25. Jahresbericht

des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2002 den 25. Jahresbericht zum 31. März 2003 (§ 33 Abs. 1 Bremisches Datenschutzgesetz – BremDSG). Redaktionsschluss für die Beiträge war der 31. Dezember 2002.

Ein redaktioneller Hinweis an dieser Stelle sei noch gestattet. Die meisten Sachverhalte beurteilen sich noch nach altem Recht, dies wird durch die Kennzeichnung der Paragraphen mit dem Kürzel "BrDSG" deutlich. Soweit schon neues Recht anzuwenden war, ist dies an der Benennung mit der Abkürzung "BremDSG" zu erkennen.

Sven Holst
Landesbeauftragter für den Datenschutz

Der Mensch hat mit elektronischen Mitteln
die Übertragung des Gedankens beschleunigt.
Ganz und gar misslungen ist ihm allerdings,
die Qualität des Gedankens zu verbessern.

Peter Ustinov in „Der Alte Mann und Mr. Smith“

Inhaltsverzeichnis

1. Vorwort

Dieser Jahresbericht mit über 120 verschiedenen Beiträgen gibt die Bandbreite der unterschiedlichen Herausforderungen wieder, denen sich meine Dienststelle im letzten Jahr stellen musste. Dabei sind noch nicht einmal alle Felder angesprochen. So wird zum Beispiel eine Vielzahl von Bürgereingaben wegen ihrer Spezialität ebenso wenig wiedergegeben wie verschiedene auf meiner Homepage hinzugekommene Beiträge. Allein der im Anhang veröffentlichte Pressespiegel gibt die Vielfältigkeit der Themen wieder und macht zugleich deutlich, dass der Datenschutz über das ganze Jahr hinweg kontinuierlich in der Öffentlichkeit wahrgenommen wird. Dabei muss in den meisten Fällen vor einer datenschutzrechtlichen Beurteilung der Sachverhalt vor Ort aufgeklärt, neue technische Umgebungen eingeschätzt und spezialgesetzliche Regelungen berücksichtigt werden.

Gelegentlich wehren sich die geprüften Stellen mit Haken und mit Ösen; so konnte zum Beispiel ein Betrieb mit weit über hundert Beschäftigten erst beim dritten Gesprächstermin ohne die Androhung von Zwangsmaßnahmen davon überzeugt werden, dass er einen betrieblichen Beauftragten für den Datenschutz zu bestellen hat. Dabei stieg die Anzahl der Gesprächsteilnehmer auf Seiten des Betriebes von Mal zu Mal. Beim letzten Termin saßen neben Vertretern der Geschäftsleitung, dem Personalchef und einem Rechtsanwalt auch Verbandsvertreter. Erst durch die vor den Augen der Versammelten durchgeführte Systemuntersuchung der im System abgebildeten Zugriffsrechte konnte bewiesen werden, dass weit mehr als vier Personen Zugriff auf personenbezogene Daten nahmen und damit die Voraussetzungen zur Bestellung eines betrieblichen Beauftragten für den Datenschutz nach dem Bundesdatenschutzgesetz erfüllt waren.

Ich will mich an dieser Stelle nicht darüber beklagen, dass datenverarbeitende Stellen bis zum Äußersten gehen, das ist ihr gutes Recht. Auch das anlässlich der Prüfung vorgetragene Argument, die Bestellung eines betrieblichen Datenschutzbeauftragten sei ein Kostenfaktor, eine gesetzlich nicht vorgeschriebene Bestellung führe zu einer Wettbewerbsverzerrung, will ich gelten lassen, wenn umgekehrt akzeptiert wird, dass auch die Nichtbestellung eines betrieblichen Datenschutzbeauftragten bei Vorliegen der gesetzlichen Voraussetzungen gegenüber anderen Konkurrenten, die dieser Pflicht nachgekommen sind, eine Wettbewerbsverzerrung darstellt. Ich will zudem nicht den Eindruck erwecken, als stelle sich die Privatwirtschaft nur widerwillig dem Datenschutzrecht. Ich berichte dies nur, weil auch dieser Fall - wie viele andere - keinen Eingang in meine Berichterstattung über die Tätigkeit der Datenschutzaufsichtsbehörden gefunden hat. Alle Aktivitäten lassen sich einfach nicht aufzählen, ohne den Rahmen zu sprengen, es muss immer bei einer Auswahl bleiben.

Insgesamt bin ich bereits angesichts der im Bericht vorgestellten Arbeit erstaunt, wie leistungsfähig meine Dienststelle wieder mit einem doch recht kleinen Personalstab war.

Ein Zweites sei vorangestellt. Da noch vor der Sommerpause die Bürgerschaft neu gewählt wird und sich danach auch der Datenschutzausschuss neu zusammensetzen wird, ist es mir ein Anliegen, die in wirklich allen Belangen gute und konstruktive Zusammenarbeit mit dem Datenschutzausschuss über alle Fraktionen und über die gesamte Legislaturperiode hinweg und die wesentliche

Unterstützung, die meine Arbeit durch den Ausschuss erfahren hat, hervorzuheben. Dabei ist der Datenschutzausschuss in vielen Fragen selbst initiativ geworden (vgl. Ziff. 4.2 dieses Berichts), hat eigene Datenschutzthemen beraten, hat sich vielfach vor Ort über die Praxis informiert und beharrlich die Umsetzung seiner Beschlüsse durch die datenverarbeitenden Stellen verfolgt. Dabei habe ich es nie als Last empfunden, den Datenschutzausschuss von meinen Ideen zu überzeugen - auch die Vertreter der senatorischen Bereiche hatten diese Möglichkeit - sondern ich habe die Auseinandersetzungen vor dem Datenschutzausschuss immer auch als Prüfstein für die Nachvollziehbarkeit meiner Vorschläge begriffen.

1.1 Novellierung BremDSG abgeschlossen

Das herausragende Ereignis für den Datenschutz in 2002 im Lande Bremen ist sicherlich die Novellierung des Bremischen Datenschutzgesetzes (genauer vgl. Ziff. 1.15 dieses Berichts). Mit den Änderungen wurde den Anforderungen aus der EU-Datenschutzrichtlinie von 1995 entsprochen und der Anschluss an ein einheitliches europäisches Datenschutzniveau erreicht. Verbunden damit sind eine Stärkung der Rechte der Betroffenen gegenüber den datenverarbeitenden Stellen, eine Stärkung der Rechte des Parlaments und eine Verbesserung meiner Kontrollmöglichkeiten. Mit Unterstützung des Datenschutzausschusses und durch die Entscheidung des Parlaments konnte die gesetzlich vorgeschriebene Pflicht zur Bestellung behördlicher Beauftragter für den Datenschutz durch alle öffentlichen Stellen im Lande, die personenbezogene Daten verarbeiten, erreicht werden. Entsprechende Regelungen finden sich im Bundesdatenschutzgesetz und in den Datenschutzgesetzen der meisten anderen Länder. Von dieser Vorschrift erwarte ich besondere Auswirkungen auf die Qualität des Datenschutzes, wird damit doch deutlich gemacht, dass es das ureigenste Interesse der datenverarbeitenden Stellen selbst ist, den datenschutzrechtlichen Anforderungen Rechnung zu tragen. Natürlich wird nicht von vornherein alles perfekt laufen. Ich will aber meinen Beitrag dazu leisten, dass die behördlichen Datenschutzbeauftragten in den Stand versetzt werden, ihre im novellierten Datenschutzgesetz beschriebenen Aufgaben zu erfüllen. Als ersten Schritt bereite ich dazu zweitägige Schulungen vor.

1.2 Selbstverteidigung im Internet

Ein Klick auf dem heimischen PC erlaubt es dem Surfer, mit allen Teilen der Welt in Verbindung zu treten, dort Informationen abzurufen oder Geschäfte zu tätigen. Im gleichen Zuge aber verrät der Benutzer seine Interessen, seine Vorlieben, seine Konsumgewohnheiten oder Freizeitgestaltung, eventuell auch seine sexuellen Neigungen oder politischen Vorstellungen. Allerorts belauern große Rechenmaschinen das Internet; ohne sein Wissen wird der Betroffene beobachtet, analysiert und kategorisiert. Aber all dies muss der Surfer nicht untätig hinnehmen. Die mit Unterstützung der Verbraucherseite einer großen Bremer Tageszeitung durchgeführte Aktion "Selbstverteidigung im Internet " (vgl. Ziff. 17.2 dieses Berichts) zeigt mögliche Gegenwehr auf. Die Aktion ist schon jetzt ein voller Erfolg. Die Möglichkeiten zur Verteidigung der eigenen Datenschutzrechte werden den Besuchern meiner Internetseiten Schritt für Schritt und mit praktischen Beispielen erläutert (vgl. Ziff. 1.13 dieses Berichts und unter www. datenschutz.bremen.de). Wesentliches Anliegen dieser Initiative

ist es, die Daten auf dem heimischen PC vor unberechtigten Zugriffen zu schützen und die Internetnutzer zu befähigen, sich vor unbewusster Preisgabe ihrer Daten im Internet zu verteidigen (vgl. in diesem Zusammenhang auch die Konferenzentschließung „Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet“, Ziff. 15.8 dieses Berichts).

Ich bin überrascht über den großen Erfolg, der sich nicht nur in den stark gewachsenen Zugriffszahlen auf meine Homepage wiederspiegelt, sondern auch in zahlreichen an meine Dienststelle gerichteten positiven E-Mails. Dabei kann ich natürlich nicht quantifizieren, wie viele im Lande Bremen lebende Bürger ich mit meinem Angebot erreiche, Zugriffe können von allen Orten erfolgen. Gleichwohl kann davon ausgegangen werden, dass die starken Zuwachsraten in den letzten beiden Monaten vornehmlich auf die Publikationen in den Bremer Presseorganen zurückzuführen sind. In dem Maße, wie die Seiten meines Angebotes zunehmen, wird deutlich, dass die Pflege und Weiterentwicklung des Internetangebotes eigene personelle Kapazitäten beanspruchen, über die ich nicht in ausreichenden Maße verfüge. Gleichwohl bin ich bemüht, das - wie andere mir versichern - qualitativ hochwertige Angebot weiter aufrechtzuerhalten, denn ich stelle auf Grund von Bürgernachfragen fest, dass das Angebot mich in vielen alltäglichen Fragen entlastet: Bürgern, die meine Internetseiten besucht haben, brauche ich bestimmte Verfahren nicht mehr zu erläutern oder über ihre Datenschutzrechte nicht mehr aufzuklären, sie stellen gezielt weitergehende Fragen.

1.3 Indiskretionen bei Themen in den Untersuchungsausschüssen

Im Berichtsjahr wurden zwei parlamentarische Untersuchungsausschüsse (UA) durchgeführt, der UA "Bau und Immobilien" und der UA "Rechnungsprüfungsamt Bremerhaven". Insbesondere im Juni und Anfang Juli 2002 wurden durch Presse, Rundfunk und Fernsehen laufend detaillierte Informationen beziehungsweise Kopien von Originalunterlagen veröffentlicht, die im Zusammenhang mit der Durchführung dieser Untersuchungsausschüsse standen. Das heimliche Zuspielen dieser zum Teil sehr persönlichen Informationen und Unterlagen an die Medien war in diesem Umfang in Bremen ein Novum. Bei mir gingen deswegen aus verschiedenen Bereichen, aber auch von Betroffenen selbst, Beschwerden ein. Da die Unterlagen für eine Vielzahl von Personen zugänglich waren und ich wegen des Medienprivilegs auch keine Möglichkeit habe, bei den Unternehmen selbst Nachforschungen danach anzustellen, aus welcher Quelle die zugespielten Unterlagen stammen könnten, habe ich mich mit einem Appell an die Öffentlichkeit gewandt und die Einhaltung der Datenschutzbestimmungen gefordert. Es mag zwar sein, dass Informationen, die in den den Medien übergebenen Unterlagen enthalten waren, später im Rahmen der Verhandlungen im Untersuchungsausschuss bekannt werden, über diese Bekanntgabe entscheidet aber nicht der Einzelne, sondern der jeweilige Untersuchungsausschuss. Der Ausschuss entscheidet, ob und in welchem Umfang Informationen der Öffentlichkeit in einem geordneten Verfahren zugänglich gemacht werden. Voraussetzung hierfür ist, dass die Informationen im Zusammenhang mit dem Untersuchungsauftrag stehen. Von den Medien hätte ich mir in dieser Frage etwas mehr Sensibilität gewünscht.

1.4 Verfaxtes Fax

Diese Bemerkung einer Beschäftigten habe ich als Überschrift dieses Beitrags genommen, weil das Wort „verfaxtes" so ähnlich klingt wie „verhextes" oder „verflixtes" und beides spielt wohl mit eine Rolle bei der Absendung von Dokumenten per Faxgerät, wenn eine falsche Empfängernummer verwendet wird. Waren es in den letzten Berichtsjahren Unterlagen der Kriminalpolizei, die fehlgeleitet wurden, lief in diesem Jahr eine ganze Reihe von Beschwerden im Zusammenhang mit dem Einsatz von Faxgeräten auf. Ich habe exemplarisch vier gravierende Datenschutzverletzungen in diesen Bericht aufgenommen. In einem Fall wurden laut Presseberichten Einschreibebriefe mit umfangreichen Unterlagen, Personal- und Disziplinarangelegenheiten betreffend, versehentlich an einen falschen Adressaten gefaxt (vgl. Ziff. 5.1 dieses Berichts), in einem anderen Fall wurden Gehaltsmitteilungen per Fax an ein vielen Personen zugängliches Gerät gefaxt (vgl. Ziff. 13.2 dieses Berichts), in einem dritten Fall landeten ärztliche Unterlagen aus Krankenhäusern bei völlig unbeteiligten Privatleuten (vgl. Ziff. 8.7 dieses Berichts). Schließlich wurde ein Schulentwicklungsbericht mit vollständigem Namen, Geburtsdatum, Schule und Klasse des Kindes, der an das Amt für Soziale Dienste gesendet werden sollte, an einen privaten Haushalt gefaxt (vgl. Ziff. 10.5 dieses Berichts). In dem Schreiben über drei Seiten heißt es u. a. (Name geändert): „Mia wiederholte die erste Klasse, in der zweiten und dritten Klasse konnte und kann sie den Anforderungen im Unterricht kaum oder gar nicht gerecht werden. Das Lesen fällt ihr immer noch sehr schwer, mühsam geübte Diktate kann sie im normalen Klassentempo nicht mitschreiben. .... Ähnliche Lernprobleme hat Mia auch im Fach Mathematik. .... Ihre Lese-und Rechtschreibschwäche ist nicht selten Auslöser für Frustration, Unlust, Stöhnen und Traurigkeit ...usw."

Ist es mangelnde Sensibilität oder sind die Personen nicht hinreichend in die Funktionalität der Faxgeräte, die häufig als Kombigeräte (Fax und Kopierer) eingesetzt werden, eingewiesen? Man weiß es nicht. In allen geschilderten Fällen wurde jedenfalls gegen die geltenden Telefax-Regeln verstoßen. Mehr, als die Beschäftigten immer einmal wieder auf die grundlegenden Regeln beim Faxversand hinzuweisen, wie sie z. B. im roten Behördentelefonbuch der bremischen Verwaltung enthalten sind, kann man wohl nicht tun. Dort steht z. B.: „Soll nur ein bestimmter Empfangsberechtigter das Fax erhalten, so vereinbaren Sie seine Anwesenheit am Faxgerät..." oder „Der Absender ist für die ordnungsgemäße Übermittlung der Daten verantwortlich. Deshalb müssen Sie sich mit den Funktionen und der Wirkungsweise des Fax-Gerätes vertraut machen" usw.. Anders sieht die Lage in Bremerhaven aus; hier streite ich seit über einem dreiviertel Jahr dafür, dass überhaupt erst einmal Faxregeln als Konkretisierung der Transportkontrolle gem. § 7 Abs. 2 Nr. 9 BrDSG in Kraft gesetzt werden.

1.5 Miles and More

Nicht nur, dass sich viele Bürger an Preisausschreiben beteiligen und dabei freiwillig und kostenlos Informationen an Marketing- und Werbewirtschaft liefern, auch in so genannten Markt- und Meinungsforschungserhebungen werden seitenweise Informationen über Haushalt und Lebensstil auch der Mitbewohner freimütig preisgegeben. In einem Fall gab es 3 Fahrräder zu gewinnen bei über 100.000 Einsendungen. Über die wohl besten personenbezogenen Informationen aber verfügen die

so genannten „Kundenbindungs- oder Rabattsysteme", ob sie nun Payback, Happy Digits oder wie auch immer heißen. (Bei Payback gab es übrigens Ende November 2002 immer noch keine mit der zuständigen Datenschutzaufsichtsbehörde abgestimmte Einwilligungserklärung zur Datenverarbeitung, vgl. schon 24. JB, Ziff. 14.7.) Diese Systeme verfügen zum Teil branchenübergreifend über Informationen zum Konsumverhalten. Selbst bei Bargeldzahlung wird der Kunde hier aus der Anonymität gelockt. Jeder Warenkorb lässt sich personenbezogen analysieren. Im "Data Warehouse" lassen sich diese Daten mit entsprechenden Werkzeugen unter beliebigen Aspekten auswerten. In Bonussystemen werden für "Miles and More" Reisegewohnheiten, Urlaubsziele, Autogeschmack bei Mietwagen, Kreditkarten, Freizeitverhalten "and more" preisgegeben. Dieses System machte im Berichtsjahr in besonderer Weise auf sich aufmerksam. Durch die Bonusmeilen-Affäre war die Lufthansa in erhebliche Erklärungsnot geraten, weil Flugdaten von Abgeordneten an die BILD-Zeitung gelangt waren. Das Blatt startete eine Kampagne mit der Überschrift: „Wer hat Ihren Ferien-Flug bezahlt, Herr Minister?" und veröffentlichte in Folge gezielt namentlich genannte Bundestagsabgeordnete, die bei den Flügen erworbene Bonusmeilen zu privaten Zwecken eingesetzt haben sollen. Wegen der Bonusmeilen-Affäre sind mehrere Politiker von ihren Ämtern zurückgetreten, staatsanwaltschaftliche Ermittlungen wurden eingeleitet und der Bundestagspräsident schaltete sich ein. Noch nie habe ich so vernehmlich aus weiten politischen Kreisen den Ruf nach dem Datenschutz vernommen. Bei eigener Betroffenheit wird dann plötzlich konkret, wofür der Datenschutz steht, auch wenn gelegentlich die selben Personen in anderem Zusammenhang den Datenschutz als Hemmnis geißeln. Eine Datenschutzprüfung ergab schließlich, dass aus dem Kreis der Beschäftigten eines Call-Centers eine Liste mit personenbezogenen Daten gezielt an Dritte weitergegeben worden war. Fragen der Zweckbindung und einer technischen Zugriffsbegrenzung wurden laut, in jedem Falle war dies ein Warnschuss für alle Unternehmen.

1.6 Zur Europäischen Dimension des Datenschutzes

Dass ein Datenschutz, der an nationalen Grenzen Halt macht, keine großen Erfolge verzeichnen kann, ist spätestens bekannt, seit ein elektronisches Telefonbuch mit der in Deutschland aus Gründen des Datenschutzes verbotenen Invertsuche kurzerhand im benachbarten Ausland produziert und von dort aus vertrieben wurde. Multinationale Unternehmen können ihre Datenverarbeitung beliebig in andere Länder verlagern, die Globalisierung der Datenverarbeitung durch das Internet ist hinlänglich bekannt. Mit Inkrafttreten der EU-Datenschutzrichtlinie ist jedem Bundesland in Deutschland klar geworden, dass auch auf EU-Ebene geschaffene datenschutzrechtliche Rahmenbedingungen auf die Bedingungen der Datenverarbeitung im eigenen Land Einfluss haben können. Es liegt daher auf der Hand, dass, will ich zukünftige Entwicklungen auf dem Gebiet des Datenschutzes rechtzeitig erkennen, ich mich insoweit auch international orientieren muss. Was die technische Entwicklung anbelangt, liegt dies ohnehin auf der Hand, aber auch für die rechtliche Entwicklung gilt Entsprechendes.

Ich will dies an einem Beispiel aus jüngster Zeit verdeutlichen. Im Oktober 2002 unterrichtete die Bundesregierung den Bundesrat über den Vorschlag für eine Richtlinie des europäischen Parlaments zur Harmonisierung der Rechts- und Verwaltungsvorschriften der Mitgliedstaaten über den

Verbraucherkredit (vgl. BR-Drs. 756/02). Im Kapitel III dieser Drucksache finden sich Regelungen zum Schutz der Privatsphäre. Positiv zu vermerken ist eine in Art. 7 vorgesehene enge Zweckbindung der persönlichen Daten, die im Zuge des Abschlusses oder der Abwicklung von Kreditverträgen bei Verbrauchern und Garanten oder bei Dritten erhoben werden. Sie sollen nur zum Zweck der Einschätzung ihrer finanziellen Situation und ihrer Fähigkeit zur Rückzahlung verarbeitet werden dürfen. Diskussionsbedarf hingegen besteht bei den Regelungen in Art. 8. Hier werden die Mitgliedstaaten „zwecks Registrierung der Verbraucher und Garanten, die ihren Zahlungsverpflichtungen nicht nachgekommen sind" verpflichtet, eine zentrale Datenbank zu betreiben. Darüber hinaus werden die Kreditgeber verpflichtet, vor jeder Kreditvergabe die zentrale Datenbank abzufragen.

Mit diesen Regelungen würde der Grundstein für eine europäische Kreditauskunftei gelegt. Ich habe daher die Datenschutzaufsichtsbehörden informiert und dieses Thema zur nächsten Sitzung der AG Kreditwirtschaft angemeldet, an der auch regelmäßig Vertreter der Bundesverbände der Kreditwirtschaft (ZKA) teilnehmen.

1.7 Zur Situation der Dienststelle

Ich denke, die Leistungsfähigkeit meiner Dienststelle kommt in dem vorgelegten Bericht zum Ausdruck. Solche Ergebnisse können nur mit einem für den Datenschutz hoch motivierten Team erreicht werden. Da tut es gut, wenn, wie anlässlich der letzten Parlamentsdebatte über den Bericht und den Antrag des Datenschutzausschusses zum 24. Jahresbericht in der Bremischen Bürgerschaft geschehen, die Arbeit der Dienststelle gewürdigt und die Leistungsbereitschaft anerkannt wird.

Ein Zugang zum Internet besteht jetzt an allen Arbeitsplätzen; ich bewerte diese Entwicklung positiv, zeigt sich doch in der alltäglichen Arbeit, dass aktuelle Recherchen im Internet häufig die Aufgabenerledigung erleichtern. Eine gewisse Behinderung ist allerdings durch die von der BreKom vorgenommenen Sperrungen eingetreten. Für verschiedene Prüfungen benötige ich einen ungehinderten Internetzugang, eine Lösung des Problems zeichnet sich aber schon ab. Zum Teil auch erziehungszeitbedingte Abgänge und Vakanzen konnten nicht immer nahtlos überbrückt werden. Soweit ich Ersatz finden konnte, haben sich die neuen Kräfte hervorragend eingearbeitet. Die Administration des Hausnetzes wird intern durchgeführt und läuft weitestgehend problemlos. Gleiches gilt für die technische Betreuung der Homepage. Kleine Umbauarbeiten zur Effektivierung der Aktenverwaltung und zur Verbesserung der Archivierung sind abgeschlossen, mit der Umstellung auf eine Pendelregistratur soll nach Abgabe des Tätigkeitsberichtes begonnen werden.

1.8 Öffentlichkeitsarbeit und Presseresonanz

Auch im letzten Berichtszeitraum habe ich zu verschiedenen Datenschutzfragen Presseerklärungen herausgegeben, um die Öffentlichkeit, insbesondere aber die Bürgerinnen und Bürger über neue Datenschutzentwicklungen zu informieren. Einen Überblick über die Resonanz zu Datenschutzthemen in und um Bremen und Bremerhaven bietet der Pressespiegel unter Ziff. 16.1. Sehr positiv aufgenommen worden ist die sechsteilige Serie, veröffentlicht unter dem Motto „Selbstverteidigung im Internet“. Insgesamt bin ich mit der Resonanz auf meinen Internetauftritt sehr zufrieden. Die

Datenschutz-Seiten konnten im Berichtsjahr durchschnittlich 14.285 Seiten-Anfragen pro Monat verzeichnen, was einer Nutzung von durchschnittlich 469 Anfragen pro Tag entspricht. Oder, mit anderen Worten, mein Internetangebot wird pro Tag durchschnittlich von 100 Bürgern besucht. Dabei fällt auf, dass die Seiten-Anfragen in den Monaten, in denen die oben beschriebene Internetaktion durchgeführt wurde, kontinuierlich anstiegen, um im Januar 2003 maximale Zahlen von 22.949 Anfragen in diesem Monat bzw. 740 pro Tag zu erreichen. Diese Zahlen machen deutlich, dass die Attraktivität der Datenschutz-Website durch die veröffentlichte Internetaktion stark erhöht werden konnte.

Ein weiterer Schwerpunkt meiner Öffentlichkeitsarbeit war die Beteiligung an der Erarbeitung und Herausgabe von Merkblättern zum Datenschutz im nicht öffentlichen Bereich, insbesondere bei Vereinen, Handels- und Wirtschaftsauskunfteien und im Adresshandel. Die Unterlagen können bei mir angefordert werden.

1.9 Von meiner Dienststelle durchgeführte Fortbildungsmaßnahmen

Wie in den letzten Jahren hat der Landesbeauftragte für den Datenschutz an verschiedenen Einrichtungen Fortbildungs- und Qualifizierungsmaßnahmen durchgeführt oder mitgestaltet. Dieses erfolgte für Mitarbeiter der bremischen Verwaltung allgemein, aber auch für Sachbearbeiter in der Sozialverwaltung.

Ebenso wurden Informations- und Schulungsveranstaltungen zu speziellen Fragestellungen (neues BDSG, neue DV-Technik, neue Software) durchgeführt.

Ich plane in Zusammenarbeit mit dem Aus- und Fortbildungszentrum der bremischen Verwaltung sowie dem Technik-Referat des Senator für Finanzen, im Frühjahr/Sommer 2003 spezielle Kurse für behördliche Beauftragte für den Datenschutz einzurichten. Diese Kurse sollen die nach dem neuen § 7 a BremDSG in den Behörden und bremischen Einrichtungen zu bestellenden Datenschutzbeauftragen befähigen, ihre Aufgaben zu erfüllen.

1.10 Eingabenschwerpunkte

Erneut erhielt ich eine Vielzahl von Bürgereingaben, die sich bei mir über die Verarbeitung ihrer personenbezogenen Daten beklagten. Die Eingaben richteten sich zu etwa gleichen Teilen gegen Stellen des öffentlichen und des nicht öffentlichen Bereichs. Während die Eingaben im öffentlichen Bereich insbesondere die Verarbeitung personenbezogener Daten durch die Polizei, die Sozialverwaltung und Einrichtungen des Gesundheitsdienstes betrafen, bezogen sie sich im nicht öffentlichen Bereich speziell auf Fragen des Arbeitnehmerdatenschutzes und des Adresshandels sowie die Datenverarbeitung von Auskunfteien und privaten ärztlichen Einrichtungen. Die bei mir eingegangenen Eingaben führten häufig zu Prüfungen. Als Ergebnis musste ich oft die Nichteinhaltung der zu beachtenden datenschutzrechtlichen Vorschriften feststellen und zu deren Einhaltung auffordern. Bei schwerwiegenden Verstößen habe ich Bußgeldverfahren eingeleitet.

1.11 Kooperationen

§ 27 Abs. 5 BrDSG lautet: „Der Landesbeauftragte für den Datenschutz arbeitet mit den Behörden und sonstigen Stellen, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz im Bund und in den Ländern zuständig sind, sowie mit den Aufsichtsbehörden nach § 38 des Bundesdatenschutzgesetzes zusammen." Diese Vorschrift beinhaltet Möglichkeit und Pflicht zur Zusammenarbeit, in der Praxis ist es jedoch schlichte Notwendigkeit. Angesichts der immer noch rasanten technischen Entwicklung auf allen Gebieten der Informationsverarbeitung und der engen personellen Ressourcen bei fast allen für den Datenschutz zuständigen Dienststellen, sind sowohl der Bundesbeauftragte wie die Landesbeauftragten auf der einen Seite und die Datenschutzaufsichtsbehörden auf der anderen Seite gezwungen, zu kooperieren und Lasten zu verteilen.

Neben der Mitarbeit in verschiedenen Arbeitskreisen der Konferenz der Datenschutzbeauftragten des Bundes und der Länder spiegeln sich die wesentlichen Ergebnisse der Zusammenarbeit in den Entschließungen der Konferenz wieder, die ich dem Bericht angefügt habe (vgl. Ziff. 15. dieses Berichts). Den Vorsitz in diesem Jahr führte Rheinland-Pfalz.

Insbesondere auch durch das Interesse der Wirtschaft an einer möglichst einheitlichen Anwendung datenschutzrechtlicher Vorschriften, haben die Länder ein Gremium der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich, den Düsseldorfer Kreis, eingerichtet. Mitglieder des Düsseldorfer Kreises sind die Vertreter der obersten Aufsichtsbehörden der Länder, wie der Landesdatenschutzbeauftragten, soweit sie auch Aufsichtsbehörden für den nicht öffentlichen Bereich sind, sowie der Bundesbeauftragte für den Datenschutz, der bundesweit für den Telekommunikationsbereich zuständig ist. Die Beschlüsse des Düsseldorfer Kreises werden überwiegend durch die Arbeitsgruppen „Versicherungswirtschaft", „Kreditwirtschaft", „Auskunfteien", „Tele-und Mediendienste" und „Internationaler Datenverkehr" vorbereitet. Ich arbeite in den ersten drei der genannten Arbeitsgruppen regelmäßig mit. Der Düsseldorfer Kreis tagt zweimal jährlich, die Arbeitsgruppen nach Bedarf, in der Regel ein- bis zweimal jährlich. An den Sitzungen des Düsseldorfer Kreises in 2002 habe ich teilgenommen. Den Vorsitz führte dieses Jahr das Land Baden-Württemberg. Einzelne Ergebnisse aus diesem Bereich finden sich unter dem Punkt „Datenschutz in der Privatwirtschaft " wieder (vgl. Ziff. 14. dieses Berichts).

Nicht unerwähnt bleiben soll auch die gute Zusammenarbeit mit der landeseigenen „datenschutz nord GmbH“. Ich pflege mit der GmbH einen regelmäßigen Gedankenaustausch. Ich habe bei der GmbH das Internet-Prüfwerkzeug „OPTuM“ erworben. Meiner Anregung entsprang letztendlich die Entwicklung eines Internet-Switches, eines Schalters auf dem Desktop des PCs, mit dem zwischen dienstlicher und privater Internetnutzung umgeschaltet werden kann. Mit diesem Schalter ist eine klare Grenzziehung zwischen beiden Bereichen möglich, auch ein völlig getrennter und selbständig geschützter Versand und Empfang privater E-Mails kann damit erreicht werden, wenn der User sich z. B. bei einem Freemailer eine eigene Mailbox einrichtet.

Abgerundet werden soll der Bericht über die Kooperationen mit dem Hinweis auf meine Teilnahme am Erfa-Kreis der betrieblichen Beauftragten für den Datenschutz. Dieser in der Region besonders aktive

Kreis umfasst eine Mitgliederzahl im wohl dreistelligen Bereich. Auf der letzten Sitzung z. B. konnten rund 60 Teilnehmerinnen und Teilnehmer gezählt werden. Der branchenübergreifende Kreis bemüht sich, in den Betrieben auftretende Fragen und Entwicklungen unter Aspekten des Datenschutzes zu behandeln und Anregungen für konkrete Lösungen zu entwickeln. Auch Hilfestellungen zur Erfüllung der im BDSG genannten Aufgaben werden angeboten. Neben dem reinen Erfahrungsaustausch werden in den Sitzungen, die i.d.R. drei bis vier Mal im Jahr stattfinden, auch konkrete Themen behandelt, die mit dem Referat eines Mitgliedes oder eingeladenen Referenten eingeleitet werden. Ich habe die Möglichkeit, die Sicht der Aufsichtsbehörde vorzutragen, dabei wird immer gleich eine Vielzahl von Multiplikatoren erreicht.

1.12 Technik-Splitter

Im August 2002 meldete sich ein Bürger, der bei einem Bremer Markt ein Notebook gekauft hatte, dass ihm als Auslaufmodell, aber Neugerät, mit 24 Monaten Garantie verkauft worden war. Er wunderte sich, das auf den Festplatten des Notebooks relativ viel Speicherplatz belegt war, nach eingehender Analyse der Platten stellte er Daten von drei mittlerweile in Konkurs gegangenen Unternehmen darauf fest. Darunter waren unter anderem Briefe an das Finanzamt, an Debitoren, an die Handelskrankenkasse und Mitarbeiterzeugnisse. Leider hat er mir diese Daten nicht zur Verfügung gestellt, so dass ich den Vorfall nicht weiter verfolgen konnte.

Die Chiffriermaschine "Enigma" diente im militärischen Bereich zur Verschlüsselung geheimer Nachrichten. Ein danach konzipiertes Handy soll unerlaubtes Mithören von Telefongesprächen durch verschlüsselte Übertragung verhindern. Das Gerät soll Ende Dezember 2002 für einen Preis von rund 3.200 Euro zu erwerben sein. Der ständige technische Wettlauf zwischen Hase und Igel geht also weiter.

Zum Schluss des Berichtsjahres hat Presseberichten zufolge erneut ein Virus namens "SQL-Slammer" zugeschlagen. Der gerade mal 376 Byte große Schädling griff dabei keine PCs an oder löschte irgendwelche Daten, sondern befiel ausschließlich Server und machte sich dabei eine Sicherheitslücke, u. a. in dem Microsoft-Programm SQL Server 2000, zu Nutze. Der Virus verbreitete sich über Internet in Windeseile, alle 30 Sekunden wurde ein neuer Server befallen, allein in den USA fielen bei der Bank of America 13.000 Bankautomaten für einen Tag aus. Bei neuartigen Viren hilft die beste Firewall leider nur begrenzt.

Blaue Zähne (Bluetooth-Technik) müssen wohl nicht gezogen werden, wenn die richtigen Sicherheitseinstellungen vorgenommen werden. Die Technik ist für drahtlose Verbindungen im Nahbereich zwischen PCs, Druckern, Handys und anderen Peripheriegeräten einsetzbar (vgl. Ziff. 2.9 dieses Berichts). Allerdings müssen die richtigen Sicherheitseinstellungen vom Anwender vorgenommenen werden. Da diese Technik in immer größerem Maße zum Einsatz gelangt, habe ich den AK Technik der Datenschutzbeauftragten gebeten zu prüfen, ob es notwendig ist, für die Benutzer eine Hilfestellung für die vorzunehmenden Sicherheitseinstellungen zu erarbeiten. Die Beliebtheit solcher Technik ist nicht weiter verwunderlich, denn auf kurzen Distanzen, etwa in einem Gebäude, bieten die drahtlosen Verbindungen eine deutlich höhere Übertragungsgeschwindigkeit als GSM oder UMTS. Zudem ist die Installation von WLANs (wireless local area network = schnurloses Netz). So ist

beispielsweise denkbar, dass Hausgemeinschaften ein eigenes WLAN installieren, sich so zum Netzbetreiber aufschwingen und die Nutzung untereinander kostenfrei stellen.

Neue Handys ermöglichen standortbezogene Dienste. Erforderlich dafür ist ein WAP-fähiges Handy. Das Handy erkennt den momentanen Aufenthaltsort (in Deutschland) automatisch und zeigt dem Besitzer die von ihm gewünschten Adressen, z. B. von Hotels, Restaurants, Apotheken oder Kinos, an. Dabei kann man Angaben mit unterschiedlicher Genauigkeit auswählen. Hierfür ist eine Freigabe durch den Besitzer vorgesehen. Für die Benutzer dieser Dienste ist allerdings auch interessant, wie lange standortbezogene Daten nach Inanspruchnahme solcher Dienste, etwa für den Abrechnungsverkehr, gespeichert bleiben. Hier bedarf es noch weiterer Aufklärung. Presseberichten zufolge geht die Industrie davon aus, dass es bereits im kommenden Jahr in Deutschland mehr mobile als stationäre Internetterminals geben wird. Seien erst einmal die mobilen Breitbandnetze flächendeckend installiert, würden neue leicht bedienbare Geräte schnell den Markt erobern, wobei insbesondere die Konvergenz der digitalen Technologien bei elektronischen Geräten für den einfacheren Konsumenten eine weitere treibende Kraft sein wird.

1.13 Internet-Auftritt: www.datenschutz.bremen.de

Der im Jahr 2001 begonnene Internetauftritt des Landesbeauftragten für den Datenschutz (vgl. 24. JB, Ziff. 1.2.) ist eine Erfolgsstory. Im Berichtszeitraum wurde die Internetseite kontinuierlich weiterentwickelt und ausgebaut. Dabei wurde besonderes Augenmerk darauf gerichtet, die Bürgerinnen und Bürger auf die Risiken und Gefahren der Informationstechnologie für auf Datenschutz und Datensicherheit hinzuweisen und ihnen eine Fülle von praktischen Tipps und Informationen an die Hand zu geben, um den Selbstschutz im Umgang mit PC und Internetanschluss zu verbessern.

Unter dem Motto „Selbstverteidigung im Internet“ habe ich auf meiner Internetseite auf die spezifischen Gefahren für personalbezogene Daten hingewiesen und Schutzmöglichkeiten aufgezeigt. Ich empfehle jedem Internetnutzer dringend, sich mit den hier aufgezeigten Fragen zu beschäftigen und entsprechend seinen eigenen Interessen und der eigenen Risikobereitschaft die richtigen Entscheidungen zu treffen. Der Beitrag besteht aus fünf verschiedenen Teilen, die in regelmäßigen Abständen auf der Datenschutz-Homepage veröffentlicht wurden und sich mit den wichtigsten Themen rund um PC- und Internetsicherheit beschäftigen. Die Aktion wurde zeitnah durch den Weser-Kurier begleitet, wobei jeweils eine Zusammenfassung des jeweiligen Themas unter der Rubrik „Tipps für Verbraucher“ veröffentlicht wurde. Nachfolgend werden die einzelnen Themenbereiche kurz beschrieben.

- Der erste Teil der Aktion beschäftigt sich mit den Funktionsweisen der verschiedenen Arten von Computerviren und geht detailliert auf ihre Gefahrenpotentiale ein. Da in jüngerer Vergangenheit vor allem die enormen Schäden durch sog Würmer wie „I Love You“ ins Licht der Öffentlichkeit gerückt wurden, wurde besonderes Augenmerk darauf gerichtet, den Bürgerinnen und Bürgern vorbeugende Schutzmaßnahmen gegen diese Art der virtuellen Schädlinge aufzuzeigen. Da sich

Würmer in erster Linie durch infizierte E-Mail-Anhänge weiterverbreiten, wurde speziell zum Thema „sicher Mailen“ umfangreich informiert.

- Teil zwei der Aktion beschäftigt sich schwerpunktmäßig mit sog. „aktiven Inhalten“, ebenfalls sicherheitskritischen Funktionen, die unbemerkt aus dem Internet geladen und so unbeabsichtigt zur Ausführung kommen können. Dabei sind die verschiedensten Manipulationen an Daten und Programmen auf den Rechnern der PC-Nutzerinnen und -Nutzer denkbar. Als Konsequenz daraus wird den Bürgern dadurch gezeigt, wie sie den von ihm genutzten Web-Browser so konfigurieren können, dass bereits ein guter Basisschutz verwirklicht ist.
- Lag im ersten und zweiten Teil der Aktion der thematische Fokus auf dem Bereich der Datensicherheit, so wurde im dritten Teil in erster Linie der Schutz der persönlichen Daten thematisiert. Sog. Cookies und Web-Bugs können das Surfverhalten des Nutzers auskundschaften, um so regelrechte Surfprofile anzulegen und zu vermarkten. Der Weg zum „gläsernen Surfer“ ist da tatsächlich nicht mehr weit. Des Weiteren stehen immer mehr Programme (sog. Spyware) im Verdacht, Anwenderinnen und Anwender auszuspionieren und personenbezogene Daten über das Internet zum jeweiligen Hersteller zu versenden. Auch hier werden dem Bürger sinnvolle und nützliche Vorbeuge- und Schutzmaßnahmen aufgezeigt.
- Im vierten Teil werden einige Grundlagen der PC-Sicherheit erläutert und den Bürgerinnen und Bürgern nützliche Tipps zur Verbesserung der Systemsicherheit mit auf den Weg gegeben.
- Der letzte Teil der Aktion befasst sich abschließend und ergänzend mit virtuellen Plagen, die dem PC-Anwender Zeit und Geld kosten können. Hier werden sog. Spam (elektronische Werbung) und 0190-Dialer thematisiert, über rechtliche Hintergründe informiert und technische Schutzmaßnahmen angeboten. Es war ein Anliegen des Datenschutzausschusses der Bremischen Bürgerschaft, dass ich auch auf diese Gefahren hinweise.

Alle Kapitel sind mit Bildmaterial angereichert, anschaulich dargestellt und Schritt für Schritt erläutert. Es wird für das nächste Jahr angestrebt, dieses Angebot auszubauen und regelmäßig auf den neusten Stand der technischen Entwicklung zu halten.

1.14 Informationsfreiheitsgesetz

Die Bürgerschaftsfraktion Bündnis 90/Die Grünen hat im Sommer 2001 den Entwurf eines Bremer Informationsfreiheitsgesetzes (Bürgerschafts-Drs. 15/768 vom 04. Juli 2001) vorgelegt. Die Bremische Bürgerschaft (Landtag) hat den Gesetzentwurf an den Datenschutzausschuss und an den Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten überwiesen. Diese Ausschüsse haben am 03. Mai 2002 eine gemeinsame öffentliche Anhörung zu diesem Thema durchgeführt und Sachverständige angehört. Darüber ist ein Protokoll erstellt worden (Ausschussprotokolle A/IuKM und A/DA vom 03.05.02).

Auch ich habe als Sachverständiger an der Anhörung teilgenommen und habe in meinem Referat insbesondere dargelegt, dass sich ein Recht auf freien Informationszugang gegenüber öffentlichen Stellen mit den Prinzipien des Datenschutzes in Einklang bringen lässt.

Bei Schaffung eines Bremischen Informationsfreiheitsgesetzes ist insbesondere zu berücksichtigen, dass das Datenschutzniveau bei der Verarbeitung personenbezogener Daten mit Blick auf verschiedene allgemeine Datenschutzregelungen im BremDSG nicht abgesenkt werden darf. Eine vorherige Prüfung der Auswirkungen in allen Zweigen der Verwaltung (z. B. Privileg der Strafverfolgungsbehörden; Prüfung, welcher Anwendungsraum für den Verfassungsschutz bleibt) ist vorher anzustreben. Das Verhältnis zu verschiedenen Geheimhaltungsvorschriften ist genau zu klären.

Des Weiteren habe ich vorgeschlagen, den Umfang der Aufgaben des Informationsfreiheitsbeauftragten klar zu definieren. Die Sicherung der unabhängigen Stellung auch für diese Funktion ist erforderlich. Im Zeitalter elektronischer Medien ist eine Festlegung der notwendigen Dokumentation von Verwaltungshandeln vorzunehmen, sonst besteht die Gefahr, dass das Recht auf freien Informationszugang leer laufen könnte, weil z. B. elektronisch geführte Entscheidungsprozesse der Akte nicht mehr zu entnehmen sind.

Die institutionelle Kontrolle der Verwaltung durch Parlament, Deputation, Beiräte, Datenschutzbeauftragte und Gerichte, in vielen Fällen auch durch die sog. "Vierte Gewalt", die Medien, hat sich bewährt. Das Informationsfreiheitsrecht wird daher mehr der Informationsbefriedigung, Transparenz und Nachvollziehbarkeit öffentlichen Handelns dienen als der Verwaltungskontrolle.

Schließlich halte ich den Weg, die elektronisch gespeicherten Informationen der Verwaltung an einem allgemein zugänglichem Ort der Öffentlichkeit zur Verfügung zu stellen, für richtungsweisend, nicht nur unter dem Gesichtspunkt des „papierlosen Büros“, sondern auch, weil den Bürgern elektronische Recherchemöglichkeiten bei der Suche zur Verfügung gestellt werden könnten und darüber hinaus die Verwaltung bei einer Einsichtnahme nicht belastet würde.

Dabei ist anzumerken, dass der Gedanke, Regelungen zum Informationszugang zu schaffen, schon älter ist. Eine Regelung über das Prinzip des freien Zugangs zu Informationen wurde bereits im Jahr 1766 in Schweden und im Jahre 1966 durch den "Freedom of Information Act" in den USA geschaffen. In Deutschland wurde im Jahre 1994 das Umweltinformationsgesetz (UIG) vom 08. Juli 1994, BGBl. S. 1490 (Neubekanntmachung des UIG vom 03. August 2001, BGBl. S. 2218) geschaffen. Damit erfolgte die verspätete Umsetzung der EU-Richtlinie über den freien Zugang zu Informationen über die Umwelt (EU-Richtlinie vom 07. Juni 1990, 90/313/EWG). Erstmalig wurde damit ein freier Zugang für jedermann zu bei Behörden vorhandenen Informationen - allerdings nur über die Umwelt - rechtlich verankert.

Allgemeine Informationszugangsgesetze gibt es bereits in den Ländern Brandenburg, Berlin, Nordrhein-Westfalen und Schleswig-Holstein. Im Bund hat das Bundesministerium des Innern in der letzten Legislaturperiode des Deutschen Bundestages den Referentenentwurf eines Informationsfreiheitsgesetzes mit Stand vom 20. Dezember 2000 vorgelegt. Der Entwurf ist jedoch nicht in das Gesetzgebungsverfahren eingebracht worden. Die Koalitionsvereinbarung 2002 bis 2006 der neuen Rot/Grünen Bundesregierung sieht vor, erneut ein Informationsfreiheitsgesetz für die Bundesbehörden einzubringen, das dem Grundsatz des freien Zugangs zu dadurch öffentliche Stellen gespeicherten Daten und Akten Geltung verschafft.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Entschließung vom 08./09. März 2001 betont, dass das Recht auf informationelle Selbstbestimmung des Einzelnen dem freien Zugang zu behördeninternen Informationen nicht entgegensteht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben.

Der Datenschutzausschuss hat aufgrund der Anhörung nachfolgende Anforderungen an ein Bremisches Informationsfreiheitsgesetz unter datenschutzrechtlichen Gesichtspunkten formuliert:

- Beibehaltung des Datenschutzniveaus bei der Verarbeitung personenbezogener Daten.
- Prüfung der Anwendbarkeit und Auswirkungen eines Informationszugangsrechts auf alle Zweige der Verwaltung. Das Verhältnis zu verschiedenen Geheimhaltungsvorschriften ist dabei zu klären.
- Prüfung, ob ein Verweis auf eine entsprechende Anwendung der Vorschriften des Bremischen Datenschutzgesetzes über die Aufgaben und Befugnisse des Landesbeauftragten ausreichend ist, um die Stellung eines Informationsbeauftragten zu beschreiben, oder ob eine weitergehende Präzisierung erforderlich ist. Die unabhängige Stellung ist dabei auch auf die Funktion des Beauftragten für Informationsfreiheit zu übertragen.
- Beseitigung möglicher Wertungswidersprüche zu anderen Informationszugangsregelungen. Die schon jetzt durch gesetzliche Regelungen festgelegten Informationsrechte der Bürger/-innen dürfen nicht eingeschränkt werden.
- Prüfung, ob der Abwägungsprozess zwischen Informationszugang und dem Schutz personenbezogener Daten durch weitere und klarere Kriterien wie beispielsweise im Berliner Informationsfreiheitsgesetz besser strukturiert werden könnte.
- Festlegung klarer Regeln für die Dokumentation des Verwaltungshandelns auch bei der Verwendung elektronischer Medien.
- Abgleich mit den Zielbestimmungen der EU zum Informationsrecht.

Nach der Anhörung hat der Ausschuss für Informations- und Kommunikationstechnologie und Medienangelegenheiten mehrheitlich der Bürgerschaft vorgeschlagen, den Gesetzesantrag der Fraktion Bündnis 90/Grüne abzulehnen. Zwischen beiden Koalitionsfraktionen SPD und CDU bestehe keine Einigkeit über ein bremisches Informationsfreiheitsgesetz. Während die Vertreter der SPD-Fraktion sich dafür aussprächen, ein derartiges Gesetz zu beschließen, stünden die Vertreter der CDU-Fraktion auf dem Standpunkt, zunächst die sich aufgrund der Erfahrungen in den anderen Ländern abzeichnenden Novellierungen der jeweiligen Informationsfreiheitsgesetze abzuwarten und in die Überlegungen auch die finanziellen Auswirkungen eines solchen Gesetzes einzubeziehen. Aufgrund der Koalitionsabsprache sei daher der Gesetzentwurf abzulehnen (Bürgerschafts-Drs. 15/1251 vom 01. Oktober 2002). Dies ist dann leider auch so geschehen. Es bleibt abzuwarten, ob in der nächsten Legislaturperiode die Thematik erneut auf der Agenda stehen wird.

1.15 Mit den Änderungen im Bremischen Datenschutzgesetz Erreichtes

Nach gründlicher Vorbereitung durch das Justizressort und eingehenden parlamentarischen Beratungen (vgl. Bericht und Antrag des Datenschutzausschusses der Bremischen Bürgerschaft vom

05.12.2002, Drs. 15/1321), trat im Dezember 2002 eine Reihe wesentlicher Änderungen des Bremischen Datenschutzgesetzes in Kraft (BremGBl. vom 20. Dezember 2002, Nr. 67). Mit der Novellierung wurden verschiedene Ziele erreicht:

- Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 (ABl. EG Nr. L 281/31) wurde umgesetzt.
- Eine Anpassung an die neuen Entwicklungen der Informations- und Kommunikationstechnologien in den letzten Jahren wurde durch Regelungen zu mobilen Datenverarbeitungsmedien (Chipkarten) und zur Videoüberwachung sichergestellt.
- Die Rechte des Datenschutzausschusses und des Landesbeauftragten für den Datenschutz wurden gestärkt.
- Die Rechte der Bürgerinnen und Bürger zur Durchsetzung ihres informationellen Selbstbestimmungsrechts wurden erheblich verbessert.

Damit hat Bremen einmal mehr besondere Datenschutzakzente gesetzt. Die mit den gesetzlichen Änderungen für die Bürger unmittelbar erreichten Verbesserungen stellen sich im Einzelnen wie folgt dar:

Einwilligung: Soweit die Betroffenen in die Verarbeitung ihrer Daten einwilligen sollen, werden höhere Anforderungen an die wirksame Einwilligung des Betroffenen gestellt. Danach ist die Einwilligung nur noch dann wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Außerdem kann die Einwilligung auch in elektronischer Form mit einer digitalen Signatur nach Maßgabe des Signaturgesetzes erteilt werden (§ 3 Abs. 4 BremDSG).

Widerspruchsrecht: Neuerdings können Betroffene bei Vorliegen schutzwürdiger Interessen wegen ihrer besonderen Situation gegen die Datenverarbeitung widersprechen. Es bedarf dann einer Prüfung, ob das dargelegte schutzwürdige Interesse des Betroffenen das Interesse der verantwortlichen Stelle an dieser Verarbeitung überwiegt (§ 22 a BremDSG).

Schadensersatz: Der Anspruch auf Schadensersatz gegenüber verantwortlichen Stellen wird bei unzulässiger Datenverarbeitung auf nicht automatisierte Verarbeitungen erweitert (§ 23 BremDSG).

Unterrichtung beim Einsatz von Chipkarten: Neu ist auch eine Regelung über mobile Datenverarbeitungsmedien (z. B. Chipkarten). Ihr Einsatz ist nur zulässig mit Einwilligung des Betroffenen oder aufgrund einer Rechtsvorschrift. Außerdem sind die verantwortlichen Stellen verpflichtet, die Betroffenen über die Funktionsweise dieser Datenverarbeitungsmedien zu unterrichten (§ 20 a BremDSG).

Einsicht in Verfahrensbeschreibungen durch jedermann: Jedermann kann die von den verantwortlichen Stellen festzulegenden Beschreibungen für automatisierte Verfahren, mit denen personenbezogene Daten verarbeitet werden, dort einsehen (§ 8 Abs. 3 BremDSG).

Verarbeitung besonderer Arten von Daten: Die Verarbeitung besonderer Arten von Daten (Angaben über die rassische und ethnische Herkunft, politische Meinung, religiöse oder philosophische

Überzeugung, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben) unterliegt einer engeren Zweckbindung (§ 3 Abs. 2 BremDSG).

Automatisierte Einzelentscheidung: Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, dürfen grundsätzlich nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden, die der Bewertung einzelner Persönlichkeitsmerkmale dienen (§ 5 BremDSG). Außerdem ist der Auskunftsanspruch des Betroffenen auf den logischen Aufbau einer derartigen automatisierten Verarbeitung der ihn betreffenden Daten erweitert worden (§ 21 Abs. 1 Nr. 3 BremDSG).

Aus der Vielzahl weiterer Änderungen und Verbesserungen seien noch folgende hervorgehoben: Das neue Datenschutzgesetz enthält eine Regelung über die Videoüberwachung öffentlich zugänglicher Bereiche. Videoüberwachung ist danach nur dann zulässig, wenn sie zum Schutz von Personen oder des Eigentums oder Besitzes oder zur Zugangskontrolle erforderlich ist und schutzwürdige Belange der Betroffenen nicht überwiegen. Sie muss durch den Leiter der verantwortlichen Stelle angeordnet werden. Hierbei sind Zweck, räumliche Ausdehnung und die Dauer der Videoüberwachung zu dokumentieren (§ 20 b BremDSG).

Um eine wirksame Einhaltung des neuen Gesetzes zum Schutze der Bürgerinnen und Bürger in den Behörden sicherzustellen, ist vorgeschrieben, dass jede Dienststelle einen behördlichen Beauftragten für den Datenschutz zu bestellen hat, dem konkret beschriebene gesetzliche Aufgaben und Befugnisse obliegen. Kleinere Dienststellen können einen gemeinsamen behördlichen Datenschutzbeauftragten bestellen (§ 7 a BremDSG).

Eine wichtige Neuregelung zum Schutz der Persönlichkeitsrechte der Betroffenen ist das Datenschutzaudit. Danach soll die bremische Verwaltung Verfahren und technische Einrichtungen vorrangig einsetzen, deren Vereinbarung mit den Vorschriften über den Datenschutz und die Datensicherheit in einem förmlichen Verfahren festgestellt wurde (§ 7 b BremDSG).

Den technischen Neuerungen wird dadurch Rechnung getragen, dass die Regelungen zu den technischen und organisatorischen Maßnahmen um die Grundsätze der Datenvermeidung und Vorabkontrolle erweitert worden sind. Datenvermeidung bedeutet, dass die Gestaltung und Auswahl von Datenverarbeitungssystemen sich an dem Ziel auszurichten haben, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Vorabkontrolle bedeutet, dass die verantwortlichen Stellen vor der Entscheidung über die Einführung oder wesentliche Änderung eines automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, zu untersuchen haben, ob und in welchem Umfang mit der Nutzung dieses Verfahrens Gefahren für die Rechte der Betroffenen verbunden sind (§ 7 BremDSG).

Des Weiteren sind die Kontrollmöglichkeiten des Landesbeauftragten für den Datenschutz verbessert worden. So kann ich von den verantwortlichen Stellen nach festgelegten Vorgaben strukturierte Auswertungen aus automatisierten Informationssystemen verlangen, soweit dies die bei den jeweiligen Stellen bestehenden technischen Möglichkeiten zulassen (§ 27 Abs. 2 Nr. 2 BremDSG).

Schließlich bedeutet die Novellierung auch eine Stärkung der Rechte des Parlaments. Danach soll der Senat spätestens sechs Monate nach Ausscheiden des Landesbeauftragten für den Datenschutz

einen Nachfolger vorschlagen. Die Auswahl erfolgt im Benehmen mit dem Datenschutzausschuss der Bremischen Bürgerschaft (§ 24 Abs. 1 BremDSG). Außerdem legt das Gesetz jetzt nicht mehr nur den Zeitpunkt fest, zu dem der Landesbeauftragte für den Datenschutz seinen Jahresbericht vorzulegen hat, sondern jetzt ist auch der Senat gebunden, spätestens fünf Monate nach der Abgabefrist des Jahresberichts der Bremischen Bürgerschaft dazu die Stellungnahme vorzulegen (§ 33 Abs. 2 BremDSG).

Das Bremische Datenschutzgesetz (BremDSG) ist am 18. Dezember 2002 in Kraft getreten. Eine Neuveröffentlichung soll in Kürze erfolgen.

2. Telekommunikation, Teledienste und Medien

2.1 Stadtinformationssystem Bremen (www.bremen.de)

Im letzten Jahr wurde das Stadtinformationssystem bremen.de einer datenschutzrechtlichen Prüfung unterzogen (vgl. 24. JB, Ziff. 2.1), wobei sich ähnliche Probleme zeigten, die bereits bei der Prüfung des Portals bremerhaven.de angetroffen wurden (vgl. 23. JB, Ziff. 2.2.2).

Zum einen existierte keine Privacy Policy, im Rahmen derer der Benutzer darauf hingewiesen wird, in welcher Weise personenbezogene Daten unter bremen.de gespeichert werden. Zum anderen wurden auf dem Webserver sämtliche Zugriffe IP-Nummern-bezogen protokolliert und zu statistischen Zwecken einen Monat aufbewahrt, bevor sie gelöscht wurden.

Die Umsetzung der geforderten Maßnahmen verzögerte sich, da seitens des Senators für Finanzen (SfF), Bestrebungen bestanden, die Betreibung des Stadtportals in die Privatwirtschaft abzugeben. Wie der Presse zu entnehmen war, scheiterte dieses Vorhaben zunächst; das Vergabeverfahren konnte nicht erfolgreich abgeschlossen werden. Daher betreibt die Freie Hansestadt Bremen das Stadtinformationssystem bis auf weiteres selbst, um die erforderlichen technischen Kompatibilitäten und Integrationen zu sichern.

Weiterhin soll eine in 2003 neu zu gründende 100%-ige stadtbremische Gesellschaft (Public Private Partnership) neben redaktionellen Serviceleistungen die kommerzielle Verwertung des Stadtinformationssystems erbringen.

Aufgrund dieses Umgestaltungsprozesses war die Verantwortlichkeit für die geforderten Änderungen nicht geklärt, die nur zum Teil realisiert wurden. Es wurde erreicht, dass in den Bereich einer integrierten E-Mail-Abo-Funktion von Stellenausschreibungen und Pressemitteilungen eine Datenschutzerklärung aufgenommen wurde, im Rahmen derer die Abonnenten über die Speicherung ihrer personenbezogenen Daten informiert werden. Eine generelle Datenschutzerklärung für das gesamte Angebot existiert weiterhin nicht. Es wurde jedoch seitens des Senator für Finanzen zugesichert, dass ein Passus über Speicherung und Aufbewahrung der IP-Adressen umgehend in die Bedingungen (z. B. ins Impressum) aufgenommen wird.

Weiterhin wurde für das Jahr 2003 zugesagt, die unzulässige Speicherung und Aufbewahrung der vollständigen IP-Adressen auf dem Webserver zu unterlassen und statt dessen eine Aggregation der IP-Adressen in den Protokolldatensätzen zu realisieren. Die diesbezügliche Entwicklung werde ich weiterhin begleiten.

2.2 MEDIA@Komm

2.2.1 eGovernment - Fortsetzung von MEDIA@Komm

Auch im Berichtsjahr sind eine Reihe von eGovernment-Anwendungen (elektronische Verwaltung) von der bremischen Verwaltung in Zusammenarbeit mit der „bremen online services GmbH & Co. KG“ (bos) konzipiert und weiterentwickelt worden. Diese Anwendungen, etwa 100 an der Zahl, betreffen eine Vielzahl von Lebenslagen und sind unterschiedlich stark differenziert.

So können sich Bürger übers Internet z. B. Formulare für die Einzugsermächtigung beim Finanzamt, die steuerliche Anmeldung eines Betriebes, die Hundesteuererklärung bis zur Zweitwohnungssteueranmeldung herunterladen. Weiter ist es möglich, Wunschkennzeichen bei der Kfz-Zulassungsstelle online zu bestellen, Urkunden beim Standesamt anzufordern oder Sprechstunden zu buchen.

Aus datenschutzrechtlicher Sicht sind im Berichtsjahr keine wesentlichen Problemfelder zu benennen. Das MEDIA@Komm-Projekt wird bundesweit beachtet, wesentliche Grundlagen des in einer Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeiteten Handlungsempfehlungen „datenschutzgerechtes eGovernment“ sind durch das Projekt in Bremen beeinflusst (vgl. Ziff. 2.2.2 dieses Berichts). Allerdings wurden einige Anwendungen neu modelliert und, wie unter Ziffer 2.2.3 berichtet, wurden die einzelnen Anwendungen in einem Masterplan neu ausgerichtet.

2.2.2 eGovernment-Handbuch

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten, an der ich mich maßgeblich beteiligt habe, hat kurz vor Ende des Jahres 2002 ihre Arbeiten an einer Handlungsempfehlung „datenschutzgerechtes eGovernment“ abgeschlossen und in einer Broschüre herausgegeben. Diese Handlungsempfehlungen sind auch im Internet unter www.datenschutz.de abrufbar.

Der Auftrag der Konferenz bestand darin, weitgehend einheitliche Kriterien für die im Internet zunehmenden eGovernment-Anwendungen zu entwickeln, die einen weitgehenden Schutz der personenbezogenen Daten gewährleisten. Ziel war es ferner, diese Handlungsempfehlungen schnell zu erarbeiten, damit Entwickler von eGovernment-Anwendungen diese in ihre Konzeption mit einbeziehen können.

Ich hoffe, dass von den Anregungen reichlich Gebrauch gemacht wird und ein Wettbewerb - im Sinne des Datenschutzes - effektivster eGoverment-Anwendungen entsteht. Es ist unter den Verfassern der Broschüre verabredet, sie fortzuschreiben.

2.2.3 eGovernment-Masterplan

Im Oktober 2002 überreichte der Senator für Finanzen - zuständig für die TuI-Entwicklung in der Freien Hansestadt Bremen - einen Masterplan eGovernment. Aufgabe dieses Planes ist es,

festzustellen, wie sich das eGovernment in Bremen entwickelt hat und wie es in die eGovernment-Strategie Bremens einzuordnen ist.

Ziel der eGovernment-Leistungen soll u. a. sein, die Verwaltungsreformbemühungen zu unterstützen und die Verwaltungsleistungen effektiver zu gestalten. Sie soll die Kundenfreundlichkeit verbessern und gleichzeitig aber auch die öffentlichen Haushalte entlasten.

Bei der Steigerung der Effektivität sollen die nachfolgenden Kriterien als Indikatoren angeführt werden:

- Prozessbeschleunigung
- Entlastung von Routineaufgaben
- Datenqualität
- Direkte Kosteneinsparungen
- Transparenz des Verfahrens
- Rechtssicherheit
- Controlling.

Für den LfD kommt es bei all diesen Betrachtungen darauf an, dass das informationelle Selbstbestimmungsrecht der Bürger so wenig wie möglich eingeschränkt wird, der Bürger weiß, wie er seine Verwaltungsleistung abrufen kann und welche Daten dabei über ihn wo gespeichert werden. Hierbei ist insbesondere in den Blick zu nehmen, dass nicht die Verwaltung entscheidet, was für den Bürger richtig ist, sondern der Bürger darüber entscheidet, auf welchem Wege er seine Dienstleistung abfordert.

Zu beachten ist auch die neue Regelung in § 7 des Bremischen Datenschutzgesetzes (BremDSG). Den Prinzipien der Datensparsamkeit und -vermeidung ist Rechnung zu tragen und Daten sind so früh wie möglich zu anonymisieren bzw. zu pseudonymisieren.

2.3 Zentraler Verzeichnisdienst für die bremische Verwaltung

Das Betriebssystem Windows 2000 wurde von Microsoft als Nachfolger von Windows NT für den Einsatz auf Einzel-Rechnern und für Unternehmenslösungen entwickelt.

Ein wesentlicher Bestandteil von Windows 2000 ist der zentrale Verzeichnisdienst Active Directory, der die Integration unterschiedlichster Verzeichnisse ermöglicht, in der alle relevanten Informationen über das Netzwerk, seine Benutzer bis hin zu Telefon- und E-Mail-Adressverzeichnissen hinterlegt sind, die bislang an verschiedenen Stellen mit gleichlautendem Inhalt gepflegt werden mussten.

Unter dem Aspekt von Datenschutz und Datensicherheit bietet der Einsatz von Windows 2000 und der Aufbau eines Active Directories für die bremische Verwaltung sowohl Vor- als auch Nachteile. Vorteil ist, dass dieses Betriebssystem eine Reihe zusätzlicher Funktionen enthält, die zur Sicherheit des Bremischen Verwaltungsnetzes (BVN) beitragen können. Diese sind u. a. folgende:

- Das Dateisystem EFS (Encryption File System) erlaubt den Benutzern, Daten oder ganze Verzeichnisse auf lokalen Datenträgern online zu verschlüsseln. Dies ist beispielsweise bei Verlust von Wechselplatten oder bei Diebstahl des Gerätes ein entscheidender Vorteil gegenüber Windows NT.

- Die Zertifikatsdienste von Windows 2000 ermöglichen den Aufbau einer Schlüssel-Infrastruktur (Public Key Infrastructure - PKI), die dazu genutzt werden kann, bei Bedarf einen großen Kreis von Benutzern zu authentifizieren und diesen Benutzern verschlüsselte und signierte Daten zuzuschicken (vgl. Ziff. 2.4 dieses Berichts).
- Um die Integrität, Authentifizierung und Vertraulichkeit von Netzwerkdaten zu gewährleisten, unterstützt Windows 2000 das Internet Protocol Security (IPSec). IPSec gestattet die Verschlüsselung (Ende-zu-Ende-Verschlüsselung) der Datenübertragung auf der Netzwerkschicht.
- Windows 2000 ermöglicht nicht nur die Authentifzierung der Benutzer gegenüber einem Domänen Controller, sondern unterstützt auch umgekehrt Identitätsnachweise bestimmter Netzwerkdienste gegenüber dem Benutzer. Für beide Arten der Authentifzierung verwendet Windows 2000 das Sicherheitsprotokoll Kerberos, Version 5.

Auf der anderen Seite sind mit dem Einsatz eines Active Directory auch ganz konkrete sicherheitstechnische Probleme verbunden, da sich der Geltungsbereich der Domänen auf wesentlich größere Organisationsbereiche als bisher erstreckt. Während in der bremischen Verwaltung bislang ca. 200 Domänen eingerichtet waren, beschränkt sich druch den Einsatz des Active Directory die Anzahl der Domänen auf einige wenige. Diese sind im wesentlichen die sog. Root-Domäne „land.bremen.de“ und die sog. Second-level-Domäne „verwaltung.land.bremen.de“. Anstelle der ehemaligen NT-Domänen wurden und werden sog. Organisationseinheiten (OU) eingerichtet, zwischen denen - im Gegensatz zu einer NT-Lösung mit mehreren Domänen - permanente Vertrauensstellungen mit OU-übergreifendem Zugriff existieren. Die bisherigen NT-Barrieren auf Domänenebene müssen statt dessen durch eine strikte Vergabe der Zugriffsrechte auf OU-Ebene ersetzt werden. Dieses kann mittels sog. Gruppenrichtlinien (Group Policies) realisiert werden und kann bei nicht ausreichender Konfiguration in großen Verwaltungen ein erhebliches administratives Risiko darstellen. Ein weiterer Nachteil von Active Directories besteht darin, dass Passwortrichtlinien per Voreinstellung verzeichnisübergreifend gelten. Darüber hinaus richtet Windows 2000 standardmäßig zwischen allen Domänen transitive (gegenseitige) Vertrauensstellungen ein. Traut also Domäne A der Domäne B und Domäne B der Domäne C, dann traut auch Domäne A der Domäne C.

Für das Administrieren (Vergabe von Rechten, Einrichten von Benutzerkonten) der Domänen gibt es, wie unter Windows NT, die Gruppe der Administratoren. Durch die Vertrauensstellungen der Domänen untereinander ergibt es sich aber nicht automatisch, dass ein Administrator einer Domäne Rechte auf allen anderen Domänen haben soll. Eine Ausnahme bilden hier die Administratoren der Stamm-Domäne (Root-Ebene), sie sind einer speziellen Gruppe, den Organisations-Administratoren angegliedert. Die Organisations-Administratoren bekommen automatisch die Berechtigung, sich in allen Domänen der Gesamtstruktur mit unbeschränktem Zugriff anzumelden.

Zum jetzigen Zeitpunkt ist die Installation des Active Directory Service (ADS) für die bremische Verwaltung abgeschlossen. Der Datenumfang im ADS entspricht dem bisherigen globalen Adressbuch von Exchange (E-Mail-System) und einigen für das Projekt Docman (Dokumentenmanagement-System der bremischen Verwaltung) nötigen Erweiterungen wie Organisationskennzeichen (OKZ) und Raumnummer. Im Rahmen des Pilotbetriebes nehmen derzeit

alle senatorischen Behörden mit einigen Teilnehmern über das Projekt Docman teil. Aufgrund von Problemen im Bereich der bereits angesprochenen Realisierung einer dezentralen Administration, konnte das Pilotprojekt 2002 nicht abgeschlossen werden. Ziel ist dabei ebenso wie für zukünftige Erweiterungen, die Gestaltungsmöglichkeiten der bisherigen NT-Domänen-Administratoren beizubehalten, ohne gleichzeitig den Aufwand für den Betrieb einer eigenen Domäne zu haben. Dabei ist geplant, dass die Pilotteilnehmer auf Wunsch für ihre OU alle Rechte als Administrator bei der BreKom beantragen können. Insbesondere können sie auch eigene Sicherheitsrichtlinien, sog. GPO's (Group Policy Objects) entwickeln, die die Standardvorgaben für ihre eigene OU verschärfen, aber nicht abschwächen können. Dies betrifft z. B. Passwortlänge und -komplexität.

Die Fortführung des Pilotprojektes sowie die fortschreitende Entwicklung der Produktiv-Einführung des ADS soll kontinuierlich weiter verfolgt werden, wobei die oben aufgeführten kritischen Aspekte dieser neuen Technologie einer genaueren Prüfung unterzogen werden sollten. Dabei werden, wie bisher, die anstehenden technischen Umstellungen von meiner Dienststelle im Rahmen der entsprechenden Gremien kritisch verfolgt und unter Aspekten von Datenschutz und Datensicherheit beratend begleitet werden.

2.4 Aufbau einer PKI-Struktur in der bremischen Verwaltung

Im Rahmen einer Neuorganisation der Verzeichnisstruktur der bremischen Verwaltung ist der Aufbau eines Active Directory Service (ADS) als Verzeichnisdienst auf der Basis von Windows 2000 in Angriff genommen worden. Ein entsprechendes Pilotprojekt wird voraussichtlich im nächsten Jahr beendet werden (vgl. Ziff. 2.3 dieses Berichts). Über den Verzeichnisdienst soll unter anderem eine Public Key Infrastruktur (PKI) realisiert werden, die zum einen zur Verschlüsselung von Informationen und zum anderen zum gleichzeitigen elektronischen Signieren genutzt werden kann. Dabei kommt vor allem der Verschlüsselung und der Signatur des E-Mail-Verkehrs eine große Bedeutung zu.

Elektronische Post wird auf dem Weg durch das Internet von zahlreichen Rechnern weitergeleitet, bis sie bei ihrem eigentlichen Empfänger ankommt. Jeder, der Zugang zu diesen Netzwerkrechnern hat, kann die Nachricht mitlesen, ohne dass Absender und Empfänger dies bemerken. Der Absender kennt meistens noch nicht einmal den Weg, den die Nachricht zum Empfänger überhaupt nimmt. Es kann davon ausgegangen werden, dass ein Großteil des Internet-Datenverkehrs automatisiert überwacht und nach Schlüsselbegriffen ausgewertet wird. Um zu verhindern, dass sensible Informationen beim Transport über das Internet von Außenstehenden mitgelesen werden, sollten die Nachrichten beim Absender vorab verschlüsselt und beim Empfänger wieder entschlüsselt werden.

Bisher wurde zu diesem Zweck innerhalb der bremischen Verwaltung die frei verfügbare Verschlüsselungssoftware PGP (Pretty Good Privacy) genutzt. Eine Integration in ein bestehendes System dürfte in diesem Zusammenhang eine Vereinfachung und damit Erhöhung der Akzeptanz darstellen und ist daher unter Datenschutz-Aspekten grundsätzlich zu begrüßen. Die neue Technologie soll über den Einsatz von sog. Smartcards realisiert werden.

Ein durch die datenschutz nord GmbH im Auftrag des Senators für Finanzen erstelltes Grobkonzept liegt bereits vor und beschreibt den äußeren Rahmen der PKI-Struktur für die bremische Verwaltung,

sowie technische und rechtliche Anforderungen an den Betreiber der PKI. Es wird noch eine weitere Ausarbeitung im Rahmen eines Feinkonzeptes erfolgen.

Auch bei dieser an sich aus Datenschutzsicht wünschenswerten Weiterentwicklung sind verschiedene kritische Aspekte zu beachten. Zu nennen wären hier beispielsweise die Gebäude- und Raumsicherheit, ein detailliertes Betreiberkonzept für den Betrieb der sog. Certificate Authority (CA) und Kontrollmaßnahmen für die Administration, etc..

Die Weiterentwicklung dieses Projektes ist direkt von der Einführung des ADS abhängig. Da die Pilotphase des ADS-Projektes in der bremischen Verwaltung (vgl. Ziff. 2.3 dieses Berichts) im Jahr 2002 nicht abgeschlossen werden konnte, wurde dieses Projekt zunächst zurückgestellt und wird im nächsten Jahr erneut in Angriff genommen.

Dabei wird, analog zu der Einführung des ADS für die bremische Verwaltung die Weiterentwicklung dieser neuen Technologie von meiner Dienststelle in den entsprechenden Gremien begleitet und deren sicherheitskritische Aspekte in beratenden Stellungnahmen und Gesprächen thematisiert werden.

2.5 Orientierungshilfe Windows XP

Im Rahmen der Zusammenarbeit der Datenschutzbeauftragten der Länder arbeite ich im Arbeitskreis Technik (AK Technik), der sich mit allen Datenschutzfragen bei der Nutzung von Technologien beschäftigt. Unter anderem gehen aus diesem Arbeitskreis immer wieder verschiedenste Orientierungshilfen hervor. Die neueste Orientierungshilfe, die sich momentan in der Endabstimmung befindet und die im Frühjahr 2003 veröffentlicht werden wird, befasst sich mit dem Thema „Windows XP“.

Die Orientierungshilfe bezieht sich hauptsächlich auf die „Professional“-Version von Windows XP und richtet sich an versierte Anwender (wie z. B. Administratoren), die Erfahrungen mit den Windows-Betriebssystemen haben und auch Schwachstellen älterer Windows-Versionen kennen. Im Mittelpunkt der Orientierungshilfe stehen dabei datenschutzrechtlich relevante Gesichtspunkte. Wesentliche sicherheitsrelevante Aspekte des Betriebssystems werden beleuchtet, um das Betriebssystem sinnvoll in diesen Punkten konfigurieren zu können. Es wird zusätzlich über bestehende Sicherheitsmängel berichtet und Hinweise darauf gegeben, wie diese Mängel beseitigt bzw. eingeschränkt werden können.

Insbesondere wird besprochen, dass in Windows XP zahlreiche Komponenten eingebaut sind, die über das Internet mit Microsoft Kontakt aufnehmen können. Dies ist teilweise nicht transparent für den Anwender. So wird empfohlen, Module abzuschalten, die automatisch Kontakt zu Microsoft aufnehmen und z. B. automatische Aktualisierungen des Betriebssystems vornehmen.

Ein Beispiel, bei dem Daten zu Microsoft übertragen werden, die Personenbezug aufweisen können, ist laut Orientierungshilfe der Windows XP Media Player. Der Media Player übermittelt an Microsoft, welche Musikstücke und Videos der Nutzer abspielt. Zusätzlich wird auch die eindeutige Identifikationsnummer des Media Player selbst mit übermittelt. Kann diese Identifikationsnummer (ID) mit personenbezogenen Daten verknüpft werden (z. B. bei der Anmeldung für den Microsoft Media

Newsletter, bei der Microsoft neben der Media-Player-ID auch Name und E-Mailadresse des Abonnenten erhält), kann Microsoft relativ einfach Profile über Hör- und Sehgewohnheiten der Anwender zusammenstellen und diese Informationen könnten dann vermarktet werden (was laut Jonathan Usher, Microsoft Sprecher, derzeit nicht geplant ist, für die Zukunft aber nicht auszuschließen sei). Diese Verfahrensweise ist datenschutzrechtlich sehr bedenklich. Die Orientierungshilfe empfiehlt in diesem Fall, auf einen anderen Player auszuweichen oder, sollte dies nicht möglich oder gewollt sein, das Abschalten des Internetzugriffsrechts des Windows Media Player.

Weitere Hinweise zur „Selbstverteidigung im Internet“ sind auf meinen Internet-Seiten unter www.datenschutz.bremen.de/tipps/verteidigung/default.htm zu finden.

2.6 Content-Anbieter im Internet

Im letzten Jahr wurden neben dem Stadtinformationssystem bremen.de (vgl. Ziff. 2.1 dieses Berichts) eine repräsentative Anzahl weiterer Content-Anbieter (u. a. Banken, Verlage, Online-Shops; vgl. 24. JB, Ziff. 2.2) einer Online-Prüfung unterzogen. Dabei kamen die folgenden Prüfkriterien, die sich aus dem Bundesdatenschutzgesetz (BDSG) und dem Teledienstedatenschutz-gesetz (TDDSG) herleiten, zum Einsatz:

- Setzen von Cookies und Unterrichtung darüber
- Kennzeichnung von Pflichtfeldern
- Gesetzeskonforme Anbieterkennzeichnung
- Verwendete Zahlungsverfahren und derer Sicherheit
- SSL-Verschlüsselung
- Vorhandensein einer Datenschutzerklärung (Privacy Policy)

Unter Bezugnahme auf diese Prüfkriterien wurden die Angebote der 24 Contentanbieter zwischenzeitlich zum Teil erheblich verbessert. Dabei ist festzustellen, dass die gesetzlichen Vorgaben, vor allem im Hinblick auf die Anbieterkennzeichnung, nun von nahezu allen Anbietern erfüllt werden.

Weiterhin stellt sich nach nunmehr einem Jahr die folgende Situation im Hinblick auf die Prüfkriterien dar:

Cookies: Von den fünf Anbietern, die permanente Cookies setzten, verzichtete 1 Anbieter im Berichtszeitraum auf das Setzen von Cookies. 3 der 5 Anbieter setzen Cookies in Zusammenhang mit der Nutzung von Online-Banking, wobei der Bürger im Rahmen einer Privacy Policy über das Setzen der Cookies noch zu informieren ist. Ein Contentanbieter setzt Cookies, ohne dass das Internetangebot dieses erforderlich machen würde. Ein weiterer Anbieter integrierte erst im Berichtszeitraum das Setzen von Cookies in sein Internetangebot.

Von den zwei Content-Anbietern, die sich im Berichtszeitraum temporärer Session-Cookies bedient haben, verzichtete einer auf das Setzen derselben. Der andere Anbieter behielt diesen Mechanismus bei, ohne in einer Privacy Policy über das Setzen von Cookies zu informieren. Bei nicht permanenten

Cookies ist diese Praxis allerdings als weniger problematisch anzusehen als bei permanenten, da keine Daten dauerhaft gespeichert und übermittelt werden.

Pflichtfelder: Bei der Erhebung unnötiger Daten und bei der Kennzeichnung von dementsprechenden Pflichtfeldern hat sich die Praxis der geprüften Contentanbieter kaum geändert. Die Kennzeichnung der entsprechenden Formularfelder ist vor allem innerhalb der Internetangebote in Teilen des Verlagswesens in Bremen als unzureichend zu erachten. Weiterhin ist bei 5 von 24 Anbietern zwecks Registrierung bzw. Anmeldung als Kunde die Angabe von Telefonnummer und E-Mail-Adresse notwendig. Bei einem Anbieter muss zur Anmeldung das Geburtsdatum eingegeben werden. Ein weiterer Anbieter weist ein Formularfeld Kundeninfo („Wie wurden Sie auf uns aufmerksam“) als Pflichtfeld aus.

Impressum: Existierte noch im letzen Jahr bei 7 Anbietern kein Impressum und wiesen fast alle vorhandenen kleinere oder größere Mängel auf, so kann für den Berichtszeitraum erfreulicherweise festgestellt werden, dass alle Anbieter ein Impressum eingefügt haben und die gefundenen Mängel zum großen Teil beseitigt wurden. Es sind nun überall der Sitz des Unternehmens sowie Verantwortliche genannt. Zum Teil lässt die Benennung des Impressums unter Kontakt, Info o. ä. noch etwas zu wünschen übrig oder die Informationen sind auf verschiedenen Seiten verteilt und so nicht einfach zu finden.

Zahlungsverfahren: An den von den Contentanbietern genutzten Zahlungsverfahren hat sich wenig geändert. Als häufigste Bezahlverfahren sind weiterhin die Zahlung per Bankeinzug oder wahlweise per Rechnung aufgeführt. Zahlungsverfahren wie Ecash, Cyber- oder Telecash wurden von den Anbietern nicht eingeführt.

SSL-Verschlüsselung: Ein Anbieter stellt im Gegensatz zum vergangenen Jahr den Nutzern bei der Übermittlung personenbezogener Daten eine sichere Internetverbindung (SSL) zur Verfügung. 7 Anbieter übertragen weiterhin die Bankverbindungsdaten ihrer Kunden unverschlüsselt über das Internet. Es wird angestrebt, diesen Zustand bald möglichst zu beheben.

Privacy Policy: Im Gegensatz zum letzten Jahr geben nunmehr 4 von 24 Anbietern dem Nutzer Auskunft darüber in welchem Umfang seine Daten (z. B. die IP-Adresse) auf dem Webserver der Anbieter gespeichert werden. Auch hier besteht noch Nachbesserungsbedarf. Die vorhandenen Datenschutzerklärungen sind nicht leicht aufzufinden und nicht vollständig. Als positive Verbesserung ist die Privacy Policy eines Anbieters zu nennen, die sich direkt auf der Startseite befindet und alle geforderten Informationen enthält.

Es wurden im Berichtszeitraum weitreichendere Prüfungen nach § 38 BDSG von 2 Contentanbietern eingeleitet. Dabei handelte es sich um einen Kartenverkaufsservice und ein Versorgungsunternehmen. Die Internetangebote der beiden Anbieter wurden mit dem von der datenschutz nord GmbH vertriebenen Onlinetool „OPTuM“ überprüft und den beiden Unternehmen die automatisch generierten Prüfberichte zugesandt.

Zusammenfassend lässt sich sagen, dass das Angebot des Kartenverkaufsservices vor allem Schwächen im Bereich der Anbieterkennzeichnung, der Privacy Policy und der Datenerhebung im Rahmen von Pflichtfeldern aufwies. Das Angebot des Versorgungsunternehmens verfügte ebenfalls

über keine hinreichende Privacy Policy und die Bankverbindungsdaten der Kunden wurden unverschlüsselt über das Internet übertragen (keine SSL-Verschlüsselung).

Die Stellungnahmen beider Unternehmen zu den Online-Prüfberichten liegen vor. Zusammenfassend ist zu sagen, dass das Versorgungsunternehmen seine Internetpräsenz zum Anfang dieses Jahres verändern, d. h. verbessern wird, womit einige der angesprochenen Fragestellungen geklärt sind. Durch die Umstellung ergaben sich jedoch auch zusätzliche Fragen, bezüglich derer das Versorgungsunternehmen um Beratung durch den Landesbeauftragten für den Datenschutz gebeten hat.

Der Kartenverkaufsservice reagierte ebenfalls mit einer Neugestaltung bzw. Verbesserung seiner Internetpräsenz, welche allerdings erst im Laufe des Februars produktiv gehen wird. Eine erneute bzw. weiterführende Beurteilung ist für diesen Zeitpunkt vorgesehen. Allerdings warf die Stellungnahme des Kartenverkaufsservices zusätzliche Fragen bezüglich des Themenkomplexes „Protokollierung“ auf, denen im Weiteren nachzugehen ist. Festzuhalten bleibt, Stellungnahmen der Unternehmen liegen vor, die noch verbleibenden Fragen werden demnächst in Gesprächen mit den Unternehmen abgearbeitet.

2.7 Aufhebung der Rufnummernunterdrückung

In Call-Centern, die selbst als Telefonvermittlungsstelle an das öffentliche Telefonnetz angebunden sind, ist prinzipiell eine Aufhebung der vom Anrufer gewünschten und an seinem Telefon bzw. seiner Telefonanlage oder durch seinen Telefonanbieter vorgenommenen Konfiguration Unterdrückung der Übermittlung der eigenen Rufnummer möglich (vgl. 24. JB, Ziff. 2.4).

Wie angekündigt, habe ich im Land Bremen verschiedene Call-Center u. a. auch zu diesem Sachverhalt geprüft. Dabei habe ich keine Call-Center festgestellt, bei denen aufgrund der Art ihres Anschlusses eine Aufhebung der Rufnummernunterdrückung möglich ist.

2.8 Arbeitskreis Technik und Arbeitsgemeinschaft Telekommunikation

Im Rahmen meiner Tätigkeit nehme ich an verschiedenen Arbeitsgruppen auf Ebene der Datenschutzbeauftragten des Bundes und der Länder und auf Ebene der Obersten Aufsichtsbehörden teil. Um technische, organisatorische und damit zusammenhängende rechtliche Fragestellungen geht es dabei im Arbeitskreis Technik (AK Technik, „Konferenz der Datenschutzbeauftragten“, vgl. auch Ziff. 2.5 dieses Berichts) und in der Arbeitsgruppe „Telekommunikation, Tele- und Mediendienste“ des „Düsseldorfer Kreises“ (AG Telekommunikation). Während auf der Ebene des Düsseldorfer Kreises im wesentlichen rechtliche Fragestellungen bearbeitet werden, arbeitet der AK Technik im technisch organisatorischen Bereich.

Innerhalb dieser Arbeitsgruppen wurde im Berichtszeitraum wieder eine umfangreiche Anzahl verschiedener Themen behandelt. Die AG Telekommunikation befasste sich u. a. mit Fragen der Zulässigkeit der Protokollierungen von Internet-Aktivitäten (hier insbesondere die Speicherung der IP-Adresse durch Access-Provider), Regelungen für die dienstliche und private Nutzung des Internet am Arbeitsplatz in Privatwirtschaft und öffentlicher Verwaltung, die mögliche Aufhebung von

Rufnummernunterdrückung durch Call-Center (vgl. auch 24. JB, Ziff 2.4 und Ziff. 2.7 dieses Berichts), Fragestellungen rund um die Gesetzgebung zur Telekommunikation, Speicherungen von Nutzungsdaten bei speziellen Service-Providern (die z. B. sog. Banner-Server betreiben und durch Auswertungen derer Nutzungsdaten Profile über Nutzer bilden können) und der Entwicklung von Standards für Internet-Auftritte der Werbewirtschaft.

Der AK Technik hat sich u. a. mit Fragestellungen rund um biometrische Identifikationssysteme und Massenverfahren (im Hinblick auf die erfolgten Änderungen von Pass- und Personalausweisgesetz), Orientierungshilfen zu Windows XP und Kryptographie, digitale Signaturen, Public-Key-Infrastrukturen und Maßnahmen und Methoden zur Durchsetzung vertrauenswürdiger Informationstechnik befasst. Die Maßnahmen und Methoden zur Durchsetzung vertrauenswürdiger Informationstechnik waren dabei eines der zentralen Themen. Ich habe dieses Thema nochmals in diesem Jahresbericht unter Ziff. 3.5 „Common Criteria“ vertieft.

2.9 Bluetooth

Im Gegensatz zur herkömmlichen Verbindung von Computern und Peripheriegeräten via Kabel werden diese zunehmend mittels Funkverbindungen untereinander vernetzt. Für den Aufbau von Funk-Lans ist „WLAN“ das Mittel der Wahl. Damit lassen sich große und komplexe Funknetze aufbauen, mit einigen Zusatzfunktionalitäten sind diese auch sicher zu bauen. Ein Beispiel für ein großes Funknetz ist das Funk-Lan der Bremer Uni, das ich bereits im letzten Jahr einer datenschutzrechtlichen Prüfung unterzogen hatte (vgl. 24. JB, Ziff. 10.2).

Für die Verbindung von Rechnern mit anderen Peripheriegeräten lässt sich auch „Bluetooth“ einsetzen, eine Technologie, die entwickelt wurde, um das Kabelwirrwarr zu eliminieren. Gern wird die Technik auch in Altbauten verwendet, um eine Kabelverlegung zu vermeiden. Mit Bluetooth können PCs z. B. mit Druckern, Tastaturen, Mäusen, Scannern, Digitalkameras, einem ISDN-Anschluss oder Handys verbunden werden.

Ebenso wie bei den WLAN besteht aber die Gefahr von unerlaubter Nutzung von Ressourcen oder des Mithörens des Datenverkehrs durch Dritte. Das in den Bluetooth-Spezifikationen festgeschriebene Frequenz-Hopping-Verfahren (1600 mal pro Sekunde wird der Sendekanal gewechselt) bietet keinen Schutz gegen Abhören, es dient lediglich dazu, die Datenübertragung zwischen den Geräten robuster gegen Störungen zu machen. Serienmäßig sind bei der Steuersoftware für Bluetooth-Geräte meistens alle Sicherheitsfunktionen abgeschaltet. Jedoch bieten die Bluetooth-Geräte einige Möglichkeiten, die Kommunikation untereinander und die Nutzung der Dienste abzusichern. So können beim Aufbau der Verbindungen untereinander entweder einseitige, zweiseitige oder aber keine gegenseitige Authentifizierungen durchgeführt werden. Jeder Anwender kann damit eine eigene Trust-Domäne aufbauen, in der alle Geräte nach erfolgter Authentifizierung gegenseitig untereinander kommunizieren dürfen. Gesicherte Verbindungen können aufgebaut werden, wenn sich die Gegenstellen im ersten Schritt mittels einer PIN authentifizieren. Dabei sollten nicht die vom Hersteller ab Werk eingestellten PINs verwendet werden, sondern frei vergebene, aus Buchstaben und Zahlen zusammengesetzte PINs. Der zweite Schritt ist die Einschaltung der Verschlüsselung. Der Datenstrom sollte dabei mit 128bit verschlüsselt werden.

In einigen Anwendungsfällen kann es sinnvoll sein, dass der Zugriff auf verschiedene Dienste via Bluetooth autorisiert werden muss, also z. B. eine Bestätigung beim Anwender eingeholt wird, bevor ein bestimmter Dienst genutzt werden kann. Der Anwender kann in diesen Fällen die Nutzung auch ablehnen. Zusätzlich sollten alle Bluetooth-Geräte im sogenannten „Non-discoverable-Mode“ betrieben werden. In diesem Betriebsmodus antwortet das Bluetooth-Gerät nicht auf jede Anfrage anderer Bluetooth-Geräte. Im Discoverable-Mode wird mindestens immer mit der eigenen Geräte-Adresse geantwortet, die im Non-discoverable-Mode nicht preisgegeben wird. Das Gerät kommuniziert dadurch nur mit ihm bekannten anderen Bluetooth-Geräten.

Authentifizierung und Verschlüsselung sollte, wo möglich und sinnvoll, möglichst für alle Bluetooth-Endgeräte und -Dienste eingeschaltet werden. Die Geräte sollten alle im Non-discoverable-Mode betrieben werden. Bei einigen speziellen Anwendungssituationen ist es sinnvoll, zusätzliche Sicherungsmaßnahmen wie IPsec-Verschlüsselung für die Übertragung von Daten zwischen den Endgeräten zu implementieren.

Die verschiedenen Möglichkeiten, eine sichere Verbindung herzustellen, werde ich auch auf meiner Internetseite mit entsprechenden Handlungsabläufen publizieren. Bluetooth ist nämlich eine Technik auch für den Hausgebrauch und bei Verwendung der Standardeinstellungen ist nicht auszuschließen, dass die gesamte Nachbarschaft die übertragenen Daten mitliest.

3. Datenschutz durch Technikgestaltung und -bewertung

3.1 Web.Punkte

Über meine Prüfung von Web.Punkten berichtete ich bereits im letzten Jahresbericht (vgl. 24. JB, Ziff. 3.5). Web.Punkte sind besondere Internet-Cafés an Schulen, die außerhalb des Unterrichts auch interessierten Bürgern und schulexternen Organisationen zur Verfügung stehen. Bei der Prüfung im letzten Jahr hatte ich festgestellt, dass die Accounts der einzelnen Arbeitsplätze der Web.Punkte nicht gegeneinander abgeschottet sind, was eine unzulässige Einsichtnahme durch andere Nutzer innerhalb des Web.Punktes ermöglichte. Ich habe mich daraufhin an den für die Betreuung verantwortlichen Schul-Support-Service e.V. (S3) gewandt und diesen aufgefordert, die festgestellten Mängel in allen Web.Punkten zu beseitigen. S3 hat daraufhin die Grundkonfigurationen aller von ihm betreuten Web.Punkte entsprechend meinen Anforderungen angepasst und die Mängel somit beseitigt. Von den insgesamt 19 in Bremen installierten Web.Punkten sind die Maßnahmen bei 14 Web.Punkten bereits umgesetzt. An zwei Schulen sind die Web.Punkte aufgrund von baulichen Maßnahmen zeitweilig außer Betrieb. S3 hat zugesichert, dass bei Wiederinbetriebnahme die Konfigurationen dieser Web.Punkte ebenfalls angepasst werden. Drei Schulen betreiben ihre Web.Punkte eigenverantwortlich. Ich beabsichtige, diese Schulen im Jahr 2003 einer datenschutzrechtlichen Prüfung zu unterziehen.

3.2 Software P-Switch

Innerhalb des Bremischen Verwaltungsnetzes (BVN) soll Mitarbeiterinnen und Mitarbeitern neben der dienstlichen Nutzung des Internetzugangs auch die private Nutzung erlaubt sein. Dabei ist zu beachten, dass hinsichtlich der dabei zulässigen Protokollierung der Nutzung, je nachdem ob privat oder dienstlich im Internet gesurft wird, unterschiedliche Rechtskontexte (generell zu diesem Thema vgl. die Konferenzentschließung unter Ziff. 15.3 dieses Berichts) gelten. Ich hatte daher eine klare Trennung dieser beiden Bereiche vorgeschlagen. Um diesem Umstand nachzukommen sollen, ähnlich der bestehenden Regelung beim Telefonieren, Nutzerinnen und Nutzer aktiv zwischen dienstlicher und privater Internet-Nutzung umschalten können. Dazu ist von der datenschutz nord GmbH eine Erweiterung für den Internet Explorer von Microsoft entwickelt worden. Diese Erweiterung, die den Namen „P-Switch“ trägt, ist ein Programm, dass die Systemeinstellungen des Internet Explorer verändert. Es wird, je nachdem, ob der Nutzer auf private oder dienstliche Nutzung umschaltet, der vom Internet Explorer zu nutzende zentrale Proxy-Server umgeschaltet. Im Bremer Verwaltungsnetz sind zu diesem Zweck zwei verschiedene Proxy-Server im Einsatz, die unterschiedliche Konfigurationen zur Protokollierung der Internet-Nutzung haben. Die bei der BreKom, dem Standort der Proxy-Server, durchgeführte zentrale Protokollierung der Internet-Nutzung hat den Vorteil, dass nur an einer Stelle darüber gewacht werden muss, was nach welchen Regelungen protokolliert wird. Der Switch (Schalter) eignet sich natürlich auch für den Einsatz in Unternehmen.

Dort gibt es vergleichbare Probleme hinsichtlich der privaten Nutzung des Internets und auch der haftungsrechtlichen Fragen, wenn eine klare Trennung nicht erkennbar ist.

Die aktuell eingestellte Nutzungsart wird dem Nutzer gegenüber in einem Icon auf dem Desktop transparent dargestellt. In dem Hintergrund des Browsermenüs wird ein Wasserzeichen hinterlegt. Das Wasserzeichen stellt im Fall der dienstlichen Nutzung den eingekreisten Buchstaben „D“ dar, während der privaten Nutzung handelt es sich um den eingekreisten Buchstaben „P“. Zusätzlich wird das animierte Logo des Microsoft Internet Explorer durch Logos ersetzt, die wiederum das eingekreiste „D“ bzw. „P“ darstellen.

Das Programm P-Switch besteht aus einer einzigen Dialogbox, die während der Internet-Nutzung immer im Vordergrund des Desktops angezeigt wird. Die Dialogbox ist von ihren Abmessungen her so klein wie möglich gehalten, um die Darstellung am Bildschirm so wenig wie möglich zu stören. Benutzer können jedoch die Dialogbox auch minimieren oder schließen, um die Anzeige gar nicht zu stören. Die Dialogbox selbst besteht aus drei Schaltflächen (eine zum Ändern des Nutzungsstatus, eine zur Anzeige eines Hilfetextes, eine um die Dialogbox zu schließen) und einer Statusanzeige, auf welchen Nutzungsmodus, dienstlich oder privat, der Internet Explorer aktuell eingestellt ist.

P-Switch arbeitet sowohl mit Einzelplatz PC, die direkt an das BVN angeschlossen sind als auch mit den in vielen Dienststellen bereits im Einsatz befindlichen Terminalserver-Lösungen zusammen. Auch bei den Terminalserver-Lösungen kann von jedem einzelnen Nutzer oder jeder einzelnen Nutzerin individuell der Nutzungsstatus geändert werden. Dabei werden die Nutzungsstati der anderen Nutzer des Systems nicht verändert.

Mit P-Switch soll innerhalb des BVN ein in Bedienung und Installation einfach gebautes Werkzeug zum Einsatz kommen, dass es ermöglicht, auf für den Nutzer unkomplizierte Weise die datenschutzrechtlichen Anforderungen der dienstlichen und privaten Internet-Nutzung am Arbeitsplatz zu erfüllen. Das Programm ist sehr einfach zu bedienen und der Nutzungskontext wird den einzelnen Nutzern immer aktuell angezeigt. Im Zusammenspiel mit der Protokollierung der Internet-Nutzung auf den Proxy-Servern im BVN ergibt das ein wirksames System, um sowohl dienstliche als auch private Nutzung des Internets an Arbeitsplätzen in der Bremer Verwaltung zu ermöglichen, als auch ein Kontroll-Instrument für die Nutzung zu haben. Die Protokollierung wird standardmäßig nicht personenbezogen (IP-adressenbezogen) erfolgen, bei konkretem Verdacht auf missbräuchliche Nutzung kann eine dann anlassbezogene, zeitlich begrenzte Vollprotokollierung durchgeführt werden, um die Gefahr einer zukünftigen missbräuchlichen Internet-Nutzung zu minimieren. Der Umfang der Protokollierung auf den beiden im BVN im Einsatz befindlichen Proxy-Servern soll in einer Internetrichtlinie (Dienstanweisung) festgehalten werden, sie wird momentan vom Senator für Finanzen mit dem Gesamtpersonalrat und mir abgestimmt.

3.3 Biometrische Verfahren

Durch die Terroranschläge vom 11. September 2001 sind sogenannte biometrische Verfahren stärker in das Licht der Öffentlichkeit gerückt. So ist im Terrorismusbekämpfungsgesetz, das nach dem 11. September mit Hochdruck aus dem Boden gestampft wurde und zum 01. Januar 2002 in Kraft

getreten ist, geregelt, dass in Pass und Personalausweis neben dem Lichtbild und der Unterschrift auch weitere biometrische Merkmale von Fingern oder Händen oder Gesicht des Personalausweisinhabers enthalten sein dürfen. Lichtbild, Unterschrift und weitere biometrische Merkmale können auch in mit Sicherheitsverfahren verschlüsselter Form in den Pass oder Personalausweis eingebracht werden. Welche biometrischen Merkmale in Pass und Personalausweis eingebracht werden sollen, stand zum Zeitpunkt des Inkrafttretens des Terrorismusbekämpfungsgesetzes noch nicht fest und ist auch bis zum heutigen Tage noch nicht geklärt. Ein separates Bundesgesetz soll gemäß dem Terrorismusbekämpfungsgesetz regeln, welche biometrischen Merkmale in verschlüsselter Form in die Ausweispapiere einfließen und wie sie gespeichert, verarbeitet und genutzt werden dürfen.

Die Unklarheit, welches biometrische Merkmal in die Ausweispapiere einfließen soll, resultiert aus dem derzeitigen Stand der Technik und dem derzeitigen allgemeinen Informationsstand über die Qualität von biometrischen Verfahren.

Biometrie bedeutet soviel wie „Vermessung des Lebens“ und ist die Idee, Merkmale des Menschen zu dessen eindeutigen Identifizierung auch mit technischen Mitteln zu nutzen. Biometrische Verfahren sind somit technische Methoden, um Menschen zu identifizieren. Sie können sowohl zur Identifizierung von Personen eingesetzt werden, als auch zur Authentifizierung der Personen für bestimmte Anwendungen, wie z. B. Zutritt zu bestimmten Bereichen in Rechenzentren oder Flughäfen. Die Authentifizierung auf biometrischer Basis stellt damit eine Alternative zu konventionellen Authentifizierungsmethoden, wie der Besitz eines Schlüssels oder einer Chipkarte oder der Kenntnis eines Passwortes dar.

Damit ein biologisches Merkmal für eine eindeutige Identifizierung oder Authentifizierung genutzt werden kann, muss es verschiedene Anforderungen erfüllen. So muss es sich eindeutig zu einer Person (auch bei eineiigen Zwillingen) zuordnen lassen, es muss eine Merkmalskonstanz aufweisen, also z. B. durch Alterung oder geänderte Frisur nicht beeinflusst werden und es muss eine weite Verbreitung haben, da möglichst alle potenziellen Nutzer dieses Merkmal haben sollten. Das zur Identifizierung oder Authentifizierung eingesetzte Verfahren muss sich zusätzlich hinsichtlich Kosten, Dauer und Methode einer Messung eignen und die Nutzung muss akzeptabel sein, insbesondere darf die Person die sich dem Verfahren unterzieht, keinerlei gesundheitlichen Beeinträchtigungen ausgesetzt sein. Die Merkmale, die eingesetzt werden könnten, sind vielfältig. Verfahren sind beispielsweise denkbar und teilweise auch realisiert für die Erkennung von Gesicht, Iris, Fingerabdruck, Handgeometrie, Venenmuster auf dem Handrücken, Ohrform, Unterschrift, Stimme, Sprechverhalten, DNA, Körpergeruch, Gang oder Sitzverhalten.

Biometrische Merkmale lassen sich in drei verschiedene Merkmalsklassen einordnen: Genotypische (in den Genen verankerte Merkmale), konditionierte Merkmale (erlernte Verhaltensweisen) oder randtypische Merkmale (zufällig entstandene). Die Verfahren werden entweder berührungslos oder mit Berührung (Person muss Sensorfläche o. ä. berühren) durchgeführt. Berührungslose Verfahren sind z. B. Gesichts- oder Stimmerkennung, Verfahren mit Berührung etwa Fingerabdruck- oder Unterschriftenerkennung.

Der Vorgang einer Identifizierung oder Authentifizierung läuft grundlegend immer in vier Schritten ab: Zuerst die Aufnahme der Daten am Sensor, danach die Vorverarbeitung der Daten zu deren Verbesserung mittels mathematischer Verfahren (Beseitigung von Störungen etc.), daran anschließend erfolgt die Merkmalextraktion zur signifikanten Beschreibung der Daten und abschließend erfolgt die Klassifikation der Merkmale. Die klassifizierten Merkmale können dann bei einer Authentifizierung gegen eine Merkmaldatenbank laufen gelassen werden, um z. B. Berechtigungen abzuprüfen oder zur Identifikation genutzt zu werden, wenn etwa sichergestellt werden soll, das Person und zugehöriger Personalausweis auch wirklich zusammengehören.

Grundsätzlich gibt es bei biometrischen Verfahren einige Schwierigkeiten, die beachtet werden müssen. Für jede einzelne Durchführung einer Identifikation oder Authentifikation hat man mit wechselnden Qualitäten der am Scanner aufzunehmenden Daten zu tun. Bei Erkennung von Gesichtern spielen z. B. die aktuelle Beleuchtungssituation, die am Ort der Erkennung herrschende Witterung oder Änderungen des Outfits von Personen, wie z. B. Brille oder Bart eine entscheidende Rolle. Bei der Erkennung von Fingerabdrücken (und letztendlich auch allen anderen biometrischen Verfahren) treten z. B. auch Probleme wie „Translation“ („verschobenes Aufsetzen des Fingers auf den Sensor“), „Rotation“ („verdrehtes“ Aufsetzen), „Skalierung“ (Fingerabdruck erscheint durch schwachen oder starken Anpressdruck an den Sensor unterschiedlich groß), „Bildqualität“ (bedingt z. B. durch trockene, nasse, abgenutzte oder schmutzige Finger) auf. Die Qualität der Referenzdaten muss entsprechend hoch sein, um diesen möglichen Fehlerquellen entgegenzuwirken. Beim sogenannten „Roll-Out“, dem Bekanntmachen einer Person gegenüber einem System, werden hierfür mehrfach die gleichen Daten aufgenommen um optimierte „gemittelte“ Referenzdaten zu erhalten. Letztendlich kann aber auch die Anatomie selbst eine Barriere für die Nutzung biometrischer Verfahren sein. So gibt es bei schätzungsweise zwei bis vier Prozent der Bevölkerung mangelnde Merkmalsausprägungen für die Teilnahme an biometrischer Fingerabdruckerkennung. Diese Zahlenwerte lassen sich in etwa auf alle biometrischen Verfahren übertragen.

Die Qualität der technischen Implementierungen biometrischer Verfahren lässt heute noch vielfach zu wünschen übrig. So hat ein Test einer Computerzeitschrift (c’t 11/2002) gezeigt, dass bestehende Implementierungen relativ einfach ausgehebelt werden können. Zusätzlich hat die Studie BioIS, die das Fraunhofer Institut für Graphische Datenverarbeitung in Darmstadt (IGD) im Auftrag des Bundeskriminalamtes (BKA) und des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durchgeführt hat, gezeigt, dass die Erkennungsleistungen vieler Geräte nicht akzeptabel sind. Die Fehlerquoten sind zu hoch.

Terrorismusbekämpfungsgesetz und der Forschungs- und Entwicklungsstand zu biometrischen Verfahren zwingen zu einer Überprüfung der geeigneten Technologien. Gerade Kenntnisse im Zusammenhang mit biometrischen Massenverfahren wie Erweiterung von Pass- und Personalausweis fehlen. Die speziellen datenschutzrechtlichen Aspekte solcher Verfahren und die Einbindung in Personalausweisen und Pässen sind auch auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder behandelt worden. Die wesentlichen Ergebnisse sind in einer Entschließung zusammengefasst, die unter Ziff. 15.1 dieses Berichts zu finden ist.

Das BSI hat 2002 mehrere Projekte aufgelegt, um Erfahrungen mit biometrischen Massenverfahren zu sammeln und zu verdichten. Darunter sind die Studien „BioFinger“ (Untersuchung der zeitlichen Stabilität des Fingerabdruckverfahrens), „BioFace“ (Untersuchung zur zeitlichen Stabilität von Identifikationsverfahren anhand von Bilddatenbanken zur Erkennung von Personen aus Menschenmassen heraus) und „BioMarkt“ (Marktstudie für biometrische Systeme).

3.4 Installation von Webcams

Der Radio-Bremen-Sender „Bremen Vier“ hat mich um Beratung gebeten, ob es zulässig wäre, in Büros von Firmen, die einen Blick auf besonders befahrene Straßen- und Kreuzungsbereiche bieten, Webcams zu installieren. Die Webcams sollten auf einer „Bremen Vier“-Homepage verlinkt werden und ein zusätzliches Internetangebot im Funk-Verkehrsdienst darstellen. Die Kameras sollten keine Details zu erkennen geben; auch sollte es keine Zoom-Funktion geben. Zweck sei lediglich eine Übersicht über die Verkehrsdichte in diesen Bereichen.

Ich habe dem Sender empfohlen, die Zoomauflösung programmtechnisch so einzustellen, dass die vorgenannten Merkmale, wie Kfz-Kennzeichen, Gesichter, etc. nicht erkannt werden können. Damit die Zoomauflösung durch Aktivitäten der Internetnutzer, z. B. über Tools wie „zoomen“ und „scharfzeichnen“ nicht so verändert werden kann, dass die Merkmale dann doch erkennbar wären, sollten die Einstellungen auf dem Rechner regelmäßig überprüft werden. Die Umsetzung wurde zugesagt.

3.5 Common Criteria

Sowohl für Einzelpersonen als auch für Unternehmen und die öffentliche Verwaltung sind Informationen innerhalb von Datenverarbeitungsanlagen (IuK-Technik) und der darauf laufenden Softwareprodukte als kritisch anzusehen. Für die einen sind sie äußerst wichtige Betriebsmittel, andere, wie Einzelpersonen, erwarten selbstverständlich, dass ihre persönlichen und personenbezogenen Daten nur für bestimmte Zwecke genutzt werden, vertraulich bleiben und nicht unautorisiert verändert werden können. Vielen Anwendern von Informationstechnik fehlen notwendiges Wissen und nötige Mittel, um zu beurteilen, ob die eingesetzten Systeme vertrauenswürdig sind. Auf Marketing-Aussagen und Versicherungen der Softwareentwickler möchte sich niemand wirklich abschließend verlassen. Um Anwendern die Möglichkeit zu geben, ihr Vertrauen in die eingesetzten Systeme und die darin implementierten Sicherheitsmaßnahmen zu erhöhen, sind auf internationaler Ebene die Common Criteria („Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“) geschaffen worden. Dabei handelt es sich um eine Weiterentwicklung und Harmonisierung der europäischen, US-amerikanischen und kanadischen Bestrebungen, Prüfkriterien für datenschutzfreundliche Produkte zu schaffen. In diesem Zusammenhang zu nennen sind „Information Technology Security Evaluation Criteria” (ITSEC), „Trusted Computer Security Evaluation Criteria” (TCSEC, Orange Book) und „The Canadian Trusted Computer Product Evaluation Criteria V3.0e” (CTCPEC).

Für den Datenschutz sind die Common Criteria von besonderer Bedeutung. Mit ihnen wurden erstmals Anforderungen zum Schutz der Privatsphäre in einem Kriterienkatalog definiert, die über

Staatsgrenzen hinaus anerkannt sind. Mit Hilfe der in den Common Criteria beschriebenen „Protection Profiles“ (PP, Schutzprofile) ist es auch möglich, international vergleichbare und somit auch prüffähige datenschutzspezifische Anforderungen für bestimmte Produkte oder Produkttypen zu definieren. Die Schutzprofile bieten dadurch für die Anwender von IuK-Technik die Möglichkeit, ihre Bedürfnisse zur IT-Sicherheit sowohl den Herstellern als auch Zertifizierungsstellen gegenüber deutlich zum Ausdruck zu bringen - unabhängig von bereits bestehenden Produkten.

Der Arbeitskreis „Technische und organisatorische Datenschutzfragen“ der Konferenz der Datenschutzbeauftragten des Bundes und der Länder (AK Technik) hatte 1998 eine Arbeitsgruppe gebildet, die ein Schutzprofil zu den Aspekten Verschlüsselung und Pseudonymisierung erstellen sollte, um so bereits im Vorfeld von Produktentwicklungen wesentliche datenschutzrechtliche Anforderungen wiedergeben zu können.

Da im Laufe der Entwicklungsarbeiten deutlich wurde, dass die Verwendungsbreite von Produkten auf Basis des zu entwickelnden Schutzprofils nicht nur den Bereich der Pseudonymisierung, sondern auch die verschlüsselte lokale Datenspeicherung und die sichere Datenübertragung über Netzwerke umfassen könnte, wurde das BSI gebeten, die Fertigstellung und Fortentwicklung des Schutzprofils sowie dessen Evaluierung und formale Registrierung durchzuführen. Dieses beauftragte 2001 das Deutsche Forschungszentrum für Künstliche Intelligenz GmbH (DFKI) mit der entsprechenden Schutzprofilfertigstellung. In den Entwicklungsprozess wurden von der DFKI neben dem BSI, der Datenschutzbundesbeauftragte wie auch Vertreter mehrerer Unternehmen aus der Privatwirtschaft eingebunden.

Die von der DFKI entwickelten Schutzprofile sind im Jahr 2002 evaluiert und registriert worden. Bei den beiden Schutzprofilen handelt es sich um:

- Benutzerbestimmbare Informationsflusskontrolle („MU“, Mehrbenutzervariante)

- Benutzerbestimmbare Informationsflusskontrolle („SU“, Einbenutzervariante)

Der Kerngedanke der Sicherheitsanforderungen, die in den Schutzprofilen definiert sind, ist die Kontrollierbarkeit aller Informationsflüsse eines Rechners gemäß einstellbarer Informationsflussregeln. Diese Anforderungen können aus rechtlichen, organisatorischen und technischen Rahmenbedingungen abgeleitet und vom Anwender vorgegeben werden (z. B. verschlüsselte Speicherung oder verschlüsselte Übertragung). Diese Schutzprofile (Titel: BISS Benutzerbestimmbare Informationsflusskontrolle) sind im Internet unter der Adresse www.bfd.bund.de/technik/protection_profile.html abrufbar (Registrierungskennzeichen: BSI-PP-0007-2002 und BSI-PP-0008-2002).

Mit diesen zertifizierten Protection Profiles ist eine Basis dafür geschaffen, dass Hersteller entsprechende Produkte entwickeln bzw. evtl. bereits existente Produkte entsprechend modifizieren können und Anwender von den Herstellern Produkte verlangen können, die diesen Schutzprofilen gerecht werden.

4. Bürgerschaft - Die Arbeit des Datenschutzausschusses

4.1 Ergebnisse der Beratung des 24. Jahresberichts

Bericht und Antrag des Datenschutzausschusses vom 15. Januar 2003 zum 24. Jahresbericht des Landesbeauftragten für den Datenschutz vom 22. März 2002 (Bürgerschafts-Drs. 15/1106) und zur Stellungnahme des Senats vom 29. August 2002 (Bürgerschafts-Drs. 15/1224)

Bericht

Die Bürgerschaft (Landtag) hat in ihrer Sitzung am 15. Mai 2002 den 24. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung vom 19. September 2002 die Stellungnahme des Senats zur Beratung und Berichterstattung an den Datenschutzausschuss überwiesen.

Der Ausschuss hat sich in vier Sitzungen am 11.09.2002, 16.10.2002, 04.12.2002 und 15.01.2003 mit dem Jahresbericht und der Stellungnahme befasst. Den Schwerpunkt der Beratungen bildeten diejenigen Punkte, über die auch in dem Zeitraum zwischen der Veröffentlichung des 24. Jahresberichts im März 2002 und der Übermittlung der Stellungnahme des Senats an die Bremische Bürgerschaft im August 2002 kein Einvernehmen zwischen dem Landesbeauftragten für den Datenschutz und den betroffenen Ressorts erzielt werden konnte. Bei der Beratung hat der Ausschuss den Landesbeauftragten für den Datenschutz, Vertreter der betroffenen Ressorts sowie einen Vertreter des Gesamtpersonalrats und den stellvertretenden Abteilungsleiter der Personalabteilung des Zentralkrankenhauses Sankt-Jürgen-Straße angehört. Die wesentlichen Beratungsergebnisse sind nachfolgend aufgeführt. Die Textziffern in den Überschriften entsprechen denen des 24. Jahresberichtes.

Web.Punkte (Tz. 3.5): Um der Gefahr einer Aufspaltung der Bevölkerung in „Teilnehmer und Nicht-Teilnehmer am Informationszeitalter“ entgegenzutreten, sind in 30 weiterführenden Schulen in Bremen und Bremerhaven Internet-Cafés eingerichtet worden. Diese werden als „Web.Punkte“ bezeichnet und zur Unterrichtszeit am Vormittag für schulische Zwecke, nachmittags auch von schulexternen Personen und Institutionen genutzt. Bei der Prüfung eines dieser „Web.Punkte“ hat der Landesbeauftragte für den Datenschutz festgestellt, dass die so genannten Home-Directories, die den Nutzern für Downloads aus dem Internet zur Verfügung gestellt werden, nicht ausreichend gegeneinander abgeschottet wurden. Dies ermöglichte eine unzulässige Einsichtnahme durch Nutzer innerhalb des „Web.Punktes“. Außerdem war es möglich, sich unter einem anderen Account, der zu einem bestimmten Arbeitsplatz gehört, an einem anderen Arbeitsplatz anzumelden und so zu sehen, welche Inhalte ein Nutzer an einem bestimmten Platz aus dem Internet heruntergeladen hat.

Der Ausschuss begrüßt, dass diese Mängel nach Mitteilung der für die Konfiguration der „Web.Punkte“ verantwortlichen Stelle, des so genannten S3-Teams der Universität Bremen, inzwischen in nahezu allen „Web.Punkten“ abgestellt sind. Die drei „Web.Punkte“, die nicht vom S3-

Team, sondern von den Schulen selbst betreut werden, wird der Landesbeauftragte für den Datenschutz im nächsten Berichtsjahr prüfen.

Prüfung der Führung der Personalakten bei verschiedenen Personalstellen (Tz. 5.1): Der Landesbeauftragte für den Datenschutz hat bei der Prüfung der Führung von Personalakten und Personaldaten in insgesamt sieben Personalstellen Mängel festgestellt.

In fünf Personalstellen wurde in den eingesehenen Grundakten kein Verzeichnis aller Teil- und Nebenakten geführt, so dass die Beschäftigten bei der Einsichtnahme ihrer Hauptakten nicht erkennen konnten, ob weitere Personalteilakten über sie geführt werden.

Ferner wurde überprüft, ob die Richtlinien über die Erhebung und Führung von Personalaktendaten vom 25. Mai 1996 (Brem.ABl. S. 433) eingehalten werden. Dabei stellte sich heraus, dass Krankheits- und Urlaubsunterlagen in allen geprüften Personalstellen länger als nach den Richtlinien zugelassen aufbewahrt und teilweise vorschriftswidrig in den Grundakten und nicht in den Teilakten abgelegt waren. Außerdem wurden in fünf Personalstellen die Personalakten von ausgeschiedenen Bediensteten zu lange aufbewahrt.

Weiterer Prüfungsgegenstand war die Aufbewahrung von Beihilfe- und Kindergeldakten. Auf eine Anweisung des damaligen Senators für Jugend, Gesundheit und Soziales aus dem Jahr 1987 wurden im Zentralkrankenhaus Sankt-Jürgen-Straße Beihilfe- und Kindergeldakten aufbewahrt. Dies widerspricht jedoch der nach § 93 b Satz 2 Bremisches Beamtengesetz vorgeschriebenen Trennung der Beihilfebearbeitung von der Personalverwaltung.

Der Datenschutzausschuss begrüßt, dass die festgestellten Mängel nach Mitteilung aller geprüften Personalstellen inzwischen beseitigt wurden. Da Verstöße gegen die Richtlinien über die Erhebung und Führung von Personalaktendaten vom 25. Mai 1996 auch in der Vergangenheit bereits Gegenstand von Beanstandungen waren (vgl. 22. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31.03.2000, Drs. 15/266, Tz. 5.1 und Jahresbericht 1999 des Rechnungshofes der Freien Hansestadt Bremen vom 21.07.1999, Drs. 15/28, Tz. 65), bittet der Ausschuss den Senat, alle Behörden, Eigenbetriebe und sonstigen Stellen noch einmal eindringlich auf die Richtlinien hinzuweisen und zu deren Einhaltung anzuhalten.

Unterlagen über personelle Angelegenheiten beim Personalrat (Tz. 5.3): Der Landesbeauftragte für den Datenschutz ist einem Hinweis einer Mitarbeiterin des Zentralkrankenhauses Sankt-Jürgen-Straße nachgegangen, wonach der dortige Personalrat Unterlagen zu ihrer Person über personelle Angelegenheiten zu lange aufbewahre. Auf Nachfrage hat der Personalrat dies bestätigt und zugesagt, in Zukunft Unterlagen mit personenbezogenen Daten, die nicht erforderlich sind, sofort, die übrigen spätestens nach fünf Jahren zu vernichten.

Der Datenschutzausschuss hat diesen Vorfall zum Anlass genommen, den Gesamtpersonalrat zu bitten, alle Personalräte für den datenschutzgerechten Umgang mit Unterlagen mit personenbezogenen Daten zu sensibilisieren. Der Gesamtpersonalrat hat die Personalräte in einem Rundschreiben, das mit dem Landesbeauftragten für den Datenschutz abgestimmt ist, bereits auf die Problematik hingewiesen. Der Ausschuss begrüßt dies ebenso wie die Ankündigung des Vertreters des Gesamtpersonalrats, diesen Punkt in einer Gesamtpersonalratssitzung noch einmal aufzugreifen.

INPOL-neu läuft nicht (Tz. 6.7): Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit 1992 unter der Bezeichnung "INPOL-neu" eine Fortentwicklung eines gemeinsamen Informationssystems. Infolge von Anlaufschwierigkeit wurde die Einführung des neuen Systems mehrfach verschoben. Nach der ursprünglichen Konzeption war unter anderem vorgesehen, dass das Bundeskriminalamt für die Länder Auftragsdatenverarbeitung durchführt. In diesem Zusammenhang hat der Landesbeauftragte für den Datenschutz darauf hingewiesen, dass eine Aufweichung der Trennung der Datenbestände zwischen Bund und Ländern zu befürchten sei. Auch seien die Fragen der Protokollierung, der Verantwortung über die gespeicherten Daten und der Zugriffsmöglichkeiten aus datenschutzrechtlicher Sicht noch nicht zufriedenstellend gelöst.

In seiner Stellungnahme zum 24. Jahresbericht hat der Senat darauf hingewiesen, von der ursprünglichen Konzeption für „INPOL-neu“ sei inzwischen abgewichen worden. Der Datenschutzausschuss hat einen Vertreter des Innenressorts dazu angehört und sich das neue Konzept erläutern lassen. Dabei wurde insbesondere deutlich, dass vonseiten des BKA für die Länder keine Auftragsdatenverarbeitung mehr angeboten wird.

Der Datenschutzausschuss stellt fest, dass durch die jetzigen Veränderungen des Projektes „INPOL-neu“ die Grundlage für die Bedenken des Landesbeauftragten für den Datenschutz entfallen ist.

Änderung des Bremischen Meldegesetzes (Tz. 6.12.1): Der Landesbeauftragte für den Datenschutz hat darauf hingewiesen, dass die durch Gesetz vom 30.10.2001 (Brem.GBl. S. 347) erfolgte Änderung des Bremischen Meldegesetzes infolge fehlender Übergangsfristen Probleme bei der Umsetzung aufwerfe. Insbesondere sei eine zeitgerechte Anpassung der beiden automatisierten Einwohnermeldeverfahren (DEMOS in Bremen und Meso 96 in Bremerhaven) nicht erfolgt.

In seiner Stellungnahme hat der Senat mitgeteilt, dass in Bremen eine Vielzahl von Umsetzungsschritten bereits erfolgt sei. In den Fällen, in denen eine technische Anpassung an die geänderte Rechtslage noch ausstehe, stellten Dienstanweisungen die Umsetzung durch manuelle Eingabeverfahren sicher. Auf die Umsetzung der Regelungen, die auf Grund der Änderung des Zweiten Gesetzes zur Änderung des Melderechtsrahmengesetzes aus dem Jahre 1994 in das Bremische Meldegesetz übernommen worden sind, werde insoweit verzichtet, als diese an das durch das Dritte Gesetz zur Änderung des Melderechtsrahmengesetzes vom 3. April 2002 geänderte Melderrechtsrahmengesetz erneut angepasst werden müssten.

In Bremerhaven ist eine vollständige Anpassung des DV-Systems an das geänderte Melderecht noch nicht erfolgt. Die mit der Entwicklung der Software für das DV-Verfahren der Meldestelle betraute Firma ist der Stellungnahme des Senats zufolge jedoch unverzüglich über die Gesetzesänderung unterrichtet worden. Nach Mitteilung des Innenressorts hat die Firma der Meldestelle inzwischen neue Programmteile für die regelmäßige Datenübermittlung zur Verfügung gestellt und die Lieferung weiterer Software angekündigt. Die bereits gelieferten Programmteile werden jetzt eingesetzt und getestet.

Der Datenschutzausschuss hält es für vertretbar, dass die Einwohnermeldeverfahren insoweit nicht angepasst werden, als diese in absehbarer Zeit infolge der Novellierung des Melderechtsrahmengesetzes erneut umgestellt werden müssten. Er begrüßt, dass die Umsetzung der

Änderungen des Bremischen Meldegesetzes in Bremen im Übrigen weitgehend abgeschlossen ist, und erwartet die zügige Anpassung des in Bremerhaven verwendeten Meldeverfahrens Meso 96 an das geänderte Bremische Meldegesetz in Abstimmung mit dem Landesbeauftragten für den Datenschutz.

Bundestagswahl 2002 (Tz. 6.12.6): Der Landesbeauftragte für den Datenschutz hat die Bundestagswahl im September 2002 zum Anlass genommen zu prüfen, auf welche Weise das Widerspruchsrecht der Bürger hinsichtlich der Weitergabe ihrer Daten an politische Parteien und andere Stellen und Einrichtungen im Meldeverfahren gewährleistet wird. Nach der derzeit geltenden Verordnung über die Muster der Meldescheine vom 23.11.2001 (Brem.GBl. S. 429) ist auf den Vordrucken für die amtliche Meldebestätigung am Ende ein Hinweis auf die „Hinweise zur kostenfreien Eintragung von Datenübermittlungs- und Auskunftssperren auf dem Vorblatt“ enthalten. Das Vorblatt wiederum weist auf einen weiteren Vordruck für eine Erklärung des Betroffenen zu den von ihm gewünschten Datenübermittlungssperren hin, den die Meldestelle bereit halte. Auf diesem Formular hat der Bürger erneut Angaben zu seiner Person zu machen.

Der Landesbeauftragte für den Datenschutz hat kritisiert, dass dieses komplizierte Verfahren die Rechtswahrnehmung der Betroffenen erheblich beeinträchtige, und angeregt, statt der Aufzählung der einzelnen Möglichkeiten einer Übermittlungssperre im Vorblatt gleich ein Kästchen für die Entscheidung des Bürgers auf dem Meldebogen vorzusehen.

Der Datenschutzausschuss schließt sich dieser Kritik an und bittet das Innenressort, im Rahmen der im Jahr 2003 zu erwartenden Anpassung des Bremischen Melderechts an das novellierte Melderechtsrahmengesetz Möglichkeiten für ein bürgerfreundlicheres und die Rechtswahrnehmung erleichterndes Verfahren zu prüfen.

Prüfung des Justiznetzes (Tz. 7.1): Gegenstand der Prüfungen im Berichtszeitraum des 24. Jahresberichts war auch das Justiznetz des Senators für Justiz und Verfassung, das von dem Landesbetrieb Justiz-Dienstleistungen der Freien Hansestadt Bremen (JUDIT Bremen) betrieben wird. Der Landesbeauftragte für den Datenschutz hat im Zuge der Prüfung Maßnahmen zur Erhöhung der Sicherheit des Justiznetzes empfohlen.

Standortübergreifende Zugriffe auf Dienste der 22 verschiedenen Standorte des Justiznetzes über den zentralen Switch erfolgen nur in Ausnahmefällen und nur nach expliziter Freigabe. Wurde ein Übergang von einem Standort auf den anderen zugelassen, so wurde nach den Feststellungen des Landesbeauftragten für den Datenschutz bei der Freischaltung allerdings nicht nach einzelnen Diensten differenziert. Infolgedessen waren gleich sämtliche auf den Rechnern verfügbare Dienste auch standortübergreifend verfügbar. Die Anregung des Landesbeauftragten, zur Erhöhung der Sicherheit im Rahmen freigeschalteter Verbindungen nur die jeweils benötigten TCP/IP-Dienste freizugeben, hat der Betreiber des Justiznetzes umgesetzt.

Ferner erfolgte die Datenübertragung im Justiznetz grundsätzlich unverschlüsselt, so dass das Risiko der Einsichtnahme der Daten durch Mitarbeiter des Betreibers des Justiznetzes und des Telekommunikationsbetreibers bestand. Auf Anregung des Landesbeauftragten für den Datenschutz wurden in einem Pilotprojekt zunächst die zwischen Bremen und Bremerhaven übertragenen Daten

mittels IPSec verschlüsselt. Der Vertreter des Justiressorts hat erklärt, nach den dabei gemachten Erfahrungen seien nunmehr sämtliche WAN-Strecken des Justiznetzes verschlüsselt worden.

Der Ausschuss stellt fest, dass das Justizressort den Empfehlungen des Landesbeauftragten für den Datenschutz zur Erhöhung der Sicherheit des Justiznetzes nachgekommen ist.

Internet-Nutzung durch Schulen (Tz. 10.1): Der Landesbeauftragte für den Datenschutz hat bereits in seinem 22. Jahresbericht unter Tz. 10.3 über die Internet-Nutzung durch Schulen berichtet und auf wichtige datenschutzrechtliche Anforderungen hingewiesen. In seinem 23. Jahresbericht (Tz. 10.1) hat der Landesbeauftragte feststellen müssen, dass entgegen der Zusage des Senators für Bildung und Wissenschaft weder eine Orientierungshilfe noch eine Muster-Nutzungsordnung für die schulische Internet-Nutzung erstellt worden war. Außerdem war es nicht wie vereinbart zu einem Workshop beim Landesinstitut für Schule (LIS) mit Vertretern des Ressorts und den Webmastern der Schulen unter Beteiligung des Landesbeauftragten gekommen.

Im Berichtszeitraum des 24. Jahresberichts hat dieser Workshop zum Thema „Datenschutzkonforme Internet-Nutzung an Schulen“ nunmehr stattgefunden. Gegenstand des Workshops waren unter anderem Fragen der Gestaltung von Internet-Auftritten der Schulen, der Verwaltung von elektronischen Postfächern und der inhaltlichen Beschränkung von Downloads aus dem Internet in das lokale Netz der Schulen. Eine Orientierungshilfe und eine Muster-Nutzungsordnung sollten vom Senator für Bildung bis zum Frühjahr 2002 vorgelegt werden.

Vor allem der Bedarf für eine Orientierungshilfe ist bei der von dem Landesbeauftragten für den Datenschutz im Berichtsjahr durchgeführten Überprüfung der Praxis im Umgang mit dem Internet an Schulen deutlich geworden. Der Landesbeauftragte hat festgestellt, dass bei den Verantwortlichen eine große Unsicherheit über die datenschutzrechtlichen Anforderungen an die Internet-Nutzung besteht. Dies betrifft insbesondere Fragen der Zulässigkeit und des Umfangs von Datenspeicherung bzw. der Protokollierung von Benutzer-Aktivitäten.

Auf mehrfaches Drängen des Datenschutzausschusses hat das Bildungsressort endlich die geforderten Handlungsanweisungen vorgelegt. Die „Richtlinien zur schulischen Nutzung des Internets“ enthalten Regelungen über die Nutzungsberechtigung, die Aufsicht, die Nutzung von Inhalten und über Eingriffe in die Hard- und Softwareinstallation. Sie werden ergänzt durch eine „Orientierungshilfe für den Einsatz des Internets an Schulen“. Diese unterstützt die Schulen in rechtlichen und technischen Fragen des Datenschutzes und der Datensicherheit, aber auch des Medienrechts und macht Vorgaben für die Behandlung dieser Themen im Unterricht. Schließlich wurden ein „Muster für eine Nutzungsordnung der Computereinrichtungen an Schulen“ sowie ein „Muster für eine Nutzungsordnung für Grundschülerinnen und Grundschüler und für Schülerinnen und Schüler mit besonderem Förderbedarf“ entworfen. Die schriftliche Anerkennung dieser Nutzungsordnungen durch die Schülerinnen und Schüler sowie deren Erziehungsberechtigte soll Voraussetzung für ihre Zulassung als Nutzer außerhalb des Unterrichts sein.

Der Ausschuss begrüßt die Erstellung der Orientierungshilfe, der Richtlinien sowie der Nutzungsordnungen durch das Bildungsressort.

Prüferfahrungen bei der Führung von Schullaufbahnakten (Tz. 10.3): Eingaben Betroffener haben den Landesbeauftragten für den Datenschutz veranlasst, an zwei Bremer Schulen die Einhaltung der datenschutzrechtlichen Bestimmungen über die Führung von Schullaufbahnakten zu überprüfen.

An beiden Schulen wurden Verstöße gegen die Richtlinien zur Führung der Schullaufbahnakten festgestellt. Besonders sensible Daten, wie Gesundheits- und Verhaltensdaten, wurden nicht wie nach den Richtlinien vorgesehen getrennt von den übrigen Unterlagen in einem separaten Teil aufbewahrt. Außerdem fehlten die für die Aufnahme dieser sensiblen Unterlagen in die Schullaufbahnakte benötigten Einwilligungserklärungen der Betroffenen. Ferner wurden an einer Schule Schullaufbahnakten stets ohne Zustimmung der Betroffenen weitergegeben.

Weiterhin wurde an beiden Schulen ein Verstoß gegen die nach § 18 Abs. 1 des Gesetzes zum Datenschutz im Schulwesen (SchulDSG) bestehende Pflicht zur Sperrung von personenbezogenen Daten ausgeschiedener Schüler festgestellt. Auch die Richtlinie über die Sicherung, Aufbewahrung und Aussonderung von Schriftgut in den Schulen wurde nicht beachtet. Darin ist festgelegt, dass personenbezogene Daten in nicht automatisierten Dateien und in Akten nach Ablauf bestimmter Fristen grundsätzlich zu löschen sind, wenn sie nicht mehr benötigt werden. In beiden Schulen waren die Aufbewahrungsfristen zum Teil erheblich überschritten worden.

Der Vertreter des Bildungsressorts hat erklärt, es werde eine Dienstanweisung erarbeitet, die die Schulen zur Beachtung der datenschutzrechtlichen Bestimmungen anhalte. Außerdem würden entsprechende Fortbildungsmaßnahmen angeboten. Schließlich werde bei den Schulleiterbesprechungen zukünftig ein Jurist anwesend sein.

Der Ausschuss begrüßt die vom Senator für Bildung und Wissenschaft eingeleiteten Schritte und erwartet, dass die geprüften Schulen ihre Erklärung gegenüber dem Landesbeauftragten für den Datenschutz, die aufgetretenen Mängel beseitigen zu wollen, umsetzen.

Antrag

Die Bürgerschaft (Landtag) möge beschließen:

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

4.2 Weitere Themen der Beratungen im Datenschutzausschuss

Über die unter Ziff. 4.1 dargestellten Ergebnisse hinaus hat sich der Datenschutzausschuss u. a. auch mit den nachfolgend aufgelisteten Themen beschäftigt:

- Gesetz zur Änderung des Bremischen Datenschutzgesetzes und anderer Gesetze (Drs. 15/1208)
- Gesetz zur Einrichtung eines Registers über unzuverlässige Unternehmen („Korruptionsregister“)
- Biometrische Verfahren
- Problematik der 0190-Telefonnummern
- Entwurf und Anhörung zum Informationsfreiheitsgesetz
- Datenschutz nord GmbH – Bericht der Geschäftsführung

- b.i.t. Betrieb für Informationstechnologie (Wirtschaftsbetrieb der Stadt Bremerhaven) – Bericht der Betriebsleitung
- Weitergabe von Daten an die Adressbuchverlage durch die Meldestellen
- Weitergabe von Film-, Ton- und Fotomaterial an die Polizei durch Reporter
- Zahl der Telefonüberwachungen in Bremen
- Änderung der Meldedatenübermittlungsverordnung

Die Sitzungen des Datenschutzausschusses sind in der Regel öffentlich, sie finden außerhalb der Parlamentsferien einmal im Monat statt.

5. Personalwesen

5.1 Unsichere Versendung personenbezogener Unterlagen per Telefax

Vom Magistrat der Stadt Bremerhaven ist ein Telefax fehlübermittelt worden, das eine Personal- und Disziplinarangelegenheit eines Magistratsmitarbeiters betraf. Ich bat den Magistrat daher Anfang Februar 2002 um Stellungnahme. Nach Erinnerungen erhielt ich vom Magistrat Mitte Juni eine Antwort. Darin wurde die Falschübermittlung mit einer Falscheingabe in das Telefax-Gerät begründet, so dass das Fax bei einer Privatfirma und nicht bei der ursprünglich als Empfänger vorgesehenen Stelle ankam. Der Magistrat erklärte zu der Fehlübermittlung weiter, dass diese mit einem erst wenige Tage zuvor neu angeschafften und installierten Fax-Gerät passiert sei. Unmittelbar nach Bekanntwerden der Fehlleitung sei mit der Firma, die das Fax-Gerät installiert hatte, die Löschung von Programmierungen vereinbart worden. Außerdem sei seit dem Zeitpunkt des fehlgeleiteten Faxes sichergestellt, dass jedem Fax ein entsprechendes standardisiertes Formblatt vorangeht, so dass selbst bei einer künftigen Fehlleitung für einen Empfänger der Absender eindeutig erkennbar wird und damit um sofortige Rückgabe bzw. Rücksprache gebeten werde.

Die Stellungnahme des Magistrats hielt ich für nicht ausreichend, denn ich hatte nicht nur zu dem speziellen Fehlfax um Antwort gebeten, sondern eine generelle Prüfung verlangt. Im Gegensatz zur bremischen Verwaltung gibt es für den Bereich des Magistrats der Stadt Bremerhaven bislang nämlich keine Regelungen, aus denen sich die bei der Benutzung von Telefax-Geräten erforderlichen Schutzmaßnahmen ergeben. Ich verwies den Magistrat daher Ende Juni 2002 auf die seit vielen Jahren für die bremische Verwaltung geltenden Telefax-Regeln, und ich empfahl, diese Regeln für den Bereich des Magistrats zu übernehmen. Der Magistrat hat sich daraufhin bereit erklärt, sie in den Erlass einer allgemeinen Geschäftsanweisung zur Behandlung von Posteingängen und Postausgängen aufzunehmen, der aber noch der Vorbereitung bedürfe.

Meine Nachfragen u. a. im August und Oktober nach dem Sachstand blieben unbeantwortet. Auf weitere telefonische Nachfrage erhielt ich Mitte Dezember eine Nachricht über den Eingang meines Schreibens mit dem Hinweis, man habe mein Schreiben nunmehr zur weiteren Bearbeitung weitergeleitet. Anfang Januar erhielt ich vom zuständigen Sachbearbeiter die Nachricht, der Vorgang sei bei ihm eingegangen, er werde die Angelegenheit weiter verfolgen, es erscheine ihm aber wenig zweckmäßig, für den Faxbereich ein gesondertes Regelwerk zu erlassen.

5.2 Aufbewahrung von Dienstaufsichtsbeschwerden

Aufgrund einer Eingabe habe ich festgestellt, dass im Personalamt der Stadt Bremerhaven in einer Generalakte enthaltene Dienstaufsichtsbeschwerden frühestens erst 15 Jahre nach Erledigung vernichtet, teilweise sogar dauernd aufbewahrt werden. Hierzu hat das Amt erklärt, es beachte insoweit den Bericht „Kommunale Schriftgutverwaltung“ der Kommunalen Gemeinschaftsstelle für

Verwaltungsvereinbarung (KGSt), der diese Empfehlung in einer Lose-Blatt-Sammlung tatsächlich enthielt.

Dagegen habe ich bei Prüfungen von Personalstellen in der bremischen Verwaltung festgestellt bzw. erfolgreich darauf hingewirkt, dass derartige Unterlagen, die nicht zur Personalakte zu nehmen sind, entsprechend § 93 f Bremisches Beamtengesetz (BremBG) in der Regel ein Jahr nach Erledigung zu vernichten sind.

Aus diesen Gründen habe ich in Absprache mit den Datenschutzbeauftragten des Bundes und der Länder der KGSt mitgeteilt, dass die dort empfohlene Frist viel zu lang und nicht vereinbar mit den beamtenrechtlichen Vorschriften der Länder ist. Ich habe angeregt, die entsprechenden Aussagen des vorgenannten Berichts dieser Rechtslage anzupassen. Ergänzend habe ich gebeten, darauf hinzuweisen, dass bei Schriftgut mit personenbezogenen Daten, zu dem keine bereichsspezifische gesetzliche Aufbewahrungsfrist besteht, der behördliche Datenschutzbeauftragte (soweit vorhanden) oder der jeweilige Landesbeauftragte für den Datenschutz eingeschaltet werden kann.

Die KGSt hat daraufhin mitgeteilt, dass sie bei einer Neuauflage meine vorgenannten Hinweise berücksichtigen und in den KGSt-Informationen veröffentlichen wird.

Nachdem ich das Personalamt der Stadt Bremerhaven auf die Antwort der KGSt hingewiesen und erneut verlangt habe, dass die Dienstaufsichtsbeschwerden, die sich in der Generalakte befinden, spätestens ein Jahr nach Erledigung zu vernichten sind, hat diese erst nach mehrfachen Mahnungen erklärt, nunmehr ebenfalls diese Vorgänge entsprechend § 93 f BremBG, also in der Regel ein Jahr nach Erledigung, zu vernichten.

5.3 Umgang mit Krankmeldungen

Nach Einführung eines elektronischen Dienstplans im Zentralkrankenhaus Reinkenheide (ZKH) haben die Beschäftigten ihre Krankmeldungen bzw. Arbeitsunfähigkeitsbescheinigungen nicht mehr direkt bei der Personalstelle, sondern bei der jeweiligen Stations- bzw. Fachabteilungsleitung abzugeben. Sobald die entsprechenden Daten in den elektronischen Dienstplan eingegeben worden sind, werden die Bescheinigungen an die Personalabteilung weitergeleitet.

Daraufhin habe ich aus dem ZKH mehrere Hinweise erhalten, wonach die Arbeitsunfähigkeitsbescheinigungen häufig offen auf den Schreibtischen in den Stationen liegen würden und dadurch von Kollegen, Patienten und Besuchern eingesehen werden könnten. Darüber hinaus könnten sie z. B. durch die Angabe der Fachärzte auf den Bescheinigungen auf bestimmte Erkrankungsarten schließen.

Ich habe daraufhin beim ZKH nachgefragt, ob statt dessen nicht das bisherige Verfahren beibehalten werden könne, damit auf diese Personaldaten nur die ohnehin mit Personalangelegenheiten betrauten Beschäftigten Zugriff haben, um insoweit der Anforderung des § 93 a Abs. 3 Bremisches Beamtengesetz (BremBG) gerecht zu werden. Danach dürfen Zugang zu Personalakten nur Personen haben, die mit der Bearbeitung von Personalangelegenheiten beauftragt sind und soweit dies für diese Zwecke erforderlich ist. Dies gilt auch für den Zugang im automatisierten Abrufverfahren.

Das ZKH hat daraufhin erklärt, es wolle keine organisatorische Änderung vornehmen, sondern werde die Stations- und Fachabteilungsleiter besonders verpflichten und wolle den Transport der Arbeitsunfähigkeitsbescheinigungen den gesetzlichen Bestimmungen anpassen.

Erst auf Nachfrage hat das ZKH dann erklärt, als Alternativlösung böte sich an, zumindest für den zahlenmäßig größten Bereich des Pflegedienstes festzulegen, dass die Bescheinigungen bei der Pflegedienstleitung abzugeben sind, die dann die entsprechenden Daten in den Dienstplan eingibt und die Unterlagen an die Personalabteilung weiterleitet.

Nachdem ich diese Alternative akzeptiert und Anfang Juni 2002 nach der Umsetzung gefragt habe, ist vom ZKH erklärt worden, mit der Pflegedienstleitung würden die näheren Einzelheiten der Entgegennahme, Eingabe der Daten und Weiterleitung der Arbeitsunfähigkeitsbescheinigungen geregelt. Das ZKH hatte noch um etwas Geduld gebeten und es werde unaufgefordert auf die Angelegenheit zurückkommen. Mitte September 2002 ist vom ZKH dann erklärt worden, nun solle doch durch Umstellung des Programms versucht werden, die Verarbeitung der Krankmeldungen ausschließlich durch die Personalabteilung vornehmen zu lassen.

Auf erneute Anfrage Mitte November 2002 hat das ZKH erklärt, die Verarbeitung der Krankmeldungen durch die Personalabteilung sei in der Praxis sehr schwer durchführbar und führe zu erheblichen Störungen im Arbeitsablauf. Anfang des Jahres 2003 solle mit der Pflegedirektion nach geeigneten Lösungen - unter Beachtung der datenschutzrechtlichen Bestimmungen - gesucht werden. Das ZKH will mich über das Ergebnis unterrichten.

Ich habe jetzt dem ZKH eine letzte Frist zur Regelung dieser Angelegenheit eingeräumt. Ich kann es nicht hinnehmen, dass das ZKH offensichtlich nicht bereit ist, hier eine Lösung vorzulegen.

5.4 Chipkarten im Rahmen der Freien Heilfürsorge

Die Stelle für Beihilfe und Freie Heilfürsorge bei der Stadt Bremerhaven beabsichtigt, für die Beamten der Polizei und der Feuerwehr als Ersatz für die bisherigen Krankenscheine Chipkarten einzusetzen.

Ich habe auf die seinerzeit anstehende Novellierung des Bremischen Datenschutzgesetzes (BremDSG) hingewiesen, wonach ein neuer § 20 a BremDSG eine Regelung über mobile Datenverarbeitungsmedien enthalten wird. Danach ist der Einsatz dieser Medien (Chipkarten) nur aufgrund einer Rechtsvorschrift oder mit Einwilligung der Betroffenen zulässig. Weiter habe ich auf die weiteren Anforderungen dieser Regelung hingewiesen. Danach muss die verantwortliche Stelle den Betroffenen auf seinen Wunsch in allgemein verständlicher Form u. a über die Funktionsweise des Mediums unterrichten und ihn bei der Ausgabe über seine Rechte nach § 4 BremDSG aufklären.

Die Behörde hat mitgeteilt, dass sie nur mit Einwilligung der Betroffenen die Chipkarten ausgeben wird. Sie hat mir hierzu den Entwurf einer Einverständniserklärung zur Verfügung gestellt; sie entspricht den datenschutzrechtlichen Anforderungen.

Nachdem die Angelegenheit damit erledigt war, hat der Magistrat die entsprechende Verwaltungsvorschrift „Grundsätze über die Durchführung der Freien Heilfürsorge“ lediglich

dahingehend geändert, dass er die Worte „Krankenschein“ und „Zahnbehandlungsschein“ durch das Wort „Krankenversichertenkarte“ ersetzt hat. Das Wort „Freiwilligkeit“ kam dabei nicht vor.

Ich habe mich daraufhin vergewissert, ob der Regelung in § 20 a BremDSG tatsächlich Rechnung getragen wird. Der Magistrat hat daraufhin erklärt, die Einführung der Krankenversichertenkarte beruhe auf dem Grundsatz der Freiwilligkeit. Bis auf wenige Ausnahmen liege das schriftliche Einverständnis vor. Bei der Ausgabe der Krankenversichertenkarten werde ein Informationsblatt herausgeben, das die gesetzlich geforderten Hinweise enthalten werde.

5.5 Trennung der Beihilfe von der Personalverwaltung in den ZKH’s

Bei einer Prüfung der Personalakten beim Zentralkrankenhaus St.-Jürgen-Straße hatte ich erfahren, dass in allen Zentralkrankenhäusern (ZKH’s) der Stadtgemeinde Bremen die Beihilfeakten in den Personalabteilungen geführt werden, obwohl die Berechnung der Beihilfe bei Performa Nord erfolgt (vgl. 24. JB, Ziff. 5.1, vorl. Abs.). Diese Verfahrensweise verletzt das Trennungsgebot nach § 93 b Bremisches Beamtengesetz (BremBG), wonach die Beihilfeakte von der übrigen Personalakte getrennt aufzubewahren ist und die Beihilfe in einer von der übrigen Personalverwaltung getrennten Organisationseinheit bearbeitet wird; Zugang sollen nur Beschäftigte dieser Organisationseinheit haben.

Aufgrund meines Vorschlags, entsprechend der Rechtslage und Verfahrensweise der übrigen bremischen Verwaltung die Beihilfeakten bei Performa Nord zu führen, hat der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales erklärt, es würde von den ZKHs als „Rückschritt“ angesehen, wenn die Beihilfeakten bei Performa Nord geführt würden, zumal die senatorische Dienststelle mit den dortigen Personalabteilungen übereingekommen sei, durch Umorganisation innerhalb der eigenen Bereiche dem Trennungsgebot besser Rechnung zu tragen.

Auf Nachfrage hat das Ressort erklärt, nunmehr werde organisatorisch sichergestellt, dass die Personalstellen lediglich die Anträge der Beschäftigten offen entgegennehmen und prüfen, ob die Antragsteller beihilfeberechtigt sind, wobei die ärztlichen Rechnungen diesen Anträgen jedoch in einem verschlossenen Umschlag beizufügen seien. Die Rücksendung der Beihilfebescheide und die ärztlichen Rechnungen würden - wie bisher - von Performa Nord in verschlossenen Umschlägen direkt an die Antragsteller gesandt. Die Durchschriften dieser Bescheide würden - ebenfalls in einem verschlossenen Umschlag - an das jeweilige ZKH gesandt. Diese Unterlagen würden nach Angaben der senatorischen Dienststelle nur noch zu Rechnungs- und Steuerprüfungszwecken verwendet, so dass die Durchschriften getrennt von den Personalakten und separat von den Personalstellen aufbewahrt würden.

Das Verfahren entspricht nunmehr dem Trennungsgebot, insbesondere weil die Personalstellen insoweit keine medizinischen Daten mehr zur Kenntnis nehmen können.

5.6 Personaldaten bei Personalräten, Frauenbeauftragten und den Schwerbehindertenvertrauensleuten

Eine Eingabe, über die ich in meinem letzten Jahresbericht unter Ziff. 5.3 (Unterlagen über personelle Angelegenheiten beim Personalrat) berichtet habe, hat mich veranlasst, alle Personalräte in der bremischen Verwaltung auf bei der Verarbeitung von Personaldaten zu beachtende Datenschutzanforderungen hinzuweisen. Hierzu habe ich dem Gesamtpersonalrat (GPR) die Anforderungen über die Erhebung, die Aufbewahrung, Löschung und Vernichtung von Personaldaten und Unterlagen, insbesondere über personelle Angelegenheiten sowie die Einhaltung der Geheimhaltungspflichten nach dem Bremischen Personalvertretungsgesetz dargelegt und gebeten, die Personalräte darüber zu unterrichten. Der GPR hat sich dankenswerterweise dazu bereit erklärt, die Unterrichtung ist dann in Form eines Rundschreibens erfolgt.

Auch die Bremische Zentralstelle für die Verwirklichung der Gleichberechtigung der Frau (ZGF) habe ich über die gleichen Anforderungen und die Bedeutung der Schweigepflicht der Frauenbeauftragten in der bremischen Verwaltung nach dem Landesgleichstellungsgesetz unterrichtet. Auch die ZGF hat die Frauenbeauftragten in Form eines Rundschreibens darüber unterrichtet.

Hinsichtlich der Verarbeitung durch die Schwerbehindertenvertrauensleute habe ich in gleicher Weise den Gesamtvertrauensmann der Schwerbehinderten über die Anforderungen nach dem Sozialgesetzbuch Neuntes Buch (Rehabilitation und Teilhabe behinderter Menschen) unterrichtet. Aufgrund der besonderen Situation, dass die Vertrauensleute besonders sensible Gesundheitsdaten über die Schwerbehinderten verarbeiten, ist mit dem Gesamtvertrauensmann der Schwerbehinderten vereinbart worden, den Ende Oktober 2002 neu gewählten Schwerbehindertenvertrauensleuten erst nach erfolgter Einarbeitungszeit in einer Versammlung die besonders zu beachtenden Datenschutzbestimmungen vorzutragen und mit ihnen zu erörtern.

5.7 Veröffentlichung von Personaldaten im Intranet

Eine im Sozialzentrum Mitte/Östliche Vorstadt Beschäftigte hat moniert, dass ein Dokument mit Änderungen ihres Arbeitsvertrages in das Verwaltungsnetz der Dienststelle eingestellt wurde, so dass dadurch alle dort Beschäftigten Kenntnis über die Maßnahme erlangen konnten.

Auf meine Anfrage hat die Dienststellenleitung erklärt, das Dokument sei durch einen Verfahrensfehler in einem nicht dafür vorgesehenen Laufwerk abgespeichert worden. Obwohl dieses Laufwerk öffentlich nicht zugänglich gewesen sei, konnte ein eingeschränkter Kreis von Behördenmitarbeitern das Dokument einsehen. Das Dokument ist dann unverzüglich aus dem Verwaltungsnetz entfernt worden.

5.8 Offener Versand von Rechnungen mit privaten Telefongebühren

Eine Eingabe wandte sich dagegen, dass der Bremer Baubetrieb Rechnungen über private Telefonkosten der Handys hausintern offen verschickte und die Rechnungen über mehrere Tage offen

in den Postfächern der betroffenen Beschäftigten liegen würden. Dadurch seien die darin enthaltenen privaten Gesprächsdaten für andere Kollegen des Betriebes einsehbar.

Aufgrund meiner Anfrage hat der Bremer Baubetrieb erklärt, die hausintern offene Versendung von Handyabrechnungen würde seit mehreren Jahren praktiziert und habe nie zu Beanstandungen geführt. Gleichwohl werde der Betrieb nunmehr das Fernmeldegeheimnis nach § 85 Telekommunikationsgesetz (TKG) einhalten, indem solche Schriftstücke nur noch in verschlossenen Umschlägen an die Mitarbeiter weitergereicht werden.

5.9 Vollständiger Vorname in E-Mail-Adresse

Eine Beschäftigte in der bremischen Verwaltung hat moniert, dass ihre E-Mail-Adresse aufgrund der neuen E-Mail-Richtlinien (BremABl. vom 07. März 2002, S. 223) nunmehr ihren vollständigen Vornamen enthält, obwohl bisher nur der Anfangsbuchstabe des Vornamens Bestandteil ihrer E-Mail-Adresse war. Sie habe zwar kein Problem, wenn die neue E-Mail-Adresse nur innerhalb ihrer Dienststelle verwendet wird. Da sie jedoch auch außerhalb ihrer Dienststelle und außerhalb der bremischen Verwaltung genutzt werden müsse, macht sie die Beeinträchtigung schutzwürdiger Interessen geltend, weil sie aus persönlichen Gründen ihren Vornamen auch nicht im öffentlichen Telefonbuch veröffentlicht habe.

Auch ich halte die obligatorische Aufnahme des vollständigen Vornamens in die E-Mail-Adresse nicht für erforderlich. Gleichwohl ist anlässlich der Beratungen zur neuen E-Mail-Richtlinie von seiten des Senators für Finanzen erklärt worden, die bisherige Angabe nur des Anfangsbuchstabens des Vornamens und des vollständigen Nachnamens hätte teilweise zu missverständlichen oder beleidigenden Namensbezügen bzw. Assoziationen geführt. Aus diesem Grunde sei die Angabe des vollständigen Vornamens in der E-Mail-Adresse erforderlich.

Unabhängig davon ist die E-Mail-Richtlinie im Lichte des § 93 Bremisches Beamtengesetz (BremBG) anzuwenden. Danach dürfen Beschäftigtendaten verarbeitet werden, soweit dies u. a. zur Durchführung organisatorischer Maßnahmen erforderlich ist und dadurch schutzwürdige Belange des Betroffenen nicht beeinträchtigt werden. Aufgrund der eingangs begründeten Beschwerde der Betroffenen werden insoweit schutzwürdige Belange beeinträchtigt.

Im Übrigen enthält das neue Bremische Datenschutzgesetz (BremDSG) ein Widerspruchsrecht in § 22 a BremDSG. Danach dürfen personenbezogene Daten nicht verarbeitet werden, soweit der Betroffene der Verarbeitung bei der verantwortlichen Stelle widerspricht und eine Prüfung ergibt, dass das schutzwürdige Interesse des Betroffenen wegen seiner besonderen persönlichen Situation das Interesse der verantwortlichen Stelle an dieser Verarbeitung überwiegt.

Ich habe der Beschwerdeführerin daher geraten, unter Hinweis auf die vorgenannten Rechtsvorschriften von ihrer Beschäftigungsdienststelle zu verlangen, dass ihre neue E-Mail-Adresse entsprechend umgestaltet wird. Zwischenzeitlich konnte ich bei der Dienststelle der Beschäftigten erreichen, dass nur der Anfangsbuchstabe des Vornamens mit dem Nachnamen verwendet wird.

6. Inneres

6.1 Videoüberwachung Bahnhofsvorplatz

"Bahnhofsvorplatz nun immer im Blick" titelte eine Bremer Tageszeitung. Anfang Oktober 2002 ging die polizeiliche Videoüberwachungsanlage auf dem Bahnhofsvorplatz in Bremen in Betrieb, ohne dass den datenschutzrechtlichen Anforderungen in ausreichendem Maße Rechnung getragen worden war. Weder war ich rechtzeitig über die Planungen zum Aufbau dieses automatisierten Informationssystems unterrichtet worden, noch hatte ich Möglichkeiten auf die Auswahl von Hard- und Software, die Installation oder die Datenübertragungswege Einfluss zu nehmen, kurzum bei der Vorbereitung, Inbetriebnahme und der weiteren Durchführung der Videoüberwachung auf dem Bahnhofsvorplatz in Bremen musste ich Verstöße gegen das Bremische Datenschutzgesetz und gegen die Bestimmungen des Polizeigesetzes feststellen.

Wäre eine Videoüberwachung tatsächlich nur mit dem Einsatz eines Fernrohrs durch einen Polizeibeamten vergleichbar, hätte ich mich nicht besonders beklagt. Ein solcher Vergleich hinkt aber, denn er verkennt nicht nur die technischen Möglichkeiten moderner Videoüberwachungsanlagen, sondern lässt auch die Auswirkungen einer Videoüberwachung außer Acht. Die installierte Überwachungsanlage hat nämlich ständig alle Personen im Blick, die sich im videoüberwachten Bereich aufhalten. Dabei wird nicht nur deren Anwesenheit an einer bestimmten Örtlichkeit registriert, sondern auch, wie sie sich dabei geben, wie sie gekleidet sind, was sie mit sich tragen und mit wem sie sich dort aufhalten und wie sie sich etwaigen Begleiterinnen oder Begleitern oder Dritten gegenüber verhalten. Auch kann festgestellt werden, welches Gebäude oder welches Geschäft sie betreten.

Die Videokamera selbst befindet sich an einem Mast der BSAG zwischen dem Hotel "Mercure" und den Straßenbahnhaltestellen. Sie ist als Videokamera für einen Laien nicht zu erkennen, da sie sich in einem kleinen zylindrischen Behälter von ca. 30 Zentimeter Durchmesser befinden, der in etwa fünf Metern Höhe angebracht ist. Die Videokamera auf dem Bahnhofsvorplatz kann vom Polizeipräsidium (Lagezentrum) aus gesteuert werden. Mit der Anlage lassen sich mit Hilfe eingebauter Zoom-Objektive Videobilder bis ins Detail vergrößern, wobei der Zoom-Bereich vom Herdentorsteinweg über die Kreuzung Bahnhofstraße bis hin zum Aufgang Überseemuseum reicht.

Und hiermit ist ein weiterer Mangel angesprochen. Hinweisschilder sollen den Bereich der Überwachung markieren und allen Bürgern klar machen, dass sie sich in dem beobachteten Bereich befinden. Die Anbringungsorte der Schilder, die Anbringungshöhe und die optische Gestaltung stellen dies in dem eben genannten Überwachungsbereich nicht ausreichend sicher. Die etwa DIN A3 großen Schilder in der Grundfarbe Dunkelblau sind schlecht zu lesen

und fallen im Erscheinungsbild nicht auf; man muss sie suchen. Die Schilder stehen zum Teil weit innerhalb des überwachten Bereichs, das Problem wird durch die eingefügten Bilder deutlich sichtbar. Die angebrachten Hinweisschilder erreichen damit nicht den vom Gesetz verlangten Zweck. Nach § 29 Abs. 3 BremPolG sollen die Hinweisschilder "deutlich sichtbar und erkennbar" sein. Sinn und Zweck ist es Straftäter abzuschrecken und den rechtschaffenden Bürger über seine mögliche Beobachtung zu informieren, damit er sein Verhalten darauf einstellen kann. Beide Ziele werden mit den jetzigen Hinweisschildern nicht erreicht.

Der Beobachtungsmonitor für die Videobilder steht im Polizeipräsidium in der Vahr, hier wird auch die Videoaufzeichnung durchgeführt; dies ermöglicht eine nachträgliche Auswertung einzelner Videosequenzen, es können auf CD-gebrannte Auszüge oder Ausdrucke gefertigt werden. Weil unterschiedslos sämtliche Personen, die in den Bereich der Videokamera kommen, erfasst und damit ganz überwiegend völlig unverdächtige Personen durch die Polizei ins Visier genommen werden, habe ich vorgeschlagen, zu prüfen ob nicht mit dem Einsatz moderner Software, die in der Lage ist, ähnlich wie bei Fernsehübertragungen aus Gerichtssälen vor den Verhandlungen, die Gesichter von Passanten zu verschleiern, die polizeilichen Zwecke gleichwohl erreicht werden könnten, denn eine solche Verschleierung kann dann zur Verfolgung von Straftaten nachträglich aufgehoben werden. Zu diesem Vorschlag erfolgte seitens der Polizei Bremen bisher keine Reaktion.

Angesichts der langen und kontroversen parlamentarischen Diskussion über die Einführung der Videoüberwachung für die Polizei wäre die Polizei Bremen gut beraten gewesen, sich frühzeitig mit meiner Dienststelle in Verbindung zu setzen und im Vorwege alle Datenschutzfragen zu klären, denn bei Inbetriebnahme einer technischen Anlage, die in das informationelle Selbstbestimmungsrecht der Betroffenen eingreift, müssen datenschutzrechtlichen Anforderungen bereits gewährleistet sein. Ein Datenschutzkonzept (Dateibeschreibung und indirektes Verzeichnis) lagen mir auch Ende 2002 nicht vor. Die geschilderten Mängel habe ich daher gegenüber dem Senator für Inneres, Kultur und Sport gem. § 29 BremDSG beanstandet und ihn zur Stellungnahme aufgefordert.

Perspektive Ausgang Hauptbahnhof Bremen - Südseite -

6.2 Rasterfahndung

Die Rasterfahndung war auch Ende 2002 noch nicht abgeschlossen. Mehrere Sequenzen von Datenabgleichen müssen noch beim Bundeskriminalamt (BKA) geführt werden. Ging ich noch im Frühjahr letzten Jahres davon aus, ich könnte noch vor der parlamentarischen Sommerpause in 2002 einen abschließenden Bericht abliefern, so muss ich jetzt davon ausgehen, dass dies wohl frühestens im Sommer 2003 erfolgen kann. Gleichwohl habe ich mich entschlossen, dem Senator für Inneres,

Kultur und Sport und dem Datenschutzausschuss einen Zwischenbericht zu erstatten, wesentliche Ergebnisse hieraus sollen an dieser Stelle wiedergegeben werden.

Nach den Anschlägen vom 11. September 2001 in den USA und der Verbindungslinie zu in Hamburg lebenden Terroristen, wurde bundesweit nach Hintermännern und sog. Schläfern gefahndet. Das Hauptproblem bestand bei der Suche darin, dass sich die Personen überwiegend völlig unauffällig verhalten hatten. Damit war plötzlich ein großer Personenkreis potentiell verdächtig. Die Innenminister sah in dem Instrument der Rasterfahndung das geeignete Mittel, weitere Anhaltspunkte zu gewinnen und Verdächtige zu verunsichern.

Die Polizei Bremen und die Ortspolizeibehörde Bremerhaven haben gegenüber den nachfolgend angegebenen Stellen Anordnungen erlassen, bestimmte Datensätze an die Polizei zu übermitteln. Die Anordnungen wurden vom Senator für Inneres, Kultur und Sport gebilligt.

- Stadtamt Bremen – Ausländeramt
- Stadtamt Bremen – Einwohnermeldeamt
- Bundesverwaltungsamt in Köln
- Hochschule Bremen
- Hochschule Bremerhaven
- Verwaltungspolizei Bremerhaven - Ausländeramt
- Internationale Universität Bremen
- Universität Bremen
- Handelskammer Bremen
- Industrie- und Handelskammer Bremerhaven
- Verwaltungspolizei Bremerhaven - Einwohnermeldeamt

In dem Datenabgleich wurden alle männlichen Personen im Alter von 18 bis 40 Jahren, die aus namentlich genannten, überwiegend arabischen Ländern stammen oder dort geboren sind und in der Bundesrepublik einen legalen Aufenthaltsstatus haben, einbezogen. Ich wurde über die Anordnungen, in der Regel nach einer Woche, längstens nach 23 Tagen, unterrichtet. Die von der Anordnung betroffenen Stellen haben ihre eigenen Datenbestände nach den vorgegebenen Rasterkriterien überwiegend selbst selektiert und das Ergebnis der Polizei zur Verfügung gestellt (Grunddatensätze). Lediglich die Handelskammer Bremen hat eine unselektierte Datei übergeben.

Bei der Polizei Bremen ist das K 61 mit der Durchführung der Maßnahme betraut. Das K 61 beauftragte die ID Bremen GmbH mit dem Abgleich der angelieferten Daten auf Landesebene. In den Datenabgleich wurden rund 90.000 Datensätze aus dem Ausländerzentralregister und 10.000 Datensätze aus den Bereichen der anderen genannten Stellen einbezogen.

Die Ergebnisse des Datenabgleichs bei der ID Bremen GmbH wurden von K 61 in einer separaten Arbeitsdatei gespeichert. Im Februar 2002 befanden sich 589 Datensätze in dieser Datei, Anfang Januar 2003 sind es 664 Datensätze, weil einige Datensätze noch aus anderen Ländern hinzugekommen sind. K 61 hat diese Datensätze zum Abgleich mit den Datensätzen aus anderen Bundesländern an das BKA übermittelt. In der Verbunddatei beim BKA sollen etwa 28.000 Personendatensätze gespeichert sein, davon stammen knapp 600, also rund 2,15 Prozent aus Bremen. Beim BKA werden in verschiedenen Datenläufen Datenabgleiche mit anderen Dateien durchgeführt. Nach Abschluss der jeweiligen Datenabgleiche beim BKA sind die Ergebnisse von dort

an K 61 übermittelt worden. Bis Anfang Januar 2003, nach Bearbeitung der 10. Abgleichsserie beim BKA, hatte K 61 weit über 200 Fälle von Namensidentitäten festgestellt, in der Nachbearbeitung blieben dann insgesamt 18 Personenidentitäten, die als Verdachtsfälle jetzt mit konventionellen polizeilichen Methoden weiter bearbeitet werden.

Die Löschung der Grunddatensätze oder die Vernichtung der Datenträger der meisten der eingangs genannten Stellen ist zwischenzeitlich erfolgt. Auch bisher als überschüssig festgestellte Daten aus den Abgleichen bei der Polizei wurden von K 61 gelöscht. Die Löschung der rund 600 in Bremen erstellten Datensätze kann beim BKA, wie bei K 61 (natürlich mit Ausnahme der Verdachtsfälle) nach Ende der Abgleichsserien beim BKA erfolgen.

Die Durchführung der Rasterfahndung wurde zwischenzeitlich gerichtlich überprüft, das OVG Bremen hat am 08.07.2002 einen Beschluss gefasst, dessen Leitsätze lauten:

- § 36 i BremPolG, der die Durchführung einer präventiv-polizeilichen Rasterfahndung erlaubt, ist mit höherrangigem Recht vereinbar.
- Die am 11. September 2001 in den USA erfolgten Terroranschläge rechtfertigen es, eine präventiv-polizeiliche Rasterfahndung durchzuführen.
- Soweit ein Bundesland aus der Rasterfahndung gewonnene Personendaten an das BKA liefert, trägt es die datenschutzrechtliche Verantwortung dafür, dass der dort durchgeführte weitere Datenabgleich rechtmäßig erfolgt. Der beim BKA durchgeführte Datenabgleich muss jedenfalls nach Abschluss der Maßnahme gegenüber dem Betroffenen transparent gemacht werden können.

Ich habe bei beteiligten Stellen mehrere Prüfungen durchgeführt. Meine datenschutzrechtliche Stellungnahme basiert im Wesentlichen auf der spezialgesetzlichen Regelung des § 36 i BremPolG, welche die Rasterfahndung regelt.

Ich habe festgestellt, dass die polizeilichen Anordnungen nicht in ausreichender Form die vom Gesetz geforderten Erwägungen wiedergeben, sie sind daher in mehrerer Hinsicht mangelbehaftet. Dies gilt sowohl hinsichtlich der Begründung einzelner Raster-Merkmale, wie auch hinsichtlich der Erforderlichkeit, der Geeignetheit und Verhältnismäßigkeit der Maßnahme, auch wenn sie nunmehr durch die gerichtliche Entscheidung bestätigt wurde. Eine erforderliche Anordnung zu Verwendung der nach § 29 d Luftverkehrsgesetz erhobenen Daten im Rahmen der Zuverlässigkeitsprüfung fehlt.

Auch die Frist, in der ich über die Anordnungen unterrichtet wurde, entspricht nicht dem Gesetz. § 36 i Abs. 3 BremPolG sieht meine unverzügliche Unterrichtung vor. Nur so kann verhindert werden, dass meine Kontrollrechte nicht leer laufen.

Die Regelung zur Rasterfahndung in § 98 b StPO sieht eine richterliche Kontrolle vor. Bei der Gesetzgebungsberatung des § 36 i BremPolG wurde vehement um die Einführung einer richterlichen Kontrolle der Anordnung einer Rasterfahndungsmaßnahme gestritten. Der Verzicht, so wurde seinerzeit argumentiert, werde mit der gleichwertigen und effektiveren Kontrolle durch Parlamentarische Kontrollkommission (PKK) und des Landesbeauftragten für den Datenschutz nicht nur kompensiert, sondern sogar verbessert. Dies hätte ich für meine Rolle allenfalls bestätigen

können, wenn mir auch tatsächlich die Möglichkeit gegeben worden wäre, die verschiedenen Datenverarbeitungsschritte des Verfahrens vorab zu beeinflussen. Meine personellen Kapazitäten erlauben es nicht, mich ständig nach dem Verfahrensstand und den nächsten geplanten Schritten zu erkundigen. Durch eine bessere Unterrichtung über die jeweils nächsten Schritte durch die Polizei Bremen hätten sicherlich einige Fehler, so z. B. bei der Datenverarbeitung im Auftrag vermieden werden können.

Auch die vorgenannte unselektierte Datenübermittlung an K 61 entsprach nicht den rechtlichen Regelungen, ich habe daher empfohlen die verpflichteten Stellen schon mit der Anordnung anzuhalten, dass sie vorrangig nur bestimmte Datensätze entsprechend den festgelegten Rasterkriterien liefern sollen. Auch der Auftrag an die ID Bremen GmbH zur Zusammenführung der Daten ist rechtlich mangelbehaftet, er entspricht nicht den Vorgaben von § 9 BrDSG zur Auftragsdatenverarbeitung.

Schließlich habe ich die Rückgabe der Daten an die anliefernden Stellen problematisiert, weil diese Stellen die Daten nur für Zwecke der Rasterfahndung zusammengestellt haben und daher unter keinen rechtlichen Gesichtspunkten diese Rasterdaten selber für andere Zwecke weiterverarbeiten dürfen.

Ich habe meinen Prüfbericht mit einer Reihe von Vorschlägen zur Verbesserung des Datenschutzes bei der Rasterfahndung versehen.

Anzumerken ist, dass Bremen gut daran getan hat, zunächst die Rechtsgrundlage abzuwarten, bevor die öffentlichen Stellen durch Anordnung gezwungen wurden, die geforderten Daten für die Rasterfahndung an die Polizei zu übermitteln. So wurden leidvolle Erfahrungen, die andere Länder machten, vermieden. Aus der jetzigen Sicht relativiert sich auch die Hektik, mit der damals auch in Bremen versucht wurde, vorab Rasterdaten zu erhalten, sind doch die Datenläufe beim BKA auch jetzt, 16 Monate später, immer noch nicht abgeschlossen. Und gerade erst aus dieser Datenverarbeitung beim BKA werden die “Verdachtsfälle” gewonnen. Ein von Bremen sicherlich nicht zu verantwortender Missstand, der nicht nur unter sicherheitspolitischen Gesichtspunkten anzuprangern ist, sondern der Umstand führt auch dazu, dass das informationelle Selbstbestimmungsrecht der meisten der davon betroffenen Personen ungebührlich lange beeinträchtigt wird, denn ihre Daten sollen auch in Bremen erst gelöscht werden, wenn alle Abgleichsserien beim BKA abgeschlossen sind.

Es hat sich gezeigt, dass im Land Bremen große Datenbestände (100.000 Datensätze) durchgearbeitet werden mussten, um 589 Datensätze herauszufiltern. Ob diese so gewonnenen Datensätze Betroffener hinreichende Ermittlungsansätze bieten werden, ist fraglich. Dies zeigt, dass neben der ökonomischen Betrachtung polizeilicher Arbeit es fraglich ist, ob eine solche bundesweit angelegte Maßnahme auf derart fragwürdigem Fundament den Eingriff in die verfassungsrechtlich geschützten Rechte Unzähliger rechtfertigen.

In jedem Fall bedarf es aber nach Abschluss der Maßnahmen und der Ermittlungen einer Evaluierung des Verfahrens der Rasterfahndung. Es scheint, dass bei der ”Rasterfahndung Terroranschlag USA” mit Hilfe des Instruments der Rasterfahndung keine konkreten Verdachtsfälle aufgedeckt werden

konnten, auf die die Polizei nicht auch ohne die Rasterfahndung gestoßen wäre. Gleichwohl wäre selbst diese Ergebnis kein generelles Argument gegen den Einsatz der Rasterfahndung schlechthin. Es bedarf daher genauerer wissenschaftlicher Untersuchungen.

Ich werde bis zum Abschluss der Rasterfahndung und der sich daran anschließenden Maßnahmen bei meinen begleitenden Prüfungen mein besonderes Augenmerk darauf richten, dass zu Unrecht in Verdacht geratene Personen umfassend rehabilitiert werden, und es dürfen an keiner Stelle Datenschatten zu diesen Personen verbleiben, die bei anderen Anlässen später zu Beeinträchtigungen führen können.

6.3 Abschiebungsgewahrsam bei der Polizei Bremen

Auf Grund des Gesetzes über den Abschiebungsgewahrsam vom 4. Dezember 2001 hat der Senator für Inneres, Kultur und Sport den Erlass über die Durchführung der Abschiebungshaft in Gewahrsamseinrichtungen des Polizeivollzugsdienstes (Gewahrsamsordnung) vom 6. Juni 2002 und die Ausführungsvorschrift zu § 11 Abs. 2 des Gesetzes über den Abschiebungsgewahrsam herausgegeben. Zu den Entwürfen dieser Regelungen habe ich im Frühjahr 2002 jeweils Stellung genommen.

Ende September 2002 fand eine Prüfung des Polizeigewahrsams der Polizei Bremen (PGW) statt. Diese Prüfung hatte zum Anlass, die Umsetzung dieser Regelungen zu prüfen und Probleme, die vor Ort auftreten, zu erkennen bzw. aufzuarbeiten. Es war erkennbar, dass die Mitarbeiter des Abschiebungsgewahrsams eine datenschutzgerechte Verarbeitung der Daten gewährleisten wollen.

Geprüft habe ich das Verfahren im Abschiebungsgewahrsam, insbesondere die Erhebung, Speicherung, Löschung und Weiterleitung von personenbezogenen Daten der Abschiebungshäftlinge.

Den Antrag auf Aufnahme einer Person in den Abschiebungsgewahrsam stellt die Ausländerbehörde. Dieser Antrag wird nur vollziehbar, wenn der zuständige Richter diesem zustimmt, d. h., einen entsprechenden richterlichen Beschluss erlässt. Wird der Betroffene aus anderen Gründen (Festnahme auf Grund einer Straftat) in Polizeigewahrsam genommen, so bedarf es gleichwohl eines Beschlusses für die Überführung in den Abschiebungsgewahrsam. Über jede Gewahrsamsnahme wird ein Protokoll (Aufnahmeschein/Laufzettel) gefertigt.

Dieser Aufnahmeschein/Laufzettel verbleibt für die Dauer der Gewahrsamsnahme in einem sogenannten Zellenfach (für jede Zelle gibt es ein Regalfach) auf der Wache des Polizeigewahrsams. Neben den Angaben über Name, Vorname, Geburtsdatum und Geburtsort sowie (bisherige) Anschrift - soweit vorhanden/bekannt - werden festgehalten: Datum und Uhrzeit der Festnahme, der Grund der Festnahme und der Veranlasser der Festnahme. Zusätzlich wird vermerkt, ob und welche Gegenstände abgenommen und in Verwahrung genommen wurden. Die abgenommenen Gegenstände (Messer, Scheren u. ä.) gemäß Ziffer 2.8.1 der Gewahrsamsordnung werden im Zellenfach und die auf Wunsch des Abschiebungshäftlings verwahrten Wertgegenstände bzw. Geld werden im Wertschrank gesichert verschlossen.

Die Grunddaten aus dem Aufnahmeschein/Laufzettel (Name, Vorname, laufende Nr., Zelle, Aufnahmedatum und Datum des Endes der Sicherungshaft) werden in das

Gewahrsamsbuch/Aufnahmebuch übernommen. Es dient dem lückenlosen Nachweis der Inhaftierten. Es werden auch die im Polizeigewahrsam befindlichen Personen erfasst.

In das Übergabebuch werden alle wichtigen Hinweise, die Häftlinge, die Zelle oder technische Mängel betreffen, eingetragen. Die Eintragungen betrafen z. B. Besuch beim Zahnarzt, Defekt einer Sprechanlage oder Klingel sowie Ausgabe von bestimmten Medikamenten zu einer bestimmten Zeit. Das Übergabebuch dient der Unterrichtung des/der nächstfolgenden Wachteams.

In das Besucherbuch werden alle Besucher von Häftlingen eingetragen. Es wird vermerkt der Name und Vorname des Besuchers, seine Adresse sowie der Name der besuchten Person. Die Besuche sind ca. 30 Minuten vorher anzumelden und werden vom Wachpersonal zeitlich zugeteilt. Die Besucher werden gemäß Ziffer 3.12 der Gewahrsamsordnung behandelt, d. h. die Besucher und die mitgebrachten Sachen werden regelmäßig durchsucht. Der Besuch von Rechtsanwälten wird nicht kontigentiert und auch nicht überwacht.

Nach Entlassung eines Abschiebungshäftlings werden die Aufzeichnungen über den Abschiebungshäftling zur Abrechnungsstelle (innerhalb des Polizeigewahrsams) gegeben, die Rechnung für den Kostenträger (zuständige Ausländerbehörde) erstellt und die Unterlagen (Aufnahmeschein/Laufzettel, richterlicher Beschluss usw.) als begründende Unterlagen der Kopie der Rechnung beigefügt. Diese Unterlagen werden zur Zeit 10 Jahre im PGW aufbewahrt.

Außer kleinen Handhabungsfehlern - die mit der Polizei noch aufgearbeitet werden müssen - (z. B. veraltete Formulare, die keine hinreichende Aufklärung der Betroffenen gewährleisten oder die Kennzeichnung der Haftfähigkeit der Gewahrsamsperson, ebenso muss noch ein Verfahren entwickelt werden, wie die Abrechnungsunterlagen gesperrt und früher gelöscht werden) wurde festgestellt, dass die Mitarbeiter im Abschiebungsgewahrsam bemüht sind, die Rechte der Abschiebungshäftlinge zu wahren.

Es wurde mitgeteilt, dass eine Sozialarbeiterin beim Senator für Inneres, Kultur und Sport eingestellt wird, die sich um die persönlichen Belange der Abschiebungshäftlinge kümmern soll.

6.4 EVA-HB

Im letzten Jahr berichtete ich umfassend über die Konzeptionsarbeiten zu einem neuen elektronischen Vorgangsbearbeitungssystem (EVA) für die Polizei im Lande Bremen (vgl. 24. JB, Ziff. 6.6), dass das bisherige ISA-D-Verfahren ablösen soll. Die Einführung des Systems war für den Sommer 2002 vorgesehen. Dieser Termin konnte nicht gehalten werden, die Einführung wurde auf Ende 2002 verschoben. Ende des Jahres stellte sich dann heraus, dass auch zu diesem Zeitpunkt das System nicht in Betrieb genommen werden konnte, weil die Integration der Altdaten aus dem bisherigen ISA-D-System (sog. Migration) nicht vollständig gelungen war. Jetzt wird mit einer Inbetriebnahme im Frühjahr 2003 gerechnet. Ich hoffe nicht, dass sich die leidvollen Erfahrungen der Polizei anderer Länder in Bremen wiederholen.

Datenschutz kann in solchen Systemen nur gewährleistet werden, wenn die einzelnen Nutzer eines solchen Systems hinreichend sicher damit umgehen können. Ich habe deshalb immer wieder darauf gedrungen, die Polizeibeamten rechtzeitig zu schulen. Die Schulungen der Mitarbeiter der Polizei

wurden im Laufe des Berichtsjahres vorgenommen. Dabei traten noch einige datenschutzrechtliche Fragen auf,deren ich mich weiter annehme.

6.5 Projekt INPOL-Land

Anlässlich einer Sitzung des Datenschutzausschusses der Bremischen Bürgerschaft im Dezember 2002 erfuhr ich beiläufig, dass die Beschaffung von Hard- und Software für ein DV-Verfahren „INPOL-Land“ abgeschlossen bzw. kurz vor dem Abschluss sei, dass die ersten Tests unmittelbar bevorstünden sowie die Migration der Altdaten aus ISA in das neue „INPOL-Land“ vorbereitet und getestet würde.

Über dieses Vorhaben bin ich entgegen der eindeutigen Bestimmung in § 27 Abs. 3 Bremisches Datenschutzgesetz nicht ordnungsgemäß unterrichtet worden, obwohl ich rechtzeitig über Planungen zum Aufbau automatisierter Informationssysteme, mit denen personenbezogene Daten verarbeitet werden sollen, unterrichtet werden muss. Das habe ich sowohl dem Senator für Inneres, Kultur und Sport als auch dem Polizeipräsidenten der Polizei Bremen mitgeteilt. Daraufhin erhielt ich eine mündliche Zusage, mich zu beteiligen. Weiteres ist aber bisher nicht geschehen.

Es ist mir unverständlich, dass ich über ein solch wichtiges DV-Verfahren der Polizei nicht frühzeitig und umfassend unterrichtet werde. Nur wenn ich die Gelegenheit habe, frühzeitig die datenschutzrechtlichen Aspekte geltend zu machen, kann es gelingen, die datenschutzgerechte Ausgestaltung eines solchen Systems sicherzustellen. Nachträgliche Anpassungen gestalten sich in der Regel schwieriger und sind meistens kostenintensiver.

Wie ich bereits berichtet hatte (vgl. 24. JB, Ziff. 6.6), gab und gibt es erhebliche Probleme, den Polizeien ein modernes, leistungsfähiges DV-System zur Aufgabenerfüllung zur Verfügung zu stellen. Nachdem lange Zeit geplant war, für interessierte Länder das INPOL-System des Bundes im Wege der Datenverarbeitung im Auftrag auch den Ländern zur Verfügung zu stellen, ist der Bund von dieser Zusage abgerückt. Im Gegenzug hat der Bund diesen Ländern die Nutzung der INPOL-Software auf ihren eigenen DV-Systemen angeboten. Dieses angepasste „INPOL-Land“-System soll einerseits die Datenhaltung für das Land im Bereich der Kriminalpolizei ermöglichen und gleichzeitig als Übermittlungssoftware für die Dateneingabe und den Datenabruf aus dem INPOL-System des Bundeskriminalamtes dienen.

6.6 DNA-Analyse bei der Polizei Bremen

Ich hatte berichtet, dass die Einwilligungserklärung und die Belehrung der Betroffenen bei der freiwilligen Entnahme von DNA-Material datenschutzrechtlichen Anforderungen nicht genügte (vgl. 23. JB, Ziff. 6.1.1). Der Datenschutzausschuss der Bremischen Bürgerschaft hatte der Polizei Bremen und dem LfD aufgegeben, eine einvernehmliche Lösung herbeizuführen (vgl. 24. JB, Ziff. 4.1).

Ich habe die Polizei in der Angelegenheit mehrfach beraten. Ende September 2002 wurde mir mitgeteilt, dass meine Anregungen akzeptiert würden. Mitte Oktober wurde mir der neue Vordruck übersandt; er entspricht jetzt datenschutzrechtlichen Anforderungen.

Nicht zu verwechseln ist die Entnahme von DNA-Material mit der daran anschließenden Untersuchung und Einspeicherung der personenbezogenen Daten in polizeiliche Dateien beim BKA. Hier bleibt es weiterhin dabei, - und dies hat die Polizei Bremen mir noch einmal bestätigt – dass im eigenen Aufgabenbereich spätestens vor der Untersuchung des DNA-Materials eine richterliche Anordnung herbeigeführt wird.

6.7 City-Server

Durch eine Vorlage zu einer Deputationssitzung erhielt ich im November 2002 davon Kenntnis, dass der Senator für Inneres, Kultur und Sport insbesondere mit den Ortsämtern sich dafür interessiert, dass in der Stadtgemeinde Bremen ein sog. City-Server eingerichtet wird.

Der City-Server wird digitale Aufnahmen von allen Straßenzügen in Bremen mit den darin befindlichen Häusern, jeweils als Straßenansicht enthalten. Verbunden sind diese Aufnahmen mit der Angabe geostationärer Punkte, der Angabe des Straßennamens und der Blickrichtung der Aufnahme als Himmelsrichtung sowie dem Aufnahmedatum. Praktisch ist es so, dass im City-Server einzelnen Fotos vergleichbare Bilder abgelegt werden, so als wenn ein Fotograf entlang einer Straße alle fünf oder zehn Meter ein Foto machen würde.

Der City-Server soll in vielen Fällen (Planung von Veränderungen im Straßenraum, Stellungnahme zu Bauanträgen usw.) eine Besichtigung vor Ort erübrigen.

Der genannten Deputationsvorlage war nicht zu entnehmen, dass die senatorische Behörde sich Gedanken um den Datenschutz bei Einsatz eines solchen Produktes gemacht hat.

Mit Schreiben vom 19. November 2002 habe ich den Senator für Inneres, Kultur und Sport auf evtl. zu prüfende datenschutzrechtliche Belange aufmerksam gemacht. Beigefügt war das Protokoll der Beratungen des Datenschutzausschusses aus dem Jahre 1999, in dem dieses Verfahren als datenschutzrechtlich nicht unproblematisch eingestuft wird.

Beschaffung und Einsatz des Produktes werden vom Innensenator weiter betrieben, ohne das die aufgeworfenen datenschutzrechtlichen Fragen geklärt sind. Der Senator für Inneres, Kultur und Sport hat zugesagt, mich über den City-Server umfassend zu unterrichten und die Übersendung einer Demo-CD angekündigt. Weder Unterlagen noch die Demo-CD sind bisher bei mir eingetroffen.

Soweit der City-Server für die Belange der Polizei, der Feuerwehr und für Planungsbehörden eingesetzt werden soll, bestehen sicher keine durchgreifenden datenschutzrechtlichen Bedenken gegen den Einsatz des City-Servers, wenn die organisatorischen und technischen Maßnahmen nach §§ 7 und 8 BremDSG getroffen werden. Erhebliche Bedenken bestehen jedoch, wenn nicht öffentliche Stellen (z. B. Makler) oder Privatpersonen auf die Bilddaten beliebig zugreifen können.

6.8 Polizeicomputer vergisst Hilflosigkeit nicht

Von einem großen Krankenhaus erging vor Jahren ein Hilfeersuchen an die Polizei, weil eine Patientin es verlassen hatte und die Gefahr bestand, dass sie hilflos umher irrte. Dieses Hilfeersuchen mit den personenbezogenen Daten der Patientin wurde in dem System ISA gespeichert.

Schon wenige Stunden nach dem Hilfeersuchen des Krankenhauses war die Patientin wieder in der Obhut des Krankenhauses und dieses hatte ordnungsgemäß die Rückkehr der Patientin der Polizei gemeldet. Auch dieses ist bei der Polizei in den DV-Systemen vermerkt worden.

Die Patientin war zwischenzeitlich als geheilt entlassen worden. Nunmehr erhielt sie bei einem Kontakt mit der Polizei davon Kenntnis, dass sie in den polizeilichen Systemen mit dem Merkmal „hilflos“ gespeichert ist. Darüber war sie sehr verwundert, denn einerseits war die Meldung des Krankenhauses sehr lange her und andererseits hatte sie nie die Hilfe der Polizei erhalten.

Bei meiner Prüfung dieses Vorgangs konnte ich feststellen, dass die Frau tatsächlich mit dem Merkmal „hilflos“ im Polizeicomputer gespeichert war, der gesamte Datensatz wurde umgehend gelöscht. Der Vorgang zeigt, dass Informationssysteme als Unterstützungssysteme für die Polizeiarbeit hilfreich sein können, aber sie müssen auch gepflegt werden und Daten, die für eine Hilfeleistung nicht mehr benötigt werden, sind dann auch zu löschen.

6.9 Bürger-Service-Center

Anfang Dezember 2002 hat das neue Bürger-Service-Center (BSC) seinen Betrieb aufgenommen. Zu dem Gesamtkonzept habe ich Stellung genommen (vgl. 24. JB, Ziff. 6.9). Zur Zeit gibt es keine wesentlichen Änderungen, da weder Datenverarbeitungsverfahren zum Einsatz kommen, die die verschiedenen angebotenen DV-Anwendungen zusammenfassen, noch ist das organisatorische Konzept geändert worden. Anwendungen, die unter ein besonderes Berufs- oder Amtsgeheimnis fallen, werden grundsätzlich getrennt von den allgemeinen Anwendungen des Stadtamtes und hier von besonderen Mitarbeiterinnen/Mitarbeitern durchgeführt. Allerdings werden die Mitarbeiterinnen und Mitarbeiter des BSC für alle Aufgaben (Ausnahme: Steuerverfahren) ausgebildet. Die Zuweisung der Beschäftigten zu dem jeweiligen Einsatzbereich wird je nach Arbeitsanfall durch die Leitung des BSC vorgenommen. Nach einer Anlaufphase beabsichtige ich, beim BSC zu prüfen, ob die verabredeten Vorgaben eingehalten werden.

6.10 Kampfhundedaten an die Steuerbehörde

Im Berichtsjahr bat mich das Stadtamt Bremen um datenschutzrechtliche Beratung. Das Stadtamt war von der Steuerbehörde Finanzamt Bremen-Mitte, zuständig für die Festsetzung der Hundesteuer, gebeten worden, die Daten der Kampfhundehalter für die Jahre 2000 bis 2002, die das Stadtamt Bremen auf Grund der Vorschriften über das Führen gefährlicher Hunde (Kampfhunde) erhoben hat, zu übermitteln. Das Stadtamt Bremen war sich nicht sicher, ob eine solche Übermittlung zulässig sei.

Die Steuerbehörde hielt die Übermittlung gemäß §§ 12 und 13 BrDSG für zulässig, weil sonst das Festsetzen der Hundesteuer nicht möglich sei und damit erhebliche Nachteile für das Gemeinwohl eintreten würden.

In meiner Stellungnahme habe ich darauf hingewiesen, dass die Datenerhebungsregelungen im Steuerrecht (Abgabenordnung und bremisches Abgabengesetz) abschließend sind. Danach käme als Datenübermittlungsvorschrift § 93 AO in Betracht. Diese Vorschrift setzt jedoch voraus, dass dem Auskunftspflichtigen, in diesem Fall also dem Stadtamt, von der Steuerbehörde mitgeteilt werden

muss, zu welchem Steuerpflichtigen ihr Mitteilung gemacht werden soll. Ein Auskunftsrecht praktisch zu einer Vielzahl von Steuerpflichtigen steht ihr nach dieser Vorschrift nicht zu. Eine solche allgemeine Ermittlungsregelung ergibt sich zwar aus § 208 AO, aber dieses Recht steht allein der Steuerfahndung zur Verfügung.

Ich habe deshalb darauf hingewiesen, dass eine Übermittlung der Daten der Kampfhundehalter nach geltendem Recht nicht zulässig ist.

6.11 Beratung des Gesetzes über den Verfassungsschutz in Bremen

Im Frühjahr 2002 übersandte der Senator für Inneres, Kultur und Sport einen Entwurf zur Novellierung des Gesetzes über den Verfassungsschutz im Lande Bremen. Der Entwurf sieht wesentliche Erweiterungen der Befugnisse des Landesamtes für Verfassungsschutz Bremen vor. So sollen die Datenerhebungsregelungen stark erweitert werden, so dass der Verfassungsschutz in Zukunft umfassende Auskünfte von Kreditinstituten, Finanzdienstleistungsinstituten und Finanzunternehmen verlangen kann. Ferner soll er wesentliche Auskunftsrechte gegenüber Postdienstunternehmen und Telekommunikationsunternehmen erhalten. Danach wären diese Unternehmen u. a. verpflichtet, Auskunft zu Berechtigungskennungen, Kartennummern, Standortkennungen sowie Rufnummern oder Kennung von anrufenden und angerufenen Telekommunikationspartnern zu erteilen.

Es soll dem Verfassungsschutz erlaubt werden, durch technische Mittel (z. B. Sprach- oder/und Videoübertragung) im Bereich des Hausrechtes (Artikel 13 Grundgesetz) Daten zu erheben. Weiter sollen andere Behörden verpflichtet werden, den Verfassungsschutz bei Tarnmaßnahmen zu unterstützen. Auch soll die Befugnis zur Datenverarbeitung über Jugendliche erweitert werden. Ferner sieht der Gesetzesentwurf bereichsspezifische Regelungen zur Datenverarbeitung vor, obwohl diese abschließend im Bremischen Datenschutzgesetz beschrieben sind.

Ein Teil der vorgeschlagenen Regelungen zieht mit den Regelungen im Terrorismusbekämpfungsgesetz für das Bundesamt für Verfassungsschutz gleich, in vielen Bereichen geht der Gesetzentwurf aber noch darüber hinaus. Ich habe zu dem Entwurf am 19. April 2002 eine Stellungnahme abgegeben. Dabei habe ich deutlich gemacht, dass eine Erweiterung der Befugnisse des Verfassungsschutzes immer zugleich eine erweiterte Befugnis zum Eingriff in das informationelle Selbstbestimmungsrecht der Bürger mit sich bringt. Eine Erweiterung der Befugnisse ist daher nur unter den vom Bundesverfassungsgericht festgelegten Bedingungen zulässig. Der Gesetzgeber ist dabei beweispflichtig dafür, dass die vorgeschlagenen Änderungen erforderlich, angemessen, verhältnismäßig sind und im überwiegenden Interesse liegen. Gerade bei einem Geheimdienst, wie es der Verfassungsschutz ist, muss der Gesetzgeber besonders sorgfältig die Rechte der Bürger schützen, denn viele der normalen datenschutzrechtlichen Schutzregelungen, wie z. B. Auskunfts- und Akteneinsichtsrechte, gelten gegenüber dem Verfassungsschutz nur sehr eingeschränkt.

Eine Antwort auf meine Stellungnahme erhielt ich vom Senator für Inneres, Kultur und Sport am 8. August 2002. Diese beiden Schriftsätze sollen nun als Gesprächsgrundlage dienen. Ein Gespräch wird voraussichtlich erst Anfang 2003 stattfinden.

6.12 Meldewesen

6.12.1 Änderung der bremischen Meldedatenübermittlungsverordnung

In 2002 befasste ich mich erneut mit mehreren Entwürfen zur Änderung der bremischen Meldedatenübermittlungsverordnung, die mir der Senator für Inneres, Kultur und Sport übersandt hatte. Geplant ist derzeit u. a. die Einrichtung von Online-Zugriffen auf das Einwohnermelderegister durch die Amtsgerichte Bremen, Bremen-Blumenthal und Bremerhaven sowie das Landgericht Bremen. Die Online-Zugriffe sollen den Gerichten für Zwecke der Ermittlung von Amts wegen für in Rechtsangelegenheiten anhängige Verfahren sowie im Rahmen des Erbschein- und Testamenteröffnungsverfahrens und im Rahmen der Nachlasssicherung gewährt werden. In meiner Stellungnahme zu den geplanten Online-Zugriffen habe ich u. a. eine Protokollierung der einzelnen Zugriffe unter Angabe des jeweiligen Verfahrensaktenzeichens und der TCP-IP-Adresse sowie der Benutzerkennung zur Voraussetzung für die Gewährung der Online-Zugriffe gemacht. Der Senator für Justiz und Verfassung hat mir mitgeteilt, dass gegen eine Umsetzung dieser Forderung durch die Gerichte aus seiner Sicht keine Bedenken bestehen.

Eine weitere Änderung der bremischen Meldedatenübermittlungsverordnung hat sich im Berichtszeitraum hinsichtlich der Aufnahme des § 12 Abs. 3 ergeben. Danach werden dem Jugendamt Bremen zum Zwecke der Steuerung der Vergabe von Kindergartenplätzen an alle Kinder, die einen Rechtsanspruch auf den Besuch eines Kindergartens von ihrem vollendeten 3. Lebensjahr an bis zum Schuleintritt haben, jährlich zum 30. November aus dem Melderegister der Meldebehörde der Stadtgemeinde Bremen die vollständigen Namen, Geburtstage, gesetzlichen Vertreter und Anschriften mit Ortsteilnummer und Wohnungsstatus übermittelt. Auch hierzu habe ich eine datenschutzrechtliche Stellungnahme abgegeben.

Daneben bestehen Überlegungen, u. a. auch die Einrichtung von Online-Zugriffen für die Bremer und Bremerhavener Entsorgungsbetriebe und für die für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach dem Abfallrecht zuständigen Behörden der Stadtgemeinden Bremen und Bremerhaven. Den Bremer und Bremerhavener Entsorgungsbetrieben soll es damit ermöglicht werden, für die Wahrnehmung ihrer Aufgaben im Rahmen der Abfall-Behälter-Ausstattung nach den Abfallortsgesetzen und der darauf basierenden Gebührenfestsetzung der Abfallgebühren die Anzahl der unter einer Adresse gemeldeten Personen sowie für Zwecke der Erhebung von Gebühren die vollständigen Namen, Adressen, Geburts- und Sterbedaten und bei einem Umzug die neue Adresse des Betroffenen zu erhalten.

Der beabsichtigte Online-Zugriff auf die Meldedaten ist nach meiner Auffassung weder geeignet noch erforderlich. Nach den von den Bremer und Bremerhavener Entsorgungsbetrieben zu beachtenden Rechtsvorschriften dürfen die Entsorgungsbetriebe für die Erfüllung ihrer Aufgaben nur Daten über die Eigentümer von Grundstücken, auf denen Abfälle anfallen, verarbeiten. Aus dem Einwohnermelderegister können keine Auskünfte, ob eine gemeldete Person Grundstückseigentümer ist, bezogen werden. Nur mit Hilfe eines speziellen Programms könnte aus dem Melderegister die Anzahl der unter einer Adresse gemeldeten Personen ermittelt und in einer besonderen Aufbereitung

verfügbar gemacht werden. Da der beabsichtigte Online-Zugriff vom Senator für Bau und Umwelt beantragt wurde, soll dieser zunächst mit diesem näher erörtert werden.

Darüber hinaus soll den für die Verfolgung und Ahndung von Ordnungswidrigkeiten nach Abfallrecht zuständigen Behörden der Stadtgemeinden Bremen und Bremerhaven online die vollständigen Namen, Anschriften, Einzugs- und das Geburtsdatum sowie das Geschlecht des jeweils Betroffenen für die Wahrnehmung der genannten Aufgabe zur Verfügung gestellt werden. Eine für die Erforderlichkeit und Verhältnismäßigkeit des Online-Zugriffs ausreichende Begründung fehlt bisher. Auch dieser Punkt wird daher Gegenstand der genannten Besprechung sein.

6.12.2 Erteilung von Sammelauskünften durch die Meldebehörde Bremen

Von der Meldebehörde Bremen können nach § 32 bremisches Meldegesetz (BremMeldG) verschiedene Auskünfte aus dem Einwohnermelderegister auch an Personen, die nicht Betroffene sind, und andere als die in § 30 Abs. 1 BremMeldG bezeichneten öffentlichen Stellen erteilt werden. Während sich der Datenkatalog bei der einfachen Melderegisterauskunft nach § 32 Abs. 1 BremMeldG auf Vor- und Familiennamen, akademische Grade und Anschriften beschränkt, können bei der erweiterten Melderegisterauskunft nach § 32 Abs. 2 BremMeldG zusätzliche Angaben, wie z. B. Geburts- und Sterbedaten, Familienstand, frühere Namen und Anschriften sowie die Staatsangehörigkeit, beauskunftet werden. Hiervon zu unterscheiden sind die nach § 32 Abs. 3 BremMeldG von den Meldebehörden erteilten Gruppenauskünfte.

Im Hinblick hierauf hat die bremische Meldebehörde bereits vor mehreren Jahren ein PC-gestütztes Auskunftsverfahren für Adressauskünfte aus dem Melderegister entwickelt, bei dem für Auskunftsersuchen mit vielen Einzelanfragen von großen Kunden, wie z. B. der Handelskammer Bremen, der Sparkasse Bremen, der Bremer Straßenbahn AG, Adress-Research/Deutsche Bundespost, statt Papier auch Disketten verwendet werden können. Für die Erteilung der Sammelauskünfte wird ein standardisiertes Datensatzformat verwendet, das zwischen der Meldebehörde und den Kunden vereinbart wird. Die Auskunftsdaten werden von der Meldebehörde auf die von der um Auskunft ersuchenden Stelle übersandten Diskette im vereinbarten Format ausgegeben. Der Datenträgertransport erfolgt dann entweder per Post oder per Botendienst.

Ich habe das Sammelauskunftsverfahren geprüft und dabei folgendes festgestellt: Seit dem vergangenen Jahr kann der Datenträgertransport auch elektronisch erfolgen, indem die Dienste der bremen online services GmbH & Co. KG (bos) genutzt werden. Statt eine Diskette zu transportieren, können Großkunden mit vielen Einzelanfragen ihre Auskunftsersuchen neuerdings auch über das Internet verschicken. Hierzu besorgen sich die Großkunden eine Signaturkarte und lassen sich zur Teilnahme an dem neuen Verfahren bei der bos registrieren. Die Einzelanfragen werden vom jeweiligen Kunden erfasst, von ihm mit der Signaturkarte signiert und verschlüsselt und dann über Leitung an die bos geschickt; dort werden sie in einer für die Meldebehörde eingerichteten E-Mail-Box eingespeichert. Nach Eingang einer neuen Anfragedatei benachrichtigt bos die Meldebehörde per E-Mail. Die Meldebehörde holt sich sodann per Leitung/Internet die abgelegte Anfragedatei, verifizirt den Absender, entschlüsselt sie und gibt sie auf Diskette aus. Diese Diskette wandert dann zu dem Auskunftsplatz und wird dort genauso wie andere Diskettenanfragen auch bearbeitet, d. h.,

eingelesen, mit dem DEMOS-Datenbestand verglichen und das Ergebnis wird auf Bildschirm in Tabellenform dargestellt. Bei eindeutigen Treffern erscheint der Name mit neuer Anschrift und ggf. weiteren Angaben (z. B. verstorben, evtl. das Geburtsdatum und das Sterbedatum). Bei nicht eindeutigen Fällen muss der Bearbeiter jeden Fall einzeln am Bildschirm/PC (DEMOS-Zugriff) bearbeiten. Das Ergebnis wird auch in diesem Fall auf Diskette ausgegeben und dann wieder zum Internet-Arbeitsplatz transportiert, dort eingelesen, mit der Signaturkarte signiert und an die bos in die E-Mail-Box des Kunden bzw. Datenempfängers verschickt. Von dort holt er sich dann seine Melderegisterauskünfte ab.

Bei dem dargestellten PC-Verfahren wird nicht nach der Art der Melderegisterauskunft differenziert. Obgleich das erforderliche berechtigte Interesse möglicherweise nicht vorliegt, hat die anfragende Stelle stets die Möglichkeit von der Meldebehörde alle die Daten zu erhalten, die Teil der sog. erweiterten Melderegisterauskunft (vgl. Ziff. 14.16 dieses Berichts) sind. Eine Überprüfung dahingehend, ob ein berechtigtes Interesse bzw. gar ein rechtliches Interesse für eine erweiterte Melderegisterauskunft tatsächlich bei der Anfrage vorliegt, erfolgt durch die Meldebehörde nicht, auch nicht stichprobenweise. Ein Benachrichtigungsschreiben der Meldebehörde, das bei erweiterten Auskünften nach § 32 Abs. 2 BremMeldG außerdem vorgeschrieben ist, fehlt ebenfalls. Auf dieses könnte bei der Erteilung einer erweiterten Melderegisterauskunft nur verzichtet werden, wenn ein rechtliches Interesse vorliegt.

Ich habe die undifferenzierte Erteilung von Sammelauskünften gegenüber der Meldebehörde Bremen kritisiert. Eine Antwort steht derzeit noch aus.

6.12.3 Verordnung über das Verfahren bei der elektronischen Anmeldung

Nach § 17 Abs. 5 bremisches Meldegesetz (BremMeldG) kann der Meldepflichtige die von ihm zu erhebenden Daten unter Beachtung der Vorgaben des Signaturgesetzes auch elektronisch an die Meldebehörde senden, soweit eine Rechtsverordnung nach § 36 Abs. 2 BremMeldG dies zulässt. Dabei ist sicherzustellen, dass bei der elektronischen Übertragung der Daten eine unbefugte Kenntnisnahme nicht erfolgen kann.

Hierzu hat der Senator für Inneres, Kultur und Sport nun im Berichtszeitraum die Verordnung über die elektronische Erfüllung der Meldepflicht erlassen. Nach dieser Verordnung kann der Meldepflichtige die von ihm zu erhebenden Daten auch elektronisch an die zuständige Meldebehörde senden. Dies ist jedoch nur bei einem Wohnungswechsel innerhalb der Stadtgemeinden Bremen und Bremerhaven zulässig. Darüber hinaus enthält die Verordnung Regelungen zur Gestaltung des Verfahrens und der Art der Daten, die dabei übertragen werden dürfen.

In meiner Stellungnahme zu der Verordnung habe ich u. a. eine Konkretisierung des Katalogs der von der Meldebehörde bei der Anmeldung zu erhebenden Daten verlangt. Außerdem habe ich darauf hingewiesen, dass, um Veränderungen der Daten auf dem Wege der Datenübertragung auszuschließen, nur eine verschlüsselte Übertragung zulässig sein darf und die Daten nur innerhalb des Melderegisterverfahrens entschlüsselt können werden dürfen. Außerdem habe ich eine Regelung verlangt, nach der nur am Meldeverfahren beteiligte und hierzu befugte Personen Kenntnis von den

Daten der Meldepflichtigen erhalten dürfen. Bei der Signatur und der Verschlüsselung der Daten für die Übertragung ist zudem zu gewährleisten, dass ein standardisiertes sicheres Verfahren eingesetzt wird, das mindestens dem OSCI-Standard entspricht.

Der Senator für Inneres, Kultur und Sport hat meine Anregungen beim Entwurf der Verordnung weitgehend berücksichtigt. Die Verordnung wurde von der Innendeputation bereits beschlossen, sie ist aber noch nicht erlassen worden. Der Grund liegt darin, dass das zugrunde liegende systemtechnische Verfahren noch nicht realisiert werden konnte.

7. Justiz

7.1 Zugriffe auf kinderpornographische Internetseiten

„Skandal um schmuddelige Kinderpornos, Verfahren gegen Richter eingestellt“ titelte im Oktober 2002 eine Bremer Tageszeitung. Diese Presseberichterstattung hat viele Beschäftigte verunsichert. Sie befürchteten eine Vollprotokollierung aller ihrer Internetzugriffe, verbunden mit einer personenbezogenen Auswertung. Ich bin deshalb der Sache nachgegangen.

Mitarbeiter beim Senator für Finanzen haben im Rahmen einer nicht personenbezogenen Teilprotokollierung in Form von URL-Hitlisten innerhalb eines Zeitraums von vier Wochen der aus dem Bremer Verwaltungsnetz (BVN) heraus aufgerufenen Internet-Seiten Hinweise darauf erlangt, dass rechtswidrige Inhalte von Mitarbeitern der bremischen Verwaltung in größerem Umfang heruntergeladen wurden. Diese Anhaltspunkte führten zu einer Strafanzeige gegen Unbekannt bei der Staatsanwaltschaft Bremen (StA).

Bedingt durch die Struktur des Verwaltungsnetzes (BVN) ist eine zentrale Vollprotokollierung der Internet-Nutzung der einzelnen PC in der Regel nicht durchführbar, weil die Internet-Nutzung aus dem BVN heraus nur möglich ist, wenn dazu Proxy-Server genutzt werden. Teilweise wird aus einzelnen Dienststellen heraus direkt von den Arbeitsplätzen auf die Proxy-Server der BreKom zugegriffen, teilweise betreiben die einzelnen Dienststellen eigene Proxy-Server oder nutzen für den Internet-Zugriff Terminalserver. Dies hat zur Folge, dass eine Vollprotokollierung auf den Proxy-Servern der BreKom nicht direkt die IP-Adresse des Arbeitsplatzrechners der Beschäftigten liefern kann, von denen aus rechtswidrige Inhalte aus dem Internet genutzt werden. Da die BreKom-Proxies nur die IP-Adressen der Proxy-Server in den Dienststellen erkennen können, nicht jedoch die IP-Adressen der daran angeschlossenen Arbeitsplatz-PC erhält, musste eine Vollprotokollierung der Internetzugriffe an den Proxy-Servern der einzelnen betroffenen Dienststellen durchgeführt werden.

Die StA hat zunächst ein Ermittlungsverfahren gegen Unbekannt eröffnet und bei Gericht insgesamt sechs richterliche Beschlüsse für die Protokollierung auf den entsprechenden Proxy-Servern in verschiedenen Bereichen der Verwaltung erwirkt. Die Beschlüsse gem. §§ 103, 105 StPO lauteten auf eine Protokollierungsdauer von vier Wochen und enthielten die Kennung von ganz bestimmten Internet-Seiten (URLs) und bestimmten Suchbegriffen, die den Verdacht auf den Zugriff auf kinderpornographische Inhalte nahe legen. Auf eine Nennung der genauen Adressen aus den richterlichen Beschlüssen soll hier verzichtet werden. Alle im folgenden angefallenen IP-Adressen-bezogenen Protokolldaten, die von den betroffenen Stellen geliefert wurden, sind zur UJs-Akte der StA genommen worden und sollen dort verbleiben. Sie sollen das Schicksal der Akte teilen und sollen daher nach Ablauf der Aufbewahrungsfrist von fünf Jahren gelöscht werden.

Mit Ausnahme der im Bereich Justiz protokollierten Daten sind die aus den anderen Bereichen von den entsprechenden Dienststellen gelieferten Protokolldaten zur weiteren Auswertung und Verdichtung der Kriminalpolizei (Polizei Bremen) übergeben worden. Die Rücklieferung der

Auswertungsergebnisse von der Kripo an die StA steht noch aus, sie wird nicht vor Ablauf eines Jahres erwartet. Damit wird das Beweismaterial weitgehend wertlos werden, weil entsprechende Zuordnungen auf den PC nicht mehr vorgenommen werden können, weil sie in der Regel dann dort gelöscht sind. Bei gleichgelagerten Fällen im Privatbereich werden die zugehörigen PC nach Auskunft der StA in der Regel für die Dauer des Ermittlungsverfahrens beschlagnahmt.

Für den Bereich Justiz wurden die Auswertungen der Protokolldaten im Auftrag der StA von Judit durchgeführt. Dort wurden die Protokolldaten nach den Kriterien aus den richterlichen Beschlüssen ausgewertet und aufbereitet. Die gewonnenen Daten sind auf CD-Rom an die Staatsanwaltschaft geliefert worden. Die Staatsanwaltschaft hat somit von Judit nur gefilterte Protokolldaten erhalten.

Aufgrund dieser Auswertung verdichteten sich die Anhaltspunkte aus einer Menge von rund 20 PCs schließlich auf vier konkrete Fälle (Rechner/IP-Adressen). Die StA hat für diese Arbeitsplatz-PC im Bereich der Justiz richterliche Beschlüsse zur Überprüfung der im einzelnen auf den PC konkret gespeicherten Daten erwirkt. Bei diesen Fällen hat sich anhand der Protokolldaten der Verdacht erhärtet, dass gezielt nach Seiten mit kinderpornographischen Inhalten gesucht wurde und die Inhalte dieser Seiten dann auf die Festplatte der Arbeitsplatz-PC heruntergeladen und abgespeichert wurden.

Die StA hat sodann bei vier Personen die Ermittlungsverfahren weiter betrieben. In diesem Rahmen hat es zwei Durchsuchungen (Arbeitsplatz-PC und privater häuslicher PC) gegeben. In einem Fall führte das gefundene kinderpornographische Bildmaterial zu einer vorläufigen Einstellung nach § 153 a StPO mit der Auflage, ein Bußgeld zu zahlen und sich einer Therapie zu unterziehen. Die anderen Fälle wurden eingestellt.

Alle in diesem Zusammenhang angelegten Js-Ermittlungsakten werden nebst der aufbereiteten Protokolldaten auf CD direkt bei der Leitung der Staatsanwaltschaft unter Verschluss gehalten und voraussichtlich ebenfalls nach Ablauf von fünf Jahren vernichtet.

Als vorläufig datenschutzrechtliche Beurteilung möchte ich festhalten:

Die eingangs genannten Befürchtungen der Beschäftigten können im wesentlichen relativiert werden. Zum einen wurden nur genau bestimmte Internetseiten mit (kinder)pornographischen Inhalten protokolliert. Es wurden also nicht alle, sondern streng ausgewählte Zugriffe protokolliert. Von einer zulässigen dienstlichen Nutzung in diesen Fällen konnte somit niemand ausgehen. Zum anderen wurden die protokollierten Daten zunächst näher untersucht, ob es sich tatsächlich um strafbewährte Inhalte handelte, denn unter den Adressen befinden sich auch andere Inhalte. Schließlich wurde nur in den Fällen, in denen sich der konkrete Verdacht tatsächlich erhärtete die IP-Adresse einem konkreten Rechner zugeordnet und dann wurde geprüft, welche Person die tatsächliche Verfügungsgewalt über den Rechner hatte. Unabhängig davon, dass ich die richterlichen Beschlüsse nicht zu würdigen habe und auch keinen rechtlichen Grund dazu sehe, habe ich bei meiner Prüfung im Dezember 2002 den Eindruck gewonnen, dass die Staatsanwaltschaft sehr behutsam mit den Ergebnissen umgegangen ist. Zu prüfen bleibt allerdings noch, ob und in welchem Umfang bei den Stellen, die die richterlichen Beschlüsse durchgeführt haben, selbst Datenspuren verblieben sind. Dies war vor Redaktionsschluss nicht mehr leistbar.

7.2 Öffnung von gerichtlichen Registern u. Verzeichnissen fürs Internet

Der erste Anstoß für die Automatisierung von bei den Gerichten geführten Registern und Verzeichnissen kam durch das Registerverfahrensbeschleunigungsgesetz vom 20. Dezember 1993, das die Automation des Handelsregisters, des Grundbuchs und weiterer öffentlicher Register ermöglichte. Mit der Digitalisierung des Handels-, Vereins-, Partnerschafts- und Genossenschaftsregisters oder dem Schuldnerverzeichnis entstand - getragen von der Bund-Länder-Kommission (BLK) - der Gedanke, neben dem Online-Zugriff öffentlicher Stellen und insbesondere der Gerichte, auch privaten Stellen den Zugriff auf diese Daten oder Teile dieser Daten über das Internet zu ermöglichen.

In den Bereich der Internetöffentlichkeit gehören auch die Insolvenzverfahren. Die Datenschutzbeauftragten des Bundes und der Länder hatten bereits mit Blick auf die Änderungen der Insolvenzordnung (vgl. 24. JB, Ziff. 15.8) ihre Besorgnis zum Ausdruck gebracht, dass Informationen aus dem Insolvenzverfahren, die in das Internet eingestellt werden, in ihrer Verwendung nicht begrenzt werden können, ihre Speicherung nicht zeitlich beherrschbar ist und dass die Löschung dieser personenbezogenen Daten nicht sichergestellt werden könne. Das Bundesjustizministeriums hat nunmehr die im letzten Jahresbericht (vgl. 24. JB, Ziff. 7.3.2) bereits beschriebene Verordnung am 12. Februar 2002 erlassen. In einer Prüfbitte hat der Deutsche Bundestag die Frage aufgeworfen, wie verhindert werden kann, dass Daten nach Ablauf der gesetzlichen Löschfrist durch Dritte über das Internet weiter verbreitet werden. Dieses Problem durch eine neue rein insolvenzrechtliche Bußgeldvorschrift zu lösen, die die Ahndung eines solchen Verhaltens zulässt, wird als unzureichend angesehen. Die Bundesminister der Justiz und des Innern haben die Anregung des Bundesbeauftragten für den Datenschutz positiv aufgenommen, durch Änderung der §§ 29 und 43 Bundesdatenschutzgesetz (BDSG) einen besseren Schutz der Betroffenen zu bewirken.

Der Vorschlag zielt darauf ab, die Erhebung und Speicherung von Daten zum Zwecke der Übermittlung und die Übermittlung dieser Daten im Internet nur innerhalb einer bestimmten Frist zuzulassen, wenn sie von öffentlichen Stellen im Rahmen gesetzlicher Fristen in das Internet eingestellt wurden. In § 43 Abs. 2 Nr. 1 und 2 BDSG soll jeweils das Merkmal in "nicht oder nicht mehr allgemein zugänglich " geändert werden. Ein Verstoß gegen §§ 29 BDSG könnte dann als Ordnungswidrigkeit geahndet werden (genauer vgl. BT-Drs. 15/181).

Die Online-Register-Information ermöglichte die Online-Recherche in den Registerdatenbanken des Amtsgerichts und die Bestellung von amtlichen Registern. Nach einer Bilanz von Media@Komm Bremen nutzen in Bremen insbesondere Rechtsanwälte, Notare, Banken und Versicherungen dieses Angebot intensiv, weil sie sich so den Gang zum Amtsgericht ersparen. Es soll monatlich ca. 3.000 Zugriffe geben.

Für Bremen hatte ich seinerzeit beim Online-Zugriff auf das Handelsregister auf die Einhaltung der gesetzlichen Bestimmungen gedrängt und dem Zugang nur für einen bestimmten Personenkreis als geschlossene Benutzergruppe verbunden mit einer Beschränkung der angezeigten Daten zugestimmt. Dem wurde auch entsprochen. Mittlerweile ist aber § 9 a Handelsgesetzbuch (HGB) geändert worden und erlaubt nunmehr unter bestimmten Voraussetzungen jedermann ohne vorherige

Genehmigung den Online-Zugriff auf die Daten des elektronischen Handelsregisters. Ich habe gegen einen erweiterten Zugriff auf das Handelsregister in Form von Einzelabrufen keine datenschutzrechtlichen Bedenken erhoben, wenn sichergestellt ist, dass den Regelungen von § 9 Abs. 1 HGB (Nutzung nur zu Informationszwecken) und von § 9 a Abs. 2 HGB (Verfahren einer Nutzungskontrolle) entsprochen wird.

7.3 Anordnung über Mitteilung in Strafsachen (MiStra)

Eine bundesweite Anordnung über Mitteilung in den Strafsachen regelt die Mitteilung personenbezogener Daten von Amts wegen durch Staatsanwaltschaften oder Gerichte an öffentliche Stellen für andere Zwecke als für die sie erhoben worden sind. Da verschiedene Forderungen der Datenschutzbeauftragten des Bundes und der Länder bereits wiederholt bei Änderungen der MiStra nicht berücksichtigt wurden, hat sich der letztjährige Vorsitzende der Konferenz der Datenschutzbeauftragten des Bundes und der Länder in einem abgestimmten Schreiben an den Vorsitzenden der Justizministerkonferenz gewandt und auf aus datenschutzrechtlicher Sicht wichtige Punkte hingewiesen:

Sofern eine Mitteilung über ein Strafverfahren nach der gesetzlichen Vorgabe erst nach einer individuellen Bewertung beispielsweise über das Vorliegen eines öffentlichen Interesses erfolgt, soll der Betroffene über diese Übermittlung der Daten informiert werden.

Mitteilungen über die Einstellung eines Verfahrens gem. § 71 Abs. 2 StPO wegen Schuldunfähigkeit des Betroffenen sollen, wenn diese nur vorübergehende Natur war und das zu Grunde liegende Gutachten älter als fünf Jahre ist oder weitere Ermittlungen nicht zur Erhebung der öffentlichen Klage führen würden, unterbleiben. Im übrigen sollen die Betroffenen über derartige Mitteilungen unterrichtet werden.

Die Mitteilungen sollen nur stattfinden, sofern hierfür auf Seiten des Empfängers ein konkreter und ausreichender Bedarf besteht und nur in dem Umfang erfolgen, wie sie für die Aufgabenerfüllung des Empfängers erforderlich ist.

Der Eingang des Schreibens ist vom Vorsitzenden der Justizministerkonferenz bestätigt worden, die Vorschläge sollen beraten werden.

8. Gesundheit und Krankenversicherung

8.1 Interne Vernetzung des Gesundheitsamtes Bremen

Bei einer im vergangenen Berichtsjahr durchgeführten Prüfung ausgewählter Sicherheitsaspekte des internen Netzes des Gesundheitsamtes Bremen (GAB) sind einige Schwachstellen deutlich geworden. Das GAB sagte daraufhin zu, entsprechende Gegenmaßnahmen zu treffen (vgl. 24. JB, Ziff. 8.2).

Deren Umsetzung überprüfte ich mit folgendem Ergebnis im September 2002:

Es ist kein hausinternes E-Mail-Konzept entwickelt worden, allerdings werden weiterhin nach Aussage des GAB keine sensiblen, insbesondere keine patientenbezogenen Daten, per E-Mail verschickt.

Die Netzstruktur ist mit dem Ziel, die in den einzelnen Abteilungen des GAB gespeicherten Daten entsprechend den Vorgaben im Gesetz über den öffentlichen Gesundheitsdienst und der auf dessen Grundlage erlassenen Datenschutzverordnung vor unbefugten Zugriffen aus anderen Abteilungen zu schützen, verändert worden; die Abschottung der einzelnen Abteilungen des GAB voneinander wurde durch Definitionen der Zugriffsberechtigungen über das Netz (Freigaberechte) sowie durch die Vergabe von Zugriffsberechtigungen auf Datei- und Verzeichnisebene für den Anwendungsbereich der einzelnen Abteilungen erreicht. Durch die Beibehaltung einer zentralen Administration über die Domäne GAB bleibt der administrative Zugriff auf alle Abteilungsserver bestehen. Auch die Freigaberechte können nur durch die zentrale Administration vergeben werden. Das bedeutet, dass eine Steuerung des Zugriffs auf die File-Server der Abteilungen bzw. auf bestimmte Verzeichnisse nicht durch die Abteilungen selbst übernommen werden kann.

Aus diesem Grund ist trotz der strukturellen Verbesserung des Netzes weiterhin eine starke Revision erforderlich. Dafür wurde inzwischen ein eigenes Benutzerkonto für die Revision eingerichtet.

Die bereits 2001 geforderte und vom GAB zugesagte Differenzierung des Verfahrens und eine genaue Beschreibung der Ziele der Revision war zum Zeitpunkt der Prüfung noch nicht erfolgt. Lediglich eine nicht weiter dokumentierte Benutzerstruktur soll durchgeführt worden sein. Ich habe das GAB nochmals (wie bereits im letzten Berichtsjahr) darauf hingewiesen, dass innerhalb des Revisionskonzeptes u. a. die Verfahren, Fragestellungen, verwendete Tools und Prüfschemata für verschiedene Systemebenen (Betriebssystem, Datenbank, Firewall etc.) beschrieben werden müssen. Darüber hinaus fehlt inhaltlich die Überprüfung der Zugriffsrechte für sensible Objekte.

Die Aktivierung der Überwachungsanforderungen als Grundlage der Revision für alle sensiblen Objekte des GAB war bei meiner Prüfung noch nicht erfolgt, weil sie noch nicht durch die Fachabteilungen definiert worden sind. Um eine Abschottung vertraulicher Schriftstücke auch gegenüber der Administration gewährleisten zu können, erarbeitet das GAB momentan einen Vorschlag zur Bereitstellung eines Verschlüsselungstools.

Insgesamt sind im Berichtjahr insbesondere hinsichtlich der Abschottung der Abteilungsserver weitere strukturelle Verbesserungen im GAB erfolgt. Da das Gesamtkonzept von einer leistungsfähigen

Revision getragen wird, habe ich das GAB aufgefordert, die Revision mit eindeutig im Konzept differenziert definierten Inhalten (s. o.) und entsprechenden Dokumentationen der Tätigkeiten umgehend mit regelmäßigen Abständen bzw. anlassbezogen durchzuführen.

Ich werde die Entwicklung dieses letzten Bausteins eines aus Sicht des Datenschutzes nicht optimalen, aber schlüssigen Netzkonzeptes im nächsten Jahr weiterhin begleiten und prüfen.

8.2 Interne Vernetzung des Gesundheitsamtes Bremerhaven

Im August 2002 übersandte mir das Gesundheitsamt Bremerhaven ein Datenschutz- und Datensicherungskonzept zur internen Vernetzung. Neben einer Kurzbeschreibung der Netzinfrastruktur und Netzkomponenten lag der Schwerpunkt auf der sich momentan im Einführungsprozess befindlichen Software „Octoware“. Diese Fachanwendung unterstützt die Gesamtheit der Arbeits- und Verfahrensabläufe insbesondere der einzelnen Fachabteilungen, für die spezielle Module bereitgestellt werden. Seit März des Berichtsjahres befindet sich das Gesundheitsamt bereits mit den Modulen Infektionsschutz, Kommunalhygiene, Trinkwasser und Badewasser im Echtbetrieb. Weitere Module, wie beispielsweise der amtsärztliche und der sozialpsychiatrische Dienst, werden folgen.

Ich habe die mir vorgelegte Konzeption zum Anlass genommen, die Fachanwendung „Octoware“ unter folgenden Aspekten zu prüfen: Administrationskonzept/Administratorentool, Fernwartung, Zugriffslogik, Trennung der Daten für verschiedene Aufgabenbereiche im allgemeinem Adressbuch und den Zentraldateien der Fachabteilungen, Reportsystem, Protokollierung und Revision.

Es ergaben sich folgende wesentliche datenschutztechnische Sachverhalte, die entweder bereits vom Gesundheitsamt für den Betrieb des Systems vorgegeben oder als Konsequenz meiner Prüfung von mir gegenüber dem Gesundheitsamt formuliert worden sind.

Alle Nutzer des Verfahrens mit Administratorrechten haben fachmodulübergreifenden Zugriff auf alle sensiblen Daten des Gesundheitsamtes. Diese umfassenden Zugriffe, verbunden mit der inhaltlichen Kenntnisnahme der Daten, sind für die Aufgabe der Administration nicht erforderlich. Dieser außerhalb der Berechtigungsstruktur des Systems liegende Zugriff ist deshalb datenschutzrechtlich problematisch. Allerdings ist bei einigen Administrationsarbeiten die Kenntnisnahme personenbezogener Daten nicht vermeidbar.

Ich habe deshalb dem Gesundheitsamt eine Installation von Revisionsmechanismen vorgeschlagen. Sinnvolle Revisionsmechanismen ermöglichen die Prüfung der Rechtestruktur des Systems auf allen Ebenen und die Prüfung der Zugriffe auf die Daten des Gesundheitsamtes durch Protokollanalyse oder direkte aktuelle Stichprobe. Die Zugriffe auf das System über interne und/oder externe Administrationsrechte müssen deshalb protokolliert werden. Die Protokolle können auf verschiedenen Systemebenen wesentliche Informationen für die Revision liefern. Als Grundlage für eine interne Datenschutzkontrolle des EDV-Systems sollte das Revisionskonzept Bestandteil des Datenschutzkonzeptes werden.

Weiter habe ich die Beschränkung der Administrationstätigkeiten für die Fernwartung/-diagnose durch die Softwarefirma und in der eigenen Organisation vorgeschlagen. Die für Wartung und Diagnose

zuständige Firma sollte, wie bereits vom Gesundheitsamt geplant, nur nach Freigabe durch die Administratoren des Gesundheitsamtes einen administrativen Zugriff für vorab definierte Zwecke erhalten. Die Systemarbeiten werden während ihrer Ausführungen von den Administratoren des Gesundheitsamtes geprüft. Es ist erforderlich, eine Vereinbarung über den Umfang der Fernwartung (Diagnose, Pflege) zu treffen (vgl. § 9 Abs. 4 BremDSG). Eine Kenntnisnahme personenbezogener Daten ist dabei so weit wie möglich auszuschließen. Die Administratoren des Gesundheitsamtes besitzen Anwendungsrechte in den Fachmodulen, die die einzelnen Aufgabenbereiche des Gesundheitsamtes abbilden, um einzelne Nutzer in der Systemanwendung unterstützen zu können. Diese Unterstützung ist keine originäre Aufgabe der Systemadministratoren und widerspricht durch die Notwendigkeit entsprechender Zugriffe auf (auch) medizinische Dokumente in einzelnen Modulen dem datenschutzrechtlichen Grundsatz, im Rahmen von Administrationsaufgaben soweit möglich keine personenbezogenen Daten zur Kenntnis zu nehmen. Im Sinn einer organisatorischen Beschränkung der Administration ist es sinnvoll, zukünftig die Unterstützung der Nutzer von der Adminstration abzukoppeln .

Insgesamt stellt die Zugriffssteuerung von „Octoware“ alle für die Umsetzung datenschutzrechtlicher Anforderungen erforderlichen Einstellungsmöglichkeiten zur Verfügung. Von besonderer Bedeutung ist dies zur Realisierung der Datentrennung für verschiedene Aufgabenbereiche im allgemeinen Adressbuch des Gesundheitsamtes und den Zentraldateien der Fachbereiche. Im allgemeinen Adressbuch sind keine Identitätsmerkmale zusammen mit Ordnungsmerkmalen gespeichert, was das Auffinden der Falldokumentationen ermöglicht. Demnach ist es keine unzulässige Zentraldatei.

Die Zentraldateien der Fachbereiche eröffnen direkte Zugriffe auf die Falldokumentationen und entsprechen insoweit nicht unmittelbar der Sollvorschrift des § 2 Abs. 1 der Verordnung (VO) zu § 33 Abs. 3 des Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG), wonach Suchdateien nur das Auffinden von Dokumenten ermöglichen dürfen. Da aber Zugriffe auf diese Dokumentationen für Nutzer ohne entsprechende Rechte gesperrt werden können, eröffnet das System eine dem Zweckbindungsgebot des § 32 Abs.1 ÖGDG und des § 1 der VO sowie dem Beratungsgeheimnis des § 31 Abs. 2 Satz 6 ÖGDG gerecht werdende Möglichkeit zur differenzierten Vergabe von Zugriffsrechten. Wesentliche Voraussetzung für einen datenschutzgerechten Betrieb des Systems ist eine entsprechende Konfiguration der Zugriffsstruktur. Da sich das System momentan im Aufbau befindet, habe ich diese noch nicht geprüft.

Die Einhaltung des Zweckbindungsgebotes muss auch in den im System zur Verfügung stehenden Auswertungsmöglichkeiten über den Datenbestand im Rahmen des Reportsystems gewährleistet sein. Standardreports werden modulspezifisch für entsprechende Anforderungsprofile bereitgestellt und bewegen sich insofern innerhalb des durch die Zugriffslogik vorgegebenen Rahmens. Für die Administration stellt das System auf Anwendungsebene eine Möglichkeit zur Verfügung, Datenbankfragen fachabteilungsbezogen zu hinterlegen. Auch wenn hier bereits eine Einschränkung auf die Fachabteilungen vorgenommen wurde, sind innerhalb dieses Rahmens beliebige Auswertungen des Datenbestandes möglich. Ich habe hier zur Sicherung der Zweckbindung empfohlen, ein Verfahren für die Antragsstellung durch die Fachabteilungen zu entwickeln und das Datenschutzkonzept entsprechend zu ergänzen.

Insgesamt bietet die vom Gesundheitsamt Bremerhaven ausgewählte Fachanwendung „Octoware“ bis auf die Möglichkeit einer für die Revision erforderlichen Protokollierung der Zugriffe umfassende Möglichkeiten im Rahmen der Zugriffssteuerung, das Verfahren datenschutzgerecht mit allen Funktionen in Betrieb zu nehmen.

Ich werde die Einführung des Systems weiter begleiten, eine Reaktion des Gesundheitsamtes auf meine Vorschläge steht noch aus.

8.3 Das Bremer Mammographie-Screening-Projekt

Das Bremer Mammographie Screening-Projekt war im Jahr 2000 begonnen worden, ohne dass die mit mir abgestimmte Software installiert worden war. Dies aber war die Voraussetzung für die Realisierung des mit mir abgestimmten Datenschutzkonzepts. Folge war unter anderem, dass im Projekt automatisiert gespeichert wurde und ausgewertet werden konnte, aus welchen Gründen Bremerinnen telefonisch ihre Teilnahme abgesagt hatten. Genau das aber soll nicht sein. Wer nicht teilnimmt, darf nicht erfasst werden, so die rechtliche und politische Grundlage des Projekts. Allenfalls anonymisierte Daten dürfen gespeichert und ausgewertet werden. Auf meine Beanstandung hin wurde die Speicherung der Absagen umgehend eingestellt, die Software, die derartiges von vornherein verhindert hätte, wurde unter Hochdruck installiert und in Betrieb genommen. Dies habe ich im letzten Jahresbericht (vgl. 24. JB, Ziff. 8.4) ausführlich dargestellt. Inzwischen konnte ich mich davon überzeugen, dass auch die Daten der vor Inbetriebnahme der Software untersuchten Frauen in das neue System eingepflegt worden sind.

Das Projekt hat mir seitdem wiederholt Vorstellungen zur Änderung des Konzeptes vorgelegt. In der Regel handelte es sich um aus praktischen Gründen sicher sinnvolle und datenschutzrechtlich unbedenkliche Weiterentwicklungen. Auf einen jüngst an mich herangetragenen Vorschlag, von den nicht teilnehmenden Frauen, deren Name, Geburtsdatum und Anschrift nicht gespeichert werden dürfen, über das Geburtsjahr hinaus auch den Geburtsmonat aufzunehmen, habe ich allerdings zurückhaltend reagiert.

Ein neues Problem ist eingetreten. Das Zentralkrankenhaus Sankt-Jürgen-Straße scheint keinen ausreichenden Raum für das medizinische Archiv des Projekts bereitstellen zu können. Gegen einige der in Überlegung befindlichen Ersatzstandorte bestehen datenschutzrechtliche Bedenken. Die rechtliche Verpflichtung zur ordnungsgemäßen Archivierung von Behandlungsunterlagen muss sichergestellt werden. Ich erwarte von den Verantwortlichen, dass sie eine angemessene Lösung finden.

8.4 Vernetzung und digitale Behandlungsdokumentation in Krankenhäusern

Seit 2000 habe ich in den vier kommunalen Zentralkrankenhäusern (ZKH) im Lande Bremen, die ein SAP-basiertes Informationssystem einsetzen, die Berechtigungskonzepte für die Administration des Systems durch interne und externe Kräfte, für die Verwaltung sowie für Ärzte und Pflegekräfte geprüft (vgl. 23. JB und 24 JB, jeweils Ziff. 8.1.). Das in 2001 geprüfte Zentralkrankenhaus Bremen-Ost hat

mir im Berichtsjahr ein Berechtigungskonzept zugeleitet, dessen Festlegungen zur Vergabe von Berechtigungen an Systemadministration und Verwaltung den datenschutzrechtlichen Anforderungen entsprechen. Im ZKH Sankt-Jürgen Straße, das ich als letztes der vier Krankenhäuser im Berichtsjahr geprüft habe, konnte ich feststellen, dass hier bereits die gebotenen Vorkehrungen getroffen waren. Der Zugriff der Systemadministration auf digitalisiert gespeicherte Behandlungsdaten ist weitgehend ausgeschlossen, der Zugriff der Verwaltung nur in genau definiertem Umfang zulässig.

Schwieriger zu lösen sind die datenschutzrechtlichen Probleme, die die Zugriffsrechte von Ärzten, Therapeuten und Pflegekräften auf die digitalisiert gespeicherte Dokumentation der Behandlung im Krankenhaus aufwerfen. Ich habe Zweifel daran geäußert, ob Zugriffsrechte in der Weite durch Behandlungsnotwendigkeiten indiziert seien. Die Krankenhäuser hielten dem entgegen, dass zum einen die Zugriffslogik des eingesetzten, auf SAP aufsetzenden Dokumentationssystems die vom Gesetz eingeforderten Begrenzungen nicht hergebe und dass zum anderen stationäre Behandlung, Therapie und Pflege zunehmend interdisziplinär strukturiert seien. Einig war man sich aber darin, dass der Zugriff auf Patientendaten im Einzelfall nur zulässig sei, soweit dies für Behandlung, Therapie oder Pflege erforderlich ist. Abteilungsübergreifende Zugriffe können z. B. bei Verlegung des Patienten, bei Anforderung einer Mitbehandlung durch einen Arzt einer anderen Fachabteilung, bei Anforderung von Leistungen der Radiologie, des Labors oder der Anästhesie oder bei Einsatz abteilungsübergreifend eingesetzter Therapeuten oder Pflegekräfte erforderlich werden.

Wie in den Vorjahren berichtet, standen geltendes Recht und technisches System zueinander im Widerspruch. Das haben auch die Anhörungen im Datenschutzausschuss der Bremischen Bürgerschaft ergeben (vgl. Ziff. 8.6 dieses Berichts).

Im Verlauf von vier Workshops in den geprüften Krankenhäusern gelang es, unter Beteiligung von Informatikern, Ärzten, Therapeuten und Pflegekräften eine sowohl datenschutzrechtlich als auch aus Sicht der beteiligten Akteure aus den Krankenhäusern akzeptable und durch die Software-Firma auf der Basis des Moduls IS-H*MED umsetzbare Lösung zu entwickeln, die in 2003 eingesetzt werden kann und soll. Die wichtigsten Punkte, die ich dabei erreichen konnte, will ich im Folgenden kurz skizzieren.

Wird die Verlegung oder die Leistungsanforderung im System abgebildet, so wird zugleich der hierfür erforderliche Zugriff freigegeben. Dies ist bei abteilungsinternen Verlegungen eingerichtet. Bei der abteilungsübergreifenden Leistungsanforderung ist es erst z. T. realisiert, z. B. bei radiologischen oder Laborleistungen, im Übrigen wird es angestrebt.

Für den Fall, dass die Leistungsanforderung nicht im System abgebildet ist, kann sich der angesprochene Mitarbeiter einer anderen Fachabteilung einen auf 24 Stunden begrenzten lesenden Zugriff verschaffen („dynamischer Behandlungsauftrag“). Zuvor ist in einem Pflichttextfeld eine von der zur Auswahl gestellten Begründungen anzugeben oder aber in einem Freitextfeld die Begründung zu konkretisieren. Die Begründungskategorien werden in Tabellen abgespeichert, die über Reports regelmäßig durch die Revision/den Datenschutzbeauftragten des Krankenhauses auszuwerten sind. Zugleich wird dem behandelnden Arzt in der Transaktion „Klinischer Arbeitsplatz“ auf seinem Bildschirm automatisch angezeigt, dass jemand über den „dynamischen Behandlungszugriff“ auf die

durch ihn geführte Dokumentation zugegriffen hat. Durch Klicken kann er dann erfahren, wer wann mit welcher Begründung auf welche Dokumente zugegriffen hat.

Der Abschluss der Behandlung (für Ärzte 90 Tage nach Entlassung, für Pflege und Therapie in kürzerer Frist) soll im System abgebildet werden. Voraussetzung für den abteilungsübergreifenden Zugriff („dynamischer Behandlungsauftrag“) ist danach, dass eine dritte Stelle (i.d.R. Aufnahme- oder die Notaufnahme) die erneute Aufnahme desselben Patienten zur Behandlung im Krankenhaus in das System eingegeben hat. Die Mitarbeiter der jetzt den Patienten behandelnden Abteilung können dann nach Maßgabe der oben dargestellten Regeln auf die Dokumentation der abgeschlossenen Behandlung zugreifen, und dies nicht nur für die Dauer von 24 Stunden, sondern für die gesamte Dauer der neuen Behandlung.

Für bestimmte Daten, insbesondere die Dokumentation einer psychiatrischen oder psychotherapeutischen Behandlung (mit Ausnahme von rein somatischen Werten), kann und soll im System eine besonders hohe Schutzstufe definiert werden. Auf diese Daten soll ohne Freigabe des derzeit oder früher behandelnden Arztes aus einer anderen Abteilung nicht zugegriffen werden können.

Ich werde den Einsatz des Konzeptes bei den beteiligten Krankenhäusern weiter verfolgen.

Ich habe das technische Konzept des „dynamischen Behandlungsauftrags“ auch den Datenschutzbeauftragten des Bundes und der anderen Länder vorgestellt, da die Rechtsgrundlagen, die Behandlungsnotwendigkeiten und die Software für Krankenhausinformationssysteme bundesweit mit denen im Lande Bremen vergleichbar sind. Es wurde interessiert aufgenommen und anerkannt, dass die in Bremen entwickelten Lösungen auch Grundlage der Bewertung von Krankenhausinformationssystemen in anderen Ländern sein können.

8.5 Gesundheitsnetz Bremen

Die kommunalen Krankenhäuser St.-Jürgen-Straße, Bremen-Ost, Bremen-Nord, Links der Weser und das Evangelische Diakonie-Krankenhaus bauen derzeit einen DV-gestützten Kommunikationsverbund Gesundheitsnetz Bremen auf.

Ziel ist es zunächst, einen gemeinsamen sicheren elektronischen Kommunikationsweg zwischen den Krankenhäusern und gesicherte Zugänge der Kommunikationspartner zu öffentlichen Netzen, wie z. B. dem Internet, einzurichten. Diese Wege sollen dann auch niedergelassenen Ärzten und anderen beteiligten Berufsgruppen des Gesundheitswesens zur Verfügung gestellt werden. Die Entwicklung beschränkt sich dabei nicht nur auf die Erhöhung der Anzahl und Art beteiligter Berufsgruppen von Kommunikationspartnern. Vielmehr soll auch der Funktionsumfang um telemedizinische Anwendungen (wie etwa Telekonsil) erweitert werden.

Bereits im Jahr 2000 wurden sicherheitstechnische Richtlinien für die IT-Infrastruktur des Kommunikationsverbundes Gesundheitsnetz Bremen im Entwurf einer teilnehmerübergreifenden Security Policy festgelegt. Sie enthält Richtlinien und Vereinbarungen bezüglich der Zugriffs- und Datensicherheit innerhalb des Kommunikationsverbundes.

Dazu gehören u. a. die Festlegung der Sicherheitsziele und des Sicherheitsniveaus sowie die Schaffung einer strukturellen Grundlage durch eine Systematisierung der Kommunkationsbereiche unter Einbeziehung nicht am Kommunikationsverbund beteiligter externer Kommunikationspartner. Darüber hinaus werden besondere Gefährdungspotentiale berücksichtigt und Vorgaben zu Betrieb und Management von Sicherheitskomponenten gemacht. Die übergreifende Security Policy verpflichtet die Teilnehmer am Kommunikationsverbund auch zu Maßnahmen hinsichtlich ihrer eigenen Anwendungen und Infrastruktur.

Neben der übergreifenden Security Policy ist ein Rahmendatenschutzkonzept entwickelt worden. Es enthält u. a. konkrete Systemanforderungen zum Schutz der krankenhausinternen Infrastruktur gegenüber internen und externen Angriffen sowie Systemanforderungen zur Umsetzung technischer und organisatorischer Maßnahmen gem. § 7 BremDSG.

Diese für alle am Kommunikationsverbund beteiligten Partner geltenden Dokumente definieren organisatorische Rahmenbedingungen, die sicherstellen, dass

- sich jeder Teilnehmer am Kommunikationsverbund zur Anerkennung und Einhaltung der Regelungen aus den Dokumenten schriftlich verpflichtet,
- alle Teilnehmer geeignete technische und organisatorische Maßnahmen ergreifen, um ihre für die Kommunikation eingesetzte Sicherheitstechnologie ständig an das Niveau der aktuellen Bedrohungssituation anzupassen,
- alle Teilnehmer für ihre Organisation interne Security Policies entwickeln, die auf den differenzierten Vorgaben der übergreifenden Security Policy basieren,
- die Verantwortlichkeiten für das Sicherheitsmanagement durch Benennung von Sicherheitsbeauftragten bei jeder teilnehmenden Organisation festgelegt werden,
- jeder Teilnehmer am Kommunikationsverbund in einem Sicherheitsrat mitarbeitet, der u.a. für die regelmäßige Revision der übergreifenden Security Policy zuständig ist und ein feed-back der Sicherheitsstruktur der teilnehmenden Organisation ermöglicht,
- eine Revision bei den einzelnen Netzteilnehmern stattfindet, die sicherstellt, dass Sicherheitsmaßnahmen entsprechend dem Stand der Technik im Verhältnis zum festgestellten aktuellen Bedrohungspotential verändert werden und die missbräuchliche Nutzung der IT-Systeme und der mit ihnen verarbeiteten Daten des Krankenhauses durch die Erstellung aussagefähiger Protokolle und eines darauf aufbauenden Revisionsmechanismus verhindert.

Die Krankenhäuser Bremen-Ost und Links der Weser haben bereits eine interne Security Policy für ihre eigenen Häuser entwickelt, in denen verschiedene Datensicherungsmaßnahmen zur Minimierung des durch die Vernetzung der Häuser und durch die Öffnung zum Internet entstehenden Gefährdungspotentials konkret beschrieben werden.

Das Krankenhaus Links der Weser hat zusätzlich noch einen Strukturentwurf „internes Datenschutzkonzept Firewall“ entwickelt. Da die Wirksamkeit der Sicherheitsmaßnahmen von der Umsetzung in jeder einzelnen Komponente des Systems bei allen Teilnehmern abhängt, habe ich mich über das Firewallsystem dieses Krankenhauses vor Ort informiert. Dabei konnte ich feststellen,

dass die technischen Möglichkeiten, die moderne Firewallsysteme aus heutiger Sicht zum Schutz einer IT-Infrastruktur bieten, weitgehend eingesetzt worden sind. Durch den zusätzlichen Einsatz von IDS (Intrusion Detection System) und Virenscanner können Angriffe und Virenverbreitung weitgehend verhindert werden. Die Effektivität der Firewall hängt jedoch letztlich vom zugrundeliegenden Regelwerk ab

Der Betrieb einer wirkungsvollen Firewall in Kombination mit entsprechenden Prüfmechanismen (IDS, Virenscanner) ist eine komplexe Aufgabe (dazu gehören die Einrichtung sinnvoller Transferregeln, deren Konsolidierung, ständige Systempflege, Reaktion auf Warnmeldungen u.v.m). Wie in der übergreifenden Security Policy bereits geplant, wurde die Leistung „managed Firewall“ deshalb an eine Firma vergeben. Ich hatte zunächst gefordert, dass hierbei sichergestellt werden muss, dass die Auftragnehmerin bei der Administration keinen Zugriff auf Patientendaten nehmen dürfe. Da die Administration von Sicherheitskomponenten Systemrechte mit großer Eingriffstiefe erforderlich macht, ist diese Beschränkung auf technischer Ebene nicht möglich. Eine Kenntnisnahme von Patientendaten kann technisch nicht ausgeschlossen werden. Besonders kritisch wird dies, wenn die Administration an eine Fremdfirma vergeben wird. Hier galt es, dass durch die Fremdvergabe verursachte Risiko mit dem Gewinn abzuwägen, der daraus entsteht, dass die Administration mit dem erforderlichen speziellen Fachwissen erfolgt. In der Novellierung des KHDSG (vgl. Ziff. 8.6 dieses Berichts) wird deshalb die Fremdvergabe nicht untersagt, die Krankenhäuser werden jedoch verpflichtet, den Zugriff auf Patientendaten soweit wie möglich auszuschließen.

Auch wenn eine Gefährdung der IT-Infrastruktur des Kommunikationsverbundes Gesundheitsnetz Bremen durch die Nutzung „legaler Türen“ der eingerichteten Policies und bisher unbekannter Viren nicht auszuschließen ist, ist die dargestellte Systematik der Sicherheitskonzeption und deren Inhalte geeignet, dem Gefährdungspotential für Gesundheitsdaten, dass durch die Vernetzung und Öffnung der DV-Systeme der am Kommunikationsverbund Beteiligten entstanden ist, wirksam zu begegnen.

Ich werde die Entwicklung des Netzes weiterhin begleiten. Projekte wie „iBON“ (Integratives Bremer Onko-Hämatologie Netzwerk), dessen Einrichtung die Deputation für Gesundheit im April des Berichtsjahres beschlossen hat, weisen auf zukünftige datenschutzrelevante Themen wie etwa die Autorisierung des Datenzugriffs durch den Patienten selbst mithilfe einer Chipkarte, die Autorisierung der teilnehmenden Ärzte über eine Health Professional Card und Architekturmodelle bezüglich der Form der Datenspeicherung (beispielsweise bei der Entwicklung einer elektronischen Patientenakte) hin.

8.6 Fortschreibung des bremischen Krankenhausdatenschutzgesetzes

Mit meiner Berichterstattung über die Probleme der krankenhausinternen Vernetzung (vgl. Ziff. 8.4 dieses Berichts) befasste sich auch der Datenschutzausschuss der Bremischen Bürgerschaft. Ergebnis war ein interfraktioneller Antrag, in dem die Bremische Bürgerschaft den Senat einstimmig aufforderte, einen Entwurf zur Änderung des Krankenhausdatenschutzgesetzes (KHDSG) vorzulegen, der den medizinischen Behandlungsnotwendigkeiten und den Bedingungen der modernen DV-Technik entspricht, der zugleich aber beibehält, dass Patientendaten krankenhausintern weder unbegrenzt noch unbefristet verfügbar sein dürfen.

Am 07.01.2003 hat der Senat der Bürgerschaft einen mit mir abgestimmten Entwurf zur Änderung des KHDSG vorgelegt (Bürgerschafts-Drs. 15/1341). Der Entwurf hält daran fest, dass der krankenhausinterne, aber abteilungsübergreifende Austausch bzw. Abruf von Patientendaten nur zu bestimmten im Gesetz aufgeführten Zwecken, insbesondere für eine Mit- oder Nachbehandlung, zulässig ist, erlaubt aber den abteilungsübergreifenden Abruf von Patientendaten im Rahmen des unter Ziff. 8.4 dargestellten „dynamischen Behandlungsauftrags“. Verbunden damit sind die Gebote, nur Befugten Zugriff auf Patientendaten zu gewähren und Patientendaten nach abgeschlossener Behandlung zu sperren. In der mit mir auch insoweit abgesprochenen Begründung zum Gesetzentwurf heißt es hierzu nunmehr, dass in Absprache mit der Verwaltung und mir Terminpläne und Vorgehensweisen zur Mängelbeseitigung entwickelt werden sollen. Überdies sei es Aufgabe der Krankenhäuser, bei der Beschaffung neuer Systeme die Vorgaben des Datenschutzes in das Verfahren einzubeziehen.

Da nicht nur die interne, sondern auch die externe Vernetzung der Krankenhäuser in Datennetzverbünden mit anderen Krankenhäusern, niedergelassenen Ärzten oder anderen Angehörigen von Heilberufen (Gesundheitsnetz Bremen, im folgenden Netz genannt) auf der Tagesordnung steht (vgl. Ziff. 8.5 dieses Berichts), bot sich die Gelegenheit an, auch insoweit das KHDSG auf den neuesten Stand von Medizin und Technik zu bringen. Wollen Krankenhäuser Patientendaten zum automatisierten Abruf in einem Netz bereitstellen, so müssen sie sichergestellt haben, dass die einzelnen Abrufe nur mit Einwilligung der betroffenen Patienten erfolgen können, die Abrufe dem Krankenhaus angezeigt und mittels Protokollierung ausgewertet und kontrolliert werden. Will ein Krankenhaus seinerseits Patientendaten aus dem Informationssystem eines Netzpartners abrufen, so hat der Verantwortliche zuvor die Einwilligung des Patienten einzuholen. Die nach wie vor grundsätzlich erforderliche Schriftform kann entfallen, wenn durch technische Maßnahmen sichergestellt ist, dass die Daten nur unter Mitwirkung des Patienten, etwa mit Hilfe eines nur ihm zur Verfügung stehenden Schlüssels, freigegeben werden können.

Mit der Fortschreibung des KHDSG betritt die Bremische Bürgerschaft legislatives Neuland. Sie reagiert damit auf den verstärkten Einsatz der IuK-Technologie im Gesundheitswesen, auf die mehr und mehr interdisziplinäre Behandlung Kranker und auf die zunehmende Integration stationärer und ambulanter Versorgung. Zugleich versucht sie, ausgehend vom bisher geltenden Recht, den krankenhausinternen Zugriff auf im Informationssystem gespeicherte Patientendaten an den Behandlungsauftrag und den krankenhausübergreifenden Zugriff an die Einwilligung des Patienten zu knüpfen.

8.7 Fax-Irrläufer aus Krankenhäusern

In Krankenhäusern werden nicht nur digitale Informationssysteme von hoher Komplexität eingesetzt, in Krankenhäusern passieren auch ganz banale Pannen. So war ich im Berichtsjahr zweimal damit konfrontiert, dass aus einem der kommunalen Krankenhäuser im Lande Bremen - jeweils einem anderen - unbeteiligten Dritten, die mich darüber informierten, wichtige, für behandelnde Ärzte bestimmte Patientenunterlagen, zugefaxt worden waren. Ich befürchte, dass dies nur die Spitze eines Eisbergs ist, dass zum einen von Krankenhäusern, aber auch von Arztpraxen aus, täglich eine hohe

Zahl sensibler medizinischer Dokumente gefaxt wird und dass zum anderen zu einem geringen Prozentsatz, aber doch immer wieder, die Faxe beim falschen Empfänger landen. Der Grund wird meist eine falsche Fax-Nummer sein, es können aber auch technische oder Bedienungsfehler aufgetreten sein, ein Unbefugter kann das Fax entnommen haben. Wie auch immer, die Folgen können schwerwiegend sein. Ein Unbefugter erhält Kenntnis von den der ärztlichen Schweigepflicht unterliegenden Daten und damit die Möglichkeit, sie für welche Zwecke auch immer zu nutzen. Der eigentliche Adressat hingegen erhält die Daten nicht, dringend gebotene Untersuchungen und Therapien können verzögert werden. All dies ist nicht neu, dafür um so ärgerlicher. Das Faxen medizinischer Dokumente zu verbieten, ist wirklichkeitsfremd, ist es doch gerade die gebotene Schnelligkeit der Kommunikation, die zum Faxen veranlasst.

Gleiches gilt in noch höherem Maße für die Versendung per E-Mail. Die Digitalisierung und Vernetzung der von Behandlungsdokumentationen sowie das verständliche Bestreben, Behandlungsabläufe zu beschleunigen, wird diese Kommunikationsform zur Norm werden lassen. Aber auch sie birgt hohe Risiken. Es gilt, Integrität und Authentizität der Nachricht sowie die Zugriffsberechtigung des Lesers zu garantieren. Hierfür haben Krankenhäuser wie andere öffentliche Stellen ein Sicherheitskonzept zu entwickeln (vgl. Ziff. 8.1 dieses Berichts). Andernfalls dürfen Patientendaten nicht per E-Mail verschickt werden. Unverschlüsselte Übertragungen haben in aller Regel ohnehin zu unterbleiben.

Auf meine Anregung hin hat der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales die mir vorgetragenen Pannen zum Anlass genommen, per Rundschreiben die kommunalen Krankenhäuser der Stadtgemeinde Bremen auf die notwendigen technischen und organisatorischen Vorkehrungen bei der Versendung sensibler Daten per Fax und per E-Mail hinzuweisen. Ich habe das Papier auch dem Bremerhavener kommunalen Krankenhaus zugeleitet.

8.8 Vertraulichkeit sozialpsychiatrischer Beratung

In bemerkenswerter Weise hat sich erneut ein Konflikt zugespitzt, den ich bereits in verschiedenen Jahresberichten thematisiert habe, so erstmals 1990 (vgl. 13. JB, Ziff. 2.6.3, zuletzt im 17. Jahresbericht unter Ziff. 12.2.1). In Bremen laufen zwei Konzepte gegeneinander, ohne dass bis in die jüngste Vergangenheit versucht worden wäre, sie aufeinander abzustimmen: Vertraulichkeit der Beratung einerseits, regionale Zusammenfassung von Beratung, Therapie und Behandlung psychisch Kranker sowie deren Begutachtung im Rahmen eines Verfahrens zur Zwangseinweisung andererseits.

Auf der einen Seite steht das Bemühen, das Vertrauen der Klienten des Sozialpsychiatrischen Dienstes des Gesundheitsamtes (SpsD) in die Vertraulichkeit freiwilliger Beratung bzw. Therapie zu schützen und damit auch die Arbeit des SpsD zu unterstützen. Zu diesem Zweck dürfen die hochsensiblen Daten, die ein Klient dem SpsD im Rahmen einer Beratung bzw. Therapie freiwillig anvertraut, nicht für andere Zwecke verarbeitet oder genutzt werden, es sei denn, der Betroffene hatte eingewilligt oder es kann eine gegenwärtige Gefahr für ihn selbst oder jemand anders nicht anders abgewehrt werden. Auf der anderen Seite steht das Konzept, alle fachlichen Hilfen, seien sie freiwillig oder mit Zwang verbunden, in über die Stadtgemeinde Bremen verteilten regionalen

Behandlungszentren im Rahmen einer persönlichen Beziehung zwischen dem Klienten/Patienten/eingewiesenen Patienten und einem Arzt oder Therapeuten auf der Grundlage einer umfassenden Informationsgrundlage zu gewähren. Auf der einen Seite stehen gesetzliche Regelungen zur strikten Zweckbindung in § 32 des bremischen Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG) aus dem Jahre 1995, konkretisiert in einer Datenschutzverordnung von 1999, und in § 47 des bremischen Gesetzes über Hilfen und Schutzmaßnahmen bei psychischen Krankheiten (PsychKG). Auf der anderen Seite steht ein vom Zentralkrankenhaus Bremen-Ost und vom Gesundheitsamt Bremen entwickeltes Konzept aus dem Berichtsjahr.

Die genannten gesetzlichen Regelungen verbieten ausdrücklich das, was das Konzept anstrebt. Die Gesetze haben Vorrang vor dem Fachkonzept. Hierauf habe ich dessen Verfasser und den Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales hingewiesen, mich aber zugleich bereit erklärt, an einer Fortschreibung der Gesetze dann beratend zu beteiligen, wenn angesichts der Rechtslage auch das Konzept auf den Prüfstand gestellt wird.

8.9 Anforderung von Entlassungsberichten durch Krankenkassen

Krankenhäuser dürfen den gesetzlichen Krankenkassen (GKV) nur die für die Abrechnung ihrer Behandlung erforderlichen, im Sozialgesetzbuch (SGB) einzeln und abschließend aufgeführten Patientendaten übermitteln. Entsprechendes gilt für die Abrechnungsunterlagen, die niedergelassene Ärzte an die Kassenärztlichen Vereinigungen zu übermitteln haben. Bei Zweifeln und in anderen Fällen ist das Überprüfungsverfahren im SGB V – Krankenversicherung – genau geregelt. Vor Erbringung gesetzlich im einzelnen bestimmter Leistungen, darüber hinaus bei Erkrankungen/Behandlungen von besonderer Schwere bzw. Dauer, dürfen auf Anforderung der GKV deren medizinische Dienste (MDK) die Versicherten untersuchen und Behandlungsunterlagen von Krankenhäusern und Ärzten einsehen bzw. anfordern sowie für die GKV fachliche Gutachten erstellen. Diese Aufgaben nehmen für den MDK schweigepflichtige Ärzte wahr. Das Gesetz sieht ausdrücklich vor, dass die Krankenhäuser und Ärzte die vom MDK angeforderten Unterlagen unmittelbar diesem zuleiten sollen. Der MDK seinerseits soll der GKV das Ergebnis seiner Untersuchung und die für die GKV erforderlichen Befunde zuleiten. Das Gesetz trägt damit zum einen der besonderen Schutzbedürftigkeit der Behandlungsdokumentation, zum anderen der Konzentration des medizinischen Fachverstandes beim MDK Rechnung.

Die GKV hat sich in der Vergangenheit nicht immer mit dieser gestuften Aufgabenwahrnehmung und der dieser entsprechenden Datengrundlage abgefunden. Bundesweit, so auch im Lande Bremen, forderten Krankenkassen mit den unterschiedlichsten Begründungen von Krankenhäusern für die nachbehandelnden Ärzten bestimmte Entlassungsberichte und von den Ärzten Behandlungsbefunde an. Die Datenschutzbeauftragten des Bundes und der Länder gingen oft vergeblich gegen diese, in einigen Fällen durch Sozialgerichte gestützte, Praxis an. Jetzt hat das Bundessozialgericht, wie zuvor bereits das mit der Rechtsaufsicht über bundesweit tätige Kassen betraute Bundesversicherungsamt - dies angestoßen durch den Bundesbeauftragten für den Datenschutz – eindeutig für den Datenschutz entschieden. Aus dem SGB folge zwingend, dass nicht die GKV, sondern nur der MDK über die Abrechnungsdaten hinaus Behandlungsunterlagen von den Krankenhäusern und Ärzten anfordern

dürfe. Umgekehrt dürften Letztgenannte auch nicht zu Unrecht angeforderte Unterlagen zur Verfügung stellen. Bereits vor Bekanntwerden des Urteils des Bundessozialgerichts hatte der für die Rechtsaufsicht über die bremischen Krankenkassen zuständige Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales in einer Reaktion auf eine entsprechende Initiative meinerseits seine zuvor anders lautende Auffassung korrigiert und den seiner Rechtsaufsicht unterstehenden Krankenkassen und Krankenhäusern zustimmend die Auffassung des Bundesversicherungsamtes mitgeteilt.

8.10 Steuerung von Versicherten durch die gesetzlichen Krankenkassen

Die Krise des Gesundheitssystems ist in aller Munde. Schlagworte wie Kostenexplosion, Abrechnungsbetrug, Ärzte-Hopper, Fallmanagement beherrschen die Diskussion. Längst ist der am 04.11.1999 bis zum Gesetzesbeschluss des Deutschen Bundestages gediehene Versuch, mit der Gesundheitsreform 2000 den gesetzlichen Krankenkassen eine für die Rechnungs-, Qualitäts- und Wirtschaftlichkeitskontrolle ärztlicher Leistungen ausreichende Datengrundlage zu garantieren, zugleich aber die Persönlichkeitsrechte der Versicherten durch Pseudonymisierung ihrer Daten zu wahren (vgl. ausführlich 22. JB, Ziff.8.8, zuletzt 24. JB, Ziff.8.4), aufgegeben worden. Neue Vorhaben sind an seine Stelle getreten. Es wird immer deutlicher; inzwischen geht es nicht mehr nur um Kontrolle von Ärzten und anderen Erbringern medizinischer Leistungen, es geht auch um die Steuerung der Versicherten durch die Krankenkassen. Zunächst gilt es, per Auswertung versichertenbezogener Daten deren Verhalten transparent zu machen, anschließend, auf sie Einfluss zu nehmen. Gesundheitspolitik dringt in die Persönlichkeitssphäre ein. Kostenminimierung, Qualitätsverbesserung und Missbrauchskontrolle sind höchst effektive Argumente dafür. Der Datenschutz als Teil des Schutzes der Persönlichkeitsrechte der betroffenen Versicherten scheint auf verlorenem Posten zu stehen.

Die im Risikostrukturausgleich zwischen den gesetzlichen Krankenkassen jetzt gesetzlich verankerten Disease Management Programme (DMPe) sind ein eindrucksvolles Beispiel für diese Entwicklung. Als Reaktion auf die wegen der nach Alter, sozialem Hintergrund und Gesundheitsrisiken höchst unterschiedlichen Zusammensetzung ihrer Mitglieder auseinanderklaffenden Finanzsituation der einzelnen Krankenkassen hat der Gesetzgeber bereits vor einigen Jahren den Risikostrukturausgleich (RSA) zwischen ihnen geschaffen. Er ist jetzt durch das Instrument der DMPe ergänzt worden: Je mehr Mitglieder einer Kasse an einem DMP teilnehmen, desto besser steht sie im RSA da. DMPe sollen Ablauf und Qualität der medizinischen Versorgung bei bestimmten chronischen Erkrankungen durch Einsatz verbindlich auf der Grundlage medizinischer Evidenz festgelegter und zwischen beteiligten Ärzten, Krankenhäusern und anderen Beteiligten aufeinander abgestimmter Behandlungsprozesse optimieren. Vorerst wurden per Rechtsverordnung Brustkrebs- und Diabetes-mellitus-Erkrankungen für die Entwicklung je eines DMP ausgewählt.

Die in Frage kommenden Versicherten können frei entscheiden, ob sie sich in ein DMP einschreiben. Verweigern sie sich, hat dies nur zur Folge, dass sie nicht an der neuen Versorgungsform teilnehmen können. Wollen sie teilnehmen, müssen sie in die dafür im SGB V und in der RSA-Verordnung vorgesehene Verarbeitung ihrer Daten einwilligen. Hier liegt das Problem: Die Kassen sollen die

Abrechnungen der Ärzte für ihre Leistungen an Teilnehmer an einem DMP einschließlich der Diagnosen und Befunde sowie fortlaufend detaillierte Dokumentationen der ärztlichen Behandlung und des Krankheitszustandes einschließlich der Befunde und Laborparameter, und dies alles jeweils versichertenbezogen, erhalten. Zum einen sollen die Kassen damit ihre Versicherten unterstützen und betreuen, zum anderen sollen die Dokumentationen dem Bundesversicherungsamt vorgelegt werden können, damit dieses stichprobenweise prüfen kann, ob einzelne Versicherte zu recht in das DMP einbezogen wurden. Wie die Betreuung der Versicherten - in der Begründung zum Entwurf für die RSA-Verordnung hieß es noch „Steuerung" - genau aussehen soll, ist bislang nicht transparent. Jedenfalls kommen die Kassen bei einer kleinen, aber kostenträchtigen Gruppe von Versicherten ihrer Vorstellung näher, anstelle der Ärzte die Behandlung ihrer Versicherten selbst zu lenken und zu koordinieren. Hat das SGB V diese Aufgabe nicht den Hausärzten übertragen? Aus der Sicht des Datenschutzes ist sie bei den Hausärzten jedenfalls besser untergebracht: Sie unterliegen der ärztlichen Schweigepflicht und dürfen ihre koordinierende Tätigkeit nur mit Einwilligung ihrer Patienten ausüben. Hingegen unterliegen die Mitarbeiter der gesetzlichen Krankenkassen, die derartige Lenkungs- und Beratungsfunktionen wahrnehmen sollen, keiner persönlichen Schweigepflicht. Selbst die auf meine Anregung hin und auf Vorschlag des Bundesbeauftragten für den Datenschutz in das Verfahren eingebauten Restriktionen (Regelungen zur Zugriffsbegrenzung, Zweckbindung, Datenlöschung) können nicht vergessen lassen, dass innerhalb der Kassen leider noch kein Beratungsgeheimnis besteht und dass sich die Kassen den Forderungen der Datenschützer, strenge technische und organisatorische Vorkehrungen für interne Begrenzungen für Zugriffe auf Versichertendaten zu treffen, bislang hartnäckig widersetzen. Leider hat auch der Bundesgesetzgeber die in dem Gesetzesbeschluss des Bundestages von 1999 (BR Drs. 609/99 Nr. 124a) verankerte Schweigepflicht für in den Kassen tätige Versichertenberater inzwischen wieder aus seinem legislativen Programm gestrichen. Man darf gespannt sein, für welche Zwecke die Kassen die ihnen offen stehenden ärztlichen Dokumentationen ihrer in ein DMP eingeschriebenen Mitglieder künftig nutzen werden.

Wenig beruhigend wirken die in der RSA-Verordnung gebliebenen Restbestände einer Pseudonymisierung des Versichertenbezugs der Dokumentationen. Zum einen sollen diese in nur wenig reduziertem Datenumfang den Kassen personenbezogen vorgelegt werden. Zum anderen soll die Pseudonymisierung laut Verordnung nicht etwa in einer für den Persönlichkeitsschutz der Betroffenen, sondern die in einer für die Zwecke der DMPe geeigneten Form erfolgen. Überdies sind die Voraussetzungen für die Herstellung des Versichertenbezugs weit gefasst. Zwar sollen die behandelnden Ärzte ihre Patienten vor jeder einzelnen Übermittlung einer Behandlungsdokumentation an die Kasse um Einwilligung bitten. Fehlen dieser aber zwei zeitlich fällige Dokumentationen hintereinander, wird der Patient aus dem DMP ausgeschlossen. Die Folge ist, dass eine bereits eingeleitete Behandlung aus medizinfremden Gründen geändert werden muss. Da bleibt wenig Spielraum für eine autonome Entscheidung des Patienten.

Inzwischen sind sowohl bundesweit als auch auf Bremen bezogen Entwicklungen zu beobachten, die jedenfalls einen Teil meiner Bedenken gegenstandslos werden lassen könnten. Bundesweit ist der Datensatz der Behandlungsdokumentationen, den die Krankenkassen versichertenbezogen erhalten sollen, reduziert worden, wie es heißt, auf das zwingend erforderliche Maß. Zudem hat mir die

Kassenärztliche Vereinigung Bremen kürzlich Unterlagen zu den Vereinbarungen über DMPe vorgelegt, die sie für das Land Bremen mit den gesetzlichen Krankenkassen abschließen will. Es scheint so, als könne man sich in Bremen darauf verständigen, dass die Krankenkassen diese Behandlungsdokumentationen nur zum Zwecke der Beratung der Versicherten, nicht etwa für eine darüber hinausgehende Steuerung nutzen dürften. Eine abschließende Wertung muss ich mir allerdings noch vorbehalten, da der Abstimmungsprozess noch läuft.

9. Jugend, Arbeit und Soziales

9.1 Interne Vernetzung des Amtes für Jugend und Familie Bremerhaven

Im August 2002 informierte ich mich auf der Grundlage des mir im letzten Berichtsjahr überreichten Datenschutzkonzeptes (vgl. 24. JB, Ziff. 9.1) über dessen technische Umsetzung hinsichtlich der Anbindung des Subnetzes des Amtes für Jugend und Familie an das Magistratsnetz, des dezentralen Netzzugriffs durch die Stadtteilbüros, der Konfiguration des Servers (Sicherheitseinstellungen, Domönestruktur, Benutzergruppen, Zugriffsrecht u. a.), auf dem die Software („KIK“) des allgemeinen Sozialdienstes installiert ist und der dezentralen Anwendung dieser Software im Stadtteilbüro Süd. Dabei konnte ich feststellen, dass die im Datenschutzkonzept beschriebenen Datensicherheitsmaßnahmen umgesetzt waren.

Aufgrund der über die Inhalte des Konzeptes gewonnenen hinausgehenden Informationen habe ich dem Amt weitere Vorschläge zur Verbesserung des Datenschutzniveaus gemacht. Die Konfiguration des Betriebssystems des Servers, auf dem sich die Datenbank mit den Klientendaten des allgemeinen Sozialdienstes befindet, sollte dokumentiert werden und ein höheres Sicherheitsniveau durch bestimmte Systemeinstellungen (wie z. B. Schutz der Dateien mit Sicherheitseinstellungen, keine Standardfreigaben, kein Gastzugang) erreichen. Da die Planungen für den Ersatz der Software „KIK“ bereits laufen, soll dieses bei der Neuinstallation entsprechend berücksichtigt werden.

Die Außenstellen des Amtes für Jugend und Familie (Stadtteilbüros) sind über Festverbindungen u. a. mit dem zentral im Verwaltungshochhaus/Stadthaus 1 untergebrachten Server verbunden, auf dem die „KIK-Software“ installiert ist und die Klientendatenbank liegt. Die Stadtteilbüros greifen über aktive Netzkomponenten auf das Netz zu. Um dieses ausreichend zu schützen, ist die Konfiguration dieser Komponenten, wie z. B. des Einwahlrouters (Packetfilter, Accesslisten, Abschaltung nicht benötigter Leistungsmerkmale, Schutz der Routingtabellen etc.) von zentraler Bedeutung. Der Router, über den die Stadtteilbüros auf das Magistratsnetz und auf die Daten von Klientinnen und Klienten innerhalb des Subnetzes des Amtes für Jugend und Familie zugreifen, wird von der B.I.T (Betrieb für Informationstechnologie Bremerhaven) verwaltet. Das Amt für Jugend und Familie bleibt aber verantwortlich für die Sicherheit seiner Daten.

Ich habe empfohlen, dass die für die Sicherheit des Subnetzes des Amtes für Jugend und Familie relevanten Sicherheitsinformationen der Administration zugänglich und jederzeit abrufbar sein sollten und evtl. an entsprechenden Stellen in das Netzkonzept integriert werden. Darüber hinaus sollten die Administrationstätigkeiten (insbesondere im Rahmen der Benutzerverwaltung) protokolliert und im Bedarfsfall (wie z. B. bei Verdacht unberechtigter Zugriffe oder im Rahmen einer Stichprobe) einer internen Revision, eventuell durch den Datenschutzbeauftragten des Amtes, unterzogen werden.

Ich gehe davon aus, dass meine Empfehlungen spätestens bei Einführung des neuen Systems berücksichtigt werden.

9.2 Vernetzung der städtischen Kindertagesheime und Einsatz von KIS

Das Kindergarten-Informationssystem (KIS) wurde zur automatisierten Verarbeitung der Sozialdaten von Eltern mit Kindern in Kindertagesheimen (KTH) für das Aufnahmeverfahren und die Beitragsberechnung vom Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales entwickelt. Es wurde seit 1998 in den 74 städtischen Kindertagesheimen auf Stand-Alone-Geräten eingesetzt. 1999 hatte ich das Verfahren insbesondere auf die Zulässigkeit der Datenkataloge, der verfügbaren Funktionen und der Sicherheit der Systemumgebung geprüft (vgl. 22 JB, Ziff. 9.1). Im April 2002 wurde mir vom Ressort der erste Entwurf einer Veränderung der technischen Infrastruktur des Systems zur Beratung vorgelegt.

Demnach sollen die Kindertagesheime an das Intranet der bremischen Verwaltung angeschlossen werden und in die Domäne der senatorischen Dienststelle über den Aufbau einer Terminalfarm (Terminalserver im Anwendungsmodus unter Windows 2000 mit dem Zusatzprodukt Citrix Metaframe) integriert werden. Zum Ende des Berichtsjahres soll das Verfahren im Echtbetrieb laufen. Dabei ändern sich die erfasste Daten, die Datenstruktur, die Bearbeitungsfunktionen und die Zugriffsstruktur nicht.

Die wesentliche technische Veränderung besteht darin, dass sich der Ort, wo Dateien und Datenbanken (File-Server) geführt werden sowie der Ort der Anwendungen (Terminalserver) von den einzelnen KTHs auf die senatorische Dienststelle verlagert. Die Rechner in den KTHs werden für das Verfahren als Terminals eingesetzt, d. h. es gibt keine lokalen Anwendungen und Datenspeicherungen mehr.

Wesentliche organisatorische Veränderung ist der zentrale administratorische Zugriff auf den File-Server als Speicherort der KTH-Daten. Hierzu habe ich zunächst verschiedene technische und organisatorische Datenschutzmaßnahmen formuliert. So habe ich die Installation von zwei Netzwerkkarten empfohlen, um ein Transfernetz zu bilden, das vom internen Netz der senatorischen Dienststelle getrennt ist; die Deaktivierung nicht benötigter Serverdienste und die Verschlüsselung der Daten auf dem Transportweg über Citrix (Codierung auf dem Niveau von 128 Bit vom Terminalserver zu den Clients und umgekehrt). Weiter soll ein Packetfilter auf Serverebene eingerichtet werden, der Internetzugang ohne Risiko für die Server im lokalen Netz gestaltet werden und eine möglichst gestaffelte Administration (Terminalserver, Domänenadministration, Administration des File-Servers) erfolgen.

Diese Anforderungen sind z. T. in den mir im Entwurf im August 2002 vorgelegten Datenschutzkonzept aufgenommen worden. Darüber hinaus enthält es angemessene Datensicherungsmaßnahmen auf der Ebene der lokalen Rechner in den KTHs, hinsichtlich der Authentifizierungsverfahren für den Zugang zum Bremer Verwaltungsnetz und dem Netz der senatorischen Dienststelle. Auch die bisherige Zugriffslogik durch eine entsprechende Datei- und Verzeichnisstruktur, gekoppelt mit dem Zugriffs- und Berechtigungssystem auf Netz- und Anwendungsebene, ist sichergestellt. Es fehlt im Konzept die Deaktivierung nicht benötigter Serverdienste. Das Ressort sagte jedoch eine entsprechende Überprüfung der Dienste zu. Für eine sichere Gestaltung des Internetzugangs ist es außerdem erforderlich, die Internetanbindung über

einen Terminalserver zu realisieren, der nicht in die Domäne des Ressorts integriert ist. Die bisherige Integration schließt eine direkte Gefährdung des internen Netzes durch Trojaner, Java-Applets, Active-X-Komponenten etc. nicht aus. Eine logische Trennung vom internen Netz ist daher notwendig.

Als datenschutzrechtlich erheblich problematisch bewerte ich das Fehlen eines Netzkonzeptes, auf das sich dieses Datenschutzkonzept bezieht.

Es ist, wie auch hier beim Einsatz vom Terminalservern für das Verfahren KIS, nicht möglich, einen Rückschluss aus den im Konzept beschriebenen Datensicherungsmaßnahmen auf die Systemumgebung zu ziehen. Dies bedeutet, dass eine unsichere Umgebung sich kontraproduktiv auf die für die Fachverfahren erstellten Sicherheitsstandards auswirken könnte. Es fehlt das Netzkonzept, dass die alle Komponenten umfassende Sicherheitsstruktur und den sensiblen Bereich der Administration inklusive Revision und Protokollierung beschreibt.

Für das Verfahren KIS ist in diesem Zusammenhang von besonderer Bedeutung, dass für die Aufbereitung der KTH-Daten zu Planungszwecken eine Abschottung zu den Sozialdaten sichergestellt wird.

Das bereits im Zusammenhang mit anderen Fachverfahren (wie etwa OASIS, SOLID, HORIZONT) von mir angemahnte Datenschutzkonzept für das interne Netz des Ressorts fehlt weiterhin. Ohne dieses Konzept und seine Umsetzung kann die Datensicherheit aller in diesem Netz laufenden Fachverfahren nicht gewährleistet werden. Ich habe deshalb die senatorische Dienststelle angeschrieben und werde weiterhin mit Nachdruck das entsprechende Konzept fordern.

9.3 Sozialgeheimnis im Amt für Soziale Dienste Bremen

Vor rund 10 Jahren habe ich durchgesetzt, dass innerhalb des Amtes für Soziale Dienste die Mitarbeiter nur Zugriff auf die Unterlagen der Klienten erhalten, die sie für die Erfüllung ihrer jeweiligen Aufgaben benötigen. Insbesondere ging es darum, dass Mitarbeiter der Wirtschaftlichen Jugendhilfe vom Sozialdienst nur bestimmte Unterlagen, die für die Kostenentscheidung erforderlich sind, erhalten. Dies sind der Antrag auf die Hilfe, der gesetzlich erforderliche Hilfeplan und das Protokoll der Hilfekonferenz. Alle anderen fachlichen Unterlagen, wie Gutachten und Berichte von Einrichtungen, verbleiben beim Sozialdienst. Dies wurde in zwei Dienstanweisungen der Amtsleitung festgehalten (vgl. zuletzt 17 JB, Ziff. 12.3.6).

Inzwischen ist das Amt umorganisiert worden. Seine Dienste sind in zwölf Sozialzentren zusammengefasst worden, Fall-Manager sollen die Wirtschaftliche Hilfe effektivieren. Auf meine Anregung hin und in Abstimmung mit mir ist nun die Dienstanweisung des Amtes zum Datenschutz in der Jugend- und Sozialhilfe überarbeitet worden. Dabei war mir wichtig, dass die oben skizzierte interne Differenzierung des Zugriffs auf Klientendaten erhalten blieb. Sie gilt jetzt ausdrücklich auch für die Zusammenarbeit innerhalb der und zwischen den Sozialzentren.

Die Gelegenheit wurde genutzt, die Dienstanweisung auch der aktuellen Gesetzeslage anzupassen. Erfreulich ist vor allem, dass den Mitarbeitern des Amtes jetzt klare Hinweise dafür gegeben werden, wie sie auf Amtshilfeersuchen anderer öffentlicher Stellen reagieren sollen. Dabei wurde insbesondere klargestellt, wie restriktiv der Gesetzgeber in § 68 Abs.1,2 Sozialgesetzbuch X (SGB) die

Voraussetzungen und den Umfang der Übermittlung von Sozialdaten gefasst hat, dass Amtshilfeersuchen nicht an einzelne Mitarbeiter, sondern an die Amtsleitung zu richten sind und dass schließlich die jüngst in § 68 Abs.3 SGB X zugelassenen Datenabgleiche zum Zwecke der Rasterfahndung nach Terroristen ein automatisiertes Verfahren, nicht jedoch Einzelanfragen bzw. -auskünfte zum Inhalt haben können.

9.4 Kooperation der Arbeits- und Sozialämter

Seit Jahren wird über die Neustrukturierung der Arbeits- und Sozialverwaltung diskutiert, um einen Abbau der Arbeitslosigkeit und eine Kostenminderung zu erreichen. Derzeit steht die Umsetzung der Empfehlungen der Hartz-Kommission an. Die u. a. in Rede stehende Integration von Arbeits- und Sozialämtern in Job-Centern oder die Zusammenführung von Arbeitslosen- und Sozialhilfe haben schon deshalb eine datenschutzrechtliche Dimension, weil Datenflüsse zwischen verschiedenen Sozialleistungsträgern, der Bundesanstalt für Arbeit und den Gemeinden als Trägern der Sozialhilfe intensiviert werden sollen. Da die Kontrollaufgaben sowohl des Bundesbeauftragten für den Datenschutz über die Bundesanstalt als auch die der Landesbeauftragten über die Sozialämter tangiert sind, ist auch deren Zusammenarbeit gefordert.

Bereits am 01.01.2001 ist das Bundesgesetz „zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe“ in Kraft getreten. In gleichlautenden in das SGB III – Arbeitsförderung – und in das Bundessozialhilfegesetz (BSHG) eingefügten Vorschriften

- wird den Arbeits- und Sozialämtern die Möglichkeit eröffnet, gemeinsame Anlaufstellen (Vorläufer der Job-Center in der Terminologie der Hartz-Kommission) zu schaffen und
- wird dem Bundesministerium für Arbeit und Sozialordnung die Aufgabe übertragen, regionale Modellvorhaben (MoZarT) zu fördern.

Als ich im November 2002 durch einen Pressebericht davon erfuhr, dass in Bremen geplant sei, Arbeits- und Sozialamt kooperieren zu lassen, wandte ich mich an das kommunale Amt für Soziale Dienste (AfSD), in das in Bremen das Sozialamt eingegliedert ist und bat um Auskunft über datenschutzrechtlich relevante Schritte. Dabei bot ich meine Beratung an. Zugleich unterrichtete ich den Bundesbeauftragten für den Datenschutz davon. Das Amt nahm mein Beratungsangebot an. Zunächst - so hieß es - sei an die Installation von Schnittstellen zwischen den Informationssystemen beider Seiten noch nicht gedacht. Vielmehr sollten lediglich Mitarbeiter des kommunalen Amtes in Räumen des Arbeitsamtes arbeiten und dort über einen Bildschirm Zugriff auf Sozialhilfedaten über das Programm PROSOZ, über einen anderen Bildschirm auf im System des Arbeitsamtes gespeicherte Sozialdaten nehmen können. Nach Erhalt genauerer Informationen über Umfang und Verfahren des Datenaustauschs (Erhebung und Nutzung der durch den Kooperationspartner gespeicherten Sozialdaten sowie deren Übermittlung an diesen) werde ich in Abstimmung mit dem Bundesbeauftragten für den Datenschutz das Projekt beraten und bewerten.

Im Lande Bremen ist als MoZArT-Projekt die Einrichtung von Assessment-Centern in Bremen und in Bremerhaven bewilligt worden. Die Projekte laufen vom 01.01.2002 bis zum 30.04.2003. Die Center selbst werden durch zwei Gesellschaften privaten Rechts betrieben. Ihre Aufgabe ist es, die berufliche

Eignung (Potenzialanalyse) von insgesamt 800 ihnen durch Arbeits- oder Sozialamt zugewiesenen Erwerbslosen zu ermitteln und auf einem ausführlichen Ergebnisbogen dorthin zurückzumelden. Das Bundesrecht legitimiert die zur Durchführung der MoZArT-Projekte erforderliche Verarbeitung von Sozialdaten. Dank schriftlicher Auskünfte des AfSD Bremen, des Amtes für kommunale Arbeitsmarktpolitik Bremerhaven und der Träger der beiden Assessment-Center sowie eines Gesprächs mit dem AfSD und dem Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales konnte ich feststellen, dass die Betroffenen vor ihrer Zuweisung und der Übermittlung ihrer Daten an das Assessment-Center ausreichend unterrichtet und um ihr Einverständnis in die hierfür erforderliche Übermittlung ihrer Daten gebeten werden. Allerdings wurde sowohl in Bremen als auch in Bremerhaven die Bitte um Erteilung des Einverständnisses mit dem Hinweis auf die Mitwirkungspflichten von Hilfeempfängern und der Androhung der Kürzung von Leistungen bei Nichterscheinen bzw. Abbruch der Teilnahme ohne Grund verbunden. Die Teilnahme am Assessment-Verfahren sollte also nicht etwa auf einer freiwilligen Entscheidung beruhen. Nun ist es aber auch Vorgabe des Bundesgesetzgebers, die Modellvorhaben so auszugestalten, dass den Arbeitslosen durch ihre Einbeziehung keine rechtlichen und finanziellen Nachteile entstehen. Auf meinen entsprechenden Hinweis hin teilte mir das AfSD mit, man sehe inzwischen davon ab, bei Verweigerung des Einverständnisses in die Zuweisung Leistungen zu kürzen. Vom Bundesbeauftragten für den Datenschutz erfuhr ich inzwischen, das Arbeitsamt Bremen kläre die von ihm zugewiesenen Arbeitslosen darüber auf, dass sie ohne für sie nachteilige Folgen über eine Teilnahme an der Maßnahme entscheiden könnten. Ich habe verlangt, die Betroffenen auf diese Änderung hinzuweisen.

Das Bundesministerium für Arbeit und Sozialordnung beauftragte „infas“ mit der im SGB III und im BSHG vorgesehenen bundesweiten Auswertung der MoZArT-Projekte. Das ursprünglich von „infas“ den obersten Landessozialbehörden, d. h. auch dem Bremer Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales zur Genehmigung vorgelegte Konzept sah vor, dass die an Modellprojekten beteiligten Arbeits- und Sozialämter, aber zum Vergleich auch nicht beteiligte Ämter, personenbeziehbare Daten aller Hilfeempfänger ohne deren Einwilligung an „infas“ übermitteln sollten. Zwar ist dies gesetzlich nicht ausgeschlossen, sofern es für die Durchführung des Vorhabens erforderlich ist, schutzwürdige Belange der Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an dem Vorhaben erheblich überwiegt. Wegen des Umfangs der einzelnen Datensätze, aber auch des gesamten dann bei „infas“ zur Verfügung stehenden Datenbestandes legten die Datenschutzbeauftragten des Bundes und der Länder einhellig Wert darauf, dass entsprechend der Vorgabe der jüngst neu gefassten Datenschutzgesetze von der Möglichkeit zur Pseudonymisierung der Daten Gebrauch gemacht wird. In einem langwierigen Prozess der Auseinandersetzung und Abstimmung gelang es, mit „infas“ und den Genehmigungsbehörden ein Konzept abzustimmen, in dem die übermittelten Datensätze so verkürzt sind, dass „infas“ die einzelnen Hilfeempfänger nicht identifizieren kann, aber doch die einzelnen Fälle umfassend auswerten kann, und dies auch dann, wenn ein Arbeitsloser Hilfe sowohl vom Arbeits- als auch vom Sozialamt bezogen hat.

Das Amt für Soziale Dienste Bremen und das Sozialamt Bremerhaven wurden überdies in der Genehmigung verpflichtet, vor der Übermittlung personenbezogener Adress- und Telefondaten einer

Auswahl von Hilfeempfängern an „infas“ für eine telefonische Befragung die davon Betroffenen auf die beabsichtigte Übermittlung hinzuweisen und ihnen Gelegenheit zum Widerspruch zu geben. Damit wurde eine im April 2002 in das Bundessozialhilfegesetz eingefügte Anforderung umgesetzt. Ich konnte mich im Berichtsjahr auch davon überzeugen, dass bei der bundesweit durch „infas“ und des Zentrum für Sozialpolitik der Universität Bremen durchgeführten „Verlaufs- und Ausstiegsanalyse“, in deren Rahmen ehemalige Sozialhilfeempfänger befragt werden, das Hinweisgebot beachtet wird.

9.5 Mitteilungen über Maßnahmeaustritt an Bremer Arbeit GmbH

Ein Beschäftigungsträger hat mir das formalisierte Schreiben „Mitteilungen über Maßnahmeaustritt“ der Bremer Arbeit GmbH (BAG) zur Prüfung vorgelegt. Insbesondere wurde moniert, dass die BAG nach diesem Formularschreiben von den Beschäftigungsträgern eine Kopie des Arbeits- bzw. Fort- und Weiterbildungsvertrages verlangt, obwohl diese Verträge eine Vielzahl von Daten enthalten, die für die Wahrnehmung von Kontrollbefugnissen der BAG nicht erforderlich sind.

Darüber hinaus wurde mit dem Formularschreiben der BAG verlangt, die konkreten Gründe beim „Abbruch aus persönlichen Gründen“ anzugeben, obwohl es ausreicht, dort ebenfalls aufgeführte bestimmte standardisierte Gründe anzukreuzen. Außerdem sollten die jeweiligen Vermittlungshemmnisse frei angegeben werden, obwohl es sich hierbei um hoch sensible Daten, z. B. über psychische Beeinträchtigungen, handeln kann.

Die BAG hat das Formularschreiben aufgrund meiner vorgenannten Bedenken und Anregungen entsprechend umgestaltet.

9.6 Bremer und Bremerhavener Arbeit GmbH

Das Land Bremen hat in 2001 seine Eigengesellschaften Bremer Arbeit GmbH (BAG) und Bremerhavener Arbeit GmbH (BRAG) mit der Förderung von Maßnahmen im Rahmen seines beschäftigungspolitischen Aktionsprogramms beauftragt. Rechtsgrundlage der Beleihungsverträge ist das Gesetz zur Übertragung von Aufgaben staatlicher Förderung an juristische Personen privaten Rechts (Beleihungsgesetz) einschließlich seiner Anlagen 4 und 5. Ich habe im Berichtsjahr beide Gesellschaften beraten.

Die BAG führt auch die arbeitsmarktpolitischen Förderprogramme der Stadtgemeinde Bremen durch. Sie berät und vermittelt ihr vom kommunalen Amt für Soziale Dienste zugewiesene arbeitslose Sozialhilfeempfänger. Damit sind ihr Aufgaben der Hilfe zur Arbeit nach dem Bundessozialhilfegesetz (BSHG) übertragen worden, die bisher der kommunale Eigenbetrieb Werkstatt Bremen wahrgenommen hatte. Somit hat die BAG wie ein Sozialleistungsträger das Sozialgeheimnis ihrer Klienten nach Maßgabe des Sozialgesetzbuches zu wahren. Ich habe der BAG darüber hinaus empfohlen, das Sozialgesetzbuch (SGB) auch dann anzuwenden, wenn sie in Durchführung von Landesaufgaben Beschäftigungsträger fördert und im Rahmen von deren Kontrolle die Daten der Teilnehmer verarbeitet.

Anders verhält es sich bei der BRAG. Sie hat nur Landesaufgaben, etwa die der finanziellen Förderung von Beschäftigungsträgern, übernommen. In Bremerhaven ist die Hilfe zur Arbeit beim

kommunalen Amt für Arbeitsmarktpolitik verblieben. Die BRAG nimmt daher nicht die Aufgaben eines Sozialleistungsträgers wahr. Sie wird allerdings wie die BAG in Handlungsformen des öffentlichen Rechts tätig. Ich habe der BRAG deshalb empfohlen, ihre Datenverarbeitung, z. B. die der Teilnehmer an geförderten Beschäftigungsmaßnahmen, in den Rahmen des Bremischen Datenschutzgesetzes zu stellen.

Nachdem jetzt auch das Bremische Datenschutzgesetz (BremDSG), wie zuvor schon das Sozialgesetzbuch (SGB), grundlegend novelliert worden ist, bedeutet dies nicht, dass die BRAG im Vergleich zur BAG ein wesentlich geringeres Datenschutzniveau einzuhalten haben wird. So verpflichtet nunmehr das BremDSG auch sie, einen eigenen Datenschutzbeauftragten zu bestellen. Ich habe die BRAG darauf hingewiesen.

Die BAG hatte mir zur Prüfung und Bewertung die Vordrucke vorgelegt, auf denen sie gegenüber der Europäischen Union über von ihr mit Mitteln aus dem Europäischen Sozialfonds geförderte Beschäftigungsprojekte und deren Teilnehmer berichten sollte. Ich konnte feststellen, dass die Teilnehmerdaten vor Übermittlung der ausgefüllten Unterlagen anonymisiert werden sollen bzw. bei der BAG – das gleiche gilt für die BRAG – verbleiben sollen und dort bei Stichproben von Beauftragten der EU eingesehen werden können. Hiergegen habe ich keine Einwände erhoben, vorausgesetzt, dass die diesem Verfahren zugrundeliegende Berichtspflicht der Träger der BAG bzw. der BRAG gegenüber der BAG bzw. der BRAG durch die Arbeitsverträge mit den Teilnehmern bzw. durch deren Einwilligungen legitimiert sind. Mir ist durch Beratungsgespräche mit einzelnen Trägern bekannt, dass davon ausgegangen werden kann, dass dies berücksichtigt wird.

Ein anderer Vordruck wurde von der BAG auf meinen Vorschlag hin geändert. Ein Beschäftigungsträger hatte ihn mir zur Prüfung und Bewertung vorgelegt. Auf dem Formular sollten Beschäftigungs-, Fortbildungs- und Weiterbildungsträger bei Abbruch einer durch die BAG geförderten Maßnahme durch einen Teilnehmer - wohl zwecks Evaluation und Controlling - über die Gründe des Abbruchs berichten. So wurde für den Fall, dass Grund des Abbruchs die Aufnahme einer Beschäftigung ist, die Vorlage der Kopie des Arbeitsvertrages verlangt. Ich wandte dagegen ein, der frühere Teilnehmer sei doch nicht gehalten, dem Maßnahmeträger diesen Vertrag zu überlassen. Überdies enthalte dieser Daten, die für die BAG nicht relevant seien. Die BAG begnügt sich inzwischen mit der bloßen Angabe, dass der „Abbrecher“ eine Beschäftigung aufgenommen habe. Zugleich verlangte die BAG bei Abbrüchen aus persönlichen Gründen deren konkrete Angabe. Auch etwaige Vermittlungshemmnisse sollten konkret angegeben werden. In beiden Fällen kann es sich um höchst sensible Daten handeln, etwa um psychische Beeinträchtigungen. Auf meinen Vorschlag hin verlangt die BAG nunmehr, dass der Träger eine von mehreren standardisierten Begründungskategorien ankreuzt.

9.7 „Bürgertelefone“ in Bremen und Bremerhaven

In Bremerhaven öffentlich höchst umstritten, in Bremen ohne nennenswerte öffentliche Debatte, wurden im Berichtsjahr in den beiden Städten sogenannte „Bürgertelefone“ installiert, allerdings mit unterschiedlichen Zielsetzungen. Einmal geht es um die Aufdeckung von Sozialhilfemissbrauch, einmal um die Aufdeckung von Schwarzarbeit.

In Bremerhaven wurde im Vorzimmer der Leitung des Sozialamts ein Telefonanschluss für die Annahme von Anrufen von Bürgern eingerichtet. Die Bremerhavener wurden öffentlich aufgefordert, dort bei Verdacht auf Sozialhilfemissbrauch anzurufen. In Bremen hingegen lehnte der Senat dies ab. Vor Ablauf eines halben Jahres nach Einrichtung ist der Bremerhavener Anschluss inzwischen abgeschaltet worden. Dies wurde mit der geringen Zahl der eingegangenen Anrufe, insgesamt 36, vor allem aber mit deren Mangel an Stichhaltigkeit begründet, denn nur einer habe zu einer Anzeige geführt

In Bremen hingegen ist nach wie vor bei der Koordinierungsstelle zur Bekämpfung illegaler Beschäftigung des Senators für Arbeit, Frauen, Gesundheit, Jugend und Soziales ein Telefonanschluss geschaltet und öffentlich bekannt gemacht worden, über den Hinweise auf illegale Beschäftigung und Schwarzarbeit entgegengenommen werden. Innerhalb eines halben Jahres seien 173 Hinweise eingegangen.

Für beide Fälle gilt, dass ich mich an einer bewertenden Diskussion unter Stichworten wie Missbrauchsbekämpfung oder Denunziantentum nicht beteiligt habe. Ich habe allerdings den verantwortlichen Stellen kritische Fragen nach der Rechtsgrundlage, der Überprüfung der Hinweise, dem Speichermedium, der Transparenz für die Betroffenen und der Löschung haltloser Vorwürfe vorgelegt. Insbesondere ging es mir darum, dass die Betroffenen Kenntnis vom Vorwurf erhalten, dass sie Auskunft und Einsicht verlangen können und dass ihnen auf diese Weise Gelegenheit zur Stellungnahme gegeben wird.

Während das Sozialamt Bremerhaven mir - vor Abschaltung seines Anschlusses - durchweg zufriedenstellende Erklärungen gegeben hat, bemühe ich mich noch, mit den Bremer Verantwortlichen den rechtlichen Rahmen für ihr „Bürgertelefon“ zu klären. Ich habe Zweifel daran angemeldet, ob der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales zur Erfüllung eigener gesetzlicher Aufgaben befugt sei, zulasten der von Hinweisen betroffenen Bürger deren Daten zu verarbeiten. Zum anderen habe ich um Unterlagen gebeten, die ggf. belegen können, dass seitens anderer zuständiger Stellen, etwa der mit der Verfolgung von illegaler Beschäftigung und Schwarzarbeit, ein Auftrag zur Datenverarbeitung erteilt wurde. Zu klären ist insbesondere, welches die für die Rechtmäßigkeit der Datenverarbeitung verantwortliche und den Betroffenen gegenüber auskunftspflichtige Stelle ist. Ich verweise insofern auf die Bedenken, die ich gegen die seinerzeit geplante Einrichtung eines Informationsverbundes gegen illegale Beschäftigung bei derselben Stelle geäußert hatte (vgl. zuletzt 22. JB, Ziff. 9.3).

10. Bildung und Wissenschaft

10.1 Schulen ans Netz – Internet-Nutzung durch Schulen

Zu Beginn des Berichtsjahres trat endlich die kleine Arbeitsgruppe „Schulen im Netz, Datenschutz“ zusammen, bestehend aus Vertretern des Senators für Bildung und Wissenschaft und des Landesinstituts für Schulen (LIS) sowie des Landesbeauftragten für den Datenschutz, um die lange diskutierte Orientierungshilfe für die Internet–Nutzung an Schulen zu erarbeiten. Ausgangspunkt waren ein von mir erstelltes Thesenpapier zur Internet–Nutzung durch Schulen (vgl. 22. JB, Ziff. 10.3), meine Internet-Präsentation sowie Papiere einiger meiner Kollegen zur gleichen Thematik. Ein erstes Arbeitspapier (Entwurf) der Kultusminister-Konferenz zur Internet-Nutzung der Schulen wurde im Verlauf der Beratungen der Arbeitsgruppe zwar noch in die Diskussion eingeführt, konnte aber wegen des unterschiedlichen Ansatzes und der unterschiedlichen Stoßrichtung („Schulen ans Netz, Medienkompetenz der Schulen“) nicht mehr verwertet werden.

Die Mitglieder der Arbeitsgruppe haben sich zweimal getroffen und über die Strukturierung der Arbeit und terminliche Vorstellungen gesprochen. Zugleich wurden auch erste inhaltliche Diskussionen geführt. Der Landesbeauftragte hatte es übernommen, für die 3. Sitzung eine aktualisierte und auf die bremischen Besonderheiten abgestellte Orientierungshilfe zu formulieren, während die Vertreter des Bildungssenators und des LIS sich um die Punkte „Nutzungsordnung“ und „Kurzfassung Orientierungshilfe und Rundverfügung an die Schulen“ kümmern wollten.

Der Entwurf einer Orientierungshilfe wurde Mitte April 2002 vom Landesbeauftragten vorgelegt, der Entwurf einer Rundverfügung des Bildungssenators an die Schulen ebenfalls. Diese Materialien sollten bei der 3. Sitzung der Arbeitsgruppe Ende April/Anfang Mai 2002 erörtert und nach Möglichkeit auch beschlossen werden. Zu der 3. Sitzung der Arbeitsgruppe und zu einer Abstimmung der Entwürfe ist es nicht mehr gekommen, weil der Bildungssenator und das LIS sich nicht mehr an der Arbeitsgruppe beteiligten. So konnten die Arbeitsergebnisse leider auch nicht – wie es eigentlich geplant war – noch vor den Sommerferien fertiggestellt, gemeinsam publiziert und per Rundverfügung verbindlich gemacht werden.

Im Oktober des Berichtsjahres legte der Bildungssenator dem Datenschutzausschuss der Bremischen Bürgerschaft auf dessen Drängen hin eigene Materialien zu dieser Materie vor, und zwar

- eine stark an das entsprechende Papier der Kultusminister-Konferenz angelehnte Orientierungshilfe für den Einsatz des Internets an Schulen,
- einen Musterentwurf für eine Nutzungsordnung der Computereinrichtungen an Schulen,
- einen Musterentwurf für eine Nutzungsordnung für Grundschülerinnen/Grundschüler und für Schülerinnen/Schüler mit besonderem Förderbedarf sowie
- Richtlinien zur schulischen Nutzung des Internets.

Die Themen dieser Papiere sind weiter gefasst. Die Orientierungshilfe des Bildungssenators ist auf die Schule und ihre medienpädagogische Arbeit ausgerichtet und nicht nur datenschutzrechtlich auf die Schule als öffentliche Stelle bzw. Verwaltungsinstitution und als Nutzer bzw. Anbieter von Telekommunikations- und Telediensten ausgerichtet.

Formal mag damit einem allgemeinen Anliegen Rechnung getragen sein, für die praktische Handhabung des Datenschutzes in den Schulen halte ich aber nach wie vor mein Papier für die geeignetere Grundlage. Ich werde daher ergänzend dieses Papier auf meiner Homepage publizieren.

10.2 Führung von Schullaufbahnakten

Im vergangenen Jahr habe ich meine Prüfungen hinsichtlich der Führung von Schullaufbahnakten fortgesetzt. Erneut stellte ich hierbei gravierende Mängel fest. So fehlten wiederum an den überprüften Schulen in den geführten Akten die erforderlichen Einwilligungserklärungen für die Aufnahme von Unterlagen mit besonders sensiblen Daten, wie z. B. Gesundheits- und Verhaltensdaten in den Teil B der Akte, was grundsätzlich nur mit der Einwilligung der Betroffenen bzw. deren Erziehungsberechtigten zulässig ist. Auch gab es in den Akten keine Erklärung der Schulleitung, mit der diese die Einwilligungserklärung der Betroffenen ggf. ersetzen könnten. Darüber hinaus waren an einer Schule in Teil B der Akten eine Reihe von für schulische Zwecke völlig ungeeignete Unterlagen abgelegt, so im Falle eines Schülers der 7. Jahrgangsstufe umfangreiche allgemeine Verwaltungsunterlagen über ein Verfahren der Spätaussiedlung. Hier war mir bereits eine Erforderlichkeit zur Aufbewahrung der Unterlagen in keinster Weise ersichtlich. Soweit für einen Schüler weiterwirkende Daten aufbewahrt oder an eine andere Schule weitergegeben werden, halte ich dies bei Einhaltung der Regularien für unkritisch. Die geltenden Regelungen sollen lediglich verhindern, dass eine Sache, die schon längst abgetan ist, einem Schüler nicht über die gesamte Schullaufbahn anhängt.

Kritisiert habe ich außerdem das Verfahren der Weitergabe des Teils B der Schullaufbahnakte beim Wechsel eines Schülers an eine andere allgemeinbildende öffentliche Schule. Auch in diesem Punkte mangelte es an der notwendigen Einwilligungserklärung bzw. der Abgabe einer Ersetzungserklärung durch den Schulleiter.

Eine Sperrung von Daten in der Schullaufbahnakte, wie sie nach § 18 Abs. 1 BremSchulDSG vorgesehen ist, war an beiden Schulen bislang nicht erfolgt. Die Sperrung der Akten hätte zur Folge, dass die in den Akten enthaltenen personenbezogenen Daten zwar weiterhin gespeichert bleiben dürfen, eine weitergehende Verarbeitung jedoch nur noch zu eng bestimmten Zwecken zulässig ist.

Darüber hinaus waren an beiden Schulen die Fristen für die Aufbewahrung bzw. die Vernichtung der Schullaufbahnakten ausgeschiedener Schülerinnen und Schüler nicht eingehalten worden. Die regelmäßige Aufbewahrungsdauer beträgt für Schullaufbahnakten nach der Richtlinie über die Sicherung, Aufbewahrung und Aussonderung von Schriftgut in den Schulen drei Jahre. Die Aufbewahrungsfristen waren an beiden Schulen erheblich überschritten worden, an einer der beiden Schulen war eine Vernichtung bislang gar nicht erfolgt.

Begründet worden sind die festgestellten Mängel von den Schulen mit Arbeitsüberlastung und Zeitmangel. Fehlende Ressourcen würden die Verwaltungstätigkeit an den Schulen zunehmend erschweren.

Ich habe die Mängel gegenüber beiden Schulen gerügt und sie zu deren Beseitigung aufgefordert. Mir ist in der Zwischenzeit von beiden Schulen bestätigt worden, dass sie das erledigt haben. Es geht also doch!

Auch der Datenschutzausschuss der Bremischen Bürgerschaft hat sich im Herbst 2002 mit der Führung der Schullaufbahnakten befasst. Dabei erklärten die Vertreter des Senators für Bildung und Wissenschaft, dass sie eine Dienstanweisung erarbeiten wollten, die die Schulen zur Beachtung der datenschutzrechtlichen Bestimmungen anhält. Außerdem sollten für die Mitarbeiterinnen und Mitarbeiter der Schulverwaltungen Fortbildungsmaßnahmen zur Führung der Schullaufbahnakten angeboten werden. Schließlich solle bei den Schulleiterkonferenzen künftig ein Jurist anwesend sein, der über die zu beachtenden Rechtsvorschriften informieren kann. Ich werde dies zu gegebener Zeit überprüfen.

10.3 Abgabe eines Klassenbuchs an die Presse

Ein pensionierter Lehrer informierte mich Ende vergangenen Jahres darüber, dass bei Umbauarbeiten an seiner ehemaligen Schule ein bislang als gestohlen verzeichnetes Klassenbuch, das noch aus dem Schuljahr 1985/86 stammte und für eine seiner früheren Schulklassen geführt wurde, aufgefunden worden war. Genauer gesagt, war das Klassenbuch bei der Herausnahme von Deckenplatten in einem Klassenraum, über dem sich das Buch in einem Hohlraum befand, von der Decke gefallen. Wie mir der Hinweisgeber weiter mitteilte, enthielt das Buch zahlreiche Informationen über die Schülerinnen und Schüler seiner ehemaligen Klasse und auch Fotos von diesen. Von der Schule war das Buch an eine Bremer Tageszeitung weitergegeben worden, Auszüge aus ihm sollten veröffentlicht werden. An sich ein spannender Fall, aber man hat nicht in der Hand, was die Presse daraus veröffentlicht.

Ich habe daraufhin den Senator für Bildung und Wissenschaft darauf hingewiesen, dass auch Klassenbücher von der verantwortlichen Schule mit besonderer Sorgfalt zu behandeln sind, um einen Missbrauch der darin enthaltenen Daten auszuschließen. Der Senator für Bildung und Wissenschaft hat zudem in den Richtlinien über die Sicherung, Aufbewahrung und Aussonderung von Schriftgut in den Schulen für die Aufbewahrung von Klassenbüchern eine Frist von drei Jahren, nachdem dort der letzte Vorgang eingetragen wurde, festgelegt. Da die Aufbewahrungsfrist bereits viele Jahre überschritten worden war, hätte das Klassenbuch nach seinem Auffinden von der Schule vernichtet werden müssen. Die Übersendung des Klassenbuchs an die Bremer Tageszeitung war zudem unzulässig gewesen. Allenfalls mit Einwilligung der Betroffenen hätten einzelne Informationen oder Seiten preisgegeben werden können.

Die Zeitung hat das Klassenbuch dem Senator für Bildung und Wissenschaft ausgehändigt, wo es vernichtet wurde.

10.4 Forschungsvorhaben und Schulbegleitforschungsprojekte

Im vergangenen Jahr bin ich erneut mit einer Vielzahl von Forschungsvorhaben und Schulbegleitforschungsprojekten befasst worden, die das Verhalten, die Einstellungen, das Umfeld oder aber auch die Leistungsfähigkeit von Schülerinnen und Schülern betrafen. Unter anderem handelte es sich diesmal bei den Vorhaben um eine Fragebogenaktion im Rahmen der kinder- und jugendpsychiatrischen Diagnostik, eine Untersuchung zum Thema „Lebenssituation lernbehinderter Schüler auf der Grundlage neuerer sozialstruktureller Modelle“ und Befragungen zur Erforschung von Mathematikkenntnissen bei Grundschulkindern.

Daneben ging es um einen Englischtest (DESI-Voruntersuchung-SET 10 Test), der die englische Sprachfähigkeit von zufällig ausgewählten Schülern (5 Schulen, je 12 Schüler) testen und bei positivem Ergebnis in eine Haupterhebung münden soll.

Bei der Fragebogenaktion im Rahmen der kinder- und jugendpsychiatrischen Diagnostik handelte es sich um eine bundesweit durchgeführte Befragung des Universitätsklinikums Charité der Humboldt-Universität Berlin, bei der Lehrkräfte umfangreiche personenbezogene Angaben über das Verhalten ihrer Schüler machen sollten. Die Daten bezogen sich sowohl auf die Lehrkräfte, die die Fragebögen ausfüllen sollten, als auch die Schüler, über die die Auskünfte erteilt werden sollten.

In meiner Stellungnahme zu der in Bremen und Bremerhaven an insgesamt 14 Schulen geplanten Befragungsaktion habe ich insbesondere auf die Notwendigkeit der Abgabe einer Einwilligungserklärung durch die Erziehungsberechtigten hingewiesen. Waren die Erziehungsberechtigten der betroffenen minderjährigen Schüler zur Abgabe einer Einwilligungserklärung nicht bereit, so durften die Lehrkräfte zu den betreffenden Schülern keine Angaben machen. Daneben konnte auch die Beteiligung der Lehrkräfte an der Befragungsaktion nur auf freiwilliger Basis erfolgen. Des Weiteren habe ich u. a. auch eine aus meiner Sicht notwendige Anonymisierung der vorgesehenen Fragebögen und Verbesserungen im Hinblick auf den Ablauf der Befragung angeregt. Meine Verbesserungsvorschläge wurden bei der Durchführung der Befragungen im Lande Bremen berücksichtigt. Das Landesinstitut für Schule hat seine nach § 13 Abs. 7 BremSchulDSG erforderliche Genehmigung der Erhebung von der Beachtung meiner Verbesserungsvorschläge abhängig gemacht. Eine Antwort der Charité hierzu steht noch aus.

Die Untersuchung zum Thema „Lebenssituation lernbehinderter Schüler auf der Grundlage neuerer sozialstruktureller Modelle“ wurde ebenfalls bundesweit durchgeführt. Es handelt sich hierbei um eine Untersuchung der Julius-Maximilians-Universität Würzburg, bei der die Eltern minderjähriger Schüler an Förderschulen, darunter zwei Förderzentren in Bremen, mittels eines standardisierten Fragebogens nach ihren Lebensbedingungen befragt werden sollten.

Auch zu dieser Untersuchung habe ich auf die Bedeutung der Freiwilligkeit der Teilnahme an der Befragung hingewiesen und Anregungen zur datenschutzgerechteren Gestaltung des Erhebungsverfahrens und der Wahrung der Anonymität bei der Durchführung der Untersuchung gegeben. Meine Anregungen konnten bei der Durchführung der Untersuchung noch Berücksichtigung finden.

Verbesserungsvorschläge, die insbesondere die Einwilligung und freiwillige Teilnahme an der Erhebung und die Gestaltung des Erhebungsverfahrens betrafen, habe ich auch hinsichtlich der Durchführung der an mehreren Bremer Grundschulen geplanten Erhebungen zur Erforschung von Mathematikkenntnissen bei Grundschulkindern gemacht. Auch bei diesen Erhebungen wurden meine Empfehlungen berücksichtigt.

Vorbereitet für das Jahr 2003 werden derzeit mehrere große Schulleistungsstudien, u. a. die deutsche Ergänzungsstudie PISA 2003 und die DESI-Hauptuntersuchung (Deutsch-Englisch-Schülerleistungen-International). Ziel dieser Studien ist es, die Bildungsadministration mit Informationen zur Qualität des Schulsystems zu versorgen. In beiden Studien sollen Schülerinnen und Schüler hinsichtlich ihres Leistungsvermögens getestet und befragt sowie Eltern und Lehrkräfte zu verschiedenen Themen ihres persönlichen und beruflichen Umfeldes um Auskunft gebeten werden. Im Einklang mit den Datenschutzbeauftragen der anderen Bundesländer werde ich diese Vorhaben datenschutzrechtlich begleiten.

10.5 Lernschwächebericht per Fehlfax an privaten Haushalt

Wiederholt bin ich mit Fällen befasst worden, in denen Unterlagen mit sehr sensiblen personenbezogenen Daten per Telefax fehlübermittelt wurden und somit unbeteiligte Dritte von Vorgängen Kenntnis erlangt haben, die ihnen auf keinen Fall hätten bekannt werden dürfen.

So war in Bremen bei einem privaten Haushalt per Fax die Stellungnahme einer Schule zur Fördersituation eines Kindes im Hinblick auf eine wegen einer Lese-/Rechtschreibschwäche beantragten Förderung eingegangen. Eigentlich hatte die Schule die Stellungnahme an das Amt für Soziale Dienste faxen wollen, wo ein Antrag auf Unterstützung der Fördermaßnahme gestellt worden war.

Die Stellungnahme der Schule zur Fördersituation des betroffenen Kindes enthielt sehr umfangreiche Aussagen zu den Lernproblemen sowie zu den sozialen und emotionalen Problemen des betroffenen Kindes. Attestiert wurde dem Kind u. a., dass ohne eine gezielte Förderung sein ohnehin schon deutlicher Abstand zu den Leistungen der von ihm besuchten Klasse noch größer werde, Frustration und „Nichtkönnen“ sich verfestigten und es emotional sehr stark belastet würde. Bei der Wiederholung der 1. Klasse habe das Kind viel Zeit damit verbracht, sich in der neuen Klasse zurechtzufinden, seine Ängste abzubauen und Vertrauen zu sich und anderen Kindern zu entwickeln. Statt zu lernen und seine Aufgaben zu erfüllen, habe es lieber gemalt und gespielt und dadurch in den ersten beiden Klassen viel versäumt.

Die Schule begründete die Fehlübersendung des Telefaxes damit, dass irrtümlicherweise in das Telefax-Gerät eine falsche Fax-Nummer eingegeben wurde, was dazu führte, dass die betreffende Privatperson die Stellungnahme erhielt. Eine besondere Eilbedürftigkeit wurde nicht dargelegt. Gleichwohl hatte die Schule mit der Übersendung der Stellungnahme per Telefax eindeutig gegen die Telefax-Regeln der bremischen Verwaltung verstoßen. Diese sehen u. a. vor, dass bestimmte Daten aufgrund vorgeschriebener Versandart oder wegen ihrer Sensibilität (z. B. Personalangelegenheiten,

gesundheitliche Verhältnisse, Ordnungswidrigkeiten, strafbare Handlungen) nicht gefaxt werden dürfen. Auch die Stellungnahme der Schule hätte nicht per Fax übermittelt werden dürfen.

11. Bau, Verkehr und Umwelt

11.1 Datenerhebung in Kleingartengebieten

Im Frühjahr 2001 ist in den Medien darüber berichtet worden, dass Sachbearbeiter des Bauordnungsamtes auf speziellen Prüfbögen eine Vielzahl von Feststellungen vornehmen, um zu prüfen, ob in den Kleingärten unzulässig dauerhaft gewohnt wird. Daraufhin habe ich das Verfahren der Datenerhebung geprüft.

Nach § 62 Abs. 2 Satz 1 BremLBO dürfen personenbezogene Daten zur Wahrnehmung der Aufgaben des Bauordnungsamtes (Überprüfung, ob Kleingärten widerrechtlich zum dauernden Wohnen genutzt werden) grundsätzlich nur beim Betroffenen mit seiner Kenntnis erhoben werden. Soweit dies zur Erfüllung der Aufgaben erforderlich ist, dürfen nach Satz 2 dieser Vorschrift personenbezogene Daten abweichend von Satz 1 bei öffentlichen oder privaten Stellen erhoben werden.

Nach § 61 Abs. 1 Bremische Landesbauordnung (BremLBO) hat das Bauordnungsamt u. a. bei der Nutzung baulicher Anlagen darüber zu wachen, dass die öffentlich-rechtlichen Vorschriften und die aufgrund dieser Vorschriften erlassenen Anordnungen eingehalten werden.

Eine dieser Vorschriften ist der § 3 Abs. 2 Bundeskleingartengesetz (BKleingG), wonach im Kleingarten eine Laube in einfacher Ausführung mit höchstens 24 Quadratmetern Grundfläche einschließlich überdachtem Freisitz zulässig ist. Sie darf nach ihrer Beschaffenheit, insbesondere nach ihrer Ausstattung und Einrichtung, nicht zum dauernden Wohnen geeignet sein.

Zu den Ortsbegehungen durch die Sachbearbeiter: Die Bauordnungsbehörde hat dargelegt, Ortsbegehungen durch die Sachbearbeiter würden nur zwischen November und Anfang März stattfinden, also außerhalb der Jahreszeit, in der üblicherweise Kleingärten genutzt werden, und zwar nur morgens vor Tageslicht und abends nach Anbruch der Dunkelheit. Es würden nur die Gebäude von den Wegen aus erkundet, die auf den ersten Anschein deutlich sichtbar den im BKleingG festgelegten Rahmen von 24 qm um überdurchschnittlich große Aus- oder Anbauten überschreiten. Diese Objekte dürfen bis zu drei Mal im Jahr beobachtet werden, um Anhaltspunkte für eine unzulässig dauerhafte Wohnnutzung festzustellen.

Zum Prüfbogen der Sachbearbeiter: Der Prüfbogen, den die Sachbearbeiter bei ihren Ortsbegehungen verwendeten und ausfüllten, sei erstellt worden, um ihnen eine Richtschnur zu geben. Es kam nach Angaben der Bauordnungsbehörde nämlich vor, dass Sachbearbeiter aus den objektiven Beobachtungen subjektive Schlüsse zogen, z. B. Rückschlüsse auf die Art der Schuhe und deren Träger (Turnschuhe, die von einem Studenten getragen werden...). Der Prüfbogen werde jedoch nicht mehr verwendet.

Der Prüfbogen enthielt folgende Angaben:

- Daten und Uhrzeiten der Prüfungen vor Ort,

- amtliches Kennzeichen und äußere Merkmale des Pkw (beschlagene oder vereiste Scheiben, nach Regenfall trockene Fläche unter Fahrzeug oder mit Schnee überzogenes Fahrzeug),
- Pforte (verschlossen/offen),
- Schild an der Eingangspforte (ja/nein, Name und Anschrift),
- Briefkasten o. ä. für eine mögliche Postzustellung (vorhanden/nicht vorhanden),
- Klingel (ja/nein),
- Postzustellung erfolgte gerade (ja/nein),
- Fäkalienabfuhr erfolgte gerade (ja/nein),
- Spuren zu baulichen Anlagen (frische Fußspuren oder Fahrradspuren, Fußspuren im Schnee, Fußspuren im Schnee nur vor der baulichen Anlage/baulichen Anlagen zum Weg),
- Licht in den baulichen Anlagen (ein oder mehrere Fenster beleuchtet),
- Schornstein- und Rauchabzugsanlage in Betrieb (ja/nein),
- Personen auf dem Grundstück (Anzahl, Geschlecht und Alter),
- Eindruck (Es wird von einer illegalen Nutzung ausgegangen/Die baulichen Anlagen werden nicht illegal genutzt/Zur Zeit noch keine abschließende Beurteilung möglich).

Zum Inhalt der Akten: Die ausgefüllten Prüfbogen werden zu den Akten genommen. Die mir vorgelegten Akten enthielten neben Vermerken über Feststellungen vor Ort, Befragungen von Nachbarn auch Anfragen bei der Post und beim Kleingartenverein. Aus den Akten ging des Weiteren hervor, dass die Betroffenen häufig erst nach Vorliegen mehrerer Erhebungen, die sich über Monate angesammelt hatten, im Rahmen des jeweiligen Verwaltungsverfahrens angehört wurden. Die Akten sollten ca. 30 Jahre aufbewahrt werden.

Ich habe das gesamte Verfahren insbesondere unter den Gesichtspunkten der Verhältnismäßigkeit und der Erforderlichkeit der Datenerhebung untersucht und meine Bedenken dem Senator für Bau und Umwelt mitgeteilt. Daraufhin haben mehrere Gespräche stattgefunden. Dabei konnte ich eine Reduzierung der zu erhebenden Daten erreichen, so werden u. a. Angaben über Pforten, Schilder an Eingangspforten, Klingeln, gerade erfolgte Postzustellungen und Fäkalienabfuhren nicht mehr erhoben. Zu der Angabe, ob sich Personen auf dem Grundstück aufhalten, wird in Zukunft auf die Feststellungen über die Anzahl, das Geschlecht und das Alter verzichtet.

Hinsichtlich der Anfragen bei der Post habe ich grundsätzliche Bedenken geäußert. In dem von der Bauordnungsbehörde verwendeten formalisierten Schreiben an die Deutsche Post AG in Bremen (Briefzustellung) wurde nämlich angefragt, ob eine regelmäßige Briefzustellung, eine zeitlich begrenzte Briefzustellung (Sommermonate) oder keine Briefzustellung erfolgt. Es handelt sich hierbei um eine Verletzung des Postgeheimnisses nach Art. 10 Grundgesetz (GG), weil das Postgeheimnis auch Anfragen bei der Post, ob an bestimmten Grundstücken eine Briefzustellung erfolgt, umfasst. Eine Einschränkung dieses Grundrechts nach Art. 10 Abs. 2 Grundgesetz (GG) gibt es für diese Zwecke nicht. Ich konnte daher erreichen, dass auf die Postanfrage generell verzichtet wird.

Auch die Begründung für die Aufbewahrung der Akten für ca. 30 Jahre, es sei schon immer so gewesen, habe ich nicht akzeptiert. Da die Bremische Landesbauordnung keine bereichsspezifische Aufbewahrungsregelung für diese Daten enthält, kommt § 20 Abs. 3 Nr. 2 BrDSG zur Anwendung. Danach sind personenbezogene Daten zu löschen, wenn ihre Kenntnis für die speichernde Stelle zur rechtmäßigen Erfüllung der Aufgaben nicht mehr erforderlich ist.

Die Akten sollen nunmehr nach einem festzulegenden zeitlichen Ablauf, nachdem der jeweilige Vorgang abgeschlossen ist, vernichtet werden. Die Festlegung wird insbesondere zwischen den Fällen, in denen keine Anhaltspunkte für ein widerrechtliches Wohnen festgestellt wurden (unverzügliche Vernichtung) und den anderen Fällen unterscheiden. Nur in den Fällen, in denen von der Bauordnungsbehörde ein Verfahren gegen Kleingartenbesitzer eingeleitet wird, ist eine Aufbewahrungsfrist bis zum Abschluss des Verfahrens gerechtfertigt.

Inzwischen habe ich mit dem Senator für Bau und Umwelt meinen Prüfbericht und die Ergebnisse erörtert. Der dazu erstellte Ergebnisvermerk enthält insbesondere Vorgaben, dass nur die Daten erhoben werden dürfen, die für die Erfüllung der Aufgaben erforderlich sind. Der Landesverband der Gartenfreunde soll über diese Vorgaben informiert werden.

11.2 Wartung eines DV-Netzwerkes durch eine externe Stelle

Das Hochbauamt der Seestadt Bremerhaven hat mir den Service-Vertrag für die Wartung des amtsinternen DV-Netzwerkes zur Prüfung vorgelegt. Der Vertrag ist nur in einem Punkt nicht datenschutzkonform. Das Hochbauamt hat nämlich eine Firma mit dieser Aufgabe beauftragt, ohne dass diese den Bestimmungen des Bremischen Datenschutzgesetzes (BremDSG) unterliegt. Deshalb habe ich darauf hingewiesen, dass sich dieser Auftragnehmer vertraglich den Vorschriften dieses Gesetzes und meiner Kontrolle unterwerfen muss; vgl. § 9 Abs. 1 BremDSG. Außerdem habe ich das Hochbauamt gebeten, in Zukunft bei derartigen Verträgen diese Klausel regelmäßig einzufügen. Das Amt hat dies zugesagt.

11.3 Datenübermittlung bei Förderung von Regenwassernutzungsanlagen

Der Senator für Bau und Umwelt hat mich gefragt, ob die Bremer Umweltberatung e. V. als zuständige Stelle nach der Förderrichtlinie für die Gewährung von Zuschüssen bei der Gebäudeausstattung mit Regenwassernutzungsanlagen befugt ist, ohne Einwilligung der Förderempfänger der „hanseWasser GmbH“ als zuständige Abwasserabgaben erhebende Stelle die Daten der Förderempfänger zur Berechnung dieser Abgabe zu übermitteln.

Ich habe dargelegt, dass die bei der Bremer Umweltberatung e. V. vorhandenen personenbezogenen Daten der Antragsteller bzw. Förderempfänger der Zweckbindung nach § 12 BrDSG unterliegen und daher nur zu Zwecken der Antragsbearbeitung verarbeitet werden dürfen. Allerdings können die Förderempfänger bzw. Betreiber von Regenwassernutzungsanlagen von der Bremer Umweltberatung e. V. darauf hingewiesen werden, dass sie nach § 7 Abs. 3 Bremer Abwasserabgabengesetz (BrAbwAG) einer Meldepflicht gegenüber „hanseWasser GmbH“ unterliegen und ein Verstoß dagegen

nach § 12 BrAbwAG eine Ordnungswidrigkeit darstellt, die mit einer Geldbuße von 2.500,-- € geahndet werden kann. Die Geförderten können natürlich auch in die Datenweitergabe einwilligen.

11.4 Reservierung von Kfz-Wunschkennzeichen über das Internet

Die Verwaltungspolizei der Seestadt Bremerhaven hat mich gebeten, die Einführung eines Verfahrens, das es ermöglicht, Wunschkennzeichen per Internet zu reservieren, zu begleiten. Ich habe die Ausgestaltung des Verfahrens beraten. Um die Sicherheit der Datenbank der Zulassungsstelle zu gewährleisten, habe ich u. a. vorgeschlagen, technisch sicherzustellen, dass die Bürger nur auf eine ausgelagerte Datei auf einem separaten Server auf die dort aufgelisteten freien Kennzeichen zugreifen dürfen. Die Abschottung muss durch eine wirksame Firewall garantiert werden.

Die Verwaltungspolizei hat diese Anforderungen umgesetzt und nunmehr die Firewall der Firma „Checkpoint“ eingesetzt, die als konfigurierbar gilt.

11.5 Überprüfung von Beschäftigten am Bremer Flughafen

Durch die neuen Vorschriften des § 29 d Luftverkehrsgesetz und der Zuverlässigkeitsüberprüfungsverordnung, die die bisherigen Vorschriften aufgrund der Ereignisse um den 11. Sept. 2001 erheblich verschärfen, musste für den Flughafen Bremen ein ganz neues Sicherheitsüberprüfungsverfahren entwickelt und eingesetzt werden. Der Senator für Wirtschaft und Häfen wurde als zuständige Luftfahrtbehörde durch Senatsbeschluss bestimmt. Die bisherige Regelung, nach der die Polizei dafür zuständig war, war wegen der Bindung der Polizeibeamten an das Legalitätsprinzip sehr umstritten. Nunmehr sind alle Zuverlässigkeitsüberprüfungsanträge der betroffenen Personen (Flughafenmitarbeiter, Beschäftigte bei den einzelnen Luftfahrtgesellschaften und andere Personen im Flughafenumfeld, soweit sie sicherheitsempfindliche Bereiche betreten müssen) bei der Luftfahrtbehörde einzureichen und diese führt die erforderlichen Abfragen bei Polizeibehörden, dem Verfassungsschutz und dem Bundeszentralregister durch. Im Einzelfall können weitere Einrichtungen (BND, MAD, BuSt usw.) angefragt werden. Danach hat die Luftfahrtbehörde allein zu werten, ob ein Sicherheitsrisiko besteht, das eine Beschäftigung im Sicherheitsbereich des Flughafens nicht erlaubt. Die Beschäftigungsstelle erhält keine Kenntnis über die Daten, die zu der Bewertung geführt haben. Die Beschäftigungsstelle erhält lediglich eine Mitteilung darüber, ob eine Beschäftigung im Sicherheitsbereich zugelassen ist. Dem Betroffenen selbst wird vor Erlass einer Ablehnung zum Betreten des Sicherheitsbereichs Gelegenheit gegeben, sich zu dem Sicherheitsrisiko zu äußern.

Hinsichtlich der Übermittlung der Daten (Anträge der Betroffenen und Erlaubnis zur Beschäftigung im Sicherheitsbereich) zwischen Flughafen und Luftfahrtbehörde einerseits und der Luftfahrtbehörde und den Sicherheitsbehörden andererseits ist eine sichere E-Mail-Übertragung installiert worden. Dadurch wird der Erfassungsaufwand (Vermeidung von Schreibfehlern) reduziert, aber auch die Beschleunigung des Überprüfungsverfahrens erreicht. Das gesamte Verfahren ist in einem Datenschutzkonzept festgelegt.

11.6 Identitätsprüfung auf dem Flughafen

Ein Bürger hat sich an mich gewandt, da er sich bei den Grenzkontrollen seiner häufigen Geschäftsreisen oft einer verschärften Identitätsprüfung unterziehen musste. Eine Prüfung der bremischen polizeilichen Systeme ergab, dass zu seiner Person keine konkreten Gründe für derartige Kontrollmaßnahmen festgestellt werden konnten. Allerdings führte eine simulierte Personenabfrage zu dem Ergebnis, dass die betreffende Person als gesucht gekennzeichnet wurde, weil die Aliasdaten und das Geburtsdatum mit einer gesuchten Person eine gewisse Übereinstimmung zeigte.

Da diese Daten aber von einer Stelle des Bundes herrühren, habe ich den Fall zur weiteren Klärung an den Bundesbeauftragten für den Datenschutz abgegeben. Um die Überprüfungen in solchen Fällen für Betroffene zukünftig zu verhindern oder zumindest zu minimieren, ist es erforderlich, dass dem betroffenen Bürger ein Dokument (nach Schengener Informationssystem - SIS -) ausgestellt wird, das bestätigt, dass er nicht die gesuchte Person ist.

12. Finanzen

12.1 Chipsmobil

Das Projekt CHIPSMOBIL (Controlling, Haushalt, Integration, Planung, Standard, Modular, Online, Buchführung, Informatik, Logistik) zur Erneuerung des bremischen Haushalts-, Kassen- und Rechnungswesens ist im Januar 2003 in Betrieb genommen worden.

Ich habe es während der dreijährigen Entwicklungsphase begleitet (vgl. 22 JB, Ziff. 12.1, 23. JB, Ziff. 12.1, 24. JB, Ziff. 11.1) und insbesondere im 23. Jahresbericht meine Schwerpunkte dargelegt.

Teilergebnisse der Entwicklungen des vergangenen Jahres wurden mir in Form von folgenden Konzepten mitgeteilt: CCC (Customer Competence Center), dem Betreiberkonzept, dem aktuellen Berechtigungskonzept und dem Datenschutzkonzept.

Die nachfolgenden Erörterungen betreffen, ermittelt aus der Durchsicht der mir vorgelegten Konzepte, ausgewählte Datenschutzthemen. Diese erfordern an verschiedenen Stellen der Konzeptionen Konkretisierungen und möglicherweise Änderungen, um insbesondere die Überprüfbarkeit und Transparenz zu erhöhen und das datenschutzrechtliche Zweckbindungsgebot möglichst für das gesamte System zu gewährleisten.

Das SAP-Berechtigungskonzept ist in seiner Grundstruktur in der mir in 2000 vorgelegten Version (vgl. 23. JB, Ziff. 12.1) erhalten geblieben. Eine wesentliche Änderung ist der Wegfall der dezentralen Benutzeradministration. Sie sah vor, die Zuordnung einer zentral angelegten Systemnutzung zu einem bestimmten Berechtigungsprofil eigenverantwortlich von der jeweiligen Fachabteilung durchführen zu lassen. Diese Aufgabe wird nun von der zentralen Administration des Betreibers übernommen. Der Senator für Finanzen begründete diese Zentralisierung damit, dass der Aufwand zur Schaffung der für diese Aufgabe erforderlichen Organisationsstrukturen und des Aufbaus des erforderlichen System-Know-hows zu hoch gewesen wäre. Aus Datenschutzsicht ist dies eine schwächere Lösung, da die gesamte Benutzeradministration beim Betreiber liegt und die dezentrale Kontrolle, die sich durch die Zuordnung von Berechtigungsprofilen innerhalb der Fachabteilungen im System ergeben hätte, wegfällt. Die inhaltliche Verantwortung für die Änderung, Löschung oder Neuanlage einer Rolle liegt jedoch weiter bei den Dienststellenfachverantwortlichen. Der Senator für Finanzen versicherte hierzu, dass das für die Verwaltung von Berechtigungen von SAP vorgesehene Sechs-Augen-Prinzip gewährleistet bleibe. Es sieht vor, die Wahrnehmung der für die Verwaltung von Berechtigungen von SAP erforderlichen Funktionen auf drei verschiedene Rollen zu verteilen. Neben dem zentralen Benutzeradministrator beim Betreiber (Einrichtung der Benutzer) würden zur Trennung der Administration von Berechtigungen und deren Aktivierung die entsprechenden Rollen (zentraler Berechtigungsadministrator, zentraler Aktivierungsadministrator) innerhalb des Customer Competence Centers genutzt. Die Wahrnehmung dieser Rollen würde durch verschiedene Personen erfolgen. Eine gegenseitige Kontrolle von Vergabe und Freischaltung der Rechte sei dadurch gegeben. Durch diese

Form des Sechs-Augen-Prinzips und die klare Trennung von inhaltlicher und technischer Verantwortung ist diese Lösung aus Datenschutzsicht akzeptabel.

Die mir vorliegende Version des Berechtigungskonzeptes enthält keine konkreten Definitionen der fachspezifischen Rollen (bis auf die Bereiche Logistik, Finanzplanung und Haushaltsaufstellung). Der Senator für Finanzen teilte mir Ende des Jahres 2002 mit, dass diese bereits in den Berechtigungskonzepten für die einzelnen Fachthemen definiert seien. Diese fachspezifischen Rollen definieren zulässige Zugriffe auf Daten, Transaktionen und Programme.

Eine Prüfung ausgewählter Rollen mit fachübergreifenden Zugriffsmöglichkeiten, wie beispielsweise Finanz-Controlling oder Kosten- und Leistungsrechnung, steht noch aus. Zu prüfen wäre, ob sich die Rechtestruktur im System mit der für diese Rollen definierten Aufgabenstruktur deckt.

Die möglicherweise damit verbundene Problematik habe ich beispielsweise für den Bereich der Kosten- und Leistungsrechnung bereits beschrieben (vgl. 23. JB, a.a.O.) Im Blueprint zur Kosten- und Leistungsrechnung wurde deshalb in der ersten Projektphase festgeschrieben, dass personenbezogene Daten weder bei den Debitoren noch bei den Kreditoren dargestellt werden.

Inzwischen hat es auf Antrag der Regierungsfraktion eine Ergänzung des Haushaltsgesetzes gegeben, die die Verarbeitungsbefugnisse der mit der Kosten- und Leistungsrechnung beauftragten Personen regelt (§ 13 a). Sie haben demnach das Recht, die für den Zweck der Kosten- und Leistungsrechnung notwendigen Datenbestände des Rechnungswesens einzusehen und zu verarbeiten. In der Begründung wird der Datenschutzaspekt deutlich berücksichtigt. Die mit der Kosten- und Leistungsrechnung beauftragten Personen sollten den notwendigen Zugriff haben und sind befugt, die Daten im erforderlichen Umfang weiter zu verarbeiten.

Der Senator für Finanzen teilte mir hierzu mit, dass diese Ergänzung einen generellen Zugriff auf Einzelbelege legitimieren würde. Da die Begründung zur Ergänzung des Haushaltsgesetzes um den § 13 a deutlich das Erforderlichkeits- und Zweckbindungsgebot berücksichtigt, es jedoch aus meiner Sicht weiterhin nicht erforderlich ist, für die Kosten- und Leistungsrechnung personenbezogene Daten zu verarbeiten, teile ich die Interpretation des Senators für Finanzen nicht. Anderenfalls hätte er mich über den Gesetzesentwurf gem. § 27 Abs. 4 Nr. 2 BrDSG rechtzeitig unterrichten müssen, da es sich um eine Rechtsvorschrift handeln würde, die die Verarbeitung personenbezogener Daten regelt.

Der Senator für Finanzen teilte mir darüber hinaus mit, dass eine Dienstanweisung ergehen wird, die die Unterlassung der KLR-Auswertungsebene „in Blickrichtung des Personenkontos“ beinhaltet. Daraus leitet sich für mich ab, dass die ursprüngliche Aussage, diese Möglichkeit technisch zu verhindern, nicht eingehalten und durch die schwächere organisatorische Maßnahme einer Dienstanweisung ersetzt wurde. Ich werde das anhand des Rechteumfangs für die Rollen der Kosten- und Leistungsrechnung prüfen.

Neben aufgabenspezifischen zentralen Rollen mit umfassenden Zugriffsmöglichkeiten ist die Definition und die organisatorische Anbindung übergreifender Basis- und Administrationsrollen von erheblicher datenschutzrechtlicher Bedeutung.

Hierzu habe ich den Senator für Finanzen u. a. um folgende Erläuterungen bzw. Ergänzungen und Konkretisierungen im Rahmen der mir vorliegenden Konzepte gebeten:

- Eine Beschreibung der Rollen des Customer-Competence-Centers. Im Rahmen seiner Aufgaben dient das CCC als Nahtstelle zwischen SAP-Anwendern und SAP-AG. Insbesondere im Support verfügen die MitarbeiterInnen des User-Help-Desk (UHD) über gesonderte Berechtigungen im SAP/R3-System. Der Senator für Finanzen sagte hierzu eine Nachbesserung zu.

- Eine Beschreibung organisatorischer Maßnahmen beim Betreiber zum Ablauf des Verfahrens zur Vergabe von SAP-Basisberechtigungen.

- Eine Darstellung von Schutzmaßnahmen für die Rolle des mit umfangreichen Berechtigungen ausgestatteten Super-Users. Der Senator für Finanzen hat mir mitgeteilt, dass weitere Schutzmaßnahmen von SAP/R3 erläutert würden. Ich benötige dagegen die konkret von Senator für Finanzen ergriffenen Maßnahmen.

- Rahmenbedingungen für das zentrale Auditing und die Nutzung des SAP Audit-Info-Systems). Mit dem von SAP angebotenen Audit-System (AIS) sind Auswertungen außerhalb der Berechtigungsstruktur möglich. Zur Kontrolle und Überwachung der Berechtigungen einschließlich eines umfassenden Reportings werden spezielle Rollen mit dem Ziel der Durchführung eines laufenden Auditings definiert. Im Berechtigungskonzept werden hierzu die Kernberechtigungen (Zugriff auf das Berechtigungsinformationssystem, Reportingfunktionen zur Dokumentation, Zugriff auf das SAP-Audit-Info-System) genannt. Für die Nutzung des AIS sollten bestimmte Rahmenbedingungen gelten, die sicherstellen, dass Auswertungen nur im Rahmen bestimmter Aufgaben vorgenommen werden. Für sinnvoll halte ich eine entsprechende Dokumentation der Auswertungen (Ziele, Satzaufbau, Selektions- und Sortierkriterien), um sie transparent zu halten.

- Klärung der Handhabung von PC-Downloads. Es besteht die Möglichkeit des Herunterladens von R/3-Tabelleninhalten zur Weiterverarbeitung mit anderen Softwareprodukten. Das bedeutet, dass die bisher durch die Zugriffslogik des Systems geschützten Daten bezüglich ihrer Verarbeitungsmöglichkeiten keinen Beschränkungen mehr unterliegen. Dazu kommt, dass die Funktion des Downloads nur dienststellenübergreifend vergeben werden kann, d. h., fachbezogene Einschränkungen sind im Rahmen des Zugriffssystems nicht vornehmbar. Dieses Problem hat der Senator für Finanzen im Berechtigungs- und im Datenschutzkonzept wie folgt berücksichtigt. Für Rollen, die aufgrund datenschutzrechtlicher Vorgaben keine Daten aus dem SAP-System herunterladen dürfen, sollen entsprechende Einstellungen vorgenommen werden. Die Vorgaben hierzu sollten noch im Datenschutzkonzept beschrieben werden. Dieses sieht in dem mir vorliegenden Entwurf die grundsätzliche Sperrung der Download-Funktion vor. Lediglich für ausgewählte Personen sollte sie zur Verfügung gestellt werden.

  Leider teilte mir der Senator der Finanzen Ende 2002 mit, das er die oben beschriebenen technischen Restriktionen zur Steuerung der PC-Downloads nicht mehr umsetzen und das Berechtigungskonzept hierzu ändern will. Die technische Lösung soll durch eine organisatorische Festlegung ersetzt werden.

Abgesehen davon, dass das mit dieser Funktion verbundene Datenschutzproblem auch dienststellenintern vorhanden ist, halte ich es für nicht vertretbar, diese Funktion grundsätzlich allen verfügbar zu machen und den Umgang als „Anweisung im Konzept“ zu regeln.

- Beschreibung von internen Revisionsmechanismen. Es sollten u. a. der Umfang der Speicherung der Protokolldateien (insbesondere Security-Audit-Log), der Auswertungsverfahren (Tools, Fragestellungen, Zeiträume), das Berechtigungsaudit und entsprechende Dokumentationen und Rollen definiert werden. Der Einsatz von Revisionsmechanismen sind aus der Sicht des Datenschutzes ein notwendiges Werkzeug zur Gewährleistung eines datenschutzgerechten Verfahrens.
- Abschließende Erstellung eines Rahmendatenschutzkonzeptes. Dieses liegt mir als zweiter abschließender Entwurf vom November 2002 vor. Dort fehlt leider, dass für übergeordnete Kontrollinstrumente sichergestellt werden sollte, dass grundsätzlich keine Rückschlüsse auf zusammenhängende Stammdaten außerhalb des Zuständigkeitsbereiches aus der zentralen Datenbank ermöglicht werden. Allenfalls sollten anonyme statistische Auswertungen möglich sein. Der Senator für Finanzen hat diesen Satz aus dem Konzept gestrichen. Ich halte es für notwendig, Rahmenbedingungen für die Nutzung vorhandener Kontrollinstrumente zu definieren.

Ich gehe momentan davon aus, dass es nach Inbetriebnahme des komplexen Systems eine Reihe von Anpassungen der zugrundeliegenden Dokumente geben wird und die noch ausstehende Erörterung der noch bestehenden bzw. sich neu ergebenden Datenschutzfragen in diesem Rahmen erfolgen kann.

12.2 Laptopeinsatz beim Finanzamt für Großbetriebsprüfungen

Die Betriebsprüfer des Finanzamtes für Großbetriebsprüfungen in Bremen sind mit Laptops ausgestattet. Sie sollen die Prüfungsvorbereitung und -auswertung sowie die Prüfungstätigkeit vor Ort in den Betrieben unterstützen. Ich habe folgende Sicherheitseinstellungen bei den Laptops für die Betriebsprüfung geprüft:

- die Konfiguration auf Betriebssystemebene und die Art der verfügbaren Programme unter den Aspekten der Datensicherheit und Zulässigkeit der Verarbeitung,
- die Verbindung zwischen einem ausgewählten Laptop und dem LAN des Finanzamtes und,
- ausgewählte Einstellungen des Servers beim Finanzamt, auf dem die Daten der Prüfungen gespeichert werden.

Insgesamt konnte die Konzeption des Laptopeinsatzes in den geprüften Bereichen, insbesondere durch die ausschließliche Installation fachspezifischer Software für die Großbetriebsprüfungen und die durchgeführten technischen Datenschutzmaßnahmen, als angemessen bewertet werden.

Grundlage der Bewertung waren beispielsweise die Funktionsweise der Laptops im Offline-Betrieb. Für diese Betriebsart arbeiteten die Laptops mit kopierten Strukturelementen der für das LAN des Finanzamtes definierten Domäne, d. h., mit den dort geltenden Sicherheitseinstellungen. Als einzige lokale Nutzer des Laptops waren nur die Betriebsprüfer definiert. Für die Prüfungsdaten stand ein

Offline-Ordner zur Verfügung. Zugriff auf diese Daten war nur durch die zuständige Betriebsprüfer möglich. Darüber hinaus war die Möglichkeit der Verschlüsselung von Disketten und anderer Back-up-Medien gegeben.

Zur Verbesserung der Datensicherheit empfahl ich eine Veränderung der Passwortstruktur und eine Revision der Serverzugriffe beim Finanzamt auf die Ergebnisse der durchgeführten Prüfungen.

12.3 Mit Steuervergünstigungsabbau kommt Bankgeheimnisabbau

In den letzten Jahren ist eine ständige weitere Lockerung des Bankgeheimnisses und damit ein Abbau der Datenschutzrechte der Steuerpflichtigen zu verzeichnen. Nachdem mit der letzten Änderung der Abgabenordnung (AO) weitgehende Mitteilungspflichten im Bereich des Verdachts von Schwarzarbeit und illegaler Beschäftigung eingeführt wurden, zielt der jüngste Gesetzesvorschlag auf bisher geschützte Bereiche. Gesetzesgerechte Steuererhebung und grundrechtlicher Persönlichkeitsschutz stehen in einer Wechselbeziehung, die sorgfältiger Abwägung bedarf; diese lässt der Entwurf des Steuervergünstigungsabbaugesetzes vermissen.

In einem Brief hat deshalb der Bundesbeauftragte für den Datenschutz eine gemeinsame Stellungnahme der Datenschutzbeauftragten des Bundes und der Länder dem Finanzausschuss des Deutschen Bundestages zukommen lassen. Darin werden die gesetzgebenden Stellen aufgefordert, bei den geplanten Maßnahmen zur Sicherung der Steuergerechtigkeit eine datenschutzkonforme Abwägung zwischen diesen Verfassungsprinzipien vorzunehmen und die Datenschutzrechte der Bürger angemessen zu berücksichtigen. Im einzelnen wird auf folgendes aufmerksam gemacht:

- Die Aufhebung des § 30 a AO führt zu einem Wegfall des Bankgeheimnisses und damit zu einer deutlichen Störung des Vertrauensverhältnisses zwischen Banken und Kunden. Dass künftig auch verdachtsunabhängige Prüfungen in Banken angeordnet werden können, schafft den „gläsernen Bankkunden“ und erweckt den Anschein, als sei jeder Steuerpflichtige ein potentieller Steuerverkürzer. Das datenschutzrechtliche Prinzip, dass Daten grundsätzlich bei Betroffenen zu erheben sind (§ 93 a AO), wird außer Kraft gesetzt.
- Der Vertrauensverlust in der Bevölkerung wird durch die automatische Meldepflicht verschärft, die die Banken und andere Finanzdienstleister künftig gegenüber dem Bundesamt für Finanzen (BfF) haben (vgl. auch den Konferenzbeschluss unter Ziff. 15.4 dieses Berichts).
- Nach § 23 a EStG-E haben die Kreditinstitute Kontrollmitteilungen an das BfF über private Veräußerungsgeschäfte, insbesondere bei Wertpapieren, aber auch bei anderen Wirtschaftsgütern, z. B. Antiquitäten mit Namen, Anschaffungs- und Veräußerungsbeträgen sowie Anzahl zu senden.
- Gemäß § 45 d EStG-E sollen die Banken alle Kapitalerträge, bei denen ein Abzug von Steuern vorgesehen ist, mit Namen, Beträgen und Freistellungssummen dem BfF anzeigen.
- Die umfangreichen Datenübermittlungen sollen unter einem einheitlichen steuerlichen Identifikationsmerkmal (§ 139 a AO-E) beim BfF zusammengeführt werden. Dieses soll als eindeutiges lebenslanges Zuordnungsmerkmal jedes Steuerpflichtigen vom Bundesamt für

Finanzen vergeben und zukünftig bei Anträgen, Erklärungen oder Mitteilungen gegenüber Finanzbehörden angegeben werden. Dieses Identifikationsmerkmal würde damit anders als die Steuernummer zu einem einheitlichen Personenkennzeichen. Es ist zu befürchten, dass damit gegen verfassungsrechtliche Grundsätze verstoßen wird, wonach die Erschließung von Datenverbünden durch ein einheitliches Personenkennzeichen oder sonstiges Ordnungsmerkmal nicht zulässig ist. Der Datenpool beim Bundesamt für Finanzen schafft die Möglichkeit des gläsernen Steuerpflichtigen. Die Finanzbehörden hätten zukünftig die Möglichkeit einer blitzschnellen Zusammenführung von Informationen aus verschiedenen Quellen.

- Die Zusammenführung der Daten beim Bundesamt der Finanzen schafft eine bundesweite Datensammlung über alle Differenzgewinne und Kapitalerträge sowie sonstige Veräußerungsgewinne und verstärkt die Entwicklung des BfF zum zentralen Datenpool. Es besteht erfahrungsgemäß die Gefahr, dass auch andere Behörden auf solche riesigen Datenbestände zugreifen wollen.
- Die geplante Ausweitung der Befugnis zu Kontrollmitteilungen durch die Neufassung des § 194 Abs. 3 AO verstößt gegen das verfassungsrechtliche Übermaßverbot. Unabhängig von einer zulässigen Verwertung von Zufallsfunden müssen Kontrollmitteilungen über alle steuerpflichtigen Staatsbürger daran gebunden werden, dass tatsächliche Anhaltspunkte für den Verdacht einer Steuerverkürzung bereits entstanden sind. Die gegenwärtig geplante verdachtsunabhängige Befugnis zu Kontrollmitteilungen ist unverhältnismäßig.

In diesem Zusammenhang müsste es gesetzlich ausgeschlossen werden, dass kopierte Dateien und Unterlagen der Betriebe i. S. des § 147 Abs. 6 AO in den Finanzämtern für die massenhafte Herstellung von Kontrollmitteilungen verwendet werden. Da die bisherige Einschränkung des § 194 Abs. 3 AO aufgegeben wird, stehen gesetzlich keine Hindernisse gegen eine solche Auswertung der betrieblichen EDV im Wege. Dies wäre ebenfalls ein Verstoß gegen das verfassungsrechtliche Prinzip der Verhältnismäßigkeit.

Die Konferenz der Datenschutzbeauftragten von Bund und Ländern hat in diesem Zusammenhang darauf hingewiesen, dass eine Abgeltungssteuer wie in anderen europäischen Staaten (etwa Österreich und Schweiz) zu vergleichbarem Steueraufkommen führen würde, ohne dass die Banken zu umfassenden Anzeigepflichten über alle Steuerpflichtigen gezwungen würden. Es bleibt abzuwarten, ob neue Überlegungen der Bundesregierung in diese Richtung gehen und damit die Voraussetzungen schaffen, dass Kontrollmitteilungen entfielen, das Bankgeheimnis gewahrt bliebe und es bei Betriebsprüfungen weiterhin ausschließlich um die zulässige Verwertung von Zufallskunden ginge.

12.4 Fehlkuvertierung von Steuerbescheiden

In einem nicht näher abgrenzbaren Zeitraum bis etwa 14.11.2002 ist es in der Produktion der ID Bremen GmbH für die bremische Steuerverwaltung zu einer nicht ermittelbaren Anzahl von Fehlkuvertierungen von Steuerbescheiden für die Arbeitnehmerveranlagungen der Finanzämter 82 (Bremen-Ost), 84 (Bremen-Nord) und 85 (Bremerhaven) sowie wie für das aktenlose Verfahren des

Finanzamtes 73 (Bremen-West) gekommen. Die Fehlkuvertierungen wurden durch Rücksendung eines Steuerberaters und später bei der Überprüfung der versandfertigen Bescheide im Finanzamt Bremerhaven und mit Meldungen durch Steuerpflichtige entdeckt. Darüber hinaus ist nicht auszuschließen, dass von der Fehlkuvertierung auch Verfahren außerhalb der bremischen Steuerverwaltung betroffen sind. Durch die Fehlkuvertierung der Steuerbescheide wurden anderen fremde Steuerdaten bekannt gegeben und das Steuergeheimnis durch unzulässige Offenbarung verletzt.

Die für den Datenschutz in der „fidatas bremen“ und für die Aufsicht über die ID Bremen zuständige Stelle wurde erstmals am 26.11.2002 per E-Mail über das Probleme bei der Nachbehandlung im Zusammenhang mit der Kuvertierung informiert. Eine Information durch die ID Bremen GmbH an die aufsichtführende Stelle war bis zu diesem Zeitpunkt nicht erfolgt.

Durch Wartungstechniker der Kuvertierungsanlage wurde anhand des Systemprotokolls am 28.11.2002 festgestellt, dass Funktionalitäten der Steuerungssoftware der Kuvertiermaschine nicht so aktiviert waren, dass:

- Bescheide mit mehreren Blättern in einem Kuvert zusammengefasst wurden und
- verhindert wurde, dass versehentlich zwei Blätter auf einmal eingezogen werden.

Aus dem Systemprotokoll war nicht ersichtlich, wann und durch wen diese Funktionalitäten softwareseitig deaktiviert wurden. Die in der Nachbehandlung tätigen Mitarbeiter der ID Bremen GmbH erklärten übereinstimmend, dass sie die obengenannten Funktionalitäten nicht aktiviert bzw. deaktiviert hätten bzw. die betreffenden Funktionalitäten nicht kannten.

Als Ergebnis bleibt festzuhalten, dass

- die für die Einhaltung des Datenschutzbestimmungen in der ID Bremen zuständige „aufsichtführende Stelle“ zu spät über die Pannen unterrichtet wurde,
- ein Unterrichtungs- und Krisenmanagement nicht etabliert war,
- die mit der Datenverarbeitung beauftragte ID Bremen die Auftraggeber (die betroffenen Finanzämter) entgegen § 9 BremDSG über die Pannen nicht unterrichtet hat,
- die Verletzung des Steuergeheimnisses über einen (unbekannten) offensichtlich längeren Zeitraum nicht bemerkt wurde,
- Stichprobenkontrollen durch die Arbeitsnachbereitung - diese sind datenschutzrechtlich vorgesehen - nicht erfolgt sind.

Ich habe den Senator für Finanzen aufgefordert, geeignete Maßnahmen zu ergreifen, damit die Wiederholung eines solchen Fehlers vermieden wird bzw. eine schnellere Aufdeckung erfolgen kann. Geprüft werden sollten dabei die folgenden Überlegungen:

- Ob die betreffenden Steuerbescheide bei den richtigen Empfängern angekommen sind, konnte nicht geklärt werden. Sollten den betroffenen Bürgern eventuell finanzielle oder Rechtsnachteile entstehen, ist zu prüfen, ob alle Empfänger von Bescheiden, die ihnen in der fraglichen Zeit

zugestellt werden sollten, angeschrieben und auf den möglichen Fehler hingewiesen werden, damit sie sich ggf. an das zuständige Finanzamt wenden können.

- Es müssen Regelungen getroffen werden, die eine umgehende Fehlersuche ermöglichen. Es darf nicht sein, dass solche Fehler bei Bekanntwerden zunächst ignoriert werden und der betriebliche Datenschutzbeauftragte erst viel zu spät über die Datenschutzpanne unterrichtet wird. Der Fehler wurde am 21. November 2002 bemerkt, der betriebliche Datenschutzbeauftragte wurde erst am 26. November 2002 darüber unterrichtet. Oft müssen sofort Systemstände gesichert werden, um eine Fehlersuche zu ermöglichen oder die Verantwortlichkeit für gewisse Handlungen festzustellen.
- Geeignete Stichprobenverfahren mit menschlicher Kontrolle sind vorzusehen. Es reicht nicht aus, einer Maschine die Fertigungskontrolle allein zu übertragen. Wenigstens Stichproben sind in jeden Kuvertierungsvorgang einzubauen, damit ein Fehler möglichst bereits vor dem Versand entdeckt werden kann. Häufig wird zur Kontrolle ein eigener Datensatz erzeugt und den anderen Daten beigemischt, der entweder unmittelbar nach der Produktion überprüft wird oder aber in den Versand mitgegeben wird, um sowohl die Richtigkeit der versendeten Daten wie auch den Versand selbst zu überprüfen. Mit einem solchen Verfahren kann jedenfalls in den Fällen Abhilfe geschaffen werden, in denen ein einmal aufgetretener Fehler sich auf alle nachfolgenden Vorgänge auswirkt.
- Da der Fehlerbericht der „fidatas bremen" nahe legt, dass sowohl die systemseitige programmgesteuerte Blattfolgenkontrolle wie auch die manuell vom Bedienpersonal einzuschaltende Doppelblattkontrolle nicht funktioniert haben, ist in letzterem Fall auch ein menschliches Versagen nicht auszuschließen. Es sollte daher eine automatische, lückenlose und nicht manipulierbare Protokollierung relevanter Bedienschritte und ein Zugriffsschutz für sicherheitsrelevante Einstellungen eingerichtet werden.

Ich habe den Senator für Finanzen daher gebeten, zu prüfen, ob durch vertragliche Auflagen das beauftragte Unternehmen zu einer besonderen Leistungsgarantie in diesem Punkt angehalten werden und ob durch die Einrichtung zusätzlicher technischer Maßnahmen eine Verbesserung erreicht werden kann. Da der Vorfall erst am Ende des Berichtsjahrs aufgetreten ist, steht eine Antwort noch aus.

13. Bremerhaven

13.1 Prüfung der Stadtbildstelle Bremerhaven

Im Laufe des Berichtsjahres habe ich das Bildungsnetz Bremerhaven (Verbund aller 40 Bremerhavener Schulen) mit der Stadtbildstelle Bremerhaven als verantwortlichem Betreiber einer datenschutzrechtlichen Prüfung unterzogen. Gegenstand der Prüfung waren die Struktur des sehr komplexen Netzes und der Internet-Zugang für Schulen, Web-Hosting für Schulen sowie die Mail-Dienste für Schulen.

Hauptaufgabe für die Stadtbildstelle im Bereich der Struktur des Netzes für die Schulen ist der Ausbau und Betrieb desselben für die Computernutzung im Unterricht. Alle Schulen sind mit ihren Rechnern für die Ausbildung zu einer logischen Einheit (sog. Windows-Domäne) zusammengefasst. Das Bildungsnetz, das ausschließlich für die Ausbildung genutzt wird, ist komplett physikalisch und logisch vom Verwaltungsnetz der Stadtbildstelle und den Verwaltungsnetzen der Schulen getrennt.

Die Stadtbildstelle war zum Zeitpunkt der Prüfung via Funkstrecke an die Internet-Infrastruktur der Hochschule Bremerhaven angeschlossen. Die einzelnen Schulen sind per ISDN- bzw. TDSL-Verbindungen über den Provider Deutsche Telekom AG an das Internet angeschlossen. Das Bildungsnetzwerk Bremerhaven ist als Virtual Private Network (VPN), ein Verfahren bei dem der Datenaustausch der Teilnehmer verschlüsselt über sog. Tunnel durch das Internet abläuft, realisiert. Die Stadtbildstelle ist somit mit den Schulen über das Internet verbunden. Direkte Anbindungen der Schulen an die Stadtbildstelle in Form von Standleitungen existieren nicht.

In den Schulen existieren für Schüler keine persönlichen Accounts (Zugangskennungen) für die dort befindlichen Computer, lediglich für einige (wenige) Lehrer existieren solche. Auf jedem Rechner existieren gegeneinander abgeschottete Bereiche, sog. Home-Directories, in die Arbeitsdaten und Downloads aus dem Internet abgelegt werden können und welche gegen Zugriffe von anderen Arbeitsplätzen aus abgeschottet ist.

Da alle Schulen via ISDN, T-DSL oder Festverbindung direkt an das Internet angeschlossen sind, geschieht der Internet-Zugang aus dem Bildungsnetz heraus dezentral. In den einzelnen Schulen sind keine Proxy-Server im Einsatz, der Zugang zum Internet erfolgt ausschließlich über Router. Den Grundsätzen der Datensparsamkeit und der Zweckbindung der dort anfallenden Protokolldaten der Internet-Nutzung wird im Bildungsnetz dadurch Sorge getragen, dass durch die vorhandene Konfiguration die Protokollierung auf ein für den Betrieb des Netzes notwendiges Mindestmaß reduziert ist.

Die Stadtbildstelle hatte zugestimmt, dass ich im Rahmen der datenschutzrechtlichen Prüfung sowohl auf der Firewall als auch auf dem Web-Server rudimentäre Sicherheitsprüfungen in Form von Portscans durchführe. Dabei wird festgestellt, welche (Netz-) Dienste ein bestimmter Computer zur Verfügung stellt. Die Systeme selbst werden bei einem Portscan nicht angegriffen, es werden lediglich Informationen über die Systeme gesammelt. Der Portscan hat ergeben, dass auf der Firewall der

Stadtbildstelle alle nicht für den Betrieb unbedingt notwendigen Ports geschlossen sind, aber auch, dass die von der Firewall zur Verfügung gestellten Dienste mehr Informationen über das System preisgeben, als notwendig. Ich habe der Stadtbildstelle daraufhin empfohlen, diese Meldungen der Dienste abzuschalten bzw. zu verfremden, um potenziellen Angreifern die Beschaffung von Informationen über das Bildungsnetzwerk Bremerhaven so schwierig wie möglich zu gestalten. Der Portscan des Web-Servers hat zum Zeitpunkt der Prüfung eine relativ hohe Anzahl von zur Verfügung gestellten Diensten ergeben. Ich habe daraufhin die Stadtbildstelle aufgefordert, die auf dem Web-Server laufenden Dienste auf das für den Betrieb absolut notwendige Mindestmaß zu reduzieren. Dem ist die Stadtbildstelle umgehend nachgekommen.

Weiterhin fand zum Zeitpunkt der Prüfung auf dem Web-Server eine umfangreiche Protokollierung der Zugriffe aus dem Internet statt (gemäß standardmäßiger Konfiguration des eingesetzten Apache Web-Servers). Der Web-Server ist öffentlich via Internet zugänglich, die Stadtbildstelle somit Anbieter eines Teledienstes für Dritte gemäß Teledienstegesetz (TDG) bzw. Teledienstedatenschutzgesetz (TDDSG). Die umfangreiche Protokollierung der Zugriffe aus dem Internet auf den Web-Server zum Zeitpunkt der Prüfung entsprachen nicht den Regelungen im TDDSG, wonach ein Diensteanbieter personenbezogene Daten eines Nutzers ohne Einwilligung nur erheben, verarbeiten und nutzen darf, soweit dies erforderlich ist, um die Inanspruchnahme von Telediensten zu ermöglichen und abzurechnen (vgl. § 6 Abs. 1 TDDSG). Ich habe die Stadtbildstelle aufgefordert, die Protokollierung gemäß TDDSG zu gestalten. Dem ist die Stadtbildstelle nachgekommen.

13.2 Gehaltsbogen per Telefax

Die Gewerblichen Lehranstalten Bremerhaven wollten sich um Mittel aus dem EU-Projekt "Lehrlinge online" bewerben. Dazu sollten auch die Kosten, die durch die Beteiligung von Lehrkräften entstehen, dem Projekt gemeldet werden. Um diese Personalkosten zu ermitteln, hat sich die Lehranstalt an das Personalamt des Magistrats Bremerhaven gewandt und dieses hat die Bezügebögen der betreffenden Lehrkräfte an die anfragende Stelle gefaxt.

Dadurch wurden mehr als die für die Kosten- und Leistungsrechnung erforderlichen Daten übermittelt. Es hätte genügt, wenn das Personalamt die tatsächlichen Kosten ermittelt und einen Stunden- oder Tagesdurchschnittsbetrag gebildet hätte, und diese so zusammengefassten Daten den Gewerblichen Lehranstalten mitgeteilt hätte. Dieses habe ich kritisiert. Der Magistrat hat mir kurz vor Redaktionsschluss mitgeteilt, dass er eine neue Vereinbarung abgeschlossen habe, die zukünftig in solchen Fällen die Übermittlung personenbezogener Daten unterbindet. Diese Vereinbarung liegt mir noch nicht vor, so dass eine abschließende Bewertung noch nicht erfolgen konnte.

13.3 Verweisungen

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 befinden sich unter Ziff. 1.4 (Verfaxtes Fax), Ziff. 4.1 (Ergebnisse der Beratung des 24. Jahresberichts), Ziff. 5.1 (Unsichere Versendung personenbezogener Unterlagen per Telefax), Ziff. 5.2 (Aufbewahrung von Dienstaufsichtsbeschwerden), Ziff. 5.3 (Umgang mit Krankmeldungen), Ziff. 5.4 (Chipkarten im

Rahmen der Freien Heilfürsorge), Ziff. 6.12.1 (Änderung der bremischen Meldedatenübermittlungsverordnung), Ziff. 8.2 (Interne Vernetzung des Gesundheitsamtes Bremerhaven), Ziff. 8.7 (Fax-Irrläufer aus Krankenhäusern), Ziff. 9.1 (Interne Vernetzung des Amtes für Jugend und Familie Bremerhaven), Ziff. 9.6 (Bremer und Bremerhavener Arbeit GmbH), Ziff. 9.7 („Bürgertelefon“ Sozialhilfemissbrauch), Ziff. 10.4 (Schulbegleitforschung), Ziff. 11.2 (Wartung eines DV-Netzwerkes durch eine externe Stelle), Ziff. 11.4 (Reservierung von Kfz-Wunschkennzeichen über das Internet), Ziff. 12.4 (Fehlkuvertierung von Steuerbescheiden), Ziff. 13.1 (Prüfung der Stadtbildstelle Bremerhaven), Ziff. 13.2 (Gehaltsbogen per Telefax).

14. Datenschutz in der Privatwirtschaft

14.1 Patientendaten – Apotheken-Rechenzentrum – Apotheken-CD

Apotheken dürfen im Abrechnungsverfahren mit der gesetzlichen Krankenversicherung Rechenzentren einschalten. Diese bereiten die Verschreibungsdaten auf und übermitteln sie den Krankenkassen. Sie bieten den einzelnen Apotheken aber auch CDs an, auf denen sie Images und für die verschiedensten Auswertungen aufbereitete Daten aus den von der jeweiligen Apotheke eingereichten Rezepte anbieten. Im 24. Jahresbericht berichtete ich unter Ziff. 14.8 ausführlich über meine Verhandlungen mit dem in Bremen ansässigen Norddeutschen Apotheken-Rechenzentrum (NARZ), mit den Datenschutzaufsichtsbehörden der anderen Länder, mit dem Bundesministerium für Gesundheit und den Bundesorganisationen der Apotheker über eine datenschutzgerechte Ausgestaltung dieser CD. Das NARZ hatte in Abstimmung mit mir ein technisches Konzept realisierungsreif entwickelt, das die Funktionen der CD begrenzt und dem einzelnen Patienten ermöglicht, zu entscheiden, ob er mit der Nutzung seiner Daten durch die Apotheke überhaupt und wenn ja, zu welchen Zwecken im einzelnen, einverstanden ist. Da die Rechenzentren miteinander im Wettbewerb stehen, ist aber Voraussetzung für die Umsetzung des Verfahrens, dass möglichst alle Apothekenrechenzentren bereit sind, die CD mit den dargestellten Restriktionen auszuliefern. Dies ist bislang leider nicht der Fall. Eine Minderheit unter den Datenschutzaufsichtsbehörden der Länder vertritt - unterstützt durch den Bundesbeauftragten für den Datenschutz - die Auffassung, die dargestellte Verarbeitung von Verschreibungsdaten sei ungeachtet ihrer Ausgestaltung im einzelnen unzulässig. Leider ist es ihnen nicht gelungen, diese Position gegenüber den ihrer Kontrolle unterstehenden Rechenzentren durchzusetzen. Im Gegenteil: Bislang liefern diese die CD ohne die in Bremen abgesprochenen Funktionsbegrenzungen aus. Vorkehrungen dafür, dass die einzelnen Patienten damit einverstanden sind, werden auch nicht getroffen. Die große Mehrheit der Aufsichtsbehörden aber hat meine Position unterstützt und in diesem Sinne auf die ihrer Aufsicht unterstehenden Rechenzentren eingewirkt.

Das Bundesministerium für Gesundheit und Soziales ist inzwischen der Auffassung beigetreten, eine Einwilligung des Patienten könne eine über die im Sozialgesetzbuch hinausgehende Verarbeitung von Verschreibungsdaten durch Rechenzentren nicht legitimieren. Allerdings hat das Ministerium auf meine Frage, welche der mit mir abgestimmten Funktionen der durch das NARZ vertriebenen CD durch das SGB abgedeckt seien, nur einige Funktionen genannt, auf die dies nicht zutreffe, und zwar die Erstellung von Belegen für das Finanzamt sowie die Versendung von Informationsmaterial und von Geburtstagsgrüßen an die Patienten. Da das Ministerium zu den anderen Funktionen der CD eine Aussage nicht getroffen hat, habe ich - und hat anschließend auch die große Mehrheit des Düsseldorfer Kreises - daraus den Schluss gezogen, dass die Verarbeitung patientenbezogener Verschreibungsdaten durch Apotheken-Rechenzentren zur Erfüllung dieser Zwecke rechtmäßig sein könne. Dabei handelt es sich um die Quittierung von Eigenleistungen gegenüber den Krankenkassen (Zuzahlungsquittungen), die Rezeptrecherche für Patienten, Ärzte und Krankenkassen sowie den

Nachvollzug einer Retaxation (nachträgliche Neuberechnung der Abrechnung Apotheke/Kasse) durch die Apotheke. Das vom NARZ entwickelte Einwilligungsverfahren hat der Düsseldorfer Kreis nach wie vor als besonders datenschutzfreundlich bezeichnet. Er wird seine Auffassung dem Bundesministerium für Gesundheit und Soziales mitteilen und dann die Spitzenorganisationen der Apotheker anschreiben, ihnen seine Position erläutern und sie bitten, ihrerseits mit dem Ziel auf die Rechenzentren einzuwirken, dass sie bundesweit den Apotheken datenschutzgerecht ausgestaltete CDs anbieten.

14.2 KIS Kindergarten-Informationssystem bei der Arbeiterwohlfahrt

Das Programm KIS dient der automatisierten Verarbeitung der Sozialdaten von Eltern mit Kindern in Kindertagesheimen. Es wurde bisher in den 74 städtischen Kindertagesheimen (KTH) auf Stand-Alone-Geräten seit 1998 eingesetzt und unterstützt das Aufnahmeverfahren und die Beitragsberechnung. Es liefert auch statistische Daten für Planungszwecke (vgl. auch zur Veränderung der technischen Grundlagen des Verfahrens Ziff. 10.2 dieses Jahresberichts).

Das für die Städtischen Kindertagesheime erstellte Datenschutzkonzept und dessen von mir überprüfte Umsetzung (vgl. insbesondere 22. JB, Ziff. 9.1) ergaben nach zunächst festgestellten Mängeln datenschutzrechtlich angemessene Ergebnisse.

KIS wird aber auch in KTHs freier Träger, wie z.B. der Arbeiterwohlfahrt, eingesetzt. Das Ressort war damals an der Entscheidung der freien Träger für den Einsatz von KIS beteiligt und trägt die Verantwortung für die Wahrung des Sozialgeheimnisses (§ 61 Abs.4 SGB VIII). Es war demnach verpflichtet, die Umsetzung des Datenschutzkonzeptes auch in diesem Bereich zu garantieren.

Ich habe deswegen die KIS-Anwendung in einem KTH der Arbeiterwohlfahrt zu folgenden Themen geprüft:

- den Bootschutz für die Rechner des KIS-Systems,
- die Sicherheit des Dateisystems unter Windows-NT,
- die Richtlinien für die Passwortgestaltung,
- die Organisation der Administration des Systems,
- die Gruppen- und Benutzerstruktur,
- die Zugriffsprotokolle und Einstellungen der Überwachungsrichtlinien.

Insgesamt konnte als Ergebnis der Prüfung festgestellt werden, dass das sich aus dem Datenschutzkonzept ergebende Datenschutzniveau durch die technische Umsetzung in dem KTH der Arbeiterwohlfahrt gewährleistet war.

14.3 Sicherstellung von Personalunterlagen eines ehemaligen Betriebes

Von Mitgliedern des Beirats Vegesack bin ich darüber informiert worden, dass sich auf einer Industriebrache in Bremen-Vegesack in dem dortigen leerstehenden Betriebsgebäude etliche Personalunterlagen befänden.

Ich habe den Fundort in Gegenwart der Beiratsmitglieder und Vertretern des Deutschen Gewerkschaftsbundes (DGB) aufgesucht und festgestellt, dass die Unterlagen offen und für jedermann zugänglich in dem Betriebsgebäude herumlagen. Es handelte sich insbesondere um Stundennachweise, Gehaltsabrechungen und -mitteilungen und sogar um eine vollständige Akte über ein Arbeitsgerichtsverfahren. Da ich nicht in der Lage war, unverzüglich Maßnahmen zur Sicherstellung der umfangreichen Unterlagen zu treffen, haben die Vertreter des DGB die Unterlagen treuhänderisch und vorübergehend übernommen.

Aus den Unterlagen war der Name des ehemaligen Arbeitgebers eindeutig feststellbar. Aufgrund der regionalen Medienberichterstattung haben sich die Familienangehörigen des ehemaligen Arbeitgebers bei mir gemeldet und erklärt, dass die Firma vor ca. 10 Jahren an eine Firma in Karlsruhe verkauft worden sei. Daraufhin habe ich die Firma und die Aufsichtsbehörde in Baden-Württemberg eingeschaltet und auf den Missstand hingewiesen. Die Firma in Karlsruhe hat die Unterlagen inzwischen vom DGB übernommen, so dass sich nunmehr keine Unterlagen mehr in dem ehemaligen Betriebsgebäude und auf dem Grundstück befinden.

14.4 Einführung eines elektronischen Türsicherungssystems

Die Beauftragte für den Datenschutz eines Betriebes hat mir den Entwurf einer Betriebsvereinbarung über eine elektronische Türensicherung vorgelegt und angefragt, ob diese den datenschutzrechtlichen Anforderungen entspricht.

Zweck des Türsicherungssystems ist, den Diebstahl von wertvollen Betriebseinrichtungen zu verhindern. Die Beschäftigten erhalten Chipkarten, mit denen sich die Türen des Betriebes öffnen lassen. Da Diebstähle außerhalb der Geschäftszeit vorgekommen sind, ist festgelegt worden, dass die Speicherung der Freischaltung einer Tür in der Logdatei nur außerhalb der Geschäftszeit erfolgt. Aus Gründen der Transparenz der Datenverarbeitung habe ich vorgeschlagen, in der Betriebsvereinbarung die Daten aufzuführen, die sich auf der Chipkarte befinden und präzise festzulegen, welcher Personenkreis unter welchen Voraussetzungen welche Auswertungen vornehmen darf. Außerdem habe ich die zweijährige Löschungsfrist für zu lang gehalten und vorgeschlagen, dass die Daten spätestens nach ein bis drei Monaten gelöscht werden sollten. Schließlich habe ich auf die neue Rechtsvorschrift über mobile personenbezogene Speicher- und Verarbeitungsmedien (Chipkarten) nach § 6 c Bundesdatenschutzgesetz und insbesondere die darin geregelten Unterrichtungspflichten hingewiesen. Die Datenschutzbeauftragte hat zugesagt, meine Vorschläge zu übernehmen und auf die Einhaltung und Umsetzung der neuen Chipkartenregelung zu achten.

14.5 Datenerhebung bei Anbahnung eines Mietvertrages

Ich bin darüber informiert worden, dass ein Makler einem Mietinteressenten ein Formular „Selbstauskunft Miete“ aushändigte und erklärte, das vollständige Ausfüllen sei Bedingung für den Zuschlag als Mieter. In dem Formular werden Angaben verlangt über den Familienstand und ggf. den Güterstand sowie die Bankverbindung und das Vermögen, aufgeteilt nach Bank- und Sparguthaben, Wertpapiere (Kurswert), Haus- und Grundvermögen, Versicherungsansprüche sowie sonstige

Vermögen. Außerdem ist die Einwilligungserklärung so formuliert, dass eingewilligt werden soll, die Angaben bei Banken und anderen Stellen überprüfen zu können.

Ich habe den Makler darauf hingewiesen, dass die vorgenannten Angaben nicht erforderlich sind. Zur Eingehung eines Mietvertragsverhältnisses reicht es aus, wenn die Summe der monatlichen Nettoeinnahmen angegeben wird, damit der Vermieter abschätzen kann, ob der Mietinteressent die monatliche Miete regelmäßig bezahlen kann. Außerdem sollten die Stellen, bei denen mit Einwilligung des Mietinteressenten Auskünfte eingeholt werden dürfen, näher benannt werden, z. B. Auskunfteien.

Der Makler hat mir daraufhin ein neues Formular übersandt, dass die von mir monierten Angaben nicht mehr enthält. Außerdem ist die Einwilligungserklärung entsprechend meiner Anforderung geändert worden.

14.6 Elektronisches Fahrgeldmanagement

Der Verband der Deutschen Verkehrsunternehmen (VDV) hat sich an die Datenschutzbeauftragten des Bundes und der Länder sowie die Aufsichtsbehörden für den Datenschutz gewandt und ein gemeinsames Vorgehen bei der Entwicklung einer Kernapplikation für ein elektronisches Fahrgeldmanagement im öffentlichen Personenverkehr vorgeschlagen. Hierbei geht es insbesondere um folgende Aspekte:

- Bargeldlose Bezahlungen mit elektronischen Geldbörsen, z. B. der Geldkarte, der PayCard oder anderen Kundenmedien
- Elektronischer Fahrschein durch Ersatz des Papierfahrscheins durch Speicherung der Fahrkartendaten auf einer Chipkarte oder auf anderen Kundenmedien und
- Automatisierte Fahrpreisfindung durch unternehmens- bzw. netz- oder verbundübergreifende In/Out-Systeme mit aktiver oder passiver Anmeldung der Fahrgäste

Dazu hat sich eine Arbeitsgruppe aus dem Kreis der Landesbeauftragten für den Datenschutz gebildet, an der auch ich teilgenommen habe. Die Arbeitsgruppe hat mit der Datenschutzarbeitsgruppe des VDV die nachstehenden datenschutzrechtlichen Grundanforderungen an das Elektronische Fahrgeldmanagement (EFM) entwickelt, die von allen ca. 400 Mitgliedsunternehmen des VDV beachtet werden sollen.

- Transparenz: Die Datenverarbeitung durch das EFM muss transparent sein (§ 6 c Abs. 1 Nr. 2 und 3 BDSG). Dies erfordert die Festlegung der Zwecke, die Beschreibung der einzelnen Datenverarbeitungsvorgänge, differenziert nach den jeweiligen für den Fahrgast zutreffenden Geschäftsprozessen und die dabei zu verarbeitenden Daten. Weiter sind die Angaben der Identitäten und Anschriften der Stellen erforderlich, die zu den genannten Zwecken personenbezogene Daten verarbeiten und/oder bei denen die jeweiligen Rechtsansprüche geltend gemacht und Verfahrensbeschreibungen gemäß § 4 Abs. 2 Satz 2 BDSG eingesehen werden können. Auch die Einbeziehung der Unterrichtungspflichten der Kundenvertragspartner ist geboten. Deshalb sollte ein Merk- oder Informationsblatt erstellt werden, in dem der Fahrgast in allgemein verständlicher Form über die vorgesehene Datenverarbeitung - auch durch zentrale

Servicestellen oder andere autorisierte Dritte - und über seine Rechte nach §§ 34, 35 BDSG unterrichtet wird.

- Widerspruchsrecht: Der VDV sollte mit seinen Kundenvertragspartnern verabreden, dass der Kunde bei Vertragsabschluss schriftlich erklärt, ob er der Übermittlung oder Nutzung seiner Daten zu Zwecken der Werbung und der Markt- und Meinungsforschung widersprechen möchte oder nicht. Daran müssten sich dann auch autorisierte Dritte halten**.**
- Wahlmöglichkeit: Den Fahrgästen muss nach Information über die vertraglich bedingte Datenverarbeitung eine freie Entscheidung zwischen anonymer Fahrt und besonderen Leistungsangeboten (z. B. best pricing) überlassen bleiben.
- Datensparsamkeit: Alle Leistungsmerkmale und Geschäftsprozesse sind nach dem Prinzip der Datenvermeidung und Datensparsamkeit (§ 3 a BDSG) zu gestalten. Insbesondere dürfen keine Daten verarbeitet werden, die kundenbezogene Bewegungsprofile ermöglichen. Das bedeutet, dass Dateien für Planungszwecke und zur Optimierung des Angebots anonym zu erheben oder zu anonymisieren sind. Soweit Daten für besondere Leistungsangebote oder das Reklamationsmanagement benötigt werden, sind diese pseudonym zu erheben und zu speichern, so dass ohne Wissen und Wollen des betroffenen Fahrgastes eine Zuordnung zu seiner Person ausgeschlossen ist. Werden zu Zwecken des Reklamationsmanagements nutzungsbezogene Daten auf mobile Speichermedien (Chipkarte) geschrieben, muss es dem Fahrgast ermöglicht werden, diese Daten auf eigene Verantwortung zu löschen.
- Getrennte Verarbeitung: Es müssen die jeweils erforderlichen technischen und organisatorischen Maßnahmen getroffen werden, um eine getrennte Verarbeitung im Sinne der Nr. 8 der Anlage zu § 9 BDSG zu gewährleisten.
- Zweckbindung der Ticketdaten: Darüber hinaus dürfen keine kunden- oder kartenbezogenen Auswertungen zu fremden Zwecken erfolgen. Zu Abrechnungszwecken im Verkehrsverbund dürfen allenfalls (pseudonyme) kartenbezogene Daten übermittelt werden.
- Vorabkontrolle: Von dem oder der betrieblichen Datenschutzbeauftragten ist vor Inbetriebnahme des EFM eine Vorabkontrolle durchzuführen (§ 4 d Abs. 5 und 6 BDSG) und zu dokumentieren.
- Zugriffsberechtigung: Der Lesezugriff für das Kontrollpersonal muss auf die zur Kontrolle notwendigen Daten beschränkt sein, insbesondere auf dem Speichermedium des Fahrgastes.
- Datenschutzgerechte Gestaltung der Systemkomponenten: Die Systemkomponenten, die von Fahrgästen bedient werden, sind datenschutzgerecht so zu gestalten, dass keine Möglichkeit für Unbefugte besteht, an Terminals für bargeldlose Zahlung die Eingabedaten, insbesondere Authentifikationsdaten zur Kenntnis zu nehmen. Fehlermeldungen der Zugangserfassungssysteme dürfen die Betroffenen nicht öffentlich diskriminieren und die Fahrgäste müssen in angemessenem Umfang die Möglichkeit haben, den Inhalt der Chipkarte jederzeit auslesen zu können.

- Schutz gegen Missbrauch: Es müssen Vorkehrungen (z. B. Sperrung, Verschlüsselung) getroffen werden, die den Fahrgast gegen missbräuchliche Verwendung der Daten durch Dritte bei Verlust des Speichermediums schützen.
- Löschung: Die Dauer der für bestimmte Geschäftsprozesse erfolgenden Speicherung personenbezogener Daten muss so kurz wie möglich sein. Für die jeweiligen Geschäftsprozesse sind Regelfristen für die Löschung der Daten festzulegen (§ 4 e Satz 1 Nr. 7 BDSG). In den Terminals gespeicherte Daten sollten nach erfolgreicher Datenübertragung an den Rechner des Verkehrsunternehmens gelöscht werden.

14.7 Videoüberwachung innerhalb des Bahnhofsgebäudes in Bremen

Das Bahnhofsmanagement Bremen der Deutsche Bahn AG Station & Service (DB) hat mich zur Vorstellung des Sicherheitskonzeptes der DB im Hauptbahnhof Bremen eingeladen. Ein wesentlicher Bestandteil dieses Konzeptes ist die Videoüberwachung an allen Ein- und Zugängen (auch vom Bahnsteig) sowie den Schließfachbereichen. Hierbei sind die Vorgaben des § 6 b Bundesdatenschutzgesetz (BDSG) einzuhalten.

Die DB hält die Videoüberwachung (Beobachtung) zur Gewährleistung eines ungestörten Betriebsablaufs, Einhaltung der Hausordnung, Durchführung unternehmerischer Prävention hinsichtlich der Sicherheitslage, Sicherstellung von Eigentümerinteressen und Koordinierung sowie Einsatzsteuerung der Service-, Sicherheits- und Sauberkeitsdienste in Personenbahnhöfen, also auch dem Hauptbahnhof Bremen, für erforderlich.

Grundsätzlich sind alle Bahnhofsnutzer (z. B. Beschäftigte und Fahrgäste) von der Beobachtung betroffen. Von der Aufzeichnung betroffen sind Nutzer der Notrufsäulen und Bahnhofsnutzer beim Vorliegen einer Straftat, Ordnungswidrigkeit oder bei Verstoß gegen die Hausordnung. Anlassbezogene Aufzeichnungen werden nach 72 Stunden bzw. drei Tagen gelöscht. Zugriffsberechtigte sind der Bahnhofsmanager, der Leiter der Sicherheitszentrale und der Schichtleiter.

Das vorgenannte Konzept ist mit der zuständigen Datenschutzaufsichtsbehörde Berlin abgestimmt, weil die DB ihren Sitz in Berlin hat. Entsprechend meiner Bitte hat die DB mir die Verfahrensbeschreibung nach § 4 e BDSG sowie ein Exemplar des Schildes zur Verfügung gestellt, dass die Bahnhofsnutzer auf den nach § 6 b BDSG erforderlichen Umstand der Videoüberwachung hinweist.

Ich habe der DB nach Durchsicht der Unterlagen mitgeteilt, dass die Videoüberwachung einschließlich der Verfahrensbeschreibung den datenschutzrechtlichen Anforderungen entspricht. Darüber hinaus habe ich der DB vorgeschlagen, dass der Servicepoint im Hauptbahnhof Bremen jedermann entsprechend Auskunft erteilt und nach § 4 g Abs. 2 BDSG die Verfahrensbeschreibung über die Videoüberwachung auf Antrag zur Verfügung stellt. Nach Informationen der DB soll die Videoüberwachung im Sommer 2003 starten.

14.8 Personalausweisdaten bei Bezahlung mit EC-Karte

Ein Bürger monierte, dass er bei der Bezahlung mit seiner EC-Karte anlässlich einer Kfz-Untersuchung seinen Personalausweis vorlegen musste und dass daraus seine Daten abgeschrieben wurden.

Auf Anfrage hat der TÜV Nord Straßenverkehr GmbH (TÜV) erklärt, er habe mit der Firma InterCard einen Vertrag über die Einzahlung mit EC-Karte abgeschlossen. Danach werde nach dem Zufallsprinzip beim Bezahlen ein Belegformular ausgedruckt, auf dem dann Name, Anschrift und Ausweisnummer des Kunden eingetragen werden müssen. Im Falle der Nichteinlösung des Geldes werde der entsprechende Beleg an InterCard herausgegeben. Nur mit diesem Verfahren erstatte InterCard bei Nichteinlösung das Geld.

Auf Nachfrage erklärte der TÜV, die an InterCard zu gebenden Belege würden dort zehn Jahre und die übrigen beim TÜV verbleibenden Belege sieben Jahre lang aufbewahrt. Da diese Aufbewahrungszeiten viel zu lang sind, habe ich vorgeschlagen, die Belege spätestens nach einem Jahr zu vernichten. Der TÜV hat dies zugesagt. Darüber hinaus sollte der Kunde vor dem Bezahlvorgang auf dieses Verfahren hingewiesen werden.

14.9 Unterstützung des betrieblichen DSB durch die verantwortliche Stelle

Der betriebliche Beauftragte für den Datenschutz (DSB) eines Unternehmens fragte mich, ob es zur Unterstützungspflicht des DSB durch die verantwortliche Stelle nach § 4 f Abs. 5 Bundesdatenschutzgesetz (BDSG) gehöre, dem DSB einen Online-Zugriff auf die Datenverarbeitungssysteme, mit denen personenbezogene Daten verarbeitet werden, einzurichten.

Ob explizit ein solcher Zugriff im Einzelfall erforderlich ist, um auf die Einhaltung der Vorschriften über den Datenschutz hinwirken zu können, ist immer von den jeweiligen Bedingungen abhängig. Hierbei ist jedoch zu beachten, dass ein solcher Zugriff angemessen sein muss. Nicht angemessen wäre es, wenn der DSB einen unbegrenzten Zugriff auf alle personenbezogenen Daten hätte. In der Regel sollte der DSB daher nicht ohne Wissen des Betroffenen oder Beschäftigten auf dessen Daten Zugriff nehmen können.

Angemessen dürfte es sein, ihm einen Zugriff einzurichten, der es ihm ermöglichen würde, festzustellen, welche Hard- und Software eingesetzt wird, welche Auswertungen von wem nach welcher Auswertungsmatrix vorgenommen werden und welche Personen welche Zugriffsrechte und /oder Administrationsrechte haben.

Auch der Zugriff auf Protokolle über evtl. unberechtigte Zugriffe dürfte angemessen sein. Soweit er überprüfen möchte, ob und ggf. welche personenbezogenen Daten automatisiert verarbeitet werden, ist ihm zu gestatten, jederzeit vom Gerät aus, auf den die Anwendung läuft, Einsicht in die jeweiligen Masken zu nehmen.

14.10 Datenschutz im Verein

Auch im letzten Berichtsjahr erreichten mich sehr viele Anfragen - insbesondere von Vereinsfunktionären - zu dem Thema „Richtiger Umgang mit Daten in einem Verein“.

Offensichtlich ist in den Vereinen die Erkenntnis gewachsen, dass nach dem neuen Bundesdatenschutzgesetz auch neue Verantwortlichkeiten bestehen. Viele Nachfrager waren überrascht, dass das BDSG nun in jedem Fall auch für die Datenverarbeitung in Vereinen gilt.

Viele Einzelfragen wurden an konkreten Einzelbeispielen geklärt. In der überwiegenden Anzahl der Fälle habe ich auf eine Informationsschrift zum "Datenschutz im Verein" (die ich auf Anforderung versende) hingewiesen.

Der Text des Faltblattes wird auf meiner Homepage unter www.datenschutz.bremen.de demnächst veröffentlicht.

14.11 Herkunft der Adressdaten bei Reiseveranstalter

Ein Bürger wollte wissen, woher ein Reiseveranstalter seine Daten habe. Von dem Reiseveranstalter erhielt er hierzu zunächst keine Antwort.

Gemäß § 34 Abs. 1 Bundesdatenschutzgesetz (BDSG) kann der Betroffene auch Auskunft über die Herkunft seiner Daten verlangen. Eine Prüfung ergab, dass die Bremer Firma diese Daten von einer englischen Gesellschaft erhalten hatte, die sie wiederum beauftragt hatte, eine Aktion "Werbung für schöne Reisen" durchzuführen. Die Bremer Firma hat die Adressen nur zur Erledigung des Auftrages bekommen und sofort nach Abschluss der Werbeaktion zurückgeben müssen. Deshalb waren logischerweise keine Daten mehr bei der beauftragten Firma zu prüfen.

In Absprache mit dem Eingeber hat die Bremer Firma die englische Gesellschaft aufgefordert, die Betroffenendaten zu löschen, damit er nicht erneut mit Werbepost konfrontiert wird. Die Herkunft der Adressdaten konnte nicht abschließend geklärt werden, allerdings kann vermutet werden, dass sie aus der Teilnahme an einem Preisausschreiben stammen, in der der Betroffene „Reisen“ als Hobby angegeben hat.

14.12 SB-Zonen bei Kreditinstituten

In Anrufen beschwerten sich Kunden eines Kreditinstituts, dass die in den Geschäftsräumen aufgestellten neuen SB-Kundenterminals in keinster Weise den Datenschutz sicherstellten. Die neuen Bildschirme waren sehr viel größer geworden und standen sehr eng nebeneinander. Dabei boten weder die Bildschirme noch sonstige Einrichtungen Sichtschutz, so dass die neben oder hinter dem Anwender stehenden Personen einen Blick auf die angezeigten Daten nehmen konnten. Hinzu kam, dass bereits auf dem Start-Bildschirm in großen Zahlen die Salden der Konten angezeigt wurde, ohne dass dieser Vorgang vom Benutzer beeinflusst werden konnte. Die Kunden zeigten sich empört über die mangelnde Sensibilität des Kreditinstituts für den Datenschutz. Ich wandte mich an den betrieblichen Datenschutzbeauftragten des Kreditinstituts, das sich scheinbar ohne Überlegungen zum Datenschutz für die Aufstellung solcher Geräte entschieden hatte. Dieser erklärte mir, die

Tastatur werde gegen Einsichtnahme Dritter geschützt und der Monitor sei mit einem Filter ausgestattet, der eine seitliche Einsichtnahme verhindere. Man hätte darüber hinaus zeitgleich mit der Installation der Terminals zwischen den Geräten Sichtschutzblenden anbringen wollen. Diese Montage habe sich aber verzögert. Tatsächlich dauerte es keine zwei Wochen, bis ausreichend hohe Sichtblenden zwischen den einzelnen Terminals angebracht waren. Zwischenzeitlich sind auch Software-Änderungen am Start-Bildschirm vorgenommen worden, so dass sich der Kunde vor dem Aufruf seiner Kontostände versichern kann, dass keine Personen hinter ihm Einblick nehmen können.

Auch in einem anderen Fall beschwerten sich Kunden über die Aufstellung von SB-Terminals im Vorraum der Schalterhalle eines Kreditinstituts. Meine Nachfrage bei dem betrieblichen Datenschutzbeauftragten ergab, dass in Kürze mit Umbauarbeiten begonnen werden solle, die SB-Zone werde danach mit neuen Geräten ausgestattet. Dies teilte ich den Beschwerdeführern mit, die sich nach dem Umbau mit den betroffenen Datenschutzmaßnahmen zufrieden zeigten.

14.13 Handels- und Wirtschaftsauskunfteien

14.13.1 Ergebnisse der Beratungen in der Arbeitsgruppe Auskunfteien

Im Berichtsjahr gab es zwei Sitzungen der Arbeitsgruppe Auskunfteien, in der sich die Obersten Datenschutzaufsichtsbehörden mit den Vertretern der Auskunfteien bzw. ihren Verbänden trafen.

Bei der Sitzung im Frühjahr ging es ausschließlich um die Schufa, speziell um die Auswirkungen der Schufa-Neustrukturierung auf die Datenschutzaufsicht (vgl. auch Ziff. 14.13.2 dieses Berichts) sowie um Fragen im Zusammenhang mit dem Schufa-Score-Verfahren, einem Bonitätsverfahren. Hierbei handelt es sich um spezielle Fragen wie Wissenschaftlichkeit des Verfahrens, Einbeziehung bzw. Nichteinbeziehung der Selbstauskünfte an Betroffene in die Berechnung des Score-Wertes, die neue Informationsbroschüre der Schufa zu diesem Verfahren und die Beauskunftung des Score-Wertes gegenüber Betroffenen.

Bei der Sitzung im Sommer 2002 standen u. a. die folgenden Themen an:

- Schufa-Klauseln in Mietverträgen/Schufa-Verträge mit Wohnungsunternehmen

  Bei diesem Punkt geht es im Wesentlichen um die Frage, ob Wohnungsunternehmen bzw. große Vermieter als Anschlusskunden der Schufa sich über potentielle Mieter vorab im Schufa-Informationssystem informieren dürfen und, ob die Wohnungsunternehmen Negativdaten über einen Mieter in das System eingeben dürfen. Die Schufa bietet den Wohnungsunternehmen einen sog. B-Anschlussvertrag an, was bedeutet, dass das Wohnungsunternehmen sich bei der Schufa über einen potentiellen Mieter informieren kann und sog. Negativdaten - ganz gleich, wer sie der Schufa gemeldet hat - erhält und sich auf der anderen Seite verpflichtet, Negativdaten zu einem Mieter in das Schufa-System zu melden. Verabredet mit den Datenschutzaufsichtsbehörden war ein besonderes Verfahren (sog. C-Verfahren, geschlossener Benutzerkreis), das ausschließlich den Wohnungsunternehmen zur Verfügung steht und nicht alle Negativdaten eines Betroffenen zur Verfügung stellt. Die Diskussion hierzu ist noch nicht abgeschlossen.

- Vernichtung der Listen aus dem Schuldnerverzeichnis über die vorzeitige Löschung von Eintragungen

  Bei diesem Punkt geht es um die Zulässigkeit der Aufbewahrung dieser Listen. Obwohl die Eintragungen im Schuldnerregister gelöscht wurden und dies den Auskunfteien in Listenform mitgeteilt wird, damit diese dann ihre eigenen Datenbestände ändern können, gibt es zumindest bei einer Auskunftei die Praxis, diese sog. Löschlisten weiterhin aufzubewahren (aus Beweissicherungsgründen). Diese Praxis wurde von einigen Datenschutzaufsichtsbehörden kritisiert. Aufgrund meiner Datenschutzprüfung bei der Auskunftei Bürgel in Bremen habe ich diesen Punkt erneut zur Diskussion in die Arbeitsgruppe eingebracht.

- Auskunftsanspruch der Betroffenen und Wahrung des Geschäftsgeheimnisses

  Bei diesem Punkt geht es um die Praxis einiger Auskunfteien, den Auskunftsanspruch eines Betroffenen unter Hinweis auf die Wahrung von Geschäftsgeheimnissen einzuschränken bzw. ganz zu verneinen. Die Datenschutzaufsichtsbehörden vertreten den Standpunkt, dass sich durch die Änderung des Bundesdatenschutzgesetzes (BDSG) auch der Auskunftsanspruch der Betroffenen erweitert hat und man nicht generell von einem Überwiegen des Geschäftsgeheimnisses über die Interessen eines Betroffenen ausgehen kann. Die Handels- und Wirtschaftsauskunfteien wurden aufgefordert, ihre Praxis zu überprüfen und die Fälle zu bestimmen, bei denen trotz Vorliegens eines Geschäftsgeheimnisses eine Auskunftserteilung möglich ist. Die Diskussion ist noch nicht abgeschlossen.

- Datenübermittlung an Drittländer ohne angemessenes Datenschutzniveau

  Es wurde über einen Mustervertragsentwurf diskutiert, der zwischen den einzelnen Auskunfteien und ihren Vertragspartnern im Drittland geschlossen werden soll. Die Datenschutzaufsichtsbehörden wiesen darauf hin, dass verbindliche Unternehmensregelungen im Sinne von § 38 a BDSG nicht genehmigungsbedürftig, sondern nur konkrete Datenübermittlungen nach § 4 c BDSG genehmigungsbedürftig sind. Von einer Genehmigung könne abgesehen werden, wenn die Auskunfteien die von der Europäischen Kommission entwickelten Standardvertragsklauseln in ihr Vertragssystem übernehmen würden. Sollte dies nicht gewünscht werden, müssten Einzelgenehmigungsanträge für die gewünschten Datenübermittlungen bei den zuständigen Datenschutzaufsichtsbehörden gestellt werden. Die Diskussion ist noch nicht abgeschlossen.

14.13.2 Datenschutzaufsicht bei der neu strukturierten Schufa

Seit dem 1. Januar 2002 gibt es eine neue Gesellschaftsstruktur bei der Schufa: Die bis dahin selbständigen Schufa Regionalgesellschaften (GmbH) wurden zur Schufa Holding AG mit Sitz in Wiesbaden verschmolzen. Diese AG ist seither die einzige rechtlich selbständige Schufa-Gesellschaft. Schon vorher im Mai 2001 wurde die Bundes-Schufa-Vereinigung der Deutschen Schutzgemeinschaften für Allgemeine Kreditsicherung e.V. mit der im Jahre 2000 neu geschaffenen Schufa Holding AG verschmolzen. Diese nimmt Beratungs- und Betreuungsaufgaben für die einzelnen Schufa Gesellschaften wahr und betreut das zentrale DV-System.

Organisatorisch hatte sich die Schufa Holding AG in 5 sog. Regionalleitungsstandorte mit jeweils identischen Aufgaben untergliedert (Hamburg, Berlin, Bochum/Dortmund, Frankfurt/Wiesbaden, München/Stuttgart). Einige bisherige Schufa-Standorte wurden geschlossen. Der Schufa-Standort Bremen gehört als Untergliederung zum Regionalleitungsstandort Hamburg.

Eigentümer der Schufa Holding AG sind im Wesentlichen die Banken und Sparkassen sowie Einzelhandels- und Versandhausunternehmen, die sich in Eignerpools mit unterschiedlichen Anteilsverhältnissen gliedern und natürlich auch im größten Umfang Nutznießer der Daten sind.

Die Schufa hat gegenwärtig (2002) über 55 Mio. gespeicherte Personenstammsätze und erteilt über 60 Mio. Auskünfte pro Jahr. Neben der stark an Bedeutung verlierenden manuellen Kommunikation (per Telefon, Fax oder Schriftstück) steht die Kommunikation in elektronischer/digitaler Form (online - Kommunikation per Leitung, Filetransfer oder Datenträgeraustausch) im Vordergrund.

Als Konsequenzen der Umstrukturierung ergibt sich für die Datenschutzaufsicht daraus folgendes: Verantwortliche Stelle im Sinne des Bundesdatenschutzgesetzes (BDSG) ist die Schufa Holding AG in Wiesbaden. Der betriebliche Datenschutzbeauftragte der Schufa Holding sitzt in Wiesbaden und ist für die gesamte AG zuständig. Es wird nur noch eine Meldung nach § 4 d BDSG zum Register der Datenschutzaufsichtsbehörden abgegeben, und zwar bei der für Wiesbaden zuständigen Datenschutzaufsichtsbehörde (Regierungspräsidium Darmstadt).

Das gesamte Prüf- und Beratungsgeschäft in Sachen Schufa ist auf das Regierungspräsidium Darmstadt übergegangen. Allerdings sollen nach einer Verabredung zwischen der Schufa Holding AG und der AG Auskunfteien des Düsseldorfer Kreises ungeachtet der Frage der Zuständigkeit Beratungen von anfragenden Bürgern sowie übliche Standardfälle wie bisher von den jeweiligen örtlichen Aufsichtsbehörden unter Hinweis auf die an sich fehlende Zuständigkeit bearbeitet werden. Sollten sich im Einzelfall Auffassungsunterschiede mit der Schufa oder Grundsatzfragen abzeichnen, ist der jeweilige Fall zuständigkeitshalber an das Regierungspräsidium Darmstadt abzugeben. Gleiches gilt auch auf Seiten der Schufa. Kontroverse oder grundsätzliche Fälle werden von den Regionalleitern an die Zentrale in Wiesbaden abgegeben.

Verwaltungsakte, Bußgeldbescheide oder evtl. Strafanzeigen gegenüber der Schufa erfolgen nur noch durch das Regierungspräsidium Darmstadt bzw. die zuständigen hessischen Behörden. Über die neue Praxis soll zu gegebener Zeit ein Erfahrungsaustausch in der AG Auskunfteien des Düsseldorfer Kreises erfolgen.

Die Neustrukturierung hat natürlich auch Konsequenzen für die Betroffenen. Die Bearbeitung von schriftlichen Anfragen und Eingaben von Betroffenen bei der Schufa soll schrittweise von den Regionalleitungsstandorten weg auf die Standorte Bochum und Hannover konzentriert werden. Langfristig dürfte mit einer Zentralisierung bei einem Standort oder bei der Zentrale in Wiesbaden zu rechnen sein.

Die Möglichkeit, als Betroffener Auskunft über die gespeicherten Daten durch persönliche Kenntnisnahme zu erlangen (§ 34 Abs. 6 BDSG), soll von dieser Zentralisierung der Anfragenbearbeitung nicht betroffen sein, d. h., man kann als Betroffener weiterhin an den Regionalleitungsstandorten oder den weiteren Standorten persönlich Kenntnis von den eigenen Daten

nehmen. Allerdings muss man sehen, dass einige Schufa-Standorte geschlossen wurden. Die unmittelbare Kenntnisnahme seiner Daten durch den Betroffenen wurde dadurch geschmälert; es dürfte bei weiterer Zentralisierung der Standorte oder der Geschäftsfelder weiter erschwert werden, wenn es nicht gelingt, ein elektronisches Surrogat (z. B. über das Internet) zu schaffen.

14.13.3 Datenschutzprüfung bei Bürgel Bremen

Im Berichtsjahr habe ich eine Datenschutzprüfung bei der Bürgel Wirtschaftsinformationen Seitz GmbH & Co. KG (kurz: Bürgel Bremen) durchgeführt. Die Prüfung erstreckte sich u. a. auf die

- Meldepflicht, §§ 4 d, 4 e BDSG
- Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten, §§ 4 f, 4 g BDSG
- Verpflichtung der Mitarbeiter auf das Datengeheimnis, § 5 BDSG
- Auftragsdatenverarbeitung, § 11 BDSG
- Automatisierte Abrufverfahren, § 10 BDSG
- Überprüfung des dargelegten berechtigten Interesses bei Datenübermittlungen nach § 29 Abs. 2 Nr. 1 a BDSG
- Benachrichtigung der Betroffenen, § 33 BDSG.

Der Prüfung vorgeschaltet war eine Besichtigung der Geschäftsräume (Räumlichkeiten, Arbeitsplätze, EDV-Einrichtungen). Bürgel Bremen ist eine der 62 Bürgel-Auskunfteien und Inkassobüros im Bundesgebiet, die eine gemeinsame Datenbank bei ihrer Zentrale, der Bürgel Wirtschaftsinformationen GmbH & Co. KG in Hamburg, betreiben. Diese Datenbank enthält über 14 Mio. Datensätze (3 Mio. Unternehmen, 11 Mio. Privatpersonen). Auskünfte werden ausschließlich an Bürgel-Kunden gegeben. Sie erfolgen per Telefon, schriftlich sowie in zunehmendem Umfang online oder im Batchverfahren. Darüber hinaus werden die Daten des Bürgel-Datenbank-Systems auch an andere Datenbanken weitergegeben bzw. übermittelt und für weitere Zwecke wie z. B. die Bonitätsprüfung von Kundendateien genutzt. Bürgel Bremen ist dabei für die „Bremer“ Daten verantwortlich.

Bürgel Bremen betreibt daneben das Inkasso. In den Geschäftsräumen von Bürgel Bremen gibt es einen für alle Mitarbeiter offenen Raum mit chronologisch geordneten Inkassoakten (Pendelregistratur). Nach den gegebenen Erläuterungen werden die in Auftrag genommenen Inkassofälle nicht über die zentrale Bürgel-Datenbank bearbeitet, es werden aber Teilinformationen aus den Inkassofällen in den zentralen Auskunfteidatenbestand eingepflegt. Die Bearbeitung der Inkassofälle bei Bürgel Bremen ist nach den gegebenen Erläuterungen auf einen Teil der Mitarbeiter begrenzt, die nicht gleichzeitig auch auskunfteispezifische Arbeiten erledigen. Auf die Inkassoakten dürfen nur die Inkassomitarbeiter Zugriff nehmen. Zu der Recherche von Auskunfteidaten werden auch die in die zentrale Bürgel-Datenbank eingepflegten Daten aus dem Inkassobereich herangezogen (z. B. die Anzahl aller von den Bürgel-Gesellschaften betriebenen Inkassos zu diesem Betroffenen, sämtliche Angaben zu den von Bürgel Bremen gegenüber dem Betroffenen betriebenen Inkassos) und bei der Bildung der Bonitätskennziffer mit berücksichtigt.

Nach Auffassung der Datenschutzaufsichtsbehörden besteht zwischen den Bereichen Inkasso und Auskunftei eine funktionelle Schranke. Ob eine Datenübermittlung vom Inkassobereich in den Auskunfteibereich zulässig ist, bestimmt sich nach den Regeln des § 28 BDSG. Die skizzierte Bürgel-Praxis, die übrigens auch von anderen Handels- und Wirtschaftsauskunfteien betrieben wird, ist datenschutzrechtlich nicht unproblematisch.

Zur Meldepflicht nach §§ 4 d, 4 e BDSG: Bürgel Bremen hatte sich im Juli 2001 neu zum Register des Landesbeauftragten für den Datenschutz nach § 38 Abs. 2 BDSG angemeldet. Der Inhalt der Meldung wurde überprüft. Im Juli 2002 erfolgte eine Änderungsmeldung. Die sich daraus ergebenden Fragen und Bewertungen habe ich Bürgel Bremen in einem Prüfbericht zugeleitet. Themen sind dabei z. B. die hinreichende Beschreibung der Daten oder Datenkategorien im Hinblick auf die im Bürgel-Informationssystem (DB-Systems) gespeicherten Daten, die verschiedenen Fragen der Nachvollziehbarkeit des Bonitätsindexes, u. a. hinsichtlich der Gewichtung der Merkmale und der Rechenmethode (wie sie sich ähnlich auch beim Score-Wert-Verfahren der Schufa stellen, vgl. Ziff. 14.13.1 dieses Berichts), in welchem Umfang konkrete Übersichten über online-Datenempfänger geführt werden müssen, wie den gesetzlichen Löschfristen besser Rechnung getragen werden kann, Fragen der geplanten Datenübermittlung an Drittstaaten, die Möglichkeit zur Verbesserung der Aufgabenwahrnehmung des betrieblichen Datenschutzbeauftragten, der in Hamburg sitzt, Fragen der Auftragsdatenverarbeitung nach § 11 BDSG und noch fehlende Angaben nach § 10 Abs. 2 Satz 2 BDSG bezgl. des automatisierten Abrufverfahrens, um die wesentlichen Themen zu nennen.

Die bei einer Auskunftei anfragenden Stellen müssen ein berechtigtes Interesse darlegen, das sie berechtigt, die gewünschte Information zu erhalten. Anlässlich der Prüfung habe ich eine Stichprobe gezogen und die Dokumentation des dargelegten berechtigten Interesses bei Datenübermittlung nach § 29 Abs. 2 Nr. 1 a BDSG geprüft.

Nach den gegebenen Erläuterungen werden seitens Bürgel Bremen insgesamt etwa 17.500 Auskünfte pro Jahr (einschließlich aller online- und Batch-Auskünfte) erteilt und bei 3 Auskünften pro Monat das jeweils dargelegte berechtigte Interesse überprüft. Eine solche Überprüfungsquote würde damit die mit dem Düsseldorfer Kreis vereinbarte 2 Promille-Quote erfüllen.

Bürgel Bremen legte auf Verlangen Unterlagen vor, die die Überprüfung des berechtigten Interesses bei Anfragen dreier Kunden im Oktober 2002 betrafen. Während das berechtigte Interesse in einem der Fälle die Warenabrechnung betraf, wurde als Grund in den beiden anderen Anfragefällen gegenüber der Auskunftei die geplante Aufnahme von Geschäftsbeziehungen mit den Betroffenen angegeben. Hinsichtlich der Abrechnung von Waren in dem einen Fall konnten von Bürgel Bremen Rechnungskopien vorgelegt und damit das berechtigte Interesse dargelegt werden. In den beiden anderen Fällen fehlten konkrete Unterlagen, die das berechtigte Interesse begründen konnten. Ich habe Bürgel Bremen aufgefordert, sich in diesen beiden Fällen um entsprechende Unterlagen zu bemühen und sie mir zu Prüfzwecken vorzulegen.

Eine abschließende Stellungnahme von Bürgel Bremen steht noch aus, einige der festgestellten Fragen bedürfen noch weiterer Erörterung im Düsseldorfer Kreis. Hierzu zählt auch die Behandlung von Daten aus den Schuldnerverzeichnissen. Bürgel Bremen erhält nach § 915 d Abs. 1 Zivilprozessordnung (ZPO) i.V.m. § 2 SchuVVO Vollabdrucke in Listenform aus den

Schuldnerverzeichnissen der Amtsgerichte seines Zuständigkeitsbereiches. Diese sog. „Schuldnerlisten“ werden von Bürgel Bremen über einen Zeitraum von insgesamt drei Jahren aufbewahrt. Begründet wird die dreijährige Aufbewahrungsdauer u. a. mit von der Auskunftei benötigten Beweismöglichkeiten. Es müsse der Auskunftei beispielsweise möglich sein zu belegen, dass eine unrichtige Auskunft ein Fehler des Amtsgerichts und nicht der ihrige sei. Enthalten in den Abdrucken bis zum Ablauf der dreijährigen Aufbewahrungsdauer sind auch solche Eintragungen, die im Schuldnerverzeichnis bereits vorzeitig gelöscht wurden. Über die vorzeitige Löschung einer Eintragung im Schuldnerverzeichnis ist Bürgel Bremen nach § 915 g Abs. 2 ZPO zu unterrichten. Eine Verpflichtung, eine im Schuldnerverzeichnis vorzeitig gelöschte Eintragung in den Abdrucken/Schuldnerlisten zu streichen (löschen), ergibt sich nach meiner Auffassung aus § 15 Abs. 4 SchuVVO, der besagt, dass Löschungsmitteilungen nach § 15 Abs. 2 SchVVO zu vernichten oder zu löschen sind, sobald die vorgenommenen Änderungen bekannt sind. Zudem kann den Bestimmungen des § 915 g ZPO die Absicht des Gesetzgebers entnommen werden, die Löschungsfristen für Eintragungen in Abdrucken, Listen und Aufzeichnungen den für das Schuldnerverzeichnis geltenden Fristen anzupassen. Insofern ist eine Löschung der vorzeitig im Schuldnerregister gelöschten Eintragungen zu verlangen.

Bürgel Bremen vertritt hierzu eine andere Auffassung und verweist auf die in der AG Auskunfteien geführte Diskussion. Es bestehen aber Zweifel, ob die allgemeinen Datenschutzregelungen des BDSG (§ 35 Abs. 3 Nr. 2 und 3) hier überhaupt zum Tragen kommen oder ob die Regelungen der ZPO und der SchuVVO als spezifisches Recht nicht vorrangig und abschließend sind. Ich werde dieses Thema nochmals in den Gremien des Düsseldorfer Kreises zur Sprache bringen.

Auch hinsichtlich der telefonischen Benachrichtigung des Betroffenen über die Speicherung seiner Daten im System einer Auskunftei bedarf es bezüglich Inhalt und Klarheit noch einer weiteren Klärung. Ursache war die Eingabe eines Betroffenen. Bei meiner Prüfung habe ich festgestellt, dass zu diesem (Inhaber eines Handwerksbetriebes) von Bürgel Bremen ein Datensatz im Bürgel-Informationssystem angelegt wurde, was auf eine erste Anfrage durch einen Bürgel-Kunden (Normalanfrage) vom 18.10.2000 zurückzuführen war. Am 20.10.2000 war anlässlich dieser Anfrage telefonisch Kontakt mit dem Betroffenen aufgenommen worden. Die Kontaktaufnahme diente dazu, Daten über den Betroffenen und seinen Betrieb zu recherchieren. Angeblich erfolgte hierbei auch die Benachrichtigung gemäß § 33 BDSG. Dies wird vom Betroffenen allerdings bestritten.

Es stellt sich hierbei die Frage, ob die Verbindung einer telefonischen Recherche beim Betroffenen mit einer (angeblichen) Benachrichtigung die Anforderungen nach § 33 BDSG erfüllt. Ich habe hier erhebliche Zweifel, nicht zuletzt deshalb, weil die Beweisbarkeit einer solchen Benachrichtigung gegenüber den Datenschutzaufsichtsbehörden schwierig ist. Dieses Thema will ich in den Gremien des Düsseldorfer Kreises weiter erörtern. Dabei ist unstreitig, dass auch telefonisch benachrichtigt werden kann.

14.13.4 Bürgereingabeprüfung bei Creditreform Bremen

Aufgrund einer Eingabe habe ich die Datenübermittlung durch Creditreform Bremen an eine Lebensversicherung überprüft und bin zu dem Ergebnis gekommen, dass ein berechtigtes Interesse für die Datenübermittlung durch Creditreform Bremen an die Lebensversicherung nicht dargelegt werden konnte. Die Datenübermittlung an die Versicherung war nach meiner Auffassung somit nicht zulässig (§ 29 Abs. 2 BDSG). Dies habe ich sowohl dem Petenten als auch der Creditreform Bremen und der Versicherung mitgeteilt.

Die Versicherung stützte sich bei der Darlegung ihres berechtigten Interesses gegenüber Creditreform Bremen auf Verpflichtungen aus dem Geldwäschegesetz sowie eine diesbezügliche Verlautbarung des Bundesaufsichtsamtes für das Versicherungswesen (jetzt Bundesanstalt für Finanzdienstleistungsaufsicht) aus dem Jahre 1996.

Das Geldwäschegesetz verlangt von der Versicherung eine Identitätsprüfung, interne Sicherungsmaßnahmen (bezüglich der Geldwäsche sicherlich!) und in Verdachtsfällen eine Anzeige bei den zuständigen staatlichen Strafverfolgungsbehörden. Eine „Bonitätsprüfung“, d. h., eine Anfrage bei einer Auskunftei mit nachfolgender Datenübermittlung durch diese werden hingegen nicht gefordert. Eine solche Anfrage bzw. Datenübermittlung kann für die Erfordernisse des Geldwäschegesetzes nach meiner Auffassung auch nichts hergeben.

Ich habe den Vorgang in den Düsseldorfer Kreis eingebracht und angeregt, die Angelegenheit in der Arbeitsgruppe zu erörtern. Den Bundesbeauftragten für den Datenschutz habe ich gebeten, die Angelegenheit mit der neuen Bundesanstalt für Finanzdienstleistungsaufsicht zu erörtern mit dem Ziel, zu neuen, in sich abgestimmten Verlautbarungen hinsichtlich der Anwendung des Geldwäschegesetzes zu kommen.

14.14 Beratungen in der Arbeitsgruppe Internationaler Datenverkehr

Die Arbeitsgruppe Internationaler Datenverkehr des Düsseldorfer Kreises, in der sich die Obersten Datenschutzaufsichtsbehörden u. a. mit Vertretern der EU-Kommission sowie mit Firmen- und Verbandsvertretern treffen, hat im Berichtsjahr dreimal getagt, wobei ich nicht an allen Sitzungen teilgenommen habe. Die Arbeitsgruppe beschäftigt sich im Augenblick intensiv mit der Anwendung der neuen Regelungen des Bundesdatenschutzgesetzes (BDSG) zur Datenübermittlung ins Ausland, speziell in Länder außerhalb des EU- und des EWR-Bereichs (§§ 4 b, 4 c BDSG).

Innerhalb der EU und des EWR-Gebietes sind Datenübermittlungen im Rahmen des Anwendungsbereiches des Rechts der Europäischen Gemeinschaften im Rahmen der normalen Übermittlungsbestimmungen (z. B. §§ 28, 29, 30 BDSG) grundsätzlich zulässig. Es gilt das Prinzip des ungehinderten Datenflusses innerhalb der EU und des EWR-Bereiches. Sollen Daten an ausländische Stellen außerhalb des Geltungsbereiches der EG-Datenschutzrichtlinie übermittelt werden, so muss bei den Datenempfängern ein angemessenes Datenschutzniveau gewährleistet sein.

Besteht dies nicht, wäre dennoch eine Datenübermittlung unter bestimmten im BDSG genannten Ausnahmetatbeständen (§ 4 c Abs. 1 BDSG) zulässig, z. B. wenn eine Einwilligung des Betroffenen

vorliegt oder es zur Vertragserfüllung erforderlich ist. Sollten diese Ausnahmetatbestände nicht vorliegen, dann sieht das Gesetz die Genehmigung einzelner Übermittlungen oder bestimmter Arten von Übermittlungen durch die zuständige Datenschutzaufsichtsbehörde vor (§ 4 c Abs. 2 BDSG). Eine Genehmigung kann erteilt werden, wenn die verantwortliche Stelle (der Datenexporteur) ausreichende Garantien (z. B. Vertragsklauseln, verbindliche Unternehmensregelungen) hinsichtlich des Schutzes des Persönlichkeitsrechtes und der Ausübung der damit verbundenen Rechte vorweist. Hier muss die zuständige Datenschutzaufsichtsbehörde also prüfen, ob ausreichende Garantien, sprich, ein angemessenes Datenschutzniveau beim Datenempfänger bzw. im Drittland, vorliegen.

Die Vertragsgestaltung zwischen den verantwortlichen Stellen und etwaige verbindliche Unternehmensregelungen innerhalb eines Unternehmensverbandes spielen hierbei eine wichtige Rolle. Die Arbeitsgruppe Internationaler Datenverkehr hat sich in ihren Sitzungen deshalb nicht nur mit der Gestaltung einzelner solcher Unternehmensregelungen befasst (z. B. Daimler-Chrysler, Gesamtverband der Deutschen Versicherungswirtschaft - GDV), sondern auch Gedanken über die Bedeutung derartiger Regelungen gemacht. Dabei ist klar, dass die Arbeitsgruppe nicht die jeweils zuständige(n) Datenschutzaufsichtsbehörde(n) ersetzen kann, sondern nur auf bundesweite Abstimmung und einheitliche Auslegung der schwierigen neuen Rechtsmaterie hinwirken kann.

Aufgrund der Diskussionen in der Arbeitsgruppe hat der Düsseldorfer Kreis hat zur Bedeutung verbindlicher Unternehmensregelungen bei Datenübermittlungen in Drittländer einen in der Arbeitgruppe vorbereiteten Beschluss gefasst (vgl. Ziff. 16. dieses Berichts).

14.15 Sammelauskünfte aus dem Melderegister an die BSAG

Ein Empfänger von Sammelauskünften der Meldebehörde Bremen (vgl. auch Ziff. 6.12.2 dieses Berichts) ist die Bremer Straßenbahn AG (BSAG), von der im Datenträgeraustausch (Diskette) derartige Auskünfte bei der Meldebehörde Bremen eingeholt werden. Sammelauskünfte sind in einer Tabelle zusammengefasst, Einzelauskünfte zum Wohnsitz einer bekannten Person. Ein Bereich, in dem solche Auskünfte eingeholt werden, ist die Beitreibung des erhöhten Beförderungsentgeltes in Fällen von Beförderungserschleichung. Kann dieses Beförderungsentgelt nicht sofort entrichtet werden, werden die Personalien notiert, dem Schwarzfahrer wird daraufhin per Post eine Zahlungsaufforderung zugeleitet. Sind solche Briefe nicht zustellbar, wird versucht, die neue Anschrift über die Meldebehörde zu ermitteln.

Ein weiterer Grund für die Einholung von Sammelauskünften bei der Meldebehörde Bremen besteht, wenn mit Kunden der BSAG ein Abonnementsvertrag abgeschlossen wurde und die Kunden für die BSAG unter der ihr bekannten Adresse nicht erreichbar sind. Außerdem werden von der BSAG bei der Meldebehörde Bremen Sammelauskünfte im Rahmen des Vertriebs von Fahrscheinen im freien Verkauf zur Ermittlung des Verbleibs von Fahrkartenhändlern eingeholt. Die Einholung von Sammelauskünften dient dabei stets der Feststellung von Adressen, über die die Meldebehörde Bremen nach § 32 Abs. 1 BremMeldG Auskunft erteilt.

Der von der BSAG für die Anforderung von Sammelauskünften bei der Meldebehörde Bremen verwendete Anfragedatensatz besteht aus dem akademischen Grad, dem Zusatznamen, dem Namen

und dem Vornamen sowie der Anschrift (Straße, Hausnummer und Zusatzbuchstabe) und dem Geburtsdatum des Betroffenen. Der daraufhin von der Meldebehörde erzeugte Ausgabedatensatz besteht aus den bei der Eingabe verwendeten Datenfeldern zzgl. Postleitzahl und Wohnort sowie ggf. dem Sterbedatum des Betroffenen. Der Ausgabedatensatz geht damit über die in § 32 Abs. 1 BremMeldG (einfache Melderegisterauskunft) genannten Daten hinaus. Er umfasst auch Daten der erweiterten Melderegisterauskunft (Geburtsdatum, Sterbedatum) nach § 32 Abs. 2 BremMeldG.

Nach § 32 Abs. 2 BremMeldG ist die Erteilung einer erweiterten Melderegisterauskunft nur zulässig, soweit jemand ein berechtigtes Interesse glaubhaft macht. Eine Übermittlung dieser beiden letztgenannten Daten in allen Fällen ist sicherlich nicht erforderlich, sie kann darüber hinaus nur in den Fällen gewährt werden, in denen der Datenempfänger ein besonderes rechtliches Interesse glaubhaft war. Hierauf habe ich die Meldebehörde hingewiesen, eine Antwort steht derzeit noch aus.

14.16 Umstellung des Registers der meldepflichtigen Stellen

Nachdem sich die Regelungen zur Registerführung durch die Datenschutzaufsichtsbehörden mit der Novelle zum Bundesdatenschutz grundlegend geändert haben, war eine Umstellung des Registers der meldepflichtigen Stellen auch bei der Datenschutzaufsichtsbehörde in Bremen erforderlich (vgl. 24. JB, Ziff. 14.6). Die Umstellungsarbeiten konnten im vergangenen Jahr weitgehend abgeschlossen werden. Von insgesamt 152 Firmen, die vor der Umstellung des Registers geführt wurden, sind zwischenzeitlich 126 gelöscht worden. Nicht mehr im Register verzeichnet sind im wesentlichen die Stellen, die personenbezogene Daten im Auftrag als Dienstleistungsunternehmen verarbeiten oder nutzen, also z. B. Service-Rechenzentren, Datenerfassungsbetriebe, Mikroverfilmer. Bei den verbliebenen Firmen handelt es sich in 8 Fällen um Stellen, die auch nach dem neuen Bundesdatenschutzgesetz weiterhin meldepflichtig sind, also Stellen, die personenbezogene Daten geschäftsmäßig zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung speichern. Dies sind vornehmlich Handels- und Wirtschaftsauskunfteien sowie Markt- und Meinungsforschungsinstitute. In den restlichen 18 Fällen steht eine abschließende Überprüfung der Meldepflicht noch aus.

Da der Inhalt der Meldungen sich ebenfalls geändert hatte, kann das bisher eingesetzte, inzwischen auch veraltete Datenbank-Verfahren nicht mehr verwendet werden. Für die geringe Zahl von neuen Meldungen lohnt es sich nicht, ein eigenständiges DV-Verfahren zu entwickeln. Deshalb führe ich das Register derzeit im Rahmen meiner Office-Anwendungen. Ob mittelfristig andere Datenschutzaufsichtsbehörden ein geeignetes Software-Produkt verwenden, werde ich im Auge behalten.

Das Register ist erheblich kleiner geworden. Es bleibt aber eine unbestimmte Dunkelziffer, die daraus resultiert, dass kleine und mittlere Betriebe, die zur Erledigung ihrer Arbeiten auch personenbezogene Daten für eigene Zwecke verarbeiten, wie z. B. Rechtsanwaltskanzleien, Arztpraxen und Steuerberatungsfirmen, und die keinen betrieblichen Datenschutzbeauftragten bestellt haben, sich bislang nicht zum Register angemeldet haben, obwohl sie nach dem neuen Bundesdatenschutzgesetz hierzu verpflichtet wären.

Hinweisen möchte ich an dieser Stelle auf mein Internet-Angebot zur Meldepflicht unter www.datenschutz.bremen.de. Hier stehen die relevanten Unterlagen zur Verfügung: Merkblatt zur Meldepflicht, die erforderlichen Meldeformulare, Ausfüllhinweise hierzu und die einschlägigen Bestimmungen des Bundesdatenschutzgesetzes. Diese Unterlagen können von dort heruntergeladen werden.

15. Die Entschließungen der Datenschutzkonferenzen im Jahr 2002

15.1 Biometrische Merkmale in Personalausweisen und Pässen

(Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002)

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

Fälschliche Zurückweisungen berechtigter Personen durch automatisierte Personenerkennungssysteme sind auch bei ständiger Verbesserung der Technik prinzipiell nicht zu vermeiden. Es dürfen deshalb nur Verfahren in Betracht gezogen werden, bei denen die Fehlerquote zumutbar gering ist. In Fehlerfällen muss dafür Sorge getragen werden, dass eine die Betroffenen nicht diskriminierende rasche Aufklärung erfolgt.

Zu berücksichtigen ist, dass bei der Anwendung biometrischer Verfahren Zusatzinformationen anfallen können (z. B. Krankheits-, Unfall-, Beschäftigungsindikatoren). Es muss sichergestellt werden, dass die gespeicherten und verarbeiteten Daten keine Rückschlüsse auf zusätzliche personenbezogene Merkmale erlauben.

Systeme, die biometrische Daten aus Ausweisen ohne Kenntnis der Betroffenen verarbeiten (sog. passive Systeme), sind abzulehnen.

Der Gesetzgeber hat die Verwendung biometrischer Daten in Ausweisen und Pässen grundsätzlich auf die Feststellung beschränkt, dass die dort gespeicherten Daten mit den Merkmalen der jeweiligen Ausweisinhaber und -inhaberinnen übereinstimmen; dies muss erhalten bleiben. Die Verwendung der biometrischen Merkmale für andere öffentliche Zwecke (außer der gesetzlich zugelassenen Verwendung aus dem Fahndungsbestand) wie auch für privatrechtliche Zwecke (Versicherung, Gesundheitssystem) ist auszuschließen. Deshalb hat der Gesetzgeber zu Recht die Einrichtung zentraler Dateien ausgeschlossen. Diese gesetzgeberische Entscheidung darf nicht durch den Aufbau dezentraler Dateien umgangen werden.

Die Entscheidung über das auszuwählende biometrische Erkennungssystem verlangt ein abgestimmtes europäisches Vorgehen.

15.2 Umgang mit personenbezogenen Daten bei Anbietern von Tele-, Medien- und Telekommunikationsdiensten

(Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002)

Mit der rasch wachsenden Nutzung des Internet kommt dem datenschutzgerechten Umgang mit den dabei anfallenden Daten der Nutzerinnen und Nutzer immer größere Bedeutung zu. Die Datenschutzbeauftragten haben bereits in der Vergangenheit (Entschließung der 59. Konferenz "Für eine freie Telekommunikation in einer freien Gesellschaft") darauf hingewiesen, dass das Telekommunikationsgeheimnis eine unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft ist. Seine Geltung erstreckt sich auch auf Multimedia- und E-Mail-Dienste.

Die Datenschutzbeauftragten betonen, dass das von ihnen geforderte in sich schlüssige System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt, nach wie vor fehlt. Die Strafprozessordnung (und seit dem 1.1.2002 das Recht der Nachrichtendienste) enthält ausreichende Befugnisse, um den Strafverfolgungsbehörden (und den Nachrichtendiensten) im Einzelfall den Zugriff auf bei den Anbietern vorhandene personenbezogene Daten zu ermöglichen. Für eine zusätzliche Erweiterung dieser Regelungen z.B. hin zu einer Pflicht zur Vorratsdatenspeicherung besteht nicht nur kein Bedarf, sondern eine solche Pflicht würde dem Grundrecht auf unbeobachtete Kommunikation nicht gerecht, weil damit jede Handlung (jeder Mausklick) im Netz staatlicher Beobachtung unterworfen würde.

In keinem Fall sind Anbieter von Tele-, Medien- und Telekommunikationsdiensten berechtigt oder verpflichtet, generell Daten über ihre Nutzerinnen und Nutzer auf Vorrat zu erheben, zu speichern oder herauszugeben, die sie zu keinem Zeitpunkt für eigene Zwecke (Herstellung der Verbindung, Abrechnung) benötigen. Sie können nur im Einzelfall berechtigt sein oder verpflichtet werden, bei Vorliegen ausdrücklicher gesetzlicher Voraussetzungen Nachrichteninhalte, Verbindungsdaten und bestimmte Daten (Nutzungsdaten), die sie ursprünglich für eigene Zwecke benötigt haben und nach den Bestimmungen des Multimedia-Datenschutzrechts löschen müssten, den Strafverfolgungsbehörden (oder Nachrichtendiensten) zu übermitteln.

15.3 Datenschutzgerechte Nutzung von E-Mail und anderen Internet-Diensten am Arbeitsplatz

(Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002)

Immer mehr Beschäftigte erhalten die Möglichkeit, das Internet auch am Arbeitsplatz zu nutzen. Öffentliche Stellen des Bundes und der Länder haben beim Umgang mit den dabei anfallenden personenbezogenen Daten der Beschäftigten und ihrer Kommunikationspartner bestimmte datenschutzrechtliche Anforderungen zu beachten, die davon abhängen, ob den Bediensteten neben

der dienstlichen die private Nutzung des Internet am Arbeitsplatz gestattet wird. Der Arbeitskreis Medien der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat detaillierte Hinweise hierzu erarbeitet .

Insbesondere gilt Folgendes:

1. Die Arbeitsplätze mit Internet-Zugang sind so zu gestalten, dass keine oder möglichst wenige personenbezogene Daten erhoben werden. Die Nutzung des Internet am Arbeitsplatz darf nicht zu einer vollständigen Kontrolle der Bediensteten führen. Präventive Maßnahmen gegen eine unbefugte Nutzung sind nachträglichen Kontrollen vorzuziehen.

2. Die Beschäftigten sind umfassend darüber zu informieren, für welche Zwecke sie einen Internet-Zugang am Arbeitsplatz nutzen dürfen und auf welche Weise der Arbeitgeber die Einhaltung der Nutzungsbedingungen kontrolliert.

3. Fragen der Protokollierung und einzelfallbezogenen Überprüfung bei Missbrauchsverdacht sind durch Dienstvereinbarungen zu regeln. Die Kommunikation von schweigepflichtigen Personen und Personalvertretungen muss vor einer Überwachung grundsätzlich geschützt bleiben.

4. Soweit die Protokollierung der Internet-Nutzung aus Gründen des Datenschutzes, der Datensicherheit oder des ordnungsgemäßen Betriebs der Verfahren notwendig ist, dürfen die dabei anfallenden Daten nicht zur Leistungs- und Verhaltenskontrolle verwendet werden.

5. Wird den Beschäftigten die private E-Mail-Nutzung gestattet, so ist diese elektronische Post vom Telekommunikationsgeheimnis geschützt. Der Arbeitgeber darf ihren Inhalt grundsätzlich nicht zur Kenntnis nehmen, und hat dazu die erforderlichen technischen und organisatorischen Vorkehrungen zu treffen.

6. Der Arbeitgeber ist nicht verpflichtet, die private Nutzung des Internet am Arbeitsplatz zu gestatten. Wenn er dies gleichwohl tut, kann er die Gestattung unter Beachtung der hier genannten Grundsätze davon abhängig machen, dass die Beschäftigten einer Protokollierung zur Durchführung einer angemessenen Kontrolle der Netzaktivitäten zustimmen.

7. Die gleichen Bedingungen wie bei der Nutzung des Internet müssen prinzipiell bei der Nutzung von Intranets gelten.

Die Datenschutzbeauftragten fordern den Bundesgesetzgeber auf, auch wegen des Überwachungspotentials moderner Informations- und Kommunikationstechnik am Arbeitsplatz die Verabschiedung eines umfassenden Arbeitnehmerdatenschutzgesetzes nicht länger aufzuschieben.

15.4 Neues Abrufverfahren bei den Kreditinstituten

(Entschließung der 63. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 07./08. März 2002)

Nach der Novelle des Gesetzes über das Kreditwesen soll die zuständige Bundesanstalt die von den Kreditinstituten vorzuhaltenden Daten, wer welche Konten und Depots hat, ohne Kenntnis der

Kundinnen und Kunden zur eigenen Aufgabenerfüllung oder zu Gunsten anderer öffentlicher Stellen abrufen können. Dies ist ein neuer Eingriff in die Vertraulichkeit der Bankbeziehungen.

Dieser Eingriff in die Vertraulichkeit der Bankbeziehungen muss gegenüber den Kundinnen und Kunden zumindest durch eine aussagekräftige Information transparent gemacht werden. Die Konferenz fordert daher, dass zugleich mit der Einführung dieses Abrufverfahrens eine Verpflichtung der Kreditinstitute zur generellen Information der Kundinnen und Kunden vorgesehen wird und diese die Kenntnisnahme schriftlich bestätigen. Dadurch soll zugleich eine effektive Wahrnehmung des Auskunftsrechts der Kundinnen und Kunden gewährleistet werden.

Die Erweiterung der Pflichten der Kreditinstitute, Kontenbewegungen auf die Einhaltung gesetzlicher Bestimmungen mit Hilfe von EDV-Programmen zu überprüfen, verpflichtet die Kreditinstitute außerdem zu einer entsprechend intensiven Kontenüberwachung (sog. “know your customer principle”). Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass die Überprüfung in einer Weise stattfindet, die ein datenschutzkonformes Vorgehen sicherstellt.

15.5 Geplanter genereller Identifikationszwang in der Telekommunikation

(Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Umlaufverfahren vom 24. Mai 2002)

Das Bundesministerium für Wirtschaft und Technologie hat einen Entwurf zur Änderung des Telekommunikationsgesetzes veröffentlicht. Der Entwurf hat das Ziel, jeden Anbieter, der geschäftsmäßig Telekommunikationsdienste erbringt, dazu zu verpflichten, Namen, Anschriften, Geburtsdaten und Rufnummern seiner Kundinnen und Kunden zu erheben. Die Kundinnen und Kunden werden verpflichtet, dafür ihren Personalausweis vorzulegen, dessen Nummer ebenfalls gespeichert werden soll. Die beabsichtigten Änderungen sollen in erster Linie dazu führen, auch Nutzerinnen und Nutzer von Prepaid-Karten (also die Erwerberinnen und Erwerber von SIM-Karten ohne Vertrag) im Mobilfunk erfassen zu können. Die erhobenen Daten sollen allein dem Zweck dienen, den Sicherheitsbehörden zum jederzeitigen Online-Abruf über die Regulierungsbehörde für Telekommunikation und Post bereitzustehen. Im gleichen Zuge sollen die Zugriffsmöglichkeiten der Sicherheitsbehörden auf diese Daten dadurch erheblich erweitert werden, indem auf die Kundendateien nach abstrakten Merkmalen zugegriffen werden kann.

Die Datenschutzbeauftragten des Bundes und der Länder lehnen dieses Vorhaben ab. Unter der unscheinbaren Überschrift "Schließen von Regelungslücken" stehen grundlegende Prinzipien des Datenschutzes zur Disposition. Kritikwürdig an dem geplanten Gesetz sind insbesondere die folgenden Punkte:

- Der geplante Grundrechtseingriff ist nicht erforderlich, um die Ermittlungstätigkeit der Sicherheitsbehörden zu erleichtern. Seine Eignung ist zweifelhaft: Auch die Gesetzesänderung wird nicht verhindern, dass Straftäterinnen und Straftäter bewusst und gezielt in kurzen Zeitabständen neue Prepaid-Karten erwerben, Strohleute zum Erwerb einsetzen, die Karten häufig – teilweise nach jedem Telefonat – wechseln oder die Karten untereinander tauschen. In der Begründung wird nicht plausibel dargelegt, dass mit dem geltenden Recht die

Ermittlungstätigkeit tatsächlich behindert und durch die geplante Änderung erleichtert wird. Derzeit laufende Forschungsvorhaben beziehen diese Frage nicht mit ein.

- Der Entwurf widerspricht auch dem in den Datenschutzrichtlinien der Europäischen Union verankerten Grundsatz, dass Unternehmen nur solche personenbezogenen Daten verarbeiten dürfen, die sie selbst zur Erbringung einer bestimmten Dienstleistung benötigen.
- Die Anbieter würden eine Reihe von Daten auf Vorrat speichern müssen, die sie selbst für den Vertrag mit ihren Kunden nicht benötigen. Die ganz überwiegende Zahl der Nutzerinnen und Nutzer von Prepaid-Karten, darunter eine große Zahl Minderjähriger, würde registriert, obwohl sie sich völlig rechtmäßig verhalten und ihre Daten demzufolge für die Ermittlungstätigkeit der Strafverfolgungsbehörden nicht benötigt werden. Das Anhäufen von sinn- und nutzlosen Datenhalden wäre die Folge.
- Die gesetzliche Verpflichtung, sich an dem Ziel von Datenvermeidung und Datensparsamkeit auszurichten, würde konterkariert. Gerade die Prepaid-Karten sind ein gutes praktisches Beispiel für den Einsatz datenschutzfreundlicher Technologien, da sie anonymes Kommunizieren auf unkomplizierte Weise ermöglichen. Die Nutzung dieser Angebote darf deshalb nicht von der Speicherung von Bestandsdaten abhängig gemacht werden.
- Mit der Verpflichtung, den Personalausweis vorzulegen, würden die Anbieter zusätzliche Informationen über die Nutzerinnen und Nutzer erhalten, die sie nicht benötigen, z. B. die Nationalität, Größe oder Augenfarbe. Die vorgesehene Pflicht, auch die Personalausweisnummern zu registrieren, darf auch künftig keinesfalls dazu führen, dass die Ausweisnummern den Sicherheitsbehörden direkt zum Abruf bereit gestellt werden und sie damit diese Daten auch für die Verknüpfung mit anderen Datenbeständen verwenden können.
- Auch Krankenhäuser, Hotels, Schulen und Hochschulen sowie Unternehmen und Behörden, die ihren Mitarbeiterinnen und Mitarbeitern das private Telefonieren gestatten, sollen verpflichtet werden, die Personalausweisnummern der Nutzerinnen und Nutzer zu registrieren.
- Die Befugnis, Kundendateien mit unvollständigen oder ähnlichen Suchbegriffen abzufragen, würde den Sicherheitsbehörden eine Vielzahl personenbezogener Daten unbeteiligter Dritter zugänglich machen, ohne dass diese Daten für ihre Aufgaben erforderlich sind. Die notwendige strikte Beschränkung dieser weitreichenden Abfragebefugnis durch Rechtsverordnung setzt voraus, dass ein entsprechender Verordnungsentwurf bei der Beratung des Gesetzes vorliegt.
- Der Formulierungsvorschlag des Bundeswirtschaftsministeriums lässt eine Auseinandersetzung mit dem Recht auf informationelle Selbstbestimmung der Kundinnen und Kunden der Telekommunikationsunternehmen weitgehend vermissen.
- Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesregierung und den Gesetzgeber auf, auf die geplante Änderung des Telekommunikationsgesetzes zu verzichten und vor weiteren Änderungen die bestehenden Befugnisse der Sicherheitsbehörden durch unabhängige Stellen evaluieren zu lassen.

15.6 Datenschutzgerechte Vergütung für digitale Privatkopien im neuen Urheberrecht

(Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24/25.Oktober 2002)

Zur Umsetzung der EU-Urheberrechtsrichtlinie wird gegenwärtig über den Entwurf der Bundesregierung für ein Gesetz zur Regelung des Urheberrechts in der Informationsgesellschaft beraten. Hierzu hat der Bundesrat die Forderung erhoben, das bisherige System der Pauschalabgaben auf Geräte und Kopiermedien, die von den Verwertungsgesellschaften auf die Urheberinnen und Urheber zur Abgeltung ihrer Vergütungsansprüche verteilt werden, durch eine vorrangige individuelle Lizenzierung zu ersetzen. Zugleich hat der Bundesrat die Gewährleistung eines ausreichenden Schutzes der Nutzerinnen und Nutzer vor Ausspähung personenbezogener Daten über die individuelle Nutzung von Werken und die Erstellung von Nutzungsprofilen gefordert.

Die Datenschutzbeauftragten des Bundes und der Länder weisen in diesem Zusammenhang auf Folgendes hin: Das gegenwärtig praktizierte Verfahren der Pauschalvergütung beruht darauf, dass der Bundesgerichtshof eine individuelle Überprüfung des Einsatzes von analogen Kopiertechniken durch Privatpersonen zur Durchsetzung von urheberrechtlichen Vergütungsansprüchen als unvereinbar mit dem verfassungsrechtlichen Schutz der persönlichen Freiheitsrechte der Nutzerinnen und Nutzer bezeichnet hat. Diese Feststellung behält auch unter den Bedingungen der Digitaltechnik und des Internets ihre Berechtigung. Die Datenschutzkonferenz bestärkt den Gesetzgeber, an diesem bewährten, datenschutzfreundlichen Verfahren festzuhalten. Sollte der Gesetzgeber – wie es der Bundesrat fordert – jetzt für digitale Privatkopien vom Grundsatz der Pauschalvergütung (Geräteabgabe) tatsächlich abgehen wollen, so kann er den verfassungsrechtlichen Vorgaben nur entsprechen, wenn er sicherstellt, dass die urheberrechtliche Vergütung aufgrund von statistischen oder anonymisierten Angaben über die Nutzung einzelner Werke erhoben wird. Auch technische Systeme zur digitalen Verwaltung digitaler Rechte (Digital Rights Management) müssen datenschutzfreundlich gestaltet werden.

15.7 Speicherung und Veröffentlichung der Standortverzeichnisse von Mobilfunkantennen

(Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24/25.Oktober 2002)

Die Speicherung und die Veröffentlichung der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen zur Zeit in verstärktem Maße in der öffentlichen Diskussion. Mehrere kommunale Spitzenverbände haben sich diesbezüglich bereits an die jeweiligen Landesdatenschutzbeauftragten gewandt. Unbeschadet bereits bestehender Landesregelungen und der Möglichkeit, Daten ohne Grundstücksbezug zu veröffentlichen, fordert die 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder aufgrund der bundesweiten Bedeutung der

Frage den Bundesgesetzgeber auf, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung von Mobilfunkkatastern zu entscheiden.

Dabei ist zu bestimmen, wie derartige Kataster erstellt werden sollen. Die gegenwärtige Regelung des Bundesimmissionsschutzgesetzes sieht keine ausdrückliche Ermächtigung zur Schaffung von Mobilfunkkatastern vor, so dass deren Erstellung und Veröffentlichung ohne Einwilligung der Grundstückseigentümer und -eigentümerinnen und der Antennenbetreiber keine ausdrückliche gesetzliche Grundlage hat. Bei der Novellierung ist insbesondere zu regeln, ob und unter welchen Bedingungen eine Veröffentlichung derartiger Kataster im Internet oder in vergleichbaren Medien zulässig ist. Individuelle Auskunftsansprüche nach dem Umweltinformationsgesetz oder den Informationsfreiheitsgesetzen bleiben davon unberührt.

15.8 Systematische verdachtslose Datenspeicherung in der Telekommunikation und im Internet

(Entschließung der 64. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 24/25.Oktober 2002)

Gegenwärtig werden sowohl auf nationaler als auch auf europäischer Ebene Vorschläge erörtert, die den Datenschutz im Bereich der Telekommunikation und der Internetnutzung und insbesondere den Schutz des Telekommunikationsgeheimnnisses grundlegend in Frage stellen.

Geplant ist, alle Anbieter von Telekommunikations- und Multimediadiensten zur verdachtslosen Speicherung sämtlicher Bestands-, Verbindungs-, Nutzungs- und Abrechnungsdaten auf Vorrat für Mindestfristen von einem Jahr und mehr zu verpflichten, auch wenn sie für die Geschäftszwecke der Anbieter nicht (mehr) notwendig sind. Das so entstehende umfassende Datenreservoir soll dem Zugriff der Strafverfolgungsbehörden, der Polizei und des Verfassungsschutzes bei möglichen Anlässen in der Zukunft unterliegen. Auch auf europäischer Ebene werden im Rahmen der Zusammenarbeit der Mitgliedsstaaten in den Bereichen „Justiz und Inneres“ entsprechende Maßnahmen - allerdings unter weitgehendem Ausschluss der Öffentlichkeit - diskutiert.

Die Datenschutzbeauftragten des Bundes und der Länder treten diesen Überlegungen mit Entschiedenheit entgegen. Sie haben schon mehrfach die Bedeutung des Telekommunikationsgeheimnisses als unabdingbare Voraussetzung für eine freiheitliche demokratische Kommunikationsgesellschaft hervorgehoben. Immer mehr menschliche Lebensäußerungen finden heute in elektronischen Netzen statt. Sie würden bei einer Verwirklichung der genannten Pläne einem ungleich höheren Überwachungsdruck ausgesetzt als vergleichbare Lebensäußerungen in der realen Welt. Bisher muss niemand bei der Aufgabe eines einfachen Briefes im Postamt seinen Personalausweis vorlegen oder in einer öffentlichen Bibliothek registrieren lassen, welche Seite er in welchem Buch aufschlägt. Eine vergleichbar umfassende Kontrolle entsprechender Online-Aktivitäten (E-Mail-Versand, Nutzung des WorldWideWeb), wie sie jetzt erwogen wird, ist ebensowenig hinnehmbar.

Zudem hat der Gesetzgeber erst vor kurzem die Befugnisse der Strafverfolgungsbehörden erneut deutlich erweitert. Die praktischen Erfahrungen mit diesen Regelungen sind von unabhängiger Seite zu evaluieren, bevor weitergehende Befugnisse diskutiert werden.

Die Konferenz der europäischen Datenschutzbeauftragten hat in ihrer Erklärung vom 11. September 2002 betont, dass eine flächendeckende anlassunabhängige Speicherung sämtlicher Daten, die bei der zunehmenden Nutzung von öffentlichen Kommunikationsnetzen entstehen, unverhältnismäßig und mit dem Menschenrecht auf Achtung des Privatlebens unvereinbar wäre. Auch in den Vereinigten Staaten sind vergleichbare Maßnahmen nicht vorgesehen.

Mit dem deutschen Verfassungsrecht ist eine verdachtslose routinemäßige Speicherung sämtlicher bei der Nutzung von Kommunikationsnetzen anfallender Daten auf Vorrat nicht zu vereinbaren. Auch die Rechtsprechung des Europäischen Gerichtshofs lässt eine solche Vorratsspeicherung aus Gründen bloßer Nützlichkeit nicht zu.

Die Konferenz fordert die Bundesregierung deshalb auf, für mehr Transparenz der Beratungen auf europäischer Regierungsebene einzutreten und insbesondere einer Regelung zur flächendeckenden Vorratsdatenspeicherung nicht zuzustimmen.

16. Anforderungen im Internationalen Datenverkehr

(Anforderungen des Düsseldorfer Kreises bei der Datenübermittlung in Drittländer ohne angemessenes Datenschutzniveau und bei verbindlichen Unternehmensregelungen)

1. Eine Genehmigung nach § 4 c Abs. 2 Satz 1 BDSG ist nur erforderlich, wenn kumulativ folgende Voraussetzungen vorliegen:

    a) Es muss sich um Datenübermittlungen personenbezogener Daten an Stellen handeln, die sich nicht in Mitgliedstaaten der Europäischen Union oder den EWR-Staaten befinden.

    b) Es greift keiner der in § 4 c Abs. 1 Satz 1 BDSG ausgeführten Ausnahmetatbestände ein, wie z. B. das Vorliegen einer Einwilligung des Betroffenen oder Erforderlichkeit für die Erfüllung eines Vertrages zwischen dem Betroffenen und der verantwortlichen Stelle.

    c) Für die datenimportierende Stelle im Drittland ist kein angemessenes Schutzniveau im Sinne des § 4 b Abs. 2 Satz 2, Absatz 3 BDSG gewährleistet, was von der datenexportierenden Stelle in eigener Zuständigkeit zu prüfen ist. Das angemessene Schutzniveau ist ausnahmslos dann als gewährleistet anzusehen, wenn eine positive Entscheidung der Europäischen Kommission gem. Art. 25 Abs. 6 der EG-Datenschutzrichtlinie übet ein angemessenes Datenschutzniveau für das betreffende Land vorliegt; dies ist bisher geschehen für Ungarn, die Schweiz und in begrenztem Umfang für Kanada.

2. Erfolgt die Datenübermittlung in Drittländer auf der Grundlage der von der Europäischen Kommission nach Art. 26 Abs. 4 der EG-Datenschutzrichtlinie herausgegebenen Standardvertragsklauseln, bedarf die Datenübermittlung keiner zusätzlichen Genehmigung nach § 4 c Abs. 2 BDSG.

3. Da sich die Frage der ausreichenden Garantien für jedes Drittland gesondert stellt, muss sich eine Genehmigung nach § 4 c Abs. 2 BDSG immer auf ein einzelnes konkretes Drittland beziehen, das deshalb im Antrag anzugeben ist. Dies bedeutet jedoch nicht, dass nicht in einer einheitlichen Genehmigung Übermittlungen in mehrere Drittländer zusammengefasst werden können. Ob dies möglich ist, hängt neben dem Inhalt der jeweiligen verbindlichen Unternehmensregelung insbesondere davon ab, wie genau die genehmigungsbedürftigen Datenübermittlungen beschrieben werden können.

4. Eine Genehmigung nach § 4c Abs. 2 BDSG wird unter Widerrufsvorbehalt erteilt. Der Grund dafür ist, dass die erteilte Genehmigung wegen der Pflicht zur Notifizierung nach § 4 c Abs. 3 BDSG dem Bund und von diesem nach Art. 26 Abs. 3 der EG-Datenschutzrichtlinie der Europäischen Kommission vorgelegt werden muss. Nach Art. 26 Abs. 3 i. V. m. Art. 31 Abs. 2 der EG-Datenschutzrichtlinie besteht für andere Mitgliedstaaten und für die Europäische Kommission die Möglichkeit, Widerspruch gegen die erteilte Genehmigung einzuleiten. Die Kommission kann geeignete Maßnahmen erlassen, die von den Mitgliedstaaten zu beachten sind. Der

Widerrufsvorbehalt sichert der Aufsichtsbehörde die Möglichkeit, die von der Europäischen Kommission ggf. beschlossenen Maßnahmen umsetzen zu können.

5. Unternehmensregelungen sind selbst weder genehmigungsbedürftig noch genehmigungsfähig, da nach § 4c Abs. 2 BDSG nur konkrete Datenübermittlungen genehmigungsbedürftig und genehmigungsfähig sind. Unternehmensregelungen sind lediglich bei der Prüfung der Genehmigungsfähigkeit dieser Datenübermittlungen heranzuziehen um beurteilen zu können, ob ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte gegeben sind.

17. Anhang

17.1 Auswahl von Presseberichten in Tageszeitungen/Zeitschriften im Jahr 2002 mit Themen aus dem Land Bremen

Datum	Zeitung	Titel/Inhalt
09.02.	taz-Bremen	**Rasterfahndung: Bremen droht Klage** Klage eines Studenten der Bremer Hochschule gegen die Rasterfahndung
20.02.	Weser-Kurier	**Sammelauskunft jetzt online** Neuer Service der Meldebehörde
25.02.	Die Welt-Bremen	**Rasterfahndung steht vor Gericht** Marokkanischer Student hat Klage eingereicht – Innenressort gelassen
28.02.	taz-Bremen	**Erfolglos verwanzt** Erster Erfahrungsbericht der Bundesregierung zum großen Lauschangriff
28.02.	Weser-Kurier	**Ausweise via Internet ab 2005** IM Schily stellte Programm zur Modernisierung der Behörden vor
03.03.	taz-Bremen	**Dein Password gehört mir!** Datenschützer warnt vor dem „gläsernen Angestellten“
13.03.	Weser-Kurier	**Datenschützer fordern Arbeitnehmer-Gesetz** Zum von der Bundesregierung angekündigten Datenschutzgesetz für Arbeitnehmer
13.03.	Die Welt-Bremen	**Bremer Datenschützer unterstützen Entschließung** Entschließungen zur Rasterfahndung und zu Auskunftsansprüchen von Bankkunden auf der 63. Konferenz der DSB des Bundes und der Länder
14.03.	taz-Bremen	**TV-Beweis bei Demonstrationen** Fernsehbilder sollen Abschiebegegner überführen
14.03.	Weser-Kurier	**Journalisten als Hilfspolizisten?** Debatte um Filmaufnahmen bei Demo
14.03.	taz-Bremen	**Personalakten mit Füßen getreten** In einer alten Großküche in Vegesack liegen kistenweise alte Personalakten herum
14.03.	Weser-Kurier	**Personalakten in Ruine entdeckt** Verstoß gegen Datenschutz
15.03.	taz-Bremen	**Genug konspiriert!** Datenschützer will, dass Geheimnis geheim bleibt: Indiskretion schadet dem Untersuchungsausschuss
22.03.	Nordsee-Zeitung	**„Datenschutz muss sexy sein“** Jahresbericht einen Tag vor der Neuauflage in der Bürgerschaft debattiert

23.03.	Kreiszeitung Syke	**„Die Politik hat überreagiert“** Datenschützer legt Jahresbericht vor
23.03.	Bild Bremen	**Datenspionage im Internet** Der aktuelle Jahresbericht listet alle Verstöße auf
23.03.	Die Welt-Bremen	**Datenschutzbericht vorgelegt**
23.03.	Weser-Kurier	**589 Datensätze kamen aus Bremen** Unterlagen zur Rasterfahndung Vorstellung des Jahresberichts
23.03.	taz-Bremen	**Datenschützer Holst rüffelt Böse** Jahresbericht vorgelegt
23.03.	Nordsee-Zeitung	**Private E-Mails und die Rasterfahndung** Landesbeauftragter legt Jahresbericht 2001 vor
25.03.	Delmenhorster Kreisblatt	**„Politik hat nach Anschlägen überreagiert“** Datenschützer legt Jahresbericht vor Verstöße gegen Bestimmungen moniert
26.03.	Weser-Kurier	**Wie steht es mit dem Datenschutz“** Bestellung eines betrieblichen Datenschutzbeauftragten nach dem Bundesdatenschutzgestz (BDSG)
28.03.	taz-Bremen	**Böse darf weiter rastern** Gericht sieht weiter Terror-Gefahr in Bremen
29.03.	Weser-Kurier	**Verwendung von Daten rechtens** Gerichtsentscheid zur Rasterfahndung
01.04.	STERN	**Call-Center: Die Anonymität ist gefährdet** Aus dem Jahresbericht 2001 des LfD Bremen
03.04.	Weser-Kurier	**300 Euro und keine Erkenntnis** Bilanz zur Wohnraumüberwachung
05.04.	taz-Bremen	**Aktenfund: Ultimatum ist abgelaufen** Fund von Personalakten in der Ruine einer Vegesacker Großküche
10.04.	Kreiszeitung Syke	**„Gläserner Angestellter“** Holst: Mehr Schutz am Arbeitsplatz
12.04.	Weser-Kurier	**Rasterfahndung in zwei Fällen gestoppt** Ausländische Studenten klagen erfolgreich gegen LKA
24.04.	taz-Bremen	**Telefonüberwachung seit 1999 vervierfacht** Datenschutzausschuss kritisiert Senat
07.05.	taz-Bremen	**Keine Info mit der CDU** Bremer Informations-Gesetz könnte an CDU-Geheimniskrämern scheitern
30.05.	taz-Bremen	**Datenschützer schlägt Alarm** Erklärung gegen die zwangsweise „Vorratsspeicherung“ von Telekommunikationsdaten
31.05.	Frankfurter Rundschau	**Sven Holst zur Neuregelung für Internet-** und Telekommunikationsanbieter durch den Bundesrat

05.06.	Nordsee-Zeitung	**Datenschützer kontrolliert auch Schulen** Vorstellung des LfD der Schwerpunkte des 24. Jahresberichts im Datenschutzausschuss
13.07.	Weser-Kurier	**Sven Holst wirbt für mehr Diskretion** wenn es um Unterlagen für Untersuchungsausschüsse geht
15.07.	taz-Bremen	**Genug konspiriert!** Datenschützer will, dass Geheimnis geheim bleibt: Indiskretion schadet dem Untersuchungsausschuss
18.07.	taz-Bremen	**Einsicht am Nimmerleinstag** Das Informationsfreiheitsgesetz wird Anfang August an den Stimmen der CDU scheitern ...
14.08.	Die Welt-Bremen	**Datenschutzgesetz steht vor Änderung**
14.08.	Delmenhorster Kreisblatt	**Datenschutzrecht soll neu strukturiert werden**
14.08.	BN/Weser-Kurier	**Neues Datengesetz soll Bürger stärken**
14.08.	Kreiszeitung Syke	**Datenschutzgesetz wird neu strukturiert**
14.08.	taz-Bremen	**Video Überwachung geregelt** Senat beschließt Entwurf für neues Datenschutzgesetz: Mehr Macht für Datenhüter
14.08.	Nordsee-Zeitung	**Datenschutz soll geändert werden**
15.08.	Nordsee-Zeitung	**Richter sollen zustimmen** Datenschützer fordert Anpassung der Bremer Vorschriften an das so genannte G10-Gesetz des Bundes
18.10.	Bild-Bremen	**Skandal um schmuddelige Kinderpornos** Verfahren gegen Richter eingestellt
21.10.	taz-Bremen	**Beirat fürchtet Verdrängung** von Straftaten vom Bahnhofsplatz u. a. in die westliche Innenstadt
21.10.	taz-Bremen	**Eine 3 fürs Pipi machen** Mitarbeiter und Kunden von Call-Centern werden häufig überwacht
28.10.	taz-Bremen	**Surfen ohne Selbstkontrolle** Datenschützer protestieren gegen Pläne zum Ausbau der Überwachung im Internet
01.11.	Die Welt Bremen	**E-Goverment: Bremen geht einen Schritt weiter** Online-Angebote werden jetzt „barrierefrei“ für Behinderte und ältere Menschen umgestaltet
01.11.	Weser-Kurier	**Big Brother „Orvell“ am Arbeitsplatz** Datenschutz adé: Rund-Um-Überwachung der Angestellten mit Computerprogrammen
08.11.	taz-Bremen	**Check vom Verfassungsschutz** Auskünfte des Landesamtes seit Einführung der Regelanfrage für Einbürgerungswillige
12.11.	Weser-Kurier	**Datenschutz in Theorie und Praxis** Bremer Forum vermittelt zwischen Gesetzgeber und Anwendern

26.11.	taz-Bremen	**Semantische Subtilitäten** Justizressort pocht auf die Verfassung (zur Wahl des DSB)
27.11.	BN/Weser-Kurier	**Ausschuss will mitreden** Modus für Auswahl des DSB sorgt für Konflikt
29.11.	Weser-Kurier	**Perspektive: Ein Datenschützer in jeder Behörde des Lan**des Ausschuss beriet Gesetzesänderung
05.12.	taz Bremen	**Mäurer lernt benehmen** Parlament darf bei der Auswahl des Datenschutzbeauftragten „mitmischen“
05.12.	Weser-Kurier	**Parlamentarier setzen sich durch** Zum Auswahlverfahren im Benehmen mit dem Datenschutzausschuss
05.12.	Nordsee-Zeitung	**Justizressort beugt sich dem Ausschuss** Mitspracherecht bei Auswahl des Datenschutzbeauftragten
13.12.	taz- Bremen	**Reingefunkt: Datennetze im Test** Fehlendes Sicherheitsbewusstsein der Bürger für Funknetze

17.2 Pressekampagne: „Selbstverteidigung im Internet“

Darstellung der Zeitungsartikel auf der Homepage leider nicht möglich.

17.3 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:

20. Jahresbericht 1997, Bürgerschafts-Drs. 14/1005	(Restexemplare)
21. Jahresbericht 1998, Bürgerschafts-Drs. 14/1399	(vergriffen)
22. Jahresbericht 1999, Bürgerschafts-Drs. 15/266	(Restexemplare)
23. Jahresbericht 2000, Bürgerschafts-Drs. 15/852	(vergriffen)
24. Jahresbericht 2001, Bürgerschafts-Drs. 15/1106	

Broschüre	„Mobilfunk und Datenschutz"
Broschüre	„Datenschutz bei WindowsNT"
Broschüre	„Handlungsempfehlungen datenschutzgerechtes e-Government“
Broschüre	„Vom Bürgerbüro zum Internet“
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

17.4 Index