einsatzkonzept erarbeitet, das die rechtlichen Vorgaben des Bremischen Datenschutzgesetzes berücksichtigt. Das Konzept sieht unter anderem ein Einsichtsrecht und ein Widerspruchsrecht der Betroffenen vor. Die Nutzung der Daten durch Private ist ausgeschlossen.

Der Rechtsausschuss stellt fest, dass sich die datenschutzrechtlichen Bedenken des Landesbeauftragten bezüglich des Einsatzes des City-Servers in Kürze erledigen werden.

Erteilung von Sammelauskünften durch die Meldebehörde Bremen (Tz. 6.12.2): Nach § 32 des Gesetzes über das Meldewesen (BremMeldG) darf die Meldebehörde auch Personen, die nicht Betroffene sind, und anderen als den in § 30 Abs. 1 BremMeldG bezeichneten Stellen verschiedene Auskünfte aus dem Einwohnermelderegister erteilen. Bei der so genannten einfachen Melderegisterauskunft (§ 32 Abs. 1 BremMeldG) ist der Datenkatalog auf Vor- und Familiennamen, Doktorgrad und Anschriften beschränkt. Ein besonderes Interesse muss der Auskunft Begehrende hier nicht darlegen. Im Rahmen der erweiterten Melderegisterauskunft (§ 32 Abs. 2 BremMeldG) können jedem, der ein berechtigtes Interesse glaubhaft macht, zusätzliche Daten, wie z. B. Geburtstag und -ort, Familienstand und Staatsangehörigkeiten, mitgeteilt werden.

Im Hinblick auf solche Auskunftsersuchen, bei denen große Kunden, wie z. B. die Handelskammer oder die Bremer Sparkasse, eine große Anzahl von Einzelanfragen an die bremische Meldebehörde richten, hat diese ein automatisiertes Auskunftsverfahren entwickelt. Im Rahmen dessen werden Anfragen von Großkunden seit einiger Zeit in einem besonders gesicherten Verfahren auch unter Einsatz des Internets beantwortet.

Der Landesbeauftragte für den Datenschutz hat moniert, dass bei dem automatisierten Verfahren nicht nach der Art der Melderegisterauskunft differenziert wurde. Auskünfte nach § 32 Abs. 2 BremMeldG wurden erteilt, ohne dass das berechtigte Interesse des Datenempfängers überprüft worden war. Eine Unterrichtung der Betroffenen über die erweiterte Melderegisterauskunft erfolgte in aller Regel nicht, obwohl hiervon nur abgesehen werden kann, wenn der Datenempfänger ein rechtliches Interesse geltend gemacht hat.

In seiner Stellungnahme hat der Senat eingeräumt, im Rahmen des automatisierten Auskunftsverfahrens gegenüber zwei Kunden seien regelmäßig Auskünfte erteilt worden, ohne dass das Vorliegen der gesetzlichen Vorgaben geprüft worden sei. Diese Verfahrensweise ist inzwischen eingestellt worden. Nach Auskunft eines Vertreters des Senators für Inneres und Sport wird auch im automatisierten Auskunftsverfahren vor Erteilung einer Auskunft durch die Meldebehörde in jedem Einzelfall das Vorliegen der gesetzlichen Voraussetzungen überprüft. Insbesondere ist ein berechtigtes Interesse an einer erweiterten Melderegisterauskunft schriftlich nachzuweisen.

Der Rechtsausschuss begrüßt, dass die Kritik des Landesbeauftragten für den Datenschutz aufgegriffen worden ist, und erwartet, dass die gesetzlichen Vorgaben bei der Erteilung von Melderegisterauskünften zukünftig beachtet werden.

„Bürgertelefone" in Bremen und Bremerhaven (Tz. 9.7): In Bremen und Bremerhaven wurden im Jahr 2002 so genannte Bürgertelefone eingerichtet. In Bremerhaven sollte durch die Mithilfe von Bürgern Sozialhilfemissbrauch aufgedeckt werden, in Bremen geht es um die Aufdeckung von Schwarzarbeit. Der Bremerhavener Anschluss ist inzwischen wieder abgeschaltet worden; datenschutzrechtliche Probleme gab es hier nicht. In Hinblick auf das Bürgertelefon bei der Koordinierungsstelle zur Bekämpfung illegaler Beschäftigung des Senators für Arbeit, Frauen, Gesundheit, Jugend und Soziales hat der Landesbeauftragten für den Datenschutz dagegen rechtliche Bedenken geäußert.

Insbesondere hält er den Senator für Arbeit nicht für befugt, zur Erfüllung eigener gesetzlicher Aufgaben zu Lasten der von Hinweisen betroffenen Bürger deren Daten zu bearbeiten. Darüber hinaus hat er das Fehlen eines den Anforderungen des BremDSG entsprechenden Datenschutzkonzepts bemängelt.

Der Vertreter des Senators für Arbeit hat dem Rechtsausschuss erläutert, welche Lösungen denkbar wären, um die Datenverarbeitung in seinem Haus auf eine rechtliche Grundlage zu stellen. Nach seiner Darstellung sind jedoch mit allen Modellen rechtliche oder praktische Probleme verbunden. Bis zur Sitzung des Rechtsausschuss am 14. Januar 2004 hat das Arbeitsressort kein zufrieden stellendes Konzept vorgelegt. Es hat jedoch zugesagt, ein solches in Abstimmung mit dem Landesbeauftragten für den Datenschutz in Kürze zu erstellen. Die Vertreter von Bündnis 90/Die Grünen drängen darauf, dass das Ressort im Rahmen des vorzulegenden Konzeptes insbesondere auf die Geeignetheit und Erforderlichkeit der Datenerhebung noch stärker eingeht.

Der Rechtsausschuss erwartet, dass der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales bis zum 1. März 2004 eine Lösung herbeiführt. Er bittet den Landesbeauftragten für den Datenschutz, ihn in seiner nächsten Sitzung über den Verfahrensstand zu informieren.

Antrag

Die Bürgerschaft (Landtag) möge beschließen:

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

4.3 Weitere Themen der Beratungen im Datenschutz- bzw. Rechtsausschuss

Über die unter Ziff. 4.2 dargestellten Ergebnisse hinaus hat sich der für den Datenschutz zuständige Parlamentsausschuss u. a. auch mit den nachfolgend aufgelisteten Themen beschäftigt:

In der 15. Legislaturperiode (Datenschutzausschuss)

— Ergänzung der Meldedatenübermittlungsverordnung: Datenübermittlung der Meldebehörden an die Waffenerlaubnisbehörden,

— Beachtung des Datenschutzes bei der Evaluation des Verfahrens zur begleitenden Betreuung von Opfern häuslicher Beziehungsgewalt,

— Einhaltung der datenschutzrechtlichen Vorgaben bei der Datenerhebung im Rahmen des Forschungsprojektes „Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen",

— Datei über jugendliche Intensivtäter,

— Melderegisterabgleich für Entsorgungsbetriebe,

— Gesetz zur Änderung des Bremischen Krankenhausdatenschutzgesetzes und zur Änderung des Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten,

— DNA-Probe als Standardmaßnahme im Rahmen der erkennungsdienstlichen Behandlung?,

— Selbstverteidigung im Internet.

In der 16. Legislaturperiode (Rechtsausschuss)

— Aktuelle Bundesgesetzgebung mit datenschutzrechtlichen Bezügen,

— Sprachscreening in Kindergärten oder Sprachstandserhebung 2003,

— Datenschutzrechtliche Auswirkungen der Gesundheitsreform und Bewertungen des Gesundheitssystemmodernisierungsgesetzes (GMG),

— Konsequenzen ressortübergreifender Zusammenarbeit aus einem Tötungsdelikt vom 11. Juli 2003 in der Bremer Neustadt.

Die Sitzungen des Rechtsausschusses sind in der Regel öffentlich.

5. Personalwesen

5.1 Elektronische Arbeitszeiterfassung

Vor über zehn Jahren ist entschieden worden, in der bremischen Verwaltung die elektronische Arbeitszeiterfassung einzuführen. Zunächst war vorgesehen, dass für die jeweiligen Dienststellen ein eigenes System zum Einsatz kommen sollte. Aus Kostengründen wurde dann entschieden, stattdessen ein zentrales System zu beschaffen, an das sich die jeweiligen Dienststellen anschließen können. Zuletzt habe ich darüber 1997 berichtet (vgl. 19. JB; Ziff. 8.2).

Nachdem inzwischen die Dienstvereinbarung über die Grundsätze für die Gleitende Arbeitszeit vom 17. März 1999 (Brem.ABl. S. 225) und das Datenschutz- und

Sicherheitskonzept sowie die Verfahrensbeschreibung unter meiner Beteiligung erstellt worden sind, ist das automatisierte Verfahren im Sommer 2002 zunächst in einigen Dienststellen eingeführt worden. Die Daten werden zentral bei ID Bremen verarbeitet, verantwortlich dafür ist der Senator für Finanzen. Vorgesehen ist, dass alle Dienststellen der bremischen Verwaltung nach und nach an das Zentralsystem angeschlossen werden.

5.2 Mobile Arbeitsgestaltung bei Führungskräften

Der damalige Senator für Bau und Umwelt hat mir ein Konzept zur mobilen Arbeitsgestaltung bei Führungskräften zugesandt. Danach bestehe das Erfordernis, im Bedarfsfall PC-gestützte Arbeit, die sich auf am Arbeitsplatz vorhandene Programme und Daten bezieht, auch von zu Hause aus erledigen zu können und ggf. auf Dienstreisen ebenfalls einen Zugriff auf das Bremer Verwaltungsnetz (BVN) zu haben.

Ich habe ihm eine Vielzahl zu beachtender Anforderungen dargelegt, die im Wesentlichen denen der alternierenden Telearbeit entsprechen, z. B. die schriftliche Verpflichtung, die technischen und organisatorischen Maßnahmen im häuslichen Bereich einzuhalten und die schriftliche Einwilligung, dass ich die Einhaltung des Datenschutzes im häuslichen Bereich einschließlich des dienstlich genutzten Privat-PC überwachen kann. Vor dem Einsatz sollte eine Vorabkontrolle stattfinden und eine Verfahrensbeschreibung für die mobile Arbeitsgestaltung erstellt werden.

Die senatorische Stelle hat zugesagt, meine Anforderungen umzusetzen.

5.3 Keine allgemeine Überprüfung zu den „Rosenholz-Dateien"

Der Bundesrat hat im Herbst 2003 eine Entschließung zur Überprüfung der Mitarbeiterinnen und Mitarbeiter des öffentlichen Dienstes auf Zusammenarbeit mit dem Staatssicherheitsdienst (Stasi) der ehemaligen DDR unter Verwendung der „Rosenholz-Dateien" gefasst. Mit den mit der Freigabe dieser Dateien gewonnenen neuen Erkenntnisse soll weiterer Aufschluss über mögliche Tätigkeiten Angehöriger des öffentlichen Dienstes für die Stasi gewonnen werden.

Den Medien habe ich entnommen, dass von den 16 Bundesländern lediglich Thüringen eine allgemeine Überprüfung vornehmen will. Nach Auskunft vom Senator für Finanzen wird Bremen auf eine derartige Überprüfung verzichten. Sie solle nur bei konkretem Anlass erfolgen. Insoweit orientiert sich der Senator für Finanzen an der Rechtsprechung zur Prüfung der Verfassungstreue. Ich halte diese Vorgehensweise unter Beachtung des Grundsatzes der Verhältnismäßigkeit für angemessen.

Im Übrigen hat die Bürgerschaft (Landtag) in ihrer 10. Sitzung am 18. Dezember 2003 einen Beschluss gefasst, wonach die Mitglieder der Bremischen Bürgerschaft bei der Bundesbeauftragten für die Unterlagen des Staatssicherheitsdienstes, auch unter Einbeziehung der so genannten Rosenholz-Dateien, überprüft werden sollen. Die Ergebnisse sollen an den Präsidenten der Bre-mischen Bürgerschaft übermittelt werden. Dieser wird gebeten, den Verfassungs- und Geschäftsordnungsausschuss über die Ergebnisse der Überprüfung unverzüglich fortlaufend zu informieren (Beschlussprotokoll Nr. 16/154 – 16/158).

5.4 Entwurf einer Internet-Richtlinie

Im Jahr 2002 wurde die missbräuchliche Nutzung des Internets von dienstlichen PC festgestellt (vgl. meinen Prüfbericht im 25. JB, Ziff. 7.1). Die dabei festgestellten Verstöße gaben Anlass zur Schaffung einer Internet-Richtlinie für die bremische Verwaltung. Der Senator für Finanzen hat sodann den Entwurf einer Internet-Richtlinie vorgelegt, der nach mehrfacher Abstimmung mit mir den datenschutzrechtlichen Anforderungen entspricht. Die senatorische Behörde hat sich dabei äußerst kooperativ gezeigt.

Als besonders bedeutsam sind Art, Umfang und Zeiten der Protokollierung von Zugriffen auf Internet-Seiten einzustufen. Hierbei galt es, bei der dienstlichen Nutzung des Internets den Grundsatz der Verhältnismäßigkeit und bei der privaten Nutzung des Internet das Fernmeldegeheimnis zu beachten. Des Weiteren

war es wichtig, diese Protokollierungsregelung klar und verständlich zu formulieren, um dem Grundsatz der Transparenz der Datenverarbeitung Rechnung zu tragen.

Demzufolge ist geregelt worden, dass die Protokollierung grundsätzlich auf den für die Internetnutzung zur Verfügung stehenden zentralen Systemen des Providers bei der Brekom erfolgt. Hierbei soll die Software „P-Switch" eingesetzt werden, die den Nutzern das aktive Umschalten zwischen dienstlicher und privater und Internetnutzung ermöglicht (vgl. 25. JB, Ziff. 3.2).

Für sämtliche Zugriffe (auch private) auf das Internet werden die vollständigen IP-Adressen, gekürzt um die drei letzten Ziffern des abrufenden Arbeitsplatz-PC, die aufgerufenen Internetseiten (URL), das Datum und die Uhrzeit des Abrufs sowie der Umfang der Datenmenge protokolliert. Dabei werden die Protokolldaten der dienstlichen und privaten Zugriffe zentral auf getrennten Systemen gehalten. Die Protokolldaten aller Zugriffe werden nach spätestens 90 Tagen gelöscht.

Die zentral erhobenen Protokolldaten dürfen nur vom Senator für Finanzen gemeinsam mit dem Gesamtpersonalrat ausgewertet werden, wenn tatsächliche Anhaltspunkte den Verdacht auf eine der festgelegten unzulässigen Nutzungen begründen. Dabei hat sich die Auswertung zu beschränken auf die Feststellung des Transfervolumens und die Anzahl sowie die Analyse der aufgerufenen Seiten. Die Analyse beschränkt sich bei privaten Zugriffen auf unzulässige Inhalte, die ebenfalls in der Richtlinie aufgeführt sind.

Erst wenn sich bei einer Auswertung dienstlicher Zugriffe der Verdacht auf eine unzulässige Nutzung, die eindeutig nicht in dienstlichem Zusammenhang steht, bestätigt, werden anstelle der Netzwerkadressen für einen Zeitraum von 30 Tagen die vollständigen IP-Adressen gespeichert. Derartige Auswertungen dürfen nur auf den IP-Nummernkreis der betroffenen Dienststelle erfolgen. Die Dienststellen beauftragen für diese Auswertungen den Provider und haben ihren Personalrat und den Landesbeauftragten für den Datenschutz davon unverzüglich zu informieren.

Die insoweit erstellten Protokolldaten unterliegen der Zweckbindung und sind vom Senator für Finanzen, der Dienststelle und dem örtlichen Personalrat umgehend auszuwerten. Das Ergebnis ist in einer Niederschrift festzuhalten und dem Senator für Finanzen schriftlich mitzuteilen. Alle anderen Protokolldaten, die nicht unmittelbar zum Nachweis eines bestätigten Verdachts dienen, sind sofort zu vernichten.

Nachdem sich das In-Kraft-Treten dieser Richtlinie immer mehr hinauszögerte, hat sich der Rechtsausschuss der Bürgerschaft (Landtag) ausführlich mit diesem Thema befasst und den Senator für Finanzen aufgefordert, die Richtlinie baldmöglichst in Kraft zu setzen. Dies ist nach Abstimmung mit dem Gesamtpersonalrat Ende 2003 geschehen. Die nachhaltige Unterstützung durch den Rechtsausschuss hat wesentlich dazu beigetragen.

Im Amtsblatt der Freien Hansestadt Bremen wurde „Die Richtlinie für die Bereitstellung und Nutzung von Internet/Intranet-Zugängen" veröffentlicht (Brem.ABl. vom 10.02.2004, S. 77).

5.5 Aushang mit personenbezogenen Bewerberdaten

Ich bin darauf hingewiesen worden, ein Konrektor der Hochschule Bremerhaven habe mehrfach personenbezogene Angaben bzw. Informationen über Bewerber per Aushang hochschulintern veröffentlicht, z. B. das Protokoll einer Sitzung der Auswahlkommission für die Stelle einer(s) Lehrbeauftragten. Auch dieses Protokoll habe personenbezogene Daten über die dort genannten Bewerber enthalten.

Der Konrektor hat den Sachverhalt zwar bestritten, jedoch wurde mir glaubhaft dargelegt, dass der Rektor ihn bereits mehrfach aufgefordert habe, diese Art der Veröffentlichung zu unterlassen. Schließlich hat der Konrektor auf mein Drängen hin erklärt, er werde in Zukunft die entsprechenden Datenschutzbestimmungen einhalten.

5.6 Prüfung der Personalaktenführung

Meine im Jahr 1999 begonnene Datenschutzprüfung bei Personalstellen (vgl. 22. JB, Ziff. 5.1) habe ich auch in diesem Jahr fortgesetzt. Anfang Dezember 2003 habe ich beim Personalreferat des Senators für Bildung und Wissenschaft mit einer Stichprobe geprüft, ob die Vorgaben der Verwaltungsvorschrift über die Erhebung und Führung von Personalaktendaten (PAVwV) vom 1. Oktober 2001 (Brem.ABl. S. 761) eingehalten werden.

Dabei stellte ich u. a. fest, dass sich im Personalreferat noch Beihilfeakten befanden, obwohl bereits seit mehreren Jahren Performa Nord die Beihilfestelle ist und dort die Beihilfeakten zu führen sind. Des Weiteren waren nicht in allen Grundakten ein Verzeichnis über Teil- und Nebenakten vorhanden. In den Krankheitsakten befanden sich Krankmeldungen, die teilweise über zehn Jahre zurücklagen, obwohl eine Aussonderung nach spätestens fünf Jahren zu erfolgen hat. Außerdem ergab die Überprüfung, dass ärztliche Unterlagen (z. B. ärztliche Untersuchung mit dem Befund einer chronischen Augenerkrankung) in den Grundakten offen aufbewahrt wurden.

Ich habe dem Leiter des Personalreferats der senatorischen Dienststelle einen ausführlichen Prüfbericht übersandt und ihn gebeten, die jeweils aufgeführten Mängel abzustellen. Er wird mich über das Ergebnis unterrichten.

6. Inneres

6.1 Polizei

6.1.1 INPOL-HB

Nach Jahren des Wartens wurde in Bremen als einem der ersten Länder die Polizei an das neue INPOL-System angeschlossen. Zu dem Zweck erhielt die Bremer Polizei eine Anwendung, die so genannte INPOL-Land-Anwendung, die auf den bremischen Polizeiservern läuft und die Schnittstellen zu der Bundesanwendung INPOL beim BKA bedient. Es handelt sich um eine moderne serverbasierte DV-Anwendung, die die rechenzentrumsorientierte Anwendung ablöst.

Zurzeit gibt es unter den Beauftragten für den Datenschutz in Bund und Ländern eine Abstimmung über die neukonzipierte Errichtungsanordnung. Wenn diese abgeschlossen ist, werde ich mit der Polizei Bremen eine solche auch für das Land Bremen beraten.

6.1.2 NIVADIS an Stelle von EVA-HB

In den letzten beiden Jahresberichten (vgl. 24. JB, Ziff. 6.6 und 25. JB, Ziff. 6.4) berichtete ich ausführlich über die Konzeptionsarbeiten zu einem neuen Vorgangsbearbeitungssystem „EVA-HB". Diese Arbeiten waren bereits sehr weit fortgeschritten und die Polizeibeamten waren weitgehend für die Anwendung durch Schulungen vorbereitet. Auch waren so genannte Migrationstests (Überführung der Altdaten aus ISA in das neue Verfahren) mehr oder weniger erfolgreich durchgeführt worden. Im Frühjahr des Berichtsjahres wurde ich darüber unterrichtet, dass Bremen beabsichtigt, die Einführung von EVA-HB – ob aus technischen oder Kostengründen, wurde nicht deutlich – nicht weiter zu verfolgen. Es werde geprüft, das Vorgangsverwaltungssystem der niedersächsischen Polizei zu übernehmen. Dazu solle die vorhandene Infrastruktur der Bremer Polizei genutzt werden und die bremischen Polizeidaten in – von der niedersächsischen Anwendung abgeschotteten – Datenbanken beim Informationszentrum Niedersachsen – Landeseigenbetrieb – (IZN) im Auftrag verarbeitet werden.

In den letzten Wochen und Monaten sind umfangreiche Untersuchungen hinsichtlich der technischen Realisierbarkeit, aber auch insbesondere hinsichtlich der unterschiedlich ausgestalteten Polizeiarbeit von der Polizei Bremen in Zusammenarbeit mit der niedersächsischen Polizei und dem Rechenzentrum IZN vorgenommen worden. Über die Ergebnisse bin ich durch die fortlaufende Übersendung der Protokolle der Arbeitssitzungen unterrichtet worden. Für Anfang des Jahres 2004 ist eine Besprechung zu datenschutzrechtlichen Fragestellungen zwischen den vorgenannten Stellen, dem behördlichen Datenschutzbeauftragten der Polizei Bre-

men und den Landesbeauftragten für den Datenschutz der Länder Niedersachsen und Bremen vorgesehen. Etwas irritiert hat mich allerdings ein Pressebericht aus Hannover mit dem Titel „NIVADIS läuft nicht", wonach das Antwort-Zeitverhalten nicht akzeptabel sein soll.

6.1.3 Rasterfahndung in Bremen abgeschlossen

Über die Rasterfahndung nach den Anschlägen in New York habe ich bereits in den beiden letzten Jahresberichten geschrieben (vgl. 24. JB, Ziff. 6.3 und 25. JB, Ziff. 6.2). Nunmehr kann ich über den Abschluss der Rasterfahndung im Lande Bremen berichten.

Am 11. April 2003 wurden die Rasterfahndungsdaten der Polizei Bremen beim Bundeskriminalamt (BKA) gelöscht. Auf meine Bitte bestätigte das BKA im Oktober 2003, dass bremische Daten aus diesen Datenbeständen der bundesweiten Rasterfahndung nicht an Nachrichtendienste und auch nicht an ausländische Polizeidienststellen weitergegeben wurden.

Am 10. September 2003 wurden die Rasterfahndungsdaten, welche die Polizei Bremen in der Arbeitsdatei „Rasterfahndung Terroranschlag USA" bei sich gespeichert hatte, gelöscht.

Einige wenige Datenbestände wurden zur weiteren Aufklärung aus der Datei der Rasterfahndung herausgenommen und der konventionellen Datenverarbeitung bei der Staatsschutzabteilung der Polizei zur weiteren Abklärung übergeben. Es handelte sich um zunächst zirka 40 Fälle, diese Zahl hat sich aber nach Mitteilung der zuständigen Stelle bereits Anfang Oktober 2003 halbiert. Die verbliebenen rund 20 Fälle habe ich einer weiteren exemplarischen Prüfung unterzogen. Zu einer von mir daraus ausgewählten Stichprobe habe ich mir die Akten vorlegen lassen. Die von mir geprüften Akten gaben keinen Anlass zu einer Beanstandung. Allerdings konnte ich dabei feststellen, dass die aus der Rasterfahndung stammenden Personen der Polizei bereits in anderen Zusammenhängen hinlänglich bekannt waren.

Im Berichtsjahr hatte ich erneut Anlass, mich mit der Frage zu beschäftigen, ob die Übermittlung eines gesamten Datenbestandes durch die Handelskammer Bremen erforderlich war. Dabei konnte ich feststellen, dass durch das Fehlen des Merkmals „Staatsangehörigkeit" in den Datensätzen der Datenbank „Gefahrgutfahrerschulung" der Handelskammer Bremen sich nicht hinreichend selektieren ließ und auf Anforderung der Polizei eine Vielzahl von Personendatensätzen übermittelt wurde, auf die die Rasterkriterien im Übrigen nicht zutrafen. Da eine Nacherfassung des fehlenden Merkmals durch die Handelskammer Bremen nicht zumutbar war, hat sie sich formalrechtlich korrekt verhalten. Ich hätte es jedoch begrüßt, wenn ich mit diesem Problem befasst worden wäre. Eine datenschutzfreundliche Lösung hätte in der Anwendung eines so genannten black-box-Verfahrens liegen können, wie weiter unten dargestellt.

Eine andere Frage musste im Zuge der Beendigung der Rasterfahndung entschieden werden: Waren nunmehr die Personen, deren Daten in die Rasterfahndung mit einbezogen worden waren, bei denen aber nichts festgestellt worden war, darüber zu unterrichten? Das OVG Bremen hatte in seinem Urteil vom 8. Juli 2002 (Az: 1 B 155/02) festgestellt, dass das Land Bremen für die von ihm an das BKA gelieferten Daten die datenschutzrechtliche Verantwortung dafür trage, dass der dort durchgeführte weitere Datenabgleich rechtmäßig erfolge. Der beim BKA durchgeführte Datenabgleich müsse jedenfalls nach Abschluss der Maßnahme gegenüber dem Betroffenen transparent gemacht werden können.

Bei der Entscheidung der Frage war zu berücksichtigen, dass der Polizei nicht die aktuellen Meldedaten der Betroffenen vorlagen. Fast zwei Jahre später hätte sie diese erst mühsam recherchieren müssen, wegen der hohen Fluktuation im Ausländerbereich wäre es vielleicht nicht einmal möglich gewesen, die momentan aktuelle Adresse der Betroffenen ausfindig zu machen. Ein solch zweifelhafter Aufwand ist nicht geboten und ist aus datenschutzrechtlichen Überlegungen auch nicht wünschenswert, denn dies würde in vielen Fällen eine Berichtigung der Adressen erfordern und daher nur zu einer Verlängerung der Speicherfristen bei der Polizei führen. Die richterliche Vorgabe habe ich auch nicht so verstanden,

dass nunmehr die Polizei verpflichtet sei, die Daten aller von der Rasterfahndung Betroffenen in einer Sperrdatei weiter aufzubewahren, um gegebenenfalls bei eingehenden Auskunftsersuchen dem Betroffenen Antwort erteilen zu können. Ich habe den Richterspruch vielmehr so interpretiert, dass Betroffenen generell Auskunft erteilt werden muss, ob und wie sie in die Rasterfahndung mit einbezogen worden sind oder nicht. Ich forderte deshalb eine Dokumentation der Verarbeitungsschritte (welche Daten wurden zu welchem Zeitpunkt erhoben und mit welchen Daten abgeglichen). Da einem Betroffenen selbst seine Daten bekannt sind, könnte die Polizei ihm abstrakt darüber Auskunft geben, dass wenn er bestimmte Merkmale besaß, er die Voraussetzungen erfüllt habe und damit davon ausgehen könne, dass er mit seinem Datensatz in die Rasterfahndung einbezogen wurde. Die von mir geforderte Dokumentation kann bei Fragen von Betroffenen auch dazu dienen, diese über die konkreten Schritte in der Datenverarbeitung auch beim BKA zu unterrichten.

Ende November waren alle meine Prüfungen abgeschlossen, am 2. Dezember 2003 habe ich die Öffentlichkeit über die Ergebnisse unterrichtet.

Offen geblieben war allerdings noch, wie mit meiner im 25. Jahresbericht geäußerten Kritik umgegangen werden sollte. Zwischen dem Innenressort und mir gab es unterschiedliche Meinungen über die Auslegung der polizeirechtlichen Vorschriften der Rasterfahndung. Der Senat hatte insoweit in seiner Stellungnahme in allen wesentlichen Punkten meinen Rechtsausführungen widersprochen (vgl. Stellungnahme des Senats, Bürgerschafts-Drs. 16/25).

Diese Fragen konnten nunmehr durch die Behandlung im Rechtsausschuss entschieden werden (vgl. Ziff. 4.2 dieses Berichts). Nach der Sitzung des Rechtsausschusses habe ich mich noch im Dezember mit dem Innenressort über alle strittigen Punkte mit nachfolgend dargestellten Ergebnissen verständigt:

— Beteiligung des Landesbeauftragen für den Datenschutz

  Der Landesbeauftragte für den Datenschutz hat nach § 36 i Abs. 3 BremPolG einen Anspruch darauf, unverzüglich von einer Maßnahme nach § 36 i Abs. 1 BremPolG unterrichtet zu werden. Es wurde festgelegt, dass mit mir bereits vor dem Erlass einer solchen Maßnahme ein Informationsgespräch stattzufinden hat, soweit nicht zeitlich zwingende Gründe dem entgegenstehen.

  Einvernehmlich wurde für künftige Verfahren festgelegt, dass ich bereits dann zu unterrichten bin, wenn die Anordnung des zuständigem Leiters der Vollzugspolizei Bremen oder Bremerhaven vom Senator für Inneres und Sport bestätigt wurde und den anordnenden Stellen, d. h., der Polizei, zugegangen ist. Dafür sprach u. a. die Erwägung, dass die Kontrolle des Datenschutzbeauftragten nach der Konzeption der gesetzlichen Regelung eine gerichtliche Kontrolle ersetzen soll. Außerdem steht der Inhalt der Anordnungen ab diesem Zeitpunkt definitiv fest, so dass ich bereits ab diesem Zeitpunkt beratend auf das Verfahren Einfluss nehmen kann.

  Die Unterrichtung des Landesbeauftragten soll zweckmäßigerweise zukünftig vorab durch Fax oder E-Mail erfolgen. Es hatte sich bei der letzten Unterrichtung herausgestellt, dass es über den konventionellen Postweg zu teilweise langen Brieflaufzeiten kam.

— Verfahren bei der Erstellung der Anordnungen

  Die anordnenden Stellen erhielten die Empfehlung, im Zuge der Erstellung einer Anordnung nach § 36 i BremPolG den Datenschutzbeauftragten des Hauses zu beteiligen.

  Die Begründung der Anordnung soll zu den einzelnen gesetzlichen Erfordernissen jeweils Aussagen enthalten. Aus der Begründung muss ersichtlich sein, dass diese Erfordernisse geprüft worden sind.

— Durchführung der Maßnahmen

  Soweit eine Auswahl von Daten aus dem Gesamtbestand der übermittelnden Stelle erforderlich ist, ist diese Auswahl durch die übermittelnde Stelle selbst vorzunehmen. Es ist nicht statthaft, dass die übermittelnde Stelle der Polizei

ihren Gesamtbestand überlässt und die Polizei selbst eine Auswahl durchführen muss.

Soweit eine Datenselektion durch die übermittelnde Stelle nicht selbst durchgeführt werden kann, bietet sich in geeigneten Fällen das so genannte black-box-Verfahren an. Dabei werden die Daten an eine dritte Stelle, z. B. das Rechenzentrum, übermittelt, die eine Auswahl anhand der polizeilichen Kriterien vornimmt. In diesem Verfahren werden nur die ausgewählten Daten der Polizei anschließend zur Verfügung gestellt.

Bei der Beteiligung dritter Stellen, die eine Datenaufbereitung durchführen, ist darauf zu achten, dass eine klare schriftliche Auftragserteilung erfolgt.

— Zweckbeschränkung der Daten bei der Übermittlung an andere Polizeien

Bei der Weitergabe von Daten an andere Behörden, die mittels eines Datenabgleichs gewonnen worden sind, wurde die Fortführung der Zweckbeschränkung nach §§ 36 d Abs. 2, 36 b Abs. 6 BremPolG der empfangenden Stelle auferlegt (vgl. meine Darlegung im 24. JB, Ziff. 6.2).

— Abschluss der Maßnahmen

Beim Abschluss der Maßnahme ist unter meiner Beteiligung zu klären, ob und gegebenenfalls wie eine Benachrichtigung der von dem Datenabgleich betroffenen Personen erfolgt.

Nach Abschluss der Maßnahme ist eine Konzeption zur Rückgabe der Datenträger und zur Löschung nicht mehr benötigter Daten zu entwickeln.

Auch wenn die Ergebnisse der Rasterfahndung nicht dafür sprechen, das dieses Mittel in Zukunft häufig für die Erfüllung polizeilicher Aufgaben herangezogen werden wird, war es wichtig, diese Klarstellungen zu erzielen. Die Rasterfahndung bleibt eine im bremischen Polizeigesetz geregelte, zulässige Maßnahme. Für den Fall, dass sie wieder zum Einsatz kommen sollte, wird dies aus Anlass eines ähnlich gravierenden Vorfalles geschehen mit den damit verbundenen eiligen, ja zum Teil hektischen Erscheinungen. Dann aber wäre es zu spät, die jetzt getroffenen Vereinbarungen, die den Datenschutz wesentlich verbessern werden, zu verabreden.

6.1.4 Videoüberwachung auf dem Hauptbahnhofsvorplatz

Über die Videoüberwachung durch die Polizei auf dem Hauptbahnhofsvorplatz habe ich im 25. JB unter Ziff. 6.1 ausführlich berichtet.

Im Laufe des Berichtsjahres wurde die Dienstanweisung für den Einsatz der Videoüberwachung in der endgültigen Fassung fertiggestellt, welche die gesetzlichen Regelungen aus dem Bremischen Polizeigesetz (BremPolG §§ 29 und 30) umsetzten. So wird z. B. bestimmt, wer Zugriff auf die Videosequenzen haben darf, wie dies dokumentiert wird und wie die Löschung der Videoaufzeichnungen erfolgt. Ferner wird in der Dienstanweisung der Aufzeichnungsbereich festgeschrieben, damit in keine Wohnung (z. B. ab 1. Stock der angrenzenden Häuser) Einblick genommen wird.

Schließlich wurden neue, größere Hinweisschilder aufgestellt, die auf die Videoüberwachung hinweisen. Durch die Vermittlung des Rechtsausschusses wurde auch dieses Thema zufriedenstellend gelöst (vgl. Ziff. 4.2 dieses Berichts).

6.1.5 Projekt „PolMobil" wurde eingestellt

Im Berichtsjahr wurde ich von der Polizei Bremen um datenschutzrechtliche Begleitung eines neuen interessanten Projektes gebeten. Dieses Projekt, „PolMobil" genannt, sah die Möglichkeit der Nutzung von DV-Systemen der Polizei im Streifenwagen bzw. in speziellen Einsatzfahrzeugen sowie durch den Polizeibeamten unmittelbar am Einsatzort vor. Es sollte mit der Telekom und T-Systems durchgeführt werden. In einem Pilotprojekt sollten Möglichkeiten und Risiken des Einsatzes untersucht werden. Erste datenschutzrechtliche Fragestellungen waren:

In welchen Bereichen können mobile DV-Systeme (Notebook, PDA, UMTS-Geräte u. ä.) die Arbeit der Polizei vor Ort unterstützen und wie kann gleichzeitig garantiert werden, dass die Datenübertragung von und an die mobilen DV-Geräte sicher übertragen und die Daten auf den Geräten sicher verarbeitet werden? Wie können Daten verschlüsselt werden, ohne dass die Nutzbarkeit der Geräte dadurch wesentlich beeinträchtigt wird? Mit welchen Verfahren können Daten in die mobilen DV-Systeme übertragen werden und wie werden Daten aus ihnen wieder in die stationären Polizeisysteme zurück übertragen? Wie können die Geräte gegen Zugriff und Manipulation gesichert werden?

Zu diesen Fragen wurden einzelne Szenarien von der Polizei Bremen erarbeitet und mit mir erörtert. Die Zusammenarbeit wurde allerdings abrupt beendet, da das Projekt nicht weiter verfolgt wird. Gleichwohl kann aus der Zusammenarbeit das Fazit gezogen werden, dass eine so frühzeitige Befassung des Datenschutzbeauftragten mit dem Projekt aus Datenschutzsicht die Chance geboten hätte, zu guten und tragbaren Ergebnissen zu gelangen.

6.2 City-Server

Mit City-Server wird ein Gesamtsystem bezeichnet, das alle Straßenzüge in Bremen mit den darin befindlichen Häusern, die aus verschiedenen Blickwinkeln digital fotografiert wurden, enthält. Verbunden sind diese Aufnahmen mit der Angabe geostationärer Punkte, der Angabe des Straßennamens und der Blickrichtung der Aufnahme als Himmelsrichtung sowie dem Aufnahmedatum. Die digitalen Aufnahmen wurden während der Fahrt eines Fahrzeuges hergestellt und auf elektronischen Medien gespeichert. Dabei werden alle auf der Straße befindlichen Personen, Kraftfahrzeuge, Schilder, Gegenstände und sonstigen Begebenheiten abgelichtet, die sich gerade zufällig während der Durchfahrt des Fahrzeuges im Umfeld befunden haben. Es liegt auf der Hand, dass, verbunden mit den genannten Angaben, ein Personenbezug leicht hergestellt werden kann (vgl. auch 25. JB, Ziff. 6.7).

Im Laufe des Jahres gab es verschiedene Überlegungen zu möglichen Einsatzbereichen des Systems in der Verwaltung. Angeschafft war es nun einmal, die Notwendigkeit des Einsatzes wurde von den angesprochenen Stellen unterschiedlich, z. T. zurückhaltend bewertet. Ende 2003 zeichnete sich ab, dass der City-Server ausschließlich für die Aufgabenerledigung verschiedener Behörden im Lande Bremen verwendet werden soll: Durch den City-Server sollen die Aufgaben der Ortsämter, der Feuerwehr, der Polizei und bestimmter bauender und planender Ämter unterstützt werden.

So sollen in den Ortsämtern die so genannten Stadtteilmanager (früher „Sachbearbeiter für kommunale Angelegenheiten") durch den City-Server z. B. bei folgenden Aufgaben unterstützend eingesetzt werden:

— den Baugenehmigungsverfahren,

— der Planung von Radverkehrsanlagen,

— der Überprüfung von Verkehrszeichen,

— dem Aufstellen von Müll- und Sammel-Containern,

— der Bürgerberatung,

— der Beurteilung von Baulücken,

— den Schulwegsicherungsmaßnahmen,

— der Beratung im Zusammenhang mit Entscheidungen der Orts- und Stadtteilbeiräte.

Nachdem zunächst im Bauressort die Einsatzmöglichkeiten kritisch beurteilt wurden, soll nun wohl doch auch hier der City-Server Einzug halten. Die Mitarbeiter der planenden und bauenden Behörden im Bereich des Senator für Bau und Umwelt sollen voraussichtlich bei der Erledigung ihrer Aufgaben durch den Einsatz des City-Servers unterstützt werden. Geprüft wird noch der Einsatz des City-Servers für Zwecke der Feuerwehr und des Katastrophenschutzes und im Rahmen der Polizeiarbeit.

Bereits der Datenschutzausschuss hatte in der letzten Legislaturperiode für den Einsatz des City-Servers ein Datenschutzkonzept eingefordert. Als im Herbst 2003 noch immer kein Konzept vorlag, befasste sich der Rechtsausschuss der Bremischen Bürgerschaft mit dem Thema und unterstützte meine Forderung, den gesetzlichen Verpflichtungen aus dem Bremischen Datenschutzgesetz nachzukommen und endlich ein Einsatz- und Datenschutzkonzept zu erstellen (vgl. Ziff. 4.2 dieses Berichts).

Der Senator für Inneres und Sport hat die Anwendbarkeit des Bremischen Datenschutzgesetzes verneint, gleichwohl hat er auf Drängen des Rechtsausschusses der Bremischen Bürgerschaft den Entwurf eines Einsatz- und Datenschutzkonzeptes vorgelegt. Der noch in Abstimmung befindliche Entwurf sieht vor, dass

— betroffene Bürger, sofern sie selbst abgelichtet wurden, beantragen können, dass sie unkenntlich gemacht oder aber die Bilder aus der Bilddatei gelöscht werden;

— betroffene Bürger, die zwar nicht selbst erkennbar abgelichtet wurden, aber deren Grundstück, Haus, Kraftfahrzeug oder sonstige Belegenheit dargestellt wird, in begründeten Fällen die Löschung dieser Bilder verlangen können;

— vor Präsentationen, z. B. anlässlich einer Beiratssitzung, zu prüfen ist, ob Personen – erkennbar – abgelichtet wurden. In diesen Fällen sind die Personen unkenntlich zu machen oder die Bilder auszublenden;

— von bestimmten Bereichen (z. B. AIDS- oder Drogenberatungsstellen) keine Aufnahme gemacht werden oder die Bilder auszublenden sind.

In dem Entwurf ist vorgesehen, das Einsatzkonzept zunächst für zwei Jahre in Kraft zu setzen und dann zu evaluieren.

6.3 Stadtamt

6.3.1 Die Daten psychisch Kranker beim Stadtamt Bremen

Aus Anlass meiner datenschutzrechtlichen Befassung mit Fragen der Datenverarbeitung im Zusammenhang mit dem Tötungsdelikt in der Neustadt habe ich auch die in solchen Fällen vorgesehene Datenverarbeitung beim Stadtamt geprüft (vgl. Ziff. 8.2.5 dieses Berichts).

Beim Stadtamt Bremen werden die Daten von psychisch kranken Personen, für die eine Unterbringung in einer entsprechenden Behandlungseinrichtung durch den zuständigen Amtsrichter angeordnet worden ist, gespeichert.

Diese Speicherung erfolgt sowohl in Akten als auch in einer elektronisch geführten Datenbank. Bei der elektronischen Datenbank handelt es sich aber um eine veraltete Datenbankanwendung, auf der sich keine zeitgemäßen datenschutzrechtlichen Schutzmechanismen implementieren lassen. So gibt es z. B. keine Protokollierung und die DV-Anwendung lässt keine Trennung für verschiedene Anwender (Vertretung) zu. Da die Datenbank umgestellt werden soll, habe ich keine Änderung mehr für dieses Verfahren verlangt, aber meine Beteiligung bei der Neukonzeption eingefordert. Dabei ist auch die Änderung der Aktenverwaltung für diesen sensiblen Bereich zu prüfen.

6.3.2 Bürger-Service-Center (BSC)

Nachdem das BSC ein Jahr in Betrieb ist, habe ich die Einrichtung einer ersten Datenschutzprüfung unterzogen.

Ich konnte dabei feststellen, dass die mit mir seinerzeit abgestimmten Festlegungen im Planungskonzept hinsichtlich des Schutzes bestimmter personenbezogener Daten, wie z. B. die Daten aus dem Einladungsverfahren nach § 84 Ausländergesetz, umgesetzt sind und besonders geschützt und getrennt von anderen Daten gespeichert werden.

Auch der Bürgerservice „Steuer" wird räumlich und personell vollkommen getrennt abgewickelt. Dieses wird u. a. auch dadurch deutlich, dass die Einrichtung der Finanzbehörden in einem eigenen, selbständigen Gebäudebereich untergebracht sind.

Weiter konnte ich mich davon überzeugen, dass die personenbezogenen Daten nach der Abwicklung des Betreuungsgeschäfts durch das BSC gelöscht werden.

Auch das BSC-eigene Call-Center habe ich geprüft.

Aus dem Prüfgespräch wurde ersichtlich, dass Mitarbeiteraus- und -fortbildung einen hohen Stellenwert einnimmt und Mitarbeitern, die in bestimmten Arbeitsbereichen noch nicht eingearbeitet wurden, keine Bürger für diese Aufgaben zugewiesen bekommen. Dies sichert eine korrekte Datenerhebung und -verarbeitung. Einen Vorteil für die Mitarbeiterinnen und Mitarbeiter stellt die Besuchersteuerung dar, denn sie können sich an Hand dieser Daten bereits auf den Bürger einstellen und eventuell erforderliche Vorarbeiten treffen.

Es fehlen aber noch ein Organisationsplan und ein Datenschutzkonzept. Diese habe ich angemahnt.

6.3.3 Einsatz eines Video-Trupps der Polizei im Auftrag des Stadtamtes auf einem Straßenfest

Im September des Berichtsjahres erhielt ich davon Kenntnis, dass der Bilddokumentationstrupp der Polizei Bremen (Bedo-Trupp) im Auftrag des Stadtamtes – Gaststättenaufsicht – Videoaufnahmen eines Straßenfestes machen wollte. Ein Betroffener beklagte sich bei mir und fragte, ob die Maßnahme zulässig sei.

Meine Nachprüfungen ergaben, dass der Bedo-Trupp bereits im Vorfeld des Festes Videoaufnahmen von den Lokalitäten gemacht hatte, in denen später das Fest stattfinden sollte. Geplant waren weitere Aufnahmen beim laufenden Fest, um so gegebenenfalls bei Auflösung des Festes wegen „drangvoller Enge" Beweismaterial in den Händen zu haben. Wäre dieser Plan in die Tat umgesetzt worden, wären viele Besucher des Festes heimlich videographiert worden. Hierzu kam es allerdings nicht mehr, weil wegen verschiedener Querelen mit den Ordnungskräften der Eigentümer des Grundstückes das Fest kurzerhand absagte.

Gleichwohl bin ich der Sache nachgegangen, um auch für die Zukunft Klarheit zu haben. Ich hatte erhebliche Bedenken gegen ein derartiges Vorgehen, denn die berechtigten Interessen der Betroffenen wären durch eine Videoaufzeichnung erheblich berührt worden. Da weder im Ordnungs-, Versammlungs- noch Polizeirecht eine ausreichende Rechtsgrundlage für derartige Datenerhebungen existiert, habe ich das Stadtamt Bremen um Stellungnahme gebeten.

Nachdem der stellvertretende Leiter des Stadtamtes von der Aktion Kenntnis erhielt, hat er verfügt, dass die Aufnahmen zu löschen sind. Die Verfügung wurde auch dem Bedo-Trupp übermittelt. Die Löschung wurde mir bestätigt. Das Stadtamt Bremen hat mir schriftlich mitgeteilt, dass weitere Videoaufzeichnungen in der Zukunft nicht beabsichtigt seien.

6.3.4 Schwarzarbeit

Das Stadtamt ist im Sommer mit einem Konzept an mich herangetreten, den Eigenbetrieb des Landes Bremen „fidatas-bremen" mit der Auswertung von Datenträgern zu beauftragen, die im Rahmen der Bekämpfung der illegalen Beschäftigung und der Schwarzarbeit beschlagnahmt worden sind. Die zuständige Organisationseinheit beim Stadtamt Bremen verfügt nicht über hinreichende Kenntnisse und die technische Ausstattung, um die konfiszierten Datenträger auszuwerten. Damit dieses datenschutzkonform erfolgt, wurde die „fidatas-bremen" schriftlich mit der Auswertung dieser Datenträger gemäß § 9 Bremisches Datenschutzgesetz (BremDSG) beauftragt. Dabei wurden die Datenverarbeitungsschritte im Einzelnen beschrieben und festgeschrieben.

6.3.5 Waffenrecht

Durch die Änderung des Waffengesetzes vom 11. Oktober 2002 (Bundesgesetzblatt Teil I Seite 3970), das am 1. April 2003 in Kraft trat, sind einerseits die Hürden für die Erteilung einer Waffenerlaubnis angehoben, aber auch die Datenverarbeitungsvorschriften erweitert worden. So wird z. B. bei Antragstellern, die das 25. Lebensjahr noch nicht vollendet haben, ein psychologisches Gutachten angefordert, das die psychische Eignung des Antragstellers zum Führen von Waffen zum Inhalt hat.

Die Meldebehörde erhält über jeden Erlaubnisinhaber Kenntnis und ist verpflichtet, die Tatsache der waffenrechtlichen Erlaubnis in den Meldedatensatz aufzunehmen. Sie ist ferner verpflichtet, die Waffenstelle beim Stadtamt Bremen über Veränderungen des Meldedatensatzes (Fortzug, Aberkennung der bürgerlichen Ehrenrechte u. a.) entsprechend zu informieren.

Anlässlich einer Prüfung beim Stadtamt konnte ich mich davon überzeugen, dass die Daten innerhalb eines DV-Netzes der Waffenstelle verarbeitet werden; Außenanschlüsse bestehen nicht. Datenübermittlungen an andere Stellen werden konventionell abgewickelt.

Zurzeit besteht die Hauptaufgabe der Waffenstelle, die Altdaten in das neue Verfahren zu integrieren. Es liegen noch nicht alle Rechtsverordnungen zu dem neuen Waffenrecht vor.

Die Waffenstelle hat mir zugesagt, sobald die neue, an das neue Waffenrecht angepasste Software „Waffenerlaubnisse" installiert wird, mich unverzüglich zu unterrichten und ein Datenschutzkonzept zu erstellen.

6.4 Übermittlung von Einwohnermeldedaten im Vorfeld der Bürgerschafts- und der Stadtverordnetenwahl

Wie bereits bei früheren Wahlen erhielt ich auch im Vorfeld der letztjährigen Wahlen zur Bremischen Bürgerschaft und zur Bremerhavener Stadtverordnetenversammlung zahlreiche Briefe und Anrufe von Bürgern, die sich bei mir über die Zusendung von Wahlwerbeschreiben beklagten. Ich habe daraufhin die vor den Wahlen durchgeführten Datenübermittlungen an Parteien bei den Meldebehörden in Bremen und Bremerhaven überprüft.

Von der Meldebehörde Bremen sind im Vorfeld der Bürgerschaftswahl aus dem Einwohnermelderegister zu wahlberechtigten Einwohnern, die der Übermittlung ihrer Daten nicht widersprochen haben, Auskünfte an die FDP, die „Schill-Partei" Rechtsstaatlicher Offensive (PRO) und die DVU erteilt worden.

Von der Meldebehörde Bremerhaven sind vor der Bürgerschaftswahl Daten wahlberechtigter Einwohner, die der Datenübermittlung nicht widersprochen haben, an die DVU und zweimal zu unterschiedlichen Altersgruppen an die PRO erteilt worden.

Im Vorfeld der Wahl zur Bremerhavener Stadtverordnetenversammlung, zu der neben den deutschen auch die EU-Staatsangehörigen wahlberechtigt sind, sind von der Meldebehörde Bremerhaven dreimal Auskünfte aus dem Einwohnermelderegister an die DVU erteilt worden. Zu bemängeln war dabei insbesondere, dass die DVU auf ihre erste Anfrage die Daten aller am Wahltage 17-jährigen Einwohner Bremerhavens mit deutscher oder EU-Staatsangehörigkeit erhalten hat, obwohl diese bei der Wahl zur Stadtverordnetenversammlung nicht wahlberechtigt waren. Übermittelt werden dürfen nach § 33 Abs. 1 Meldegesetz (BremMeldG) nur Daten Wahlberechtigter, die der Übermittlung ihrer Daten nicht widersprochen haben. Zudem sind aufgrund der Anfrage zwei Auswertungen aus dem Einwohnermelderegister, bei denen nach deutscher und EU-Staatsangehörigkeit differenziert wurde, durchgeführt worden. Es ist somit bei der Zusammensetzung der Gruppe, deren Daten an die DVU übermittelt worden sind, nach der Staatsangehörigkeit unterschieden worden, was mit § 33 Abs. 1 S. 1 BremMeldG nicht zu vereinbaren ist. Aufgrund der festgestellten Mängel erklärte sich die Meldebehörde Bremerhaven zu einer Änderung des bei der Auskunftserteilung angewandten Verfahrens bereit. Eine eingehendere Überprüfung der Daten, die nach § 33 Abs. 1 BremMeldG übermittelt werden sollen, ist mir zugesagt worden.

Außerdem habe ich gegenüber der Meldebehörde Bremerhaven die verspätete öffentliche Bekanntmachung der Möglichkeit des Widerspruchs nach § 33 Abs. 1 S. 6 BremMeldG bemängelt. Nach § 33 Abs. 1 S. 7 BremMeldG ist der Betroffene außer bei seiner Anmeldung bei der Meldebehörde rechtzeitig (früher acht Monate) vor jeder Wahl oder Stimmabgabe auf das Widerspruchsrecht hinzuweisen. Die öffentliche Bekanntmachung im Hinblick auf die Bürgerschaftswahl war ca. fünf Monate vor dem Wahltermin erfolgt. Bereits vor der öffentlichen Bekanntmachung war bei der Meldebehörde Bremerhaven das Anforderungsschreiben der DVU eingegangen und mit der Erstellung der beantragten Auskunft begonnen

worden. Nach § 33 Abs. 1 S. 2 BremMeldG darf die Meldebehörde Auskünfte in den sechs der Wahl oder Stimmabgabe vorangehenden Monaten erteilen. Die öffentliche Bekanntmachung sollte daher so rechtzeitig erfolgen, dass dem Betroffenen eine angemessene Reaktionszeit – mindestens ein Monat – verbleibt, um von seinem Recht gegenüber der Meldebehörde Gebrauch machen zu können.

Kritisiert habe ich die verspätete öffentliche Bekanntmachung der Widerspruchsmöglichkeit außerdem im Hinblick auf die Datenübermittlungen im Vorfeld der Wahl zur Stadtverordnetenversammlung. Die Meldebehörde Bremerhaven hat sich bereiterklärt, die Bekanntmachung künftig zu einem früheren Zeitpunkt durchzuführen. Für die bevorstehende Wahl zum europäischen Parlament, die am 13. Juni 2004 stattfinden soll, ist die Widerspruchsmöglichkeit bereits am 8. November 2003 bekannt gemacht worden.

7. Justiz

7.1 Anbindung des LSG Niedersachsen-Bremen an das BVN

Ein gutes Beispiel für die in diesem Jahresbericht unter Ziff. 3.1 beschriebene notwendige Öffnung des Bremer Verwaltungsnetzes (BVN) ist die Anbindung des gemeinsamen Landessozialgerichts (LSG) Niedersachsen-Bremen mit Hauptsitz in Celle und einer Zweigstelle in Bremen. In der Zweigstelle arbeiten Bedienstete beider Bundesländer. Zweigstelle und Hauptstelle sind Bestandteil des Virtual Private Network (VPN) „izn Justiz", (izn = Informatikzentrum Niedersachsen, Betreiber des niedersächsischen Landesnetzes), das zum Landesdatennetz Niedersachsen („izn") gehört. Alle Teilnehmer am „izn Justiz" bilden eine virtuelle, geschlossene Benutzergruppe innerhalb des niedersächsischen Landesdatennetzes. Bedienstete des LSG mit Dienstort Celle müssen zukünftig Zugriff auf das bremische Haushaltssystem „Chipsmobil" erhalten, bestimmte Bedienstete des LSG mit Dienstort Bremen sollen Zugriff auf das zentrale Content-Management-System (CMS) und das zentrale „Mitarbeiterportal" erhalten. Das BVN soll an dieser Stelle also in klar definiertem Umfang in Richtung Landesdatennetz Niedersachsen geöffnet werden. In Abstimmung zwischen dem Senator für Finanzen (SfF) als Betreiber des BVN, dem IuK-Ausschuss der bremischen Justiz, dem Eigenbetrieb Judit, der BreKom, dem izn und mir ist es gelungen, hierfür eine Lösung zu schaffen, die dem neuen Struktur- und Sicherheitskonzept (Ziff. 3.1 dieses Berichts) folgt. Weil ich relativ spät beteiligt wurde und einige Informationen fehlten, konnte ich meine Zustimmung erst mit einiger Zeitverzögerung geben. Die Umsetzung des Projektes ist nach meinen Informationen noch um den Jahreswechsel 2003/2004 vollzogen worden. Im kommenden Jahr beabsichtige ich, die konkrete Umsetzung des Konzeptes einer Prüfung zu unterziehen.

7.2 Absenderangaben bei Mahnsachen des Amtsgerichts Bremen

Ein Bürger teilte mir mit, dass er eine Einschreibesendung von der Mahnabteilung des Amtsgerichts Bremen erhalten hat. Hierbei wurde ein Briefumschlag mit folgender Absenderangabe verwendet:

Amtsgericht Bremen – Abteilung für Mahnsachen – Postfach 10 79 43 – 28079 Bremen

Der Betroffene war mit der Art der Absenderangabe nicht einverstanden, da hieraus ersichtlich sei, dass die Einschreibesendung einen Mahnbescheid enthält. Hiermit sei nach außen für Dritte (z. B. Postmitarbeiter) erkennbar, dass gegen den Betroffenen ein Mahnverfahren eingeleitet worden war. Der Betroffene fühlte sich hierdurch in seinen datenschutzrechtlichen Belangen verletzt.

Ich bin an das Amtsgericht Bremen herangetreten und habe um Abhilfe gebeten. Das Amtsgericht Bremen hat daraufhin neue Umschläge bestellt, die den datenschutzrechtlich bedenklichen Zusatz „Abteilung für Mahnsachen" nicht mehr aufweisen. Darüber hinaus wurde auch die Materialverwaltung beauftragt, Umschläge aus anderen Verfahren auf gleichartige Zusätze zu prüfen.

7.3 Veröffentlichung der Insolvenzbekanntmachungen im Internet

Die Insolvenzgerichte in Bremen und in Bremerhaven lassen seit Herbst 2003 die öffentlichen Bekanntmachungen in Insolvenzsachen nicht mehr wie bisher in den

örtlichen Tageszeitungen abdrucken, sondern veröffentlichen diese im Internet unter „www.insolvenzbekanntmachungen.de". Die Möglichkeit hierzu ist durch § 9 Insolvenzverordnung (InsO) und die darauf gestützte Rechtsverordnung geschaffen worden, in der die näheren Einzelheiten sowie die datenschutzrechtlichen Anforderungen dieser Art der Bekanntmachung geregelt sind. Erreicht werden sollen neben der Kostenersparnis dadurch vor allem eine leichtere und schnellere Informationsmöglichkeit interessierter Dritter sowie eine effizientere Bearbeitung der erforderlichen Veröffentlichungen durch die Gerichte.

Die Web-Site wird dabei federführend vom Land Nordrhein-Westfalen betreut, das derzeit aufgrund von Verwaltungsvereinbarungen die Insolvenzbekanntmachungen aus bereits acht Bundesländern veröffentlicht. Bereits dies erscheint unter Datenschutzgesichtspunkten als nicht ganz bedenkenfrei, da die Zusammenführung an einer zentralen Stelle der bisher nach Gerichten getrennten Veröffentlichungen das Recht des von der Insolvenz betroffenen Schuldners wegen der damit einhergehenden erhöhten Aufmerksamkeit und leichten Zugänglichkeit ungleich stärker berührt.

Zum Tätigwerden habe ich mich aus einem anderen Grunde veranlasst gesehen: Auf mein Betreiben hin, unterstützt von den anderen Landesdatenschutzbeauftragten und insbesondere durch den Bundesbeauftragten für den Datenschutz, sind in die bundesgesetzlichen Regelungen Anforderungen zu technischen Schutzvorkehrungen aufgenommen worden, die z. B. verhindern sollen, dass Insolvenzschuldner auch lange nach Ablauf ihrer Insolvenz immer noch mit diesem Makel gebrandmarkt weiter im Internet gespeichert sind (vgl. 23. JB, Ziff. 7.2). § 9 InsO verlangt für die auf der Internetseite veröffentlichten Insolvenzdaten einen dem Stand der Technik entsprechenden Kopierschutz. Dadurch soll verhindert werden, dass die dem Nutzer angezeigten Informationen von ihm auf seinem Rechner gespeichert werden können und er diese weiterverarbeiten kann. Dieser Kopierschutz war bisher nur für einen Teilbereich der Veröffentlichungen umgesetzt. Auf meine Intervention hin ist dieser Kopierschutz nun für sämtliche abgerufene Daten eingeführt worden. Gleichwohl halte ich die technische Umsetzung noch nicht für hinreichend, da sie nur über ein Java-Skript realisiert ist und dies auch von wenig versierten Anwendern leicht umgangen werden kann. Es ist zweifelhaft, ob diese Lösung tatsächlich dem Stand der Technik entspricht. Es ist daher geplant, die technische Arbeitsgruppe der Datenschutzbeauftragten mit diesen Fragen zu befassen.

Die Datenschutzkonformität habe ich leider erst prüfen können, nachdem die bremischen Gerichte bereits erste Insolvenzbekanntmachungen auf der Internetseite eingestellt hatten, da ich von der Teilnahme Bremens an den Internetveröffentlichungen erst aus der Tagespresse erfahren habe. Ich erlaube mir daher noch einmal auf die Vorschrift des § 27 Abs. 3 BremDSG hinzuweisen, die eine rechtzeitige Information des Landesbeauftragten für den Datenschutz beim geplanten Einsatz neuer Informationstechniken fordert, um zu den datenschutzrechtlichen Auswirkungen Stellung nehmen zu können.

7.4 Datenschutzkontrolle bei JUDIT

Im Nachgang zu den strafrechtlichen Ermittlungen wegen Zugriffen auf kinderpornografische Internetseiten im Jahr 2002 habe ich – entsprechend meiner Ankündigung im letzten Jahresbericht (vgl. 25. JB, Ziff. 7.1) – abermals Datenschutzkontrollen vorgenommen. Konkretes Ziel war die Prüfung, ob die im Zuge der damaligen Ermittlungen aufgrund richterlicher Beschlüsse erstellten Protokolle über die Internetzugriffe noch im DV-System vorhanden sind. Bei dem für die DV-Betreuung der Justiz zuständigen Eigenbetrieb JUDIT wurde die Löschung versichert.

Für einen Zeitraum von vier Wochen im August 2002 war JUDIT ebenso wie anderen Dienststellen durch richterlichen Beschluss eine personenbezogene Protokollierung der Internetnutzung auferlegt worden. In diesem Zeitraum wurden ca. 2,8 Millionen Protokoll-Datensätze aufgezeichnet, was der Beachtung der datenschutzrechtlichen Bestimmungen besondere Bedeutung zukommen lässt. Vor diesem Hintergrund war es datenschutzrechtlich fragwürdig, einen verantwortlichen Mitarbeiter von JUDIT in die strafrechtlichen Ermittlungen einzuschalten und mit der Aufbereitung und Auswertung der Protokolldaten zu beauftragen. Dies hätte wegen der zum Teil besonders sensiblen Daten, die einen Einblick auch in intime

Lebensumstände von Kollegen gewähren können, nur durch die Polizei oder einen externen Sachverständigen vorgenommen werden sollen. Zudem kann auf diese Weise eine in diesem Falle unzulässige Selbstkontrolle unterbunden werden.

Die Datenschutzkontrolle habe ich des Weiteren ausgedehnt auf die generelle Protokollierung der dienstlichen und privaten Internetnutzung durch die Mitarbeiter im Bereich von JUDIT. Dabei hat sich herausgestellt, dass für einen Zeitraum von 90 Tagen die Internetzugriffe arbeitsplatzbezogen mit IP-Adresse und aufgerufener URL umfassend protokolliert wurden. Nach diesem Zeitraum war eine automatische Löschung vorgesehen. Ich habe in meinem Prüfvermerk auf die grundsätzliche Unzulässigkeit einer solchen Aufzeichnung hingewiesen und um Änderung gebeten. Zu den rechtlichen Rahmenbedingungen verweise ich insofern auf Ziff. 11.3 dieses Berichts.

7.5 Ungeprüfte Aktenherausgabe bei Forschungsprojekt zur Telekommunikationsüberwachung

Neben dem unter Ziff. 2.5 dieses Berichts beschriebenen Forschungsprojekt des Max-Planck-Institutes gab es noch ein weiteres Forschungsvorhaben zur Telekommunikationsüberwachung der Universität Bielefeld mit dem Namen „Wirksamkeitsbedingungen von Richtervorbehalten bei Telefonüberwachungen". Ich war bei diesem Forschungsprojekt insoweit zuständig, als auch Daten bei der Staatsanwaltschaft Bremen erhoben bzw. von dieser an die Universität Bielefeld übermittelt wurden. Für das Forschungsprojekt wurden Aktenanalysen aus insgesamt 554 Telefonüberwachungen (aus 173 Strafverfahren) und 56 Interviews mit Polizei, Staatsanwälten und Richtern geführt. Die Ergebnisse dieses Forschungsprojektes wurden 2003 veröffentlicht. Anders als das Forschungsprojekt des Max-Planck-Institutes, das mit der zuständigen Datenschutzkontrollbehörde in enger Zusammenarbeit ein Datenschutzkonzept erarbeitete, ist das Forschungsprojekt der Universität Bielefeld im Hinblick auf die Einhaltung der datenschutzrechtlichen Anforderungen in Bremen unzulänglich verlaufen. Ich wurde weder in der Vorbereitungsphase noch während des konkreten Projektes in das Verfahren einbezogen. Auch mit der für die Universität Bielefeld zuständigen Landesbeauftragten für den Datenschutz von Nordrhein-Westfalen ist keine konkrete Abstimmung erfolgt. Eine solche Abstimmung und die Vorlage eines Datenschutzkonzeptes wären jedoch dringend ratsam gewesen, da in den von Bremen zur Verfügung gestellten Strafakten sensible personenbezogene Daten enthalten waren. Zudem wurden auch während der Interviews personenbezogene Daten erhoben. Da ich erst nach Abschluss des Forschungsvorhabens davon erfuhr, konnte ich nur noch nachträglich feststellen, das datenschutzrechtliche Belange nicht hinreichend berücksichtigt wurden.

Zweifelhaft ist zunächst, ob überhaupt schon zu dem Zeitpunkt, wo die Strafakten eingesehen bzw. diese an die Universität Bielefeld herausgegeben wurden, eine die Datenverarbeitung legitimierende gesetzliche Grundlage bestand. § 476 der Strafprozessordnung (StPO) – der eigens für derartige Vorhaben geschaffen wurde – ist erst im August 2000 in Kraft getreten. In einem Gespräch mit der Staatsanwaltschaft Bremen wurde deutlich, dass das Forschungsprojekt Ende 1999 begonnen hat.

Weiterhin wurden die gesamten Akten ohne vorherige Entfernung der Gesprächsprotokolle weitergegeben. Nur hochsensible Aktenbestandteile, wie medizinische Sachverständigengutachten, die nicht im Zusammenhang mit den zur erforschenden Fragen standen, wurden entfernt. Alle anderen Bestandteile wurden ohne vorherige Selektion weitergegeben. Dies ist aus datenschutzrechtlicher Sicht zu beanstanden. Es hätte eine einzelfallbezogene Prüfung stattfinden müssen, welche Daten für den konkreten Forschungszweck erforderlich waren. Nur Aktenbestandteile, die bis hin zur richterlichen Entscheidung entstanden sind, konnten für die Bewertung des Forschungsvorhabens entscheidungserheblich gewesen sein, da es in diesem Projekt um die Wirksamkeitsbedingungen des Richtervorbehalts ging und nicht um die Rechtmäßigkeit oder Effizienz der Telekommunikationsüberwachung. Allenfalls in den Fällen, in denen eine zweite Anordnung ergangen ist, wäre die Übersendung auch dieses Teils für das Forschungsvorhaben von Relevanz. Das hätte aber im Einzelfall geprüft werden müssen.

Schließlich wurde auch nicht geprüft, ob – wie es § 476 Abs. 1 S. 2 StPO vorsieht – die Informationen in anonymisierter Form hätten weitergegeben werden können. Über eine Anfertigung von Kopien und deren Schwärzung von personenbezogenen Daten hatte man sich keine Gedanken gemacht.

Diese Fehler hätten vermieden werden können, wenn mit mir ein Datenschutzkonzept abgestimmt worden wäre. Dies hätte Regelungen bezüglich des Zugangs zu den Daten, Aktenlagerung, Anonymisierung und Kopierbeschränkungen enthalten müssen.

Zwischen dem Senator für Justiz und Verfassung, der Staatsanwaltschaft Bremen und mir besteht Einigkeit darüber, dass das Forschungsprojekt in Bezug auf die einzuhaltenden datenschutzrechtlichen Vorschriften unbefriedigend verlaufen ist. Für die Zukunft wurde verabredet, dass kommende Forschungsprojekte mit mir abgestimmt werden. Außerdem wurde dem Senator für Justiz und Verfassung und der Staatsanwaltschaft Bremen ein Merkblatt für den Datenschutz bei Forschungsprojekten übersandt.

8. Gesundheit und Krankenversicherung

8.1 Bremische Krankenhäuser

8.1.1 Das fortgeschriebene Bremische Krankenhausdatenschutzgesetz

Am 26. Februar 2003 trat das Gesetz zur Änderung des Bremischen Krankenhausdatenschutzgesetzes (BremKHDSG) in Kraft (Brem.GBl. S. 47). Das BremKHDSG bietet jetzt eine zeitgemäße Rechtsgrundlage für die Digitalisierung der Patientendokumentation in den Krankenhäusern und für den digitalisierten Austausch von Patientendaten der bremischen Krankenhäuser untereinander sowie mit Arztpraxen und anderen Leistungserbringern im Gesundheitswesen in vernetzten Strukturen (ausführlich vgl. 25. JB, Ziff. 8.6).

8.1.1.1 Interne Vernetzung und digitale Behandlungsdokumentationen

§ 3 Abs. 2 und 3 BremKHDSG bestimmen einerseits, dass die digitalisierte Behandlungsdokumentation nur den Ärzten, Pflegekräften und Therapeuten aus der behandelnden Fachabteilung im Krankenhaus zur Verfügung steht und von hier aus für Zugriffe aus anderen Fachabteilungen freigegeben werden muss. Andererseits erlaubt es unter besonderen Umständen bei bestimmten Voraussetzungen derartige Zugriffe durch mit- oder nachbehandelnde Ärzte, Pflegekräfte und Therapeuten auch ohne vorherige Freigabe. Hierfür muss aber das Dokumentationssystem durch technische Vorkehrungen gewährleisten, dass die Zugriffe einer Begründung bedürfen, dass sie nur zeitlich begrenzt eröffnet werden, dass jeder Zugriff dem behandelnden Arzt angezeigt wird und dass die Zugriffe mit Verantwortlichen und Begründungen protokolliert werden. Das in den kommunalen Krankenhäusern im Lande Bremen eingesetzte Dokumentationssystem bietet, entsprechend weiter entwickelt, die technische Grundlage für dieses Verfahren. Nach Abstimmung zwischen den Krankenhäusern und mir ist ein entsprechender Entwicklungsantrag gestellt worden. Der Softwareentwickler sagte eine stufenweise Realisierung zu. Bis Mitte 2004 soll das Verfahren den gesetzlichen Anforderungen voll gerecht werden. Ich werde mich davon überzeugen. Zudem wird es darauf ankommen, dass es in bremischen Krankenhäusern tatsächlich in der weiter entwickelten Form installiert wird.

8.1.1.2 Externe Vernetzung und digitale Behandlungsdokumentationen

Nach § 2 Abs. 4 BremKHDSG dürfen bremische Krankenhäuser Patientendaten mit der Möglichkeit automatisierter Abrufe zum Zwecke der Behandlung durch Ärzte, Pflegekräfte und Therapeuten aus anderen Krankenhäusern oder aus einer ambulanten Praxis speichern. Es ist aber durch technische Vorkehrungen zu gewährleisten, dass der Patient zuvor gegenüber dem Abrufenden in den einzelnen Abruf eingewilligt hat, der Abruf dem Krankenhaus angezeigt wird und die externen Abrufe, in für Auswertungen geeigneter Form, protokolliert werden. Die Einwilligung des Patienten, so bestimmt es jetzt § 2 Abs. 2 BremKHDSG, muss nicht in Schriftform erteilt werden, wenn seine Mitwirkung durch technische Maßnahmen sichergestellt ist.

Im Sommer des Berichtsjahres gab eine Informationsveranstaltung des Gesundheitsressorts Gelegenheit, verantwortliche Mitarbeiter der bremischen Krankenhäuser über die Neuregelungen zu informieren. Zuvor hatte ich die neuen Bestimmungen in einem Schreiben dargestellt, dass ich zeitgleich mit ihrem In-Kraft-Treten an alle Krankenhäuser im Lande Bremen gerichtet hatte. Darin hatte ich sie auch auf eine sie bereits nach altem Recht treffende Verpflichtung hingewiesen. Patientendaten, die ein externer Netzpartner aus dem Informationssystem eines bremischen Krankenhauses abgerufen hat, sollen weiterhin einen gleichwertigen Schutz genießen. Dazu hat das jeweilige Krankenhaus seinen Partner zu verpflichten. Ich hatte die angeschriebenen Krankenhäuser gebeten, mich darüber zu informieren, mit welchen niedergelassenen Ärzten oder Angehörigen anderer Heilberufe ein Datennetzverbund eingerichtet oder geplant sei. Den eingegangenen Antworten war zu entnehmen, dass eine derartige Vernetzung noch nicht eingerichtet worden war.

In der Folgezeit führte ich Gespräche mit dem Krankenhaus St.-Jürgen-Straße über dessen Netzprojekt „iBON" (Integratives Bremer Onko-Hämatologie-Netzwerk) und dem Rotes-Kreuz-Krankenhaus (RKK) über dessen Projekt „e-health-connect". Aus den mir vorgelegten und erläuterten Produktbeschreibungen geht hervor, dass sie die Möglichkeit zu einer gesetzeskonformen Verarbeitung von Patientendaten bieten. Ich machte die Gesprächspartner nochmals schriftlich und mündlich auf die Neuregelungen zur externen Vernetzung aufmerksam und erhielt die Zusage, man werde diese berücksichtigen und mir vor der Einstellung von Patientendaten in vernetzte Strukturen die gesetzlich vorgegebenen Verfahrensbeschreibungen und Datenschutzkonzepte vorlegen. Inzwischen wurde in der Antwort des Senats vom 11. November 2003 auf die Kleine Anfrage der Fraktion der CDU in der Bremischen Bürgerschaft zu „Strukturen des Aufnahme- und Entlassungsmanagements kommunaler Krankenhäuser" (Bürgerschafts-Drs. [Landtag] 16/73) berichtet, das RKK sei mit Haupteinweisern, d. h., mit niedergelassenen Ärzten, bereits jetzt elektronisch vernetzt, das ZKH St.-Jürgen-Straße „teilweise". Am 9. April 2003, kurze Zeit nach dem BremKHDSG, trat ein Ortsgesetz in Kraft, mit dem zum 1. Januar 2004 die vier Krankenhäuser der Stadtgemeinde Bremen unter dem Dach einer Holdinggesellschaft in gGmbH umgewandelt werden sollen (Brem.GBl. S. 175). Bei der Umsetzung des Ortsgesetzes ist das BremKHDSG als vorrangiges Landesrecht zu beachten, insbesondere dürfen die beteiligten Kliniken die Daten ihrer Patienten weiterhin nur mit deren Einwilligung untereinander austauschen bzw. aus ihren Dokumentationssystemen abrufen.

Schließlich erfuhr ich vor kurzem aus dem Gesundheitsressort, man arbeite dort gemeinsam mit der Selbstverwaltung im Gesundheitswesen, der Wissenschaft und potentiellen Partnern aus der Industrie an einem Konzept für den Einsatz der elektronischen Gesundheitskarte (§ 291 a SGB V, vgl. Ziff. 8.3.3.2 dieses Berichts) und für die Telematikinfrastruktur im Gesundheitswesen einer möglichen Testregion Bremen. Auch in diesem Zusammenhang werde ich darauf achten, dass die oben dargestellten gesetzlichen Anforderungen erfüllt werden.

8.1.2 Hörscreening bei Neugeborenen

Eine flächendeckend geplante Untersuchung bei Neugeborenen im Land Bremen ist das Hörscreening. Das Hörscreening erfolgt über die apparative Ableitung so genannter otoakustischer Emissionen (OAE) in den ersten Tagen nach der Geburt eines Neugeborenen. Ziel ist es, die überwiegende Mehrzahl angeborener oder während der Schwangerschaft erworbener Hörstörungen zu bestätigen bzw. auszuschließen und so eine frühzeitige Behandlung des Kindes zu ermöglichen. Im Land Bremen wird durchschnittlich ein Kind pro Monat mit einer schwerwiegenden Hörstörung geboren. Bei im Mittel einer Hörscreeninguntersuchung pro Neugeborenem fallen in Bremen rechnerisch rund 18 Untersuchungen pro Tag an.

Bei der Ausgestaltung des Verfahrens ist insbesondere noch klärungsbedürftig, ob das Screening als freiwillige Untersuchung angeboten wird und damit der Einwilligung der Eltern bedarf oder ob der Hörtest als Teil des Behandlungsvertrags im Rahmen der Geburt zu sehen ist.

Unabhängig davon muss aber über das Hörsceening informiert werden und es muss über eventuelle mit der Untersuchung verbundene Risiken für das Kind so-

wie die relativ hohe Anzahl falsch-positiver Testungen aufgeklärt werden. Der Ablauf des Screening-Verfahrens ist für die Eltern transparent zu machen.

Daneben ist ein Tracking-Verfahren vorgesehen, mit dem die Eltern erreicht werden sollen, die trotz auffälligen Befunds nicht zur Nachuntersuchung erschienen sind. Ein solches Tracking kann jedoch nicht mehr Teil des Behandlungsvertrags betreffend die Geburt gesehen werden, so dass dafür jedenfalls die Einwilligung der Eltern eingeholt werden muss.

Darüber hinaus habe ich die Beteiligten auf die datenschutzrechtlichen Anforderungen an ein solches Verfahren sowie auf die Verpflichtung gemäß § 8 Bremisches Datenschutzgesetz (BremDSG) hingewiesen, vor Beginn der Verarbeitung von Echtdaten ein Datenschutzkonzept zu erstellen. Das Projekt wird in Expertenkonferenzen weiter vorangetrieben; ich werde dort die datenschutzrechtlichen Belange einbringen.

8.2 Öffentlicher Gesundheitsdienst

8.2.1 Gemeinsame Eingabestelle des Krebsregisters und der Tumornachsorgeleitstelle

Das Bremer Krebsregister ist durch das am 1. Oktober 1997 in Kraft getretene Gesetz über das Krebsregister der Freien Hansestadt Bremen (BremKRG) errichtet worden (vgl. 20. JB, Ziff. 14.1, 21. JB, Ziff. 11.1 und 22. JB, Ziff.8.1).

Aufgabe der Vertrauensstelle nach dem Krebsregistergesetz ist es, Meldungen von Ärzten über Daten von Patienten, die an Krebskrankheiten leiden, entgegen zu nehmen, auf Schlüssigkeit und Vollständigkeit zu prüfen und den epidemiologischen Datensatz (medizinische Daten ohne Personenbezug) an die Registerstelle weiterzugeben. Diese wertet die Daten nach bundeseinheitlichen Vorgaben aus und übermittelt sie an das Robert-Koch-Institut.

Die Vertrauensstelle ist verpflichtet, sicherzustellen, dass die bei ihr gespeicherten Daten nicht zu anderen als den gesetzlich definierten Zwecken genutzt werden können. Darüber hinaus muss sie verhindern, dass die Daten unbefugt eingesehen und genutzt werden können (§ 4 Abs. 1 Satz 2 i. V. m. § 6 Abs. 2 BremKRG). Die Vertrauensstelle löscht die medizinischen Daten der gemeldeten Patienten umgehend nach deren Übermittlung an die Registerstelle, spätestens aber nach Ablauf von drei Monaten. Sie speichert danach die Identitätsdaten nur noch in verschlüsselter Form.

Die Aufgabe der Tumornachsorgeleitstelle ist u. a. die Erfassung der von den behandelnden Ärzten gemeldeten Behandlungs- und Untersuchungsdaten zum Krankheitsverlauf mit dem Ziel der Erstellung einer auswertbaren Behandlungsdokumentation zum Zweck der Nachsorge für jeden gemeldeten Patienten in genau festgelegtem Umfang. Grundlage hierfür ist die Einwilligung der Patienten, während die Datenübermittlung an das Krebsregister auf gesetzlicher Grundlage mit Widerspruchsmöglichkeit der Patienten erfolgt.

Die Datenbestände beider Stellen werden aufgrund der unterschiedlichen Aufgabenstellungen und gesetzlichen Verpflichtungen in verschiedenen lokalen EDV-Netzen ohne externe Anschlüsse verarbeitet. Eigenständige Datenschutzkonzepte bilden die Grundlage für eine datenschutzgerechte Verarbeitung der Daten.

Es wurde in der Praxis jedoch sehr schnell deutlich, dass sich die in die Systeme auf der Grundlage unterschiedlicher Meldebogen einzugebenden Datenmengen weitgehend überschneiden.

Um die Arbeit der doppelten Eingabe zu vermeiden, wurde in Abstimmung mit mir ein Konzept für eine zentrale Eingabestelle der Vertrauensstelle des Bremer Krebsregisters und der Tumordokumentations-/Nachsorgeleitstelle von beiden Stellen entwickelt. Die grundsätzliche Anforderung war dabei, das in den Datenschutzkonzepten festgelegte Datenschutzniveau der beiden Stellen nicht zu unterschreiten.

Technisch wurde dieses Niveau bisher u. a. durch die Eigenständigkeit der beiden Netze, d. h. deren physikalische Trennung, umgesetzt. Um die Möglichkeit einer

gemeinsamen Eingabe zu schaffen, musste die physikalische Trennung der beiden Server aufgehoben und die Datensicherheit auf der logischen Ebene erbracht werden.

Dabei wurden u. a. folgende wesentliche Maßnahmen vorgesehen:

— Authentifizierungsverfahren

  Anmeldung am Netz, am Datenbankserver und an der Datenbank. Steuerung des Zugriffs auf Objekte in der Datenbank über Berechtigungen. Die vier Sicherheitsebenen verhindern bei entsprechender Konfiguration den Zugriff nicht berechtigter Benutzer auf die Daten.

— Die Erhaltung eigener Datenbanken für die beiden Stellen

  Es werden beispielsweise aus dem System der zentralen Eingabestelle für die Vertrauensstelle nur die Daten extrahiert und in die Datenbank der Vertrauensstelle übernommen, auf die die Vertrauensstelle gemäß dem Krebsregistergesetz Zugriff haben darf. Die gemeinsame Eingabe von Stammdaten wird über eine für die Mitarbeiterinnen und Mitarbeiter beider Stellen im Zugriff liegende Tabelle realisiert. Die zentrale Eingabestelle ist eine virtuelle Datenbank ohne eigene Dateien. Die Datenspeicherung erfolgt nach Aktivierung entsprechender Filterfunktionen in Abhängigkeit von Widerspruch oder/und Einwilligung der Patienten.

Durch diese Struktur werden die Authentifizierungen der Mitarbeiterinnen und Mitarbeiter je nach Organisationszugehörigkeit unterschiedlich definiert, es wird kein gemeinsamer Datenbestand aufgebaut.

Im Juni des Berichtsjahres habe ich die zentrale Eingabestelle aufgesucht, um zu prüfen, ob die im Datenschutzkonzept beschriebenen Datenschutzmaßnahmen wirkungsvoll in die Praxis umgesetzt worden sind.

Als Ergebnis konnte ich feststellen, dass die zentrale Eingabestelle die rechtlich gebotene Trennung der Datenbestände der beiden Stellen auf logischer Ebene abgebildet hat.

8.2.2 Mammographie Screening

8.2.2.1 Projekt Bremen

In den Vorjahren habe ich mich intensiv mit der Vorbereitung und der Anfangsphase des Bremer Mammographie Screening-Projekts befasst, auch im vergangenen Jahr begleitete ich die Fortentwicklung des Projektes.

Im 25. JB hatte ich unter Ziff. 8.3 berichtet, dass es dem Projekt schwer fiel, angemessene Archivräume für seine medizinische Dokumentation zu finden. Inzwischen ist mir mitgeteilt worden, im Gebäude der Frauenklinik des ZKH St.-Jürgen-Straße, demselben Gebäude, in dem das Projekt selbst untergebracht ist, seien geeignete, sichere Räumlichkeiten gefunden worden.

Im Berichtsjahr trug mir das Screening-Zentrum vielfältige Vorstellungen zur Änderung des abgestimmten Datenschutzkonzepts vor. In der Regel konnte ich sie akzeptieren. Allerdings bin ich bestrebt, die Grundlagen des Konzepts nicht in Frage stellen zu lassen. Zu diesen gehört die Anonymisierung der Meldedaten der Frauen, die auch nach einer Nacheinladung zum Screening diese nicht wahrnehmen (vgl. 24. JB, Ziff. 8.4). So sendet die Untersuchungsstelle die Einladungsliste mit dem Vermerk, welche Eingeladenen den vorgeschlagenen Termin wahrgenommen haben, nicht mehr täglich, sondern nur noch wöchentlich zurück. Dies reiche aus, da die Einladungsstelle die Liste erst zwei Wochen später für das Erinnerungsschreiben an die nicht erschienenen Frauen mit einem neuen Terminvorschlag benötige. Zudem bewahrt die Untersuchungsstelle die Einladungslisten für die Dauer von drei Wochen nach dem Einladungsdatum auf. Als Grund hierfür wird angegeben, häufig wendeten sich Frauen, denen der angebotene Untersuchungstermin nicht passe, nicht an die Einladungsstelle, sondern kämen zu einem späteren Termin direkt zur Untersuchungsstelle. Die müsse man dann erst an die Einladungsstelle verweisen, bevor man sie untersuchen könne. Es steht zu erwar-

ten, dass das Datenschutzkonzept immer einmal wieder bei der Lösung praktischer Fragen als hinderlich empfunden wird. Dies aber sollte nicht dazu führen, dass fortlaufend die Festlegungen des Datenschutzkonzepts aufgeweicht werden, die direkt den politischen Konsens bei der Beschlussfassung über das Projekt umzusetzen bestimmt sind. Positiv bewerte ich, dass das fortgeschriebene Datenschutzkonzept jetzt zusagt, dass die Einladungsstelle die Daten der Nicht-Teilnehmerinnen etwa drei Wochen nach dem diesen angebotenen zweiten Untersuchungstermin anonymisiert.

Schließlich musste ich mich, angesprochen durch die Ärztekammer Bremen, damit auseinander setzen, dass es immer wieder vorkommt, dass untersuchte Frauen beim Warten auf die Abklärungsuntersuchung nach auffälligem Befund im Warteraum der Befundungsstelle unerwartet auf Nachbarinnen in der gleichen Situation treffen. Es leuchtet ein, dass dies geeignet sein kann, das Unbehagen in dieser angespannten Situation noch zu steigern. Das Screening-Projekt wies darauf hin, dass Einladungs- und Untersuchungsverfahren und damit auch zeitlich sich unmittelbar anschließende Nachuntersuchungen aus guten Gründen wohngebietsweise organisiert seien und sich deshalb die beklagten Zusammentreffen nicht immer vermeiden ließen. Überdies sei die räumliche Situation beengt. Die Leitung des ZKH St.-Jürgen-Straße ihrerseits sieht keinen Anlass, hier Abhilfe zu schaffen. Die räumliche Situation sei nicht schlechter als in vergleichbaren anderen Einrichtungen der Klinik. Ich bedauere es in Übereinstimmung mit der Ärztekammer, dass die Verantwortlichen so wenig Engagement zeigen, durch das Projekt produzierte Härten für davon Betroffene für die Zukunft auszuschließen.

8.2.2.2 Bundesweites Screening als Regelangebot

Veranlasst durch einen Beschluss des Deutschen Bundestages bereitete im Berichtsjahr der Bundesausschuss der Ärzte und Krankenkassen auf der Grundlage des § 92 SGB V eine Änderung der Krebsfrüherkennungsrichtlinien mit dem Inhalt vor, das Mammographie Screening bereits vor Beendigung und Auswertung der Modellprojekte bundesweit als Teil der medizinischen Regelversorgung für Frauen im Alter von 50 bis 69 Jahren einzuführen. Auf Wunsch des Bundesbeauftragten für den Datenschutz wurde auch mir Gelegenheit gegeben, meine Vorstellungen unmittelbar einzubringen. Dabei bemühte ich mich, auf die für das Bremer Projekt verabschiedeten Rechtsgrundlagen hinzuweisen und sie zu erläutern. Ich wollte damit insbesondere der Gefahr vorbeugen, dass die neuen Früherkennungsrichtlinien den in Bremen geltenden rechtlichen Rahmen außer Acht lassen. Zunächst aber hatte der Bundesausschuss nicht bedacht, dass ohnehin keine Rechtsgrundlage dafür besteht, die Daten der Frauen, die das freiwillige Angebot nicht wahrnehmen, weiter zu verarbeiten. Deren Identitätsdaten müssen – wie in Bremen gewährleistet – nach erfolglosem Einladungsverfahren anonymisiert werden. Personenbezogene Daten des Bremischen Krebsregisters – entsprechendes gilt auch für in den Krebsregistern anderer Bundesländer gespeicherte Daten – dürfen für einen Abgleich mit Befunden des Screenings nur dann zur Verfügung gestellt werden, wenn zuvor die betroffenen Frauen, vermittelt durch ihren behandelnden Arzt, der Vertrauensstelle des Registers ihr Einverständnis gegeben haben.

Dem Bundesausschuss musste zudem vermittelt werden, dass das Recht der Gesetzlichen Krankenversicherung – das SGB V und die Früherkennungsrichtlinie – allein keine ausreichende Rechtsgrundlage für ein Screening-Programm bietet, das mit Hilfe von Meldedaten alle, nicht nur die gesetzlich krankenversicherten, Frauen einer Arbeitsgruppe einbezieht, dass vielmehr hierfür – wie in Bremen im Gesetz über den Öffentlichen Gesundheitsdienst – noch die landesrechtlichen Voraussetzungen geschaffen werden müssen. Ich hoffe, dass der in Bremen gefundene Konsens und die positiven Erfahrungen mit dem auf seiner Basis durchgeführtem Modellprojekt Eingang finden in die zum Redaktionsschluss dieses Berichts mir noch nicht bekannten neuen Bundesregelungen.

8.2.3 Interne Vernetzung des Gesundheitsamtes Bremerhaven

Im Jahr 2002 habe ich aufgrund des mir vorgelegten Datenschutz- und Datensicherungskonzeptes im Zusammenhang mit der Einführung der Fachanwendung „Octoware" ausgewählte Sicherheitsaspekte geprüft (vgl. 25. JB, Ziff. 8.2). Die

modular aufgebaute Fachanwendung unterstützt die Gesamtheit der Arbeits- und Verfahrensabläufe, insbesondere die der einzelnen Fachabteilungen des Gesundheitsamtes. Im Jahr 2002 liefen die Module Infektionsschutz, Kommunalhygiene, Trinkwasser und Badewasser bereits im Echtbetrieb. Im Jahr 2003 sind die Module Amtsärztlicher Dienst und Sozialpsychiatrischer Dienst dazugekommen. Als Ergebnis der Prüfung traten einige Sachverhalte zu Tage, die aus datenschutzrechtlicher Sicht verbesserungsbedürftig waren. Meine im Jahr 2003 vorgenommene Nachprüfung ergab, dass die festgestellten Schwachstellen weitgehend beseitigt worden sind.

So sind die Möglichkeiten verschiedener im System standardmäßig angelegter Administrationsrollen weitgehend eingeschränkt worden. Die vorinstallierten Administrationsrollen für Externe zur Durchführung der Fernwartung durch die Softwarefirma wurden deaktiviert, so dass keine der Firma zugeordneten Rollen mehr im System aktiv sind. Probleme werden über die Hotline gelöst. Somit ist ausgeschlossen, dass im Rahmen der Wartung Externe auf sensible Daten des Gesundheitsamtes zugreifen können.

Die Möglichkeit der internen Systemadministration des Gesundheitsamtes, fachmodulübergreifend auf alle sensiblen Daten des Gesundheitsamtes zugreifen zu können, wurde eingeschränkt. Der Administrationsbereich ist dadurch auf Kernaufgaben, wie beispielsweise die Datenpflege, begrenzt. Die umfangreichen Anwendungsrechte in den Fachmodulen, um Anwenderinnen und Anwender in der Systemanwendung unterstützen zu können, bestehen nicht mehr. Für diese Aufgaben sind für die einzelnen Module Support-Accounts geschaffen worden. Optimal wäre es gewesen, wenn der Support durch Mitarbeiterinnen und Mitarbeiter der entsprechenden Abteilungen des Gesundheitsamtes gewährleistet werden könnte. Dies ist aber aus personellen Gründen nicht möglich. Das Gesundheitsamt hat jedoch ein entsprechendes Administrationskonzept entwickelt und die erforderliche Struktur bereits geschaffen.

Darüber hinaus hat das Gesundheitsamt ein Revisionskonzept entwickelt, das insbesondere eine Transparenz der Administrationstätigkeiten für den behördlichen Datenschutzbeauftragten ermöglicht. Diese Revision erfolgt vierteljährlich als Stichprobe der Zugriffsprotokolle mithilfe einer Excel-Tabelle insbesondere mit dem Ziel, Zugriffe auf sensible Dokumente zu prüfen. Gleichzeitig werden die Sicherheitseinstellungen anhand einer Checkliste geprüft, so dass Veränderungen des Systemzustandes in Bezug auf die Sicherheitseinstellungen erfasst, dokumentiert und gegebenenfalls wieder rückgängig gemacht oder verbessert werden können. Den Zugriff auf die Protokolldatei hat der behördliche Datenschutzbeauftragte des Gesundheitsamtes.

Auch das im letzten Jahresbericht (vgl. 25. JB, Ziff. 8.2) erörterte Problem des direkten Zugriffs auf vertrauliche Dokumente im Rahmen der zentralen Dateien der einzelnen Fachbereiche wurde auf technischer und organisatorischer Ebene gelöst. Die Systemadministration macht den Mitarbeiterinnen und Mitarbeitern das systemseitig mögliche Verfahren zum Schutz der Dokumente bekannt. Die Mitarbeiterinnen und Mitarbeiter werden dazu verpflichtet, die Dokumente, die einem besonderen Vertrauensschutz unterliegen, entsprechend zu schützen.

Als abschließendes Prüfergebnis konnte ich feststellen, dass das Gesundheitsamt Bremerhaven ein datenschutzgerechtes Verfahren implementiert hat.

8.2.4 Sprachstandserhebung bei Schulanfängern

Zu Beginn des Berichtsjahrs wurde in Regie des Jugendressorts eine Sprachstandserhebung durchgeführt, in die alle schulpflichtigen Kinder und so genannten Karenzkinder einbezogen wurden. Dies hatte Verunsicherung bei einigen Eltern ausgelöst, die fragten, ob ihre Kinder an der Erhebung teilnehmen müssten oder ob es sich um eine freiwillige Untersuchung handelte; immerhin wurden auch Daten aus sensiblen Bereichen, wie dem familiären Umfeld, erhoben.

Die angestrebte obligatorische Teilnahme aller Kinder, also auch derjenigen, die kein Kindertagesheim (KTH) besuchen, hat nur dann eine rechtliche Grundlage, wenn die Sprachstandserhebung als Teil der Schuleingangsuntersuchung nach § 36 Bremisches Schulgesetz, durchgeführt wird. Die Zuständigkeit dafür liegt ge-

mäß § 14 Abs. 6 des Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG) bei dem Schulärztlichen Dienst des Gesundheitsamtes. Das Gesundheitsamt war aber nur an einem Punkt öffentlich hervorgetreten, nämlich in einem an die Eltern der im Sommer 2003 zur Einschulung anstehenden Kinder versandten Informationsblatt.

Daher setzte ich mich mit dem Ressort in Verbindung, um eine Abstimmung des Verfahrens zu erzielen und insbesondere die notwendigen Arbeitsschritte für die Gestaltung einer Datenverarbeitung im Auftrag des Gesundheitsamtes zu erörtern. Dazu gehörte zunächst, dass die Möglichkeit der Einflussnahme des Gesundheitsamtes gewahrt und es gegenüber den Erhebungskräften weisungsbefugt ist sowie die Einhaltung der ärztlichen Schweigepflicht auch durch die Erhebungskräfte. Schließlich muss das Gesundheitsamt für die Erhebungskräfte, Träger und Eltern klar als Ansprechpartner ersichtlich sein.

Nachdem ich darauf innerhalb eines halben Jahres keine inhaltliche Reaktion erhalten hatte, erklärte sich der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales erst auf Betreiben des Rechtsausschusses bereit, an der Umsetzung der datenschutzrechtlichen Anforderungen mitzuwirken.

Daraufhin wurde mit meiner Beratung ein schriftlicher Auftrag des Gesundheitsamtes an den Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales gemäß § 9 Bremisches Datenschutzgesetz (BremDSG) erarbeitet, der die vorgenannten Festlegungen enthält. Aus ihm geht auch hervor, dass die Universität ausschließlich anonymisierte Erhebungsbogen erhält und das Deckblatt mit den Identitätsdaten beim Ressort verbleibt. Nach Abschluss der Auswertungen durch die Universität werden die Bögen und die Auswertungen dem Ressort zugeleitet. Anschließend werden im Auftrag des Gesundheitsamtes die Deckblätter und die Bögen beim Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales zusammengeführt und die Eltern über das Förderangebot informiert. Die Deckblätter sowie die Erhebungsbogen und die Liste der zu fördernden Kinder werden danach dem Gesundheitsamt überstellt und dort aufbewahrt. Die ebenfalls neu konzipierte Elterninformation macht den Ablauf des Verfahrens transparent. Somit wurde erreicht, dass die Sprachstandserhebung nun datenschutzkonform durchgeführt wird. Hilfreich wäre jedoch eine Regelung der Untersuchung im Schuldatenschutzgesetz.

8.2.5 Sozialpsychiatrie – Zweckbindung und Verhinderung von Gewalttaten

Ende 2000 verabschiedete die Bremische Bürgerschaft ein neues Gesetz über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG, Brem.GBl. S. 471 vom 22.12.2000). Dessen § 47 Abs. 1 unterwirft die zur Durchführung des Gesetzes erhobenen und gespeicherten Daten, insbesondere Untersuchungsergebnisse und ärztliche Zeugnisse, einer besonders strengen Zweckbindung. Ihre Übermittlung, etwa an die Vollzugspolizei, ist nur gestattet, wenn der Betroffene eingewilligt hat oder wenn eine gegenwärtige Gefahr für Leib oder Leben des Betroffenen oder Dritter nicht anders abgewendet werden kann. Die Bestimmung richtet sich in erster Linie an die Sozialpsychiatrischen Dienste (SPsD) der Gesundheitsämter und an die Kliniken, in denen Kranke nach dem PsychKG untergebracht sind, nach ihrem Satz 2 aber auch an die Ortspolizeibehörden, die nach § 9 PsychKG die Anordnung einer Unterbringung beantragen und ihrem Antrag ein ärztliches Zeugnis beifügen muss, das i. d. R. der SPsD ausgestellt hat. Der Senat hatte in der Vorlage, mit der er das PsychKG in die Bremische Bürgerschaft einbrachte, die strikte Zweckbindung mit der herausragenden Bedeutung der in Frage stehenden Daten für den Persönlichkeitsschutz der psychisch Kranken begründet. Hingegen darf die Polizei Daten über psychisch Kranke, die sie selbst erhoben oder von anderen als den oben genannten Stellen erhalten hat, im Rahmen der §§ 36 d, 36 f Bremisches Polizeigesetz (BremPolG) für polizeiliche Zwecke nutzen oder ihrerseits übermitteln. Auch das Vormundschaftsgericht Bremen, das über die Unterbringung psychisch Kranker zu entscheiden hat, ist durch das bremische PsychKG nicht daran gehindert, im Rahmen der §§ 69 k und 70 n des seine Aufgabenerfüllung regelnden Bundesgesetzes über die Freiwillige Gerichtsbarkeit (FGG) über seine Entscheidungen und Erkenntnisse Mitteilungen etwa an die Vollzugspolizei zu machen.

Im Sommer des Berichtsjahres wurde in der Stadtgemeinde Bremen eine psychisch kranke Frau beschuldigt, eine Nachbarin getötet zu haben (vgl. Ziff. 6.3.1

dieses Berichts). Zuvor war sie zweimal nach Vorlage eines sozialpsychiatrischen Gutachtens im ZKH Bremen-Ost untergebracht worden, das Vormundschaftsgericht hatte eine Betreuung angeordnet und wieder aufgehoben, die Vollzugspolizei war wiederholt, zuletzt auch durch das spätere Opfer um Schutz vor der Beschuldigten angerufen, tätig geworden. Die genannten Stellen hatten hierbei vielfältig kooperiert und im Rahmen der jeweils für sie geltenden gesetzlichen Bestimmungen Daten ausgetauscht. Im polizeilichen Informationssystem ISA waren fremdgefährdende Handlungen der Beschuldigten gespeichert.

Zunächst war nach der Tat daran gedacht worden, dass die Unterbringungsstelle im Stadtamt, der Vollzugspolizei, zwecks Speicherung in ISA Mitteilung von allen Unterbringungsverfahren, auch von bereits zurückliegenden Fällen, machen sollte. Dies aber hätte auch die Kranken betroffen, von denen eine Gefahr für andere gar nicht ausgeht. Die nach der Tat durch die Ressorts für Inneres, Justiz und Gesundheit eingerichtete Arbeitsgruppe hingegen schlägt vor, die Mitteilungen zu Unterbringungsverfahren auf Kranke mit Fremdgefährdungspotential zu beschränken. Aber auch hier musste ich auf die Zweckbindungsregelung des § 47 Abs. 1 PsychKG hinweisen. Das Stadtamt dürfe nicht schon dann ihm durch den SPsD im Rahmen eines Unterbringungsverfahrens zugänglich gemachte Daten an die Polizei übermitteln, wenn ein Fremdgefährdungspotential erkennbar sei. Voraussetzung sei vielmehr, dass im Einzelfall eine gegenwärtige Gefahr für Leib oder Leben anderer nur durch Einschaltung der Polizei abgewendet werden kann. Die Arbeitsgruppe hat darauf vorgeschlagen, den bereits in anderen Fällen die strenge Regelung des § 47 PsychKG abschwächenden § 48 PsychKG zu ändern. Nach dieser Vorschrift ist bereits jetzt der SPsD befugt, die Führerschein- bzw. Waffenscheinstelle der Ortspolizeibehörde zu unterrichten, wenn er befürchtet, dass ein psychisch Kranker sich oder andere durch das Führen von Kraftfahrzeugen oder durch den Umgang mit Waffen gefährden könnte. Ich habe erklärt, dass eine maßvolle Erweiterung des § 48 PsychKG denkbar sei. Die strenge Zweckbindung nach § 47 Abs. 1 PsychKG verbiete allerdings schon jetzt nicht, dass das Stadtamt seine Unterbringungsakten daraufhin prüfe und bewerte, ob im Einzelfall wegen Fremdgefährdung durch Beschluss des Vormundschaftsgerichts die Unterbringung angeordnet worden sei und gegebenenfalls auf der Grundlage von § 36 d BremPolG zum Zwecke der Gefahrenabwehr der Polizei davon Mitteilung mache, denn der Gerichtsbeschluss wird ihm nach FGG durch das Gericht mitgeteilt und fällt daher nicht unter die Zweckbindung nach § 47 PsychKG.

8.3 Gesetzliche Krankenversicherung

8.3.1 Disease Management Projekte

Ich hatte im letzen Jahr darüber berichtet, dass die im Rahmen des Risikostrukturausgleichs (RSA) zwischen finanzstarken und finanzschwachen gesetzlichen Krankenkassen verankerten Disease Management Programme (DMP) zu neuen Formen der Verarbeitung patientenbezogener medizinischer Daten durch bürokratische Organisationen – hier die Gesetzliche Krankenversicherung (GKV) und das Bundesversicherungsamt (BVA) – führen (vgl. 25. JB, Ziff. 8.10). Mittlerweile ist von einem milliardenteuren Flop die Rede. Unter den Beteiligten (GKV, Ärzte und BVA als Schaltstelle für den RSA) hat längst die Zeit der Schuldzuweisungen eingesetzt. Es wollte von vornherein nicht so recht einleuchten, warum Qualität und Wirtschaftlichkeit der Behandlung chronisch Kranker sich dadurch verbessern sollen, dass ausführliche bis ins Einzelne vorgeschriebene ärztliche Dokumentationen über die Behandlung der GKV und dem BVA übermittelt werden. Genau dies aber schreibt die RSA-Verordnung (RSAV) in ihrem § 28 f vor, übrigens ein Negativbeispiel für eine durch Überkomplexität schier unverständlich gewordene Rechtsnorm. Dass dieses Novum – der Zugriff auf ärztliche Behandlungsdokumentationen war bislang Ärzten, Krankenhäusern und den Medizinischen Diensten der GKV vorbehalten – aus Datenschutzsicht höchst bedenklich ist, liegt auf der Hand. Inzwischen habe ich die Vereinbarungen für das im Land Bremen angelaufene Projekt für an Diabetes Mellitus Erkrankte erhalten. Danach sollen die beteiligten Krankenkassen die ihnen in versichertenbezogener Form zugeleiteten ärztlichen Dokumentationen ausschließlich zum Zweck der Information der jeweils betroffenen Versicherten nutzen dürfen. Zugleich wird versichert, die Dokumentationen seien nur den für das Programm zuständigen Mitarbeitern zugänglich. Daraus schließe ich, dass die Dokumentationsdaten nicht zu anderen Zwecken genutzt werden sollen und von den für andere Zwecke gespeicherten Ab-

rechnungsdaten getrennt bleiben sollen. Zudem gehe ich vorerst davon aus, dass diese Regelungen auch bei weiteren, auf andere chronische Erkrankungen gerichtete Projekte der gleichen Art eingehalten werden.

Inzwischen ist eine weitere mit den DMP verbundene Problematik in den Vordergrund getreten: Nach dem mir vorgelegten Bremer DMP-Vertrag sollen die beteiligten Ärzte vorerst bis zur Beendigung des öffentlichen Ausschreibungsverfahrens ihre Dokumentationen nicht direkt an die GKV bzw. an eine von dieser mit der Kassenärztlichen Vereinigung (KV) gebildete Arbeitsgemeinschaft (Arge) übermitteln, sondern an ein gewerbliches Unternehmen. Dieses soll die Dokumentationen auf ihre Vollständigkeit und Plausibilität überprüfen, die erweiterte Fassung der Dokumentationen pseudonymisieren, die Dokumentationen, teils versichertenbezogen, teils pseudonymisiert, jedenfalls aber in elektronischer Form der jeweils zuständigen Krankenkasse zuleiten und schließlich die ihr durch die Ärzte zugeleiteten Unterlagen archivieren.

Als erstes warf dieser Vertrag die Frage auf, ob die GKV, die KV und die Arge damit nicht die Erfüllung ihnen obliegender Aufgaben an eine andere Stelle übertragen haben. Dies wäre mangels gesetzlicher Befugnis nicht zulässig. Da aber zugleich bis ins Einzelne gehende zwingende Vorgaben für die Erledigung der übertragenen Aufgaben, vor allem der Prüfung der Dokumentationen auf Plausibilität, vereinbart worden waren, konnte ich die Auffassung der Vertragspartner akzeptieren, dass es sich um eine im Rahmen des § 80 SGB X zulässige Datenverarbeitung im Auftrag handelt.

Eine andere Frage aber ist, ob dieser Auftrag einem gewerblichen Unternehmen erteilt werden durfte. Ursprünglich hatte man in Bremen die Vertrauensstelle des Krebsregisters, eine öffentliche Stelle, einschalten wollen. Das BVA, dem der Vertrag zwecks Zulassung vorgelegt werden musste, hatte aber unter Hinweis auf das Vergaberecht eine EU-weite öffentliche Ausschreibung verlangt. Eine mögliche Kollision des Vergaberechts mit dem Sozialdatenschutz wurde dabei nicht thematisiert. Deshalb bereitet man derzeit die verlangte Ausschreibung vor. Vorläufig wurde der Auftrag INTER-FORUM Data-Services in Leipzig erteilt.

Nach § 80 Abs. 5 Nr. 2 SGB X dürfen Sozialleistungsträger wie GKV, KV und Arge zwar grundsätzlich auch nicht-öffentliche Stellen mit der Verarbeitung von Sozialdaten beauftragen, vorausgesetzt, die übertragenen Arbeiten können bei diesen erheblich kostengünstiger erledigt werden. Der Auftrag darf aber gemäß der Vorschrift nicht den gesamten Datenbestand des Auftraggebers umfassen. Der überwiegende Teil des Datenbestandes muss weiterhin beim Auftraggeber gespeichert werden. Einer der Auftraggeber ist die Arge, eine in § 219 Abs. 2 SGB V u. a. zur Förderung der Versorgung chronisch Kranker vorgesehene Form der Kooperation zwischen der GKV und KV. § 28 f Abs. 2 Nr. 1 RSAV sieht im Rahmen von DMP-Verträgen ausdrücklich die Einschaltung einer Arge zur Pseudonymisierung des Versichertenbezugs der erweiterten Dokumentationen vor. Der gesamte durch die Arge in Erfüllung dieser Aufgabe zu speichernde Datenbestand aber wird derzeit, und zwar auf Dauer, durch den Auftragnehmer gespeichert. Dies aber widerspricht der Vorgabe des SGB.

Ich habe die bremischen Vertragspartner hierauf hingewiesen, angesichts der Vorgabe des BVA aber eine Beanstandung nicht ausgesprochen. Meiner Rechtsauffassung hat sich die überwiegende Mehrheit der Datenschutzbeauftragten der anderen Länder angeschlossen. Nachdem der Bundesbeauftragte für den Datenschutz (BfD) diese Bedenken dem BVA und dem Bundesministerium für Gesundheit und Soziale Sicherung (BMGS) vorgetragen hatte, verstand sich dieses dazu, als Lösung eine Änderung der RSAV vorzuschlagen: Die Pflicht zur Einschaltung einer Arge soll gestrichen und Auftraggeber die GKV selbst werden. Dies würde dazu führen, dass die GKV selbst in vollem Umfang auf das Pseudonymisierungsverfahren Einfluss nehmen könnte. Da dieses aber gerade dazu bestimmt ist, den Zugriff der GKV auf Versichertendaten zu begrenzen, ist dieser Vorschlag – insoweit stimme ich dem BfD zu – inakzeptabel. Demgegenüber schlägt der BfD vor, die an DMP teilnehmenden Ärzte selbst zu Auftraggebern zu erklären. Diesem Vorschlag aber kann ich ebenso wenig abgewinnen: Eine öffentliche Verantwortung für das Pseudonymisierungsverfahren würde völlig aufgegeben. Ohnehin werden beide Vorschläge der eigentlichen datenschutzrechtlichen Problematik nicht gerecht: Durch die DMP-Regelungen erhält die GKV, ob mit oder ohne

Pseudonymisierung eines Teils der Daten, erstmals Zugriff auf die ärztlichen Dokumentationen selbst, nicht mehr nur wie bislang auf Abrechnungsdaten. Die Pseudonymisierung sollte datenschutzrechtliche Akzeptanz bewirken. Das Gegenteil ist die Folge: Nun sollen die Dokumentationen bei gewerblichen Unternehmen gespeichert werden, wodurch sie den Schutz der ärztlichen Schweigepflicht und des ärztlichen Zeugnisverweigerungsrechts verlieren. Zum Redaktionsschluss dauerten die Erörterungen noch an.

8.3.2 Datenerhebung der Krankenkassen bei Ärzten über arbeitsunfähige Versicherte

Erkrankt ein Arbeitnehmer, so erhält er gemäß § 44 SGB V i. V. m. § 3 Abs. 1 S. 1 Entgeltfortzahlungsgesetz von seiner gesetzlichen Krankenversicherung nach sechs Wochen Krankengeld. In diesem Zusammenhang war es bei Bremer Krankenkassen Praxis, den behandelnden Arzt anzuschreiben und um eine Einschätzung des Gesundheitszustands des Patienten zu bitten. Dabei sollte ein Formular verwendet werden, auf dem neben der Diagnose auch die Frage gestellt wird, ob es bei der Überwindung der Arbeitsunfähigkeit andere Probleme (z. B. Arbeitsplatz, Muttersprache, soziales Umfeld) gibt.

Diese Vorgehensweise der Krankenkassen wurde im Bremer Diskussionsforum Gesundheitsrecht problematisiert. Aus datenschutzrechtlicher Sicht ist eine solche Datenübermittlung durch den Arzt unzulässig. Denn ohne eine Einwilligung des Patienten und ohne Entbindung des Arztes von seiner Schweigepflicht durch den Patienten darf ein Arzt die geforderten Daten nicht an die Krankenkasse weitergeben. Andererseits trifft den Patienten, der die Leistung von Krankengeld begehrt, eine Mitwirkungspflicht nach § 60 Abs. 1 Nr. 1 SGB I. Es besteht also eine Freiwilligkeit insoweit, als dem Versicherten die Wahl bleibt zwischen Entbindung von der Schweigepflicht oder Verzicht auf die Zahlung von Krankengeld. Darüber ist der Versicherte von seiner Krankenkasse zu informieren. Außerdem ist er darauf hinzuweisen, dass die Krankenkasse möglicherweise den behandelnden Arzt befragt; hierzu sollte sich die Krankenkasse – etwa bei Beantragung der Leistung – eine Entbindung des Arztes von der Schweigepflicht geben lassen. Bei der Anfrage an den Arzt kann dieser dann auf das Vorliegen der Schweigepflichtentbindung hingewiesen werden.

Ob allerdings die Mitwirkungspflicht nach § 60 Abs. 1 Nr. 1 SGB I sich auch auf die Offenbarung anderer als rein medizinischer Daten erstreckt, ist fraglich. Bezüglich der Frage nach „anderen Problemen", die mit dem Gesundheitszustand nicht direkt im Zusammenhang stehen, ist noch im Diskussionsforum zu klären, ob eine Weigerung des Versicherten, diese Auskunft durch den Arzt geben zu lassen, nicht unsanktioniert bleiben muss oder ob die Preisgabe dieser Informationen noch zur Mitwirkungspflicht gehört.

Hat der Versicherte in die Arztanfrage seitens seiner Krankenkasse eingewilligt, so ist der Arzt gemäß § 100 SGB X zur Erteilung der Auskunft verpflichtet. Darauf, sowie auf diese Vorschrift, müssen die Ärzte durch die Krankenkassen nach § 67 a SGB X hingewiesen werden.

Es wurde ein Papier mit diesen rechtlichen Vorgaben sowie Vorschlägen zu deren Umsetzung erarbeitet, das demnächst im Diskussionsforum Gesundheitsrecht als Ergebnis diskutiert wird. Die Krankenkassen sagten bereits zu, ihre bisherige Praxis zu ändern.

8.3.3 Gesundheitsreform 2003

8.3.3.1 Erweiterte Datenbasis für Krankenkassen

Am 19. November 2003 ist das Gesundheitsmodernisierungsgesetz (GMG) im Bundesgesetzblatt I (S. 2190) veröffentlicht worden. Mit ihm ist zum 1. Januar 2004 das SGB V, das die Gesetzliche Krankenversicherung (GKV) regelt, umfassend novelliert worden. In der Begründung der Bundestagsdrucksache werden als Ziele des GMG angeführt, in der GKV die vorhandenen Mittel effektiver einzusetzen und die Qualität der medizinischen Versorgung deutlich zu steigern. Es ist nicht Aufgabe des Datenschutzes, diese Ziele zu bewerten oder zu prüfen, ob das Gesetz geeignet ist, diese Ziele zu befördern. Hingegen ist es Aufgabe des Daten-

schutzes, aufzuzeigen, welche datenschutzrechtlich bedenklichen Entwicklungen das Gesetz befördern wird oder kann.

Vorweg sei klargestellt, dass aus Datenschutzsicht selbstverständlich zu akzeptieren ist,

— dass die GKV prüft, ob eine ärztliche Abrechnung rechnerisch richtig ist und ob der Patient leistungsberechtigt ist,

— dass die GKV prüft, ob ärztliche Abrechnungen plausibel sind oder vielmehr Anzeichen für unkorrektes Verhalten zeigen,

— dass GKV und Ärztekammer gemeinsam in gesetzlich geregelten Verfahren Wirtschaftlichkeit und Qualität der Behandlung einzelner Ärzte prüfen,

— dass die GKV die Behandlung im Einzelfall durch ihre medizinischen Dienste nachprüfen lässt und diese daraufhin ärztliche Unterlagen zur in Frage stehenden Behandlung anfordern.

Das GMG gibt jedoch deshalb Anlass zur Sorge, weil es über den bislang im SGB V vorgesehen Umfang hinaus der GKV zusätzliche medizinische Daten ihrer Versicherten zur Verfügung stellt,

— ohne dass plausibel ist, warum die Datensätze in diesem Umfang die Identifizierung des einzelnen Versicherten ermöglichen müssen,

— ohne dass die Zwecke der Nutzung ausreichend präzise festgelegt werden und

— ohne dass hinreichend bestimmt ist, dass die Daten nur zu festgelegten Zwecken genutzt werden dürfen.

Die Ärzte rechnen ihre Leistungen über die Kassenärztlichen Vereinigungen (KVen) mit der GKV ab. Als Ausgleich dafür, dass im SGB V seit 1990 eine Automatisierung von Abrechnungsverfahren und Datenbasis der GKV angestrebt wird (vgl. u. a. § 303 Abs. 3 SGB V), bestimmte der Gesetzgeber zugleich, dass der Versichertenbezug der Abrechnungsunterlagen über die Leistungen der niedergelassenen Ärzte bei den KV „herausgefiltert" und nicht an die GKV übermittelt werden solle (vgl. §§ 295 Abs. 2 SGB V, a. F.). Obgleich in der Folgezeit durch Verträge zwischen GKV und Ärzteschaft mannigfach durchlöchert, hatte dieser Filter doch zur Folge, dass jedenfalls im Regelfall die GKV die Leistungen der niedergelassenen Ärzte für ihre einzelnen Patienten nicht quartalsübergreifend überprüfen konnte. Dies war seither immer wieder Gegenstand lebhafter Diskussionen.

Ministerium und Datenschützer erzielten im Jahr 1999 Einigung darüber, dass der GKV die von ihr angestrebte bessere, für ihre Prüfaufgaben transparentere Datenbasis zur Verfügung gestellt werden solle, dass aus diesem Grunde der dargestellte Filter entfallen solle, dass zugleich aber die Daten der Versicherten auf ihrem Wege zur GKV pseudonymisiert und nur bei Vorliegen verbindlich definierter Voraussetzungen depseudonymisiert werden sollten, (vgl. hierzu 22. JB, Ziff. 8.8).

Dieses bis zu einem Gesetzesbeschluss des Deutschen Bundestages gediehene Vorhaben fiel der Blockade des Bundesrates gegen den zustimmungspflichtigen Teil der Gesundheitsreform 2000 zum Opfer, obgleich die datenschutzrechtlich relevanten Neuregelungen nicht Grund der Meinungsbildung im Bundesrat waren. In der Folgezeit einigten sich Ministerium und GKV darauf, dass die GKV zwecks „Fallmanagement" den Versichertenbezug der Abrechnungsdaten benötigt; man nutzte dieses Argument aber nur für die Ablehnung der Pseudonymisierung des Versichertenbezugs in den Abrechnungsdaten der Krankenhäuser, Apotheken und der sonstigen Leistungserbringer, tastete aber – wohl um des Friedens mit der Ärzteschaft willen – die Filterfunktion der KV bei der Abrechnung der ärztlichen Leistungen nicht an. Damit blieb es dabei: Weiterhin war die GKV nicht in der Lage, die ärztliche Behandlung einzelner Patienten über ein Quartal hinaus zu überprüfen, weder versichertenbezogen noch nur fallbezogen ohne Identifizierung des jeweiligen Versicherten.

Dies blieb auch so bis zum ersten Entwurf für ein GMG, den im Juni 2003 die Bundesregierung und die Koalitionsfraktionen den Gesetzgebungsorganen vor-

legten. Erst der nach den zwischen Koalition und Opposition geführten Konsensgesprächen neugefasste Entwurf vom September 2003 bestimmte im neugefassten § 295 Abs. 2 SGB V, dass die GKV auch die Abrechnungen der Ärzte über ihre Leistungen „versichertenbezogen" erhalten solle.

Dies wird zur Folge haben, dass die GKV nun alle für einen Versicherten erbrachten medizinischen Leistungen – auch über längere Zeiträume hinweg – verknüpfen, prüfen und bewerten kann. Da sie die Abrechnungsdaten auch in maschinenlesbarer Form erhält, ist die GKV mit Hilfe der inzwischen eingesetzten bzw. in der Entwicklung befindlichen Datenbanksysteme auch technisch dazu in der Lage oder wird es in absehbarer Zeit sein.

Macht es aus Datenschutzsicht überhaupt Sinn, dass die GKV zwar die Abrechnungen der Krankenhäuser und Apotheken mit, die der Ärzte hingegen weiterhin ohne Versichertenbezug erhält? Der Antwort vorweggeschickt sei, dass der Grund für die bisherige Ungleichbehandlung der Abrechnungen der unterschiedlichen Kategorien von Leistungserbringern nicht in erster Linie der Datenschutz, sondern eher die gesetzlich garantierte Selbstverwaltung der Ärzte und mit ihr die gesetzlich garantierte Rolle der KV im Rahmen der Abrechnung der Leistungen niedergelassener Ärzte war. Die Differenzierung ist jedenfalls nicht in erster Linie durch den Datenschutz erzwungen. Vielmehr hätte aus dessen Sicht das SGB V spätestens seit 1990, d. h. mit dem Beginn der automatisierten Verarbeitung von Abrechnungsdaten, präzise und verbindlich regeln müssen, zu welchen Zwecken die GKV die ihr übermittelten versichertenbezogenen Abrechnungsdaten nutzen darf. Dies ist leider nicht geschehen und ist auch nicht durch das GMG nachgeholt worden. Deshalb wird sich in naher Zukunft folgendes Bild bieten:

— Die GKV erhält mit den Abrechnungsdaten aller Leistungserbringer im Gesundheitswesen eine umfassende Datengrundlage über die gesundheitliche Situation und die Inanspruchnahme medizinischer Leistungen durch ihre Versicherten.

— Diese Daten liegen ihr automatisiert vor.

— In der GKV werden Datenbanksysteme entwickelt bzw. eingesetzt, die es ermöglichen bzw. mit denen ausdrücklich beabsichtigt wird, diese Daten zu vielfältigen sowie zu im Einzelnen nicht festgelegten Zwecken im Rahmen von Data Warehouse-Systemen zu verknüpfen und auszuwerten. Die Versicherten werden, obgleich die Rollen doch etwas anders verteilt sein dürften, als Kunden bezeichnet, ihre Daten als Kundendaten. Und mit diesen will man eben in gleicher Weise wie etwa ein Versand- oder ein Kreditunternehmen mit den Daten seiner Kunden verfahren. Als Beispiel sei nur das im Auftrag des Bundesverbandes der Allgemeinen Ortskrankenkassen entwickelte Datenbanksystem SAM genannt.

— Das SGB V sieht auch in der Neufassung durch das GMG nicht vor, dass die GKV die Abrechnungsdaten nur zu ganz bestimmten im Gesetz aufgeführten Zwecken nutzen darf. Vielmehr erlauben die insoweit weitgehend unverändert verbliebenen, in der Tendenz eher aufgeweichten Regelungen die bereits bekannten Auslegungen, mit denen die GKV auch Nutzungen mit dem Ziel der Überprüfung des gesundheitlichen Verhaltens einzelner Versicherter oder der Behandlung einzelner Versicherter durch einzelne Ärzte rechtfertigt.

Der Bundesdatenschutzbeauftragte hatte, unterstützt durch die Landesdatenschutzbeauftragten, im Gesetzgebungsverfahren Bedenken gegen die kurzfristig eingebrachten Verschlechterungen des GMG-Entwurfs vorgetragen und Vorschläge für Änderungen des Gesetzentwurfs vorgelegt, vgl. hierzu die Entschließung der Konferenz (Ziff. 18.12. dieses Berichts). Mehr konnte jedoch nicht erreicht werden.

— Das Plenum des Bundestages stellte fest, dass im Hinblick auf den Wegfall der bisherigen fallbezogenen Datenübermittlungen (d. h. die jetzt versichertenbezogenen Übermittlungen) bei Abrechnungen ambulanter ärztlicher Leistungen Erkenntnisse über die Erforderlichkeit und Verhältnismäßigkeit der Maßnahmen besonders wichtig seien. Er gab seiner Erwartung Ausdruck, dass angesichts der Bedeutung des Grundrechts auf informationelle Selbstbestimmung die GKV die Umsetzung der Neuregelung in Bezug auf den daten-

schutzrechtlichen Grundsatz der Datenvermeidung und Datensparsamkeit evaluieren und hierbei die Möglichkeit von Pseudonymisierungsverfahren einbeziehen solle. Bis Ende 2008 solle dann das Bundesministerium für Gesundheit und Soziale Sicherung dem Bundestag darüber berichten.

— Der Bundestagsausschuss für Gesundheit und Soziale Sicherung hatte zuvor noch dafür plädiert, es sei durch technische und organisatorische Maßnahmen (seitens der GKV) sicherzustellen, dass zur Verhinderung der Entstehung von Versichertenprofilen bei den Krankenkassen eine sektorenübergreifende Zusammenfassung der Abrechnungs- und Leistungsdaten unzulässig sei, und dass die Krankenkassen die Daten nur zu Abrechnungs- und Prüfzwecken nutzen dürften.

Die Frage drängt sich auf, warum diese Erwartungen des Bundestages sich nicht im Gesetzestext wiederfinden? Warum sind sie im Plenum bzw. gar im Ausschuss „hängen geblieben", während der zuvor zum GMG zwischen Koalition und Opposition verhandelte Konsens in anderen Punkten durchaus noch geändert wurde. Über die Gründe, warum dies in diesem aus der Sicht des Datenschutzes wesentlichen Punkt nicht geschah, können von hier aus nur Vermutungen angestellt werden. Die Evaluation soll nicht etwa ein unabhängiger Gutachter, sondern die GKV selbst vornehmen. Ob ein Ausschussbeschluss Auslegung und Anwendung eines anders lautenden Gesetzes beeinflussen kann, scheint fraglich, deshalb ist zweifelhaft, ob die Beschlüsse auf die künftige Praxis der GKV einwirken werden.

Fazit: Durch eine in „letzter Minute" in das GMG eingefügte Änderung erhält die GKV umfassend Kenntnis über die medizinische Versorgung jedes Einzelnen ihrer Versicherten, ohne dass das Gesetz angemessen präzise und verbindlich die Grenzen erlaubter Nutzungen festgelegt hätte. Die bei ihr Versicherten werden für die GKV jetzt zu „gläsernen Patienten".

8.3.3.2 Elektronische Gesundheitskarte und JobCard

Meine Kritik am GMG richtet sich nicht gegen dessen Regelung zur elektronischen Gesundheitskarte. Die von Seiten des Datenschutzes, insbesondere zum Schutz der freien Willensentscheidung und Beteiligung der Versicherten seit Jahren nachdrücklich vorgetragenen Vorstellungen (u. a. mit der Konferenzentschließung unter Ziff. 18.4 dieses Berichts) sind in den Gesetzestext eingearbeitet worden.

Nach § 291 a Abs. 2 SGB V n. F. soll die Krankenversichertenkarte, auf der bislang keine medizinischen Daten, sondern lediglich die Identitätsdaten des Versicherten und administrative Daten gespeichert sind, ab 1. Januar 2006 durch die Gesundheitskarte ersetzt werden, die geeignet sein muss, Verschreibungsdaten zu speichern. Sie soll damit auch als „elektronisches Rezept" dienen. Während diese Funktion obligatorisch ist, soll es nach § 291 a Abs. 3 dem Versicherten überlassen bleiben, ob er sich mit einer oder mehreren der anderen Funktionen einverstanden erklären will, für die die Karte gleichfalls ab 2006 geeignet sein soll, insbesondere denen der Notfallkarte, des „elektronischen Arztbriefs", der „elektronischen Arzneimitteldokumentation" oder der „elektronischen Patientenakte". Zudem, und diese Regelung ist zweifellos als ein Erfolg der Datenschutzbeauftragten zu werten, bedarf nach § 291 a Abs. 5 jeder Zugriff auf im Rahmen dieser „fakultativen" Funktionen gespeicherte Daten der vorherigen Einwilligung des Karteninhabers. Nach § 291 a Abs. 4 SGB V dürfen ohnehin nur Ärzte oder Angehörige anderer Heilberufe auf die medizinischen Daten zugreifen, die auf der Karte gespeichert sind. Der GKV stehen weiterhin lediglich die bereits auf der Krankenversichertenkarte gespeicherten administrativen Daten offen. Zudem wird nach dem neuen § 307 a SGB V mit Strafe bedroht, wer auf medizinische Daten zugreift, die auf der Karte gespeichert sind, ohne zu dem berechtigten Personenkreis (Ärzte und Angehörige anderer Heilberufe) zu gehören. Schließlich darf nach § 291 a Abs. 8 SGB V vom Karteninhaber nicht verlangt werden, jemandem den Zugriff zu gestatten, der nicht zu dem berechtigten Personenkreis gehört, oder den Zugriff zu anderen Zwecken als seiner gesundheitlichen Versorgung einschließlich der Abrechnung zu ermöglichen.

Bis zum Stichtag müssen, so bestimmt es § 291 a Abs. 7 SGB V, die Spitzenverbände der GKV, der Ärzte, Krankenhäuser und Apotheker in Kooperation mit der

Industrie und unter Beteiligung des Bundesministeriums für Gesundheit und Soziale Sicherung sowie des Bundesbeauftragten für den Datenschutz die zur Realisierung der Vorstellungen des Gesetzgebers erforderliche Informations-, Kommunikations- und Sicherheitsinfrastruktur schaffen. Zudem wird es der GKV obliegen, die Karten auszugeben und zuvor die Versicherten umfassend und allgemeinverständlich über die Funktionen der Karte und ihre Rechte zu informieren, § 291 a Abs. 2 Satz 2 SGB V.

Aber schon propagiert das Bundesministerium für Wirtschaft und Arbeit ein neues noch ehrgeizigeres Kartenprojekt: die „JobCard", die, anders als ihr Name verrät, als Multizweckkarte konzipiert ist und über den Bereich der Arbeitsvermittlung hinaus u. a. auch Funktionen in der gesundheitlichen Versorgung übernehmen soll. Steht die Gesundheitskarte à la GMG bereits schon wieder vor dem Aus, bevor sie überhaupt das Licht dieser Welt erblickt hat? Nachdenklich stimmt, dass auch an der Entwicklung der JobCard die Spitzenverbände der GKV maßgeblich beteiligt sind. Bietet sich da nicht die Gelegenheit, möglichst umgehend unbequeme datenschutzrechtliche Regulative zur Gesundheitskarte zu liquidieren? Gesetze, insbesondere auch das SGB V, werden heutzutage laufend geändert. Die Förderung des Datenschutzes steht dabei nicht immer an erster Stelle. Wie es gehen kann, ist jüngst beim GMG vorgeführt worden (vgl. Ziff. 8.3.3.1 dieses Berichts). Die Datenschutzbeauftragten des Bundes und Länder werden gemeinsam darüber zu wachen haben, dass nicht wieder über ihre Vorstellungen letztendlich dann doch hinweggegangen wird.

9. Arbeit, Jugend und Soziales

9.1 Interne Vernetzung des Sozialressorts

Im letzten Jahr (vgl. 25. JB, Ziff. 9.2) berichtete ich im Zusammenhang mit dem Anschluss der städtischen Kindertagesheime an das Intranet der bremischen Verwaltung, dass mir keine aktuelle Konzeption des Netzes für das interne Netz des Ressorts vorliegen würde. Das Konzept sollte die alle Komponenten umfassende Sicherheitsstruktur beschreiben.

Im März des Berichtsjahres erhielt ich dann vom Ressort ein aussagefähiges Datenschutzkonzept. Dieses hatte ich bereits in 2002 angemahnt, weil die Datensicherheit einzelner Fachverfahren (beispielsweise das Kindergarteninformationssystem „KIS" oder das Verfahren „Bundeserziehungsgeld") ohne Informationen über die zugrunde liegende Netzstruktur nicht bewertet werden konnte. Im April überprüfte ich dann die Netzstruktur (Domänenstruktur) auf die Verwaltungsbereiche der im Konzept genannten Domänen hinsichtlich der Zugriffs- und Ressourcensteuerung und einer möglichen Revision der Administration.

Es konnte festgestellt werden, dass die erforderliche Abschottung zwischen der Domäne des Amtes für Soziale Dienste und der senatorischen Dienststelle durch Steuerung über Gruppen, Konten und Verzeichnisse umgesetzt worden ist. Die interne Zugriffsstruktur in der senatorischen Dienststelle ist entsprechend den organisatorischen Erfordernissen auf der Systemseite angelegt worden.

Ich empfahl dem Ressort, das Datenschutzkonzept um ein Administrationskonzept zu ergänzen. Inhalt eines solchen Konzeptes wäre die Beschreibung der Aufgaben der Administration. Die Protokolle der Administratortätigkeiten sollten dem administratorischen Zugriff entzogen und für Stichproben dem behördlichen Datenschutzbeauftragten zur Verfügung gestellt werden. Damit wäre bereits die Grundlage für den Anfang einer Revision geschaffen.

Das Ressort hat die Administrationsrollen genauer beschrieben, meinen Vorschlag zur Revision jedoch nicht angenommen. Ich habe diesen Vorschlag noch einmal begründet und gehe davon aus, dass er entsprechend umgesetzt wird oder das Ressort einen neuen Lösungsansatz entwickelt, um die Administrationstätigkeiten transparenter zu machen.

9.2 Abgleich der Daten von Sozialhilfeempfängern mit dem Kfz-Register

Im ersten Quartal des Berichtsjahres machten die örtlichen Medien auf den erstmals in Bremen geplanten Datenabgleich der Sozialleistungsträger mit den Kfz-

Zulassungsstellen aufmerksam. Mit dem Abgleich soll festgestellt werden, ob ein Hilfeempfänger den Besitz eines Kfz verschwiegen und so möglicherweise ihm nicht zustehende Leistungen erhalten hat.

Es wird verglichen, ob am Stichtag des Datenabgleichs ein Empfänger von Leistungen nach dem Bundessozialhilfegesetz (BSHG) oder dem Asybewerberleistungsgesetz (AsylbLG) auch als Halter eines Fahrzeugs bei der Zulassungsstelle gemeldet ist. Berücksichtigt werden alle Fahrzeuge ab 125 ccm (Motorräder, PKW, LKW, Anhänger).

Grundlage für den grundsätzlich zulässigen Abgleich ist § 117 Abs. 3 BSHG. Bei der Diskussion mit der für die Durchführung des Abgleichs verantwortlichen Stelle, dem Amt für Soziale Dienste (AfSD), ergaben sich aber zwei datenschutzrechtlich relevante Aspekte: Zum einen stellte sich die Frage, auf welchen (zurückliegenden) Zeitraum sich der Abgleich am Stichtag beziehen darf. Denn gerade für den ersten Abgleich mag die Information von Interesse sein, ob jemand bereits in der Vergangenheit Halter eines Kfz war. Nach der eindeutigen Formulierung des § 117 Abs. 3 f BSHG ist es jedoch lediglich zulässig, zu ermitteln, ob ein Hilfeempfänger aktuell, d. h., im Abgleichsmonat, Halter ist. Ich habe diesen Punkt mit dem AfSD erörtert und darauf geachtet, dass sich die Datenverarbeitung in dem gesetzlich zulässigen Rahmen bewegt.

Es ergab sich dabei noch die Frage, wie mit einem bei der Zulassungsstelle eingetragenen Sperrvermerk umzugehen ist. Gemäß § 41 Abs. 3 Straßenverkehrsgesetz (StVG) ist die Übermittlung trotz bestehender Sperre im Einzelfall zulässig, wenn an der Kenntnis der gesperrten Daten ein überwiegendes öffentliches Interesse, insbesondere an der Verfolgung von Straftaten, besteht. Diesbezüglich habe ich gegenüber dem AfSD die Rechtsauffassung vertreten, dass in einem solchen Fall ein automatisierter Abgleich nicht vorgenommen, sondern dann nur anlassbezogen für eine konkrete Person abgefragt werden darf, ob sie als Halter eines Kfz eingetragen ist. Wegen der Auslegung des § 41 StVG habe ich den Bundesbeauftragten für den Datenschutz um Stellungnahme gebeten.

9.3 Funk-LAN-Verbindung im Amt für Jugend und Familie Bremerhaven

Im März des Berichtsjahres wurde ich von der für die EDV-Organisation und die Gestaltung technischer Datenschutzmaßnahmen zuständigen Stelle des Amtes für Jugend und Familie darüber informiert, dass das Stadtteilbüro Nord aufgrund räumlicher Engpässe planen würde, eine Zweigstelle mit drei PC-Arbeitsplätzen einzurichten, die per Funk in das bestehende Subnetz eingebunden werden sollten. Die zum Einsatz kommende Technik sollte das auf dem Standard IEEE 802.11 basierende WLAN sein. Die Einbindung ist erforderlich, um zentrale Dienste (Fax, E-Mail) nutzen und auf Fachanwendungen zugreifen zu können.

WLAN bedeutet wireless local area network und ist eine Kabellostechnologie. Ein WLAN kann als eigenständiges drahtloses Subnetz über einen Access Point (Funkzelle) per Kabel an ein Verwaltungsnetz angeschlossen werden.

Bisher war das Stadtteilbüro über eine Standleitung an das Subnetz des Amtes für Jugend und Familie angebunden. Dieser Sicherheitsstandard ist im „Konzept zur Gewährleistung des Datenschutzes und der Datensicherheit im Bereich des Amtes für Jugend und Familie" (vgl. 24. JB, Ziff. 9.1 und 25. JB, Ziff. 9.1) festgelegt.

Funkstrecken haben grundsätzlich eine höhere Anfälligkeit in Bezug auf die Zugangs- und Abhörsicherheit. Die Authentifikation gegenüber dem Access Point (dieser wird direkt per Kabel an das Verwaltungsnetz angeschlossen) und die auf dem RC4-Algorithmus basierende WEB-Verschlüsselung sind wesentliche Schwachstellen, denen mit entsprechender Sicherheitstechnik begegnet werden muss. Es sind daher verschiedene Bereiche sicher zu gestalten.

— Die Authentifikation der Maschine gegenüber dem Access-Point.

  Hierzu ist nicht die standardmäßige Authentifizierung über die MAC-Adresse zu zählen (Hardwareadresse der Netzwerkkarte), die der Methode des MAC-Spoofings, dem Vortäuschen einer meistens vorher abgehörten MAC-Adresse, nicht standhält und

— die Benutzerauthentifikation gegenüber dem Netz des Amtes für Jugend und Familie.

— Aufgrund der Sensibilität der Daten ist es außerdem wichtig, die Daten selbst auf der Funkstrecke sicher zu verschlüsseln. Ich habe deshalb gegenüber dem Amt für Jugend und Familie folgende Anforderungen definiert:

  — Abschottung des Funknetzes durch die Bildung eigener Subnetze,

  — Verschlüsselung der Inhaltsdaten,

  — Integriertes Sicherheitsmanagement unter Einbeziehung der WLAN-Komponenten,

  — VPN-Verschlüsselung unter Einbeziehung einer Firewall (diese trennt zwei Netzwerke mit unterschiedlichen Sicherheitsanforderungen).

Das Amt für Jugend und Familie hat mir die Umsetzung sämtlicher Anforderungen zugesagt.

9.4 Telefonische Hinweise auf illegale Beschäftigung in der Stadtgemeinde Bremen

Bereits im letzten Jahr habe ich berichtet, dass das Arbeitsressort einen Telefonanschluss geschaltet und öffentlich bekannt gemacht habe, über den seine Koordinierungsstelle zur Bekämpfung illegaler Beschäftigung Hinweise auf Schwarzarbeit und illegale Beschäftigung entgegennimmt (vgl. 25. JB, Ziff. 9.4). Ich hatte daraufhin im November 2002 das Ressort angeschrieben und um Darlegung der Zuständigkeit, die Daten der durch Hinweise betroffenen Bürger zu verarbeiten, und um Auskünfte zur Ausgestaltung der Datenverarbeitung gebeten. Im Februar 2003 erhielt ich schließlich die erbetenen Auskünfte. Die eingegangenen Hinweise – so wurde berichtet – würden auf einem Formblatt festgehalten, das als Text auf einem Stand-alone-PC gespeichert werde. Zugleich würden die Identitätsdaten der Betroffenen unter Zusammenfassung des Sachverhalts in einer Tabelle gespeichert. Die Formblätter würden per Fax an als zuständig erkannte Verfolgungsbehörden, etwa das Stadtamt, das Hauptzollamt, Sozialversicherungsträger oder Finanzbehörden, übermittelt. Diese würden dann eine Rückmeldung veranlassen, wenn ein Verfahren eingeleitet worden ist. Bisher seien Auskunftsansprüche Betroffener nicht erhoben worden. Es seien noch keine, aufgrund der Hinweise gespeicherten Daten gelöscht. Festlegungen über Löschfristen seien nicht getroffen worden.

Ich bezweifelte gegenüber dem Ressort, dass ihm die Befugnis zur Verarbeitung der Daten der Betroffenen zustehe, da in den vielfältigen Vorschriften zur Bekämpfung illegaler Arbeit und Schwarzarbeit eine oberste koordinierende Landesbehörde nicht aufgeführt sei. Diese Aufgabe komme nach dem SGB III vielmehr der Bundesagentur für Arbeit (vormals Bundesanstalt für Arbeit) zu. Darüber hinaus habe man es versäumt, die nach § 8 BremDSG gebotenen Festlegungen über die automatisierte Verarbeitung personenbezogener Daten (Datenschutzkonzept) zu treffen. Insbesondere sei es nicht akzeptabel, dass das Ressort seiner Verantwortung für die Pflege der Dateien (Berichtigung bzw. Löschung widerlegter oder nicht bestätigter Hinweise, Festlegung regelmäßiger Löschfristen), wie für die Erteilung von Auskünften an Betroffene nicht gerecht werde.

Der Senat teilte in seiner Stellungnahme zu meinem 25. Jahresberichts mit, es werde an Ansätzen zur Lösung der datenschutzrechtlichen Probleme gearbeitet. Dennoch erfuhr ich, selbst auf eine Erinnerung hin, nichts über etwaige Arbeitsergebnisse. Erst in der Sitzung des Rechtsausschusses der Bremischen Bürgerschaft am 5. November 2003 erklärte ein Vertreter des Ressorts, bis zum Ende des Jahres werde man einen Vorschlag vorlegen können. In der Sitzung des Rechtsausschusses Anfang Januar 2004 erklärte ein Vertreter des Arbeitsressorts, er werde dem Ausschuss bis Ende Februar 2004 ein Datenschutzkonzept für die in der Koordinierungsstelle geführte automatisierte Datei mit den Daten aus den eingegangenen Hinweisen vorlegen. Egal, wie sich dieser Bereich in Zukunft neu gestalten wird, wenn die unter Ziff. 13.5 dieses Berichts dargestellten bundesgesetzlichen Regelungen umgesetzt werden, so lange personenbezogene Daten im

Ressort verarbeitet werden, muss hierbei den datenschutzrechtlichen Belangen Rechnung getragen werden.

Es bleibt festzuhalten, dass, jedenfalls weit über ein Jahr lang, Bürgerdaten ohne Festlegung eines geordneten Verfahrens verarbeitet wurden. Mit dieser Kritik ist nicht die Absicht verbunden, illegale Beschäftigung und Schwarzarbeit zu beschönigen oder gar zu decken. Aber auch die Bürger, die in diesem Zusammenhang zu Recht oder zu Unrecht in Verdacht geraten, haben Anspruch darauf, dass ihre Daten in einem rechtsstaatlichen Verfahren verarbeitet werden.

9.5 Spendenaktion Weihnachtshilfe

In der Weihnachtszeit ist in Bremer Tageszeitungen täglich über das Gute zu lesen, das die Weihnachtshilfe durch einmalige, mittels Spenden der Leser ermöglichte Beihilfen hat bewirken können. Jemand, dessen Hilfeantrag abgelehnt worden war, hatte vergeblich um Rückgabe der eingereichten, seine Bedürftigkeit belegenden Unterlagen gebeten und sich anschließend an mich gewandt. Vom Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales, der die Durchführung der gemeinsam mit der Bremer Tageszeitungen AG verantworteten Aktion übernommen hat, erfuhr ich, dass man die Unterlagen der erfolgreichen Bewerber aus steuerlichen Gründen für die Dauer von fünf Jahren aufbewahren müsse. Über den Umgang mit Unterlagen abgelehnter Bewerber aber hatte man sich noch keine Gedanken gemacht. Ich schlug vor, diese Unterlagen nach Ablauf des folgenden Jahres zu vernichten, sofern sie nicht zuvor auf Wunsch des Betroffenen zurückgegeben worden seien. Entsprechende Fristen schlug ich für die aus den Anträgen in eine Excel-Tabelle übernommenen Daten der Antragstellerinnen und Antragsteller vor. Als Reaktion erhielt ich ein Datenschutzkonzept für die Spendenaktion Weihnachtshilfe, in dem meine Vorschläge aufgegriffen worden sind. Auch im Übrigen trifft das Konzept die durch § 8 Bremisches Datenschutzgesetz (BremDSG) vorgegebenen Festlegungen.

9.6 Supervision für Adoptiveltern

In Bremerhaven bietet ein Verein, in dem sich Adoptiv- und Pflegeeltern organisiert haben, Supervision für seine Mitglieder durch einen Psychologen an. Das Amt für Jugend und Familie zahlt Zuschüsse zur Honorierung der Supervisoren. Vor der Entscheidung über die Zuwendung für das Jahr 2003 verlangte das Amt vom Verein, ihm die Namen der Teilnehmer der Supervision in 2002 zu nennen. Öffentliche Mittel könnten nur bewilligt werden, wenn die Teilnehmer bekannt seien. Der Verein lehnte dies ab. Er berief sich auf die berufliche Schweigepflicht des Psychologen nach § 203 StGB und darauf, dass ihre Anonymität Voraussetzung dafür sei, dass die Eltern das Angebot wahrnehmen.

Ich habe das Amt darauf aufmerksam gemacht, dass die Teilnehmer des vorausgegangenen Jahres mit seinem Verlangen nicht hätten rechnen müssen. Sie hätten schon deshalb den Psychologen nicht von seiner Schweigepflicht entbinden können. Auch der Verein selbst, dem der Psychologe nach deren Einwilligung die Namen der Teilnehmer genannt habe, sei durch § 39 Abs. 1 BDSG, daran gehindert, diese Daten an Dritte weiterzuleiten. Deshalb müssten die Eltern zunächst um ihre Einwilligung in die Weiterleitung gebeten werden. Daneben habe ich das Amt darauf hingewiesen, dass der hier einschlägige § 44 der Landeshaushaltsordnung (LHO) und die ergänzenden Nebenbestimmungen (Ziff. 11.2 der VV-LHO zu § 44 und die Allgemeinen Nebenbestimmungen zur Projektförderung in der Anlage 2 zu den VV-LHO zu § 44) nicht verlangten, die Identitätsdaten der Teilnehmer offen zu legen.

Das Amt hat daraufhin auf die Nennung der Teilnehmer des Projekts in 2002 verzichtet und sich mit anonymisierten Angaben begnügt. Für 2003 – und damit voraussichtlich auch für die Folgejahre – besteht man auf die Benennung der Teilnehmer, sichert allerdings im Gegenzug zu, die Daten nur zur Prüfung der ordnungsgemäßen Verwendung der Zuwendung durch die dafür zuständigen Mitarbeiterinnen und Mitarbeiter nutzen zu wollen. Nachdem der Verein sich damit einverstanden erklärt hatte, erhob ich keine Bedenken mehr gegen das Verfahren. Die Folge ist, dass der Verein nunmehr die Einwilligung in die Weitergabe des jeweiligen Namens zur Voraussetzung der Teilnahme wird machen müssen.

10. Bildung und Wissenschaft

10.1 Forschungsvorhaben und andere Erhebungen an Bremer Schulen

Ein wesentlicher Bestandteil meiner Tätigkeit im Bereich Bildung und Wissenschaft lag auch im vergangenen Jahr wieder in der Abgabe von Stellungnahmen zu Forschungsvorhaben und Schulbegleitforschungsprojekten. In zunehmendem Maße werde ich darüber hinaus um die datenschutzrechtliche Bewertung von Vorhaben gebeten, die die Evaluierung schulischer Projekte betreffen.

10.1.1 Pisa 2003 und DESI

Wie bereits im 25. Jahresbericht (Ziff. 10.4) angekündigt, befasste ich mich im vergangenen Jahr noch einmal näher mit den Studien „Pisa 2003" und „DESI". Beide Studien dienen der Ergänzung der vorhergehenden Pisa-Studie und sollen den Kultusministern und Kultusministerinnen der Länder grundlegende Informationen über den Leistungsstand der Schüler und Schülerinnen geben. Der früheren Pisa-Studie vergleichbare datenschutzrechtliche Anforderungen waren auch bei „Pisa 2003" und „DESI" zu berücksichtigen und daher bereits bei der Konzeption der Erhebungen eingeflossen. Gleichwohl konnten durch die gemeinsamen Bemühungen der Datenschutzbeauftragten des Bundes und der Länder noch Verbesserungen hinsichtlich der für die Erhebungen vorgesehenen Unterlagen, insbesondere in den Informationsschreiben für die Erziehungsberechtigten und deren Einwilligungserklärungen und der Organisation der Erhebungen, erreicht werden.

10.1.2 Vergleichsarbeiten an Bremer Schulen (VERA)

Gemeinsam mit sechs anderen Bundesländern beabsichtigt Bremen, bei Schülern und Schülerinnen der vierten Jahrgangsstufe ab Herbst 2004 in den Fächern Mathematik und Deutsch so genannte Vergleichsarbeiten durchzuführen. Ziel der Vergleichsarbeiten ist es, den Lehrkräften eine zusätzliche Orientierung über den Leistungsstand der eigenen Klasse zu ermöglichen, wobei sie hierfür auch Informationen über andere Klassen mit ähnlicher Schülerzusammensetzung erhalten sollen. Der Konzeption der Vergleichsarbeiten diente eine im Berichtszeitraum von der Universität Koblenz-Landau durchgeführte Normierungsstudie, bei der Daten von Schülern und Lehrkräften erhoben werden sollten und zu der ich um Stellungnahme gebeten wurde.

Da von den Schülern und Schülerinnen auch Angaben über die ethnische und rassische Herkunft sowie zu etwaigen gesundheitlichen Beeinträchtigungen erhoben werden sollten, die zu den besonderen Arten personenbezogener Daten nach § 2 Abs. 6 Bremisches Datenschutzgesetz (BremDSG) zählen, habe ich insbesondere eine Änderung der Informationsschreiben und der Einwilligungserklärungen für erforderlich befunden. Außerdem habe ich auch bei diesem Vorhaben Änderungen an der Organisation der Erhebung für erforderlich erachtet.

Eine Rückäußerung des Senators für Bildung und Wissenschaft zu meiner Stellungnahme steht noch aus.

10.1.3 Reihenuntersuchung in einer Berufsschule

Im Rahmen ihres Schulprofils beabsichtigte eine öffentliche Berufsschule in Bremen, die Förderung besonders begabter und motivierter Schüler und Schülerinnen zu intensivieren.

Hierzu hat die Schule allen Schülern und Schülerinnen des ersten Lehrjahres das Angebot einer Testuntersuchung, bestehend aus einem wissenschaftlich überprüften Intelligenztest und einer Fragebogenerhebung, gemacht. Die Erhebung war nicht Teil des Unterrichts.

Dieses Vorhaben ist wie folgt zu beurteilen: Zum Auftrag der Schule nach § 3 Abs. 2 Bremisches Schulgesetz (BremSchulG) gehört auch die Verpflichtung, zur eigenen Fortentwicklung beizutragen. Nach § 9 Abs. 1 S. 2 BremSchulG sind Schule u. a. aufgefordert, eine eigene Entwicklungsperspektive unter Berücksichtigung ihrer Schüler herauszuarbeiten. Eine Befugnis, die vorgesehenen Datener-

hebungen durchzuführen, ergibt sich aus den gesetzlichen Bestimmungen jedoch nicht. Bei Erhebungen wie der geplanten ist deshalb darauf zu achten, dass diese möglichst unter freiwilliger Beteiligung der Betroffenen durchgeführt werden. Über die geplante Durchführung der Erhebungen sind die Betroffenen rechtzeitig näher zu informieren. Bei einer Nichtteilnahme dürfen den Betroffenen keine Nachteile entstehen. Wie mir der Senator für Bildung und Wissenschaft mitteilte, will die Berufsschule entsprechend meiner Empfehlungen verfahren. Die Schüler und Schülerinnen sollen deshalb selbst entscheiden, ob sie an der Untersuchung teilnehmen wollen.

10.1.4 Erhebungen im Projekt „Jump Plus"

Im vergangenen Jahr bin ich vom Senator für Bildung und Wissenschaft über ein Vorhaben informiert worden, das u. a. der Evaluation des an einem Schulzentrum der Sekundarstufe I durchgeführten „Eisbergmodells" dienen sollte. Nach ihrem beruflichen Werdegang sollten dabei ehemalige Schüler und Schülerinnen der Schule befragt werden, die an dem Schulprojekt teilgenommen hatten. Mit dem Eisbergmodell versucht die Schule, ihren Schülern und Schülerinnen den beruflichen Einstieg bzw. das Durchhalten in der Berufswelt zu erleichtern. Die Untersuchung wollte allerdings nicht die Schule selbst durchführen, sondern ein privatwirtschaftlich organisiertes Bildungszentrum im Rahmen des von ihm eingerichteten Projektes „Jump Plus". Zielgruppe dieses Projektes waren ausbildungs- und arbeitsgeeignete junge Erwachsene unter 25 Jahren, für welche die Teilnahme an dem Projekt eine berufsvorbereitende oder auch weiterbildende Maßnahme darstellte. Für die Durchführung des Projekts sollte die Schule dem Bildungszentrum vorab die Namen, Geburtsdaten, Adressdaten sowie die Staatsangehörigkeit der einzelnen Betroffenen übermitteln.

In meiner Stellungnahme habe ich den Senator für Bildung und Wissenschaft darauf aufmerksam gemacht, dass schulrechtliche Vorschriften die Übermittlung der genannten Daten von der Schule an das Bildungszentrum nicht zulassen, denn es handelt sich nicht um eine Untersuchung nach § 13 Abs. 1 des Gesetzes zum Datenschutz im Schulwesen (BremSchulDSG). Die Übermittlung wäre auch nicht nach § 18 Abs. 1 BremSchulDSG zulässig. Ich habe daher empfohlen, dass die Schule vor der Datenübermittlung die Betroffenen um ihre Einwilligung bittet. Der Senator für Bildung und Wissenschaft erklärte mir, dass meiner Empfehlung entsprochen werden soll.

10.1.5 Erhebung zum Projekt „Lehrer im Team – Qualitätsentwicklung an der Schule"

Mehrere Bremer Schulen haben sich zur Teilnahme an einem Programm der Robert-Bosch-Stiftung mit dem Titel „Lehrer im Team – Qualitätsentwicklung an der Schule" bereit erklärt. Durch dieses Programm sollen die beteiligten Schulen gefördert werden, die Qualität ihres Unterrichts nachhaltig zu verbessern. Im Rahmen der Programmteilnahme sollen Schüler und Schülerinnen sowie Lehrkräfte der teilnehmenden Schulen von einem externen Forschungsinstitut zu unterschiedlichen Aspekten befragt werden. Während die Schüler u. a. zu ihren Einstellungen zum Unterricht, über ihre Mitschüler und Lehrer sowie ihre häusliche Situation befragt werden, sollen die Lehrkräfte insbesondere über ihren Unterricht sowie ihre Arbeitssituation und -belastung befragt werden.

Auch zu dieser Erhebung habe ich den Senator für Bildung und Wissenschaft auf die einzuhaltenden datenschutzrechtlichen Anforderungen hingewiesen. Er hat sich bereiterklärt, für die Einhaltung der zu beachtenden Vorschriften zu sorgen.

10.1.6 Merkblatt zur Durchführung von Forschungsprojekten

Das Merkblatt zur Durchführung von Forschungsprojekten durch Hochschulen oder andere öffentliche Forschungseinrichtungen ist im Berichtsjahr von mir aufgrund der Novellierung und Neufassung des Bremischen Datenschutzgesetzes (BremDSG) vom 4. März 2003 (Brem.GBl. S. 85) überarbeitet und an diese Vorschriften angepasst worden.

Die wesentliche Änderung des Merkblatts bezieht sich auf die Verarbeitung besonderer Arten personenbezogener Daten (Angaben über die rassische und ethni-

sche Herkunft, die politische Meinung, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben). Die Einwilligung in die Verarbeitung dieser Daten muss sich nach den neuen Regelungen ausdrücklich darauf beziehen.

Das Merkblatt kann bei meiner Dienststelle angefordert werden und ist auf meiner Homepage www.datenschutz.bremen.de/Recht abrufbar.

10.2 Durchführung einer Fotoaktion an einer Grundschule

Eine öffentliche Grundschule in Bremen bat mich im Berichtsjahr um die datenschutzrechtliche Beurteilung eines Angebots, das sie von einem Fotounternehmen erhalten hatte. Der Schule war eine Fotoaktion mit all ihren Schülern und Schülerinnen angeboten worden. Außerdem umfasste ein zweiter Teil des Angebots die Erstellung einer CD-ROM mit einer Bilddatei und umfangreichen Schülerdaten zur Unterstützung der Schulverwaltung. Für den Fall, dass die Grundschule das Angebot des Fotounternehmens annehmen würde, erklärte sich dieses außerdem bereit, der Schule für die Unterrichtstätigkeit einen Sponsorenbeitrag zur Verfügung zu stellen.

Weder das Gesetz zum Datenschutz im Schulwesen noch andere Rechtsvorschriften enthalten eine Rechtsgrundlage, nach der die Durchführung der angebotenen Fotoaktion oder die Weitergabe von Schülerdaten im Rahmen dieser Aktion zulässig wäre. In meiner datenschutzrechtlichen Bewertung des Angebots teilte ich der Schule daher mit, dass die Teilnahme der Schüler und Schülerinnen an der Fotoaktion einschließlich der Erstellung der Fotos durch das Unternehmen nur zulässig sei, wenn die Erziehungsberechtigten hierzu ihre schriftliche Einwilligung gegeben haben. Die Erziehungsberechtigten sind über die geplante Fotoaktion zu unterrichten. Soweit Schülerdaten zur Erstellung der CD-ROM weitergegeben werden, so müsse auch dieses in die Unterrichtung der Eltern einbezogen werden. Kein Kind dürfe zur Teilnahme gezwungen werden. Des Weiteren empfahl ich der Schule, mit dem Fotounternehmen einen Vertrag abzuschließen, in dem genau geregelt ist, wie mit dem die Schüler und Schülerinnen betreffenden Daten- und Fotomaterial zu verfahren ist.

Die Schule hatte zuvor bereits auf eigene Veranlassung auf die Annahme des zweiten Teils des Angebots, der die Erstellung einer CD-ROM mit Schülerdaten vorsah, verzichtet. Darüber hinaus hat die Schule zugesagt, bei einer Annahme des Angebots meiner datenschutzrechtlichen Bewertung zu folgen.

Aus meiner Sicht wird im geschilderten Fall noch einmal deutlich, wie wichtig genaue Kenntnisse bei den Schulen im Hinblick auf die von ihnen zu beachtenden datenschutzrechtlichen Vorschriften sind. Wie der Presse zu entnehmen war, planen zahlreiche öffentliche Schulen vor dem Hintergrund knapper Kassen die Aufnahme oder Intensivierung des Kontaktes mit Unternehmen der Privatwirtschaft. Dabei dürfen die Regelungen des Gesetzes zum Datenschutz im Schulwesen nicht unberücksichtigt bleiben.

11. Bau, Verkehr und Umwelt

11.1 Gesetz zur Änderung des Bremischen Wassergesetzes (BremWG)

Der Entwurf dieser Gesetzesänderung ist mir vom Senator für Bau, Umwelt und Verkehr Ende August 2003 zur Stellungnahme zugeleitet worden. Er enthält in § 170 a BremWG Regelungen zur Informationsbeschaffung und -übermittlung personenbezogener Daten zur Erfüllung der Aufgaben nach diesem Gesetz.

Ich habe vorgeschlagen, die jeweiligen Personengruppen, deren personenbezogene Daten für die dort genannten Zwecke verarbeitet werden sollen, im Gesetzestext zu benennen, und empfohlen festzulegen, dass nur die personenbezogenen Daten erhoben und verarbeitet werden dürfen, die für die jeweils genannten Zwecke erforderlich sind.

Mitte Dezember 2003 habe ich bei der senatorischen Dienststelle nachgefragt, ob meine Änderungsvorschläge, die ich im September 2003 zugeleitet hatte, berücksichtigt werden bzw. worden sind. Ohne eine Antwort erhalten zu haben,

habe ich nunmehr zur Kenntnis nehmen müssen, dass die Gesetzesänderung am 23. Dezember 2003 in Kraft getreten ist (Brem.GBl. S. 401). Da ich nicht zu erkennen vermochte, dass die Regelung meine Vorschläge berücksichtigte, habe ich nachgefragt.

Das Ressort hat erklärt, dass aufgrund der Komplexität der umzusetzenden Bestimmungen, der Anzahl der abzuarbeitenden Stellungnahmen und durchzuführenden Gesprächstermine sowie des sich aus der EU-Wasserrahmenrichtlinie und dem Wasserhaushaltsgesetz ergebenden Zeitdrucks nicht möglich war, mich während des Verfahrens auf dem Laufenden zu halten. Allerdings hat die senatorische Dienststelle zugesagt, anlässlich einer weiteren im Jahre 2004 notwendigen Novellierung des BremWG würde ich in der gebotenen Weise beteiligt werden.

11.2 Stromverbrauch in Kleingartengebieten

Aufgrund der Anfrage eines Rechtsanwaltes im Auftrage einer Mandantin habe ich bei der swb Enordia angefragt, ob und gegebenenfalls in welchen Fällen und in welchem Umfang die swb Enordia Stromverbrauchsdaten an das Bauordnungsamt übermittelt. Das Bauordnungsamt erhebt solche Daten bei öffentlichen und nicht öffentlichen Stellen zur Prüfung, ob in Kleingärten unzulässig gewohnt wird.

Nach Angaben des Energieunternehmens werden derartige Auskünfte nur bei schriftlicher Anfrage mit Angabe der Rechtsgrundlage, aus der das Unternehmen eine Verpflichtung dazu erkennen kann, erteilt. Bisher seien in den Jahren 1999 und 2001 in zwei Fällen aufgrund der §§ 61, 62 Bremische Landesbauordnung (BremLBO) Auskünfte erteilt worden mit dem Hinweis, die Bauordnungsbehörde habe die angeforderten Daten bei den Betroffenen nicht erheben können. In einer weiteren Anfrage habe das Unternehmen wegen einer nicht ausreichend erkennbaren Verpflichtung dazu eine Auskunft verweigert.

Diese Fälle stammen aus der Zeit vor meiner Prüfung beim Bauordnungsamt im Jahre 2001 und der daraufhin erfolgten Vereinbarung über die Datenerhebung in Kleingärten mit dem Bauressort im Jahre 2002 (vgl. 25. JB, Ziff. 11.1), so dass das seinerzeitige Verfahren nunmehr obsolet ist.

Ich habe daher dem Rechtsanwalt anheim gestellt, sich wegen einer auf seine Mandantin bezogenen Prüfung direkt an den Beauftragten für den Datenschutz der swb Enordia zu wenden.

11.3 Datenschutzkontrolle beim Senator für Bau, Umwelt und Verkehr und nachgeordneten Dienststellen

Auch in diesem Berichtszeitraum habe ich wieder ausgewählte Dienststellen der bremischen Verwaltung einer datenschutzrechtlichen Prüfung unterzogen. Beim Senator für Bau, Umwelt und Verkehr sowie beim Bauamt Bremen-Nord und dem Bremer Baubetrieb habe ich wie angekündigt (vgl. 25. JB, Ziff. 7.1) geprüft, ob die DV-Protokolldaten, die im Zuge der strafrechtlichen Ermittlungen wegen Zugriffen auf kinderpornografische Internetseiten angefallen waren, in den betreffenden Dienststellen zum Prüfungszeitpunkt noch vorhanden waren.

Während die senatorische Dienststelle und der Bremer Baubetrieb die von den richterlichen Beschlüssen im Juli/August 2002 umfassten Protokolldaten auf ihren Servern gelöscht hatten, waren diese Daten beim Bauamt Bremen-Nord zum Zeitpunkt der Prüfung und damit ca. ein Jahr später rechtswidriger Weise noch gespeichert. Die besondere datenschutzrechtliche Bedeutung erschließt sich bei Betrachtung des Ausmaßes der aufgezeichneten Daten: Bereits für jenen Zeitraum von vier Wochen, in dem die Vollprotokollierung aufgrund richterlichen Beschlusses rechtmäßig erfolgte, waren allein beim Bauamt Bremen-Nord mehr als 350.000 Protokolleinträge zu verzeichnen.

Darüber hinaus habe ich die Kontrolle der dienstlichen und privaten Internetnutzung durch die Behördenmitarbeiter in Augenschein genommen und datenschutzrechtlich bewertet.

Auch dabei habe ich bestätigt gefunden, dass selbst in einem einzelnen Ressort die Gestaltung der Internettechnik zu datenschutzrechtlich unterschiedlichen Ergebnissen führen kann. Während beim Senator für Bau, Umwelt und Verkehr eine

Aufzeichnung der Internetaktivitäten nicht stattfindet und daher datenschutzrechtlich keinerlei Probleme aufwirft, habe ich beim Bauamt Bremen-Nord auf die Unzulässigkeit des behördlichen Verhaltens hinweisen müssen. Dort waren über lange Zeit die DV-Einstellungen so vorgenommen worden, dass alle Aufrufe von Internetseiten mit ihrer URL und dem jeweiligen Arbeitsplatzrechner in einer zentralen Datei erfolgten. Selbst wenn eine konkrete Auswertung der Internetprotokolle nicht vorgesehen ist, lässt ohne richterlichen Beschluss die Personenbeziehbarkeit der Eintragungen die Protokollierung unzulässig werden. Dies ist rechtlich im Wesentlichen dadurch verursacht, dass mit Duldung der privaten Internetnutzung von Mitarbeitern die Stellung als Dienstherr oder Arbeitgeber nunmehr von der Funktion als Zugangsprovider überlagert wird. Damit greifen im Verhältnis zum Beschäftigten die Vorschriften des Telekommunikationsgesetzes und der Telekommunikations-Datenschutzverordnung ein, die derartige Aufzeichnungen nur sehr eingeschränkt zulassen, etwa zu Abrechnungszwecken oder um im Einzelfall technische Störungen beheben zu können, vgl. § 89 Abs. 1 S. 1 TKG i. V. m. §§ 6 ff. TDSV. Diese Bestimmungen tragen in ihrem restriktiven Charakter daher zur umfassenden Sicherung des Fernmeldgeheimnisses gemäß § 85 Abs. 2 und 3 TKG bei.

Im Ergebnis gilt Vergleichbares aber auch für ein Protokollierungssystem, wie ich es beim Bremer Baubetrieb vorgefunden habe. Neben einer zulässigen Software, die unerwünschte Web-Seiten sperrt, wird dort ebenfalls eine Vollprotokollierung aller Internetzugriffe eingesetzt. Zwar ist beim Bremer Baubetrieb die Nutzung des Internets ausschließlich für dienstliche Zwecke zugelassen, so dass nicht die speziellen Datenschutzregelungen des TKG und der TDSV eingreifen. Nicht übersehen werden darf jedoch, dass dann die allgemeinen datenschutzrechtlichen Vorschriften zur Anwendung kommen. Für den Bereich des Arbeits- oder Dienstverhältnisses ist dabei aber anerkannt, dass dem berechtigten Interesse der Beschäftigten, keiner vollständigen und permanenten Überwachung ausgesetzt zu sein, eine besondere Bedeutung zukommt. Ohne Anhaltspunkte auf eine missbräuchliche Nutzung ist daher auch in diesem Fall eine umfassende Protokollierung unzulässig. Regelmäßig muss mithin ebenfalls beachtet werden, dass die Standardprotokollierungen der Betriebssysteme zu ändern oder abzuschalten sind.

Dem berechtigten Interesse des Arbeitgebers an der Verhinderung rechtswidriger Nutzungen kann datenschutzkonform auf andere Weise entsprochen werden. Hier ist zum einen an den Einsatz einer Filtersoftware zu denken, wie sie beim Bremer Baubetrieb bereits erfolgreich im Einsatz ist, die nach vorher eingestellten Kriterien einzelne Web-Seiten für den Aufruf vom Arbeitsplatz sperrt. Zum anderen können auch eine größere Anzahl von Arbeitsplatz-Rechnern zu einer Gruppe zusammengefasst werden und nur deren IP-Adresse im System beim Web-Seiten-Aufruf protokolliert werden, so dass der einzelne Internetzugriff nicht mehr einer bestimmten Person zugeordnet werden kann. Bei einem Verdacht auf Missbrauch kann dann für einen bestimmten Zeitraum eine individuelle Protokollierung vorgenommen werden.

Es kommt auch in Betracht, ein Software-Tool einzusetzen, das dem Nutzer die Möglichkeit gibt, bei einer Internetnutzung anzugeben, ob diese zu dienstlichen oder privaten Zwecken erfolgt (z. B. der so genannte „P-Switch" der datenschutz nord GmbH). Diese Lösung bietet sich an, weil nach der zukünftig für die Internetnutzung im BVN maßgeblichen „Richtlinie für die Bereitstellung von Internet/Intranet-Zugängen" (Brem.ABl. S. 77 ff. vom 1.2.2004) ein solchermaßen differenzierendes Programm Voraussetzung für die private Internetnutzung am Arbeitsplatz sein wird. Die danach getrennt stattfindende Protokollierung der dienstlichen und der privaten Internetzugriffe ermöglicht es, unterschiedliche Auswertungsmaßstäbe vorzusehen und die Einsichtnahme in die Protokollierung insbesondere der privaten Nutzung nur sehr eingeschränkt zu eröffnen.

Nach der genannten Richtlinie werden sämtliche Protokolle der dienstlichen und privaten Internetnutzung nach 90 Tagen gelöscht, und ein Zugriff auf die Inhalte der Protokolle wird nur zulässig sein bei Vorliegen konkreter und auf Tatsachen gestützter Anhaltspunkte, die einen Verdacht missbräuchlicher Nutzung begründen. Im Falle privater Internetnutzung setzt ein Missbrauch dabei den Zugriff auf strafbare Inhalte oder Inhalte mit schwerwiegenden Verstößen gegen ethische

Grundsätze voraus. Die Richtlinie nimmt hierzu Bezug auf § 12 Abs. 1 Mediendienstestaatsvertrag.

12. Wirtschaft und Häfen

12.1 Luftsicherheit

12.1.1 Zuverlässigkeitsüberprüfungen nach § 29 d Luftverkehrsgesetz

Im letzten Jahresbericht habe ich über die Überprüfung von Beschäftigten am Bremer Flughafen berichtet (vgl. 25. JB, Ziff. 11.5). Sie müssen sich einer Sicherheitsüberprüfung unterziehen. Ich habe dieses Verfahren weiter verfolgt und bei den verschiedenen beteiligten Stellen im Lande Bremen kontrolliert. Dabei konnte ich feststellen, dass der Datenaustausch

— zwischen dem Senator für Wirtschaft und Häfen als zuständige Stelle und

— der Flughafen Bremen GmbH,

— dem Landesamt für Verfassungsschutz

— und der Polizei Bremen

überwiegend in elektronisch verschlüsselter Form erfolgt.

Beim Senator für Wirtschaft und Häfen gehen die Anträge der Beschäftigten des Bremer Flughafens und der dort tätigen Betriebe – soweit deren Beschäftigte sicherheitsempfindliche Bereiche betreten müssen – elektronisch und später auch in Papierform ein. Der elektronische Versand soll der Beschleunigung und der Vereinfachung dienen. Der Senator für Wirtschaft und Häfen reicht die Anfragedaten in dem erforderlichen Umfang an die obengenannten bremischen Stellen ebenfalls elektronisch und verschlüsselt weiter.

Vom Landesamt für Verfassungsschutz wird die entsprechende Anfragetabelle an das Bundesamt für Verfassungsschutz übermittelt und kommt innerhalb eines Tages mit den entsprechenden Hinweisen zurück. Diese Hinweise werden konventionell abgearbeitet und die „verwertbaren" Hinweise an den Senator für Wirtschaft und Häfen übermittelt. Für alle Personen, zu denen keine Informationen beim Verfassungsschutz vorliegen, erfolgt eine „Negativmeldung" auf elektronischem Weg. Die Anfragelisten werden nur kurze Zeit (drei Monate) für eventuelle Nachfragen aufbewahrt und dann für die Unterrichtung der Parlamentarischen Kontrollkommission anonymisiert.

Die Anfrage bei der Polizei Bremen geht bei der Flughafenwache der Polizei ein. Anlässlich meiner Prüfung habe ich festgestellt, dass das Verfahren wesentlich verbessert werden kann und an die Stellen verlagert werden sollte, bei denen die Daten (Kriminalaktennachweis und Staatsschutzdaten) vorliegen. Zur schnellen Erledigung werden auch telefonische Anfragen getätigt. Dabei können Verständigungsfehler auftreten. Dies könnte vermieden werden, wenn die Daten direkt der überprüfenden polizeilichen Stelle zugeleitet werden. Die Flughafenwache fragt auch die Daten bei außerbremischen Polizeidienststellen ab. Ich habe in einer Besprechung dem Senator für Wirtschaft und Häfen mitgeteilt, dass diese außerbremischen Polizeidienststellen von der zuständigen Stelle angefragt werden müssen, da für den Ersuchten sonst nicht erkennbar ist, ob es sich um ein Auskunftsersuchen nach Polizeirecht oder nach § 29 d Luftverkehrsgesetz handelt. Diese Frage wird zurzeit mit dem Senator für Inneres und Sport geklärt.

In den wenigen Fällen, in denen Erkenntnisse vorliegen, die zu Zweifeln an der Zuverlässigkeit des Antragstellers geführt haben, wurden die Antragsteller im Sinne der Luftverkehrszuverlässigkeitsüberprüfungsverordnung zu den Erkenntnissen angehört, und es wurde nach dem Verwaltungsverfahrensrecht weiter vorgegangen. Die zum Zeitpunkt der Prüfung vorliegenden Fälle wurden von mir geprüft und sind datenschutzrechtlich nicht zu beanstanden.

Geprüft wurde von mir auch, ob Arbeitgeber (Flughafen Bremen GmbH oder Betriebe am Bremer Flughafen) Erkenntnisse aus dem Überprüfungsverfahren erhalten haben. Durch Stichproben in den Überprüfungsvorgängen habe ich festgestellt, dass erkennbar keine inhaltlichen Daten an Arbeitgeber weitergegeben wurden. Die Arbeitgeber erhielten jeweils nur das Ergebnis der Überprüfung.

12.1.2 Luftsicherheitsgesetz

Seit dem Herbst 2003 liegt der Entwurf des Luftsicherheitsgesetzes vor.

Dieses Gesetz erweitert nicht nur die Befugnisse der Luftsicherheitsbehörden dahingehend, die Bundeswehr zu beauftragen, gegen fliegende Störer vorzugehen und sie im Notfall abzuschießen, sondern verdichtet auch die Überprüfung aller auf Flughäfen und -plätzen beschäftigten und sich aufhaltenden Personen. Auch werden nicht nur Luftverkehrsflughäfen erhöhte Sicherheitsvorkehrungen zu treffen haben, sondern auch einfache Flugplätze: nicht nur, dass die Personenüberprüfungen wesentlich intensiviert werden sollen, sondern auch, dass die an der Personenüberprüfung beteiligten Stellen zukünftig alle Überprüfungsfälle speichern müssen, damit sie im Falle neuer Erkenntnisse die zuständige Überprüfungsstelle über diese unterrichten kann, damit die Überprüfungsstelle ihre bisherige Risikoanalyse überprüfen und notfalls revidieren kann.

Dadurch wird dieses Verfahren „perfektioniert", die überprüften Personen unterliegen damit einem ständigen Überprüfungsfokus.

Der Gesetzesentwurf befindet sich zum Zeitpunkt des Redaktionsschlusses in der Beratung des Deutschen Bundesrates.

12.2 Maritime Sicherheit

Auf Grund der Ereignisse im Zusammenhang mit dem Terroranschlag in den USA vom 11. September 2001 wurden auch die Sicherheitsmaßnahmen im maritimen Bereich wesentlich verstärkt. Die in den letzten Jahren zu beobachtende Praxis, Hafenanlagen offen zugänglich zu halten, soll nicht mehr aufrechterhalten werden. Häfen, die insbesondere Verkehr mit den nordamerikanischen Häfen betreiben wollen, müssen sich strengen bis strengsten Sicherheitsauflagen unterwerfen. Insoweit besteht eine Parallele zum Luftverkehrs- bzw. Luftsicherheitsgesetz (vgl. Ziff. 12.1.1 dieses Berichts).

Durch den Entwurf eines „Gesetzes zur Änderung des Internationalen Übereinkommens von 1974 zum Schutz des menschlichen Lebens auf See und zum Internationalen Code für die Gefahrenabwehr auf Schiffen und in Hafenanlagen" vom 26. September 2003 (BR-Drs. 695/03) wurde ich erstmals mit dieser Materie befasst. Aus dem Gesetzentwurf geht hervor, dass die Betreiber von Schiffen und Hafenanlagen deutlich verstärkte Sicherheitsvorkehrungen treffen müssen.

Im Herbst des Berichtsjahres hat mich der Senator für Wirtschaft und Häfen frühzeitig über seine Pläne und seine Vorstellungen zur Umsetzung der beabsichtigten Sicherheitsvorgaben unterrichtet.

In diesem Zusammenhang ist geplant, das Hafenbetriebsgesetz dahingehend zu ändern und zu ergänzen, dass die Gefahrenabwehr gesetzeskonform ausgeführt werden kann. Es sind dazu normenklare Regelungen hinsichtlich der Zuverlässigkeitsüberprüfungen der im Hafen Beschäftigten zu treffen und die sicherheitsempfindlichen Bereiche und die Funktionen zu beschreiben. Ferner müssen die Rechte der zu überprüfenden Personen beschrieben und dafür gesorgt werden, dass die Eingriffe in das Persönlichkeitsrecht nur im erforderlichen Umfang erfolgen.

Es ist geplant, beim Senator für Wirtschaft und Häfen eine „zuständige Stelle" für die Gefahrenabwehr in den bremischen Häfen – nicht nur Seeverkehrshäfen – einzurichten. Ihre Aufgabe soll es sein, Risikobewertungen und Gefahrenabwehrpläne für die Häfen erstellen zu lassen und zu genehmigen. Zu diesem Zweck ist sie befugt, alle erforderlichen Daten zu erheben. Dies gilt für Daten über die Hafenanlagen, über alle Betriebe in den Häfen, wie Betriebe, die Waren anliefern oder abholen wie auch Dienstleister in den Häfen. Ferner haben diese Einrichtungen so genannte Gefahrenbeauftragte zu bestellen und der zuständigen Stelle zu melden.

Ferner wird die zuständige Stelle für eine Zuverlässigkeitsüberprüfung für bestimmte Beschäftigte in den Häfen zuständig sein.

Im Vorgriff auf die gesetzlichen Bestimmungen werden bereits Maßnahmen zur Umsetzung ergriffen. Dazu muss das bremische Hafenbetriebsgesetz neu gefasst

und voraussichtlich eine Zuverlässigkeitsüberprüfungsverordnung erlassen werden. Diese Rechtsnormen werden zurzeit in der senatorischen Behörde beraten. Ich bin bemüht, diesen Prozess zu begleiten, und achte darauf, dass nur Daten im erforderlichen Umfang erhoben werden sollen und möglichst wenige Stellen Kenntnis von den personenbezogenen Daten im Prüfverfahren der Zuverlässigkeit erhalten. Nur das Ergebnis dieser Prüfung darf den für die Sicherheit Verantwortlichen später bekanntgegeben werden.

12.2.1 Folgen für die Häfen

In den Häfen sind Beauftragte für die Gefahrenabwehr zu bestellen. Sie sind dazu berufen, Risikoanalysen für die Hafenanlagen zu erstellen und laufend anzupassen sowie entsprechende Gefahrenabwehraufgaben zu erfüllen. Sie haben u. a. sicherzustellen, dass der Zugang zu den Hafenanlagen kontrolliert, die Hafenanlagen überwacht, Bereiche mit Zugangsbeschränkungen festgelegt und dauernd überwacht werden und die ständige Benutz- und Verfügbarkeit von Nachrichtenmitteln sichergestellt wird. Diese Sicherheitsmaßnahmen sind je nach Sicherheitslage eventuell zu verstärken.

12.2.2 Folgen für die Betriebe und die Schiffe in den Häfen

In jedem Betrieb, der Schiffe abfertigt, sind Beauftragte für die Gefahrenabwehr zu bestellen, die Risikoanalysen für die Betriebe und die Schiffe zu erstellen haben. Diese Risikoanalysen gehen ebenfalls in Gefahrenpläne ein und sind laufend fortzuschreiben.

12.2.3 Folgen für Einwohner, Beschäftigte und Besucher in den Häfen

Die Erhöhung der Sicherheitsmaßnahmen hat naturgemäß Einfluss auf die Bewohner (z. B. Haus- und Schleusenmeister) und Besucher in den Häfen. Während die Maßnahmen für die Besucher sporadischer Natur sind und durch Kontrollen ihrer Identität, ihres Gepäcks und ihrer Fahrzeuge beim Betreten und Verlassen der Hafenanlagen wahrgenommen werden und das Verbot, bestimmte Hafenbereiche zu betreten, kontrolliert wird, sind die Folgen für die Einwohner und Beschäftigten in den Häfen wesentlich intensiver. Sie werden gründlicher als die Besucher kontrolliert. Wenn sie darüber hinaus in den „gesicherten" Bereichen arbeiten oder sogar wohnen, werden sie, und unter Umständen auch ihre Familienangehörigen, einer Zuverlässigkeitsüberprüfung unterzogen.

13. Finanzen

13.1 Steueränderungsgesetz 2003

13.1.1 Lebenslänglich

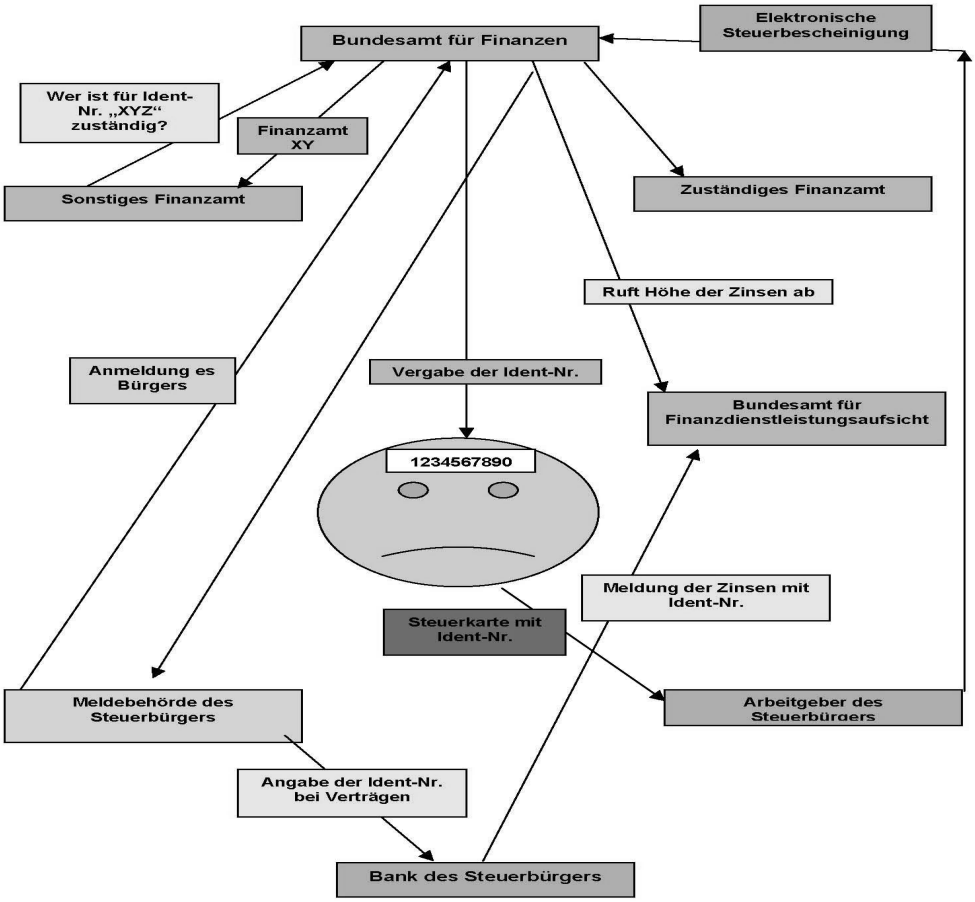
Das Steueränderungsgesetz 2003 vom 15. Dezember 2003 (BGBl. I S. 2645 ff.), in Kraft getreten am 1. Januar 2004, bringt verschiedene neue, gesetzliche Regelungen. Für die datenschutzrechtliche Bewertung sind folgende von Bedeutung:

— Die Einführung eines Identifikationsmerkmals für Privatpersonen (Identifikationsnummer) und wirtschaftlich arbeitende Betriebe und Personen (Wirtschaftsidentifikationsnummer), das vom Bundesamt für Finanzen vergeben wird.

— Die Verpflichtung aller Kreditinstitute (Banken und Sparkassen), alle Zinseinkünfte von Bürgern und Betrieben elektronisch an das Bundesamt für Finanzen zu melden.

— Die Verpflichtung aller Arbeitgeber – wenige härtebedingte Ausnahmen – alle steuerpflichtigen Einkünfte unter Angabe des Identifikationsmerkmals auf elektronischem Weg dem zuständigen Finanzamt zu melden. Der Arbeitnehmer erhält – mit seiner Steuerkarte – nur noch eine Bestätigung, welche Daten an das Finanzamt übermittelt wurden.

— Die Einführung der Identifikationsnummer (Ident-Nr.) führt zu einem steuerrechtlichen und einem lohnabrechnenden Ordnungsmerkmal. Das Verfahren und die Nutzung dieser Ident-Nr. habe ich nachstehend bildlich/schematisch dargestellt.



Die Datenschutzbeauftragten in Bund und Ländern sind mit mir der Auffassung, dass noch nicht abzusehen ist, welche Verknüpfungen zukünftig mit der Ident-Nr. möglich sind und wie die im Gesetz vorgesehene Zweckbindung begrenzt werden kann. Ich selbst habe erhebliche Zweifel, dass dies gelingt. In der vorgesehenen Zweckbegrenzungsvorschrift, „ihre Daten nur insoweit nach der Ident-Nr. ordnen oder für den Zugriff erschließen, als dies für regelmäßige Datenübermittlungen zwischen ihnen und den Finanzbehörden erforderlich ist", sehe ich keine wirksame Beschränkung, so lange keine hinreichende Sanktion für Verstöße gegen eine weitergehende Verwendung formuliert wird. Viele andere Verwendungen sind denkbar. Da es sich um ein bundesweit eindeutiges Identifikationsmerkmal handelt, könnte sie z. B. auch als Personalnummer in einem Betrieb, als Mitgliedschaftsnummer in einem Verein (Nachweis der Gemeinnützigkeit) oder für sonstige Zwecke, die im entferntesten Sinne für steuerliche Belange von Bedeutung sein können, verwendet werden.

Jedem Bürger wird bereits ab Geburt eine Ident-Nr. zugeordnet werden, die der Meldebehörde mitgeteilt wird. Ich befürchte, dass die Ident-Nr. die Nachfolge des einst geplanten und für verfassungswidrig erklärten Personenkennzeichens antreten wird. Da die Ident-Nr. durch die Meldungen aus dem Meldebestand stets aktuell sind, entsteht daraus ein bundesweites Melderegister (Zentraldatei). Dessen Verwendung kann allenfalls durch eindeutige gesetzliche Zweckbegrenzungen, die auch hinreichend amtshilfefest sind, gesichert werden. Wenn dies nicht gelingt, sehe ich die Gefahr, dass auf dem Bundespersonalausweis, dem Pass, jedem Vertrag und jeder Rechnung zukünftig die Ident-Nr. angegeben werden muss, um eine eindeutige Identifikation vornehmen zu können.

Wenn dies kommt und die Mitteilungspflichten und die Abrufmöglichkeiten der Finanzbehörden wie in den letzten Jahren immer umfassender werden, dann braucht der Steuerbürger eines Tages keine Steuererklärung mehr abgeben, denn die dafür erforderlichen Daten liegen den Finanzbehörden bereits vor.

13.1.2 Fortfall der Lohnsteuerkarte

Die Zeit der „guten alten" Lohnsteuerkarte geht dem Ende entgegen, bzw. sie verliert ihre bekannten Funktionen. So werden die Steuerbürger auch in Zukunft noch

eine solche erhalten, aber die wird neben den bisherigen Merkmalen eine Identifikationsnummer (Ident-Nr.) enthalten. Diese Nummer wird jedem Bürger, sobald ein Meldedatensatz über ihn angelegt wurde, einmal zugeteilt und soll ein (Steuer-) Leben gelten, denn diese Identifikationsnummer wird alle Datensätze im Bereich der Finanzverwaltung steuern. Ganz gleich, ob ein Antrag auf Steuerermäßigung oder -erstattung, eine Stundung, ein Vollstreckungsaufschub, eine Eigenheimzulage oder andere steuerliche Sachverhalte geklärt werden, immer wird diese Identifikationsnummer anzugeben sein.

Insbesondere werden die Lohnsteuerzahlungen des Arbeitgebers damit zuortenbar, oder auch die Lohnsteuerbescheinigungen des Arbeitgebers, die beim Ausscheiden eines Mitarbeiters oder am Ende des Kalenderjahres an das Finanzamt gesendet werden, werden über die Ident-Nr. an das für den Steuerbürger zuständige Finanzamt gesteuert.

Der Steuerbürger erhält von seinem Arbeitgeber in Zukunft keine ausgefüllte oder mit einen Aufkleber versehene Lohnsteuerkarte zurück, sondern einen Durchschlag der vorstehend genannten Lohnsteuerbescheinigung, die nur als Nachweis für den Arbeitgeber gilt, aber keinen Nachweis darstellt, die der Steuererklärung beigefügt werden muss, da die Daten bereits beim zuständigen Finanzamt vorliegen.

Dieses Verfahren stellt insbesondere ein starke Entlastung der Arbeitgeber dar, denn die Pflege der Lohn(steuer)konten wird dadurch noch weitgehender automatisiert und die Daten erhalten die Finanzbehörden elektronisch.

Im kommenden Berichtsjahr wird zu prüfen sein, ob und welche datenschutzrelevanten Umstellungsprobleme entstehen.

13.2 ELSTER (Elektronische Steuererklärung)

Für Dezember des Berichtsjahres kündigte ich eine Prüfung des Verfahrens ELSTER an. Der Landeseigenbetrieb „fidatas bremen" – das zuständige Finanzamt für dieses Verfahren – bat mich um eine Verschiebung. „fidatas" informierte mich aufgrund eines von mir erstellten Fragenkataloges vorab schriftlich über einzelne datenschutzrechtliche Aspekte des Verfahrens:

Danach ist die Übermittlung von Steuererklärungsdaten von Steuerpflichtigen bzw. deren Bevollmächtigten an die bremische Steuerverwaltung möglich, d. h., die erste Projektphase in Bremen umgesetzt. Eine Rückübermittlung der Bescheiddaten kann auf Grund der derzeit vorhandenen gesicherten Übertragungswege noch nicht erfolgen.

Die Steuerdaten werden von der Clearing-Stelle (in Nordrhein-Westfalen) per ISDN an den Server des ELSTER-Verfahrens (ECC-Server) übermittelt. Es sind Maßnahmen ergriffen worden, um die Einwahl Dritter zu verhindern.

„fidatas" stellte die Übertragung der Daten vom ECC-Server zum ELSTER-Verfahren (eigene DFÜ-Verbindung ohne externe Anschlüsse) und die Übertragung zur Weiterverarbeitung an die ID-Bremen dar. Für beide Übertragungswege werde ich die Frage der sicheren Übertragung (technisch und organisatorisch) im nächsten Berichtsjahr prüfen.

Momentan halte ich auf beiden Strecken eine Verschlüsselung bzw. den Aufbau eines VPN-Tunnels zur ID-Bremen für erforderlich.

Die Verschlüsselung der Steuerdaten durch die Steuerpflichtigen während der Übertragung wird dadurch ermöglicht, dass der öffentliche Schlüssel des Finanzamtes per E-Mail an die Mandanten versandt wird. Der für die Entschlüsselung der Daten erforderliche geheime Schlüssel verbleibt beim Finanzamt. Einige Übertragungsvorgänge (wie etwa Administratorzugriffe, Übermittlungen an die ID-Bremen) werden protokolliert.

Da das Verfahren bereits im Echtbetrieb läuft, habe ich die Erstellung eines Datenschutzkonzeptes für den bremischen Anwendungsteil angemahnt.

Es sind darin u. a. zu beschreiben:

— Die Absicherung der Datenübermittlung an den ECC-Server per ISDN durch die Clearingstelle.

— Die Absicherung der Übertragung der Daten vom ECC-Server zum ELSTER-Verfahren.

— Die Absicherung der Übertragung der Daten zur ID-Bremen.

— Die interne Zugriffsstruktur des ELSTER-Verfahrens.

— Die Absicherung des ECC-Servers.

— Protokollierung der Zugriffe auf die Steuerdaten.

Ich beabsichtige, die angekündigte Prüfung in 2004 nachzuholen.

13.3 Chipsmobil – Entwicklung des Rahmendatenschutzkonzeptes

Das Projekt CHIPSMOBIL (Controlling, Haushalt, Integration, Planung, Standard, Modular, Online, Buchführung, Informatik, Logistik) zur Erneuerung des bremischen Haushalts-, Kassen- und Rechungswesens habe ich auch in diesem Berichtsjahr über die dreijährige Entwicklungsphase hinaus (vgl. 22. JB, Ziff. 12.1; 23. JB, Ziff. 12.1; 24. JB, Ziff. 11.1) begleitet.

Schwerpunkt in diesem Berichtsjahr war der Abschluss eines Rahmendatenschutzkonzeptes. Inhalt dieses Konzeptes ist die Darstellung zentraler Datenschutz- und Datensicherungsmechanismen in ihren Einzel- und Wechselwirkungen, soweit sie über die Darstellung in den Detailkonzepten (wie etwa Betreiberkonzept, Berechtigungskonzept, IT-Konzept, Konzept des Customer-Competence-Centers) hinausgehen. Mit dem Rahmendatenschutzkonzept soll eine Verbindung zwischen den an verschiedenen Stellen im System getroffenen Einzelmaßnahmen hergestellt werden. Die Beratungen hierzu fanden gemeinsam mit dem Rechnungshof und dem Gesamtpersonalrat statt.

Während der Beratung des Datenschutzkonzepts tauchten durch die Inbetriebnahme des Systems neue Fragestellungen und Sichtweisen zu bereits bekannten Problemen auf. Für viele Bereiche konnten Lösungen gefunden werden. Dazu gehören beispielsweise:

Die Definition kritischer Berechtigungen im System:

Für das Rahmendatenschutzkonzept wurde meine Interpretation dieser Berechtigungen übernommen. Demnach werden kritische Berechtigungen in drei Kategorien unterschieden

— Systemberechtigungen außerhalb der SAP-Struktur (beispielsweise Zugang zu den Verwaltungsfunktionen der Datenbank oder zu den Schnittstellen von SAP/R3 auf Betriebssystemebene).

— Kritische Berechtigungen im Sinn der SAP-Definition (beispielsweise Entwicklungs- und Customizingberechtigungen, Administrationsberechtigungen).

— Berechtigungen, die Auswertungen personenbezogener Daten innerhalb der Berechtigungsstruktur erlauben. Besonders kritisch sind davon diejenigen, die vom Zugriffsvolumen (beispielsweise Einzelbelege) und/oder der Komplexität möglicher Auswertungen (wie etwa flexible Auswertungen im Rahmen von Reports) so weitreichend sind, dass durch ihre Anwendung die Zweckbindung der Verarbeitung systemseitig nicht mehr sichergestellt ist.

Zu den ersten beiden Kategorien sind bereits im Jahr 2002 in den Detailkonzepten mit mir abgestimmte Datenschutzmaßnahmen beschrieben worden, die jedoch zu Beginn des Echtbetriebs in einem zentralen Bereich der Sicherheit (vgl. Bericht des Rechnungshofs 2003) nicht umgesetzt waren.

Im Verlauf der Beratungen zum Datenschutzkonzept wurde dann auch deutlich, dass eine Definition und Dokumentation kritischer Berechtigungen und deren Vergabe an Systemnutzer erforderlich ist, um die Voraussetzungen zu deren Prüfbarkeit zu schaffen. Der Senator für Finanzen hat diese Dokumentation in Form einer Anlage zum Berechtigungskonzept erstellt.

Die Definition kritischer Transaktionen und Berechtigungen war auch erforderlich, um die oben beschriebene, im letzten Jahr noch nicht berücksichtigte dritte Kategorie kritischer Berechtigungen im System prüfbar und auswertbar zu machen. An dieser Stelle wurde besonders deutlich, wie sich Datenschutzaspekte neu im Zusammenhang mit spezifischen Fragestellungen ergeben haben. Im Zusammenhang mit der Frage nach der Prüfbarkeit einzelner Sicherheitsaspekte des Systems wurde klar, dass es eine Reihe kritischer Berechtigungen geben kann, die in Rollendefinitionen ohne offensichtliche Erkennbarkeit enthalten sind. Datenschutzrechtlich interessant ist natürlich, welche Benutzer im Besitz dieser kritischen Berechtigungen sind und ob diese zur Ausübung der vorgegebenen Funktion erforderlich sind. Ein Beispiel für eine kritische Berechtigung ist die Möglichkeit des allgemeinen Aufrufs von Reports (Transaktion SA38 – ABAP-Reporting), durch den offene Auswertungen über die Datenbank möglich sind. Im Anhang zum Berechtigungskonzept wurde definiert, welche Art von Systemnutzern berechtigterweise diese Transaktion ausführen können.

Das Verbot von personenbezogenen Auswertungen:

Dieses Verbot wurde bereits sehr früh (vgl. 23. JB, Ziff. 12.1) im Zusammenhang mit im System angelegten Rollen (Controlling, zentrale KLR, d. h., übergeordnete Kontrollinstrumente) von mir gefordert. Im entsprechenden Blueprint (Erfassung von Geschäftsprozessen in den jeweiligen Bereichen des Einführungsprojektes) zur Kosten- und Leistungsrechnung ist daraufhin festgelegt worden, dass im System die Felder, die personenbezogene Daten beinhalten, nicht dargestellt werden. Im Verlauf der Systemeinführung stellte sich nach Aussage der Senators für Finanzen heraus, dass die Darstellung technisch nicht verhindert werden konnte. Daraufhin wurde im Entwurf des Datenschutzkonzeptes zunächst verankert, dass statistische Auswertungen ausschließlich in anonymisierter Form ohne Rückschlüsse auf zusammenhängende Stammdaten möglich sein sollten. Dieser Passus war zwar zunächst aus dem Entwurf gestrichen worden (vgl. 25. JB, Ziff. 12.1), ist jedoch im Rahmen der diesjährigen Beratung wieder in das Konzept übernommen worden. Demnach dürfen kritische Berechtigungen (s. o.), die personenbezogene Auswertungen über die zentrale Datenbasis ermöglichen, allenfalls zu Zwecken anonymer statistischer Auswertungen genutzt werden, d. h., Rückschlüsse auf zusammenhängende Stammdaten dürfen nicht erfolgen.

Nutzung des Audit-Informations-Systems (AIS):

Das AIS ist eine Zusammenfassung von SAP-Standardtransaktionen und Reports unter den spezifischen Bedarfen der Revision.

Der Zugriff auf das SAP-Audit-Info-System ist grundsätzlich dem Rechnungshof und dem Customer Competence Center (CCC) möglich, auf Anforderung auch für den Landesbeauftragten für den Datenschutz und den Gesamtpersonalrat. Für das CCC soll noch eine Rahmenanweisung für die laufende Benutzer- und Berechtigungskontrolle erstellt werden.

Protokollierung:

Es werden verschiedene Protokolldaten zu Prüfungszwecken vorgehalten. Insbesondere der „Security-Audit-Log" ist im Produktivsystem eingeschaltet worden. Die Filterfunktionen des „Securitiy-Audit-Log" sind als Anhang Bestandteil des Datenschutzkonzeptes. Demnach werden die Rollen der zentralen Administration, der Berechtigungsadministration und eines Benutzers mit umfassenden Rechten, davon speziell privilegierten Rechten für das Data Dictionary (DDIC), für die datenschutzrelevanten Funktionen (beispielsweise Benutzerstammänderung) protokolliert. Der Zugriff auf die Protokolldateien ist auf wenige Benutzer eingeschränkt. Diese haben einen durch ihren Aufgabenbereich begründeten Zugriff und werden im Datenschutzkonzept festgelegt. Da sich systembedingt nur fünf Filter für die Protokollinhalte setzen lassen, ist eine alle Rollen mit kritischen Berechtigungen umfassende Protokollierung nicht möglich.

Direkte Änderungen im Produktivsystem:

Die Vorgehensweise für direkte Änderungen im Produktivsystem ist konkret festgelegt worden und stellt ein transparentes Verfahren dar.

Verschlüsselung:

Bereits am Anfang des Projektes habe ich einen hohen Schutz der SAP-Authentifzierung und eine Verschlüsselung der Daten auf den Leitungen (auch innerhalb des BVN) für erforderlich gehalten (vgl. 23. JB, Ziff. 12.1). Der Senator für Finanzen schätzte das Risiko des Abfangens von SAP-Passworten und der Daten auf dem Transportweg als gering ein (vgl. 24. JB, Ziff. 11.1), verwies aber in der Perspektive auf die Entwicklung einer Verschlüsselung für alle über das Bremer Verwaltungsnetz laufenden Anwendungen und Systemen (Infrastrukturverschlüsselung). Die dann geschaffenen Möglichkeiten sollten dann auch für CHIPS-MOBIL nutzbar gemacht werden (IPSEC und Active Directory).

Der Senator für Finanzen bleibt bis heute bei seiner Auffassung, dass das Risiko für die unbefugte Kenntnisnahme und Manipulation der SAP-Daten gering sei und hält eine technische Lösung für nicht erforderlich, obwohl die Möglichkeit gegeben ist (ab Version Windows 2000 und höher), eine gesicherte Verbindung von SAP-Clients zum SAP-Router (über IPSEC/Maschinenzertifikate) herzustellen.

Da an dieser Stelle bisher über die Jahre keine Annäherung der Positionen zwischen mir und dem Senator für Finanzen erreicht werden konnte, habe ich zusammen mit dem Gesamtpersonalrat vorgeschlagen, eine Risikoanalyse durchzuführen, um die Basis für die Risikoeinschätzung auf konkrete Daten stützen zu können.

Der Senator für Finanzen ist darauf eingegangen und wird nach der Restrukturierung des BVN, spätestens Anfang 2005, diese Risikoanalyse vornehmen. Ich habe das Verfahren akzeptiert, weil es sinnvoller ist, eventuell erforderliche zusätzliche Datensicherungsmaßnahmen mit der neuen Struktur zu verbinden.

Download:

Der Senator für Finanzen schätzt das datenschutzrechtliche Risiko des Download (Extraktion der Daten aus dem R/3-System und Auswertung mit Standardtools oder anderen Anwendungsprogrammen) als gering ein. Aus meiner Sicht gilt dies nicht für Rollen, die kritische Berechtigungen (s. o.) enthalten. Da alle Downloads aber nach Aussage des Betreibers ID-Bremen protokolliert werden und zumindest eine (wenn auch aufwändige) nachträgliche Prüfung ermöglichen, habe ich auf weitere Anforderungen verzichtet.

Insgesamt sind wesentliche Sicherheitsaspekte im Rahmen des Datenschutzkonzeptes erkannt und entsprechende technische Maßnahmen an dieser Stelle oder in den verbundenen o. g. Detailkonzepten definiert worden.

13.4 Nach Fehlkuvertierung getroffene Maßnahmen

Im letzten Jahresbericht (Ziff. 12.4) habe ich darüber berichtet, wie es durch eine falsche Programmierung der Kuvertierungsanlage der ID Bremen GmbH zu Fehlkuvertierungen von Steuerbescheiden gekommen ist.

Ich hatte dem Senator für Finanzen eine Reihe von Vorschlägen zur Vermeidung derartiger Vorfälle gemacht und zur Einrichtung eines „Krisenmanagements" geraten.

Der Senator für Finanzen hat mir mitgeteilt, dass Regelungen getroffen wurden, die eine künftige Fehlersuche verbessern und beschleunigen. Priorität haben dabei die unverzügliche Weitergabe sicherheitsrelevanter Informationen und bestimmte Maßnahmen zur Qualitätssicherung. Mit der ID Bremen GmbH wurden eindeutige Geschäftsprozesse definiert, die dies durch Festlegung von Kommunikationswegen und Ansprechpartnern sicherstellen. Durch diese Maßnahmen wurde meinen Anforderungen entsprochen.

13.5 Gesetz zur Intensivierung der Bekämpfung der Schwarzarbeit

Kurz vor Ablauf des Berichtsjahres erhielt ich einen ersten Entwurf eines Gesetzes zur Intensivierung der Bekämpfung der Schwarzarbeit. Dieses Gesetz wurde im Bundesfinanzministerium erarbeitet und sieht die Bündelung aller Kräfte zur Bekämpfung der Schwarzarbeit bei einer mit 7.000 Personen besetzten Superbehörde „Finanzkontrolle Schwarzarbeit" im Bereich der Bundeszollverwaltung vor.

Diese Zollbehörde soll auf 113 Standorte verteilt werden und eine zentrale Abteilung in Köln mit 120 Mitarbeitern haben. Alle Informationen im Zusammenhang mit Schwarzarbeit und illegaler Beschäftigung sollen in eine Zentraldatei aufgenommen und gespeichert werden. Auf diese Zentraldatei sollen die Zollbehörden das Recht zum Abruf haben. In einem Katalog sind die Speicher- und Löschfristen aufgeführt. Ferner sind in dem Gesetz die umfangreichen Ermittlungs-, Auskunfts- und Prüfrechte der Zolldienststellen aufgeführt.

Daneben wird diese Superbehörde unterstützt von den Finanzbehörden, der Bundesagentur für Arbeit, den Einzugsstellen für Sozialversicherungsbeiträge, den Trägern der Unfallversicherung, den Trägern der Sozialhilfe, den nach dem Asylbewerberleistungsgesetz zuständigen Behörden, den Ausländerbehörden, den für den Arbeitsschutz zuständigen Landesbehörden. Diese Behörden sind verpflichtet, die für ihre Prüfungen erforderlichen Informationen (einschließlich personenbezogener Daten) zu übermitteln. Der Bundesgrenzschutz darf die erforderlichen Daten erheben und an die Behörden der Zollverwaltung übermitteln. Mit den Landespolizeibehörden werden Daten im Einzelfall auf Ersuchen ausgetauscht, es sei denn, es handelt sich um Daten zur Ahndung oder Verhütung von Straftaten oder Ordnungswidrigkeiten im Rahmen der Bekämpfung der Schwarzarbeit. Durch die geplanten Regelungen würde die Überwachungsdichte und die staatliche Kontrollbefugnis erheblich erweitert.

14. Medien

14.1 Webcam in den Hörfunkstudios der Offenen Kanäle

Aufgrund einer Eingabe hat mir der Beauftragte für den Offenen Kanal bestätigt, dass Nutzer der Hörfunkstudios in Bremen und Bremerhaven ohne ihr Wissen und ihre Zustimmung in diesen Studios gefilmt und die Bilder simultan im Internet verbreitet werden.

Ich habe daher gefordert, dass es den Nutzern freigestellt werden muss, ob sie von der Webcam erfasst werden wollen oder nicht. Hierzu könnte die Webcam ausgeschaltet oder verdeckt werden. Außerdem habe ich verlangt, in geeigneter Weise auf diese Wahlmöglichkeit sowohl in der Nutzungsordnung als auch in den Räumlichkeiten der Hörfunkstudios hinzuweisen.

Mir ist mitgeteilt worden, dass ein Vorhang vor den übertragenden Webcams je nach Wunsch auf- oder zugezogen und damit ein Blick auf das Sendepult ermöglicht oder komplett verdeckt werden könne. Des Weiteren seien Hinweisschilder an den Außentüren der betreffenden Radiostudios angebracht worden, welche die Nutzer auf diese Möglichkeit hinweisen. Außerdem werde in dem Einführungsgespräch, das jeder Nutzer beim ersten Kontakt mit dem Offenen Kanal erhält, das Thema Internetübertragung während der Radiosendungen ausführlich behandelt. Hierbei würden die Nutzer auf ihre Wahlfreiheit hingewiesen.

14.2 Zuständigkeit bei Radio Bremen

Der Rundfunkrat von Radio Bremen hat den Vorschlag gemacht, die Überwachung des Datenschutzes bei Radio Bremen in die alleinige Zuständigkeit des Rundfunkdatenschutzbeauftragten Radio Bremens zu geben. Hierzu wurde ich von der Senatskanzlei um Stellungnahme gebeten.

Derzeit bin ich nach § 36 Bremisches Datenschutzgesetz (BremDSG) für die Datenschutzkontrolle hinsichtlich der administrativen Datenverarbeitung bei Radio Bremen zuständig, d. h., ich kontrolliere den Verwaltungsbereich. Der Rundfunkdatenschutzbeauftragte von Radio Bremen kontrolliert die journalistisch-redaktionellen Betätigung des Senders. Diese Zweiteilung der Zuständigkeit hat sich seit Jahrzehnten bewährt und ist auch gut mit den verfassungs- und europarechtlichen Vorgaben zu vereinbaren.

Weiter habe ich auf folgendes hingewiesen: Art. 28 Abs. 1 S. 2 der EG-Datenschutzrichtlinie fordert die völlige Unabhängigkeit der Datenschutzkontrollinstanzen. Ob diese zwingend notwendige Unabhängigkeit von Radio Bremen gewährleistet werden kann, stellt sich fragwürdig dar, solange der Rundfunkdatenschutzbeauftragte zugleich Angehöriger der Rundfunkanstalt ist und noch

andere administrative Aufgaben innerhalb dieser Anstalt wahrnimmt. Der derzeitige Rundfunkdatenschutzbeauftragte ist zugleich Mitarbeiter im Justiziariat. Hieraus kann sich ein Interessenskonflikt ergeben. Um den hohen Anforderungen von Art. 28 der EG-Datenschutzrichtlinie zu entsprechen, müsste der Rundfunkdatenschutzbeauftragte von sämtlichen anderen Aufgaben innerhalb der Rundfunkanstalt von Radio Bremen entbunden werden. Beim Landesbeauftragten stellt sich die Situation demgegenüber unproblematisch dar. Er verfügt unzweifelhaft über die von Art. 28 EG-Datenschutzrichtlinie geforderte „völlige Unabhängigkeit".

Vom Rundfunkrat wurde für eine Übertragung der Kontrolle auf den Rundfunkdatenschutzbeauftragten die Staatsferne des Rundfunks vorgetragen. Hierzu ist zu bedenken: Bei dem Gebot der Staatsferne geht es darum, staatliche Gestaltung oder Einwirkung zu vermeiden, die unmittelbar oder mittelbar die publizistische Arbeit beeinträchtigt. Durch die Schaffung des „Medienprivileges" hat der Gesetzgeber der Rundfunkfreiheit Rechnung getragen (vgl. Ziff. 14.3 dieses Berichts). Das Medienprivileg für die journalistisch-redaktionelle Arbeit bildet damit die verfassungsrechtlich gebotene einfachgesetzliche Lösung des grundrechtlichen Konflikts zwischen Datenschutz und Rundfunkfreiheit. Die Kontrolle des administrativen Bereiches gehört aber nicht zum verfassungsrechtlich geschützten Kernbereich der Rundfunkfreiheit. Aus diesem Grunde sehe ich auch nicht, inwiefern die Staatsferne der Rundfunkanstalt durch eine externe, unabhängige Kontrolle im administrativen Bereich in irgendeiner Weise beeinträchtigt werden könnte. Darüber hinaus ist der Landesbeauftragte für den Datenschutz keine klassische Staatsaufsicht und unterliegt auch keiner Weisungsbefugnis. Seine Legitimation hat er durch das Parlament erhalten.

In diesem Zusammenhang ist darauf hinzuweisen, dass beim Landesrechnungshof eine vergleichbare Situation besteht. Verfassungsrechtliche Bedenken gegenüber dieser Kontrollinstitution wurden bisher nicht erhoben. Anzumerken ist darüber hinaus, dass der Landesbeauftragte für den Datenschutz in entsprechendem Umfang wie bei Radio Bremen auch für die Datenschutzkontrollen bei der dritten Gewalt, der Judikative, zuständig ist. Auch von hier sind bisher keine Bedenken geäußert worden, obwohl hier im gleichen Umfang wie bei Radio Bremen jeweils im Einzelfall geprüft werden muss, ob durch eine Prüfung des Landesbeauftragten für den Datenschutz die Unabhängigkeit der Rechtssprechung tangiert würde.

In den letzten Jahren hat sich meine Prüftätigkeit in erster Linie auf die Verarbeitung von Rundfunkteilnehmerdaten bei der Gebühreneinzugszentrale (GEZ) erstreckt. Die GEZ verarbeitet für Radio Bremen im großen Umfang personenbezogene Daten (vgl. in diesem Zusammenhang die Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder zur Neuordnung der Rundfunkfinanzierung, Ziff. 18.9 dieses Berichts). Die Datenverarbeitung der GEZ ist eindeutig dem administrativen und nicht dem journalistisch-redaktionellen Bereich zuzuordnen. Gerade im Hinblick auf die GEZ mehren sich die Beschwerden aus der Bevölkerung. Durch eine Übertragung der Kontrolle des administrativen Bereiches auf den Rundfunkdatenschutzbeauftragten würde den schutzwürdigen Interessen der Betroffenen nicht ausreichend Gehör geschenkt werden, da zu befürchten ist, dass dieser sich nicht völlig frei von anderen Erwägungen machen kann.

Als wesentliches Ergebnis lässt sich festhalten, dass die geltende Rechtslage rechtskonform ist, dass ökonomische und arbeitspraktische Überlegungen dazu geführt haben, dem Landesbeauftragten für den Datenschutz die Kontrolle des administrativen Bereiches zu übertragen, dass es in den vielen Jahren, in denen die jetzige Rechtslage gilt, zu keinerlei Verletzungen des Medienprivilegs bei Datenschutzkontrollen gekommen ist. Schließlich ist nicht nachzuvollziehen, warum man sich nicht bei der erst kurze Zeit zurückliegenden Gesetzgebungsberatung zur Novellierung des Bremischen Datenschutzgesetzes zu Wort gemeldet hat. Das an die EU-Datenschutzrichtlinien angepasste Bremische Datenschutzgesetz ist knapp ein Jahr alt und sollte daher nicht ohne Not geändert werden. Eine solche Notwendigkeit vermag ich momentan nicht zu erkennen.

Ich habe den Rechtsausschuss der Bremischen Bürgerschaft über die Initiative des Rundfunkrates informiert. Er will sich auf einer der nächsten Sitzungen mit dem Thema beschäftigen.

14.3 Redaktionsdatenschutz bei der Presse

Obwohl die Presse dem nicht öffentlichen Bereich zuzuordnen ist, wird dieses Thema aus Gründen der Übersichtlichkeit im öffentlichen Bereich mitbehandelt.

Presseunternehmen verfügen über umfangreiches personenbezogenes Informationsmaterial, welches sie für ihre Berichterstattung sammeln, auswerten und veröffentlichen. Für den Bereich der journalistisch-redaktionellen Tätigkeit sind die Datenschutzgesetze jedoch nur eingeschränkt anwendbar. Das Grundgesetz garantiert in Art. 5 Abs. 1 die Pressefreiheit, welche für eine demokratische Willensbildung unabdingbar ist. Da die Presse darauf angewiesen ist, Informationen zu sammeln, um ihrem Verfassungsauftrag nachkommen zu können, partizipiert die Informationsverarbeitung am Grundrechtsschutz, sie ist daher aus dem Anwendungsbereich des Bundesdatenschutzgesetzes (BDSG) weitestgehend herausgenommen. Es gilt für die Presse das „Medienprivileg" (§ 41 BDSG). Das hat zur Folge, dass dem Landesbeauftragten für den Datenschutz in diesem Bereich keine Kompetenzen zustehen. Es besteht aber auch kein „Freibrief" seitens der Presse. Betroffene können sich im journalistisch-redaktionellen Bereich gegen unverhältnismäßige Eingriffe in ihr Recht auf informationelle Selbstbestimmung wehren. Bei datenschutzrechtlichen Verstößen ist in diesen Fällen der Deutsche Presserat zuständig, dessen Anschrift lautet:

Deutscher Presserat	Postanschrift:	Tel.: 02 28 - 9 85 72 - 0
Gerhard-von-Are-Straße 8	Postfach 71 60	Fax: 02 28 - 9 85 72 - 99
53111 Bonn	53071 Bonn	www.presserat.de

Der Deutsche Presserat hat einen Leitfaden zum Redaktionsdatenschutz herausgegeben. Dieser Leitfaden und Hilfestellungen für Betroffene können unter http://www.redaktionsdatenschutz.de abgerufen werden. Außerdem hat der Deutsche Presserat einen Beschwerdeausschuss für den Redaktionsdatenschutz eingerichtet, an den sich jeder Bürger wenden kann. Zum Jahreswechsel hat der Deutsche Presserat erstmals einen eigenen Tätigkeitsbericht zum Redaktionsdatenschutz herausgegeben.

Abschließend ist anzumerken, dass das Medienprivileg nicht gilt, wenn personenbezogene Daten von der Presse zu Verwaltungszwecken verarbeitet werden (z. B. Daten der Angestellten, Daten von Abonnenten). Hier ist die Pressefreiheit nicht in ihrem Kern betroffen. Bei datenschutzrechtlichen Verstößen in diesem Bereich steht mir ein Prüfrecht zu.

15. 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 (Datenabgleich), Ziff. 1.11 (Beratung neuer Datenschutz-Vorschriften im Land), Ziff. 4.2 (Ergebnisse der Beratung des 25. Jahresberichts), Ziff. 5.5 (Aushang mit personenbezogenen Bewerberdaten), Ziff. 6.1.3 (Rasterfahndung in Bremen abgeschlossen), Ziff. 6.4 (Übermittlung von Einwohnermeldedaten im Vorfeld der Bürgerschafts- und der Stadtverordnetenwahl), Ziff. 7.3 (Veröffentlichung der Insolvenzbekanntmachungen im Internet), Ziff. 8.2.3 (Interne Vernetzung des Gesundheitsamtes Bremerhaven), Ziff. 9.3 (Funk-LAN-Verbindung im Amt für Jugend und Familie Bremerhaven), Ziff. 9.6 (Supervision für Pflegeeltern), Ziff. 14.1 (Webcam in den Hörfunkstudios der Offenen Kanäle), Ziff. 16.4.3 (Webcam in gastronomischen Einrichtungen), Ziff. 16.7.2 (Lebensgeschichte und Biographiefragebögen in Pflegeeinrichtungen).

16. Datenschutz in der Privatwirtschaft

16.1 Kreditwirtschaft

16.1.1 Mitteilung von Kontoinformationen an den Ehepartner

In einem Fall ist mir bekannt geworden, dass durch ein bremisches Kreditinstitut dem Ehemann Auskunft über die Zinsen erteilt wurde, die auf Konten seiner Ehefrau anfielen. Dem Ehemann war bis dahin von dem Konto seiner Frau nichts be-

kannt. Der Ehemann benötigte die Zinsinformationen zur Anpassung des bei diesem Kreditinstitut für die Eheleute gemeinsam bestehenden Freistellungsauftrags.

Ein solches Vorgehen der Bank stellt einen nicht unerheblichen Verstoß gegen das Bundesdatenschutzgesetz dar. Ein Auskunftsbegehren des einen Ehepartners über Konten des anderen Ehepartners ist nur zulässig bei Vorliegen einer entsprechenden Bevollmächtigung, sofern nicht ohnehin beide Partner Kontoinhaber sind. Eine solche rechtsgeschäftlich eingeräumte Befugnis zur Informationserlangung über das fremde Konto kann auch nicht aus dem schon bestehenden gemeinschaftlichen Freistellungsauftrag geschlossen werden. Dieser stellt nur eine Anweisung des jeweiligen Kontoinhabers an das Kreditinstitut dar, bis zum angegebenen Höchstbetrag keinen Abzug von den gutgeschriebenen Zinsen des eigenen Kontos vorzunehmen. Dies gilt auch, wenn die Erklärung gemeinschaftlich von den Ehepartnern abgegeben worden ist, so dass eine inhaltliche Abhängigkeit von den zugunsten des Partners gutgeschriebenen Zinsen besteht. Eine Kompetenz, Informationen über fremde Konten des Ehepartners zu erlangen, wird mithin nicht vermittelt. Es ist daher dem Kreditinstitut auch nicht gestattet, auf Verlangen des einen Ehepartners diesem das entsprechende Freistellungsformular mit der Summe der zugunsten des anderen Ehepartners anfallenden Zinsen auszuhändigen, damit es anschließend der Kontoinhaber unterzeichnet.

Das Kreditinstitut hat zugesagt, die vorstehenden Hinweise zukünftig zu beachten.

16.1.2 Schufa-Auskunft bei Girokonto auf Guthaben-Basis

In der letzten Zeit hat sich gezeigt, dass die Kreditinstitute zunehmend dazu übergehen, auch bei Girokonten, für die ausdrücklich keine negativen Kontostände vorgesehen sind, Informationen mit der Schufa auszutauschen; die für viele Menschen schwieriger gewordene wirtschaftliche Lage verstärkt diese Tendenz noch. Selbst wenn der Kunde bei der Kontoeröffnung mitteilt, für ihn komme nur ein reines Guthaben-Konto in Betracht, wird zu diesem vom Kontoinhaber die Einwilligung in die bekannte Schufa-Erklärung gefordert und bei Verweigerung das Konto nicht eröffnet. Obwohl in diesen Fällen ein kreditorisches Risiko für das Institut nicht besteht, rechtfertigt die Kreditwirtschaft dieses Vorgehen mit dem Hinweis auf andere Risiken, die durch den Informationsaustausch mit der Schufa ausgeschlossen werden könnten. Als Beispiel werden hier Fälle angeführt, bei denen Kunden unter Hinterlassung erheblicher Schulden unbekannt verzogen sind und anschließend durch Eröffnung neuer Konten bei einem anderen Institut weiterhin unentdeckt zu bleiben beabsichtigen. Während für dieses Vorgehen zugleich die Vertragsfreiheit streitet, nach der auch Geldinstitute grundsätzlich selbst entscheiden können, welche Kontoverträge sie zu schließen bereit sind, steht dem heutzutage das faktische Bedürfnis des Kunden nach einem Girokonto entgegen, ohne das auch für Privatpersonen die Teilnahme am normalen wirtschaftlichen Leben kaum noch denkbar ist. Gerade bei negativen Schufa-Einträgen besteht dann jedoch die Gefahr der Verweigerung eines solchen Kontos. Die Problematik wird allerdings dadurch erheblich entschärft, dass sich – nicht zuletzt um einem Handeln des Gesetzgebers zuvorzukommen – die Kreditwirtschaft durch eine Empfehlung ihres zentralen Kreditinstitutes faktisch gebunden hat, ein „Konto für Jedermann" einzurichten. Dieses wird nur auf Guthaben-Basis geführt und soll gerade sozial und wirtschaftlich schwachen Bevölkerungskreisen den Zugang zu einem Girokonto ermöglichen. Auch negative Schufa-Einträge sind danach kein Grund, ein solches Konto zu verweigern, sofern nicht weitere besondere Umstände hinzutreten. Die Kreditwirtschaft hat abermals die Einhaltung der genannten Empfehlung versichert. Ich rate daher jedem, dem wegen entsprechender Einträge ein Girokonto verweigert wird, sich auf diese Empfehlung zu berufen und notfalls Kontakt zu den Ombudsleuten aufzunehmen, die bei den Verbänden der einzelnen Institutsgruppen eingerichtet sind.

16.2 Handels- und Wirtschaftsauskunfteien

16.2.1 „Undurchsichtige" Erhebung von Daten durch Unternehmen der Privatwirtschaft

Im vergangenen Jahr erhielt ich wiederholt Eingaben betroffener Bürger, die die Erhebung ihrer Daten durch Unternehmen der Privatwirtschaft beklagten. Insbesondere war es den Betroffenen nicht möglich, den Zweck der Datenerhebung

oder gar die Identität der für die Erhebung verantwortlichen Stelle aus dem Auskunftsbegehren zu entnehmen. So beschwerte sich ein Petent darüber, durch ein Inkassounternehmen ohne erkennbaren Anlass ausgefragt worden zu sein. In einem anderen Fall beklagte sich ein Betroffener, dass eine Wirtschaftsauskunftei über ihn und seine Ehefrau bei seiner Mutter Daten erhoben habe, u. a. den Namen des Arbeitgebers, ohne sich korrekt zu erkennen zu geben. Vielmehr sei der Mutter der Name eines unbeteiligten Unternehmens genannt worden.

Die Unternehmen der Privatwirtschaft haben bei der Erhebung personenbezogener Daten insbesondere § 4 i. V. m. §§ 28, 29 Bundesdatenschutzgesetz (BDSG) zu beachten. Gemäß § 4 Abs. 2 S. 1 BDSG sind personenbezogene Daten grundsätzlich direkt beim Betroffenen zu erheben. Er ist dabei in der Regel gemäß § 4 Abs. 3 S. 1 BDSG von der verantwortlichen Stelle zu unterrichten über

— die Identität der verantwortlichen Stelle,

— die Zweckbestimmungen der Erhebung, Verarbeitung oder Nutzung und

— die Kategorien von Empfängern, soweit der Betroffene nach den Umständen des Einzelfalles nicht mit der Übermittlung an diese rechnen muss.

Werden personenbezogene Daten dem entgegen durch den Auskunftsbegehrenden erschlichen, indem er beispielsweise eine falsche Identität vortäuscht, so erfüllt dies gemäß § 43 Abs. 2 Nr. 4 BDSG den Tatbestand einer bußgeldbewährten Ordnungswidrigkeit. Wird die Tat gegen Entgelt oder in der Absicht begangen, sich oder einen anderen zu schädigen, so ist sie gemäß § 44 Abs. 1 BDSG strafbar.

Angesichts der mir zugesandten Eingaben führte ich datenschutzrechtliche Prüfungen bei den betreffenden Unternehmen durch. In einem der beiden vorstehend genannten Fälle hatte das Ergebnis der Prüfung zur Folge, dass der Betroffene bei der Staatsanwaltschaft einen Strafantrag wegen einer Straftat nach § 44 Abs. 1 i. V. m. § 43 Abs. 2 Nr. 4 BDSG stellte.

16.2.2 Darlegung des berechtigten Interesses an der Auskunftserteilung

Die Erteilung einer Auskunft durch eine Wirtschaftsauskunftei setzt in der Regel voraus, dass der Anfragende ein berechtigtes Interesse an der erbetenen Information darlegt. Dieses ist von der Auskunftei zu prüfen. In der Praxis wird dies rechtskonform dadurch realisiert, dass der anfragende Kunde der Auskunftei versichert, es liege ein berechtigtes Interesse vor und die Auskunftei dieses stichprobenweise überprüft. Nach Feststellung der Datenschutzaufsichtsbehörden hat sich jedoch bei den Kunden der Auskunfteien ein bisweilen allzu großzügiger Umgang mit der Annahme eines berechtigten Interesses eingeschlichen. Dies wird teilweise auch dadurch unterstützt, dass die Auskunfteien ihren Kunden die Versicherung des berechtigten Interesses durch Formulare erleichtern, auf denen nur allgemein gehaltene Begriffe wie „Geschäftsanbahnung", „Bonitätsprüfung" oder „sonstiges berechtigtes Interesse" anzukreuzen sind. Es ist daher ein Anliegen der Aufsichtsbehörden, dem Auskunftei-Kunden deutlicher vor Augen zu führen, welche Anforderungen an das Vorliegen eines berechtigten Interesses zu stellen sind. Der Verband der Handelsauskunfteien wird hierzu den Datenschutzaufsichtsbehörden Vorschläge unterbreiten.

16.2.3 Schufa-Auskunft für einen Kleingartenverein

Ein bremischer Kleingartenverein hatte mir bestätigt, dass er Bewerber um eine Vereinsmitgliedschaft regelmäßig auffordere, den Verein zu ermächtigen, eine Auskunft bei der Schufa über sie einzuholen. Den Interessenten wurde hierfür ein entsprechendes Formular vorgelegt, das sie unterzeichnen sollten. Mir gegenüber hat der Verein erklärt, dies sei erforderlich, da ihm in zunehmendem Maße hohe Schäden durch insolvente Mitglieder entstünden.

Ich habe den Verein darauf hingewiesen, dass die Einwilligungserklärung allein keine Möglichkeit einräume, über den Betroffenen personenbezogene Auskünfte bei der Schufa zu erhalten. Mindestens wäre der Abschluss eines entsprechenden Rahmenvertrages erforderlich, der von der Schufa nur einem begrenzten Kreis von Unternehmen angeboten wird. Um gleichwohl auch den Interessen des Vereins

Rechnung zu tragen, habe ich stattdessen vorgeschlagen, dass sich der Verein um Einsichtnahme in das Schuldnerverzeichnis beim Amtsgericht bemühe sowie Einblick nehme in die öffentlichen Bekanntmachungen über die eröffneten Insolvenzverfahren.

Der Verein hat mir zugesagt, zukünftig diese Vorschläge zu berücksichtigen und auf die Vorlage von Einwilligungserklärungen für die Einholung von Schufa-Auskünften zu verzichten.

16.2.4 Schufa-Auskunft im Rahmen der Anbahnung eines Mietvertragsverhältnisses

Einem Mietinteressenten ist von einem Bremer Wohnungsunternehmen mitgeteilt worden, aufgrund einer Schufa-Auskunft könne ihm keine Wohnung zur Verfügung gestellt werden. Der Betroffene hat mir gegenüber dargelegt, er sei über die Einholung einer derartigen Auskunft vorher weder informiert worden noch habe er darin eingewilligt.

Ich habe daher dem Wohnungsunternehmen dargelegt, dass die Daten grundsätzlich beim Betroffenen zu erheben sind, andernfalls nur, wenn es zur Erfüllung des Geschäftszweckes erforderlich ist und keine überwiegenden schutzwürdigen Interessen des Betroffenen beeinträchtigt werden. Eine Beeinträchtigung liegt nicht vor, wenn ein Mindestmaß an Mitwirkung des Betroffenen gewährleistet ist.

Insoweit halte ich die regelmäßige Einholung einer Schufa-Auskunft ohne Mitwirkung des Mietinteressenten nicht für erforderlich. Ein Mietinteressent kann vorher gefragt werden, ob er eine derartige Auskunft beibringen möchte oder ob sie vom Vermieter direkt bei der Auskunftei eingeholt werden soll. Auch wenn von vornherein beabsichtigt ist, eine derartige Auskunft direkt bei der Auskunftei einzuholen, sollte der Mietinteressent vorher darauf hingewiesen werden. Dann kann er entscheiden, ob er die Anbahnung eines Mietvertragsverhältnisses abbricht oder die Datenverarbeitung hinnimmt.

Das Wohnungsunternehmen hat mir daraufhin erklärt, in Zukunft werde entsprechend verfahren.

16.2.5 Erhebung vermeintlicher Insolvenzdaten über einen Mietinteressenten

Ein Bremer Wohnungsunternehmen hat den Abschluss eines Mietvertrages mit einem Mietinteressenten abgelehnt unter Hinweis auf eine Eintragung über die Eröffnung eines Insolvenzverfahrens zu seiner Person. Weil der Betroffene dieses bestritt, hat er eine Bescheinigung des Amtsgerichts Bremen erhalten und diese dem Wohnungsunternehmen vorgelegt. Trotzdem sei ihm der Abschluss eines Mietvertrages verwehrt worden.

Auf meine Anfrage erklärte das Wohnungsunternehmen, diese Eintragung habe sie von der Auskunftei Infoscore Consumer Data GmbH in Baden-Baden erhalten. Offensichtlich wegen meiner Aktivitäten und dem Hinweis auf die Bescheinigung des Amtsgerichts war das Unternehmen nun bereit, dem Mietinteressenten eine Wohnung anzubieten.

Nachdem der Betroffene aufgrund meiner Empfehlung die Bescheinigung des Amtsgerichts Bremen InfoScore vorlegte, erfuhr er von dieser, es handele sich um eine Verwechslung, die Auskunftei werde die Daten entsprechend berichtigen.

16.2.6 Erweiterung des Geschäftsfeldes der Schufa

Die Schufa Holding AG ist im Berichtsjahr erneut ins Datenschutz-Blickfeld einer breiteren Öffentlichkeit getreten. Dies ist weniger durch die bereits im letzten Jahresbericht angesprochene gestraffte Unternehmensstruktur der Schufa begründet; vielmehr erfordert die zunehmende Ausdehnung des geschäftlichen Tätigkeitsfelds des Unternehmens eine verstärkte Beachtung durch die Datenschutzaufsichtsbehörden. Während die Schufa nach ihrer ursprünglichen Firmierung als „Schutzgemeinschaft für allgemeine Kreditsicherung" im Wesentlichen zur Informationsbereitstellung für die Kreditwirtschaft tätig war, soll nunmehr das Geschäftsfeld des Nichtbanken-Sektors ausgebaut werden. Dies gilt insbesondere für die

Schwerpunkte Wohnungswirtschaft, Versicherungsgesellschaften und Inkassounternehmen. Die Datenschutzproblematik entsteht dabei weniger aus den Teilbereichen an sich, als vielmehr aus ihrer Betreuung aus einer Hand bei der Schufa, da diese praktisch über jeden Einwohner, der in Deutschland ein Konto besitzt, Daten verarbeitet. Zurzeit sind dies Daten zu ca. 59 Millionen Personen. Es kann daher nicht von der Hand gewiesen werden, dass mit der Eröffnung weiterer Geschäftsfelder der sensible Datenbestand unter Zurückdrängung bisher bestehender Restriktionen weiten Teilen der Wirtschaft zur Verfügung gestellt wird. Dabei besteht die Gefahr, dass dem Betroffenen ein bestimmtes Verhalten im Einzelfall durch die Weitergabe der Information durch die Schufa in seinem alltäglichen Leben zum Nachteil gereicht. Es muss mithin aus der Sicht des Datenschutzes zumindest ein besonderes Augenmerk auf eine weitgehende Trennung der einzelnen Tätigkeitsfelder gelegt werden und hinreichend geprüft werden, welche Art von personenbezogenen Daten im jeweiligen Teilbereich tatsächlich erforderlich ist.

16.2.7 Wahrung des Geschäftsgeheimnisses bei Auskunftsbegehren des Betroffenen

Bei der Erteilung einer Auskunft sind Auskunfteien verpflichtet, den Betroffenen über die Datenübermittlung zu benachrichtigen. In der Vergangenheit ist es jedoch vielfach vorgekommen, dass dem Betroffenen anschließend die Information darüber verweigert wurde, welcher Stelle die zu seiner Person gehörenden Daten übermittelt wurden. Dies wurde regelmäßig pauschal mit dem Geschäftsgeheimnis begründet, das es zu wahren gelte und dem besonderen Interesse des Auskunftsempfängers an seiner Geheimhaltung. Die Datenschutz-Aufsichtsbehörden haben demgegenüber seit langem einen offeneren Umgang mit der Information über den Auskunftsempfänger gefordert, da die Wahrung des Geschäftsgeheimnisses gegenüber dem Informationsanspruch des Betroffenen datenschutzrechtlich einen Ausnahmefall bildet und einer Abwägung im Einzelfall bedarf.

Es besteht die Aussicht, dass die Auskunfteien zukünftig bereit sind, sich für wichtige Fallgruppen generell nicht mehr auf ein zu wahrendes Geschäftsgeheimnis berufen, um eine Auskunft über die Identität des Auskunftsempfängers zu verweigern. Dies betrifft z. B. die Fälle, in denen der Betroffene begründete Zweifel an der Richtigkeit der Daten vorträgt oder Auskunftserteilungen an Unternehmen aus den Bereichen der Kredit- und Versicherungswirtschaft, des Versandhandels oder Telekommunikationsbranche erfolgen. Sofern dies in der Praxis auch umgesetzt wird, wäre ein erheblicher datenschutzrechtlicher Fortschritt erreicht, zumal die überwiegende Anzahl der Fälle, bei denen bislang eine Berufung auf das Geschäftsgeheimnis erfolgte, von den genannten Fallgruppen erfasst wird.

16.2.8 Datenübermittlung durch Auskunftei an Factoring-Bank

In einem Fall hat mir ein Petent berichtet, dass eine Auskunftei personenbezogene Daten über ihn an eine Bank übermittelt hatte. Der Petent selbst stand dabei in keiner Beziehung zur Bank, so dass er sich den Hintergrund der Übermittlung nicht erklären konnte. Die Aufklärung wurde zunächst dadurch erschwert, dass die Bank bei meiner Bitte um Aufklärung einen Warenkredit als ihr berechtigtes Interesse angab. Tatsächlich entsprach diese weitgehend formularmäßig abgegebene Erklärung jedoch nicht den Tatsachen, sondern stellte eine allzu starke Verkürzung des Sachverhaltes dar. Ich verweise an dieser Stelle auch auf meine Ausführungen zu Ziff. 16.2.2 dieses Berichts.

In dem angesprochenen Fall handelte die Bank dagegen tatsächlich als Factor und hatte eine Forderung aufgekauft, die der Petent als Schuldner durch einen Warenkauf auf Ziel bei einem Handelsunternehmen hatte entstehen lassen und die anschließend von diesem Unternehmen an die Bank im Wege des Forderungsverkaufs an die Bank abgetreten wurde. Die Bank mag in einer solchen Konstellation einzelfallbezogen ein berechtigtes Interesse an der Datenübermittlung durch eine Auskunftei haben, um die Bonität des Schuldners beurteilen zu können. Ich halte es jedoch für datenschutzrechtlich unzulässig, wenn ein einzelner Factoring-Fall von der Bank zum Anlass genommen wird, zum Zwecke der Festsetzung einer Kreditlinie für eventuelle weitere, in der Zukunft liegende Ankäufe von Schulden dieses Betroffenen sich bereits im Vorfeld Daten über ihn übermitteln zu lassen. Der Unterschied ist signifikant, da bei Einräumung einer Kreditlinie die Daten

auch nach Abwicklung des Einzelfalls weiterhin verarbeitet werden können. Im Falle des Petenten hat sich jedoch herausgestellt, dass es sich nur um einen Einzelfall handelte und im Übrigen die Factoring-Bank nach eigenem Bekunden entgegen eines ersten Anscheins nur Forderungen von Geschäftskunden ankauft.

16.3 Arbeitnehmerdatenschutz

16.3.1 Betriebsvereinbarung zur E-Mail- und Internetnutzung

Journalisten eines Medienunternehmens haben moniert, nach der dort beabsichtigten Betriebsvereinbarung würde bei jeder Abwesenheit ihr jeweiliges E-Mail-Fach automatisch an einen Vertreter umgleitet. Hierbei könnte hinsichtlich der eingehenden privaten E-Mails das Fernmeldegeheimnis gefährdet sein. Das Fernmeldegeheimnis werde auch verletzt, weil alle Internetzugriffe personenbezogen protokolliert würden.

Nach Gesprächen mit der Geschäftsführung, dem Beauftragten für den Datenschutz und dem Betriebsrat ergab sich, dass ein erhebliches geschäftliches Interesse des Medienunternehmens besteht, dass eingehende Informationen – auch per E-Mail – unverzüglich in die Berichterstattung einfließen und diese deshalb auf die automatische Weiterleitung nicht verzichtet werden kann. Aus diesem Grunde ist nunmehr in der Betriebsvereinbarung festgelegt worden, dass eine private E-Mail-Nutzung nicht zulässig ist. Insoweit muss jeder Nutzer selbst dafür sorgen, dass er keine privaten E-Mails erhält.

Unabhängig davon, ob vor Ort die private oder nur die dienstliche Internet-Nutzung erlaubt wird, haben sich die Geschäftsleitung und der Betriebsrat letztendlich darauf geeinigt, Internetzugriffe nur noch gruppenbezogen zu protokollieren. Dabei muss die Gruppe aus mindestens zehn bis 15 Personen bestehen. Soweit bei diesen anonymisierten Auswertungen in der Betriebsvereinbarung präzise beschriebene unzulässige bzw. rechtswidrige Internetzugriffe erfolgen, wird unter Beteiligung des Betriebsrats und des Beauftragten für den Datenschutz für einen begrenzten Zeitraum in der Gruppe personenbezogen protokolliert, von der die unzulässige Nutzung ausging.

Diese in der Betriebsvereinbarung dezidiert festgelegte Verfahrensweise gewährleistet einerseits die Einhaltung des Fernmeldegeheimnisses und stellt eine dem Grundsatz der Verhältnismäßigkeit entsprechende Kontrolle der Arbeitnehmer dar, auch weil die Beschäftigten eindeutig über Art und Ausmaß dieser angemessenen Protokollierung und Kontrolle informiert sind.

Die Betriebsvereinbarung ist nach Angaben des Beauftragten für den Datenschutz in der geänderten Form Anfang 2004 in Kraft getreten. Sie werde für alle Nutzer ins unternehmenseigene Intranet gestellt. Außerdem würden die in der Betriebsvereinbarung angesprochenen Nutzergruppen eingerichtet. Danach sei vorgesehen, den Mitarbeitern nutzergruppenweise den Inhalt der Betriebsvereinbarung und damit auch eventuell daraus erwachsende Konsequenzen nahe zu bringen. Die Teilnahme an diesen Veranstaltungen bestätige der Mitarbeiter durch Unterschrift. Nach Abschluss der Schulungen würden die in der Betriebsvereinbarung festgelegten Prozeduren eingeführt. Vorher erfolge keinerlei Protokollierung.

16.3.2 Information des Betriebsrats über fehlzeitenbedingte Mitarbeitergespräche

Ein Unternehmen aus der Luftverkehrsbranche hat mich über das Konzept „Fehlzeitenbedingte Mitarbeitergespräche" unterrichtet und gefragt, ob die obligatorische Einbeziehung des Betriebsrats in jedem Einzelfall zulässig ist.

Ich habe dargelegt, dass es zu den Aufgaben des Betriebsrats nach § 80 Abs. 1 Nr. 2 Betriebsverfassungsgesetz (BetrVG) gehört, darüber zu wachen, dass das vorgenannte Konzept zugunsten der Beschäftigten verwirklicht wird. Daher kann dem Betriebsrat die Mitwirkung nicht verwehrt werden, wenn dies zu einer Behinderung seiner gesetzlichen Aufgabe führen kann. Ob der Betriebsrat über jedes anstehende Gespräch informiert werden und an jedem Gespräch teilnehmen muss, obliegt seiner eigenen Beurteilung im Rahmen des § 80 Abs. 2 Satz 2 BetrVG. Hierbei könnte berücksichtigt werden, ob die jeweiligen Beschäftigten des

Unternehmens die Einschaltung des Betriebsrats wünschen. Soweit der Betriebsrat es für erforderlich hält, über anstehende Gespräche vorher informiert zu werden, wird ihm dies nicht verwehrt werden können.

16.3.3 Aufzeichnen telefonischer Bestellungen durch ein Call-Center

Ich bin gefragt worden, ob es zulässig ist, dass ein Unternehmen, das Stadtautos im Rahmen von „CarSharing" an Privatkunden vermietet, alle telefonischen Bestellungen bei ihrem Call-Center aufzeichnet. Nach meiner Prüfung hat sich folgendes Bild ergeben: CarSharing basiert darauf, dass Privatpersonen Kunden des Unternehmens und damit Teilnehmer des vom Unternehmen betriebenen CarSharings werden. Insoweit bilden sie eine geschlossene Benutzergruppe. Mit dem Erhalt einer AutoCard erhält jeder Kunde die Möglichkeit, jederzeit ein Fahrzeug aus dem Fuhrpark des Unternehmens zu bestellen. Hierbei werden Kundennummer, Beginn und Ende der Fahrzeugnutzung sowie Standort des Fahrzeugs erhoben und gespeichert. Damit soll gewährleistet werden, dass der Kunde gemäß seiner Bestellung das Fahrzeug nutzen kann.

Bestellungen erfolgen telefonisch oder per E-Mail. Telefonische Betellungen werden per Band als Sprachdatei aufgezeichnet. Sie dauern i. d. R. 30 bis 45 Sekunden. Die Gespräche haben regelmäßig einen rein geschäftlichen Charakter und sind erforderlich, um Reklamationen zu klären, wenn dem Kunden die Nutzung nicht in der bestellten Weise möglich ist (Fahrzeug steht nicht am gewünschten Standort oder zur gewünschten Zeit nicht zur Verfügung, Ausstattung entspricht nicht der Bestellung, etc.). Außerdem wird die monatlich oder vierteljährlich berechnete Nutzung nicht immer vom Kunden akzeptiert.

In diesen Fällen besteht nur die Möglichkeit, anhand der jeweiligen Aufzeichnung der Gespräche nachzuweisen, was tatsächlich bestellt worden bzw. wer für den Fehler verantwortlich ist. Hierbei wird vor dem Kunden die jeweilige telefonische Aufzeichnung seiner Bestellung abgespielt, wenn sich herausstellt, dass das Verschulden beim Kunden liegt. Die Aufzeichnungen können nur von einem bestimmten PC aktiviert werden. Diese Aktivierung wird protokolliert. Die Kunden werden über die Aufzeichnung, deren Zweck und die dreimonatige Speicherdauer im Handbuch informiert. Jeder Kunde, also jeder Teilnehmer dieser geschlossenen Benutzergruppe, erhält ein Exemplar des Handbuches.

Bei der Aufzeichnung der telefonischen Bestellungen werden auch die Äußerungen der Arbeitnehmer im Call-Center erfasst und gespeichert. Die Aufzeichnungen werden nur zu dem vorgenannten Zweck der Beweissicherung verwendet. Eine Leistungs- und Verhaltenskontrolle findet nach Angaben des Unternehmens nicht statt. Die Arbeitnehmer sind über den Zweck der Aufzeichnungen informiert und haben die Möglichkeit, durch Umschaltung private Telefongespräche zu führen, die nicht aufgezeichnet werden.

Da keine Alternative zur Aufzeichnung der Telefongespräche vorhanden ist, ist sie zur Wahrung der berechtigten Interessen des Call-Centers erforderlich. Die genannte Zweckbindung und die Transparenz der Aufzeichnungen für die Teilnehmer und Arbeitnehmer sowie die kurze Speicherdauer lassen den Schluss zu, dass die schutzwürdigen Interessen der Betroffenen die Aufzeichnungen nicht überwiegen. Aus diesen Gründen sind die Voraussetzungen des § 28 Abs. 1 Nr. 2 Bundesdatenschutzgesetz (BDSG) erfüllt.

Es liegt auch kein Verstoß gegen § 201 Strafgesetzbuch (StGB) (Verletzung der Vertraulichkeit des Wortes) vor, da die Kenntnis der Gesprächsteilnehmer von der Aufzeichnung bereits die Anwendbarkeit dieser Rechtsvorschrift ausschließt.

16.3.4 Der Personalfragebogen nach erfolglosem Abschluss eines Bewerbungsverfahrens

Ein Bürger monierte, dass ihm nach erfolgloser Bewerbung bei einer Firma die Herausgabe seines Personalfragebogens verwehrt worden sei mit dem Hinweis, der von ihm ausgefüllte Fragebogen sei nun Eigentum der Firma. Da sich die Bewerbung erledigt hatte, war eine anhaltende Datenspeicherung nicht mehr erforderlich. Auf meine Intervention hat die Firma den Personalfragebogen vernichtet.

16.4 Webcams und Videoüberwachung

16.4.1 Videoüberwachung in der Innenstadt

Ein Bürger hat mich darauf hingewiesen, dass entlang der drei Karstadt-Schaufensterfronten (Obern- und Sögestraße sowie Lloydpassage) Videokameras so installiert und ausgerichtet sind, dass sie auch die Gehwege und den Bereich der Straßenbahnhaltestelle erfassen. Insoweit würden auch Personen erfasst, die sich nicht unmittelbar an den Schaufenstern des Kaufhauses aufhalten.

Auf Nachfrage habe ich gemeinsam mit dem Beauftragten für den Datenschutz des Karstadt-Konzerns vor Ort den Videoeinsatz auch durch Blick auf die Bildschirme überprüft. Hierbei hat sich der Hinweis des Bürgers bestätigt. Die Kameras sind daraufhin in meiner Gegenwart unverzüglich so ausgerichtet worden, dass nur noch Personen erfasst werden können, die sich in unmittelbarer Nähe der Schaufensterfronten befinden. Außerdem ist mir zugesichert worden, dass die festgelegte Ausrichtung regelmäßig durch den Beauftragten für den Datenschutz überprüft wird.

16.4.2 Videoüberwachung in Bussen und Bahnen

Die Bremer Straßenbahn AG (BSAG) hat sich im Dezember 2002 an mich gewandt, um die Vorgaben für den Videoeinsatz in ihren Bussen und Bahnen abzuklären. Hierzu habe ich neben der gesetzlichen Regelung des § 6 b Bundesdatenschutzgesetz (BDSG) auf das mit den Aufsichtsbehörden der Länder und dem Verband Deutscher Verkehrsunternehmen (VDV) abgestimmte Ergebnis zur Videoüberwachung in öffentlichen Verkehrsmitteln aus dem Jahre 2001 verwiesen, das dort vorliegt.

Auf meine konkrete Nachfrage erklärte die BSAG, sie habe die folgenden Festlegungen getroffen:

— Hinweisschilder (Piktogramme), die die Fahrgäste auf die Überwachung aufmerksam machen,

— Sichtung und Separierung der Aufzeichnungen nur bei sicherheitsrelevanten Vorkommnissen (z. B. Sachbeschädigungen, Übergriffe auf andere Fahrgäste oder den Fahrer),

— Beteiligung des Beauftragten für den Datenschutz und des Betriebsrats,

— Erstellung eines Protokolls über die Einsichtnahme in die Videoaufnahmen,

— Weitergabe nur zum Zwecke der Strafverfolgung an Polizei bzw. Staatsanwaltschaft,

— Löschung der Aufzeichnungen nach spätestens 48 Stunden.

Die Ausstattung des Videoeinsatzes werde nach Angaben der BSAG Ende des Jahres 2003 beginnen und bis zum Frühjahr März 2004 für ca. zwei Drittel der Fahrzeuge abgeschlossen sein. Die dazu erforderliche Verfahrensbeschreibung werde erst dann fertig sein und mir zur Verfügung gestellt werden.

Seit Anfang 2004 haben sich eine ganze Reihe von Bürgern an mich gewandt und wollten nähere Informationen über die Videoüberwachung erhalten. Hierbei wurde auch darauf hingewiesen, dass Anfragen an die BSAG von dortigen Ansprechpartnern nicht hinreichend beantwortet werden konnten und demzufolge an mich weiter verwiesen wurden. Ich habe daher die BSAG entsprechend unterrichtet und aufgefordert, unverzüglich die Verfahrensbeschreibung zu erstellen, damit diese dann entsprechend der Anforderung des § 4 g Abs. 2 Satz 2 BDSG jedermann auf Anforderung in geeigneter Weise verfügbar gemacht werden kann.

16.4.3 Webcams in gastronomischen Einrichtungen

Mehrere Gäste eines Cafés in Bremerhaven wandten sich gegen den Einsatz einer Webcam dort. Insbesondere wurde moniert, mit Hilfe der Webcam könne jedermann jederzeit und weltweit feststellen, wer sich mit wem im Café aufhalte. Zwar befinde sich neben mehreren Werbeschildern an der Eingangstür ein Hinweis,

dass mit Betreten des Cafés in die Aufnahmen eingewilligt werde. Die Gäste monierten, sie hätten diesen Hinweis zunächst gar nicht erkannt und sie könnten nicht wirksam darin einwilligen.

Nach Bestätigung des Sachverhalts vor Ort und durch Einsichtnahme in die Homepage des Cafés hat der Inhaber mir auf Anfrage erklärt, die Webcam sei für seine Geschäftszwecke erforderlich. Er wolle den Gästen anbieten, via Internet nachzusehen, ob noch Plätze im Café frei sind und ob Bekannte, mit denen man sich vielleicht verabredet habe, schon dort seien.

Ich habe dem Inhaber dargelegt, dass die schutzwürdigen Belange betroffener Gäste tangiert sein können. Wie die Beschwerden zeigten, sei nicht gewährleistet, dass jeder Gast wirksam in den Webcam-Einsatz eingewilligt habe. Die Veröffentlichung der Videoaufnahmen von sich im Café aufhaltenden Gästen im Internet als einem grenzenlos zugänglichen Medium ermöglicht nämlich vielfältige Verknüpfungs- und Verarbeitungsmöglichkeiten, die das Persönlichkeitsrecht der Betroffenen erheblich beeinträchtigen können. Der Einsatz einer Webcam in gastronomischen Einrichtungen ist daher i. d. R. dann datenschutzkonform, wenn technische Maßnahmen gewährleisten, dass Personen im Café über diesen Weg nicht erkannt werden können. Ich habe den Inhaber gebeten, entsprechende Maßnahmen zu treffen.

Darüber hinaus hat sich der „Düsseldorfer Kreis", der Zusammenschluss der obersten Aufsichtsbehörden der Länder, mit diesem Problem befasst. Dabei stand die Diskussion unter der Prämisse, dass die gastronomische Einrichtung gerade wegen der Internetübertragung als Geschäftsidee aufgesucht werde. Danach besteht Einigkeit, dass § 6 b BDSG nicht als Ermächtigungsgrundlage für den Einsatz von Webcams in gastronomischen Einrichtungen in Betracht kommt, denn die Übertragung ins Internet stellt eine über eine reine Videoüberwachung hinausgehende Maßnahme (Verbreitung) dar. Erforderlich ist vielmehr die Einwilligung des Betroffenen; diese kann allerdings grundsätzlich auch konkludent erteilt werden. Soweit der Besuch in der gastronomischen Einrichtung als sensitives Datum zu werten ist, ist eine schriftliche Einwilligung erforderlich.

16.5 Adresshandel

16.5.1 Haushaltsumfrage zum Zweck des Direktmarketing

Ein führendes Unternehmen des Direktmarketings hat mich auch im letzten Jahr wieder durch eine regelmäßig stattfindende Haushalts-Umfrage beschäftigt. Das Unternehmen hat seinen Sitz nicht in Bremen, so dass die Aufsichtsbehörde eines anderen Bundeslandes für die datenschutzrechtliche Aufsicht nach dem Bundesdatenschutzgesetz zuständig ist. Gleichwohl habe ich mich dadurch in diesem, wie auch schon in früheren gleichgelagerten Fällen, nicht gehindert gesehen, dem von zahlreichen Bremerinnen und Bremern an mich herangetragenen Bedürfnis nach Information insbesondere durch eine verstärkte Pressearbeit Folge zu leisten. Dies entspricht der mir vom Bremischen Datenschutzgesetz auferlegten Verpflichtung zur Aufklärung und Beratung über datenschutzrechtliche Belange.

Im konkreten Fall habe ich durch eine Pressemitteilung darauf aufmerksam gemacht, dass der vom Unternehmen den Betroffenen zugesandte Fragebogen mit fast 150 Fragen nicht zu einer anonymen Befragung dient, sondern vielmehr zu Werbezwecken gezielt eingesetzt wird und dass die Lebensgewohnheiten des Einzelnen verarbeitet und gespeichert werden. Der Fragenkatalog reicht dabei vom Einkommen über das Kaufverhalten bis zu Krankheiten und Angaben über Familienangehörige. Die Aufklärung über den beabsichtigten Verwendungszweck findet sich hingegen nur bei intensiver Lektüre des einleitenden Begleittextes. Ich habe daher jedem Empfänger eines solchen Fragebogens geraten, genau zu prüfen, ob er wirklich einen derart weitreichenden Einblick in seine persönlichen Lebensgewohnheiten ermöglichen möchte.

16.5.2 Nutzung von Kundendaten im Einzelhandel

Die Möglichkeiten der modernen Datenverarbeitungssysteme und ihre zunehmende Verknüpfung geben auch dem Handel vermehrte Gelegenheiten zur Nutzung der Daten, insbesondere zu Werbezwecken. Die bekanntesten Beispiele

dürften hier die Kundenbindungssysteme, wie beispielsweise Payback oder Happy Digits sein, bei denen sich mehrere Unternehmen einem System zur Rabattgewährung anschließen und mit dem System Daten austauschen. Hierbei ist von besonderer Bedeutung die Information für den Kunden, welche seiner beim Einkauf anfallenden Daten an welche Systemteilnehmer weitergegeben und wie diese Daten genutzt werden. Nur bei einer hinreichend deutlichen Aufklärung des Kunden kann dieser wirksam in bestimmte Zwecke der Datenverarbeitung einwilligen.

Diese Erkenntnis ist aber durchaus nicht nur für bundesweit verbreitete Kundenbindungssysteme relevant. So ist mir der Fall eines von Bremen aus agierenden Internet-Versandhandelsunternehmens bekannt geworden, das im Zuge der Kunden-Bestellungen anfallende Daten an andere Unternehmen zu Werbezwecken weitergegeben hat. Zugleich ist der eigene Firmensitz mit einem Ort in den USA angegeben worden. Sowohl für die Weitergabe der Daten als auch für die Datenübermittlung in die USA kommt hier der Einwilligung des Kunden die entscheidende Bedeutung zu. Ich habe das Unternehmen daher aufgefordert, die bisher allgemein gehaltene und in seine Allgemeinen Geschäftsbedingungen aufgenommene Einwilligungserklärung neu zu fassen und dabei den Kunden nicht nur die Einzelheiten der beabsichtigten Datenverarbeitung näher zu beschreiben, sondern die Erklärung auch deutlich von den übrigen Geschäftsbedingungen abzusetzen.

16.6 Angelegenheiten von Rechtsanwälten

16.6.1 Fehlgeleiteter Schriftwechsel durch Anwaltskanzlei

Eine Petentin beschwerte sich darüber, dass sie von einer Anwaltskanzlei mehrere Schreiben erhielt, die nicht für sie, sondern für eine Mandantin der Kanzlei bestimmt waren. Die Verwechslung kam dadurch zustande, dass die Namen der beiden Frauen sehr ähnlich waren. Die Petentin ging mit dem ersten Schreiben zu der Kanzlei und wies diese auf ihre Verwechslung hin. Von der Kanzlei wurde der Petentin zugesichert, dass der Irrtum in den Unterlagen korrigiert werden würde. Als sie trotzdem erneut Post (einen von der Kanzlei beantragten Kostenfestsetzungsbeschluss des Amtsgerichts) erhielt, die wieder für deren Mandantin bestimmt war, wandte sich die Bürgerin an mich. Ich wies die Kanzlei auf ihre Geheimhaltungspflichten bezüglich der Angelegenheiten ihrer Mandanten hin und forderte sie auf, ihren Datenbestand hinsichtlich der Petentin zu korrigieren. Seitens der Kanzlei wurde mir nunmehr mitgeteilt, dass sie ihre Adressdatenbestände korrigiert hat.

16.6.2 Mandantenkorrespondenz im Müll

Mir wurden von anonymer Seite Unterlagen zugestellt, welche in einer Mülltonne gefunden worden waren. Es handelte sich hierbei um mehrere Schriftsätze eines Rechtsanwaltes und damit um personenbezogene Mandantendaten in verschiedenen Angelegenheiten, die nicht ordnungsgemäß der Aktenvernichtung zugeführt worden waren. Ich habe die Kanzlei um Stellungnahme zu dem Fund und um Nachweis darüber gebeten, wie und in welcher Weise Akten und Entwürfe vernichtet werden. Die Kanzlei teilte mir mit, dass sich um ein Versehen gehandelt habe und die Mitarbeiterinnen und Mitarbeiter nochmals auf die Notwendigkeit der Vernichtung von Schriftstücken mit personenbezogenen Daten hingewiesen worden seien. Zudem wurde ein Nachweis über die generelle Aktenvernichtung durch eine Entsorgungsgesellschaft erbracht.

16.6.3 Anschreiben bei Nachlassangelegenheiten

Eine pflichtteilsberechtigte Bürgerin (der Pflichtteil bezeichnet den Mindestanteil einer Person am Nachlass eines verstorbenen nahen Angehörigen) monierte, dass sie von einer Rechtsanwältin in einem einheitlichen Schreiben mit anderen Erbberechtigten angeschrieben worden war. Dieses Schreiben enthielt personenbezogene Daten von beiden Pflichtteilsberechtigten, u. a. den Namen und die Höhe des Pflichtteilsanspruchs. Die Bürgerin war nicht damit einverstanden, dass ihre personenbezogenen Daten einem Dritten (den anderen Pflichtteilsberechtigten) zur Kenntnis gelangten. Auf Nachfrage bei der Rechtsanwältin teilte diese mir mit, dass die personenbezogenen Daten der anderen Seite an sich hätten geschwärzt

werden sollen, dieses aber aufgrund eines Büroversehens nicht geschehen sei. Im Nachgang regte ich an, gleich zwei getrennte Ausgangsschreiben zu erstellen, was angesichts der modernen Datenverarbeitungsmöglichkeiten leicht ist. Hierdurch kann vermieden werden, dass das Schwärzen der Daten vergessen wird oder die Schwärzung unvollkommen ist.

16.7 Gesundheit und Soziales

16.7.1 Fragebogen in der Zahnarztpraxis

„Willkommen in unserer Praxis" ist ein Fragebogen überschrieben, den ein Bremer Zahnarzt seinen Patienten vorlegt, die erstmals in seine Sprechstunde kommen. Ein Patient fühlte sich dadurch zu sehr ausgeforscht und legte mir den Vordruck zur Prüfung vor. Auf ihm wurden neben Namen und Anschrift, den akuten Beschwerden, vorangegangenen Zahnarztbesuchen, dem derzeitig behandelnden Arzt noch weitere Angaben erfragt. Hierzu zählte eine ganze Reihe anderer Erkrankungen, unterteilt nach Herz- und Kreislauferkrankungen, nach Allergien, nach Infektions- und sonstigen Krankheiten, nach Operationen, nach Drogenabhängigkeit und Schwangerschaft. Zunächst äußerte ich Zweifel daran, dass die letztgenannten Angaben für die zahnärztliche Behandlung wirklich erforderlich seien und gab daher zu Bedenken, dass die Erhebung dieser Daten unzulässig sein könnte.

Der angesprochene Zahnarzt und die durch ihn eingeschaltete Zahnärztekammer Bremen gingen nicht im Einzelnen darauf ein. Die Kammer verwahrte sich dagegen, dass ich in meinem Schreiben an den Zahnarzt kritische Fragen zu dem Fragebogen gestellt und Zweifel an der Zulässigkeit verschiedener Fragen angemeldet hatte. Eine solche vorläufige Bewertung stehe mir nicht zu. Diese hätte ich dem sachverständigen Vorstand der Kammer überlassen müssen. Die Kammer teilte mir weiter mit, ihr Vorstand sei einhellig der Auffassung, es sei zulässig, diese Fragen zu stellen, da sie der Zweckbestimmung des Behandlungsvertrages dienten. Die Unabhängige Patientenberatung Bremen, die ich um eine Stellungnahme gebeten hatte, legte hingegen konkret dar, dass die einzelnen Fragen sinnvoll seien. Allerdings wurde betont, dass der Fragebogen nicht das Gespräch zwischen Zahnarzt und Patient/-in ersetzen könne.

Der Fragebogen stellt auch die Frage nach dem Arbeitgeber. Dies rechtfertigt die Kammer damit, der Zahnarzt müsse über eventuell bestehende Gefahren am Arbeitsplatz Bescheid wissen. Sie führte den Fall an, dass ein Arzt einen Patienten, der als LKW-Fahrer einer Müllentsorgungsfirma beschäftigt war, nicht gefragt habe, welchen Beruf er bei seinem Arbeitgeber ausübe. Dies aber wäre im Rahmen der Behandlung wegen möglicher Infektionsgefahren von Bedeutung gewesen. Ich entgegnete, dass dieses Beispiel die Frage nach der Berufstätigkeit, nicht jedoch die nach dem Arbeitgeber legitimieren könne. Die Antwort hierauf kann vielfalls die gewünschte Information nach bestimmten Risiken nicht liefern, da es in einem Betrieb eine Vielfalt unterschiedlicher Arbeitsplätze gibt; dafür liefert sie die unerhebliche Informationen über den Namen des Arbeitgebers und eventuell auch die, dass der Patient arbeitslos ist.

Ich machte darauf aufmerksam, dass gemäß des im Datenschutzrecht geltenden Erforderlichkeitsgrundsatzes Daten jeweils nur im erforderlichen Umfang erhoben werden dürfen und stellte anheim, die Frage nach dem Arbeitgeber durch die nach dem Beruf zu ersetzen. Im Übrigen vermag nur diese Information den seitens der Zahnärztekammer vorgetragenen haftungsrechtlichen Risiken wirksam zu begegnen. Gerade auch die vom Zahnarzt abgefragten Informationen über Vorerkrankungen unterliegen häufigen Veränderungen und sollten je nach Behandlungsumfang aktuell vom Zahnarzt erfragt werden und nicht bereits im Vorwege ohne Kenntnis darüber, welches Anliegen der Patient hat. Allerdings kann ich den Zahnarzt nicht daran hindern, die Angaben auf freiwilliger Basis unter den Voraussetzungen des § 4 a Bundesdatenschutzgesetz (BDSG) zu verlangen.

16.7.2 Lebensgeschichte und Biographiefragebögen in Pflegeeinrichtungen

Mehrfach wurde ich durch Angehörige von Bewohnerinnen und Bewohnern von Pflegeeinrichtungen in Bremerhaven bzw. in Bremen eingeschaltet. Sie waren gebeten worden, die Lebensgeschichte der Bewohnerin/des Bewohners aufzu-

schreiben bzw. Antworten auf Fragen zur Biographie zu geben und der Einrichtungsleitung zur Verfügung zu stellen. Die Qualität der Pflege solle dadurch verbessert werden, dass dem Pflegepersonal ein Zugang auch zu Menschen eröffnet werde, die ihre Wünsche und Bedürfnisse nicht mehr äußern könnten. Im einen Fall wurde den Angehörigen ein „Leitfaden für die Erstellung der Lebensgeschichte" an die Hand gegeben, im anderen Fall wurde ihnen ein Fragebogen vorgelegt. Der Leitfaden schlug etwa vor, über Ängste und schöne Erinnerungen, das „schwarze Schaf der Familie", Erziehungsstil, Tischmanieren, Religion, kulturelle, nationale und politische Identität, Beziehungen zu Geschwistern, Abneigungen/Vorlieben und über Gefühle mit Beispielen zu berichten. Vergleichbare Fragen werden im Fragebogen aufgeführt.

Die Leitungen der Einrichtungen konnten mir gegenüber plausibel darlegen, dass es sinnvoll sei, wenn sie Näheres über Persönlichkeit und Lebensgeschichte der pflegebedürftigen Bewohnerinnen und Bewohnern zu erfahren suchten. Grundsätzlich dient dies sicher der Qualität der Pflege, insbesondere in Fällen von Demenz, und ist damit durch § 28 Abs. 1 BDSG legitimiert. Allerdings habe ich vorgeschlagen, in dem an die Befragten gerichteten Begleitschreiben ausdrücklich darauf hinzuweisen, dass sie frei darüber entscheiden können, welche Themen sie behandeln bzw. welche Fragen sie beantworten wollen. Beide Pflegeeinrichtungen sagten zu, hierauf eingehen zu wollen. Zudem wurde mir versichert, dass die Lebensgeschichten/Fragebögen zur jeweiligen Pflegedokumentation genommen und nicht etwa gesondert aufbewahrt und zugänglich gemacht würden.

17. Datenschutz auf internationaler Ebene

17.1 Entscheidung des EuGH zur Weitergabe von Einkommensdaten

Der Europäische Gerichtshof (EuGH) hatte darüber zu befinden, ob die Weitergabe von Einkommensdaten von Arbeitnehmern öffentlicher Einrichtungen zum Zweck der Veröffentlichung in einem Jahresbericht mit dem Gemeinschaftsrecht vereinbar sein kann. In seinem Urteil vom 20. Mai 2003 erklärte der EuGH zunächst die EG-Datenschutzrichtlinie für anwendbar (www.curia.eu.int/de/actu/communiques/cp03/aff/cp0341de.htm). Weiterhin bejahte er die Vereinbarkeit mit dem Gemeinschaftsrecht, wenn die Weitergabe im Hinblick auf das Ziel der ordnungsgemäßen Verwaltung öffentlicher Mittel notwendig und angemessen sei. Es sei Sache der nationalen Gerichte, zu prüfen, ob hierfür die Offenlegung der Namen erforderlich ist oder ob eine anonyme Weitergabe der Daten ausreicht.

Schließlich stellte der EuGH fest, dass die Grundsätze der EG-Datenschutzrichtlinie in Bezug auf die Qualität der Daten und der Zulässigkeit der Verarbeitung von Daten unmittelbar anwendbar sind. Ein Einzelner kann sich vor den nationalen Gerichten auf sie berufen, um die Anwendung entgegenstehender Vorschriften des innerstaatlichen Rechts zu verhindern.

17.2 Veröffentlichung personenbezogener Daten Dritter im Internet

Ich berichte über diese Entscheidung des Europäischen Gerichtshofes (EuGH), die auch für die Bürger Bremens von Relevanz ist, da in dieser Entscheidung allgemeine Grundsätze zur Veröffentlichung personenbezogener Daten Dritter im Internet aufgestellt werden. Aufgrund der allgemeinen Bedeutung des Urteils berichte ich, obwohl dem Urteil die Datenverarbeitung von Kirchen zu Grunde liegt, für welche ich nicht zuständig bin.

Mit Urteil vom 6. November 2003 hat der EuGH (Az.: C-101/01) erstmals den Anwendungsbereich der EG-Datenschutzrichtlinie im Internet bestimmt. Anlass war die Einrichtung einer Internetseite durch eine Kirchenmitarbeiterin in Schweden. Diese Internetseite richtete sich in erster Linie an die Konfirmanden der Gemeinde. Sie enthielt Informationen über die Kirchenmitarbeiterin selbst und achtzehn Mitarbeiter der Gemeinde, die mit ihren Vornamen, manchmal auch mit vollständigen Namen, bezeichnet wurden. Zu einer Kollegin wurde darauf hingewiesen, dass sich diese verletzt habe und krankgeschrieben sei.

Die Kirchenmitarbeiterin wurde mit der Begründung, sie habe personenbezogene Daten in einem automatisierten Verfahren verarbeitet, ohne es der zuständigen Behörde zu melden, zu einer Geldstrafe von 4.000 Kronen (etwa 450 Euro) verurteilt. Über diese Entscheidung hatte der EuGH zu entscheiden.

Der EuGH sah das Veröffentlichen von Daten im Internet durch die Kirchenmitarbeiterin nicht als Datenübermittlung in Drittländer an. Zwar sehe die Richtlinie besondere Bestimmungen für die von den Mitgliedstaaten vorzunehmende Kontrolle der Übermittlung personenbezogener Daten in Drittländer vor. Angesichts des Entwicklungsstands des Internets zur Zeit der Ausarbeitung der Richtlinie und des Fehlens von Kriterien für die Internetbenutzung habe jedoch der Gemeinschaftsgesetzgeber unter den Begriff „Übermittlung von Daten in ein Drittland" nicht auch die Aufnahme von Daten in eine Internetseite fassen wollen, auch wenn diese Daten Personen aus Drittländern zugänglich gemacht würden.

17.3 Übermittlung von Flugpassagierdaten in die USA

Obwohl die Landesbeauftragte für den Datenschutz von Nordrhein-Westfalen für die Lufthansa (Sitz in Köln) zuständig ist, berichte ich an dieser Stelle über die Übermittlung von Flugpassagierdaten in die USA so ausführlich, weil auch Bremer Bürger von dieser Entwicklung betroffen sein können. Ich beobachte mit großer Sorge die überzogenen Forderungen der USA, in großem Umfang Zugriff auf personenbezogene Daten in Reservierungsdatenbanken zu nehmen. Nach den Terroranschlägen vom 11. September 2001 haben die USA im November 2001 eine Vorschrift erlassen, nach welcher Fluggesellschaften, die Flüge nach, von oder durch die USA durchführen, den US-Zoll- und Sicherheitsbehörden elektronischen Zugang zu Fluggastdatensätzen in ihren Buchungs- und Abfertigungssystemen zu gewähren haben. Das momentan bestehende erhöhte Bedürfnis nach Sicherheit im Flugverkehr ist zweifellos anzuerkennen. Die Forderungen der USA gehen aber weit über das hinaus, was erforderlich ist.

Die USA verlangen einen Abruf von 34 Datenfeldern. Hierzu zählen auch Zahlungsart oder die Identität der Mitreisenden. Eine derartig hohe Datenanzahl ist unangemessen. Die derzeitige Situation erlaubt es den US-Behörden zudem, online auf alle im Buchungssystem gespeicherten Datenelemente zuzugreifen. Das liegt daran, dass die jetzigen Buchungssysteme es nicht ermöglichen, die Daten auszusondern und abzuschotten. De facto können die USA auf über 1.000 Datenelemente (z. B. über Behinderungen, Hotelbuchungen, Mietwagen oder vegetarisches Essen) zugreifen. Damit ist auch ein Zugriff auf sensible Daten – wie personenbezogene Daten, aus denen die ethnische Herkunft, die politische Meinung, religiöse Ansichten sowie gesundheitliche Merkmale hervorgehen – möglich, was einen eklatanten Verstoß gegen Art. 8 EG-Datenschutzrichtlinie darstellt. Der momentan unkontrollierte Einblick in die gesamten Buchungsdatenbestände ist nicht hinnehmbar.

Eine datenschutzgerechte Lösung kann nur darin liegen, dass die Zugriffsmöglichkeiten auf die zwingend erforderlichen Daten tatsächlich beschränkt wird. Das kann zum einen dadurch erfolgen, dass die Datenelemente von Fluggesellschaften aktiv übermittelt werden (so genannte Push-Lösung). Wenn hingegen die erforderlichen Daten separiert und in einer eigenen Datei bei den Fluggesellschaften gespeichert würden, kann hierauf ein Onlineabruf zugelassen werden (so genannte Pull-Lösung), weil dann nur die in jedem Einzelfall erforderlichen Daten abgerufen werden könnten. Die Fluggesellschaften sollten daher so schnell wie möglich die technischen Voraussetzungen in ihren Flugbuchungssystemen schaffen, um eine kontrollierte Übermittlung der Daten zu ermöglichen.

Die gesetzlichen Vorgaben des Datenschutzes setzen eine enge Zweckbindung voraus. Im Sinne des Schutzes von Betroffenen ist der Zweck, zu dem die Daten in die USA übermittelt werden dürfen, restriktiv zu fassen. Die Daten dürfen ausschließlich für den Zweck der Terrorismusbekämpfung und -verfolgung weitergegeben werden.

Weiterhin sind die von der Datenübermittlung Betroffenen frühzeitig und umfassend zu informieren. Ihnen müssen zur Wahrnehmung ihrer Rechte Auskunfts- und Berichtigungsansprüche garantiert werden. Erhebliche Bedeutung kommt auch der Löschung der Datenelemente zu. Die US-Behörden wollen alle Reservierungsdaten mindestens 3,5 Jahre speichern, ungeachtet der Tatsache, ob gegen eine Person ein Verdachtsmoment vorliegt oder nicht. Passagierdaten, die im Einzelfall überprüft werden, sollen zudem weitere acht Jahre gespeichert werden. Das kann eine Speicherung von 11,5 Jahren bedeuten. Derartige Fristen sind viel zu ausufernd. Darüber hinaus ist davon auszugehen, dass auch anderen US-Be-

hörden die Daten übermittelt werden. Zur Sicherstellung der Löschung müssten mit den Datensätzen die Löschungsfristdaten untrennbar verbunden sein, damit die Löschung auch in anderen Systemen gewährleistet werden kann.

Schließlich bedarf es einer regelmäßigen Überprüfung der Sicherheitslage. Es sollte daher in regelmäßigen Abständen zwischen den Gremien der EU und den USA geklärt werden, ob die Übermittlung von Flugpassagierdaten sich nach der jeweiligen Sicherheitslage noch als erforderlich darstellt.

Schon auf der Internationalen Konferenz der Datenschutzbeauftragten in Sydney wurde wegen der datenschutzrechtlichen Brisanz der Thematik eine Empfehlung für einen internationalen Transfer von Passagierdaten ausgesprochen (Ziff. 19.1 dieses Berichts).

Diese Empfehlung hat sich das Europäische Parlament in seiner Entschließung am 6. November 2003 zur Weitergabe personenbezogener Daten durch Fluggesellschaften bei Transatlantikflügen zu Eigen gemacht. Leider blieben diese datenschutzrechtlichen Anliegen bisher in den Verhandlungen mit den USA nahezu ungehört.

18. Die Entschließungen der Datenschutzkonferenzen im Jahr 2003

18.1 Forderungen an Bundesgesetzgeber und Bundesregierung

(Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003)

Immer umfassendere Datenverarbeitungsbefugnisse, zunehmender Datenhunger, sowie immer weitergehende technische Möglichkeiten zur Beobachtung und Durchleuchtung der Bürgerinnen und Bürger zeichnen den Weg zu immer mehr Registrierung und Überwachung vor. Das Grundgesetz gebietet dem Staat, dem entgegenzutreten.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, das Recht auf informationelle Selbstbestimmung der Bürger und Bürgerinnen, wie in den Verfassungen zahlreicher deutscher Länder und in den Vorschlägen des Europäischen Verfassungskonvents, als eigenständiges Grundrecht im Grundgesetz zu verankern.

Die Datenschutzbeauftragten werden Bundesgesetzgeber und Bundesregierung bei der Weiterentwicklung des Datenschutzes unterstützen. Sie erwarten, dass die in der Koalitionsvereinbarung enthaltenen Absichtserklärungen zur umfassenden Reform des Datenschutzrechtes in der laufenden Legislaturperiode zügig verwirklicht werden.

Sie sehen dabei folgende essentielle Punkte:

- Schwerpunkte für eine Modernisierung des Bundesdatenschutzgesetzes

  — Im Vordergrund muss die Stärkung der informationellen Selbstbestimmung und des Selbstdatenschutzes stehen: Jeder Mensch muss tatsächlich selbst entscheiden können, welche Datenspuren er hinterlässt und wie diese Datenspuren verwertet werden. Ausnahmen müssen so gering wie möglich gehalten und stets in einer präzise formulierten gesetzlichen Regelung festgeschrieben werden.

  — Es muss im Rahmen der gegebenen Strukturunterschiede ein weitgehend gleichmäßiges Schutzniveau für den öffentlichen und den nicht öffentlichen Bereich gelten. Die Einwilligung in die Datenverarbeitung darf nicht zur Umgehung gesetzlicher Aufgaben- und Befugnisgrenzen missbraucht werden.

  — Die Freiwilligkeit der Einwilligung muss gewährleistet sein.

  — Vor der Nutzung von Daten für Werbezwecke muss die informierte und freie Einwilligung der Betroffenen vorliegen („opt in" statt „opt out").

- Technischer Datenschutz

  Wesentliche Ziele des technischen Datenschutzes müssen darin bestehen, ein hohes Maß an Transparenz bei der Datenverarbeitung zu erreichen und den System- und Selbstdatenschutz zu stärken. Hersteller und Anbieter müssen

verpflichtet werden, den Nutzerinnen und Nutzern die geeigneten Mittel zur Geltendmachung ihrer Rechte auch auf technischem Wege zur Verfügung zu stellen.

- Realisierung von Audit und Gütesiegel als marktwirtschaftliche Elemente im Datenschutz

  Bislang ist das Datenschutzrecht in Deutschland in erster Linie als Ordnungsrecht ausgestaltet. Seine Einhaltung soll durch Kontrolle, Kritik und Beanstandung durchgesetzt werden. Dagegen fehlen Anreize für Firmen und Behörden, vorbildliche Datenschutzkonzepte zu verwirklichen. Mit dem Datenschutzaudit könnte Firmen und Behörden ein gutes Datenschutzkonzept bestätigt werden und es würde ihnen die Möglichkeit eröffnen, damit zu werben. Das Gütesiegel ist ein Anreiz, IT-Produkte von vornherein datenschutzgerecht zu gestalten und damit Marktvorteile zu erringen.

- Eine datenschutzkonforme Technikgestaltung ist eine wichtige Voraussetzung für einen effizienten Datenschutz. Audit und Gütesiegel würden die Aufmerksamkeit auf das Thema Datenschutz lenken und so die stärkere Einbeziehung von Kundinnen und Kunden fördern. Deshalb müssen die noch ausstehenden gesetzlichen Regelungen zur Einführung des im Bundesdatenschutzgesetz vorgesehenen Datenschutzaudits umgehend geschaffen werden.

- Förderung von datenschutzgerechter Technik

  Die Verwirklichung des Grundrechtsschutzes hängt nicht allein von Gesetzen ab. Auch die Gestaltung der Informationstechnik hat großen Einfluss auf die Möglichkeit für alle Menschen, ihr Recht auf informationelle Selbstbestimmung auszuüben. Bislang spielt das Thema Datenschutz bei den öffentlichen IT-Entwicklungsprogrammen allenfalls eine untergeordnete Rolle. Neue IT-Produkte werden nur selten unter dem Blickwinkel entwickelt, ob sie datenschutzgerecht, datenschutzfördernd oder wenigstens nicht datenschutzgefährdend sind.

  Notwendig ist, dass Datenschutz zu einem Kernpunkt im Anforderungsprofil für öffentliche IT-Entwicklungsprogramme wird.

  Datenschutzgerechte Technik stellt sich nicht von alleine ein, sondern bedarf auch der Förderung durch Anreize. Neben der Entwicklung von Schutzprofilen und dem Angebot von Gütesiegeln kommt vor allem die staatliche Forschungs- und Entwicklungsförderung in Betracht. Die Entwicklung datenschutzgerechter Informationstechnik muss zu einem Schwerpunkt staatlicher Forschungsförderung gemacht werden.

- Anonyme Internetnutzung

  Das Surfen im World Wide Web mit seinen immensen Informationsmöglichkeiten und das Versenden von E-Mail sind heute für viele selbstverständlich. Während aber in der realen Welt jeder Mensch zum Beispiel in einem Buchladen stöbern oder ein Einkaufszentrum durchstreifen kann, ohne dass sein Verhalten registriert wird, ist dies im Internet nicht von vornherein gewährleistet. Dort kann jeder Mausklick personenbezogene Datenspuren erzeugen, deren Summe zu einem aussagekräftigen Persönlichkeitsprofil und für vielfältige Zwecke (z. B. Marketing, Auswahl unter Stellenbewerbungen, Observation von Personen) genutzt werden kann. Das Recht auf Anonymität und der Schutz vor zwangsweiser Identifizierung sind in der realen Welt gewährleistet (in keiner Buchhandlung können Kundinnen und Kunden dazu gezwungen werden, einen Ausweis vorzulegen). Sie werden aber im Bereich des Internet durch Pläne für eine umfassende Vorratsspeicherung von Verbindungs- und Nutzungsdaten bedroht.

  Das Recht jedes Menschen, das Internet grundsätzlich unbeobachtet zu nutzen, muss geschützt bleiben. Internet-Provider dürfen nicht dazu verpflichtet werden, auf Vorrat alle Verbindungs- und Nutzungsdaten über den betrieblichen Zweck hinaus für mögliche zukünftige Strafverfahren oder geheimdienstliche Observationen zu speichern.

- Unabhängige Evaluierung der Eingriffsbefugnisse der Sicherheitsbehörden

  Schon vor den Terroranschlägen des 11. September 2001 standen den deutschen Sicherheitsbehörden nach einer Reihe von Antiterrorgesetzen und Gesetzen gegen die Organisierte Kriminalität weitreichende Eingriffsbefugnisse zur Verfügung, die Datenschutzbeauftragten und Bürgerrechtsorganisationen Sorgen bereiteten:

  Dies zeigen Videoüberwachung, Lauschangriff, Rasterfahndung, langfristige Aufbewahrung der Daten bei der Nutzung des Internet und der Telekommunikation, Zugriff auf Kundendaten und Geldbewegungen bei den Banken.

  Durch die jüngsten Gesetzesverschärfungen nach den Terroranschlägen des 11. September 2001 sind die Freiräume für unbeobachtete individuelle oder gesellschaftliche Aktivitäten und Kommunikation weiter eingeschränkt worden. Bürgerliche Freiheitsrechte und Datenschutz dürfen nicht immer weiter gefährdet werden.

  Nach der Konkretisierung der Befugnisse der Sicherheitsbehörden und der Schaffung neuer Befugnisse im Terrorismusbekämpfungsgesetz sowie in anderen gegen Ende der 14. Legislaturperiode verabschiedeten Bundesgesetzen ist vermehrt eine offene Diskussion darüber notwendig, wie der gebotene Ausgleich zwischen kollektiver Sicherheit und individuellen Freiheitsrechten so gewährleistet werden kann, dass unser Rechtsstaat nicht zum Überwachungsstaat wird. Dazu ist eine umfassende und systematische Evaluierung der im Zusammenhang mit der Terrorismusbekämpfung eingefügten Eingriffsbefugnisse der Sicherheitsbehörden notwendig.

  Die Datenschutzbeauftragten halten darüber hinaus eine Erweiterung der im Terrorismusbekämpfungsgesetz vorgesehenen Pflicht zur Evaluierung der neuen Befugnisse der Sicherheitsbehörden auf andere vergleichbar intensive Eingriffsmaßnahmen – wie Telefonüberwachung, großer Lauschangriff und Rasterfahndung – für geboten.

  Die Evaluierung muss durch unabhängige Stellen und an Hand objektiver Kriterien erfolgen und aufzeigen, wo zurückgeschnitten werden muss, wo Instrumente untauglich sind oder wo die negativen Folgewirkungen überwiegen. Wissenschaftliche Untersuchungsergebnisse zur Evaluation des Richtervorbehalts z. B. bei Telefonüberwachungen machen deutlich, dass der Bundesgesetzgeber Maßnahmen zur Stärkung des Richtervorbehalts – und zwar nicht nur im Bereich der Telefonüberwachung – als grundrechtssicherndes Verfahrenselement ergreifen muss.

- Stärkung des Schutzes von Gesundheitsdaten

  Zwar schützt die Jahrtausende alte ärztliche Schweigepflicht Kranke davor, dass Informationen über ihren Gesundheitszustand von denjenigen unbefugt weitergegeben werden, die sie medizinisch betreuen. Medizinische Daten werden aber zunehmend außerhalb des besonderen ärztlichen Vertrauensverhältnisses zu Patienten und Patientinnen verarbeitet. Telemedizin und High-Tech-Medizin führen zu umfangreichen automatischen Datenspeicherungen. Hinzu kommt ein zunehmender Druck, Gesundheitsdaten z. B. zur Einsparung von Kosten, zur Verhinderung von Arzneimittelnebenfolgen oder „zur Qualitätssicherung" einzusetzen. Die Informatisierung der Medizin durch elektronische Aktenführung, Einsatz von Chipkarten, Nutzung des Internets zur Konsultation bis hin zur ferngesteuerten Behandlung mit Robotern erfordern es deshalb, dass auch die Instrumente zum Schutz von Gesundheitsdaten weiterentwickelt werden.

  Der Schutz des Patientengeheimnisses muss auch in einer computerisierten Medizin wirksam gewährleistet sein. Die Datenschutzbeauftragten begrüßen deshalb die Absichtserklärung in der Koalitionsvereinbarung, Patientenschutz und Patientenrechte auszubauen. Dabei ist insbesondere sicherzustellen, dass Gesundheitsdaten außerhalb der eigentlichen Behandlung soweit wie möglich und grundsätzlich nur anonymisiert oder pseudonymisiert verarbeitet werden dürfen, soweit die Verarbeitung im Einzelfall nicht durch ein

informiertes Einverständnis gerechtfertigt ist. Das Prinzip des informierten und freiwilligen Einverständnisses ist insbesondere auch für eine Gesundheitskarte zu beachten und zwar auch für deren Verwendung im Einzelfall.

Der Bundesgesetzgeber wird auch aufgefordert gesetzlich zu regeln, dass Patientendaten, die in Datenverarbeitungsanlagen außerhalb von Arztpraxen und Krankenhäusern verarbeitet werden, genauso geschützt sind wie die Daten in der ärztlichen Praxis.

Geprüft werden sollte schließlich, ob und gegebenenfalls wie der Schutz von Gesundheitsdaten durch Geheimhaltungspflicht, Zeugnisverweigerungsrecht und Beschlagnahmeverbot auch dann gewährleistet werden kann, wenn diese, z. B. in der wissenschaftlichen Forschung, mit Einwilligung oder auf gesetzlicher Grundlage von anderen Einrichtungen außerhalb des Bereichs der behandelnden Ärztinnen und Ärzte verarbeitet werden.

- Datenschutz und Gentechnik

  Die Entwicklung der Gentechnik ist atemberaubend. Schon ein ausgefallenes Haar, ein Speichelrest an Besteck oder Gläsern, abgeschürfte Hautpartikel oder ein Blutstropfen – dies alles eignet sich als Untersuchungsmaterial, um den genetischen Bauplan eines Menschen entschlüsseln zu können. Inzwischen werden Gentests frei verkäuflich angeboten. Je mehr Tests gemacht werden, desto größer wird das Risiko für jeden Menschen, dass seine genetischen Anlagen von anderen auch gegen seinen Willen analysiert werden. Versicherungen oder Arbeitgeber und Arbeitgeberinnen werden ebenfalls Testergebnisse erfahren wollen.

  Niemand darf zur Untersuchung genetischer Anlagen gezwungen werden; die Durchführung eines gesetzlich nicht zugelassenen Tests ohne Wissen und Wollen der betroffenen Person und die Nutzung daraus gewonnener Ergebnisse muss unter Strafe gestellt werden.

  In der Koalitionsvereinbarung ist der Erlass eines „Gen-Test-Gesetzes" vorgesehen. Ein solches Gesetz ist dringend erforderlich, damit der datenschutzgerechte Umgang mit genetischen Daten gewährleistet wird. Die Datenschutzbeauftragten haben dazu auf ihrer 62. Konferenz in Münster vom 24. bis 26. Oktober 2001 Vorschläge vorgelegt.

- Datenschutz im Steuerrecht

  Im bisherigen Steuer- und Abgabenrecht finden sich äußerst lückenhafte datenschutzrechtliche Regelungen. Insbesondere fehlen grundlegende Rechte, wie ein Akteneinsichts- und Auskunftsrecht. Eine Pflicht zur Information der Steuerpflichtigen über Datenerhebungen bei Dritten fehlt ganz.

  Die jüngsten Gesetzesnovellen und Gesetzesentwürfe, die fortschreitende Vernetzung und multinationale Vereinbarungen verschärfen den Mangel: Immer mehr Steuerdaten sollen zentral durch das Bundesamt für Finanzen erfasst werden. Mit einheitlichen Personenidentifikationsnummern sollen Zusammenführungen und umfassende Auswertungen der Verbunddaten möglich werden. Eine erhebliche Ausweitung der Kontrollmitteilungen von Finanzbehörden und Kreditinstituten, die ungeachtet der Einführung einer pauschalen Abgeltungssteuer geplant ist, würde zweckungebundene und unverhältnismäßige Datenübermittlungen gestatten. Die zunehmende Vorratserhebung und -speicherung von Steuerdaten entspricht nicht dem datenschutzrechtlichen Grundsatz der Erforderlichkeit.

  Die Datenschutzbeauftragten fordern deshalb, die Aufnahme datenschutzrechtlicher Grundsätze in das Steuerrecht jetzt anzugehen und den Betroffenen die datenschutzrechtlichen Informations- und Auskunftsrechte zuzuerkennen.

- Arbeitnehmerdatenschutz

  Persönlichkeitsrechte und Datenschutz sind im Arbeitsverhältnis vielfältig bedroht, zum Beispiel durch

— die Sammlung von Beschäftigtendaten in leistungsfähigen Personalinformationssystemen, die zur Erstellung von Persönlichkeitsprofilen genutzt werden,

— die Übermittlung von Beschäftigtendaten zwischen konzernangehörigen Unternehmen, für die nicht der Datenschutzstandard der EG-Datenschutzrichtlinie gilt,

— die Überwachung des Arbeitsverhaltens durch Videokameras, die Protokollierung der Nutzung von Internetdiensten am Arbeitsplatz,

— die Erhebung des Gesundheitszustands, Drogen-Screenings und psychologische Testverfahren bei der Einstellung.

Die hierzu von den Arbeitsgerichten entwickelten Schranken wirken unmittelbar nur im jeweils entschiedenen Einzelfall und sind auch nicht allen Betroffenen hinreichend bekannt. Das seit vielen Jahren angekündigte Arbeitnehmerdatenschutzgesetz muss hier endlich klare gesetzliche Vorgaben schaffen.

Die Datenschutzbeauftragten fordern deshalb, dass für die in der Koalitionsvereinbarung enthaltene Festlegung zur Schaffung von gesetzlichen Regelungen zum Arbeitnehmerdatenschutz nunmehr rasch ein ausformulierter Gesetzentwurf vorgelegt und anschließend zügig das Gesetzgebungsverfahren eingeleitet wird.

- Stärkung einer unabhängigen, effizienten Datenschutzkontrolle

  Die Datenschutzbeauftragten fordern gesetzliche Vorgaben, die die völlige Unabhängigkeit der Datenschutzkontrolle sichern und effektive Einwirkungsbefugnisse gewährleisten, wie dies der Art. 28 der EG-Datenschutzrichtlinie gebietet.

  Die Datenschutzkontrollstellen im privaten Bereich haben bis heute nicht die völlige Unabhängigkeit, die die Europäische Datenschutzrichtlinie vorsieht. So ist in der Mehrzahl der deutschen Länder die Kontrolle über den Datenschutz im privaten Bereich nach wie vor bei den Innenministerien und nachgeordneten Stellen angesiedelt und unterliegt damit einer Fachaufsicht. Selbst in den Ländern, in denen die Landesbeauftragten diese Aufgabe wahrnehmen, ist ihre Unabhängigkeit nicht überall richtlinienkonform ausgestaltet.

- Stellung des Bundesdatenschutzbeauftragten

  Die rechtliche Stellung des Bundesdatenschutzbeauftragten als unabhängiges Kontrollorgan muss im Grundgesetz abgesichert werden.

- Verbesserung der Informationsrechte

  Die im Bereich der Informationsfreiheit tätigen Datenschutzbeauftragten unterstützen die Absicht in der Koalitionsvereinbarung, auf Bundesebene ein Informationsfreiheitsgesetz zu schaffen. Nach ihren Erfahrungen hat sich die gemeinsame Wahrnehmung der Aufgaben zum Datenschutz und zur Informationsfreiheit bewährt, weshalb sie auch auf Bundesebene realisiert werden sollte. Zusätzlich muss ein Verbraucherinformationsgesetz alle Produkte und Dienstleistungen erfassen und einen Informationsanspruch auch gegenüber Unternehmen einführen.

18.2 TCPA darf nicht zur Aushebelung des Datenschutzes missbraucht werden

(Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003)

Mit großer Skepsis sehen die Datenschutzbeauftragten des Bundes und der Länder die Pläne zur Entwicklung zentraler Kontrollmechanismen und -infrastrukturen auf der Basis der Spezifikationen der Industrie-Allianz „Trusted Computing Platform Alliance“ (TCPA).

Die TCPA hat sich zum Ziel gesetzt, vertrauenswürdige Personalcomputer zu entwickeln. Dazu bedarf es spezieller Hard- und Software. In den bisher bekannt ge-

wordenen Szenarien soll die Vertrauenswürdigkeit dadurch gewährleistet werden, dass zunächst ein spezieller Kryptoprozessor nach dem Einschalten des PC überprüft, ob die installierte Hardware und das Betriebssystem mit den von der TCPA zertifizierten und auf zentralen Servern hinterlegten Konfigurationsangaben übereinstimmen. Danach übergibt der Prozessor die Steuerung an ein TCPA-konformes Betriebssystem. Beim Start einer beliebigen Anwendersoftware prüft das Betriebssystem dann deren TCPA-Konformität, beispielsweise durch Kontrolle der Lizenz oder der Seriennummer, und kontrolliert weiterhin, ob Dokumente in zulässiger Form genutzt werden. Sollte eine der Prüfungen Abweichungen zur hinterlegten, zertifizierten Konfiguration ergeben, lässt sich der PC nicht booten bzw. das entsprechende Programm wird gelöscht oder lässt sich nicht starten.

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen alle Aktivitäten, die der Verbesserung des Datenschutzes dienen und insbesondere zu einer manipulations- und missbrauchssicheren sowie transparenten IT-Infrastruktur führen. Sie erkennen auch die berechtigten Forderungen der Softwarehersteller an, dass kostenpflichtige Software nur nach Bezahlung genutzt werden darf.

Wenn aber zentrale Server einer externen Kontrollinstanz genutzt werden, um mit entsprechend modifizierten Client-Betriebssystemen Prüf- und Kontrollfunktionen zu steuern, müssten sich Anwenderinnen und Anwender beim Schutz sensibler Daten uneingeschränkt auf die Vertrauenswürdigkeit der externen Instanz verlassen können. Die Datenschutzbeauftragten erachten es für unzumutbar, wenn

- Anwenderinnen und Anwender die alleinige Kontrolle über die Funktionen des eigenen Computers verlieren, falls eine externe Kontrollinstanz Hardware, Software und Daten kontrollieren und manipulieren kann,

- die Verfügbarkeit aller TCPA-konformen Personalcomputer und der darauf verarbeiteten Daten gefährdet wäre, da sowohl Fehler in der Kontrollinfrastruktur als auch Angriffe auf die zentralen TCPA-Server die Funktionsfähigkeit einzelner Rechner sofort massiv einschränken würden,

- andere Institutionen oder Personen sich vertrauliche Informationen von zentralen Servern beschaffen würden, ohne dass der Anwender dies bemerkt,

- die Nutzung von Servern oder PC davon abhängig gemacht würde, dass ein Zugang zum Internet geöffnet wird,

- der Zugang zum Internet und E-Mail-Verkehr durch Softwarerestriktionen behindert würde,

- der Umgang mit Dokumenten ausschließlich gemäß den Vorgaben der externen Kontrollinstanz zulässig sein würde und somit eine sehr weitgehende Zensur ermöglicht wird,

- auf diese Weise der Zugriff auf Dokumente von Konkurrenzprodukten verhindert und somit auch die Verbreitung datenschutzfreundlicher Open-Source-Software eingeschränkt werden kann und

- Programmergänzungen (Updates) ohne vorherige Einwilligung im Einzelfall aufgespielt werden könnten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern deshalb Hersteller von Informations- und Kommunikationstechnik auf, Hard- und Software so zu entwickeln und herzustellen, dass

- Anwenderinnen und Anwender die ausschließliche und vollständige Kontrolle über die von ihnen genutzte Informationstechnik haben, insbesondere dadurch, dass Zugriffe und Änderungen nur nach vorheriger Information und Einwilligung im Einzelfall erfolgen,

- alle zur Verfügung stehenden Sicherheitsfunktionen für Anwenderinnen und Anwender transparent sind und

- die Nutzung von Hard- und Software und der Zugriff auf Dokumente auch weiterhin möglich ist, ohne dass Dritte davon Kenntnis erhalten und Nutzungsprofile angelegt werden können.

Auf diese Weise können auch künftig die in den Datenschutzgesetzen des Bundes und der Länder geforderte Vertraulichkeit und Verfügbarkeit der zu verarbeitenden personenbezogenen Daten sichergestellt und die Transparenz bei der Verarbeitung dieser Daten gewährleistet werden.

18.3 Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik

(Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003)

Anwenderinnen und Anwender von komplexen IT-Produkten müssen unbedingt darauf vertrauen können, dass Sicherheitsfunktionen von Hard- und Software korrekt ausgeführt werden, damit die Vertraulichkeit, die Integrität und die Zurechenbarkeit der Daten gewährleistet sind. Dieses Vertrauen kann insbesondere durch eine datenschutzgerechte Gestaltung der Informationstechnik geschaffen werden. Ausbleibende Erfolge bei eCommerce und eGovernment werden mit fehlendem Vertrauen in einen angemessenen Schutz der personenbezogenen Daten und mangelnder Akzeptanz der Nutzerinnen und Nutzer erklärt. Anwenderinnen und Anwender sollten ihre Sicherheitsanforderungen präzise definieren und Anbieter ihre Sicherheitsleistungen schon vor der Produktentwicklung festlegen und für alle nachprüfbar dokumentieren. Die Datenschutzbeauftragten des Bundes und der Länder wollen Herstellerinnen und Hersteller und Anwenderinnen und Anwender von Informationstechnik unterstützen, indem sie entsprechende Werkzeuge und Hilfsmittel zur Verfügung stellen.

So bietet der Bundesbeauftragte für den Datenschutz seit dem 11. November 2002 mit zwei so genannten Schutzprofilen (Protection Profiles) Werkzeuge an, mit deren Hilfe Anwenderinnen und Anwender bereits vor der Produktentwicklung ihre datenschutzspezifischen Anforderungen für bestimmte Produkttypen beispielsweise im Gesundheitswesen oder im eGovernment detailliert beschreiben können. Kerngedanke der in diesen Schutzprofilen definierten Sicherheitsanforderungen ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Die Schutzprofile sind international anerkannt, da sie auf der Basis der „Gemeinsamen Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik (Common Criteria)“ entwickelt wurden. Herstellerinnen und Hersteller können datenschutzfreundliche Produkte somit nach international prüffähigen Vorgaben der Anwenderinnen und Anwender entwickeln. Unabhängige Prüfinstitutionen können diese Produkte dann nach Abschluss der Entwicklung nach international gültigen Kriterien prüfen.[1])

In Schleswig-Holstein bietet das Unabhängige Landeszentrum für Datenschutz ein Verfahren mit vergleichbarer Zielsetzung an, das ebenfalls zu überprüfbarer Sicherheit von IT-Produkten führt. Für nachweislich datenschutzgerechte IT-Produkte können Hersteller ein so genanntes Datenschutz-Gütesiegel erhalten. Das Landeszentrum hat auf der Grundlage landesspezifischer Rechtsvorschriften bereits im Jahr 2002 einen entsprechenden Anforderungskatalog veröffentlicht und zur CeBIT 2003 eine an die Common Criteria angepasste Version vorgestellt.[2])

Die Datenschutzbeauftragten des Bundes und der Länder empfehlen die Anwendung von Schutzprofilen und Auditierungsprozeduren, damit auch der Nutzer oder die Nutzerin beurteilen kann, ob IT-Systeme und -Produkte vertrauenswürdig und datenschutzfreundlich sind. Sie appellieren an die Hersteller, entsprechende Produkte zu entwickeln bzw. vorhandene Produkte anhand bereits bestehender oder gleichwertiger Schutzprofile und Anforderungskataloge zu modifizieren. Sie treten dafür ein, dass die öffentliche Verwaltung vorrangig solche Produkte einsetzt.

---

1) Die Schutzprofile mit dem Titel „BISS – Benutzerbestimmbare Informationsflusskontrolle“ haben die Registrierungskennzeichen BSI-PP-0007-2002 und BSI-PTT-008-2002 und sind beim Bundesbeauftragten für den Datenschutz unter http://www.bfd.bund.de/technik/protection_profile.html abrufbar.

2) Die Ergebnisse der bisherigen Auditierungen durch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein sind unter http://www.datenschutzzentrum.de/guetesiegel veröffentlicht.

18.4 Datenschutzrechtliche Rahmenbedingungen zur Modernierung des Systems der gesetzlichen Krankenversicherung

(Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003)

In der Diskussion über eine grundlegende Reform des Rechts der gesetzlichen Krankenversicherung (GKV) werden in großem Maße datenschutzrechtliche Belange berührt. Erweiterte Befugnisse zur Verarbeitung von medizinischen Leistungs- und Abrechnungsdaten sollen eine stärkere Kontrolle der Patientinnen und Patienten sowie der sonstigen beteiligten Parteien ermöglichen. Verbesserte individuelle und statistische Informationen sollen zudem die medizinische und informationelle Selbstbestimmung der Patientinnen und Patienten verbessern sowie die Transparenz für die Beteiligten und für die Öffentlichkeit erhöhen.

So sehen Vorschläge des Bundesministeriums für Gesundheit und Soziale Sicherung zur Modernisierung des Gesundheitswesens u. a. vor, dass bis zum Jahr 2006 schrittweise eine elektronische Gesundheitskarte eingeführt wird und Leistungs- und Abrechnungsdaten zusammengeführt werden sollen. Boni für gesundheitsbewusstes Verhalten und Ausnahmen oder Mali für gesundheitsgefährdendes Verhalten sollen medizinisch rationales Verhalten der Versicherten fördern, was eine Überprüfung dieses Verhaltens voraussetzt. Derzeit werden gesetzliche Regelungen ausgearbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder weisen erneut auf die datenschutzrechtlichen Chancen und Risiken einer Modernisierung des Systems der GKV hin.

Viele Vorschläge zielen darauf ab, Gesundheitskosten dadurch zu reduzieren, dass den Krankenkassen mehr Kontrollmöglichkeiten eingeräumt werden. Solche individuellen Kontrollen können indes nur ein Hilfsmittel zu angestrebten Problemlösungen, nicht aber die Problemlösung selbst sein. Sie sind auch mit dem Recht der Patientinnen und Patienten auf Selbstbestimmung und dem Schutz der Vertrauensbeziehung zwischen ärztlichem Personal und behandelten Personen nicht problemlos in Einklang zu bringen. Eingriffe müssen nach den Grundsätzen der Datenvermeidung und der Erforderlichkeit und Verhältnismäßigkeit auf ein Minimum beschränkt bleiben. Möglichkeiten der anonymisierten oder pseudonymisierten Verarbeitung von Patientendaten müssen ausgeschöpft werden. Eine umfassendere Information der Patientinnen und Patienten, die zu mehr Transparenz führt und die Verantwortlichkeiten verdeutlicht, ist ebenfalls ein geeignetes Hilfsmittel.

Sollte im Rahmen gesetzlicher Regelungen zur Qualitätssicherung und Abrechnungskontrolle für einzelne Bereiche der Zugriff auf personenbezogene Behandlungsdaten unerlässlich sein, müssen Vorgaben entwickelt werden, die

— den Zugriff auf genau festgelegte Anwendungsfälle begrenzen,

— das Prinzip der Stichprobe zugrunde legen,

— eine strikte Einhaltung der Zweckbindung gewährleisten und

— die Auswertung der Daten einer unabhängigen Stelle übertragen.

1. Die Datenschutzbeauftragten erkennen die Notwendigkeit einer verbesserten Datenbasis zur Weiterentwicklung der gesetzlichen Krankenversicherung an. Hierzu reichen wirksam pseudonymisierte Daten grundsätzlich aus. Eine Zusammenführung von Leistungs- und Versichertendaten darf nicht dazu führen, dass über eine lückenlose zentrale Sammlung personenbeziehbarer Patientendaten mit sensiblen Diagnose- und Behandlungsangaben z. B. zur Risikoselektion geeignete medizinische Profile entstehen. Dies könnte nicht nur zur Diskriminierung einzelner Versicherter führen, sondern es würde auch die sozialstaatliche Errungenschaft des solidarischen Tragens von Krankheitsrisiken aufgegeben. Zudem wären zweckwidrige Auswertungen möglich, für die es viele Interessierte gäbe, von Privatversicherungen bis hin zu Arbeitgebern. Durch sichere technische und organisatorische Verfahren, die Pseudonymisierung der Daten und ein grundsätzliches sanktionsbewehrtes Verbot der Reidentifizierung pseudonymisierter Datenbestände kann solchen Gefahren entgegengewirkt werden.

2. Die Einführung einer Gesundheitschipkarte kann die Transparenz des Behandlungsgeschehens für die Patientinnen und Patienten erhöhen, deren schonende und erfolgreiche medizinische Behandlung effektivieren und durch Vermeidung von Medienbrüchen und Mehrfachbehandlungen Kosten senken. Eine solche Karte kann aber auch dazu genutzt werden, die Selbstbestimmungsrechte der Patientinnen und Patienten zu verschlechtern. Dieser Effekt würde durch eine Pflichtkarte eintreten, auf der – von den Betroffenen nicht beeinflussbar – Diagnosen und Medikationen zur freien Einsicht durch Ärztinnen und Ärzte sowie sonstige Leistungserbringende gespeichert wären. Zentrales Patientenrecht ist es, selbst zu entscheiden, welchem Arzt oder welcher Ärztin welche Informationen anvertraut werden.

   Die Datenschutzkonferenz fordert im Fall der Einführung einer Gesundheitschipkarte die Gewährleistung des Rechts der Patientinnen und Patienten, grundsätzlich selbst zu entscheiden,

   — ob sie überhaupt verwendet wird,

   — welche Daten darauf gespeichert werden oder über sie abgerufen werden können,

   — welche Daten zu löschen sind und wann das zu geschehen hat,

   — ob sie im Einzelfall vorgelegt wird und

   — welche Daten im Einzelfall ausgelesen werden sollen.

   Sicherzustellen ist weiterhin

   — ein Beschlagnahmeverbot und Zeugnisverweigerungsrecht, in Bezug auf die Daten, die auf der Karte gespeichert sind,

   — die Beschränkung der Nutzung auf das Patienten-Arzt/Apotheken-Verhältnis und

   — die Strafbarkeit des Datenmissbrauchs.

   Die Datenschutzkonferenz hat bereits zu den datenschutzrechtlichen Anforderungen an den „Arzneimittelpass" (Medikamentenchipkarte) ausführlich Stellung genommen (Entschließung vom 26.10.2001). Die dort formulierten Anforderungen an eine elektronische Gesundheitskarte sind weiterhin gültig. Die „Gemeinsame Erklärung des Bundesministeriums für Gesundheit und der Spitzenorganisationen zum Einsatz von Telematik im Gesundheitswesen" vom 3. Mai 2002, wonach „der Patient Herr seiner Daten" sein soll, enthält gute Ansatzpunkte, auf deren Basis die Einführung einer Gesundheitskarte betrieben werden kann.

3. Die Datenschutzbeauftragten anerkennen die Förderung wirtschaftlichen und gesundheitsbewussten Verhaltens als ein wichtiges Anliegen. Dies darf aber nicht dazu führen, dass die Krankenkassen detaillierte Daten über die private Lebensführung erhalten („fährt Ski", „raucht", „trinkt zwei Biere pro Tag"), diese überwachen und so zur „Gesundheitspolizei" werden. Notwendig ist deshalb die Entwicklung von Konzepten, die ohne derartige mitgliederbezogene Datensätze bei den Krankenkassen und ihre Überwachung auskommen.

4. Die Datenschutzbeauftragten begrüßen alle Pläne, die darauf hinauslaufen, das Verfahren der GKV allgemein sowie die individuelle Behandlung und Datenverarbeitung für die Betroffenen transparenter zu machen. Maßnahmen wie die Einführung der Patientenquittung, die Information über das Leistungsverfahren und über Umfang und Qualität des Leistungsangebotes sowie eine verstärkte Einbindung der Patientinnen und Patienten durch Unterrichtungen und Einwilligungserfordernisse stärken die Patientensouveränität und die Selbstbestimmung.

18.5 Kennzeichnung von Daten aus besonders eingriffsintensiven Erhebungen

(Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003)

Das Bundesverfassungsgericht hat in seinem Urteil zur strategischen Fernmeldeüberwachung des Bundesnachrichtendienstes festgestellt, dass sich die Zweckbindung der bei dieser Maßnahme erlangten personenbezogenen Daten nur gewährleisten lässt, wenn auch nach ihrer Erfassung erkennbar bleibt, dass es sich um Daten handelt, die aus Eingriffen in das Fernmeldegeheimnis stammen. Eine entsprechende Kennzeichnung ist daher von Verfassungs wegen geboten. Dementsprechend wurde die Kennzeichnungspflicht in der Novellierung des G-10-Gesetzes auch allgemein für jede Datenerhebung des Bundesnachrichtendienstes und des Verfassungsschutzes im Schutzbereich des Art. 10 GG angeordnet.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist darauf hin, dass die Pflicht zur Kennzeichnung aufgrund der Ausführungen des Bundesverfassungsgerichts nicht auf den Bereich der Fernmeldeüberwachung beschränkt ist. Sie gilt auch für vergleichbare Methoden der Datenerhebung, bei denen die Daten durch besonders eingriffsintensive Maßnahmen gewonnen werden und deswegen einer strikten Zweckbindung unterliegen müssen.

Deshalb müssen zumindest solche personenbezogenen Daten, die aus einer Telefon-, Wohnraum- oder Postüberwachung erlangt wurden, besonders gekennzeichnet werden.

18.6 Transparenz in der Telefonüberwachung

(Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003)

Nach derzeitigem Recht haben die Betreiber von Telekommunikationsanlagen eine Jahresstatistik über die von ihnen zu Strafverfolgungszwecken durchgeführten Überwachungsmaßnahmen zu erstellen. Diese Zahlen werden von der Regulierungsbehörde für Telekommunikation und Post veröffentlicht. Auf diese Weise wird die Allgemeinheit über Ausmaß und Entwicklung der Telekommunikationsüberwachung in Deutschland informiert.

Nach aktuellen Plänen der Bundesregierung soll diese Statistik abgeschafft werden. Begründet wird dies mit einer Entlastung der Telekommunikationsunternehmen von überflüssigen Arbeiten. Zudem wird darauf verwiesen, dass das Bundesjustizministerium eine ähnliche Statistik führt, die sich auf Zahlen der Landesjustizbehörden stützt. Dabei wird verkannt, das die beiden Statistiken unterschiedliches Zahlenmaterial berücksichtigen. So zählen die Telekommunikationsunternehmen jede Überwachungsmaßnahme getrennt nach den einzelnen Anschlüssen, während von den Landesjustizverwaltungen nur die Anzahl der Strafverfahren erfasst wird.

In den vergangenen Jahren ist die Zahl der überwachten Anschlüsse um jährlich etwa 25 Prozent gestiegen. Gab es im Jahr 1998 noch 9.802 Anordnungen, waren es im Jahr 2001 bereits 19.896. Diese stetige Zunahme von Eingriffen in das Fernmeldegeheimnis sehen die Datenschutzbeauftragten des Bundes und der Länder mit großer Sorge. Eine fundierte und objektive Diskussion in Politik und Öffentlichkeit ist nur möglich, wenn die tatsächliche Anzahl von Telefonüberwachungsmaßnahmen bekannt ist. Allein eine Aussage über die Anzahl der Strafverfahren, in denen eine Überwachungsmaßnahme stattgefunden hat, reicht nicht aus. Nur die detaillierten Zahlen, die derzeit von den Telekommunikationsunternehmen erhoben werden, sind aussagekräftig genug.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert daher eine Beibehaltung der Unternehmensstatistik nach § 88 Abs. 5 Telekommunikationsgesetz sowie ihre Erstreckung auf die Zahl der Auskünfte über Telekommunikationsverbindungen, um auf diesem Wege bessere Transparenz bei der Telefonüberwachung zu schaffen.

18.7 Elektronische Signatur im Finanzbereich

(Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27./28. März 2003)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt, dass mit dem Signaturgesetz und der Anpassung von mehr als 3.000 Rechtsvorschriften in Deutschland die rechtlichen Voraussetzungen geschaffen wurden, um die „qualifizierte elektronische Signatur" der eigenhändigen Unterschrift gleichzustellen. Die administrativen und technischen Voraussetzungen sind inzwischen weitgehend vorhanden. Mehr als zwanzig freiwillig akkreditierte Zertifizierungsdiensteanbieter nach dem Signaturgesetz sind von der Regulierungsbehörde für Telekommunikation und Post (RegTP) zugelassen. Sowohl Chipkarten, die für die qualifizierte elektronische Signatur zugelassen sind, als auch die dafür erforderlichen Lesegeräte sind verfügbar.

Für die elektronische Kommunikation zwischen der Finanzverwaltung und den Bürgerinnen und Bürgern ist die „qualifizierte elektronische Signatur" gesetzlich vorgeschrieben. Die Finanzverwaltung will eine Übergangsbestimmung in der Steuerdatenübermittlungsverordnung vom 28. Januar 2003 nutzen, nach der bis Ende 2005 eine lediglich fortgeschrittene, die so genannte qualifizierte elektronische Signatur mit Einschränkungen eingesetzt werden kann. Aus folgenden Gründen lehnen die Datenschutzbeauftragten dieses Vorgehen ab:

— Die „qualifizierte elektronische Signatur mit Einschränkungen" bietet im Gegensatz zur „qualifizierten elektronischen Signatur" und der „qualifizierten elektronischen Signatur mit Anbieterakkreditierung" keine umfassend nachgewiesene Sicherheit, vor allem aber keine langfristige Überprüfbarkeit. Die mit ihr unterzeichneten elektronischen Dokumente sind unerkannt manipulierbar. Die „qualifizierte elektronische Signatur mit Einschränkungen" hat geringeren Beweiswert als die eigenhändige Unterschrift.

— Die technische Infrastruktur, die die Finanzverwaltung für die „qualifizierte elektronische Signatur mit Einschränkungen" vorgesehen hat, kann sie verwenden, um elektronische, fortgeschritten oder qualifiziert signierte Dokumente von Bürgerinnen und Bürgern und Steuerberaterinnen und Steuerberatern zu prüfen und selbst fortgeschrittene Signaturen zu erzeugen.

— Damit die Finanzverwaltung selbst qualifiziert signieren kann, reicht eine Ergänzung mit einem qualifizierten Zertifikat aus.

— Für die elektronische Steuererklärung ELSTER sollen Zertifizierungsdienste im außereuropäischen Ausland zugelassen werden, für die weder eine freiwillige Akkreditierung noch eine Kontrolle durch deutsche Datenschutzbehörden möglich ist, anstatt Zertifizierungsdienste einzuschalten, die der Europäischen Datenschutzrichtlinie entsprechen. Damit sind erhebliche Gefahren verbunden, die vermeidbar sind.

— Die elektronische Signatur soll auch zur Authentisierung der Steuerpflichtigen und Steuerberater gegenüber ELSTER genutzt werden, obwohl die Trennung der Schlüsselpaare für Signatur und Authentisierung unerlässlich und bereits Stand der Technik ist.

Die Datenschutzbeauftragten des Bundes und der Länder befürchten, dass bei Schaffung weiterer Signaturverfahren mit geringerer Sicherheit die Transparenz für die Anwenderinnen und Anwender verloren geht und der sichere und verlässliche elektronische Rechts- und Geschäftsverkehr in Frage gestellt werden könnte.

Abweichend vom Vorgehen der Finanzverwaltung hat sich die Bundesregierung sowohl im Rahmen der Initiative „Bund Online 2005" als auch im so genannten Signaturbündnis für sichere Signaturverfahren eingesetzt. Das Verfahren ELSTER sollte genutzt werden, um sogleich qualifizierten und damit sicheren Signaturen zum Durchbruch zu verhelfen.

Vor diesem Hintergrund empfiehlt die Konferenz der Datenschutzbeauftragten des Bundes und der Länder der Bundesregierung,

- dass die Finanzbehörden Steuerbescheide und sonstige Dokumente ausschließlich qualifiziert signiert versenden,

- den Bürgerinnen und Bürgern eine sichere, zuverlässige, leicht einsetzbare und transparente Technologie zur Verfügung zu stellen,

- unterschiedliche Ausstattungen für abgestufte Qualitäten und Anwendungsverfahren zu vermeiden,

- die Anschaffung von Signaturerstellungseinheiten mit zugehörigen Zertifikaten und gegebenenfalls Signaturanwendungskomponenten für „qualifizierte elektronische Signaturen mit Anbieterakkreditierung" staatlich zu fördern,

- die vorhandenen Angebote der deutschen und sonstigen europäischen Anbieter vornehmlich heranzuziehen, um die qualifizierte elektronische Signatur und den Einsatz entsprechender Produkte zu fördern,

- eGovernment- und eCommerce-Projekte zu fördern, die qualifizierte elektronische Signaturen unterhalb der Wurzelzertifizierungsinstanz der RegTP einsetzen und somit Multifunktionalität und Interoperabilität gewährleisten,

- die Entwicklung von technischen Standards für die umfassende Einbindung der qualifizierten elektronischen Signatur zu fördern,

- die Weiterentwicklung der entsprechenden Chipkartentechnik voranzutreiben.

18.8 Verbesserung statt Absenkung des Datenschutzniveaus in der Telekommunikation

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Umlaufverfahren vom 28. April 2003)

Im Zuge der bevorstehenden Novellierung des Telekommunikationsgesetzes plant die Bundesregierung neben der Abschaffung der Unternehmensstatistik (vgl. dazu Entschließung der 65. Konferenz vom 28. März 2003 zur Transparenz bei der Telefonüberwachung) eine Reihe weiterer Änderungen, die zu einer Absenkung des gegenwärtigen Datenschutzniveaus führen würden.

Zum einen ist vorgesehen, die Zweckentfremdung von Bestandsdaten der Telekommunikation (z. B. Art des Anschlusses, Kontoverbindung, Befreiung vom Telefonentgelt aus sozialen oder gesundheitlichen Gründen) für Werbezwecke weitergehend als bisher schon dann zuzulassen, wenn der Betroffene dem nicht widerspricht. Dies muss – wie bisher – die informierte Einwilligung des Betroffenen voraussetzen.

Außerdem plant die Bundesregierung, Daten, die den Zugriff auf Inhalte oder Informationen über die näheren Umstände der Telekommunikation schützen (wie z. B. PIN und PUK – Personal Unblocking Keys –), in Zukunft der Beschlagnahme für die Verfolgung beliebiger Straftaten zugänglich zu machen. Bisher kann der Zugriff auf solche Daten nur angeordnet werden, wenn es um die Aufklärung bestimmter schwerer Straftaten geht. Diese Absenkung oder gar Aufhebung der verfassungsmäßig gebotenen Schutzschwelle für Daten, die dem Telekommunikationsgeheimnis unterliegen, wäre nicht gerechtfertigt; dies ergibt sich auch aus dem Urteil des Bundesverfassungsgerichts vom 12. März 2003.

Aus der Sicht des Datenschutzes ist auch die Versagung eines anonymen Zugangs zum Mobilfunk problematisch. Die beabsichtigte Gesetzesänderung führt dazu, dass z. B. der Erwerb eines „vertragslosen" Handys, das mit einer entsprechenden – im Prepaid-Verfahren mit Guthaben aufladbaren – SIM-Karte ausgestattet ist, einem Identifikationszwang unterliegt. Dies hat zur Folge, dass die Anbieter von Prepaid-Verfahren eine Reihe von Daten wegen eines möglichen Zugriffs der Sicherheitsbehörden auf Vorrat speichern müssen, die sie für ihre Betriebszwecke nicht benötigen. Die verdachtslose rountinemäßige Speicherung zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer künftiger Straftaten würde auch zur Entstehung von selbst für die Sicherheitsbehörden sinn- und nutzlosen Datenhalden führen. So sind erfahrungsgemäß z. B. die Erwerber häufig nicht mit den tatsächlichen Nutzern der Prepaid-Angebote identisch.

Insgesamt fordern die Datenschutzbeauftragten des Bundes und der Länder den Gesetzgeber auf, das gegenwärtige Datenschutzniveau bei der Telekommunika-

tion zu verbessern, statt es weiter abzusenken. Hierzu sollte jetzt ein eigenes Telekommunikations-Datenschutzgesetz verabschiedet werden, das den Anforderungen einer freiheitlichen Informationsgesellschaft genügt und später im Zuge der noch ausstehenden zweiten Stufe der Modernisierung des Bundesdatenschutzgesetzes mit diesem zusammengeführt werden könnte.

18.9 Neuordnung der Rundfunkfinanzierung

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und und der Länder im Umlaufverfahren vom 30. April 2003)

Die Länder bereiten gegenwärtig eine Neuordnung der Rundfunkfinanzierung vor, die im neuen Rundfunkgebührenstaatsvertrag geregelt werden soll. Die dazu bekannt gewordenen Vorschläge der Rundfunkanstalten lassen befürchten, dass bei ihrer Umsetzung die bestehenden datenschutzrechtlichen Defizite nicht nur beibehalten werden, sondern dass mit zum Teil gravierenden Verschlechterungen des Datenschutzes gerechnet werden muss:

- Insbesondere ist geplant, alle Meldebehörden zu verpflichten, der GEZ zum In-Kraft-Treten des neuen Staatsvertrages die Daten aller Personen in Deutschland zu übermitteln, die älter als 16 Jahre sind. Dadurch entstünde bei der GEZ faktisch ein bundesweites zentrales Register aller über 16-jährigen Personen mit Informationen über ihre sozialen Verhältnisse (wie Partnerschaften, gesetzliche Vertretungen, Haushaltszugehörigkeit und Empfang von Sozialleistungen), obwohl ein großer Teil dieser Daten zu keinem Zeitpunkt für den Einzug der Rundfunkgebühren erforderlich ist.
- Auch wenn in Zukunft nur noch für ein Rundfunkgerät pro Wohnung Gebühren gezahlt werden, sollen alle dort gemeldeten erwachsenen Bewohner von vornherein zur Auskunft verpflichtet sein, selbst wenn keine Anhaltspunkte für eine Gebührenpflicht bestehen. Für die Auskunftspflicht reicht es demgegenüber aus, dass zunächst – wie bei den amtlichen Statistiken erfolgreich praktiziert – nur die Meldedaten für eine Person übermittelt werden, die dazu befragt wird.
- Zudem soll die regelmäßige Übermittlung aller Zu- und Wegzüge aus den Meldedaten nun um Übermittlungen aus weiteren staatlichen bzw. sonstigen öffentlichen Dateien wie den Registern von berufsständischen Kammern, den Schuldnerverzeichnissen und dem Gewerbezentralregister erweitert werden. Auf alle diese Daten will die GEZ künftig auch online zugreifen.
- Gleichzeitig soll die von den zuständigen Landesdatenschutzbeauftragten als unzulässig bezeichnete Praxis der GEZ, ohne Wissen der Bürgerinnen und Bürger deren personenbezogene Daten bei Dritten – wie beispielsweise in der Nachbarschaft oder bei privaten Adresshändlern – zu erheben, ausdrücklich erlaubt werden.
- Schließlich sollen die bisher bestehenden Möglichkeiten der Aufsicht durch die Landesbeauftragten für den Datenschutz ausgeschlossen werden, sodass für die Rundfunkanstalten und die GEZ insoweit nur noch eine interne Datenschutzkontrolle beim Rundfunkgebühreneinzug bestünde.
- Diese Vorstellungen der Rundfunkanstalten widersprechen dem Verhältnismäßigkeitsprinzip und sind daher nicht akzeptabel.
- Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen ihre Forderung nach einer grundlegenden Neuorientierung der Rundfunkfinanzierung, bei der datenschutzfreundliche Modelle zu bevorzugen sind. Sie haben hierzu bereits praktikable Vorschläge vorgelegt.

18.10 Bei der Erweiterung der DNA-Analyse Augenmaß bewahren

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder im im Umlaufverfahren vom 16. Juli 2003)

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

Die Vorschläge gehen dahin,

— zum einen als Anlasstat zur Anordnung einer DNA-Analyse künftig nicht mehr – wie vom geltenden Recht gefordert – in jedem Fall eine Straftat von erheblicher Bedeutung oder – wie jüngst vom Bundestag beschlossen – eine Straftat gegen die sexuelle Selbstbestimmung zu verlangen, sondern auch jede andere Straftat mit sexuellem Hintergrund oder sogar jedwede Straftat ausreichen zu lassen,

— zum anderen die auf einer eigenständigen, auf den jeweiligen Einzelfall bezogenen Gefahrenprognose beruhende Anordnung durch Richterinnen und Richter entfallen zu lassen und alle Entscheidungen der Polizei zu übertragen.

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

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

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

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

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

18.11 Automatisches Software-Update

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Umlaufverfahren vom 7. August 2003)

Die Datenschutzbeauftragten des Bundes und der Länder wenden sich entschieden gegen die zunehmenden Bestrebungen von Softwareherstellern, über das Internet unbemerkt auf die Personalcomputer der Nutzerinnen und Nutzer zuzugreifen.

Zur Gewährleistung der Sicherheit und der Aktualität von System- und Anwendungssoftware ist es notwendig, regelmäßig Updates vorzunehmen. Weltweit agierende Softwarehersteller bieten in zunehmendem Maße an, im Rahmen so genannter Online-Updates komplette Softwarepakete oder einzelne Updates über das Internet auf die Rechner ihrer Kunden zu laden und automatisch zu installieren. Diese Verfahren bergen erhebliche Datenschutzrisiken in sich:

- Immer öfter werden dabei – oftmals vom Nutzer unbemerkt oder zumindest nicht transparent – Konfigurationsinformationen mit personenbeziehbaren Daten aus dem Zielrechner ausgelesen und an die Softwarehersteller übermittelt, ohne das dies im derzeit praktizierten Umfang aus technischen Gründen erforderlich ist.

- Darüber hinaus bewirken Online-Updates vielfach Änderungen an der Software der Zielrechner, die dann in der Regel ohne die erforderlichen Tests und Freigabeverfahren genutzt werden.

- Ferner ist nicht immer sichergestellt, dass andere Anwendungen problemlos weiter funktionieren. Das – unbemerkte – Update wird dann nicht als Fehlerursache erkannt.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Änderungen an automatisierten Verfahren zur Verarbeitung personenbezogener Daten oder an den zugrunde liegenden Betriebssystemen Wartungstätigkeiten im datenschutzrechtlichen Sinn sind, und daher nur den dazu ausdrücklich ermächtigten Personen möglich sein dürfen. Sollen im Zusammenhang mit derartigen Wartungstätigkeiten personenbezogene Daten von Nutzerinnen und Nutzern übermittelt und verarbeitet werden, ist die ausdrückliche Zustimmung der für die Daten verantwortlichen Stelle erforderlich.

Die meisten der derzeit angebotenen Verfahren zum automatischen Software-Update werden diesen aus dem deutschen Datenschutzrecht folgenden Anforderungen nicht gerecht. Insbesondere fehlt vielfach die Möglichkeit, dem Update-Vorgang ausdrücklich zuzustimmen. Die Daten verarbeitenden Stellen dürfen daher derartige Online-Updates nicht nutzen, um Softwarekomponenten ohne separate Tests und formelle Freigabe auf Produktionssysteme einzuspielen.

Auch für private Nutzerinnen und Nutzer sind die automatischen Update-Funktionen mit erheblichen Risiken für den Schutz der Privatsphäre verbunden. Den Erfordernissen des Datenschutzes kann nicht ausreichend Rechnung getragen werden, wenn unbemerkt Daten an Softwarehersteller übermittelt werden und somit die Anonymität der Nutzerinnen und Nutzer gefährdet wird.

Die Datenschutzbeauftragten des Bundes und der Länder fordern daher die Software-Hersteller auf, überprüfbare, benutzerinitiierte Update-Verfahren bereitzustellen, die nicht zwingend einen Online-Datenaustausch mit dem Zielrechner erfordern. Auch weiterhin sollten datenträgerbasierte Update-Verfahren angeboten werden, bei denen lediglich die für den Datenträgerversand erforderlichen Daten übertragen werden. Automatisierte Online-Update-Verfahren sollten nur wahlweise angeboten werden. Sie sind so zu modifizieren, dass sowohl der Update- als auch der Installationsprozess transparent und revisionssicher sind. Software-Updates dürfen in keinem Fall davon abhängig gemacht werden, dass den Anbietern ein praktisch nicht kontrollierbarer Zugriff auf den eigenen Rechner gewährt werden muss. Personenbezogene Daten dürfen nur dann übermittelt werden, wenn der Verwendungszweck vollständig bekannt ist und in die Verarbeitung ausdrücklich eingewilligt wurde. Dabei ist in jedem Fall das gesetzlich normierte Prinzip der Datensparsamkeit einzuhalten.

18.12 Gesundheitsmodernisierungsgesetz

(Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003)

Die Datenschutzkonferenz begrüßt, dass mit den gesetzlichen Regelungen zur Gesundheitskarte und zu dem bei den Spitzenverbänden der Krankenkassen und der Kassenärztlichen Bundesvereinigung gebildeten zentralen Datenpool datenschutzfreundliche Lösungen erreicht werden konnten. Die Gesundheitskarte un-

terliegt auch künftig der Verfügungsgewalt der Patientinnen und Patienten. Für den quartals- und sektorenübergreifenden Datenpool dürfen nur pseudonymisierte Daten gespeichert werden.

Die Datenschutzkonferenz wendet sich nicht grundsätzlich gegen zusätzliche Kontrollmechanismen der Krankenkassen.

Die Datenschutzbeauftragten kritisieren, dass sie zu wesentlichen, erst in letzter Minute eingeführten und im Schnellverfahren realisierten Änderungen nicht rechtzeitig und ausreichend beteiligt wurden. Diese Änderungen bedingen erhebliche Risiken für die Versicherten:

- Für das neue Vergütungssystem werden künftig auch die Abrechnungen der ambulanten Behandlungen mit versichertenbezogener Diagnose an die Krankenkassen übermittelt. Mit der vorgesehenen Neuregelung könnten die Krankenkassen rein tatsächlich umfassende und intime Kenntnisse über 60 Millionen Versicherte erhalten. Die Gefahr gläserner Patientinnen und Patienten rückt damit näher. Diese datenschutzrechtlichen Risiken hätten durch die Verwendung moderner und datenschutzfreundlicher Technologien einschließlich der Pseudonymisierung vermieden werden können. Leider sind diese Möglichkeiten überhaupt nicht berücksichtigt worden.

- Ohne strenge Zweckbindungsregelungen könnten die Krankenkassen diese Daten nach den verschiedensten Gesichtspunkten auswerten (z. B. mit datawarehouse-systemen).

Die Datenschutzkonferenz nimmt anerkennend zur Kenntnis, dass vor diesem Hintergrund durch Beschlussfassung des Ausschusses für Gesundheit und Soziale Sicherheit eine Klarstellung dahingehend erfolgt ist, dass durch technische und organisatorische Maßnahmen sicherzustellen ist, dass zur Verhinderung von Versichertenprofilen bei den Krankenkassen

- eine sektorenübergreifende Zusammenführung der Abrechnungs- und Leistungsdaten unzulässig ist, und dass

- die Krankenkassen die Daten nur für Abrechnungs- und Prüfzwecke nutzen dürfen.

Darüber hinaus trägt eine Entschließung des Deutschen Bundestages der Forderung der Datenschutzkonferenz Rechnung, durch eine Evaluierung der Neuregelung in Bezug auf den Grundsatz der Datenvermeidung und Datensparsamkeit unter Einbeziehung der Möglichkeit von Pseudonymisierungsverfahren sicherzustellen, dass Fehlentwicklungen vermieden werden.

Die Datenschutzkonferenz hält eine frühestmögliche Pseudonymisierung der Abrechnungsdaten für notwendig, auch damit verhindert wird, dass eine Vielzahl von Bediensteten personenbezogene Gesundheitsdaten zur Kenntnis nehmen kann.

18.13 Konsequenzen aus der Untersuchung des Max-Planck-Instituts über Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation

(Entschließung der 66. Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003)

Das Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg hat im Mai diesen Jahres sein im Auftrag des Bundesministeriums der Justiz erstelltes Gutachten „Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation nach den §§ 100 a, 100 b StPO und anderer verdeckter Ermittlungsmaßnahmen“ vorgelegt. Darin hat es festgestellt, dass

— die Zahl der Ermittlungsverfahren, in denen TKÜ-Anordnungen erfolgten, sich im Zeitraum von 1996 bis 2001 um 80 % erhöht (1996: 2149; 2001; 3868) hat,

— die Gesamtzahl der TKÜ-Anordnungen pro Jahr im Zeitraum von 1990 bis 2000 von 2.494 um das Sechsfache auf 15.741 gestiegen ist,

— sich die Zahl der jährlich davon Betroffenen im Zeitraum von 1994 bis 2001 von 3.730 auf 9.122 fast verdreifacht hat,

— in 21 % der Anordnungen zwischen 1.000 und 5.000 Gespräche, in 8 % der Anordnungen mehr als 5.000 Gespräche abgehört worden sind,

— der Anteil der staatsanwaltschaftlichen Eilanordnungen im Zeitraum von 1992 bis 1999 von ca. 2 % auf ca. 14 % angestiegen ist,

— die Beschlüsse in ca. drei Viertel aller Fälle das gesetzliche Maximum von drei Monaten umfassen, drei Viertel aller Maßnahmen tatsächlich aber nur bis zu zwei Monaten andauern,

— lediglich 24 % der Beschlüsse substanziell begründet werden,

— es nur in 17 % der Fälle Ermittlungserfolge gegeben hat, die sich direkt auf den die Telefonüberwachung begründenden Verdacht bezogen,

— 73 % der betroffenen Anschlussinhaberinnen und -inhaber nicht über die Maßnahme unterrichtet wurden.

Die Telefonüberwachung stellt wegen ihrer Heimlichkeit und wegen der Bedeutung des Rechts auf unbeobachtete Kommunikation einen gravierenden Eingriff in das Persönlichkeitsrecht der Betroffenen dar, zu denen auch unbeteiligte Dritte gehören. Dieser Eingriff kann nur durch ein legitimes höherwertiges Interesse gerechtfertigt werden. Nur die Verfolgung schwerwiegender Straftaten kann ein solches Interesse begründen. Vor diesem Hintergrund ist der Anstieg der Zahl der Verfahren, in denen Telefonüberwachungen angeordnet werden, kritisch zu bewerten. Dieser kann – entgegen häufig gegebener Deutung – nämlich nicht allein mit dem Zuwachs der Anschlüsse erklärt werden. Telefonüberwachungen müssen ultima ratio bleiben. Außerdem sind die im Gutachten des Max-Planck-Instituts zum Ausdruck kommenden strukturellen Mängel zu beseitigen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert den Gesetzgeber und die zuständigen Behörden auf, aus den Ergebnissen der Untersuchung daher folgende Konsequenzen zu ziehen:

Der gesetzliche Richtervorbehalt darf nicht aufgelockert werden. Die Verwertung der angefertigten Aufzeichnungen sollte in Fällen staatsanwaltschaftlicher Eilanordnungen davon abhängig gemacht werden, dass ein Gericht rückwirkend deren Rechtmäßigkeit feststellt.

Um die Qualität der Entscheidungen zu verbessern, sollte die Regelung des § 100 b StPO dahin gehend ergänzt werden, dass die gesetzlichen Voraussetzungen der Anordnung einzelfallbezogen darzulegen sind. Die Rechtsfolgen für erhebliche Verstöße gegen die Begründungsanforderungen sollten gesetzlich geregelt werden (z. B. Beweisverwertungsverbote).

— Um die spezifische Sachkunde zu fördern, sollten die Aufgaben der Ermittlungsrichterinnen und -richter auf möglichst wenige Personen konzentriert werden. Die Verlagerung auf ein Kollegialgericht ist zu erwägen.

— Der Umfang des – seit Einführung der Vorschrift regelmäßig erweiterten – Straftatenkataloges des § 100 a StPO muss reduziert werden.

— Um eine umfassende Kontrolle der Entwicklung von TKÜ-Maßnahmen zu ermöglichen, muss in der StPO eine Pflicht zur zeitnahen Erstellung aussagekräftiger Berichte geschaffen werden. Jedenfalls bis dahin muss auch die in § 88 Abs. 5 TKG festgelegte Berichtspflicht der Betreiber von Telekommunikationsanlagen und der Regulierungsbehörde beibehalten werden.

— Der Umfang der Benachrichtigungspflichten, insbesondere der Begriff der Beteiligten, ist im Gesetz näher zu definieren, um die Rechte, zumindest aller bekannten Geprächsteilnehmerinnen und -teilnehmer zu sichern. Für eine längerfristige Zurückstellung der Benachrichtigung ist zumindest eine richterliche Zustimmung entsprechend § 101 Abs. 1 Satz 2 StPO vorzusehen. Darüber hinaus müssen die Strafverfolgungsbehörden beispielsweise durch Berichtspflichten angehalten werden, diesen gesetzlich festgeschriebenen Pflichten nachzukommen.

— Zum Schutz persönlicher Vertrauensverhältnisse ist eine Regelung zu schaffen, nach der Gespräche zwischen den Beschuldigten und zeugnisverweigerungsberechtigten Personen grundsätzlich nicht verwertet werden dürfen.

— Zur Sicherung der Zweckbindung nach § 100 b Abs. 5 StPO und 477 Abs. 2 Satz 2 StPO muss eine gesetzliche Verpflichtung zur Kennzeichnung der aus TKÜ-Maßnahmen erlangten Daten geschaffen werden.

— Die Höchstdauer der Maßnahmen sollte von drei auf zwei Monate reduziert werden.

— Auch aufgrund der Weiterentwicklung der Technik zur Telekommunikationsüberwachung (z. B. IMSI-Catcher, stille SMS, Überwachung des Internetverkehrs) ist eine Fortführung der wissenschaftlichen Evaluation dieser Maßnahmen unabdingbar. Die gesetzlichen Regelungen sind erforderlichenfalls deren Ergebnissen anzupassen.

18.14 Gravierende Verschlechterungen des Datenschutzes im Entwurf des neuen Telekommunikationsgesetzes

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Umlaufverfahren vom 21. November 2003)

Die Bundesregierung hat am 15. Oktober 2003 den Entwurf für ein neues Telekommunikationsgesetz beschlossen. Dieser Entwurf sieht jetzt zwar – entsprechend der Forderung der Datenschutzbeauftragten – die vorläufige Beibehaltung der Unternehmensstatistik zu Überwachungsmaßnahmen vor; im Übrigen enthält er aber gravierende Verschlechterungen des Datenschutzniveaus.

Insbesondere berechtigt der Gesetzentwurf die Diensteanbieter, grundsätzlich alle entstehenden Verkehrsdaten (also auch alle Zielrufnummern) unverkürzt bis zu sechs Monaten nach Versendung der Rechnung zu speichern. Damit wird ohne Not und ohne überzeugende Begründung eine Regelung aufgegeben, die bisher die Speicherung von verkürzten Zielrufnummern vorsieht, wenn die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder vollständige Löschung entscheiden. Die bisherige Regelung berücksichtigt in ausgewogener Weise sowohl die Datenschutz- als auch die Verbraucherschutzinteressen der beteiligten Personen und hat sich in der Praxis bewährt. Vollends inakzeptabel ist die inzwischen vom Rechtsausschuss des Bundesrates vorgeschlagene Pflicht zur Vorratsdatenspeicherung für sechs Monate. Gegen eine solche Regelung bestehen erhebliche verfassungsrechtliche Bedenken.

Schon die von der Bundesregierung vorgeschlagene Regelung würde dazu führen, dass Millionen von Verkehrsdatensätzen selbst dann noch unverkürzt gespeichert bleiben und dem Zugriff anderer Stellen ausgesetzt sind, wenn die Diensteanbieter sie für ihre Abrechnungszwecke nicht mehr benötigen. Das im Entwurf weiterhin vorgesehene Recht der Kundinnen und Kunden, die Speicherung gekürzter Zielrufnummern oder ihre vollständige Löschung nach Rechnungsversand zu verlangen, wird daran wenig ändern, weil nur eine Minderheit es wahrnehmen wird. Die Beibehaltung des bisherigen angemessenen Datenschutzstandards sollte nicht von der Initiative der Betroffenen abhängig gemacht werden, sondern allen zugute kommen, die nicht ausdrücklich einer weitergehenden Speicherung zustimmen. Zudem sind die Rechte der angerufenen Teilnehmerinnen und Teilnehmer zu berücksichtigen, in die durch eine Speicherung der unverkürzten Verkehrsdaten zusätzlich eingegriffen wird.

Die Datenschutzbeauftragten haben zudem stets die Zwangsidentifizierung beim Erwerb von vertragslosen (prepaid) Handys als gesetzwidrig kritisiert und sehen sich jetzt in dieser Auffassung durch das Urteil des Bundesverwaltungsgerichts vom 22. Oktober 2003 (Az.: 6 C 23.02) bestätigt. Zugleich wenden sie sich gegen die mit der TKG-Novelle geplante Einführung einer derartigen Identifikationspflicht, die zu einer verdachtslosen Datenspeicherung auf Vorrat führen würde. Wer ein solches Handy kauft, gibt es häufig ab oder verschenkt es, und ist deshalb nicht identisch mit der Person, die das Handy nutzt. Deshalb bringen diese Daten keinen nennenswerten Informationsgewinn für die Sicherheitsbehörden.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten ohne Bindung an einen Straftatenkatalog oder einen Richtervorbehalt der Zugriff auf Passwörter, PIN, PUK usw. eröffnet werden, mit denen die Inhalte oder nähere Umstände einer Telekommunikation geschützt werden. Dies würde die Möglichkeit eröffnen, von dieser Befugnis unkontrolliert Gebrauch zu ma-

chen. Die Befugnis dürfte zudem häufig ins Leere laufen, da die Anbieter diese Daten aus Gründen der Datensicherheit für sie selbst unlesbar verschlüsselt speichern.

Die Datenschutzbeauftragten des Bundes und der Länder fordern den Gesetzgeber auf, den Entwurf bei den bevorstehenden Beratungen in diesen sensiblen Punkten zu korrigieren und den gebotenen Schutz des Telekommunikationsgeheimnisses sicherzustellen.

19. Entschließungen der Internationalen Konferenz der Datenschutzbeauftragten (Auswahl)

19.1 Transfer von Daten von Flugpassagieren

(Entschließung der 25. Internationalen Konferenz der Datenschutzbeauftragten vom 12. September 2003)

Die 25. Internationale Konferenz der Datenschutzbeauftragten beschließt Folgendes:

Die Konferenz stellt fest, dass

Im Zuge des legitimen Kampfes gegen den Terrorismus und das organisierte Verbrechen werden in einigen Ländern Maßnahmen in Betracht gezogen, die die Grundrechte und Freiheiten, insbesondere das Recht auf den Schutz der Privatsphäre, gefährden könnten.

Das Risiko besteht, Demokratie und Freiheit zu gefährden, unter der Vorgabe diese Werte zu verteidigen.

Gesetzliche Anforderungen an Fluggesellschaften oder andere Transportanbieter den Zugriff an Gesamtdaten von Passagieren, die in Reservationssystemen gespeichert werden, zu gewährleisten oder diese zu übertragen, mit den internationalen Datenschutzgrundsätzen oder den Verpflichtungen der Transportanbieter, die sich auf den nationalen Datenschutzgesetzen stützen, im Konflikt stehen könnten.

Die Konferenz bekräftigt infolge dessen, dass

In der Bekämpfung des internationalen Terrorismus und des organisierten Verbrechens die Staaten unter vollständiger Achtung der Grundprinzipien des Datenschutzes reagieren sollten, denn diese Werte stellen einen integralen Bestandteil der Werte dar, die sie verteidigen.

Regelmäßige internationale Transfers von Personendaten, soweit nötig, nur innerhalb eines bestimmten Datenschutzrahmens erfolgen dürfen, z. B. auf Basis eines internationalen Abkommens, welches den datenschutzrechtlichen Anforderungen wie einem klar definierten Zweck, der verhältnismäßigen Datenerhebung, einer zeitlichen Begrenzung der Datenspeicherung, der Benachrichtigung der betroffenen Personen, der Gewährleistungen der Rechte der betroffenen Person, sowie einer unabhängigen Aufsicht gerecht wird.

19.2 Radio-Frequency Identification

(Entschließung der Internationalen Konferenz der Datenschutzbeauftragten vom 20. November 2003)

Radio-Frequency Identification (RFID) Technologie wird zunehmend für eine Reihe unterschiedlicher Zwecke eingesetzt. Während es Situationen gibt, in denen diese Technologie positive und günstige Auswirkungen hat, sind auch negative Folgen für die Privatsphäre möglich. RFID-Etiketten werden bisher vorwiegend zur Identifikation und Organisation von Gegenständen (Produkten), zur Kontrolle von Logistik oder zum Schutz der Authenzität einer Produktmarke (Warenzeichen) verwendet; sie könnten aber auch mit personenbezogenen Informationen, wie Kreditkarten-Daten, verknüpft werden und auch zur Erhebung solcher Informationen oder zur Lokalisierung oder Profilbildung über Personen benutzt werden, die Gegenstände mit RFID-Etiketten besitzen. Diese Technologie würde die unbemerkte Verfolgung und das Aufspüren von Individuen ebenso wie die Verknüpfung erhobener Daten mit bestehenden Datenbanken ermöglichen.

Die Konferenz hebt die Notwendigkeit hervor, Datenschutzprinzipien zu berücksichtigen, wenn RFID-Etiketten verknüpft mit personenbezogenen Daten eingeführt werden sollen. Alle Grundsätze des Datenschutzrechts müssen beim Design, der Einführung und der Verwendung von RFID-Technologie berücksichtigt werden. Insbesondere

sollte jeder Datenverarbeiter vor der Einführung von RFID-Etiketten, die mit personenbezogenen Daten verknüpft sind oder die zur Bildung von Konsumprofilen führen, zunächst Alternativen in Betracht ziehen, die das gleiche Ziel ohne die Erhebung von personenbezogenen Informationen oder die Bildung von Kundenprofilen erreichen;

wenn der Datenverarbeiter darlegen kann, dass personenbezogene Daten unverzichtbar sind, müssen diese offen und transparent erhoben werden;

dürfen personenbezogene Daten nur für den speziellen Zweck verwendet werden, für den sie ursprünglich erhoben wurden und sie dürfen nur solange aufbewahrt werden, wie es zur Erreichung dieses Zweckes erforderlich ist und

soweit RFID-Etiketten im Besitz von Personen sind, sollte diese die Möglichkeit zur Löschung der gespeicherten Daten oder zur Deaktivierung oder Zerstörung der Etiketten haben.

Diese Grundsätze sollten bei der Gestaltung und bei der Verwendung von Produkten mit RFID berücksichtigt werden.

Das Auslesen und die Aktivierung von RFID-Etiketten aus der Ferne ohne vernünftige Gelegenheit für den Besitzer des etikettierten Gegenstandes, diesen Vorgang zu beeinflussen, würde zusätzliche Datenschutzrisiken auslösen.

Die Konferenz und die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation wird die technischen Entwicklungen in diesem Bereich genau und detaillierter verfolgen, um die Achtung des Datenschutzes und der Privatsphäre in einer Umgebung allgegenwärtiger Datenverarbeitung sicherzustellen.

20. Anhang

20.1 Auswahl von Presseberichten in Tageszeitungen/Zeitschriften im Jahr 2003 mit Themen aus dem Land Bremen

Datum	Zeitung	Titel/Inhalt
20.01.	Nordsee-Zeitung	**Nur alte Rostlauben sind erlaubt** Sozialhilfeempfänger werden überprüft – „Kein Kavaliersdelikt"
21.01.	Nordsee-Zeitung	**Datenabgleich vom Bund geregelt** Kritik an Sozialamt für Auto-Überprüfungsaktion
22.01.	Nordsee-Zeitung	**Tipps für den Umgang mit Werbemails** Datenschützer stellt Informationen ins Internet
23.01.	taz-bremen	**Unter Beobachtung** Jagd auf Sozialhilfemissbrauch: Landesdatenschützer droht Bremerhavens Sozialdezernent
23.01.	Kreiszeitung Syke	**Datenschutz im Mülleimer?** Die Entsorgungsbetriebe wollen online auf Meldedaten zugreifen/Höhe der Einnahmen unklar
23.01.	Weser-Kurier	**Spitzenplatz beim Lauschen** Zahl der Telefonüberwachungen nahm rapide zu/ Böse sieht Lücke
23.01.	Weser-Kurier	**Bürgerschaft kurz und bündig** Verschleierungstaktik – SPD-Abgeordnete sorgt sich um den Datenschutz
26.01.	Weser-Report	**Selbstverteidigung im Internet** Datenschutzbeauftragter gibt Tipps für den Umgang mit dem Internet
26.01.	Weser-Kurier	**Für Hacker ein Kinderspiel** Funknetzwerke bergen große Risiken
27.01.	Nordsee-Zeitung	**Hinweise zu ärgerlichen Mails**
28.01.	taz-Bremen	**Klick dich ans Eck** Eine Datenbank mit Bildern aller Bremer Häuser und Straßen soll Behörden und Politikern lästige Wege ersparen. Beiräte sollen zahlen – und dafür kassieren dürfen, wenn die Daten an andere verkauft werden
13.02.	Nordsee-Zeitung	**Bedenken gegen Speicheltest** Staatsanwälte im Land haben 12.500 Täter-Akten durchforstet
14.02.	Bremer Nachrichten/ Weser-Kurier	**Gerechtere Müllgebühren? Bürger schummeln, Stadt kassiert** BEB warnt: Datenabgleich bei Müllgebühren kostet Bremen bis zu 90 Mio. Euro
20.02.	Nordsee-Zeitung	**Datenabgleich ist nicht verboten** Vergleich von Sozialhilfe- und Kfz-Daten wird in der Bürgerschaft von Datenschützern unterschiedlich bewertet
25.02.	Die Welt – Bremen	**Neue Software für Bremens Verwaltung**
05.03.	Weser-Kurier	**City Server: Patt im Beirat Mitte**
08.03.	Nordsee-Zeitung	**Polizei sucht Nadeln im Heuhaufen** Rasterfahndung zum Aufspüren potenzieller Terroristen

Datum	Zeitung	Titel/Inhalt
08.03.	Bremer Anzeiger	**Scharfe Kritik an der Rasterfahndung** Landesbeauftragter für Datenschutz kritisiert Verfahren und Effektivität
08.03.	Kreiszeitung Syke	**Daten wahllos hergegeben** Mängel bei der Rasterfahndung
08.03.	Die Welt – Bremen	**Rasterfahndung: Polizei nimmt 18 Bürger ins Visier** BKA überprüft 664 Datensätze aus Bremen. Erste Bilanz des Datenschützers. Hauptvorwurf: „Es dauert unerträglich lange"
08.03.	taz-bremen	**664 Bremer im Visier** Zum Teil unrechtmäßig und meistens erfolglos: Der Datenschutzbeauftragte rüffelt Polizei und Handelskammer wegen Verstößen bei der Rasterfahndung
10.03.	Weser-Kurier	**EU-Datenbank soll „Asyltourismus" einschränken** Fingerabdrücke werden zentral in Luxemburg gespeichert und sollen Missbrauch verhindern
11.03.	taz-bremen	**Böse wegen Holst „befremdet"** Innensenator leitet Datenschutz-Kritik an Rasterfahndung weiter an die Polizei
11.03.	Weser-Kurier	**Kritik an Kritik der Rasterfahndung** Böse und Handelskammer wehren sich
22.03.	Bremer Anzeiger	**Datenschutzbeauftragter kritisiert Videoüberwachung** Sven Holst stellt seinen Jahresbericht vor und rügt den Umgang mit Faxgeräten
22.03.	Nordsee-Zeitung	**Die unglaublichsten Pannen der Ämter** Datenschützer legt Bericht vor – „Faxen üben"
22.03.	Nordsee-Zeitung	**Videoüberwachung am Bremer Bahnhof kritisiert** Datenschützer nicht rechtzeitig informiert
22.03.	taz-bremen	**Holst gegen Hopplahopp-Videos** Der Landesdatenschützer hat seinen Bericht vorgelegt. Zwei Ärgernisse von vielen: die Überwachung am Bahnhofsvorplatz und der Fehlversand von Steuerbescheiden.
22.03.	Kreiszeitung Syke	**Deutliche Kritik an Bahnhofs-Kamera** Bremen Datenschützer legt Jahresbericht für 2002 vor
22.03.	Delmenhorster Kreisblatt	**Scharfe Kritik an Innensenator Kuno Böse** Durchs Polizeigesetz nicht abgedeckt Videoüberwachung: Rechtschaffende Bürger nur unzureichend über Beobachtung informiert
22.03.	Bremer Nachrichten/ Weser-Kurier	**„Verfaxtes" kann brisant sein** Datenschutzbericht greift auch Videoüberwachung auf
23.03.	Weser-Report	**Mit Auto gibt's weniger Geld** Sozialbehörde plant Kfz-Datenabgleich
31.03.	Bild-Bremen	**Bremer Arzt warf Patientenakten auf den Sperrmüll und halb Vegesack blätterte drin rum**

Datum	Zeitung	Titel/Inhalt
02.04.	Das BLV Wochenzeitung Bremen-Nord	Medikamente und Patienten-Akten auf dem Sperrmüll **Vegesacker Gynäkologe räumte Praxis unkonventionell**
09.04.	Bremer Nachrichten/ Weser-Kurier	**Entrümpelungswettlauf stockt** SPD und CDU streiten um Vermieterbeschleunigung
22.04.	Die Welt-Bremen	**Datenschutzausschuss berät über „City Server"** Neue Technik soll auch in Bremen virtuelle Rundgänge durch die Stadt erlauben – Beiräte erhoffen sich eigene Einnahmen
24.04.	Die Welt-Bremen	**Verein Haus und Grund gegen den „City-Server"**
30.04.	Weser-Report	**Einsatz des City-Servers in Bremen?** Pro & Contra
04.05.	Kurier am Sonntag	**UMTS-Standorte sind kein Geheimnis** Bremen nicht so zurückhaltend wie Post-Regulierungsbehörde/Lagepläne im Internet veröffentlicht
12.07.	Kreiszeitung Syke	**Früher musste man mehr durchboxen** Seit 25 Jahren hat Bremen einen Datenschutzbeauftragten/CD zum Jubiläum/„Immer wieder neu erfinden"
12.07.	taz-bremen	**Zum Geburtstag ´ne CD-Rom** Seit 25 Jahren hat Bremen einen Landesbeauftragten für den Datenschutz
12.07.	Nordsee-Zeitung	**„Datenschutz auf einem guten Weg"** Landesamt seit 25 Jahren in Bremerhaven
16.07.	Weser-Report	**25 Jahre Datenschutz in Bremen**
18.07.	Delmenhorster Kreisblatt	**Polizei: Vorwurf der Untätigkeit ist falsch** Täterin fällt schon seit 1990 auf
18.07.	Kreiszeitung Syke	**„Ordnungsgemäß weitergeleitet"** Diskussionen nach den tödlichen Messerstichen in der Neustadt/Polizei weist Vorwürfe zurück
18.07.	Bremer Nachrichten/ Weser-Kurier	**Behörden nach Bluttat unter Druck** **„Wieso lief die noch frei herum?"** Täterin hatte schon vor der Bluttat in der Neustadt wiederholt zum Messer gegriffen
21.07.	Die Welt – Bremen	**Der Bahnhofsvorplatz bleibt ein Brennpunkt** Nachts steigt die Unsicherheit – Noch keine Ergebnisse der Videoüberwachung
22.07.	taz-nord-bremen	**„Was wollen Sie machen?"** Aufregung bei den Behörden: Die 41-jährige Täterin, die vor zehn Tagen in der Neustadt ihre Nachbarin getötet hat, war der Polizei einschlägig bekannt – doch angeblich sei diese Information nicht weitergereicht worden.
25.07.	Kreiszeitung Syke	**Dienststellen wollen Zusammenarbeit verbessern** Tötungsdelikt Neustadt: „Notwendige Informationsdichte fehlte"/Beamte sollen stärker sensibilisiert werden
25.07.	Delmenhorster Kreisblatt	**Senat zieht Konsequenzen aus Mordfall** Meldesystem soll besser werden – Ständige Behördenkonferenz

Datum	Zeitung	Titel/Inhalt
25.07.	Die Welt – Bremen	**Mordfall in der Bremer Neustadt hat Konsequenzen** Die Ressorts Inneres, Justiz und Soziales wollen ihre Abstimmung verbessern – Keine gegenseitigen Schuldzuweisungen
25.07.	taz-nord-bremen	**Sensibilisieren und registrieren** Konsequenz aus tödlichem Angriff einer psychisch Kranken gegen Nachbarin: Behörden beschließen bessere Vernetzung, um auf aggressive Kranke besser zu reagieren
28.07.	Bremer Nachrichten/ Weser-Kurier	**CDU will präventive Telefonüberwachung**
29.07.	Kreiszeitung Syke	**Datenschützer reagiert zurückhaltend** Sven Holst: Erstmal sehen, was da verabredet wurde/Tötungsdelikt Neustadt: 41-Jährige in psychiatrischer Betreuung
30.07.	Bremer Nachrichten/ Weser-Kurier	**Falsche Fährte trotz DNA-Analyse** Tatverdacht erst durch weiteren Vergleich des Genmaterials entkräftet
01.08.	Kommune 21	**Nur nichts verschenken** Kommunales eGovernment in Deutschland wird häufig in einem Atemzug MEDIA@Komm genannt. Ein Vergleich zwischen den MEDIA@Komm-Städten und anderen Kommunen zeigt, wo die deutschen Kommunen insgesamt stehen
02.08.	Die Welt – Bremen	**Bürgertelefon gegen Schwarzarbeit**
05.08.	Weser-Kurier	**Neuer Anlauf zur Verbrecherjagd am Computer** Nach dem Desaster vor zwei Jahren soll das INPOL-System ab 16. August funktionieren
12.08.	Handelsblatt	**Datenschützer kritisieren Überwachungswut des Staates** Behörde registriert zunehmende Erfassung der Bürger – Mehr Rechte für das Parlament gefordert
31.08.	Weser-Report	**Der Kommentar: Falsch gelaufen** Datenschutz steht einer angemessenen pädagogischen Betreuung im Weg?
05.09.	Weser-Kurier	**„Schule kann über Haft informiert werden"** Sven Holst widerspricht der Behauptung von Bildungssenator Lemke
24.09.	Weser-Kurier	**Bremer Software bundesweit im Einsatz** Innenministerium in Berlin unterzeichnete Vertrag für „Governikus"-Nutzung
24.09.	Weser-Report	**Toter gewinnt zweimal am Tag** Post gibt Adressen an Unternehmen weiter
02.10.	taz-nord-bremen	**Datenschützer rüffelt Soziales** Noch kein Konzept für Sprach-Screening-Verfahren
02.10.	taz-bremen	**Kommt der gläserne Patient?** Datenschützer warnen vor Negativ-Folgen der Gesundheitsreform für Versicherte
02.10.	taz-bremen	**Justiz macht auf Nordstaat** Ausschuss nickt: Jugendliche Langzeitstraftäter sollen nach Hameln, Frauen nach Lübeck

Datum	Zeitung	Titel/Inhalt
05.10.	Weser-Kurier	**Datenschutzkonzept für Sprachtests angemahnt** Papier soll nun erarbeitet werden/Elternbeschwerden nach erster Untersuchung im Frühjahr
07.10.	taz bremen	**Ein angekündigter Tod?** Die Bremer Bürgerschaft debattiert morgen den Tod einer Bremer Studentin, umgebracht von der Nachbarin. Der Bremer Senat räumt fehlende „Sensibilität" für Gewalttaten mit psychiatrischem Hintergrund bei der Polizei ein
08.10.	Bremer Nachrichten/ Weser-Kurier	**Künftig mit Datenschutz** Einigkeit, aber keine Einstimmigkeit zur Sprachstandserhebung
22.10.	Bremer Nachrichten/ Weser-Kurier	**„Big Brother" künftig in Bremer Bussen und Bahnen** Fahrzeuge werden mit Videokameras ausgestattet
28.10.	Weser-Kurier	**„Vorsicht bei Lifestyle-Befragung"**
30.10.	Weser-Kurier	**Visa mit biometrischen Daten** EU und USA wollen weltweit einheitliche Identifizierung durchsetzen
30.10.	taz-nord	**Schily hilft seinem Freund aus USA** Innenminister Otto Schily verspricht dem obersten US-Heimatschützer Tom Ridge noch mehr Anstrengungen Deutschlands im Kampf gegen den Terror: Biometrische Daten im Pass und Austausch von Passagierlisten sollen „so bald wie möglich" kommen
06.11.	taz-nord-bremen	**Dampf unterm Hintern der Exekutive** So funktioniert Volksherrschaft: Ausschuss lässt Ressorts und Datenschützer antanzen und über ihre Arbeit berichten. Am Schluss gibt's Hausaufgaben
06.11.	Nordsee-Zeitung	**Große Schilder weisen auf Überwachung** Auf dem Vorplatz am Bremer Hauptbahnhof sollen größere Schilder auf Überwachung mit Videokamera hinweisen
08.11.	Kreiszeitung Syke	**Schwere Zeiten für Sexshop-Besucher** Ausschuss lässt Ressort und Datenschützer über ihre Arbeit berichten/Neue Schilder auf dem Bahnhofsvorplatz
20.11.	Delmenhorster Kreisblatt	**Vernetzung darf nicht zum gläsernen Patienten führen** Datenschutz-Experten aus der Weser-Ems-Region treffen sich zum regelmäßigen Erfahrungsaustausch
22.11.	Weser-Kurier	**PolMobil scheitert noch vor Testphase** Projekt mit Telekom-Tochter beendet
03.12.	Weser-Kurier	**Polizei löschte Daten aus der Rasterfahndung**
08.12.	Weser-Kurier	**Datenschützer gegen Steuer-PIN**

20.2 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:

22. Jahresbericht 1999, Bürgerschafts-Drs. 15/266 (Restexemplare)

23. Jahresbericht 2000, Bürgerschafts-Drs. 15/852 (vergriffen)

24. Jahresbericht 2001, Bürgerschafts-Drs. 15/1106 (Restexemplare)

25. Jahresbericht 2002, Bürgerschafts-Drs. 15/1418

Broschüre „Mobilfunk und Datenschutz“

Broschüre „Datenschutz bei WindowsNT“

Broschüre „Handlungsempfehlungen datenschutzgerechtes eGovernment”

Faltblatt „Datenschutz im Verein”

Faltblatt „Adressenhandel und unerwünschte Werbung“

Faltblatt „Handels- und Wirtschaftsauskunfteien“

BfD-Info 1 Bundesdatenschutzgesetz – Text und Erläuterungen –

BfD-Info 2 Der Bürger und seine Daten

BfD-Info 3 Schutz der Sozialdaten

BfD-Info 4 Die Datenschutzbeauftragten in Behörde und Betrieb

BfD-Info 5 Datenschutz in der Telekommunikation

20.3 Index

Druck: Anker-Druck Bremen