BREMISCHE BÜRGERSCHAFT
Landtag
15. Wahlperiode

Drucksache 15/1106
22. 03. 02

24. Jahresbericht des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2001 den 24. Jahresbericht zum 31. März 2002 (§ 33 Abs. 1 Bremisches Datenschutzgesetz — BrDSG). Redaktionsschluss für die Beiträge war der 31. Januar 2002; ich war bemüht, alle bis dahin eingehenden Äußerungen zu berücksichtigen.

Sven Holst
Landesbeauftragter für den Datenschutz

Inhaltsverzeichnis

1. Vorwort

Dieser Jahresbericht ist etwas kürzer ausgefallen als die Berichte der letzten Jahre. Das hängt nicht damit zusammen, dass meine Dienststelle weniger zu tun hatte als in den vergangenen Jahren, sondern mit einer Vereinfachung, die ich mit Senat und Datenschutzausschuss abgesprochen habe.

Andere Datenschutzgesetze sehen für die Datenschutzbeauftragten einen zweijährigen Berichtszeitraum vor. Gegen eine solche Frist habe ich mich bisher ausgesprochen, weil zum einen die Aktualität des Berichtes darunter leiden würde, zum anderen können — nicht zuletzt durch die Befassung des Datenschutzausschusses — festgestellte Mängel behoben und sonstige von mir vorgeschlagene Verbesserungen für den Datenschutz in der Regel binnen Jahresfrist erreicht werden. Diese kurzen Reaktionsfristen könnten bei einem Zwei-Jahres-Rhythmus nicht gehalten werden.

Gleichwohl bindet die Erstellung des Jahresberichts personelle Ressourcen, die für die inhaltliche Arbeit genutzt werden könnten. Ich habe daher vorgeschlagen, alle zwei Jahre einen umfassenden Bericht vorzulegen, der alle Statistiken und sonstigen Übersichten enthält und mich dazwischen auf die Berichterstattung wesentlicher, aktueller oder bereits abgeschlossener Vorgänge zu beschränken. Der Datenschutzausschuss erklärte sich mit dieser Vorgehensweise einverstanden mit der Maßgabe, dass auch bei einem Kurzbericht die Berichterstattung über „kritische Themen“ nicht zu kurz komme. Eine Vorgabe, der ich selbstverständlich auch mit dem jetzt vorgelegten Bericht nachkomme.

Weiter möchte ich darauf hinweisen, dass ich über nicht geschützte Übergänge in das Internet, die ich bei Prüfungen feststelle, nicht öffentlich berichte, um nicht zu Attacken einzuladen und den Stellen die Möglichkeit zu geben, die erforderlichen Schutzvorkehrungen zu treffen.

1.1. Folgen des Terroranschlags

Das Berichtsjahr wurde überschattet von den schrecklichen Ereignissen vom 11. September 2001 in den USA. Unmittelbar danach stand die Welt Kopf. So schienen vor allem viele öffentliche Stellen in Deutschland eine notstandsähnliche Situation anzunehmen und setzten sich über datenschutzrechtliche Vorschriften einfach hinweg. Da wurde aus anderen Ländern ohne ausreichende Rechtsgrundlage wie selbstverständlich die Übermittlung einer Vielzahl von Daten, insbesondere Studierender erbeten, ebenso forderte das Bundeskriminalamt bei den Energieunternehmen Daten „auf freiwilliger Basis“ an, als wenn die Unternehmen und nicht die Betroffenen selbst das Entscheidungsrecht über die Weitergabe ihrer Daten hätten (vgl. 14.18. dieses Berichts) und in Bremen wurde überlegt, ob auch bereits vor der parlamentarischen Beratung der Regelung zur Rasterfahndung eine entsprechende Datenübermittlung von Seiten der Universität veranlasst werden könne.

Angesichts der brisanten Stimmung habe ich in Frage kommende Stellen aufgesucht bzw. mich mit ihnen in Verbindung gesetzt und die bereits eingeleiteten und noch geplanten Aktivitäten unter datenschutzrechtlichen Gesichtspunkten besprochen, insbesondere mit dem Innenressort sowie mit der Polizei (Staatsschutz) und mit dem Landesamt für Verfassungsschutz. So konnte ich z. B. erreichen, dass erst nachdem die Regelung zur Rasterfahndung Gesetz war, eine Datenanforderung nach den in der Vorschrift festgelegten Regularien an die speichernden Stellen gestellt wurde (vgl. Ziff. 6.2. dieses Berichts).

Die Forderungen nach neuen einschneidenden Überwachungsbefugnissen für Geheimdienste und Polizei überschlugen sich nach dem Terroranschlag auf das World Trade Center und das Pentagon. Dabei handelte es sich nicht etwa um Forderungen zu Gesetzesänderungen nach Analyse der festgestellten Fakten über die Vorgehensweise der Täter und ihrer Hintermänner, um so gezielt den Terrorismus zu bekämpfen, sondern es wurden vielfach alte Hüte der Sicherheitsapologeten aus den Schubladen gezogen, die in den Jahren zuvor dorthin verbannt wurden, weil sie politisch nicht durchsetzbar waren.

Der Datenschutz war wieder einmal an allem Schuld. Der Presse war z. B. zu entnehmen, dass Bundesinnenminister Schily einen überzogenen Datenschutz für

Fahndungspannen verantwortlich machte. Den Beweis ist er allerdings bis heute schuldig geblieben. Schon in anderen Fällen hat es solche Vorwürfe gegeben, alle konnten bisher entkräftet werden. Bei näherem Hinsehen waren immer andere Ursachen für die Pannen und Misserfolge verantwortlich.

Im Übrigen hat sich der Datenschutz noch nie gegen erforderliche, geeignete und verhältnismäßige Maßnahmen gestemmt. Ohne Zweifel ist der Datenschutz keine ein für allemal feststehende Größe. Er muss immer wieder auf die konkreten technischen und gesellschaftlichen Veränderungen bezogen werden. Deshalb hätten sich die Datenschutzbeauftragten angesichts der schwierigen Situation auch nicht neuen Maßnahmen verweigert, wenn deren Notwendigkeit, Geeignetheit und Angemessenheit nachgewiesen wäre.

Das Bundesinnenministerium kam binnen kurzer Frist mit zwei Gesetzespaketen auf den Tisch, von denen allein das zweite Paket Rechtsänderungen in mehr als zwanzig Gesetzen vorsah. Sie wurden in Windeseile ohne ausreichende Beratungszeit verabschiedet. Dabei waren Stellungnahmefristen zu den Gesamtpaketen von weniger als achtundvierzig Stunden keine Seltenheit. Eine in weiten Teilen kritische Stellungnahme aus dem Justizministerium mit erheblichen rechtsstaatlichen und verfassungsrechtlichen Bedenken wurde vom Tisch gewischt, die politische Beratung in der Regierungskoalition in einer Marathonsitzung brachte keine tiefgreifenden Änderungen. Dabei wirkten die Wahlergebnisse der Schill-Partei in Hamburg noch wie Zunder. Auch die Medien mit immer neuen Enthüllungen und Mutmaßungen zu dem Vorgehen der Täter und ihrer Organisation taten ein Übriges dazu. Warnende Stimmen konnten sich in dieser Zeit kaum Gehör verschaffen (vgl. auch die Entschließungen der Konferenz der Datenschutzbeauftragten unter Ziff. 15.9., 15.14. und 15.15. dieses Berichts). Stücke der Freiheit und des informationellen Selbstbestimmungsrechtes wurden geopfert für das lose Versprechen auf mehr Sicherheit.

Ich selbst habe in der Zeit zum Teil mit anderen Landesdatenschutzbeauftragten verschiedene Presseerklärungen abgegeben (siehe meine Homepage). So erklärte ich im Oktober: „Der Schock über die Terroranschläge in den USA sitzt auch einen Monat danach zweifellos noch tief. Die Politik sollte sich aber nicht von Emotionen leiten lassen, sondern ihre Reaktionen auf die geänderte Sicherheitslage zielgenau, kühl und überlegt angehen. Wir sollten uns davor hüten, die Freiheitsrechte unserer Bürger insgesamt einzuschränken, ohne dass unter Abwägung der Vor- und Nachteile ein gesicherter Erfolg damit verbunden wäre. Das Recht auf informationelle Selbstbestimmung hat Verfassungsrang, die Bürger in Deutschland erwarten auch nach den Ereignissen, dass diesem Recht so weitreichend wie möglich Geltung verschafft wird!“

Leider verhallten in der Phase die Warnungen der Datenschutzbeauftragten weitgehend ebenso wie die zur Besonnenheit mahnenden Worte des Bundespräsidenten Rau, der anlässlich der Eröffnung des NS-Dokumentationszentrums in Nürnberg darauf hinwies, dass „Terroristen erst dann gewinnen, wenn sie uns dazu bringen, unsere Grundwerte im Kampf gegen sie aufzugeben“.

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

Die Entwicklungsphase war Anfang des Berichtsjahres abgeschlossen, am 21. März 2001 fiel der Startschuss für einen eigenen Internet-Auftritt meiner Dienststelle. Die Homepage ist unter den Internetadressen www.datenschutz-bremen.de, www.datenschutz.bremen.de und www.bremen-datenschutz.de zu erreichen. Ich möchte damit allen Bürgerinnen und Bürgern eine Vielzahl von Informationen und Tipps zum Datenschutz zur Verfügung stellen und sie insbesondere befähigen, ihre Rechte zu erkennen und selbst wahrzunehmen. Gleichzeitig verbinde ich damit die Hoffnung, dass dieses Angebot den Nutzerinnen und Nutzern ein besseres Verständnis für den Datenschutz ermöglicht.

Auf der Startseite befindet sich eine Kurzbeschreibung meiner Aufgaben sowie die Rubrik „Aktuelles“, wo u. a. die neuesten Mitteilungen und Presseerklärungen abgerufen werden können. Unter „Tipps für Bürger“ biete ich einen Online-Computer-Selbsttest an und weise auf die Broschüren hin, die bei meiner Dienststelle bestellt werden können. Wichtiger Bestandteil der Tipps ist ein Datenschutzscheckheft, in dem die Nutzerinnen und Nutzer Formschreiben vor-

finden, um schriftlich ihre Auskunfts-, Sperrungs- und Löschungsansprüche gegenüber Behörden des Landes und der Stadtgemeinden Bremen und Bremerhaven sowie nicht öffentlichen Stellen wahrzunehmen. Die Rubrik „Veröffentlichungen“ enthält meine Presseerklärungen sowie die Beschlüsse der Konferenzen der Datenschutzbeauftragten des Bundes und der Länder. Unter „Gesetzestexte“ stehen alle landesgesetzlichen Vorschriften zum Datenschutz im Lande Bremen zur Verfügung. Außerdem enthält der Internet-Auftritt Informationen über den Datenschutzausschuss der Bürgerschaft (Landtag), in dem die Ausschussmitglieder aufgelistet und die Termine und Themen der Ausschusssitzungen bekannt gegeben werden.

Das in erster Linie an den Interessen des Bürgers ausgerichtete Informationsangebot ist gut angenommen worden; das machen die vielen Nachfragen und Bestätigungen von Bürgern, die mich per Telefon oder E-Mail erreichten, deutlich. Wenn sich somit schon das bisherige Angebot gelohnt hat, bin ich gleichwohl bestrebt, mein Internetangebot aktuell zu halten und weiter zu komplettieren. Allerdings ist auch festzustellen, dass das Ziel, wenigstens ein Sachthema monatlich neu aufzunehmen, angesichts der oft zeitlich drängenden anderen Geschäfte eine eiserne Disziplin verlangt. Auch die Pflege des Angebots verbraucht mehr Kapazitäten als erwartet. Sie steigt natürlich proportional mit dem Umfang des Angebots, andererseits erhoffe ich mir durch die allmählich eintretende Routine mit dem Medium einen Zeitgewinn. Der eigentliche Gewinn des Angebots, das zugleich eine Entlastung meiner Dienststelle bringen soll, nämlich durch die vorgezeichneten Möglichkeiten die Bürger selbst zur eigenen Rechtewahrnehmung zu befähigen und zu motivieren, ist natürlich nicht messbar. Insgesamt bin ich aber mit der Resonanz des Internet-Auftritts sehr zufrieden, zumal meine Homepage im vergangenen Jahr monatlich bis zu 2243 mal besucht worden ist.

1.3. Gründung der „datenschutz nord GmbH“

Am Anfang stand die Idee, die vielen Beratungsleistungen des Landesbeauftragten für den Datenschutz, die nicht zu seinen gesetzlichen Aufgaben zählen und die er insbesondere gegenüber der Privatwirtschaft als Aufsichtsbehörde bisher unentgeltlich erbracht hatte, kostenpflichtig zur Verfügung zu stellen. Nach Beratungen mit verschiedenen Stellen der Senatsverwaltung wurde jedoch deutlich, dass der Landesbeauftragte für den Datenschutz als Kontrollinstanz unabhängig bleiben muss und daher nicht gleichzeitig kostenpflichtige DV-Beratung durchführen kann, die er nachher als Datenschutzaufsichtsbehörde oder als Landesbeauftragter für den Datenschutz kontrollieren soll. Um den Datenschutz trotz der finanziellen Engpässe im Lande Bremen zu verbessern, beschloss der Senat, eine GmbH zu gründen.

Die „datenschutz nord GmbH“ ist im April 2001 als Landesgesellschaft der Freien Hansestadt Bremen mit Sitz in Bremerhaven gegründet worden. Dieser Standort wurde bewusst mit dem Ziel ausgewählt, Bremerhaven in Kooperation mit meiner Dienststelle, die ebenfalls in Bremerhaven ihren Sitz hat, diesen zu einem über die Landesgrenzen hinaus bekannten und kompetenten Datenschutz-Standort auszubauen.

Die „datenschutz nord GmbH“ hat bislang zahlreiche Projekte durchgeführt, die unter www.datenschutz-nord.de abrufbar sind. Sie bietet sowohl privaten Unternehmen als auch öffentlichen Stellen folgendes Dienstleistungsangebot an:

— Erstellung von Datenschutz- und Sicherheitskonzepten,

— Beratung und praktische Unterstützung von betrieblichen und Konzern-Datenschutzbeauftragten,

— Beratung und Unterstützung von Mitarbeitervertretungen,

— Datenschutz-Auditing,

— Beratung in Multimedia-Fragen,

— Evaluierung der Sicherheitsmaßnahmen,

— Evaluierung von SAP-Systemen,

— Fortbildungsveranstaltungen.

Durch einen Kooperationsvertrag zwischen der „datenschutz nord GmbH“ und dem Landesbeauftragten für den Datenschutz sollen Synergieeffekte erreicht werden. Dabei ist sichergestellt, dass die Aufgabenfelder der Vertragspartner klar abgegrenzt sind. Zur Vermeidung von Konflikten ist ein Konsultationsverfahren verabredet worden. Für die gesetzlichen Aufgaben des Landesbeauftragten für den Datenschutz im öffentlichen und nicht öffentlichen Bereich ist dadurch die notwendige Unabhängigkeit gewährleistet.

1.4. Zur Situation der Dienststelle

Die technischen Voraussetzungen in der Dienststelle für eine effektive Arbeitserledigung haben sich im letzten Jahr noch einmal entscheidend verbessert. Zur Erinnerung: Noch in 2000 hatte ich endlich erreicht, dass das Hausnetz in Betrieb ging. Im Berichtsjahr wurde nun der Anschluss meiner Dienststelle an das Bremer Verwaltungsnetz über eine Standleitung realisiert. Im Laufe des Jahres ist es gelungen, alle Arbeitsplätze hier an das Bremer Verwaltungsnetz anzuschließen und an jedem Arbeitsplatz die E-Mail-Nutzung zu ermöglichen. Eine E-Mail-Richtlinie wurde nach Abstimmung mit dem Personalrat in Kraft gesetzt. Das neue Medium ist sehr schnell von allen Beschäftigten der Dienststelle angenommen worden und hat zu einer erheblichen Leistungssteigerung beigetragen.

Noch in 2001 ist mit der Vorbereitung der Web-Nutzung an allen Arbeitsplätzen der Dienststelle begonnen worden. Um zu verhindern, dass trotz Einsatz von Virenscannern verdeckte Programmfunktionen aus dem Internet geladen und am Arbeitsplatz ausgeführt werden, erfolgt der Internetzugriff über einen Terminalserver (zum Prinzip vgl. 22. JB, Ziff. 3.4.4.). Die zugehörige Nutzungsrichtlinie wurde parallel dazu erarbeitet und befindet sich in der Abstimmung. Da die notwendigen Tests bereits abgeschlossen sind, gehe ich davon aus, dass schon bei Vorlage des Berichts auch diese Anwendung in vollem Umfang in Betrieb sein wird.

Hervorheben möchte ich, dass alle hierfür notwendigen technischen Arbeiten von der Planung bis zur Umsetzung ohne Fremdhilfe vom Technikreferat der Dienststelle selbst erledigt wurden.

Bedingt durch die von allen Seiten zunehmende Nutzung des elektronischen Postversandes per E-Mail sind weitere Strukturveränderungen in der Dienststelle in Angriff zu nehmen. Im Anhang einer E-Mail befinden sich oft große Dokumente, deren Umfang bei Verfahrensbeschreibungen schon einmal leicht den Umfang von tausend Seiten oder mehr annehmen kann. Wenn dann innerhalb eines Beratungsprozesses noch verschiedene weiterentwickelte Versionen solcher Dokumente entstehen, nimmt ein solcher Vorgang oft einen Umfang an, der eine herkömmliche Geschäftsstelle und die Registratur schnell an den Rand des Leistbaren bringt. Davon einmal abgesehen, dass allein wegen des enormen Papierverbrauchs es nicht ratsam ist, solche Dokumente auszudrucken, müssen sie aber zur Dokumentation der Arbeitsergebnisse und oft zu der darauf fußenden Vereinbarungen mit Datenverarbeitern archiviert werden.

Hinzu tritt, dass die Registratur der Dienststelle, die vor über zwanzig Jahren konzipiert wurde und bisher nur in wenigen Facetten eine Änderung erfahren hat, nicht mehr anpassungsfähig ist und daher neu entwickelt werden muss. Die „Trauben“, die sich mittlerweile innerhalb des Aktenplanes gebildet haben, sind ohne eine neue Struktur nicht auflösbar.

Ich habe daher im Hause eine Arbeitsgruppe einberufen, die die Einführung eines neuen Dokumentenverwaltungssystems vorbereiten soll. Dabei sollen mehrere Ziele gleichzeitig verfolgt werden:

— Ein offenes Aktenzeichensystem, das auch noch in vielen Jahren die Integration neuer Themen unter rechtlichen und technischen Aspekten ermöglicht.

— Ein System, das die Elemente Postein- und -ausgang und den Verbleib, die Erledigung bis hin zur Archivierung und Vernichtung der Akten bzw. Löschung der Dateien verbindet.

— Eine elektronische und eine herkömmliche Aktenverwaltung sollen ermöglicht werden.

— Ein intelligentes Recherchesystem soll damit verbunden sein.

Ein Projekt, das natürlich erneut erhebliche Arbeitskapazitäten im Hause bindet, die dringend für die Erledigung der gesetzlichen Aufgaben benötigt werden. Um so erfreulicher die Motivation aller Beteiligten, sich weit über das normale Maß zu engagieren! Aber zum einen haben in der Dienststelle alle erkannt, dass es mit dem alten System nicht mehr weiter gehen kann, zum anderen, dass es keine den Anforderungen adäquate Lösung der Probleme geben kann, wenn nur jemand von außen mit deren Lösung beauftragt würde. Über den Fortgang werde ich weiter berichten.

Auch personell hat es in der Dienststelle im Berichtsjahr einige Veränderungen gegeben. Bedingt durch die Gründung der „datenschutz nord GmbH“ mussten personelle Kapazitäten aus dem Technikreferat, die dorthin abgegeben wurden, neu aufgefüllt werden. Hinzu kamen ein Weggang in die Privatwirtschaft und eine vorübergehende Beurlaubung, für die Ersatz gefunden werden musste. Hinzugewinnen konnte ich im Rahmen einer von mir mitfinanzierten Abordnung ab Dezember 2001 einen Lehrer, der bei mir ein Datenschutzprojekt für „Schüler am Internet“ entwickelt. Gerade in der jungen Generation herrscht in besonderem Maße Unsicherheit und Unwissen über das „sichere Surfen“ im Internet. Eine weitere geplante Abordnung aus dem Innenressort konnte wegen der Ereignisse des 11. Septembers leider nicht realisiert werden. Die Zielzahlen des PEP sind erreicht.

1.5. Datenschutz in der öffentlichen Meinung

Als ein Barometer für das, was die Öffentlichkeit im Lande an Datenschutzthemen interessiert, kann die Berichterstattung der regionalen Presse gewertet werden. Ich habe mich daher entschlossen, erstmals eine Auswahl von Berichten in Tageszeitungen und Zeitschriften, die im Jahr 2001 im Land Bremen erschienen sind, im Anhang dieses Berichts zu veröffentlichen (Ziff. 17.1. des Berichts). Dazu kommen natürlich weitere Berichterstattungen und Interviews in Funk und Fernsehen. Eine Aufbereitung der bundesweiten Datenschutzberichterstattung würde bei weitem den Rahmen sprengen.

Erneut erschreckende Ergebnisse kamen mit der im Sommer 2001 vorgestellten Meinungsumfrage zu Tage, die die B·A·T Freizeit-Forschungsinstitut GmbH unter dem Titel „Der gläserne Konsument — Die Zukunft von Datenschutz und Privatsphäre in einer vernetzten Welt“ veröffentlichte.

Immer mehr private Daten gehen um die Welt. Nichts gilt mehr als sicher, weil jeder PC-Nutzer Spuren im Internet hinterlässt. Ob Homebanking oder Onlineshopping — der gläserne Mensch droht Wirklichkeit zu werden. Die missbräuchliche Verwendung personenbezogener Daten bei Kauf- oder Bankgeschäften ist jederzeit möglich. Die Unsicherheit im Umgang mit den eigenen Daten entwickelt sich zum größten Hindernis für die Verwirklichung der politischen Forderung „Internet für alle“. Mehr als zwei von fünf Bundesbürgern (45 %), die beruflich oder privat einen Computer nutzen, „verzichten“ freiwillig auf das Surfen im Internet, um Datensicherheitsmängeln aus dem Wege zu gehen. Und nur jeder vierte PC-Nutzer (25 %) fühlt sich richtig darüber informiert, wie er die eigenen Daten wirksam schützen kann. Auch über den Stand der Verbreitung von PC und Internet enthält die Studie interessante Zahlen.

Noch nie war der Zugriff auf die ganz persönlichen Daten des Bürgers so einfach wie heute. Das elektronische Netz ist zur größten Datensammelmaschine der Welt geworden. Es enthält Verbraucherdaten von der Kleidergröße bis zur Bestsellerliste genauso wie Finanzdaten vom Bankauszug bis zur Steuererklärung (vgl. Ziff. 11.4. dieses Berichts).

Ein vernichtendes Zeugnis stellen die Bundesbürger dem Adresshandel aus: Nur acht von hundert Befragten trauen dem Adresshandel eine richtige Verwendung der persönlichen Daten zu. Die meisten befürchten eher persönliche Nachteile bzw. eine Beeinträchtigung ihrer Privatsphäre. Ähnlich kritisch stehen die Men-

schen heute dem Versandhandel und den Internetanbietern gegenüber. Nur jeder zehnte Bundesbürger ist von der Zuverlässigkeit dieser beiden Branchen überzeugt.

Auf die Frage: „Wie Sie wissen, gibt es Datenschutzgesetze, die sicherstellen sollen, dass Daten aus Ihrem privaten oder beruflichen Leben nicht in falsche Hände geraten... Sind Sie der Meinung, dass der Datenschutz a) mehr Bedeutung, b) weniger Bedeutung, c) gleiche Bedeutung wie bisher haben sollte", verteilten sich in Bremen die Antworten im Verhältnis von 74 % zu 0 % zu 24 %; 2 % machten keine Angaben. Die Bremer Bürger argwöhnten nach der Studie insbesondere Auskunfteien, dem Einzel-, Versand- und dem Internethandel.

1.6. Informationszugangsgesetz

Ende 2000 hat mir der Senator für Finanzen einen Arbeitsentwurf zu einem Informationszugangsgesetz vorgelegt. Nach § 1 des Entwurfs soll Zweck dieses Gesetzes sein, den freien Zugang zu den bei den öffentlichen Stellen vorhandenen Informationen sowie deren Verbreitung zu gewährleisten und die grundlegenden Voraussetzungen festzulegen, unter denen derartige Informationen zugänglich gemacht werden sollen. Hierzu habe ich eine Stellungnahme abgegeben.

Die Bürgerschaftsfraktion Bündnis 90/Die Grünen hat dann im Sommer 2001 einen eigenen Entwurf eines Informationsfreiheitsgesetzes als Antrag in die Bürgerschaft (Landtag) eingebracht (Bürgerschafts-Drs. 15/768 vom 4. Juli 2001). Der Entwurf ist u. a. dem Datenschutzausschuss zur Beratung überwiesen worden.

Informationszugangsgesetze gibt es bereits in den Ländern Brandenburg, Berlin, Nordrhein-Westfalen und Schleswig-Holstein. Im Bund gibt es nach Angaben des Bundesinnenministeriums derzeit den Referentenentwurf eines Informationsfreiheitsgesetzes mit Stand vom 20. Dezember 2000, der jedoch noch nicht vom Bundeskabinett beschlossen worden ist und nach meinen Informationen nicht mehr vor Ende der Legislaturperiode des Bundestages beraten werden wird.

Grundsätzlich unterstütze ich die Schaffung eines Informationsfreiheits- bzw. -zugangsgesetzes. Die Konferenz der Datenschutzbeauftragten hat im März 2001 eine Entschließung gefasst (vgl. Ziff. 15.4. dieses Berichts), in der betont wird, dass das Recht auf informationelle Selbstbestimmung des Einzelnen dem freien Zugang zu behördeninternen Informationen nicht entgegen steht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben.

Die in dem jeweiligen Gesetzentwurf verankerten neuen Aufgaben für den Landesbeauftragten für den Datenschutz werden jedoch nicht mit dem derzeitigen Personalbestand meiner Dienststelle zu leisten sein. Umfragen bei den jeweiligen Beauftragten in Berlin, Brandenburg, Nordrhein-Westfalen und Schleswig-Holstein haben ergeben, dass, übertragen auf Bremen, für die Aufgaben des bzw. der Landesbeauftragten für Akteneinsicht bzw. Informationszugang mindestens eine Stelle des höheren Dienstes erforderlich ist.

1.7. Stand der Novellierung des Bremischen Datenschutzgesetzes

Auch Bremen muss als eines der letzten Bundesländer sein Datenschutzrecht an die EU-Datenschutzrichtlinie anpassen. Ein besonderer Druck besteht aber nicht mehr, seit die EU-Kommission das Vertragsverletzungsverfahren gegen die Bundesrepublik eingestellt hat. Der Vorteil des langen Wartens liegt darin, dass das Landesrecht die im BDSG getroffenen Regelungen bei seiner Novellierung berücksichtigen kann und so in Terminologie, Regelungsinhalten und -tiefe eine weitgehende Homogenität mit dem Bundesgesetz erreicht werden kann.

Im Mai 2001 leitete mir der Senator für Justiz und Verfassung einen ersten Entwurf zur Anpassung des BrDSG zu, zu dem ich im Juni des letzten Jahres eine vorläufige Stellungnahme abgegeben habe. Der Entwurf wurde daraufhin im Justizressort überarbeitet und im Dezember den anderen senatorischen Ressorts zur Stellungnahme zugeleitet. Auch mir wurde noch einmal Gelegenheit gegeben, im Rahmen der Ressortabstimmung zu dem Referentenentwurf Stellung zu

nehmen. Ich habe in meiner Stellungnahme noch einige Änderungen vorgeschlagen, die u. a.

— sich unmittelbar aus der EU-Datenschutzrichtlinie ergeben,

— meine Kontrollrechte verbessern sollen,

— die Rechte des Parlaments stärken sollen,

— ein verbessertes Verfahren beim Einsatz der Videoüberwachung vorsehen,

— die verpflichtende Bestellung eines behördlichen Datenschutzbeauftragten vorsehen und

— ein Datenschutzaudit für Produkte und Verfahren ermöglichen sollen.

Ich habe in diesem Zusammenhang darauf hingewiesen, dass das Land Bremen in der Vergangenheit in vielen Bereichen des Datenschutzes eine Vorreiterrolle eingenommen hat; erinnert sei hier neben dem Bremischen Datenschutzgesetz auch an das Polizeigesetz und das Verfassungsschutzgesetz des Landes. Nicht von der EU-Datenschutzrichtlinie gefordert, enthält der Gesetzentwurf Regelungen zum Einsatz von mobilen Datenverarbeitungsmedien und zur Videoüberwachung; Regelungen, die auch ins BDSG aufgenommen wurden, um der technischen Entwicklung und den damit verbundenen spezifischen Gefahren für das informationelle Selbstbestimmungsrecht zu begegnen.

Der Verfahrensstand sieht jetzt, Ende Januar 2002, wie folgt aus: Die beim Justizressort eingegangenen Stellungnahmen werden in den Entwurf eingearbeitet, bei Bedarf findet mit mir noch eine Schlussbesprechung statt, bevor der Entwurf dann dem Senat zur Beschlussfassung zugeleitet werden wird. Wenn alles glatt geht, besteht die Möglichkeit, dass das neue Bremische Datenschutzgesetz (BremDSG) noch vor der Sommerpause verabschiedet wird.

1.8. Geändertes Bundesdatenschutzgesetz in Kraft

1995 wurde die EU-Datenschutzrichtlinie (95/46/EG vom 24. Oktober 1995, Amtsblatt der EU Nr. L 281/31) verabschiedet, die einen einheitlichen Rahmen und einheitliche Standards für das Datenschutzniveau innerhalb der Staatengemeinschaft der EU festlegt. Ein Meilenstein in der Datenschutzgeschichte war mit der Richtlinie zur Harmonisierung des Datenschutzrechts in der Europäischen Gemeinschaft gelegt. In der Richtlinie ist für die Mitgliedsstaaten eine Umsetzungsfrist in nationales Recht vorgegeben. Diese Frist war bereits im Oktober 1998 abgelaufen. Gleichwohl hatten zu diesem Zeitpunkt weder der Bund noch die meisten Bundesländer ihre Datenschutzgesetze der Richtlinie angepasst. Es war in Brüssel von der Kommission gegen die Bundesrepublik bereits ein Vertragsverletzungsverfahren eingeleitet worden, als im Mai 2001 endlich das neue Bundesdatenschutzgesetz (BDSG) in Kraft trat.

Der wesentliche Schritt, der mit dem neuen BDSG verbunden ist, liegt in der Angleichung des Datenschutzrechts für den öffentlichen und nicht öffentlichen Bereich. Daneben sind eine Reihe von Neuerungen hervorzuheben, von denen ich stichpunktartig einige nennen will:

— einen erweiterten Geltungsbereich,

— verbesserte Regelungen für den grenzüberschreitenden Datenverkehr innerhalb der EU (vgl. §§ 4 b und c),

— die Änderung der Meldepflicht (vgl. §§ 4 d und e),

— die Pflicht zur Bestellung eines Beauftragten für den Datenschutz bei öffentlichen Stellen (sog. behördlicher Datenschutzbeauftragter) neben dem im bisherigen BDSG schon bekannten betrieblichen Datenschutzbeauftragten (vgl. § 4 f),

— mehr Transparenz gegenüber den Betroffenen durch erweiterte Benachrichtigungspflichten (vgl. §§ 19 a und 33),

— erweiterte Verarbeitungsbeschränkungen in Bezug auf

  — die besondere Art der Daten (vgl. § 3 Abs. 6),

  — die Übermittlung aus dem EU-Gebiet in Drittstaaten und

  — die Widerspruchsrechte der Betroffenen (vgl. §§ 20 Abs. 5 und 35 Abs. 5),

— eine erweiterte Datenschutzkontrolle durch die Aufsichtsbehörden (vgl. § 38),

— für jedermann einsehbare Verfahrensregister (vgl. § 4 g),

— Vorabkontrolle bei sensibler Datenverarbeitung (vgl. § 4 d) und

— die erweiterten Bußgeldtatbestände und Strafantragsrechte (vgl. §§ 43, 44).

Auf die mit dem neuen BDSG verbundene Mehrarbeit auch für meine Dienststelle habe ich bereits früher hingewiesen, eine Konkretisierung enthält dieser Bericht (vgl. Ziff. 14.5.). Nicht von der EU-Datenschutzrichtlinie angestoßen enthält das neue BDSG darüber hinaus Regelungen zum Datenschutzaudit (vgl. § 9 a), zur Videoüberwachung (vgl. § 6 b) und zum Einsatz von mobilen Datenverarbeitungsmedien, wie z. B. Chipkarten (vgl. § 6 c).

Durch die Europäische Datenschutzrichtlinie sind neben den staatlichen Stellen (Bund und Länder) auch die öffentlich-rechtlichen Kirchen zur Anpassung ihres Datenschutzrechts aufgefordert. Ich bin nicht für die Kontrolle des kirchlichen Datenschutzes zuständig, gleichwohl gibt es Kontakte. Aus Gesprächen mit kirchlichen Stellen ist mir bekannt, dass Rechtsetzungsaktivitäten durch die großen Kirchen aufgenommen wurden.

1.9. Ausblick

Auf Landesebene stehen die Beratungen zur Novellierung des Bremischen Datenschutzgesetzes im Vordergrund. Danach müssen auch die bereichsspezifischen Datenschutzregelungen des Landes auf einen Anpassungsbedarf an die EG-Datenschutz-Richtlinie hin überprüft werden. Auch die Befassung des Datenschutz- und des Medienausschusses der Bürgerschaft mit dem Recht auf Informationsfreiheit steht noch vor der Sommerpause an. Die Begleitung der Einführung des neuen Vorgangsbearbeitungssystems bei der Polizei wird erhebliche Kräfte binden. Das eigene Internetangebot soll um ein Sicherheitspaket für den Bürger ergänzt werden. Geplant sind auch Veranstaltungen mit Vertretern der Wirtschaft zu den neuen Datenschutzanforderungen, die sich aus dem BDSG ergeben. Der Prüfansatz von Internetangeboten wird weiter verfolgt werden. Schließlich strebe ich eine in etwa gleiche Verteilung der Prüftätigkeiten im öffentlichen und privaten Bereich an, was nur durch eine weitere Umverteilung von Arbeitskapazitäten möglich wird. In diesem Zusammenhang überlege ich die Erstellung einer Datenschutzprüflandkarte, die derzeit noch viele weiße Flecken hätte.

Auf Bundesebene sind vor der Bundestagswahl keine gravierenden Datenschutzinitiativen zu erwarten. Mit dem Abschluss der Arbeiten am BDSG wurde zu viel Zeit verbraucht, auch die Ereignisse des 11. September waren nicht vorhersehbar. Die noch im letzten Jahr von mir erwarteten Projekte der Bundesregierung zur Schaffung eines Arbeitnehmerdatenschutzgesetzes und die Umlegung der in dem Gutachten „Modernisierung des Datenschutzrechts“ genannten Ziele zur zweiten Stufe der Datenschutzgesetzgebung, das am 12. November 2001 dem Bundesministerium des Innern übergeben wurde, müssen noch warten.

2. Telekommunikation, Teledienste und Medien

Nachdem ich im letzten Jahr schwerpunktmässig in Bremen ansässige Internet-Provider geprüft habe, habe ich mich in diesem Jahr in erster Linie auf die Anbieter von Inhalten (Content-Anbieter) der Stadt Bremen konzentriert.

Als eine der bedeutendsten Internetseiten in Bremen habe ich das Stadtinformationssystem geprüft. Weitere Content-Anbieter wurden vorerst nur einer Online-Prüfung unterzogen. Weiterhin wurde die Hochschule Bremerhaven geprüft, die den Internetzugang sowohl für Studenten als auch zum Teil für die Bremerhavener Schulen zur Verfügung stellt.

2.1. Stadtinformationssystem Bremen (bremen.de)

Im Vergleich zum Stadtinformationssystem „bremerhaven.de“ (vgl. 23. JB, Ziff. 2.2.2.) ist „bremen.de“ weitgehend eine Auskunfts- und Informationsplattform für die Stadt Bremen. Es werden weder — wie in Bremerhaven — Postfächer noch Internetzugänge für Bremer Bürger angeboten. Dennoch wurden bei der Prüfung von „bremen.de“ ähnliche Probleme deutlich wie bei der letztjährigen Prüfung des Stadtinformationssystems „bremerhaven.de“:

Im Impressum wird nicht darauf hingewiesen, in welcher Weise personenbezogene Daten im Rahmen von „bremen.de“ gespeichert werden. Dies betrifft sowohl die Speicherung von IP-Adressen als auch Daten, die im Rahmen von Formularen erhoben werden. Ich habe den Senator für Finanzen als Verantwortlichen von „bremen.de“ aufgefordert, in einer so genannten Privacy Policy dem Internetbenutzer Informationen darüber zu geben, in welchem Umfang seine Daten im Rahmen von „bremen.de“ gespeichert und weiter verwendet werden.

Auf dem Web-Server werden sämtliche Zugriffe IP-Nummern bezogen protokolliert und zu statistischen Zwecken einen Monat aufbewahrt. Erst nach Ablauf des Monats werden die Daten gelöscht. Da die Speicherung von IP-Adressen gemäß § 6 TDDSG datenschutzrechtlich nicht zulässig ist, habe ich gefordert, hierauf zu verzichten und die IP-Adressen in den Protokolldatensätzen zu aggregieren. Eine Stellungnahme steht noch aus.

2.2. Weitere Content-Anbieter im Internet

Neben dem Stadtinformationssystem „bremen.de“ wurden im Berichtszeitraum eine repräsentative Anzahl weiterer Content-Anbieter (u. a. Banken, Verlage, Online-Shops) nach den Prüfkriterien Cookies, Pflichtfelder, Impressumspflicht, Zahlungsverfahren, SSL-Verschlüsselung und Privacy Policy einer Online-Prüfung unterzogen. Dabei wurde die folgende Situation vorgefunden:

Cookies: Von fünf der 24 geprüften Contentanbieter werden Cookies auf der Festplatte des Besuchers gespeichert. Diese Cookies werden in der Regel bei weiterem Aufrufen der Internetseite wieder ausgewertet, was dazu dienen könnte, Nutzungsprofile der Besucher zu erstellen. Zwei Content-Anbieter bedienen sich temporärer Session-Cookies, die nach Beenden der Verbindung wieder gelöscht werden und nicht auf der Festplatte des Nutzers erhalten bleiben. Nur ein Anbieter weist unter einer Rubrik „Datenschutz“ der AGB explizit darauf hin, dass Cookies eingesetzt werden.

Pflichtfelder: Häufig ist beim Ausfüllen von Online-Formularen zwecks Registrierung oder Bestellung nicht ersichtlich, ob es sich um Pflichtfelder handelt, die auszufüllen sind, da diese nicht, oder nur unzureichend gekennzeichnet sind. Bei fünf von 24 Anbietern ist bei Registrierung als Nutzer bzw. Kunde die Eingabe von Telefonnummer und E-Mail-Adresse nötig. Ein Anbieter weist bei der Anmeldung als Neukunde eine Rubrik „Kundeninfo“ als Pflichtfeld aus („Wodurch wurden Sie auf uns aufmerksam?“). Bei einem weiteren Anbieter muss bei der Anmeldung das Geburtsdatum angegeben werden.

Impressum: Auf den Internetseiten von sieben Anbietern existiert kein Impressum. Bei weiteren vier Anbietern ist zwar ein Impressum vorhanden; es wird jedoch lediglich die Firmenadresse aufgeführt und kein Verantwortlicher genannt. Bei weiteren sieben Anbietern ist ein Verantwortlicher allerdings ohne Adressangabe aufgeführt.

Zahlungsverfahren: Bei drei Content-Providern kann mit Kreditkarte (SET-Verfahren) gezahlt werden. Bei weiteren zwei Anbietern ist ausschließlich die Zahlung per Nachnahme und in einem Fall per Verrechnungsscheck vorgesehen. Als häufigstes Zahlungsverfahren ist die Zahlung per Bankeinzug oder wahlweise per Rechnung aufgeführt. Zahlungsverfahren wie Ecash, Cyber- oder Telecash wurden nicht vorgefunden.

SSL-Verschlüsselung: Von den Anbietern, die die Bezahlung der Leistung per Bankeinzug anbieten, übertragen sieben Content-Anbieter die Bankverbindungsdaten ihrer Kunden unverschlüsselt über das Internet. Elf Anbieter stellen den

Nutzern bei der Übermittlung weiterer personenbezogener Daten keine sichere Verbindung zur Verfügung.

Privacy policy: Nur drei von 24 Anbietern geben dem Nutzer Auskunft darüber, in welchem Umfang seine Daten (IP-Adresse) vom Content-Provider gespeichert werden. Ob und wann diese wieder gelöscht werden, wird dabei allerdings nicht mitgeteilt.

Die vorgefundene Situation zeigt, dass seitens der Content-Anbieter die gesetzlichen Grundlagen des Teledienste-Datenschutz-Gesetzes (TDDSG) den wenigsten bekannt sein dürften. Hinsichtlich der Umsetzung der gesetzlichen Vorlagen besteht bei den geprüften Inhaltsanbietern der Hansestadt Bremen erheblicher Nachholbedarf. Die Anbieter werden im laufenden Jahr von mir angeschrieben und über notwendige Verbesserungen ihres Internetangebots informiert. Weiterhin wird gezielt eine eingehendere Prüfung einzelner Anbieter erfolgen.

2.3. Rechenzentrum der Hochschule Bremerhaven

Das Rechenzentrum der Hochschule Bremerhaven (ZBRV) stellt sowohl den Studenten als auch den Mitarbeitern der Hochschule und den Instituten einen kostenlosen Internetzugang, ein Postfach auf dem Mail-Server sowie Kapazität auf ihrem Web-Server zur Verfügung. Einige Fachbereiche haben zusätzlich eigene Mail- und Web-Server im Einsatz.

Die Hochschule Bremerhaven ist über das Gigabit-Wissenschaftsnetz (G-WIN) des Deutschen Forschungsnetzes (DFN) an das Internet angeschlossen. Zur Absicherung der Web- und Mail-Server fungiert der äußere Router als Paketfilter. Bei einem von mir durchgeführten Online-Sicherheitscheck wurde deutlich, dass diese Maßnahme unzureichend ist, da die Kommunikationsserver der Hochschule zahlreiche Dienste zur Verfügung stellen, die internetweit verfügbar und somit potentiell Angriffen aus dem Internet ausgesetzt sind. Ich habe der Hochschule Bremerhaven empfohlen, die verfügbaren Ports auf ein Mindestmaß zu beschränken und geeignete Maßnahmen zu ergreifen, um die Sicherheit der Server zu erhöhen. Weiterhin habe ich die Hochschule Bremerhaven aufgefordert, ein Netz-Sicherheitskonzept zu erarbeiten.

Bei der Nutzung des Internetzugangs der Hochschule Bremerhaven wird durch den Web-Server die vollständige IP-Adresse des Nutzers protokolliert und gespeichert. Die Protokolldateien werden erst nach einem Zeitraum von drei Wochen gelöscht. Da diese Praxis § 6 TDDSG widerspricht und die Protokolle ohnehin nicht für Auswertungen oder Statistiken benötigt werden, habe ich die Hochschule Bremerhaven aufgefordert, vollständig auf die Protokollierung zu verzichten.

Studenten und Mitarbeiter der Hochschule haben auf Antrag die Möglichkeit, von Zuhause aus über das Hochschulnetz Zugang zum Internet zu erhalten. Darüber hinaus wird ein persönliches Postfach zur Verfügung gestellt. Die Zugangsvermittlung zum Internet erfolgt durch Anbindung der Studentenwohnheime via Festverbindung oder Einwahl über einen Einwahlrouter bei der Hochschule. Der Mail-Server ist so konfiguriert, dass sowohl Absender- als auch Empfänger-Adresse bzw. deren IP-Adressen gespeichert werden. Auch diese Art der Protokollierung ist gemäß § 85 Telekommunikationsgesetz (TKG) unzulässig, wonach nicht nur die Telekommunikation, sondern auch ihre näheren Umstände dem Fernmeldegeheimnis unterliegen. Dazu gehören auch die IP-Adresse des Absenders bzw. Empfängers.

Protokolliert wird auch die Vermittlung des Internetzugangs. Da dies ebenfalls einen Teledienst darstellt, dessen Protokollierung nicht durch das TDDSG abgedeckt ist, sollte auf die Protokollierung vollständig verzichtet werden oder der Benutzer mit dem Antrag zur Benutzung der Hochschulrechner bzw. der Infrastruktur der Hochschule in die Protokollierung einwilligen.

Die Einwilligung setzt jedoch eine umfassende Information des Betroffenen über den Gegenstand der Einwilligung voraus. Diese Information des Betroffenen sollte auf einer umfassenden Nutzerordnung basieren. Die Nutzerordnung des DFN, auf die im Antrag für eine E-Mail-Adresse bzw. einen Einwahlaccount für die Hochschule Bremerhaven verwiesen wird, ist in dieser Beziehung nicht ausreichend.

Ich habe die Hochschule Bremerhaven gebeten, entweder auf die Protokollierung des Internetzugangs zu verzichten oder eine hochschuleigene Benutzerordnung zu erstellen, in der ausreichend darauf hingewiesen wird, in welchem Umfang personenbezogene Daten zu welchem Zweck wie lange gespeichert werden.

2.4. Aufhebung der Rufnummernunterdrückung

Ich nehme regelmäßig an der „Arbeitsgemeinschaft Telekommunikation, Tele- und Mediendienste“ des Düsseldorfer Kreises teil. Dort wurde u. a. die Möglichkeit zur Aufhebung der Rufnummernunterdrückung in Call-Centern thematisiert.

In den modernen digitalen Telefonnetzen wie ISDN wird in der Regel die Rufnummer eines Anrufenden (A) an eine angerufene Person (B) übermittelt. Anrufende haben aber die Möglichkeit, gegenüber ihren Telefonpartnern anonym zu bleiben, indem sie an ihren Endgeräten die Rufnummerübermittlung unterdrücken oder ihren Netzbetreiber veranlassen, die Rufnummerübermittlung generell zu unterdrücken. Allerdings wird auch bei der Unterdrückung der Rufnummerübermittlung durch den Netzbetreiber die Rufnummer für den Verbindungsaufbau notwendigerweise an alle dazwischenliegenden Vermittlungsstellen übermittelt. Lediglich die letzte Vermittlungsstelle, die Teilnehmervermittlungsstelle des Angerufenen, signalisiert die Rufnummer von A nicht weiter zu übermitteln an B. Die Rufnummeranzeige wird also unterdrückt. Dies gilt für den Fall, dass der Angerufene über einen herkömmlichen ISDN-Anschluss an das Telefonnetz angebunden ist.

Ist der Angerufene jedoch selbst als Vermittlungsstelle an das öffentliche Telefonetz angebunden (z. B. bei bestimmten Call-Centern), so wird die Rufnummer bis dahin übermittelt und der Angerufene kann die Rufnummernunterdrückung eigenmächtig aufheben, ohne dass der Anrufer in irgendeiner Weise davon Kenntnis erlangt. Dieses Verfahren verstößt gegen das Recht auf informationelle Selbstbestimmung, da der Anrufer unwissentlich seinem Telefonpartner gegenüber mittelbar seine Identität preisgibt. Besonders problematisch wäre dies z. B. auch im Bereich der Telefonseelsorge oder anderer anonymer telefonischer Beratung. Ich werde diesem Sachverhalt daher auch bei Call-Centern im Land Bremen nachgehen.

3. Datenschutz durch Technikgestaltung und -bewertung

3.1 Richtlinie Elektronische Post der bremischen Verwaltung

Nach langer und intensiver Diskussion (vgl. auch 23. JB, Ziff. 3.1.2.) ist nunmehr die Richlinie für die Nutzung der elektronischen Post verabschiedet worden. Die Richtlinie berücksichtigt Vertretungsregelungen und private Nutzungsmöglichkeiten ebenso wie Verschlüsselungsmöglichkeiten und stellt somit ein richtungsweisendes Regelwerk zur datenschutzkonformen Nutzung des E-Mail-Dienstes in der bremischen Verwaltung dar.

3.2. Telearbeit

Der Zugriff auf Rechner innerhalb des bremischen Verwaltungsnetzes von Heimarbeitsplätzen aus ist in den letzten Jahren von der bremischen Verwaltung verstärkt nachgefragt worden (vgl. 20. JB, Ziff. 11.1. und 21. JB, Ziff. 8.1.). Angesichts des zunehmenden Bedarfs an Telearbeitsplätzen wurden im vergangenen Jahr vom Senator für Finanzen Pilotprojekte initiiert, die sowohl einen sicheren als auch datenschutzkonformen Zugang von Telearbeitsplätzen zu Verwaltungsrechnern ermöglichen sollen. Konzeptionell wurden die Projekte von Arbeitsgruppen begleitet, in denen auch Mitarbeiter meiner Dienststelle vertreten sind.

In zwei Pilotprojekten wurde zunächst der Zugang zum bremischen Verwaltungsnetz durch ein ISDN-Gateway der Bremer Kommunikationstechnik (BreKom) implementiert, das der Telearbeiter zunächst anwählt. Dieses Gateway authentisiert den ISDN-Anschlussinhaber anhand einer Liste berechtigter Teilnehmer und ruft den Telearbeiter zurück. Darüber hinaus wird der gesamte Datenverkehr durch Aufbau eines VPN-Tunnels verschlüsselt.

Im Verlauf der Pilotprojekte stellte sich jedoch heraus, dass die ursprünglich angestrebte ISDN-Lösung sehr kostspielig ist. Einwahlrouter müssen in ausreichender Kapazität bereitgehalten werden, damit nicht Anschlüsse besetzt sind. Außerdem fallen entfernungsabhängige Telefonkosten an. Dies ist besonders gravierend, wenn — wie beim geplanten Einsatz von Terminalservern — die Telearbeiter während ihrer gesamten Telearbeit online sind.

Als wirtschaftlichere Alternative soll demnächst in weiteren Pilotprojekten der ISDN-Zugang durch einen Internetzugang ersetzt werden. Da der Telearbeiter bei dieser Lösung nicht mehr durch die ISDN-Anschlusskennung authentisiert werden kann, erfolgt die Authentisierung über ein X.509 Zertifikat. Mit Hilfe dieses Zertifikats wird auch der gesamte Datenverkehr über das Internet mittels IPSEC verschlüsselt. Die Authentisierung des Telearbeiters gegenüber den Servern wird zusätzlich wie bisher über Nutzerkennung und Passwort durchgeführt.

Der Zugang von Telearbeitern auf das bremische Verwaltungsnetz per Internet wird in zwei Schritten realisiert. Zunächst sollen für den Zugriff von außen nur ein zentrales dienstliches Postfach auf einem Mail-Server bei der Brekom oder feste Routen zu Terminalservern freigegeben werden. Terminalserver ermöglichen den visuellen Zugriff auf Client-Server-Verfahren bzw. auf Dokumente, ohne direkt auf die Verfahren bzw. Dokumente zugreifen zu müssen. Der direkte Zugriff der Telearbeit auf Verfahrens- bzw. Dokumenten-Server der jeweiligen Dienststellen wird erst umgesetzt, wenn positive Erfahrungen hinsichtlich des Zugangs zum Mail-Server vorliegen. Die Evaluierung der Pilotprojekte wird meine Dienststelle weiterhin zeitnah und praxisgerecht begleiten.

3.3. Fernzugriff für Führungskräfte

Beim Senator für Finanzen wurde im Juni des Berichtsjahres ein Pilotprojekt mit dem Titel „Mobile Arbeitsgestaltung bei Führungskräften“ initiiert. Es soll ermöglicht werden, sich von fest vereinbarten externen Standorten in das lokale Netz des Senators für Finanzen einzuwählen. Dabei soll ein Zugriff auf E-Mail, Dokumente und ggf. auf Datenbanken möglich sein. In einer zweiten Phase soll die Einwahlmöglichkeit auf wechselnde Standorte erweitert werden. Ein Einwählen in das lokale Netz wäre dann beispielsweise auch auf Dienstreisen möglich. Zielgruppe sind Abteilungs- und Referatsleiter. Neben einem permanenten Zugriff bei der Telearbeit (vgl. Ziff. 3.2. dieses Berichts) ist der „gelegentliche Zugriff“ eine zusätzliche Variante der externen Einwahl in das bremische Verwaltungsnetz.

Ich habe die Konzeptionierungsphase des Pilotprojektes begleitet mit dem Ziel, das gleiche Sicherheitsniveau, das bereits für die Einrichtung von Telearbeitsplätzen mit mir abgestimmt worden ist, zu erreichen. Das bedeutet im konkreten Fall folgendes:

Die an dem Pilotprojekt teilnehmenden Personen bestätigen schriftlich, mit ihrem Benutzerkonto (Steuerung des internen Zugriffs) keine personenbezogenen Daten abrufen und verarbeiten zu können. Für den Fall, dass solche Daten im Zugriff sind, wird für den externen Zugang ein zweiter Account vergeben, der diesen Zugriff nicht mehr ermöglicht.

Es wird ein Terminalserver unter Windows 2000 im Anwendungsmodus eingesetzt. Der Server ist in das Netz des Senators für Finanzen integriert und ermöglicht den Zugriff auf Windows-basierte Anwendungen. Sämtliche Anwendungskomponenten laufen auf dem Server. Die Clients haben nur Basisfunktionalität, d. h. sie dienen der grafischen Darstellung der Anwendungen und steuern die Interaktion des Benutzers mit dem Terminalserver über Tastatur und Maus.

Der Zugang zum Terminalserver ist nur über eine zweistufige Authentifizierung möglich. Es ist ein Call-Back-Verfahren auf ISDN-Ebene eingerichtet (feste ISDN-Verbindung). Es wird eine verschlüsselte Verbindung aufgebaut. Der Benutzer authentifiziert sich mit Namen und Passwort am System. Der Online-Zugriff ist nur über den Terminalserver möglich.

Eine Fülle von weiteren technischen Maßnahmen, wie etwa auf der Systemebene die Protokollierung der Einwahl, die Beschränkung von Zugriffen, die Beschrän-

kung des Befehlsumfangs etc. (Festlegung über Sicherheitsrichtlinien) oder die ausschließliche Freischaltung Citrix-entsprechender Ports, der Einsatz eines Packetfilters (IP-Filterung) sowie die Sperrung lokaler Laufwerke sichern die Kommunikation und Zugriffe zusätzlich ab.

Die Evaluierung dieses Projektes wird von meiner Dienststelle weiterhin kontinuierlich begleitet. Ziel ist es, über technische und organisatorische Maßnahmen sicherzustellen, dass durch den authorisierten Zugriff der Mitarbeiter/-innen keine personenbezogenen Daten exportiert werden und kein unauthorisierter Zugriff auf das Netz des Senators für Finanzen erfolgen kann, d. h., dass das Schutzniveau für die dort verarbeiteten personenbezogenen Daten bei der Bereitstellung externer Zugriffsmöglichkeiten erhalten bleibt.

3.4. MEDIA@Komm-Projekt

Bereits in den letzten beiden Jahren habe ich ausführlich über das bremische MEDIA@Komm-Projekt berichtet (22. JB, Ziff. 3.1. und 23. JB, Ziff. 3.4.). Inzwischen können zahlreiche Geschäftsvorfälle sowohl von den Bürgern als auch von den Unternehmen rechtsverbindlich auf der Basis elektronischer Signaturen ohne Medienbruch über das Internet abgerufen werden. Hierzu gehören der eingeschränkte Lesezugriff auf eine Kopie des Handelsregisters ebenso wie die Möglichkeit, sich Familienstandsurkunden vom Standesamt zuschicken zu lassen bzw. Nachsendeanträge bei der Deutschen Post zu stellen. Ebenso können Anwälte über den Bremer-Online-Service elektronisch Mahnbescheidanträge an das zuständige Mahngericht verschicken.

Anders als ursprünglich geplant werden zahlreiche Internet-Dienstleistungen auch ohne Einsatz einer qualifizierten elektronischen Signatur angeboten. Qualifizierte Signaturen gemäß Signaturgesetz werden nur bei solchen Geschäftsvorfällen verwendet, bei denen eine Schriftform zwingend erforderlich ist. Erfolgt die Kommunikation zwischen Bürger und Verwaltung formfrei, kann der Bürger zwischen einfacher, fortgeschrittener und qualifizierter Signatur auswählen.

Das elektronische Signieren und Verschlüsseln von Dokumenten sowie das Entschlüsseln und Verifizieren der Signaturen erfolgt beim Bremer-Online-Service über das Protokoll OSCI (Online Services Computer Interface Standard); ein entsprechender OSCI-Server ist seit Herbst letzten Jahres im Einsatz.

Datenschutz und Datensicherheitsaspekte sind bei der Konzeption des Protokolls sowie der Plattform frühzeitig berücksichtigt worden. Für das OSCI-Protokoll existiert ein umfangreiches OSCI-Sicherheitskonzept, das auf die einzelnen Sicherheitsmechanismen der OSCI-Plattform ausführlich eingeht. Für den OSCI-Server wurde ein Betriebskonzept erstellt und auch umgesetzt, das sowohl räumliche, gebäudespezifische als auch administrative Sicherheitsmaßnahmen beschreibt und Ergebnisse einer in Auftrag gegebenen Serverattacke berücksichtigt. Darüber hinaus ist der Bremer-Online-Service konform zum Teledienstedatenschutz entwickelt worden.

3.5. Web.Punkte

Der Senator für Bildung und Wissenschaft hat zusammen mit der Deutschen Telekom AG ein Kooperationsprojekt gestartet, um der Gefahr der Aufspaltung der Bevölkerung in „Teilnehmer und Nicht-Teilnehmer am Informationszeitalter“, dem so genannten digital divide, entgegenzutreten. Maximal 30 weiterführende Schulen in Bremen und Bremerhaven wurden zu diesem Zweck mit Internet-Cafés ausgestattet. Diese besonderen Internet-Cafés werden als „Web.Punkte“ bezeichnet. Die Cafés werden zur Unterrichtszeit am Vormittag für schulische Zwekke genutzt, nachmittags stehen die „Web.Punkte“ für schulexterne Personen und Institutionen zur Nutzung zur Verfügung. Damit soll die Möglichkeit geschaffen werden, interessierten potentiellen Nutzern einen betreuten Zugang zum Internet zur Verfügung zu stellen.

Im Zusammenhang mit einer von mir durchgeführten Schulprüfung habe ich auch einen „Web.Punkt“ geprüft. Dabei fiel positiv auf, dass eine (öffentliche aushängende) Nutzerordnung existierte, die von allen Nutzern zur Kenntnis genommen werden muss und deren Anerkennung und Einhaltung durch Unterschrift bestä-

tigt werden muss. In der Nutzerordnung sind auch Hinweise auf mögliche rechtliche Konsequenzen enthalten, die durch eine rechtswidrige Nutzung entstehen können. Weiterhin positiv ist, dass ein hohes Maß an Sicherheit im Hinblick auf die unerlaubte Manipulation (bis hin zur Nicht-Benutzbarkeit) der Rechner implementiert worden ist. Die Rechner werden bei Neustart immer im Urzustand gestartet. Einstellungen etc., die während der vorhergehenden Nutzung getätigt worden sind, gehen verloren.

Die Benutzer erhalten keine individuellen Kennungen (Accounts) für die Nutzung des „Web.Punktes", sondern arbeitsplatzbezogene Kennungen. Für einen begrenzten Zeitraum wird schriftlich festgehalten, welcher Nutzer an welchem Arbeitsplatz gesessen hat.

Zu bemängeln ist, dass die so genannten Home-Directories, die den Nutzern für Downloads aus dem Internet zur Verfügung gestellt werden, nicht ausreichend gegeneinander abgeschottet werden. Eine unzulässige Einsichtnahme durch Nutzer innerhalb des „Web.Punktes" ist möglich. Zudem ist es möglich, sich unter einem Account, der zu einem bestimmten Arbeitsplatz gehört, an einem anderen Arbeitsplatz anzumelden. Dies kann auch zeitgleich geschehen. Damit wäre es sehr einfach möglich, z. B. auszuspähen, welche Inhalte ein Nutzer an einem bestimmten Platz aus dem Internet herunterlädt. Ich habe daraufhin die für die Konfiguration der „Web.Punkte" verantwortliche Stelle (S3-Team der Universität) aufgefordert, die Einstellungen der Rechner der „Web.Punkte" dahingehend zu ändern, dass eine Abschottung der Accounts untereinander erreicht wird und eine zeitgleiche Anmeldung unter einem Account an zwei verschiedenen Rechnern nicht möglich ist.

Derzeit befinde ich mich in Abstimmung mit dem S3-Team bzw. der Forschungsgruppe Telekommunikation der Universität, um die Konfiguration der „Web.Punkte" entsprechend anzupassen.

4. Bürgerschaft — Die Arbeit des Datenschutzausschusses

4.1. Ergebnisse der Beratung des 23. Jahresberichts

Bericht und Antrag des Datenschutzausschusses vom 22. Februar 2002 (Drs. 15/1080) zum 23. Jahresbericht des Landesbeauftragten für den Datenschutz (Drs. 15/681 vom 30. März 2001) und zur Stellungnahme des Senats vom 9. Oktober 2001 (Drs. 15/852)

Bericht

Die Bürgerschaft (Landtag) hat in ihrer Sitzung am 16. Mai 2001 den 23. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung am 24. Oktober 2001 die Stellungnahme des Senats zur Beratung und Berichterstattung an den Datenschutzausschuss überwiesen.

Der Ausschuss hat bei der Behandlung des Jahresberichts und der Stellungnahme des Senats den Landesbeauftragten für den Datenschutz und Vertreter der betroffenen Ressorts angehört. Daraus hat sich unter anderem ergeben, dass bei der Planung und Weiterentwicklung von DV-Verfahren datenschutzrechtliche Aspekte häufig nicht ausreichend berücksichtigt werden.

Ferner wurden die vom Landesbeauftragten für den Datenschutz festgestellten Mängel auch nach Aufforderung durch den Datenschutzausschuss in einigen Fällen nicht in angemessener Zeit abgestellt. Der Datenschutzausschuss verweist auf seine weiteren Ausführungen.

Der Datenschutzausschuss fordert den Senat auf, künftig die jeweiligen Datenschutzkonzepte zeitgleich mit der DV-Entwicklung zu erstellen und, soweit es Kritik des Landesbeauftragten für den Datenschutz gibt, in angemessener Zeit Abhilfe zu schaffen.

Personalabrechnungsverfahren KIDICAP 2000 (Tz. 5.1): Der Landesbeauftragte für den Datenschutz hat in seinem 20. Jahresbericht unter Ziff. 11.5. über die Einführung eines neuen Bezügeabrechnungsverfahrens berichtet und im 21. Jahres-

bericht unter Ziff. 8.4. darüber informiert, dass ein mit ihm abgestimmtes Datenschutzkonzept vorliegt. Im Berichtszeitraum des 23. Jahresberichtes wurde die Umsetzung der im Datenschutzkonzept genannten technischen und organisatorischen Maßnahmen, die auf KIDICAP 2000 zugreifenden Organisationseinheiten sowie die sonstigen technischen Maßnahmen geprüft. Die Überprüfung der Umsetzung der am 15. März 2000 durch den Senator für Finanzen bekannt gegebenen und verbindlich erklärten Richtlinie für Einzelplätze, Server und lokale Netzwerke hat ergeben, dass im Berichtszeitraum die Virenschutzsoftware noch nicht auf dem Server implementiert war. Ferner befanden sich Protokolldaten, die älter als 180 Tage waren, seit 1998 im System. Der Datenschutzbeauftragte hat empfohlen, die Protokolldaten in regelmäßigen Abständen manuell zu löschen.

Der Landesbeauftragte hält die Aktualisierung des Datenschutzkonzeptes für das Fachverfahren KIDICAP 2000 in Bezug auf „Fehlerbereinigung“ und „Lesezugriffe der Abschnittsleitung“ für geboten. Das Datenschutzkonzept sieht die Sperrung der offenen Diskettenlaufwerke der Clients, auf denen personenbezogene Daten verarbeitet werden, oder die Bereitstellung einer Verschlüsselungssoftware für freiverwendbare Diskettenlaufwerke vor. Zum Prüfzeitpunkt fand eine Software-Evaluation für ein geeignetes kostengünstiges Produkt statt. Der genaue Zeitpunkt der Einführung der Verschlüsselungssoftware war noch offen.

Der Landesbeauftragte hat in seinem Prüfbericht darauf hingewiesen, dass Performa Nord als speichernde Stelle für die fristgerechte Löschung der Protokolldaten verantwortlich ist. Die Umsetzung der NT-Security-Guideline war zum Prüfzeitpunkt noch nicht abgeschlossen.

In seiner Stellungnahme zum 23. Jahresbericht hat der Senat erklärt, bis auf den Einsatz einer Verschlüsselungssoftware seien alle festgestellten Mängel inzwischen beseitigt worden. In der Sitzung des Datenschutzausschusses am 16. Januar 2002 erklärte ein Vertreter des Senators für Finanzen, dass inzwischen die fehlende Verschlüsselungssoftware nunmehr implementiert worden sei. Es handele sich hierbei um das Produkt PGP („pretty good privacy“).

Der Datenschutzausschuss stellt fest, dass alle in der Prüfung des Landesbeauftragten für den Datenschutz festgestellten Mängel beseitigt sind.

Prüfung des DNA-Analyseverfahrens (Tz. 6.1.1): War die Polizei früher auf Tatortspuren wie Fingerabdrücke angewiesen, hat sie mit der Entwicklung des Genomanalyseverfahrens die Möglichkeit, biologisches Material vom Tatort mit dem von Tätern und Tatverdächtigen zu vergleichen. Im März 1997 wurde die hierfür erforderliche gesetzliche Regelung zum DNA-Analyseverfahren verabschiedet. Anfang 1998 richtete das Bundeskriminalamt eine Zentraldatei für DNA-Spuren ein.

Drei Jahre nach in Kraft treten des Gesetzes hat der Landesbeauftragte für den Datenschutz bei der Polizei und Staatsanwaltschaft in Bremen eine Querschnittsprüfung des DNA-Analyseverfahrens durchgeführt. Eine allgemein verbindliche Prüfaussage konnte er nicht treffen, weil die Fallzahlen noch zu klein waren, denn von den zur Erstellung von Täterprognosen nach Bremen übermittelten 10.000 Personendatensätzen waren bislang lediglich 319 ausgewertet worden. Eine CD-ROM mit 2.000 Personendatensätzen wurde wegen fehlender Mittel zur Beschaffung einer Standardsoftware ebenfalls nicht ausgewertet.

Der Landesbeauftragte für den Datenschutz bemängelte, dass keine festen Verfahrensstrukturen existierten, die den Vorgaben des Bundesverfassungsgerichts Rechnung tragen. In der Praxis werden den Betroffenen auch dann Einwilligungserklärungen vorgelegt, wenn das Gesetz vor der DNA-Analyse eine richterliche Einzelfallentscheidung vorsieht. Auch die gesetzlich geregelte Unabhängigkeit der kriminaltechnischen Untersuchungsstelle wurde nach den Feststellungen des Landesbeauftragten für den Datenschutz nicht ausreichend beachtet.

Der Ausschuss begrüßt, dass ein Teil der bemängelten Punkte zwischen der Polizei und dem Landesbeauftragten für den Datenschutz mittlerweile einvernehmlich geklärt wurden. Ferner begrüßt der Ausschuss den zwischenzeitlich erfolgten Erwerb der Software.

Hinsichtlich der nicht rechtsadäquaten Verwendung einer Einwilligungserklärung geht der Ausschuss davon aus, dass zwischen dem Senator für Inneres, Kultur und Sport und dem Landesbeauftragten für den Datenschutz bis Anfang 2002 eine einvernehmliche Lösung gefunden wird.

Fernmeldegeheimnis und Kontrolle (Tz. 6.2.3): Auf der Grundlage einer Entscheidung des Bundesverfassungsgerichts hat der Bund die Regelungen für die parlamentarische Kontrolle im G-10-Gesetz novelliert. Die Landesbeauftragten für den Datenschutz haben darauf hingewiesen, dass für die parlamentarische Kontrolle in den Ländern eine entsprechende Anpassung an die Verfassungsrechtsprechung getroffen werden muss. Der Senat vertritt hingegen die Auffassung, der Landesgesetzgeber sei dabei an die Regelungen der §§ 14 und 15 des Gesetzes zur Neuregelung der Beschränkung des Brief-, Post- und Fernmeldegeheimnisses vom 26. Juni 2001 nicht gebunden.

Gleichwohl hat eine Bund/Länder-Arbeitsgruppe den Auftrag, einheitliche Regelungen für die Aufgabenstellung der parlamentarischen Kontrollkommission nach G 10 zu erarbeiten. Die Bereitschaft des Landesbeauftragten für den Datenschutz an der Ausgestaltung der Regelung mitzuwirken, hat der Vertreter des Senators für Inneres, Kultur und Sport nunmehr im Ausschuss begrüßt und eine Beteiligung zugesagt, sobald eine beratungsfähige Vorlage vorliegt.

Der Ausschuss erwartet einen Bericht.

Hochbaustatistik (Tz. 6.4.3): Der Landesbeauftragte für den Datenschutz hat in seinem Bericht die Vermischung von amtlicher Statistik und Verwaltungsvollzug festgestellt. Nach dem bisherigen Verfahren haben die Bauordnungsämter die Bauherren aufgefordert, Bauunterlagen und statistische Erhebungsbögen zusammen einzureichen. Nach den Bestimmungen des Hochbaustatistikgesetzes ist der Bauherr jedoch nur gegenüber dem Statistischen Landesamt auskunftspflichtig.

In seiner Stellungnahme räumt der Senat ein, dass die gebotene Trennung unterlaufen und derzeit geprüft werde, ob ähnlich wie in anderen Bundesländern durch Rechtsverordnung eine rechtliche Grundlage geschaffen werden könne. Die in der Stellungnahme des Senats angekündigte Prüfung ist noch nicht abgeschlossen. Der Senator für Inneres, Kultur und Sport wird die in Vorbereitung befindliche Vorlage mit dem Landesbeauftragten für den Datenschutz abstimmen. Die Abstimmung ist bis zum Abschluss der Beratungen im Ausschuss nicht erfolgt.

Der Ausschuss geht davon aus, dass die Prüfung durch den Senator für Inneres, Kultur und Sport in Kürze abgeschlossen sein wird.

Ermittlungsgruppe Schwarzarbeit (Tz. 6.8 und 16.6): Der Landesbeauftragte für den Datenschutz hat in seinem Bericht festgestellt, dass die rechtlichen Voraussetzungen für das Vorgehen der Ermittlungsgruppe nicht klar geregelt sind. Daraufhin wurde vom Stadtamt eine vorläufige Dienstanweisung zur Schließung von Regelungslücken erlassen.

Der Ausschuss hat zur Kenntnis genommen, dass der Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales aufgefordert ist, eine neue Regelung zur Zuständigkeit nach § 4 des Gesetzes zur Bekämpfung der Schwarzarbeit (SchwArbG) zu entwerfen und dem Landesgesetzgeber vorzulegen. Solange diese Regelungslücke besteht, werden keine Ermittlungsverfahren nach § 4 SchwArbG durchgeführt.

SAP-Prüfungen im ZKH Reinkenheide (Tz. 8.1.1) und im ZKH Links der Weser (Tz. 8.1.2): Der Landesbeauftragte für den Datenschutz hat in seinem Bericht festgestellt, dass die in den von ihm geprüften Krankenhäusern eingesetzten Informationssysteme den Ärzten und Pflegekräften Zugriff auf die dort gespeicherten Daten der gegenwärtigen und der früheren Patienten aller Fachabteilungen des jeweiligen Krankenhauses eröffnen. Dies sei in diesem Umfang weder durch den Behandlungsauftrag noch durch das Bremische Krankenhausdatenschutzgesetz abgedeckt. Die Erstellung eines differenzierten Berechtigungskonzepts und dessen Umsetzung seien erforderlich.

Die Vertreter der Zentralkrankenhäuser Reinkenheide und Links der Weser halten eine Novellierung des Krankenhausdatenschutzgesetzes hinsichtlich der im

Gesetz festgelegten Trennung der Fachabteilungen der Krankenhäuser für geboten, da sie der praktizierten interdisziplinären Behandlung zuwiderlaufe. Ferner müssten Patientendaten wegen der wesentlich verkürzten Verweildauer in den Krankenhäusern schneller abrufbar sein.

Die SAP-Software stellt den Nutzern keine Archivfunktion zur Verfügung mit der Folge, dass gegenwärtig nicht zwischen Patienten mit abgeschlossener und aktueller Behandlung differenziert werden kann. Inzwischen, so berichten übereinstimmend Vertreter der Krankenhäuser und der Landesbeauftragte, sei man bemüht, ein differenziertes Verfahren abzustimmen, das sowohl dem Schutz der Patientendaten als auch der Verantwortung des Arztes für eine fachliche Behandlung gerecht werden. Schritte seien eingeleitet, um SAP zur Modifikation der Software zu veranlassen

Der Ausschuss unterstützt die Empfehlung des Landesbeauftragten für den Datenschutz, das Bremische Krankenhausdatenschutzgesetz unter Wahrung der berechtigen Schutzbedürfnisse der Patienten unter Einbezug der neuen Entwicklungen der Technik und der Medizin fortzuschreiben. Er begrüßt die Erklärung des Senators für Arbeit, Frauen, Gesundheit, Jugend und Soziales, diese Empfehlung aufnehmen zu wollen.

Internet-Nutzung durch Schulen (Tz. 10.1): Der Landesbeauftragte für den Datenschutz hat das Fehlen einer Orientierungshilfe für Schulen und einer Nutzungsordnung festgestellt. Nach einem Workshop am 30. August 2001, an dem neben den Webmastern der Schulen auch Vertreter des Landesbeauftragten für den Datenschutz teilgenommen haben, wurde Anfang diesen Jahres eine Arbeitsgruppe eingerichtet. Diese wurde mit der Erarbeitung einer Orientierungshilfe sowie einer Nutzungsordnung beauftragt.

Durch die verstärkte Heranführung von Schülern an die Nutzung des Internets sowie bei der Präsentation der Schulen oder einzelner Projekte im Internet tritt zum Teil große Unsicherheit in Datenschutzfragen bei den verantwortlichen Lehrern auf. Der Landesbeauftragte für den Datenschutz hält es für erforderlich, dass in diesem Bereich mehr Sicherheit geschaffen wird. Die Schulbehörde hat angeboten, einen Mitarbeiter zur Begleitung dieses Projekts abzuordnen.

Der Ausschuss geht davon aus, dass die eingerichtete Arbeitsgruppe auf der Grundlage der Informationen des Landesbeauftragten für den Datenschutz Handreichungen bis Ende März 2002 erarbeiten wird.

Prüfung des Wohngeldverfahrens (BREWOG) (Tz. 11.2): Der Landesbeauftragte für den Datenschutz hat in seinem Bericht festgestellt, dass bei der Bearbeitung von Wohngeldanträgen in Bremen und Bremerhaven alle 60 Mitarbeiter des AWS — unabhängig von ihrem jeweiligen Aufgabenbereich — uneingeschränkt Zugriff auf den auch sensible Sozialdaten enthaltenden gesamten Datenbestand haben, obgleich die Einrichtung begrenzter Zugriffsberechtigungen technisch möglich ist. Grundsätzlich darf ein Zugriff nur auf die für die Durchführung der jeweiligen Aufgaben erforderlichen Daten erfolgen können.

Das dem Geschäftsbereich des Senators für Bau und Umwelt zugeordnete Amt für Wohnung und Städtebauförderung hält einen uneingeschränkten Zugriff auf sämtliche Daten — unter anderem aus Gründen der Vertretungsregelung und etwaiger Neuzuordnungen — für erforderlich. Der Landesbeauftragte für den Datenschutz hat darauf hingewiesen, dass gegebenenfalls notwendige Änderungen der Zugriffsberechtigung — ähnlich den Regelungen bei der Bearbeitung der Sozialhilfe — im Vertretungsfalle vom Systemadministrator durchgeführt werden können.

Der Ausschuss stellt einen Regelungsbedarf fest und bittet das Amt für Wohnung und Städtebauförderung, sich über die entsprechende Praxis in anderen Dienststellen zu informieren und sodann gemeinsam mit dem Landesbeauftragten für den Datenschutz eine Lösung zu entwickeln. Der Datenschutzausschuss erwartet einen Sachstandsbericht darüber noch im Frühjahr 2002.

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 hat sich der Datenschutzausschuss u. a auch mit den nachfolgend aufgelisteten Themen beschäftigt:

Konsequenzen einer Melderechtsänderung für das in Bremerhaven bestehende DV-Verfahren

Vorstellung des Netzes der Verwaltungspolizei

Zugriff der GEZ auf Meldedaten

Kfz-Zulassungsstelle: Wunschkennzeichen über Internet

Vorlage zur Gründung: Landesgesellschaft „datenschutz nord GmbH“

Einsatz neuer Software in der bremischen Verwaltung

Modellversuch „Alternierende Telearbeit“

Datenschutzkonzept für den Justizbereich

Datenschutzkonzept zum elektronischen Einbürgerungsverfahren

Rezeptrecherche mit Hilfe der NARZ-CD

Brustkrebs-Screening-Programm

Einführung eines zentralen Verzeichnisdienstes „Active Directory“ beim Einsatz von Windows 2000

Internetseite des LfD

Bremisches Informationsfreiheitsgesetz

Bremisches Polizeigesetz

Novellierung des Bundesdatenschutzgesetzes

Novellierung des Bremischen Datenschutzgesetzes

5. Personalwesen

5.1. Prüfung der Führung der Personalakten bei verschiedenen Personalstellen

Im Berichtszeitraum habe ich bei insgesamt sieben Personalstellen Prüfungen zur Führung von Personalakten und Personaldaten durchgeführt und zwar bei:

— dem Senator für Inneres, Kultur und Sport,

— dem Senator für Bau und Umwelt,

— beim Amtsgericht Bremerhaven,

— dem Aus- und Fortbildungszentrum der Bremer Verwaltung (AFZ),

— der Hochschule Bremerhaven,

— der Universität Bremen und

— dem Zentralkrankenhaus St.-Jürgen-Straße.

Dabei habe ich verschiedene datenschutzrechtliche Teilaspekte geprüft, die Ergebnisse habe ich nachfolgend zusammengefasst.

Bei fünf Personalstellen befand sich zumindest in den eingesehenen Grundakten kein Verzeichnis aller Teil- und Nebenakten. Die Aufnahme eines derartigen Verzeichnisses ist zur Wahrung des unbeschränkten Akteneinsichtsrechts des Be-

schäftigten besonders wichtig, weil er sonst bei Einsichtnahme in die Hauptakte nicht erkennen kann, dass weitere Personalteilakten zu seiner Person geführt werden.

Des Weiteren wurde in allen geprüften Personalstellen festgestellt, dass Urlaubs- und Krankheitsunterlagen länger als die in den Richtlinien über die Erhebung und Führung von Personalaktendaten (RiLi vom 25. Mai 1996, Brem. Abl. S. 433) vorgesehene Aufbewahrungsfrist von fünf Jahren in den Teilakten enthalten waren. Bei vier geprüften Personalstellen befanden sich Urlaubs- und Krankheitsunterlagen teilweise in den Grundakten, obwohl sie nach den RiLi zu den dafür vorgesehenen Teilakten zu nehmen sind. Diese Regelung hat den Zweck, dass die länger als fünf Jahre zurückliegenden Unterlagen ohne besonderen Verwaltungsaufwand vernichtet werden können. Auch beim Versand werden häufig nur die Daten aus der Grundakte von der anfordernden Stelle benötigt.

Weiterer Prüfgegenstand war die Aufbewahrung von Personalakten ausgeschiedener Bediensteter. In fünf Personalstellen werden Personalakten nach deren Abschluss länger aufbewahrt als in der vorgenannten Richtlinie vorgesehen. Danach sind die Personalakten der Bediensteten ohne Versorgungsansprüche fünf Jahre nach Vollendung des 65. Lebensjahres zu vernichten; Personalakten der Bediensteten mit Versorgungsansprüchen fünf Jahre nach Ablauf des Jahres, in dem die letzte Versorgungsverpflichtung ggf. auch gegenüber Hinterbliebenen entfallen ist. Hierüber erhalten die Dienststellen eine Mitteilung von Performa Nord. Beim Amtsgericht Bremerhaven werden diese Personalakten besonders lange aufbewahrt. Dort befinden sich Personalakten über ehemalige Bedienstete, die vor über 100 Jahren geboren wurden. Die geprüften Personalstellen — außer dem Senator für Bau und Umwelt — haben erklärt, sie hätten bisher noch keine Mitteilung von Performa Nord über den Abschluss von Personalakten erhalten. Ich habe daher diese Behörde Ende Dezember 2001 um Mitteilung gebeten, ob und ggf. nach welchem Verfahren sie ihrer Mitteilungspflicht nachkommt. Bis zum Redaktionsschluss habe ich noch keine Antwort darüber erhalten.

Weiterer Prüfgegenstand war die Aufbewahrung von Bewerbungsunterlagen. Bewerbungsunterlagen sind, soweit sie nicht an abgewiesene Bewerber zurückgegeben werden, nach § 22 Abs. 5 (BrDSG) unverzüglich zu löschen sobald feststeht, dass ein Dienst- oder Arbeitsverhältnis nicht zustande kommt, es sei denn, dass der Betroffene zur Aufrechterhaltung seiner Bewerbung in die weitere Speicherung eingewilligt hat. Meine Prüfung hat ergeben, dass die Unterlagen zwar regelmäßig an die abgewiesenen Bewerber zurückgesandt werden, jedoch ohne die Bewerbungsschreiben. Ich habe darauf hingewiesen, dass diese Schreiben Bestandteile der Bewerbungsunterlagen und demzufolge unverzüglich, also spätestens ein Jahr nach Abschluss des Auswahlverfahrens zu vernichten sind.

Die Prüfung der Beihilfe- und Kindergeldakten ergab folgendes Bild: Beim Zentralkrankenhaus St.-Jürgen-Straße werden die Beihilfe- und Kindergeldakten aufbewahrt, obwohl die Berechnung der Beihilfe und des Kindergeldes durch Performa Nord erfolgt. Hierzu ist mir eine Anweisung des damaligen Senators für Jugend, Gesundheit und Soziales vom 18. April 1997 vorgelegt worden. Da diese Anweisung für alle Zentralkrankenhäuser der Stadtgemeinde Bremen gilt, habe ich den Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales auf die nach § 93 b Satz 2 Bremisches Beamtengesetz vorgeschriebene Trennung der Beihilfebearbeitung von der Personalverwaltung hingewiesen und ein Verfahren vorgeschlagen, dass diesem Trennungsgebot entspricht, insbesondere die Führung der Teilakten bei Performa Nord, weil diese die Bescheide erstellt. Die senatorische Dienststelle hat daraufhin mitgeteilt, das Problem Anfang des Jahres 2002 mit mir erörtern zu wollen.

Ich habe den Stellen jeweils in einem Prüfbericht die festgestellten Mängel mitgeteilt. Die geprüften Personalstellen haben inzwischen erklärt, die Mängel beseitigt zu haben bzw. zu beseitigen und in Zukunft die o. g. Verwaltungsvorschrift zu beachten.

5.2. Datenverarbeitung bei Personalratswahlen

In einer Beschwerde wurde vorgetragen, dass das Wählerverzeichnis, das jeweils Namen und Privatanschriften der Wahlberechtigten zur Personalratswahl der

Dienststelle des Senators für Wirtschaft und Häfen enthielt, per E-Mail an alle Beschäftigten dieser Dienststelle übermittelt worden war. Dies war für mich Anlass, generell die Datenverarbeitung bei Personalratswahlen zu prüfen. Hierzu habe ich mir vom Gesamtpersonalrat (GPR) die Durchführungshinweise und Arbeitshilfen zukommen lassen.

Ich habe dem GPR vorgeschlagen, in der „Anlage zum Wahlvorschlag", in dem Datum, Namen und Unterschriften der Beschäftigten enthalten sind, die den Wahlvorschlag unterstützen, das Geburtsdatum dieser Beschäftigten nicht mehr aufzuführen, weil es weder in der Wahlordnung ausdrücklich vorgesehen ist, noch andere Gründe dies erforderlich machen. Soweit in größeren Dienststellen mehrere Beschäftigte den gleichen Vor- und Familiennamen haben und der gleichen Beschäftigungsgruppe angehören, sollte ein anderes Unterscheidungsmerkmal, z. B. das Organisationskennzeichen, angegeben werden.

Des Weiteren sollten in der Zustimmungserklärung für die Aufnahme in den Wahlvorschlag die Privatanschrift und die private Telefonnummer nicht mehr aufgeführt werden, weil diese Daten ebenfalls nicht in der Wahlordnung ausdrücklich vorgesehen und auch im Übrigen nicht erforderlich sind.

Außerdem sollte in der Arbeitshilfe und ggf. auch in den Durchführungshinweisen des GPR ausdrücklich darauf hingewiesen werden, dass im Wählerverzeichnis nur die Daten der Beschäftigten (Wahlberechtigten) aufgeführt werden dürfen, die für den Zweck des Wählerverzeichnisses erforderlich sind (Vorname, Familienname, getrennt nach den jeweiligen Beschäftigungsgruppen). Sinn und Zweck des Wählerverzeichnisses ist nämlich die Auslegung zur Einsicht durch die Angehörigen der Dienststelle nach § 2 Abs. 3 Wahlordnung, um insbesondere Einsprüche gegen die Richtigkeit des Wählerverzeichnisses zu ermöglichen und darüber zu entscheiden (§ 3 Wahlordnung).

Schließlich sollte in den vorgenannten Unterlagen darauf hingewiesen werden, dass das Wählerverzeichnis nur an geeigneter Stelle auszulegen ist, jedoch nicht an alle Beschäftigten z. B. per E-Mail oder Kopie übermittelt werden darf.

Ich erwarte, dass mit der Umsetzung der vorgenannten Vorschläge das Wahlverfahren in Zukunft ohne datenschutzrechtliche Probleme durchgeführt werden kann.

5.3 Unterlagen über personelle Angelegenheiten beim Personalrat

Eine Mitarbeiterin des Zentralkrankenhaus St.-Jürgen-Straße hat moniert, der dortige Personalrat bewahre Unterlagen zu ihrer Person über personelle Angelegenheiten auf, obwohl diese bereits teilweise seit zehn Jahren abgeschlossen seien. Der Personalrat hat dies bestätigt und die fraglichen Unterlagen vernichtet. Auf meinen Hinweis, dass derartige Unterlagen dann zu vernichten sind, wenn sie nicht mehr erforderlich sind, hat er zugesagt, Unterlagen mit personenbezogenen Daten, die nicht erforderlich sind, sofort, die übrigen spätestens nach fünf Jahren zu vernichten.

5.4. Einsicht in Bewerbungsunterlagen durch einen Mitkonkurrenten

Eine Bewerberin für eine Notarstelle hat mich darüber unterrichtet, dass ein Mitkonkurrent in ihre Bewerbungsunterlagen beim Hanseatischen Oberlandesgericht (OLG) Einsicht genommen habe, der vor dem OLG Beschwerde eingelegt hat. Auf meine Anfrage erklärte der Senator für Justiz und Verfassung, dass eine Pflicht zur Gewährung von Akteneinsicht nach § 29 Abs. 1 Bremisches Verwaltungsverfahrensgesetz (BremVwVfG) bestanden habe, weil sie für den Mitkonkurrenten zur Geltendmachung seiner rechtlichen Interessen erforderlich war. Ich habe der senatorischen Behörde mitgeteilt, dass dies nicht zu beanstanden sei und sie gebeten, zukünftig in derartigen Fällen jeweils die Betroffenen über Inhalt und Empfänger einer Auskunft durch Dritte schriftlich zu unterrichten — analog der Regelung über die Einsicht in Personalakten durch bzw. Auskunft an Dritte nach Ziffer 27 Abs. 4 Satz 2 der Verwaltungsvorschrift über die Erhebung und Führung von Personalakten vom 1. Oktober 2001 (Brem.Abl. S. 761). Der Senator für Justiz und Verfassung hat meine Empfehlung übernommen.

5.5. Veröffentlichung von Arbeitnehmerdaten im Internet

Ein Mitarbeiter des Instituts für Werkstofftechnik der Universität Bremen hat moniert, dass ohne seine Einwilligung sein Name, seine dienstliche Telefonnummer und E-Mail-Adresse ins Internet gestellt worden sind. Insbesondere war er nicht damit einverstanden, dass durch Eingabe seines Namens in eine Suchmaschine von jedermann festgestellt werden könne, welche berufliche Tätigkeit er ausübt. Er halte die Veröffentlichung seiner personenbezogenen Daten im Internet durch seinen Arbeitgeber nicht für erforderlich, weil er nicht ständig erreichbar sein müsse.

Auf meine Nachfrage hat das Institut mitgeteilt, eine Veröffentlichung der Daten des Betroffenen im Internet sei nicht erforderlich, so dass die entsprechenden Angaben entfernt worden sind.

5.6. Richtlinien über die Erhebung und Führung von Personalaktendaten

Die Richtlinien über die Erhebung und Führung der Personalaktendaten sind in einigen Punkten redaktionell geändert worden. Bedeutsam ist, dass nunmehr Strafregisterauszüge in die Grundakte aufzunehmen sind. Bisher wurden sie als so genannte andere Vorgänge in Sachakten aufbewahrt.

Ich habe zu dieser Neuregelung zu bedenken gegeben, dass durch die Aufnahme dieser Unterlagen und die Aufbewahrungsfrist von drei Jahren die Tilgungsfristen nach dem Bundeszentralregistergesetz unterlaufen werden könnten. Tilgungsfristen für Eintragungen im Bundeszentralregister könnten kurz nach der Vorlage beim Dienstherrn oder Arbeitgeber ablaufen, während die Aufbewahrung in der Grundakte noch drei Jahre nach Aufnahme in diese Akte erfolgen würde. Des Weiteren wäre die Vernichtung mit einem erheblichen Verwaltungsaufwand verbunden, nämlich mit der Vernichtung des Auszuges und der Neuanfertigung eines Inhaltsverzeichnisses. Es ist also zu befürchten, dass in vielen Fällen die vollständige Tilgung dieser Daten aus der Personalakte tatsächlich nicht erfolgt.

Aufgrund meiner Bedenken ist mit dem Senator für Finanzen Einvernehmen erzielt worden, dass es sich bei den Angaben aus dem Bundeszentralregister um sensible Daten handelt, so dass Führungszeugnisse mit Einträgen — wie ärztliche Unterlagen — vertrauliche Unterlagen sind, die entsprechend Ziffer 7 der Richtlinie in einem verschlossenen Umschlag zur Personalakte zu nehmen sind.

Die geänderten Richtlinien sind am 1. November 2001 als Verwaltungsvorschrift über die Erhebung und Führung von Personalaktendaten (PAVwV) (Brem.Abl. v. 1. Oktober 2001, S. 103)

6. Inneres

6.1. Geändertes Bremisches Polizeigesetz in Kraft

Das Gesetzgebungsverfahren mit den auch für den Datenschutz gravierenden Änderungen im Bremischen Polizeigesetz, über dessen Entwurf ich bereits in meinem 22. Jahresbericht (vgl. dort Ziff. 4.2.6.1.) berichtet hatte, verzögerte sich, bis eine Regelung für den Schusswaffengebrauch von der Koalition gefunden wurde. Die Zeit wurde u. a. dazu genutzt, eine Vorschrift für das Wegweisungsrecht zu beraten. Mit § 14 a wurde eine Regelung zu „Wohnungswegweisung und Rückkehrverbot zum Schutz vor häuslicher Gewalt“ noch in das Gesetz eingefügt. Anlässlich der Erörterung dieser Vorschrift wurde auch die Regelung der Datenübermittlung von der Polizei an andere öffentliche Stellen nach § 36 f in Abstimmung mit mir noch einmal verändert. Nach dem neuen Wortlaut darf die Polizei an zuständige öffentliche Stellen, wie z. B. den Sozialpsychiatrischen Dienst auch dann Daten übermitteln, wenn sie im Rahmen ihrer Aufgabenerfüllung „Anhaltspunkte für das Bestehen einer sozialen Notlage“ feststellt.

Das Gesetz, das der Senat der Bürgerschaft am 23. Januar 2001 zur Beschlussfassung zugeleitet hatte, trat mit den genannten Änderungen am 13. September 2001 in Kraft. Eine Regelung zur Rasterfahndung wurde nachträglich ergänzt, mehr dazu im nächsten Beitrag.

6.2. Gesetzgebungsberatung Rasterfahndung

Mit in Kraft treten der Änderungen im Bremischen Polizeigesetz am 13. September 2001 enthielt dieses, anders als sein Vorgänger aus dem Jahre 1983, keine Regelung zur Rasterfahndung. Angesichts der Terroranschläge vom 11. September 2001 in den USA und der danach verlangten bundesweiten Rasterfahndung, insbesondere nach so genannten Schläfern, gingen Senat und Bürgerschaft erneut an die Arbeit, um das eben verabschiedete Gesetz zu ergänzen.

Der Gesetzentwurf wurde mir mit sehr kurzer Stellungnahmefrist vom Innenressort zugeleitet, ich habe daraufhin einige Änderungsvorschläge unterbreitet. Nachdem der Senat auf seiner Sitzung am 16. Oktober 2001 den Gesetzesentwurf zur Rasterfahndung unverändert beschlossen hatte, habe ich mich mit einem Schreiben an die Fraktionen von CDU, SPD und Bündnis 90/Die Grünen gewandt, um noch im Gesetzgebungsverfahren essentielle Verbesserungen des Datenschutzes zu erreichen, insbesondere, um das hohe rechtsstaatliche Niveau, das — bei aller Datenschutzkritik im Einzelnen — in dem neuen Polizeigesetz verankert ist, bei der Ergänzung der Regelung zur Rasterfahndung (§ 36 i BremPolG-E) nicht aufzugeben.

Ich habe dabei die Einfügung eines Richtervorbehalts gefordert. Zur Begründung habe ich ausgeführt: „Das Instrument der Rasterfahndung tangiert zwangsläufig das informationelle Selbstbestimmungsrecht vieler unbescholtener Bürger. Jetzt sind es ausländische Studenten, morgen sind es deutsche Staatsbürger. Die Norm wird nicht nur für die aktuelle Lage verabschiedet, sondern besteht fort.

Die Rasterfahndung wirft nicht zielgenaue Ergebnisse aus, sie dient der Verdachtsgewinnung; Personen mit ausgerasterten Daten sind in aller Regel von weiteren polizeilichen Maßnahmen betroffen. Unter datenschutzrechtlichen Gesichtspunkten liegt es daher nahe, einen möglichst hohen Schutz der Rechtmäßigkeit vor Durchführung einer solchen Maßnahme zu garantieren. Der Bundesgesetzgeber hat deshalb bereits bei Einführung der Rasterfahndung für Zwecke der Strafverfolgung in den 80er Jahren den Grundrechtseingriff als so gravierend angesehen, dass er in § 98 b Strafprozessordnung (StPO) die richterliche Bestätigung einer Rasterfahndungsmaßnahme verlangt. Von dieser Linie sollte auch in Bremen nicht abgewichen werden.

Bei der eben erst abgeschlossenen Novellierung des Bremischen Polizeigesetzes ist insbesondere bei der Einfügung der Regelungen der Datenerhebung mit ‚besonderen Mitteln und Methoden' darauf geachtet worden, dass kein geringerer Rechtsschutz vorgesehen werde, als er beim Einsatz entsprechender Maßnahmen für Zwecke der Strafverfolgung vom Bundesgesetzgeber normiert worden ist (vgl. z. B. Regelung des Lauschangriffs in § 33 BremPolG oder des Einsatzes verdeckter Ermittler in § 35 BremPolG). Im Übrigen sehen auch eine Reihe anderer Länder in ihren Polizeigesetzen bei der Rasterfahndung eine richterlicher Kontrolle vor.

Auch das Argument, eine richterliche Überprüfung sei überflüssig, weil nach § 36 BremPolG eine parlamentarische Kontrolle stattfindet, überzeugt nicht. Diese Vorschrift sieht die Unterrichtung des Ausschusses in einem Zeitraum ‚von höchstens sechs Monaten' vor. Eine solche nachträgliche Kontrolle ersetzt eine richterliche Vorabkontrolle einer solchen Maßnahme nicht. Weiter ist zu berücksichtigen, dass — anders als mit der jetzt im Gesetzentwurf vorgesehenen Überprüfung durch Polizei und Innenressort — bei der richterlichen Kontrolle eine unabhängige dritte Gewalt mit der Entscheidung befasst wird.

Schließlich kann ich auch das Argument nicht gelten lassen, durch eine richterliche Entscheidung würde der Einsatz der Maßnahme unnötig verzögert. Richtig ist, dass die Maßnahmen der Rasterfahndung in der Regel nicht binnen kurzer Zeiten durchgeführt werden können, weil die zur Auskunft verpflichtete Stelle die an die Polizei herauszugebenden Daten zunächst selektieren müssen." Dies hat sich in der jetzt laufenden Rasterfahndung bestätigt (vgl. Ziff. 6.3. dieses Berichts).

Diese und andere Überlegungen führten und führen mich zu dem Ergebnis, dass es keine hinreichenden Gründe gibt, auf die richterliche Überprüfung vor Durchführung der Rasterfahndung zu verzichten.

Weiter habe ich in meinem Schreiben die Sicherstellung einer engen Zweckbindung der durch Rasterfahndung gewonnenen Daten verlangt. Durch den vorgesehenen versteckten Regelungsort in § 36 i BremPolGE ist die Maßnahme der Rasterfahndung nicht als ein Vorgang der Datenerhebung gekennzeichnet. Es bestand daher die Gefahr, dass die mit der Rasterfahndung gewonnenen Daten nicht einer engen Zweckbindung unterworfen werden. Die Betroffenen müssen aber nur unter gesetzlich festzulegenden hohen Voraussetzungen einen Eingriff in ihr informationelles Selbstbestimmungsrecht hinnehmen. Erhebung und Weiterverarbeitung für andere polizeiliche Zwecke sind daher einer strengen Zweckbindung zu unterwerfen. Auch nach der Regelung der Rasterfahndung in der StPO dürfen nach § 98 b StPO diese Daten in anderen Strafverfahren nur verwendet werden, wenn es zur Aufklärung einer entsprechenden Straftat zulässig ist. Insgesamt hätte ich daher einen anderen Regelungsort im Polizeigesetz, nämlich bei den Vorschriften, die die Datenerhebung mit besonderen Mitteln und Methoden regeln, favorisiert und gern mit dem auch in der StPO verwendeten Begriff der „Rasterfahndung“ in der Überschrift versehen.

In dem wichtigen Punkt der Zweckbindung der bei einer Rasterfahndung erlangten Daten wurde meinem Anliegen im Gesetzgebungsverfahren leider nur teilweise entsprochen, in den übrigen Punkten nicht. Weil man den von mir vorgeschlagenen Regelungsort nicht wählte, ist die absurde Situation entstanden, dass zwar die Daten bei der Polizei im Lande einer engen Zweckbindung unterliegen, nicht jedoch wenn sie nach § 36 d BremPolG an andere Polizeidienststellen des Bundes, der Länder oder andere öffentliche Stellen übermittelt werden. Dies kann der Gesetzgeber jetzt nur durch eine Ergänzung des Verweises in § 36 i Abs. 5 BremPolG auf §§ 36 d Abs. 2, 36 f Abs. 3 BremPolG heilen. Die Vorschrift des neu eingefügten § 36 i BremPolG zur Rasterfahndung heißt „Datenabgleich mit anderen Dateien“. Über die Anwendung der Vorschrift berichte ich nachfolgend unter Ziff. 6.3.

6.3 Durchführung der Rasterfahndung im Land Bremen

Nach den Anschlägen am 11. September 2001 in den USA und dem Erkennen einer Verbindungslinie zu in Hamburg lebenden mutmaßlichen Terroristen, die daran beteiligt waren, wurde bundesweit nach Hintermännern, den so genannten 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. Man sah in dem Instrument der Rasterfahndung das geeignete Mittel, weitere Anhaltspunkte zu gewinnen, um Verdächtige aufzuspüren.

Die in Bremen — auf im Polizeigesetz neu geschaffener Rechtsgrundlage — erstmals durchgeführte Rasterfahndung hat zu einer starken Verunsicherung insbesondere der betroffenen ausländischen Studierenden geführt und in der Presse eine nicht unerhebliche Resonanz gehabt.

Bei der Rasterfahndung werden auf der Grundlage einer Fahndungshypothese aus Fremddatenbeständen Auswertungen vorgenommen und mit anderen Datenbeständen verglichen, mit dem Ziel, einen Bestand an Datensätzen herauszufiltern, auf den die angenommenen Voraussetzungen zutreffen. Auf der Grundlage des neuen § 36 i BremPolG haben die Leiter der Polizeien in Bremen und Bremerhaven Maßnahmen zur Rasterfahndung angeordnet. Nach dieser Vorschrift bin ich darüber „unverzüglich“ zu unterrichten. Meine Unterrichtung über die Anordnungen erfolgte in der Mehrzahl der Fälle nach rund acht Tagen, in einem Fall erst nach 18 Tagen. Sie war somit in allen Fällen zu spät.

Gerade noch war mir im Gesetzgebungsverfahren auf meine Forderung nach einer vorgängigen Kontrolle durch Richtervorbehalt entgegengehalten worden, den Belangen des Datenschutzes sei durch die im Gesetz vorgesehene „unverzügliche Unterrichtung des Landesbeauftragten für den Datenschutz“ bereits mit Beginn der Maßnahme ausreichend Rechnung getragen, um einen frühzeitigen Datenschutz der Bürger zu gewährleisten.

Unter Ausnutzung moderner Kommunikationsmethoden erwarte ich, dass, nachdem der Innensenator eine solche Maßnahme gebilligt hat, ich noch am selben Tag darüber unterrichtet werde! Nur so ist gewährleistet, dass ich noch auf das

Verfahren und alle Phasen der Datenverarbeitung, insbesondere auch auf Art und Umfang der Datenerhebung Einfluss nehmen kann. In der verspäteten Unterrichtung sehe ich einen nicht unerheblichen Verstoß gegen datenschutzrechtliche Bestimmungen, den ich auch gegenüber dem Innensenator beanstandet hätte, wären daraus im konkreten Verfahren Nachteile für den Datenschutz entstanden. Ich habe auf eine förmliche Beanstandung gemäß § 29 BrDSG nur deshalb verzichtet, weil bei meiner Unterrichtung über die eingeleitete Rasterfahndung noch keine Daten von der Bremer Polizei weiter verarbeitet worden waren.

Im Zuge der bundesweiten polizeilichen Aktivitäten wurde unter Koordination des BKA eine einheitliche Kriterienliste für die Rasterfahndung entwickelt. Das Rasterprofil ist in allen Bundesländern weitgehend identisch. Allen von der Polizei Bremen und der Ortspolizeibehörde Bremerhaven vorgelegten Anordnungen zur Rasterfahndung hat der Innensenator zugestimmt. Unmittelbar nach Eingang der Unterrichtung über die erlassenen Anordnungen habe ich die Prüfung der getroffenen Maßnahmen eingeleitet. Die ersten Anordnungen der Rasterfahndung erfolgten am 1. November 2001 in Form von sieben Einzelanordnungen an verschiedene Stellen (s. u.). Diese Form der Einzelanordnungen wurde gewählt, da die Rasterkriterien sich zwar für alle Stellen gleich darstellen, jedoch nicht alle Stellen über gleiche Datenarten verfügen. Eine knappe Begründung wurde in den einzelnen Anordnungen vorgenommen und dokumentiert. Zweck der Rasterfahndungsmaßnahmen war danach die Identifizierung von handlungsfähigen Tätern oder Tätergruppen nach von dem FBI über das BKA zugeleiteten Merkmalen, die als so genannte Schläfer unerkannt geblieben sind oder untertauchen könnten. Eine Ermittlung dieser Personen erscheine auf andere Weise nicht möglich. Laut Auskunft des für die Rasterfahndung zuständigen Beamten wäre der Aufwand, die anzuliefernden Daten bei den speichernden Stellen vor Ort zu sichten, unverhältnismäßig groß. Die verschiedenen Einzelanordnungen der Rasterfahndung zur Datenselektion und Übermittlung an die Polizei wurden den folgenden Stellen zugestellt:

— Ausländerbehörden Bremen und Bremerhaven,

— Bundesverwaltungsamt in Köln (Ausländerzentralregister),

— Einwohnermeldebehörden Bremen und Bremerhaven,

— Hochschulen Bremen und Bremerhaven,

— Handelskammer Bremen und Industrie- und Handelskammer Bremerhaven,

— Internationale Universität Bremen,

— Universität Bremen.

Meine Datenschutzprüfungen vor Ort habe ich bisher bei der Polizei in Bremen und Bremerhaven sowie beim ID-Bremen GmbH vorgenommen. Dabei habe ich folgendes festgestellt: Die Daten (Datensätze) wurden den anordnenden Polizeien per Datenträger übergeben oder aber per Post übersandt. Mit Ausnahme der Datensätze der Industrie- und Handelskammern wurden die Daten durch die ID Bremen GmbH im Auftrag der Polizei Bremen — LKA — aufbereitet. Der Auftrag für die Aufbereitung durch die ID Bremen GmbH wurde zwar schriftlich erteilt, er genügt aber nicht den Vorschriften des § 9 BrDSG, denn es wurden keine hinreichenden Festlegungen für die Datenverarbeitung, noch für die technischen und organisatorischen Maßnahmen nach § 7 BrDSG getroffen.

Von den genannten Stellen wurden insgesamt rund 100.000 Personendatensätze angeliefert. Das ID-Bremen erstellt einen einheitlichen, in sich abgestimmten Datensatz. Dieser wurde ohne Überschussdaten an die zuständige Stelle bei der Polizei Bremen übergeben. Erst gegen Ende Januar 2002 wurde die Aufbereitung der Daten bei der ID-Bremen abgeschlossen. Es wurden im Land insgesamt 589 Datensätze herausgefiltert. Diese Datensätze wurden an das BKA zur Aufnahme in eine neue Verbunddatei „Terroranschlag USA“ übermittelt. Eine Kopie der Datensätze wird bei der Polizei Bremen — LKA — in die Datei „Rasterfahndung Terroranschlag USA“ überführt. Dazu wurde bei der Polizei Bremen — LKA — eine entsprechende Arbeitsdatei eingerichtet.

Der Entwurf einer entsprechenden Dateibeschreibung für diese Arbeitsdatei wurde mir ausgehändigt. Aus technischer Sicht soll es sich bei der neu zu errichtenden Datenbank um eine Datenbankanwendung handeln, die von der Polizei bundesweit eingesetzt wird. Zur weiteren Bearbeitung können normale Officeanwendungen genutzt werden. Diese Datei ist noch nicht eingerichtet.

Nach dem bundesweiten Abgleich beim BKA werden die dann ermittelten Daten an die Polizei Bremen — LKA — übermittelt und hier ergänzenden polizeiliche Ermittlungen und Abklärungen unterzogen. Alle jeweils nicht weiter benötigten Daten sollen nach Auskunft der zuständigen Stelle der Polizei Bremen sofort gelöscht werden. Die Löschung bzw. Vernichtung der in der Datei verbleibenden Daten soll nach einer bundeseinheitlichen zeitlichen Frist erfolgen. Diese soll an die in der Errichtungsanordnung des Bundeskriminalamtes angelehnt werden. Die Errichtungsanordnung ist noch nicht in Kraft gesetzt.

Eine Unterrichtung des parlamentarischen Kontrollausschusses nach § 36 BremPolG durch den Innensenator über die Rasterfahndung soll schon stattgefunden haben. Ich bin aber über die Ergebnisse nicht unterrichtet, über die Ergebnisse der Datenschutzprüfungen hat sich der Kontrollausschuss bei mir bisher nicht erkundigt. Ich habe auch die zwischenzeitlich in anderen Bundesländern ergangener Rechtsprechung darauf geprüft, ob sich aus den Urteilen Folgerungen für das in Bremen laufende Verfahren ableiten lassen. So hat das LG Berlin die Rasterfahndungsmaßnahmen in Berlin deshalb für unzulässig erklärt, weil sie zur Abwehr einer „gegenwärtigen Gefahr“ ungeeignet seien, die bremische Regelung enthält ein solches Tatbestandsmerkmal aber nicht.

Ich werde auch die weiteren Schritte der Rasterfahndung kontrollieren und nach Abschluss der Maßnahmen erneut der Öffentlichkeit berichten.

Ob das Instrument der Rasterfahndung bislang überhaupt nennenswerte Erfolge erzielt hat, ist wissenschaftlich noch nicht untersucht worden. Die Problematik der Rasterfahndung liegt darin, dass eine Vielzahl völlig Unverdächtiger (Nichtstörer) in die Fahndung mit einbezogen werden und Opfer weiterer polizeilicher Ermittlungen werden können. Sie ist nur dann erfolgversprechend, wenn sich die gesuchten Personen durch bestimmte Eigenschaften und Merkmale von den weitaus meisten Menschen unterscheiden. Ich habe zurzeit die Befürchtung, dass das Raster zu weit ist, deshalb zu viele mit einbezogen werden und die damit bundesweit zusammengetragene Anzahl an Personen und Daten eine effektive polizeiliche Abklärung nicht erlauben.

6.4. Antiterrorgesetzgebung

Wenn man von einem Durchpeitschen von Gesetzen sprechen darf, so trifft dies sicherlich auf die beiden Gesetzespakete als Reaktion auf die Anschläge vom 11. September 2001 in den USA zu. Kein anderes europäisches Land hat als unmittelbare Reaktion auf die Ereignisse vom 11. September seinen Bürgern so viele gesetzliche Einschränkungen zugemutet wie die Bundesrepublik, nicht einmal die von den Anschlägen unmittelbar betroffene USA. Dabei treffen viele der in der Bundesrepublik vorgesehenen Maßnahmen fast ausschließlich die eigene Bevölkerung. Durch das Terrorismusbekämpfungsgesetz (vgl. BR-Drs. 1059/01) werden u. a.

— dem Verfassungsschutz, z. T. MAD und BND weitreichende Eingriffsbefugnisse in Bank- und Telekommunikations- und Postgeheimnis gegeben, er darf u. a. bei Luftfahrtunternehmen Daten über Reisende erfragen,

— biometrische Merkmale in Pass und Personalausweis zugelassen,

— die Datenverarbeitungskompetenzen des Bundeskriminalamtes erheblich erweitert,

— die Datenerhebungs- und die Weiterverarbeitungsbefugnisse im Ausländer- und Ausländerzentralregistergesetz, sowie in den zugehörigen Durchführungsverordnungen erweitert und

— der Sozialdatenschutz für Zwecke der Rasterfahndung eingeschränkt.

An den Regelungen für die Schaffung einer zentralen Informationsstelle für Bankkonten wird derzeit noch gearbeitet. Nachdem ich den Innensenator über die einschlägigen Beschlüsse der Konferenz der Datenschutzbeauftragten (Ziff. 15.9., 15.14. und 15.15. dieses Berichtes) unterrichtet hatte, habe ich nach Rücksprache mit dem Innenressort — mangels Aussicht auf Erfolg — auf eine dezidierte Stellungnahme zur Behandlung der Gesetzentwürfe im Bundesrat verzichtet.

6.5. Polizeiliche Videoüberwachung öffentlich zugänglicher Orte

Auf der Grundlage des § 29 Abs. 3 des neuen Bremischen Polizeigesetzes (vgl. Ziff. 6.1. dieses Berichts) hat die Polizei die rechtliche Möglichkeit zur Videoüberwachung von öffentlich zugänglichen Orten, wenn an ihnen vermehrt Straftaten begangen werden oder an ihnen auf Grund der örtlichen Verhältnisse die Begehung von Straftaten besonders zu erwarten ist. Eine Bildübertragung und -aufzeichnung ist nur zulässig, wenn diese Maßnahme erkennbar und offen durchgeführt wird. Nach einer internen Untersuchung der Polizei treffen diese gesetzlichen Voraussetzungen auf drei Örtlichkeiten in der Stadtgemeinde Bremen zu. Die aktuellen Planungen betreffen aber nur die Vorplätze des Hauptbahnhofs und des Vegesacker Bahnhofs. Zurzeit werden die Kosten für eine Videoüberwachungsanlage (mit einer Kamera) am Hauptbahnhof ermittelt und die Ausschreibung vorbereitet. Eine Realisierung ist für Mai 2002 vorgesehen. Sobald die Umsetzung sich konkretisiert, werde ich mich einschalten und die Einhaltung der oben beschriebenen gesetzlichen Voraussetzungen kontrollieren.

6.6. Elektronisches Vorgangsbearbeitungssystem der Polizei (EVA)

Ausgelöst durch die Anforderungen, die das zentrale polizeiliche Informationssystem beim BKA (INPOL-neu) an die polizeiliche Datenverarbeitung in den Ländern stellen würde, wurde in Bremen die Suche nach einem neuen Verfahren begonnen. Dass INPOL-neu nun nicht zum geplanten Zeitpunkt eingeführt wird und die Ergebnisse der im Bund in Auftrag gegebenen Machbarkeitsstudie noch nicht vorliegen, hat Bremen nicht davon abgehalten, den eingeschlagenen Kurs weiter zu verfolgen. Der Beschaffungsauftrag ist Ende des Berichtsjahres erteilt worden.

Seit Mitte 2001 berate ich eine Arbeitsgruppe „Datenschutzkonzept“ im Rahmen des Projektes „Elektronische Vorgangsbearbeitung“ der Polizeien Bremens (EVA-HB). Dieses System soll einerseits das weitgehend papierlose Arbeiten der Polizei und gleichzeitig die Einmalerfassung der Daten, die verantwortliche Speicherung der Daten wie auch den Abruf benötigter Daten durch die jeweiligen Polizisten ermöglichen. Das System EVA-HB soll dabei einerseits die laufenden Systeme ISA und ISA-D, als auch die verschiedenen, teilweise mit Standardsoftware selbst entwickelten Systeme auf den Polizeirevieren und in anderen Organisationseinheiten ablösen. Des Weiteren soll das neue System als „Anschluss- und Oberflächensoftware“ die Brücke zu den verschiedenen Zentralsystemen (INPOL, AZR, ZEVIS usw.) schlagen.

Das System ist unter den Vorgaben des neuen Polizeigesetzes, insbesondere des § 36 a BremPolG, zu konfigurieren, wonach die Polizeidaten für die

— Strafverfolgung nach der StPO,

— zur Erforschung von Ordnungswidrigkeiten,

— zur Gefahrenabwehr,

— zur Straftatenverhinderung und

— zum Schutz von Personen einschließlich des Umfeldes

erheben und verarbeiten darf. Dieses neue System wird bereits in der ersten Variante auch via PC bzw. Notebook verfügbar sein. Diese Rechner übertragen über eine definierte Schnittstelle Daten in das Gesamtsystem. Einige der PC bzw. Notebook tauschen dabei direkt mit dem Host (Standort: ID Bremen) Daten aus, die Mehrzahl kommuniziert mit dem Host über ein Netzwerk von Servern.

Grundvoraussetzung ist ein hoher Sicherheitsstandard. So sollen nicht nur die Daten zwischen den Servern und dem Host, sondern auch jede Information, die

ein Gebäude oder eine polizeiliche Einrichtung verlässt, stets verschlüsselt übertragen werden. Damit ist das neue System wesentlich komplexer als die z. T. nebeneinander stehenden bisherigen Anwendungen. Dies erfordert für die verschiedenen Aufgaben der Polizei die Gestaltung von dezidierten Berechtigungen und Berechtigungsgruppen inklusive der dafür jeweils notwendigen Sicherungsvorkehrungen. Des Weiteren dient EVA-HB einem stets aktuellen, klaren und situationsgerechten polizeilichen Lagebild. Ziel ist es, hinreichende, datenschutzrechtlich geforderte, differenzierte Vorkehrungen zur Wahrung der Datenschutzrechte der verschiedenen Betroffenengruppen (Beschuldigte, Zeugen, Opfer, Auskunftspersonen/Hinweisgeber, zu schützende Personen u. a.) zu schaffen. Auch musste eine große Zahl von gesetzlichen Löschungsregelungen implementiert werden. Ein weiterer Aspekt betraf die Verarbeitung der polizeilichen Daten auf den Rechnern der ID-Bremen GmbH und die Ausgestaltung der Aufsicht über die Aufgabenerledigung durch die ID-Bremen GmbH, an der die Stadtgemeinde Bremen beteiligt ist.

Zum Ende des Berichtsjahres wurde ein erster Abschluss der Konzeptionsarbeiten erreicht. Die Ergebnisse sind im ersten Halbjahr des kommenden Berichtsjahres noch einmal anhand der Ergebnisse der technischen und organisatorischen sowie der dv-technischen Umsetzungen zu überprüfen. Auch sind die Fortschreibungen des Betriebskonzeptes, des IT-Konzeptes, des Berechtigungskonzeptes zu berücksichtigen. Die neue Anwendung soll im Sommer 2002 in Betrieb gehen.

6.7. INPOL-neu läuft nicht

Bund und Länder arbeiten seit 1992 daran, den Landeskriminalämtern und den anderen Polizeidienststellen der Länder ein neues, leistungsfähiges und anforderungsgerechtes dv-gestütztes Informationssystem zur Verfügung zu stellen. Nach einer mehr als fünfjährigen Planungsphase befindet sich das Projekt „INPOL-neu“ nunmehr seit 1998 in einer Realisierungshase. Ziel war es, insbesondere weil einige Systeme die 2000-Problematik der Datumsumstellung (so genannter Millenium-Crash) nicht bewältigen konnten, das neue System zum Jahr 2000 flächendeckend in Betrieb zu nehmen. Zum Zeitpunkt des Eintritts in die Realisierungsphase erkannte man, dass für die Anbindung der Anwender in den Ländern nicht nur die Datenbankanwendung „INPOL-neu“ gestaltet werden musste, sondern auch eine „gemeinsame Anschluss- und Oberflächensoftware“ erforderlich war. Diese wurde in der Zwischenzeit entwickelt und getestet. Die vollständige Implementierung des Gesamtssystems „INPOL-neu“ sollte zum 31. Dezember 2003 abgeschlossen sein. Bei den Tests stellte sich heraus, dass das Antwortzeitverhalten unakzeptabel ist, es soll auch zu Systemabstürzen gekommen sein.

Darauf hat das Bundesinnenministerium im Einvernehmen mit den Ländern eine Unternehmensberatungsfirma mit einer Untersuchung der Anlauf- bzw. Performance-Schwierigkeiten beauftragt und Ende des Jahres zusätzlich ein großes Systemhaus mit weiteren Untersuchungen in diesem Zusammenhang beauftragt. Jüngsten Presseberichten zu Folge soll das Urteil vernichtend ausgefallen sein. Es sei bisher die größte Pleite, die es mit polizeilichen Computerprogrammen gegeben habe; die Entwicklung habe bisher alleine 115 Millionen Mark verschlungen. Das System sei nicht einsetzbar, der Einführungstermin könne nicht eingehalten werden. Neben dem erheblichen finanziellen Verlust, der auch durch die Verzögerung entsteht, war durch die lange Projektphase abzusehen, dass die Datenbanksysteme bereits bei Einführung veraltet sein würden. Inwieweit jetzt über längere Zeiten „Doppelsysteme“ gewartet und deren Daten gepflegt werden müssen, bleibt abzuwarten. Welche Auswirkungen diese Entwicklung auf das neu projektierte Info-System EVA-HB der Polizei im Land haben wird, ist noch nicht abzusehen.

Diese Entwicklung ist aus Sicht des Datenschutzes um so ärgerlicher, als auch die Datenschutzbeauftragten des Bundes und der Länder in nicht unerheblichem Umfang Arbeit in Datenschutzkonzepte für INPOL-neu gesteckt haben. Im Zusammenhang mit der Konzeption von INPOL-neu gab es eine Reihe datenschutzrechtlicher Probleme, die noch nicht alle zufriedenstellend gelöst werden konnten. Zu nennen sind Fragen der

— Auftragsdatenverarbeitung für die Länder durch das BKA, hier befürchten die Datenschutzbeauftragten u. a. dass die Trennung der Datenbestände zwi-

schen Bund und Ländern aufgeweicht werden könnte (vgl. auch Entschließung der Konferenz, 23. JB, Ziff. 17.7.) Dabei würde die Verfahrensvorschrift des § 2 Abs. 1 BKAG unterlaufen werden, wonach beim BKA nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung gespeichert werden dürfen.

— Protokollierung von Zugriffen auf eigene Dateien, die nicht für die Länder vom BKA vorgegeben werden kann.

— Verantwortung über die gespeicherten Daten, insbesondere dass diese in Bezug auf die Lösch- und Prüffristen bei den Ländern verbleibt.

— Zugriffsmöglichkeiten, die differenziert zu halten sind.

6.8. Modernisierung des Funknetzes

Die Ereignisse um den Terroranschlag in New York hat den Sicherheitsbehörden einschließlich Rettungsdienst und Katastrophenschutz deutlich vor Augen geführt, wie notwendig es ist, ein sicheres und unabhängiges Kommunikationsmittel zur Bewältigung solcher oder vergleichbarer Lagen vorhalten und nutzen zu können. Es hat sich gezeigt, dass, selbst wenn von der rechtlichen Möglichkeit des Abschaltens privater Nutzer Gebrauch gemacht wird, die öffentlichen Netze nicht die Bedürfnisse der Sicherheitsbehörden abdecken können.

Es ist zu erwarten, dass ein solches Kommunikationsmittel für die Sicherheitsbehörden europaweit konzipiert werden soll. Die bisherigen Planungen haben durch die Terroranschläge eine erhebliche Belebung erfahren. So haben die zuständigen Gremien einen Zeitplan für das weitere Vorgehen festgelegt. Die Erfahrungen aus den Anschlägen werden zurzeit ausgewertet, eine Ausschreibung (ca. Dezember 2002) für ein digitales Funknetz vorbereitet und eine Vergabe für Juli 2003 geplant.

Hierbei sind natürlich auch Datenschutzaspekte zu berücksichtigen. Es ist ein sicheres und auch abhörsicheres digitales Kommunikationsmittel zu wählen, das es ermöglicht, die Informationen (Sprache, Daten, Bilder, usw.) ohne Beeinträchtigungen auszutauschen. Ich werde zusammen mit den anderen Datenschutzbeauftragten beraten, wie dieses Projekt begleitet werden kann.

6.9. Stadtamt-Zentrales Bürgeramt in der Pelzerstraße

Wie aus der Presse bekannt, plant der Senator für Inneres, Kultur und Sport seit längerer Zeit auf der Basis eines Gutachtens ein Zentrales Service-Center (ZCC) in der Innenstadt (Pelzerstraße). Die konzeptionelle Planung ist im Wesentlichen abgeschlossen. Diese Planungen habe ich schon sehr früh datenschutzrechtlich begleitet.

In dem ZCC soll ein System von Arbeitsplätzen geschaffen werden, an denen Bürger ihre gesetzlichen Pflichten und Anliegen möglichst durch einmaligen Kontakt mit der Verwaltung erledigen können. So sollen im ZCC folgende wesentliche Verwaltungsleistungen angeboten werden:

— An-, Um- und Abmeldungen im Meldebestand,

— Ummeldungen im Kfz-Register bei Umzügen innerhalb der Stadt,

— Gewerbean-, um- und -abmeldungen,

— Anträge auf Erstellung eines (polizeilichen) Führungszeugnisses an das Bundeszentralregister,

— Anträge auf Auskunft aus dem Gewerbezentralregister,

— Ausstellung von Fischereischeinen,

— Pass- und Ausweisanträge,

— Ausstellung von Steuerkarten als Landesfinanzbehörde.

Für die vorstehend genannten Aufgaben war auch bisher das Stadtamt zuständig, deshalb ergeben sich daraus noch keine grundsätzlichen datenschutzrechtlichen Bedenken gegen eine Zusammenfassung dieser Verwaltungsvorgänge in einer zentralen Stelle bzw. an einem Arbeitsplatz. Allerdings gilt diese Aussage hinsichtlich der datenschutzrechtlichen Unbedenklichkeit nur, soweit der betroffene Bürger — nach hinreichender Information — selbst den Umfang der zentralen Dienstleistung bestimmen kann. Darüber hinaus müssen flankierend technische und organisatorische Maßnahmen getroffen werden. Diese Maßnahmen beziehen sich auf die Protokollierung der DV und die Diskretion an den einzelnen Arbeitsplätzen, die einen ausreichenden Abstand der einzelnen Sachbearbeiterplätze und eine abschirmende Raumgestaltung erfordert. Dies gilt auch für die Info-Theke, an der sich die Bürger/-innen einen qualifizierten Rat holen, Sprechzeiten buchen oder sich erforderliche Vordrucke und Info-Blätter aushändigen lassen können. Schließlich ist sicherzustellen, dass nur dann, wenn der Bürger beim Sachbearbeiter im ZCC vorstellig wird, zu diesem Betroffenen Datensätze aufgerufen werden und zwar nur im Umfang der nachgefragten Serviceleistung.

Verwaltungsleistungen, die einem besonderen Amts- oder Berufsgeheimnis unterliegen, wie z. B. die Entgegennahme einer Steuererklärung, die Eintragung eines Steuerfreibetrages in die Steuerkarte oder die Beantragung von Erziehungsgeld, werden von dem ZCC ebenfalls angeboten, allerdings in speziellen Räumlichkeiten des jeweils zuständigen Amtes (Finanzamt oder Amt für soziale Dienste) und mit eigenen Mitarbeitern als „Shop-in-Shop-Lösung“. Diese Beschäftigten haben natürlich nur Zugang zu ihren speziellen DV-Systemen.

6.10. Neues DV-System in den Ausländerämtern Bremen und Bremerhaven

Auf der Grundlage des Ausländergesetzes haben die Ausländerämter in Bremen und Bremerhaven das DV-System „ADVIS“ eingeführt. Dieses System habe ich technisch geprüft. Ein Datenschutzkonzept, das die Arbeit mit dem DV-System regelt, steht für beide Ämter noch aus. Während für das Ausländeramt Bremen mir ein Entwurf bereits vorliegt, haben die Arbeiten an einem Entwurf in der Ausländerbehörde Bremerhaven erst begonnen.

6.11. Feuerwehr — Neues DV-System im Rettungsdienst

Die Berufsfeuerwehr Bremen hat im Herbst des Berichtsjahres ein neues DV-System für den Rettungsdienst eingeführt. Dieses System wird bereits bei Rettungsdiensten anderer — meist kleinerer — Einrichtungen eingesetzt und wurde den Bedürfnissen und Besonderheiten Bremens angepasst.

Die Entwicklung und Einführung des DV-Systems habe ich beraten. Grundlage dabei waren die datenschutzrechtlichen Bestimmungen des Brandschutzgesetzes vom 7. Mai 1991 (insbesondere §§ 35 ff.) und des Rettungsdienstgesetzes vom 22. September 1992 (insbesondere §§ 14 ff.), aber auch der Entwurf des Bremischen Hilfeleistungsgesetzes, der sich zurzeit in der Endabstimmung befindet. Das neue DV-System genügt den genannten Vorschriften. Schwerpunkt meiner datenschutzrechtlichen Beratung war, eine klare Zweckbindung der bei jedem Hilfeeinsatz anfallenden umfangreichen Daten, die in die Dokumentation einfließen, wie Patientendaten, Einsatzdaten, Kostenträger oder eingesetzte Kräfte und Mittel sicherzustellen.

In der Einführungsphase musste noch eine Zugriffsregelung für die Rettungsstationen und -wachen geschaffen werden, weil sie nach jedem Einsatz für eine gewisse Zeit Dokumentationsdaten (s. o.) eingeben müssen. Es wurde festgelegt, dass sie nur und so lange auf „ihre“ Daten (ihre Einsatzdaten) Zugriffsrechte haben, bis der Vorgang abgeschlossen ist. Dies ist spätestens der Fall, wenn der Einsatz abgerechnet worden ist. Danach ist ein Zugriff nur noch auf anonymisierte Daten möglich.

6.12. Meldewesen

6.12.1. Änderung des Bremischen Meldegesetzes

Der bremische Gesetzgeber hat im Berichtsjahr die lange überfällige Änderung des BremMG beschlossen (Brem.GBl. v. 2. November 2001, S. 347). Sie ist ohne Übergangsfrist Anfang dieses Jahres in Kraft getreten. Das Fehlen einer Über-

gangsvorschrift dürfte für die Umsetzung der neuen Regelungen erhebliche Probleme aufwerfen. Eine zeitgerechte Anpassung der beiden automatisierten Einwohnerverfahren (DEMOS in Bremen und Meso 96 in Bremerhaven) ist nicht möglich mit der Folge, dass die bremischen Meldebehörden in Umsetzungsverzug geraten.

6.12.2. Änderung der Bremischen Meldedatenübermittlungsverordnung

Im November des Berichtsjahres übersandte mir der Senator für Inneres, Kultur und Sport einen Entwurf zur Änderung der Meldedatenübermittlungsverordnung. Dem bremischen Landesamt für Verfassungsschutz (LfV) sollen damit automatisierte Online-Abrufrechte aus den Datenbeständen der Einwohnermeldeämter Bremens und Bremerhavens im Rahmen der Extremismus- und Terrorismusbekämpfung eingeräumt werden.

Das LfV begründete die Notwendigkeit im Wesentlichen mit der Häufigkeit der telefonischen Anfragen und der von ihm erwartetem Arbeitserleichterung, weiter seien nicht zuletzt wegen der aktuellen Sicherheitslage (11. September 2001) Personenfeststellungen und -überprüfungen, Abrufe/Abfragen beim Einwohnermeldeamt auch außerhalb der Dienstzeit der Meldeämter im Zusammenhang mit Ermittlungen und Observationen erforderlich.

Der Verfassungsschutz konnte schon immer z. B. per Telefon Einzelabfragen aus den Meldedatenregistern des Landes tätigen. Den Online-Zugriff des Verfassungsschutzes auf die Meldedatenregister aber habe ich über Jahre verhindert, weil ein unkontrollierter und intensiverer Zugriff von mir befürchtet wurde. Neben der Lösung des Problems der Nachtabfrage — die Einwohnermeldeämter sind dann nicht besetzt — haben mich zwei wesentliche Aspekte nunmehr dazu bewegt, meinen Widerstand aufzugeben:

— Ich konnte erreichen, dass jede automatisierte Abfrage aus den Melderegistern entsprechend § 6 Abs. 3 BremVerfSchG nicht manuell, sondern zwingend automatisiert protokolliert wird. Dadurch, dass alle Abrufe des Landesamtes für Verfassungsschutz aus dem DEMOS-System lückenlos aufgezeichnet werden, kann nunmehr von mir jede Abfrage und damit auch die Verwendung dieser Daten umfassend kontrolliert werden.

— Durch einen automatisierten Online-Abruf von Meldedaten wird vermieden, dass Mitarbeiter der Einwohnermeldeämter über die Befassung des Verfassungschutzes mit einer bestimmten Person Kenntnis erlangen, ein wesentlicher Datenschutzfortschritt.

Ich habe daher neben einer automatisierten Protokollierung und einer kleinen Einschränkung des zur Übermittlung freigegebenen Datensatzes, der sich auf die Übermittlung minderjähriger Kinder beim Abruf der Elterndaten bezog, keine weiteren Forderungen oder Einwände zur Einrichtung des Abrufverfahrens erhoben. Die MeldDÜV ist mittlerweile in Kraft getreten (Brem.GBl. 28. Januar 2001, S. 2)

6.12.3. Änderung des Melderechtsrahmengesetzes

Die im Jahr 2000 angelaufenen Arbeiten an einer erneuten Änderung des Melderechtsrahmengesetzes (MRRG) auf Bundesebene wurden im Berichtsjahr forciert. Derzeit befindet sich die dritte Novelle zur „Änderung des MRRG und anderer Gesetze“ im Deutschen Bundestag zur Beratung; das Gesetzgebungsverfahren soll noch in diesem Jahr, d. h. vor Ablauf der laufenden Legislaturperiode abgeschlossen werden. Mit der erneuten Änderung des MRRG sollen die erforderlichen Rahmenbedingungen für die Nutzung moderner Informations- und Kommunikationstechnologien geschaffen und einzelne Meldepflichten abgeschafft werden. So ist z. B. vorgesehen, die elektronische Anmeldung zu erlauben, den Betroffenen einen elektronischen Zugang zu den eigenen, im Melderegister gespeicherten Daten zu ermöglichen und die elektronische Datenübermittlung auch in den privaten Bereich hinein zulassen. Außerdem ist vorgesehen, die Abmeldepflicht bei inländischen Umzügen und die Mitwirkungspflicht des Wohnungsgebers beim Meldevorgang abzuschaffen. Mit dieser Gesetzesnovelle wird das MRRG, das ja Rahmenrecht für die einzelnen Landesmeldegesetze ist,

umfangreich in Richtung auf eine Öffnung der Melderegister zur Nutzung von Internet-Diensten umgestaltet. Ob die vorgesehene Ausweitung des Widerspruchrechts der Betroffenen gegen eine Datenweitergabe begrenzend wirken kann, ist angesichts der Bekanntheit und Nutzung bisheriger Widerspruchsrechte höchst zweifelhaft.

Der bremische Gesetzgeber muss die dritte Änderungsnovelle zum MRRG spätestens zwei Jahre nach ihrer Verkündung in Landesrecht umsetzen, eine neuerliche Änderung des Bremischen Meldegesetzes (BremMG) steht also ins Haus.

6.12.4. Einwohnerverfahren Meso 96 in Bremerhaven

Im Berichtsjahr habe ich — wie angekündigt — die in den Vorjahren begonnene Überprüfung des neuen DV-Verfahrens Meso 96 der Meldebehörde Bremerhaven (vgl. 23. JB, Ziff. 6.3.4.) fortgesetzt. Die von mir seinerzeit festgestellten Defizite und Mängel insbesondere im Bereich der regelmäßigen Übermittlung von Meldedaten sollten nach den mir in der Zwischenzeit zugegangenen Informationen ausgeräumt worden sein. Bei ihrer Überprüfung zeigte sich jedoch, dass dies nur z. T. der Fall war. So fehlen mir nach wie vor, z. B.

— exaktere Beschreibungen der im Meso 96-Verfahren verarbeiteten Meldedaten (Datensatzbeschreibungen und eine Beschreibung der Datenbank-/Dateienstruktur). Die mir übersandte Dateibeschreibung/Meldung zum Dateienregister stimmte mit den Datenmasken und Listausdrucken datenmäßig nicht überein,

— nähere Informationen über das neue Zugriffsverfahren MIA, das alle Online-Zugriffe der zum Magistrat gehörenden berechtigten Stellen auf das Melderegister steuert und protokolliert,

— nähere Informationen über die Nutzung der im Meso 96-Verfahren enthaltenen Wahlkomponente (Wählerverzeichnis, Zugriffsberechtigung) und

— eine vollständige Übersicht über angeschlossene bzw. zugeordnete Terminals/PC. Auch das übersandte Geräteverzeichnis war unvollständig.

Die mir übersandten Unterlagen zu den regelmäßig stattfindenden Übermittlungen aus dem Melderegister stimmten trotz Korrektur teilweise immer noch nicht mit den melderechtlichen Vorgaben überein. Auch die Führung der Kommunalstatistik und der Datenfluss zum Statistischen Landesamt Bremen im Zusammenhang mit der Bevölkerungsstatistik waren unklar.

Das Verfahren Meso 96 war zum Prüfungszeitpunkt seitens der Stadt Bremerhaven noch nicht abgenommen. Deshalb wurde vereinbart, über die Defizite und melderechtlichen Abweichungen einen gemeinsamen Vermerk zu erstellen, der als Anforderung für eine Anpassung des Meso 96-Verfahrens gegenüber dem Softwarelieferanten dienen soll. Dabei müssen dann auch die Anforderungen des novellierten BremMG und der geänderten BremMeldDÜV berücksichtigt werden. Es besteht ferner Einvernehmen, dass mir die fehlenden Unterlagen bzw. Informationen zur Verfügung gestellt und die offenen bzw. unklaren Handhabungsfragen geklärt werden. Die Prüfung des Meso 96-Verfahrens ist für mich damit vorerst beendet. Die klärungsbedürftigen Punkte werde ich weiter verfolgen.

6.12.5. MEDIA@Komm-Projekt

Im Berichtsjahr habe ich mich auf Wunsch der Projektbeteiligten an einem Beratungsgremium (Abstimminstanz) am Projekt „Fachkonzept Schnittstellen für das Einwohnermeldewesen“ beteiligt. Bei diesem vom Bund geförderten, speziellen MEDIA@Komm-Projekt geht es darum, für das Einwohnermeldewesen allgemein Lösungen und Strukturen zu finden, die es ermöglichen, Internet-Techniken und die digitale Signatur zu verwenden. Die Kommunikation zwischen Bürgern und Meldebehörde soll elektronisch unterstützt werden. Die vorhandenen automatisierten Verfahren des Einwohnermeldewesens sollen hierbei weitgehend unangetastet bleiben.

Das Beratungsgremium (Abstimminstanz) hat sich im Berichtsjahr mit dem so genannten Informationsmodell und einem Prozessmodell beschäftigt. Das Infor-

mationsmodell versucht die so genannten Informationsobjekte und ihre Beziehungen zueinander sowie strukturelle und syntaktische Änderungen des Datensatzes für das Meldewesen, einen neuen Datensatz „Xmeld“ festzulegen. Das Prozessmodell versucht die Kommunikationsprozesse abzubilden, bei denen der Bürger mit der Meldebehörde in Kontakt tritt (z. B. Anmeldung, Umzug, Melderegisterauskunft). Einige wenige Prozesse dieser Art wurden beispielhaft strukturiert.

Die Beratungsergebnisse der Abstimminstanz werden einer Entscheidungsinstanz vorgelegt. Das Beratungsgremium hat im Berichtsjahr zweimal getagt. Im Hinblick auf die MEDIA@Komm-Projekte in Bremen und die maßgebliche Beteiligung der Bremen Online Services GmbH & Co. KG (BOS) sowie in Hinblick auf die zukünftigen gesellschaftlichen Entwicklungen ist meine beratende Beteiligung von Nutzen.

6.12.6. Bundestagswahl 2002

Acht Monate vor der Bundestagswahl (am 22. September 2002) müssen die Meldebehörden durch öffentliche Bekanntmachung die stimmberechtigten Bürger darauf hinweisen, dass sie der Weitergabe ihrer Daten an die politischen Parteien widersprechen können. Diese Frist wird im Februar 2002 erreicht.

Im Datenschutzausschuss der Bremischen Bürgerschaft war seinerzeit seitens der Innenbehörde darüber hinaus zugesagt worden, die Information über das Widerspruchsrecht der Betroffenen im Meldeverfahren zu verbessern. In der neuen Verordnung über die Muster der Meldescheine vom Dezember des Berichtsjahres ist die zugesagte Informationsverbesserung in der Gestalt realisiert worden, dass folgender Hinweis aufgenommen worden ist: „WICHTIGER HINWEIS!! Beachten Sie bitte die Hinweise zur kostenfreien Eintragung von Datenübermittlungs- und Auskunftssperren auf dem Vorblatt“. Auf dem Vorblatt zur Anmeldung befindet sich ein Absatz zu Auskunftssperren und ein Absatz zu den im Zusammenhang mit den Wahlen interessierenden Datenübermittlungssperren. Dort ist in Fettdruck folgender Satz aufgenommen worden: „Falls Sie eine Übermittlungssperre wünschen, hält die Meldestelle Vordrucke für eine entsprechende Erklärung bereit. Die Erklärung kann aber auch formlos abgegeben werden.“

Positiv gewendet also zwei Hinweise an verschiedenen Stellen im Formular, negativ gewendet ein Hinweis auf einen Hinweis zur Erlangung eines Vordruckes. Falls man dann noch jeweils eine Wartemarke zu Empfang und Abgabe dieses Vordruckes ziehen muss, würde dies noch weniger zur Erleichterung der Rechtswahrnehmung beitragen. Wäre es da nicht einfacher, statt der Aufzählung der einzelnen Möglichkeiten einer Übermittlungssperre im Vorblatt gleich ein Kästchen für die Entscheidung des Bürgers vorzusehen, das zusammen mit dem Meldeformular abgegeben werden kann?

7. Justiz

7.1. Prüfung des Justiznetzes

Im Berichtsjahr habe ich das Justiznetz des Senators für Justiz und Verfassung geprüft. Betreiber des Justiznetzes ist der Landesbetrieb Justiz-Dienstleistungen der Freien Hansestadt Bremen (JUDIT Bremen). Gegenstand der Prüfung waren u. a. die physikalische und logische Struktur des Justiznetzes, dessen Anbindung an das Bremische Verwaltungsnetz (BVN), die verfügbaren Dienste und Server im Justiznetz sowie die Administration des Justiznetzes.

Das Justiznetz ist ein weitgehend sternförmiges Netz aus 22 verschiedenen Standorten in Bremen und Bremerhaven. Zentraler Punkt dieses Netzes ist ein sehr leistungsfähiger Switch, der nicht nur die 22 verschiedenen Standorte in virtuelle LAN unterteilt, sondern gleichzeitig auch als Einwahlrouter in das BVN dient.

Der zentrale Switch ist so konfiguriert, dass Übergänge von einem Standort zum anderen nur in Ausnahmefällen zugelassen sind. Standortübergreifende Zugriffe auf Server anderer Bereiche werden explizit auf Routerebene freigegeben. Eine differenzierte Freischaltung bzw. Sperrung einzelner Dienste erfolgt allerdings nicht, so dass im Rahmen von freigeschalteten Verbindungen gleich sämtliche auf den Rechnern verfügbaren Dienste standortübergreifend verfügbar sind. Um die Sicherheit zusätzlich zu erhöhen, habe ich empfohlen, im Rahmen freigeschalteter Verbindungen nur die jeweils benötigten TCP/IP-Dienste freizugeben und alle

anderen Ports entsprechend zu filtern. Dies wird inzwischen von JUDIT Bremen umgesetzt.

Die Datenübertragung im Justiznetz erfolgt unverschlüsselt, sofern nicht auf Anwendungsebene entsprechende Mechanismen umgesetzt werden. Somit besteht das Risiko, dass die unverschlüsselten Daten sowohl von Mitarbeitern des Betreibers des Justiznetzes als auch von Mitarbeitern des Telekommunikationsbetreibers mitgelesen werden; dies gilt insbesondere für Client-Server-Verbindungen zu entfernten Standorten, beispielsweise zum Amtsgericht Bremerhaven. Auf meine Anregung hin wurde bei JUDIT Bremen ein Pilotprojekt gestartet, das die zwischen Bremen und Bremerhaven übertragenen Daten per IPSec verschlüsselt. Die hierbei gemachten Erfahrungen sollen anschließend dazu genutzt werden, auch andere Übertragungswege per IPSec zu verschlüsseln.

Der Landesbetrieb Justiz-Dienstleistungen hat inzwischen auch eine von mir schon seit längerem geforderte Dokumentation sowohl des Netzes selbst als auch der jeweiligen Anwendungen im Justiznetz vorgelegt. Eine abschließende Bewertung habe ich noch nicht vorgenommen.

7.2. EUROJUST

Nach Europol nun EUROJUST: Mit dem Ratsbeschluss vom 14. Dezember 2000 (Abl.L 324, 21/12/2000, S. 2) ist eine gemeinsame Stelle zur justiziellen Zusammenarbeit aller Mitgliedstaaten der EU verabredet worden. Am 1. März 2001 nahm die neue Behörde „PRO EUROJUST“ mit 16 Staatsanwälten aus den Mitgliedstaaten in Brüssel die Arbeit auf. Vorläufiges Ziel ist es, die Koordinierung der Ermittlungs- und Strafverfolgungsmaßnahmen im Bereich schwerer grenzüberschreitender Kriminalität zu erleichtern und die Zusammenarbeit der Strafverfolgungsbehörden zu effektivieren. Zunächst ist „PRO EUROJUST“ eine Zentrale für Verbindungsstaatsanwälte und -richter, die sich gegenseitig austauschen und zu den Stellen im eigenen Land leichter Verbindungen herstellen können. Ihnen wurden hierfür keine besonderen Befugnisse eingeräumt, sie dürfen nur nach Maßgabe des Rechts des jeweiligen Entsenderstaates handeln. Zurzeit ist die Bundesrepublik dort mit je einem Repräsentanten der Bundesstaatsanwaltschaft und einem Staatsanwalt aus NRW vertreten.

„PRO EUROJUST“ ist, wie der Name schon vermuten lässt, lediglich ein Vorläufer einer späteren größeren europäischen Behörde namens „EUROJUST“. Die Festlegungen für die Ziele dieser europäischen Behörde wurden auf der Tagung des Europäischen Rates vom 15./16. Oktober 1999 in Tampere getroffen. Die Europäische Kommission unterstützt die Einrichtung (vgl. Mitteilung der Kommission vom 22. November 2000, Com[2000]746). Es ist beabsichtigt, EUROJUST mit erweiterten Kompetenzen auszustatten.

Ich habe mich zusammen mit anderen Landesbeauftragten durch einen Vertreter des BMJ über Aufbau und Ziele der Behörde im AK Justiz der Datenschutzbeauftragten unterrichten lassen und werde die Entwicklung unter datenschutzrechtlichen Gesichtspunkten weiter verfolgen. Die Konferenz der Datenschutzbeauftragten hat zur aktuellen Entwicklung einen im Anhang dieses Berichts beigefügten Beschluss gefasst (vgl. 15.17. dieses Berichts).

7.3. Justizielle Verzeichnisse im Internet

Im Berichtsjahr waren rege Aktivitäten zu verzeichnen, die Justiz durch Internetanwendungen zu entlasten und durch Internetanbindungen von justiziellen Verzeichnissen und Unterlagen bei Dritten Einkünfte zu erzielen. Ich habe mich in diesem Zusammenhang nicht darauf beschränkt, solchen Projekten gegenüber nur ablehnend gegenüber zu stehen, sondern habe auch Vorschläge unterbreitet, wie unter Einhaltung des Datenschutzes neue Verfahren und rechtliche Regelungen konzipiert werden können.

7.3.1. Daten über Zwangsversteigerung abrufbar übers Internet

In einer Anfrage eines privaten Verzeichnisdienstes aus Bremen wurde ich um Auskunft gebeten, ob bei den Gerichten vorliegende Wertgutachten über Immobilien, die zwangsversteigert werden sollen, im Internet veröffentlicht werden dürfen. Da gerade die Schuldner ein hohes Interesse an einer breiten Anpreisung

zum Zwecke einer besseren Verwertung haben werden, würde eine solche öffentliche Information in vielen Fällen sicherlich gewünscht. Einer Veröffentlichung mit Einwilligung, wobei der Name des Schuldners nicht zu erscheinen bräuchte, stünde insoweit nichts im Wege.

Allerdings kann das Vollstreckungsgericht nicht von sich aus alle Wertgutachten an eine private Stelle weitergeben. Entscheidende Hürde sind die Vorschriften der §§ 37 ff., 42 ZVG, die lediglich die Einsichtnahme im Einzelfall erlauben. Hier könnte eine Modernisierung des Rechts Abhilfe schaffen, wobei die Gerichte selbst diesen Service anbieten könnten. Es gibt darüber hinaus eine Diskussion zur Veröffentlichung von Zwangsversteigerungsterminen im Internet, worauf ich an dieser Stelle nur hinweisen möchte.

7.3.2. Verbraucherinsolvenzen im Internet

Im Bereich der Veröffentlichung insolvenzrechtlicher Daten ist der Gesetzgeber schon erheblich weiter. Die mit einer Veröffentlichung der Daten eines Insolvenzschuldners verbundene Prangerwirkung im Internet ist gegenüber einer einmaligen Bekanntmachung in der lokalen Zeitung ungleich größer. Verbindet man die Vorstellung noch damit, dass solche Daten auch lange nach Löschung im Insolvenzverzeichnis noch im Internet aufgefunden werden können, weltweit abrufbar sind und unkontrolliert weiterverwendet werden können, so schrillen die Alarmglocken beim Datenschutz. Dabei ist die Zahl derer, die für ein Insolvenzverfahren in Betracht kommen, unerwartet hoch. Presseberichten zu Folge muss jeder 25. Bremer eine eidesstattliche Versicherung (Offenbarungseid) ablegen. Diese und verschiedene andere Faktoren haben mich dazu bewegt, einer ungesteuerten Verfügbarmachung dieser Daten im Internet entscheidend entgegenzutreten. In diesem Sinne habe ich mich auch in der Konferenz der Datenschutzbeauftragten entscheidend eingesetzt. Eine genauere Beschreibung der Gefahren findet sich für den interessierten Leser in dem im Anhang zu diesem Jahresbericht beigefügten Beschluss der Datenschutzkonferenz (vgl. Ziff. 15.8. dieses Berichts).

Diese Überlegungen sind vom Justizministerium aufgegriffen worden. Die Einzelheiten der Veröffentlichung insolvenzrechtlicher Daten im Internet werden nach in Kraft treten der Änderungen in der Insolvenzordnung (vgl. BR-Drs. 689/01) am 1. Dezember 2001 nun in einer Verordnung geregelt (vgl. BR-Drs. 1082/01). Die Verordnung zielt in dem vorstehend aufgezeigten Rahmen darauf ab, personenbezogene Daten während der Verarbeitung unversehrt, vollständig und aktuell zu halten und sicherzustellen, dass diese Daten jederzeit ihrem Ursprung zugeordnet werden können (§ 2 Abs. 1 Satz 1 Nrn. 1 und 2 der Verordnung). Ferner wird — im Rahmen des technisch Möglichen — ein Kopierschutz angestrebt (§ 2 Abs. 1 Satz 1 Nr. 3 der Verordnung). Der Zugriff auf die in das Internet gestellten Daten darf während der ersten zwei Wochen nach dem Tag der Erstveröffentlichung uneingeschränkt erfolgen. Danach ist ein Abruf nur noch unter eingeschränkten Voraussetzungen möglich (§ 2 Abs. 1 Satz 1 Nr. 4 der Verordnung). Weiterhin werden der Zeitpunkt der Löschung der Daten (§ 3 der Verordnung) und durch § 4 der Verordnung die unentgeltliche Kenntnisnahme der öffentlichen Bekanntmachungen in angemessenem Umfang geregelt.

7.3.3. Vorbereitung anderer Verzeichnisse fürs Internet

Das Justizministerium hat eine Bund-Länder-Arbeitsgruppe beauftragt zu prüfen, welche Dienste und Verzeichnisse noch als Internetanwendungen angeboten werden können. Neben der Vorbereitung zur Öffnung des Handelsregisters sind u. a. die Einsicht in das Grundbuch und die Beantragung sowie die Bearbeitung von Mahnanträgen Gegenstand der Erörterung gewesen. Über die konkrete Entwicklung in Bremen berichte ich unter Ziff. 3.4. dieses Berichts.

8. Gesundheit und Krankenversicherung

8.1. Zugriff auf Patientendaten in Krankenhausinformationssystemen

8.1.1. DV-Prüfung Zentralkrankenhaus Bremen-Ost

Die im Jahr 2000 begonnene SAP-Prüfung in den bremischen Krankenhäusern wurde im vergangenen Jahr mit einer Prüfung im Zentralkrankenhaus Bremen-

Ost fortgesetzt. Obwohl die Ergebnisse der anderen Krankenhaus-Prüfungen (vgl. 23. JB, Ziff. 8.1.) vermutlich auch im ZKH Bremen-Ost bekannt waren, wurden auch hier die bisher festgestellten Schwachstellen deutlich:

Zugriffsrechte für die Verwaltung und für Externe: Das SAP-Berechtigungskonzept wies gravierende Mängel auf. Das mir zuvor zugeleitete Berechtigungskonzept war nicht umgesetzt worden. Insbesondere besaßen insgesamt 14 Mitarbeiterinnen und Mitarbeiter aus der Verwaltung und von externen EDV-Dienstleistern das Profil SAP_ALL, das zum uneingeschränkten Zugriff auf sämtliche im System gespeicherte Patientendaten berechtigt. Darüber hinaus war es möglich, direkt im Produktivsystem Änderungen vorzunehmen.

Ich habe Ende Oktober 2001 der Leitung des Zentralkrankenhauses Bremen-Ost meinen Prüfbericht zugeleitet und sie aufgefordert, die Mängel zu beseitigen. Kurz vor Redaktionsschluss erhielt ich ein überarbeitetes Berechtigungskonzept mit der Zusage, die meisten meiner Forderungen würden aufgegriffen.

Zugriffsrechte für Ärzte und Pflegekräfte: Im ZKH Bremen-Ost wurde zum Zeitpunkt der Prüfung zwar noch nicht das Modul IS-H*MED zur Dokumentation der ärztlichen Behandlung eingesetzt, jedoch das Modul IS-H, in dem auf den Stationen z. B. die Diagnosen und die Prozeduren (z. B. Operationen) gespeichert werden. Die Zugriffsregelung auf der Ebene von IS-H entspricht ebenso wie in den anderen geprüften Krankenhäusern nicht den Anforderungen des Bremischen Krankenhausdatenschutzgesetzes (KHDSG). Danach sind abteilungsübergreifende Zugriffe nur zulässig, soweit sie zur Wahrnehmung bestimmter im Einzelnen im Gesetz aufgeführter Aufgaben, insbesondere zur Erfüllung des Behandlungsauftrags, erforderlich sind. Zugriffe auf die Dokumentation einer abgeschlossenen Behandlung sind gleichfalls i. d. R. damit zu begründen, dass sie für die Erfüllung eines neuen Behandlungsauftrags erforderlich sind. Bei automatisierter Speicherung sind Onlinezugriffe zu sperren.

Die Realität in den Krankenhäusern, in denen Patientendaten mit Hilfe von IS-H oder IS-H*MED auf der Grundlage von SAP verarbeitet werden, sieht hingegen anders aus:

— Ärzte haben lesenden und schreibenden Zugriff auf diese Daten sowohl bei Patienten ihrer eigenen Station als auch der anderer Stationen.

— Ärzte, Pflegepersonal und Mitarbeiter der Aufnahme können sowohl auf die Daten aktuell behandelter Patienten als auch auf die Daten von Patienten zugreifen, deren Behandlung abgeschlossen ist.

Auf meine Aufforderung hin, ihre Informationssysteme den gesetzlichen Anforderungen anzupassen, äußerten sich die drei geprüften Krankenhäuser zunächst ablehnend und führten als Begründungen an, der unbegrenzte Zugriff von Ärzten und Pflegepersonal auf die Daten aller derzeitigen und ehemaligen Patienten sei medizinisch und organisatorisch unverzichtbar und SAP bzw. die auf das System aufgesetzten Module sähen entsprechende Begrenzungen der Zugriffe nicht vor.

Diesen Stand der Auseinandersetzung geben mein 23. Jahresbericht und die zu ihm durch den Senat abgegebene Stellungnahme wieder.

Inzwischen aber habe ich die Probleme in zwei Workshops mit Ärzten, Technikern und Datenschutzbeauftragten der beteiligten Krankenhäuser sowie mit Vertretern von SAP und von deren Kooperationspartnerin GSD (Gesellschaft für Systemforschung und Dienstleistungen im Gesundheitswesen) konstruktiv erörtert. Dort akzeptierten die Vertreter der Krankenhäuser, dass auch Ärzte auf die ärztliche Dokumentation nicht unbegrenzt, sondern nur unter bestimmten, rechtlich definierten Voraussetzungen zugreifen dürfen. Zugleich war man sich darin einig, dass der Behandlungsauftrag zentraler Gesichtspunkt sein müsse: Die für die Behandlung erforderlichen Zugriffe müssten eröffnet, hierfür nicht erforderliche Zugriffe hingegen verhindert werden. GSD jedenfalls legte nach dem ersten Workshop ein aktuelles Papier vor, das genau hierfür technische Lösungen (Stichwort „Behandlungsauftrag als dynamische Berechtigung“) vorschlägt, die in die eingesetzten Systeme implementiert werden können. Im zweiten Workshop wurden einvernehmlich Modifikationen und Präzisierungen entwickelt, die an GSD herangetragen werden sollen.

Auf Kritik sowohl seitens der Krankenhäuser als auch meinerseits ist gestoßen, dass die SAP-Vertreter sich gegenüber entsprechenden Bitten um Weiterentwicklung ihres Systems eher reserviert zeigten. Allenfalls wollten sie die Frage in eine noch zusammen mit Vertretern von Krankenhausträgern zu gründende bundesweite Arbeitsgruppe abschieben. Die Umsetzung des bisherigen Diskussionsstandes gegenüber SAP und in den Krankenhäusern soll im Februar 2002 in einem dritten Workshop erörtert werden sollen.

8.1.2. Fortschreibung des Krankenhausdatenschutzgesetzes

Als das Krankenhausdatenschutzgesetz (KHDSG) in 1989 verabschiedet wurde, wurde die ärztliche Behandlung noch durchweg auf Papier dokumentiert, mit der Folge, dass im Regelfall die Dokumentation lediglich in einem Exemplar verfügbar war. Die digitalisierte Verarbeitung der Behandlungsdaten eröffnet die Verfügbarkeit der Daten im gesamten Netz. Angesichts der besonderen Schutzbedürftigkeit dieser Daten und der ärztlichen Schweigepflicht sollte das Gesetz den damit verbundenen Risiken, aber auch den damit verbundenen Vorteilen für die medizinische Behandlung Rechnung tragen.

Ich hatte bereits auf Grund der Erfahrungen der ersten Prüfbesuche dem Senator für Gesundheit Vorschläge zur Fortschreibung des KHDSG vorgelegt. Nachdem von diesem die Bereitschaft erklärt worden war, meinen Vorschlag aufzunehmen, haben nach den Beratungen meines 23. Jahresberichts im Datenschutzausschuss jetzt die Fraktionen von SPD und CDU einen entsprechenden Antrag in die Bürgerschaft (Landtag) eingebracht.

8.2. Vernetzung des Gesundheitsamtes Bremen

Nachdem das mir vorgelegte Datenschutzkonzept für das amtsinterne Netz des Gesundheitsamtes Bremen wichtige Fragen offengelassen hatte (vgl. Ziff. 8.6. des 23. JB), musste ich bei einer Prüfung ausgewählter Sicherheitsaspekte des Netzes im April des Berichtsjahres erneut erheblichen Nachbesserungsbedarf feststellen. Das Gesundheitsamt Bremen (GAB) verpflichtete sich daraufhin, folgende Maßnahmen zu treffen:

Entwicklung eines am Entwurf des Senators für Finanzen für den E-Mail-Verkehr der bremischen Verwaltung ausgerichteten Konzepts, sobald dieser Entwurf verbindlich geworden ist. Bis dahin und bis zur Schaffung entsprechender technischer Voraussetzungen werden nach Aussage des Gesundheitsamtes sensible, insbesondere patientenbezogene Daten nicht per E-Mail verschickt. Wesentlich wird der Einsatz geeigneter Verschlüsselungsverfahren sein, durch deren Verwendung die Übermittlung sensibler personenbezogener Daten erst zulässig ist. Ich habe dem Gesundheitsamt gegenüber signalisiert, dass spezifische Lösungen, die über das Rahmenkonzept des Senators für Finanzen hinausgehen, erforderlich sein werden. Dazu gehört z. B. vor dem Hintergrund der Abschottungsverpflichtungen der einzelnen Abteilungen die Regelung des Umgangs mit Attachments oder, vor dem Hintergrund beruflicher Schweigepflichten, die Bereitstellung persönlich gebundener Schlüsselzertifikate.

Aktivierung der Überwachungsanforderungen als Grundlage einer Protokollierung und Revision für alle sensiblen Objekte des Gesundheitsamtes (z. B. Dateien mit personenbezogenen medizinischen Informationen). Das Gesundheitsamt Bremen teilte mit, dass die sensiblen Objekte alle definiert worden sind. Die Aktivierung der Überwachung dieser Objekte war bis Redaktionsschluss noch nicht abgeschlossen.

Verbesserung der Netzstruktur mit dem Ziel, die in den einzelnen Abteilungen 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. Die von mir vorgeschlagene Einrichtung abteilungsbezogener Domänen im Netz (vgl. 23. JB, Ziff. 8.6.), die eine selbständige Verwaltung abteilungsinterner Daten und einen ausschließlichen Zugriff durch die Abteilungen auf ihre Server und somit auf ihre Daten gewährleistet hätte, lehnte das Amt aus Kapazitäts- und Kostengründen ab. Es bleibt somit bei einer abteilungsübergreifenden Domäne „Gesundheitsamt Bremen“ mit einer zentralen Administration. Die Strukturverbesse-

rung des Netzes kann sich folglich nur auf das Rechteverhältnis des Domänencontrollers zu den File-Servern der Abteilungen beziehen, die als Domänenmitglieder der zentralen Steuerung unterliegen. Das Gesundheitsamt Bremen hat erklärt, es habe die File-Server hinsichtlich der Berechtigungsstruktur rekonfiguriert, um dennoch einen weitgehenden Schutz der abteilungsinternen Daten zu erreichen. Da diese Netzstruktur, anders als mein Vorschlag zur Bildung abteilungsbezogener Domänen, die systemlogische Trennung zwischen den einzelnen Abteilungen nicht ermöglicht, habe ich die vom Gesundheitsamt vorgeschlagene Lösung nur unter der Voraussetzung akzeptiert, dass eine starke Revision, insbesondere der Administratortätigkeit gewährleistet wird.

Ein erster Entwurf des Revisionskonzeptes liegt mir vor, bedarf aber noch weiterer Differenzierung des Verfahrens und der Ziele der Revision. Wichtige Bereiche sollten z. B. die Definition der Inhalte der Revision, die Systemebenen, auf denen sie durchgeführt wird und das Verfahren sein, mit dem bestimmte Fragestellungen behandelt werden. Hierbei sollte unterschieden werden zwischen regelmäßigen Stichproben (z. B. Protokollauswertungen in Bezug auf bestimmte Objekte) und anlassbezogenen Kontrollen (z. B. bestimmte Veränderungen innerhalb der Benutzerstruktur). Eine endgültige Version des Revisionskonzeptes mit den entsprechenden Inhalten liegt mir noch nicht vor. Das GAB teilte aber bereits mit, dass die organisatorische Umsetzung des Konzeptes grundsätzlich erfolgt ist, wobei für die geplante externe EDV-fachliche Unterstützung noch Verhandlungen mit möglichen Auftragnehmern geführt würden. Eine weitere datenschutzrechtliche Anforderung ist die Beschränkung der Eingriffstiefe der Administration. Sie darf sich nicht bis auf die sensiblen Inhaltsdaten der Abteilungen erstrecken. Es muss möglich sein, dass die in einzelnen Abteilungen, etwa im sozialpsychiatrischen Dienst gespeicherten Patientendaten nur in verschlüsselter Form für die Administration zugänglich sind.

Verbesserung des Schutzes des Netzes gegenüber Externen durch die Integration einer Firewall inkl. Proxy-Server. Das Gesundheitsamt Bremen teilte mit, dass die Integration beider Elemente in das Netz erfolgt sei.

Ich habe das GAB darauf hingewiesen, dass die umfassende Revision ein unverzichtbarer Baustein der Sicherheitsinfrastruktur ist. Deswegen halte ich es für notwendig, einen Zeitrahmen bis März 2002 für die bereits für Anfang dieses Jahres geplante Umsetzung des Revisionskonzeptes festzulegen. Für den Fall, dass die vollständige Umsetzung nicht bis März dieses Jahres gelingt, ist es erforderlich, das bereits erstellte Konzept inkl. der technischen und organisatorischen Maßnahmen auf die fehlende Revision abzustimmen. Dies würde in erster Linie bedeuten, die Administration des Netzes neu zu organisieren.

Insgesamt ist aber im Berichtsjahr eine wesentliche Verbesserung der Sicherheitsinfrastruktur im Sinne einer Anpassung der technischen Rahmenbedingungen an Vorgaben des Bremischen Gesetzes über den öffentlichen Gesundheitsdienst (ÖGDG) erfolgt.

8.3. Das Bremer Mammographie-Screening-Projekt

Über die Vorgeschichte des umstrittenen Bremer Mammographie-Screening-Projekts hatte ich berichtet (vgl. 23. JB, Ziff. 8.5.). Im Sommer des Berichtsjahres begann das Projekt, anhand der ihm von der Meldebehörde zugeleiteten Anschriften in einzelnen Bremer Stadtteilen Frauen im Alter von 50 bis 70 Jahren zu Röntgen-Reihenuntersuchungen einzuladen. Das den Einladungen beigefügte Informationsblatt enthielt den Hinweis, das gesamte Verfahren sei mit dem Landesbeauftragten für den Datenschutz abgestimmt. In der Tat hatte ich kurz zuvor einem Datenschutzkonzept zugestimmt, das die dem Projekt aus gesundheits- und datenschutzpolitischen Gründen gesetzten Schranken dokumentierte und die daraus resultierenden technischen Vorkehrungen zur Begrenzung der Verarbeitung der Daten der betroffenen Frauen konkretisierte.

Wie dem Projekt angekündigt, prüfte ich im September des Berichtsjahres die drei Stellen des Bremer Mammographie Screening-Projektes „Einladungsstelle im Gesundheitsamt Bremen, Untersuchungsstelle in der Knochenhauerstraße und Befundungs-/Assessmentstelle in der Frauenklinik des ZKH Sankt-Jürgen-Stra-

ße“ mit der Fragestellung, ob die verabredeten technischen und organisatorischen Maßnahmen zur Gewährleistung des Datenschutzes getroffen worden waren. Ich musste schwerwiegende Mängel bei der Verarbeitung der äußerst sensiblen personenbezogenen Daten (Meldedaten der Nichtteilnehmerinnen sowie Melde- und Gesundheitsdaten der Teilnehmerinnen) feststellen. Dies lag insbesondere daran, dass die für die Datenverarbeitung des Mammographie-Screening-Projektes eigens entwickelte Software, mit der ein wesentlicher Teil der mit mir abgestimmten technischen Maßnahmen hätte realisiert werden können, noch in keiner der drei Stellen des Projekts installiert worden war. Statt dessen wurde mit Excel-Tabellen gearbeitet. Das hatte zur Folge, dass eine den Aufgaben an den einzelnen Arbeitsplätzen des Projekts entsprechende differenzierte Zugriffsstruktur nicht installiert worden war. Folglich war es nicht möglich, die Zugriffsrechte nach Art und Zweckbestimmung der Daten zu steuern, nur bestimmte gesetzlich zulässige Auswertungen zuzulassen und andere Auswertungen auszuschließen.

Prompt hatte die Einladungsstelle eine Telefonnotizstatistik als neue Tabelle eingerichtet, die über die zulässigen Einladungsdatenfelder hinaus Datenfelder zur Speicherung medizinischer Daten, wie z. B. Absage wegen diagnostiziertem Brustkrebs, zur Verfügung stellte. Dies ermöglichte Recherchen wie etwa die Filterung von bzw. Suche nach bestimmten Absagegründen. Dies sei, so die Begründung, für statistische Zwecke erforderlich. Darüber hinaus gibt es keine Verpflichtung zur Absage, noch muss sie begründet werden. Diese Telefonnotizstatistik widersprach auch der amtlichen Begründung zur eigens im Vorlauf zu dem Projekt durch die Bremische Bürgerschaft geschaffenen Rechtsgrundlage im neuen § 15 des Gesetzes über den öffentlichen Gesundheitsdienst (ÖGDG), wonach das Projekt die Meldedaten der Frauen, die am Projekt nicht teilnehmen, nicht zu Evaluationszwecken nutzen darf und daher zu anonymisieren hat. Überdies war das im Konzept festgelegte Verfahren zur endgültigen Verschlüsselung der Daten von Frauen, die ihrer Einladung ausdrücklich widersprechen, mittels eines Hash-Codes, das eine Wiedereinladung ausschließen soll, gleichfalls nicht installiert. Schließlich war das für die vorübergehende zwecks Transportsicherung festgelegte Verschlüsselung der zwischen dem Einwohnermeldeamt und der Einladungsstelle und zwischen den drei Stellen des Projekts übermittelten Daten erforderliche PGP-Tool nicht verfügbar, d. h., die Daten wurden entgegen der Konzeptvorgabe unverschlüsselt übermittelt.

In der Untersuchungsstelle und in der Befundungsstelle gab es strukturell ähnliche Probleme. So wurden in der Befundungsstelle die Befunde in Excel-Tabellen gespeichert (Befundlisten). Auch hier war eine Regulierung der Zugriffsberechtigungen und der Auswertungen nicht möglich.

An Schärfe gewannen die Probleme noch dadurch, dass die im Datenschutzkonzept abgestimmte Protokollfunktion nicht realisiert war, d. h., selbst eine nachträgliche Kontrolle von Zugriffen war nicht gewährleistet. Zwar wurde erklärt, es sei beabsichtigt, in Kürze das im Konzept dargestellte Verfahren zu installieren. Man hatte aber unter Missachtung des abgestimmten Konzepts und unter Verletzung datenschutzrechtlich gebotener Schutzvorkehrungen mit dem Projekt begonnen, die betroffenen Frauen und mich aber in dem Glauben gelassen, das abgestimmte Konzept sei bereits umgesetzt.

Deshalb sah ich mich gezwungen, in Anwendung des § 29 des Bremischen Datenschutzgesetzes gegenüber dem Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales eine förmliche Beanstandung auszusprechen. Danach reagierte die verantwortliche Senatorin des Projektes unverzüglich. Insbesondere sagte sie zu, umgehend die Telefonnotizstatistik aufzugeben und zu löschen sowie das Anonymisierungsverfahren, das Verschlüsselungsverfahren und die übrige im Konzept dokumentierte Software mit der gebotenen Zugriffslogik zu installieren. Es wurden ernsthafte Anstrengungen unternommen, die festgestellten Mängel zu beseitigen. Ich konnte deshalb darauf verzichten, die Angelegenheit öffentlich zu machen.

Im Rahmen einer zweiten technischen Prüfung der drei Stellen des Projekts habe ich im November/Dezember 2001 festgestellt, dass inzwischen die abgestimmte projektspezifische Software funktionsfähig installiert worden war. In der Einladungsstelle waren die Daten der Nichtteilnehmerinnen aus der ersten Ein-

ladungsrunde durch Löschung der Identitätsdaten anonymisiert worden. Die Telefonnotizstatistik war gelöscht und nicht fortgeführt worden.

Inzwischen wurde mir auch erklärt: Die Rollen für den Zugang zum Betriebssystem und zur Datenbank sind definiert, und das Revisionskonzept ist umgesetzt worden, und das für die Verschlüsselung der Daten der Betroffenen auf dem Transportwege erforderliche Tool ist installiert. In der Einladungsstelle ist der Hash-Code zwecks Ausschluss erneuter Einladungen an Frauen, die ihrer Einbeziehung in das Projekt ausdrücklich widersprochen haben, installiert worden.

Kurz vor Redaktionsschluss teilte das Projekt noch mit, die Daten der Teilnehmerinnen an den ersten beiden Einladungsrunden seien in die neue Datenbank eingelesen und in den Excel-Tabellen gelöscht worden. Ich gehe davon aus, dass die Angaben zutreffen, und hoffe, mit einer in Kürze stattfindenden Prüfung vor Ort den Vorgang abschließen zu können.

8.4. Pseudonymisierung der Versichertendaten in der Krankenversicherung

Seit der umfassenden Novellierung des Bundesdatenschutzgesetzes im Sommer 2001 werden durch § 78 b SGB X auch die Sozialleistungsträger, unter ihnen die gesetzlichen Krankenkassen, zur Datenvermeidung und Datensparsamkeit aufgefordert. Soweit möglich und verhältnismäßig, sollen Sozialdaten, vor allem also die Daten der Versicherten, anonymisiert bzw. pseudonymisiert werden. Wie ich bereits berichtet hatte (vgl. 22. JB, Ziff. 8.8. und 23. JB, Ziff. 8.7.), bemühen sich die Datenschutzbeauftragten von Bund und Ländern seit der Vorbereitung der Gesundheitsreform 2000 darum, als Ausgleich für eine Verbesserung der Datengrundlage der Krankenkassen eine möglichst frühzeitige Pseudonymisierung der in den durch die Ärzte, Krankenhäuser, Apotheker und anderer Leistungserbringer den Krankenkassen zur Abrechnung ihrer Leistungen eingereichten Unterlagen enthaltenen Patienten- bzw. Versichertendaten zu erreichen. Sie erheben keine Einwendungen dagegen, dass die Krankenkassen, anders als bisher gesetzlich zugelassen, eine umfassende, über längere Zeiträume einzelfallbezogene Übersicht über die abgerechneten Leistungen erhalten, verlangen aber als ausgleichenden Schutz der Persönlichkeitsrechte der Versicherten die Pseudonymisierung der auf sie bezogenen Daten. Der Deutsche Bundestag hat denn auch am 4. November 2001 beschlossen, dass die Krankenkassen lediglich Daten erhalten sollten, aus denen sie nicht aus eigener Kraft auf die Identität der jeweiligen Versicherten schließen können. Dies sollte ihnen nur mit Hilfe einer unabhängigen treuhänderisch wirkenden Stelle für ganz bestimmte gesetzlich definierte Zwecke möglich sein. Dieser Beschluss scheiterte an der Teilblockade der Gesundheitsreform 2000 im Bundesrat.

Im Februar 2002 legte das Bundesministerium für Gesundheit den Datenschutzbeauftragten diesen Teil der Gesundheitsreform in Gestalt eines Entwurfs für ein „Transparenzgesetz“ erneut vor. Leider war auf Drängen der gesetzlichen Krankenversicherung die Pseudonymisierung „entschärft“ worden: Die Kassen sollen — wie im geltenden Recht — nur die Daten über die Leistungen der niedergelassenen Ärzte ohne Bezug auf die Identität des einzelnen Patienten erhalten. Die Daten über andere Leistungen hingegen sollen erst nach Abschluss der Leistungsabrechnung pseudonymisiert werden. Die Datenschutzbeauftragten haben eine Begründung dafür verlangt. Nachdem das Bundesministerium zunächst den Anschein erweckte, als wolle es das Vorhaben des Transparenzgesetzes vorerst fallen lassen, hat es kürzlich die Krankenkassen, Leistungserbringer und Datenschutzbeauftragten zu einem Workshop über „Datentransparenz, Datenschutz und Datensicherheit in der gesetzlichen Krankenversicherung“ eingeladen. Ich werde mich weiterhin an der Diskussion beteiligen.

9. Jugend und Soziales

9.1. Vernetzung des Amtes für Jugend und Familie Bremerhaven

Im Oktober hat mir das Amt für Jugend und Familie bei Einrichtung eines internen Netzes ein Datenschutzkonzept übersandt. Im Netz soll mit sensiblen Fachanwendungen wie etwa der elektronischen Fallakte in der Jugendhilfe gearbeitet werden. Das Netzkonzept legt technische Vorkehrungen zum Schutz des Netzwerkes fest, das ein Subnetz des Bremerhavener Magistratsnetzes ist. Es enthält Informationen zur Administration des Netzes unter anderem

— zur Definition der logischen Zugriffsstruktur auf Netzwerkebene (administrative und benutzerspezifische Zugänge),

— zur Beschreibung der eingesetzten Server für Anwendungen und Kommunikation,

— zur Anbindung der Außenstellen in den Stadtteilbüros,

— zur Konfiguration der Workstation an den einzelnen Arbeitsplätzen,

— zur Datensicherung und

— zur Administration und Zugriffslogik inhaltsbezogener Anwendungssoftware.

Die rechtzeitige Unterrichtung über Komponenten macht es mir möglich, meine Vorstellungen zum Umfang und Niveau technischer Datenschutzmaßnahmen zu formulieren. Das Konzept beschreibt jetzt eine in sich schlüssige Sicherheitsinfrastruktur.

9.2. Der Umbau des Amtes für Soziale Dienste und das Sozialgeheimnis

Die Daten, die für die Entscheidung über Sozialleistungen erhoben werden, unterliegen dem Sozialgeheimnis. Sie dürfen auch innerhalb des Sozialleistungsträgers nur Befugten, d. h. denen, für deren Aufgabenerfüllung ihre Kenntnis erforderlich ist, zugänglich gemacht werden. Sind sie einer Mitarbeiterin oder einem Mitarbeiter zu Beratungszwecken oder im Bereich der Jugendhilfe zum Zweck persönlicher und erzieherischer Hilfen anvertraut worden, darf diese bzw. dieser die Daten auch intern grundsätzlich nur mit Einwilligung der oder des Betroffenen weitergeben. Dies ist in § 35 SGB I, § 65 SGB VIII und § 203 StGB so bestimmt. Die Leistungsträger haben zur Gewährleistung dieser Regelungen technische und organisatorische Regelungen und Dienstanweisungen zu treffen (vgl. § 78 a SGB X). Die Datenschutzkonzepte für die Verfahren PROSOZ und KIS sind Beispiele für derartige Regelungen.

Organisation, Aufgabenerfüllung und informationstechnische Ausstattung des Amtes für Soziale Dienste Bremen sind in den vergangenen Jahren immer wieder umstrukturiert und erneuert worden. Dabei habe ich stets darauf hingewirkt, dass den datenschutzrechtlichen Rahmenbedingungen Rechnung getragen wird. Die Umstrukturierungen im Amt, wie die Gründung von zwölf Bezirkssozialzentren und die Einführung des Casemanagements in der Sozialhilfe, sind bereits abgeschlossen bzw. werden umgesetzt. Sie werden den amtsinternen Datenaustausch modifizieren. Sozialgeheimnis, Vertrauensschutz und Schweigepflichten sollen gewahrt bleiben. Dies wird durch den mir kürzlich vorgelegten Entwurf für eine fortgeschriebene Dienstanweisung über den Datenschutz in der Jugendhilfe und in der Sozialhilfe bestätigt. Darüber hinaus berichtete ich im letzten Jahr (23. JB, Ziff 9.1) über die Entwicklung der elektronischen Fallakte in der Jugendhilfe. Dieses Projekt ist derzeit noch nicht abgeschlossen.

Die Beleihung der Bremer Arbeit GmbH mit Aufgaben der Arbeitsförderung und Arbeitshilfe, die neuen bundesrechtlichen Vorgaben in § 18 BSHG und § 371 a SGB III zur Verbesserung der Zusammenarbeit von Arbeitsämtern und Trägern der Sozialhilfe sowie die Beteiligung Bremens an einem der in § 18 a BSHG und § 421d SGB III vorgesehenen Modellprojekte (MoZArT), schließlich das neue Job-AQTIV-Gesetz, werden sicher weitere Umstrukturierungen des Amtes für Soziale Dienste nach sich ziehen. Auch in diesem Zusammenhang gilt es, die beruflichen Schweigepflichten zu respektieren und Datenflüsse auf das erforderliche Maß zu begrenzen.

10. Bildung und Wissenschaft

10.1. Internet-Nutzung durch Schulen

Der auf meine Initiative (vgl. bereits 23. JB, Ziff. 10.1.) zustandegekommene Workshop zum Thema „Datenschutzkonforme Internet-Nutzung an Schulen“ hat nach den Sommerferien beim Landesinstitut für Schule (LIS) endlich stattgefunden. Neben Vertretern des Senators für Bildung, des LIS und meiner Dienststelle waren zahlreiche EDV-Koordinatoren der Schulen im Land Bremen bei diesem

Workshop anwesend. Dabei wurde der datenschutzrechtliche Rahmen der Internet-Nutzung durch Schulen thematisiert, u.a. in welcher Form Internet-Auftritte an Schulen zu gestalten sind, wie elektronische Postfächer administriert werden und welche Inhalte aus dem Internet in das lokale Netz der Schule heruntergeladen werden dürfen. Der Senator für Bildung hat zuletzt im Datenschutzausschuss zugesichert, auf Basis dieses Workshops zu dem Thema einen Leitfaden für die Internet-Nutzung an Schulen bis zum Frühjahr 2002 fertigzustellen, auf den dann alle Schulen als Orientierungshilfe zurückgreifen können.

Um einen Eindruck zu gewinnen, wie die gängige Praxis an den Schulen momentan ist, habe ich die Internet-Seiten verschiedener Schulen aufgerufen und bisher zwei Schulen (Humboldt-Schule Bremerhaven, Schulzentrum Blumenthal) besucht.

Vor Ort habe ich festgestellt, dass durch organisatorische Maßnahmen (z. B. kein Betreten der EDV-Räume ohne Lehrkräfte, eine solche Anordnung der Computer, dass von den Lehrkräften während des Unterrichts alle Bildschirme gesehen werden können) einer missbräuchlichen Nutzung des Internet bereits entgegengewirkt wird. Bei der Überprüfung von Download-Verzeichnissen auf den Ausbildungsrechnern fielen mir keine rechtswidrigen Inhalte auf. Technischer Handlungsbedarf besteht bei der Absicherung der Netze für die pädagogische Ausbildung, den Servern und Arbeitsplatzrechnern. Hier müssen noch geeignete Sicherungsmaßnahmen (Firewall etc.) aufgebaut oder verbessert werden.

Bei den Prüfungen war überdies festzustellen, dass in den Schulen bei Rektorat bzw. EDV-Koordinatoren große Unsicherheit über die datenschutzrechtlichen Anforderungen zur Internet-Nutzung bestand. Insbesondere Fragen zu Zulässigkeit und Umfang von Datenspeicherung bzw. Protokollierung von Benutzer-Aktivitäten wurden mit mir erörtert. Die Speicherungs- und Protokollierungspraxis musste an den geprüften Schulen noch an die rechtlichen Vorgaben angepasst werden. Weiterhin habe ich festgestellt, dass keine oder unzureichende schulinterne Nutzerordnungen existieren, in denen Nutzer des Schulnetzes auf die Rechte und Pflichten der Internet-Nutzung hingewiesen werden. Die durch die Prüfungen gesammelten Erfahrungen unterstreichen u. a deutlich den Bedarf einer Orientierungshilfe für die Internet-Nutzung durch Schulen.

10.2. Funk-LAN an der Universität Bremen

Die Universität Bremen betreibt seit Herbst letzen Jahres ein Funknetz zur Unterstützung der Lernenden und Lehrenden beim mobilen Arbeiten auf dem Campus. Die im Einsatz befindliche Technik ist das auf dem Standard IEEE 802.11 b basierende „WLAN“ (Wireless Local Area Network); das drahtlose Äquivalent zum Ethernet (IEEE 802.3). Ein Großteil des Campus ist bereits mit der WLAN-Technologie mit ca. 200 Zugangspunkten (Accesspoints) abgedeckt; der Ausbau auf 400 Accesspoints soll im zweiten Quartal 2002 praktisch abgeschlossen sein.

Bei der Einrichtung des WLAN wurde großer Wert auf die Vertraulichkeit der übertragenen Daten gelegt. Da die dazu standardmäßig im WLAN implementierten Mechanismen (WEP — „Wireless Encryption Protocol“, Verschlüsselungsalgorithmus RC4) nicht ausreichend und angreifbar sind, ist an der Universität Bremen eine VPN-Lösung (VPN = Virtual Private Network) realisiert worden. Dabei wird zwischen dem mobilen Arbeitsplatzrechner und einem VPN-Gateway, das den Übergangspunkt in das drahtgebundene Netz der Universität bildet, eine verschlüsselte Datenübertragung (Tunnel) mittels Point-to-Point Tunneling Protocol (PPTP) aufgebaut. Der Zugang zum drahtgebundenen Netz wird darüber hinaus nur dann freigegeben, wenn sich der Benutzer gegenüber dem Gateway durch ein Passwort authentisiert hat. Diese Maßnahme ist um so wichtiger, da es mittels einer handelsüblichen Funk-Netzwerkkarte technisch leicht möglich wäre, am Funknetz selbst teilzunehmen. Zukünftig wird zudem ermöglicht, das VPN alternativ über das IPSec-Protokoll aufzubauen, das im Vergleich zu PPTP noch sicherer ist. Innerhalb des Funknetzes selbst steht nur eine sehr eingeschränkte Auswahl an Diensten (DHCP, DNS, freier Web-Server für die Initialisierung des Anmeldeverfahrens) zur Verfügung. Die Nutzung des Funknetzes fällt zudem unter die allgemein gültigen Nutzungsbedingungen der Universität, deren Kenntnisnahme und Anerkennung ein Nutzer mittels Unterschrift bei Beantragung bzw. Vergabe eines herkömmlichen Accounts bestätigt. Nur Nutzer, die ei-

nen herkömmlichen Account für das drahtgebundene Netzwerk der Universität haben, sind befugt, am WLAN teilzunehmen.

10.3. Prüferfahrungen bei der Führung von Schullaufbahnakten

Zu jedem Schüler und jeder Schülerin in einer öffentlichen Schule im Lande Bremen ist eine Schullaufbahnakte zu führen. Hierbei sind von den Schulen insbesondere die Richtlinien zur Führung der Schullaufbahnakten und das Gesetz zum Datenschutz im Schulwesen (SchulDSG) zu beachten. Eingaben Betroffener haben mich im Berichtszeitraum dazu veranlasst, die Einhaltung der Bestimmungen an zwei Bremer Schulen zu überprüfen.

An beiden Schulen sind von mir vergleichbare Mängel festgestellt worden. Unter anderem war die sich aus den Richtlinien zur Führung der Schullaufbahnakten ergebende Aufbewahrung von Schülerunterlagen in zwei Teilen (A und B) an beiden Einrichtungen nur unzureichend umgesetzt worden. Mit der Aufteilung der Akte verbunden ist die Absicht, sensibleren Schülerdaten, wie Gesundheits- und Verhaltensdaten, einen besonderen Schutz zukommen zu lassen. Diese Daten, die in den Teil B der Akte aufzunehmen sind, dürfen grundsätzlich nur mit Einwilligung der Betroffenen aufbewahrt werden. Auch darf Teil B der Schullaufbahnakte grundsätzlich nur mit Zustimmung der Betroffenen weitergegeben werden. An beiden Schulen habe ich Unterlagen, die in Teil B gehört hätten, in Teil A der jeweiligen Akte festgestellt. Außerdem fehlten die für die Aufnahme dieser Unterlagen in die Schullaufbahnakte benötigten Einwilligungen oder deren Dokumentation. In einem Fall waren Unterlagen zu einem minderjährigen Schüler sogar gegen den ausdrücklichen Wunsch der Erziehungsberechtigten des Betroffenen in die Akte aufgenommen worden. An einer der beiden Schulen waren darüber hinaus für die Weitergabe des Teils B der Schullaufbahnakte keine Einwilligung eingeholt worden; die Abgabe der Schullaufbahnakte war dort stets ohne Zustimmung der Betroffenen erfolgt.

An beiden Schulen waren Akten ausgeschiedener Schüler bisher nicht gesperrt worden. Gemäß § 18 Abs. 1 SchulDSG sind personenbezogene Daten in nicht automatisierten Dateien und in Akten von der speichernden Stelle mit Ablauf des Kalenderjahres zu sperren, das dem folgt, in dem der Schüler die Schule verlassen hat. Die Daten dürfen nach ihrer Sperrung zwar weiterhin gespeichert bleiben, eine weitergehende Verarbeitung ist jedoch nur zu den gesetzlich bestimmten Zwecken zulässig.

Problematisiert habe ich gegenüber beiden Schulen auch die Dauer der Aufbewahrung der Schullaufbahnakten. Gemäß § 18 Abs. 5 SchulDSG dürfen Namen, Schulbesuchsdauer und besondere schulische Leistungen oder Ehrungen eines Schülers zeitlich unbegrenzt aufbewahrt werden, wenn sie für Schulchroniken oder sonst historisch bedeutsam sein könnten. Im Übrigen sind personenbezogene Daten in nicht automatisierten Dateien und in Akten nach Maßgabe einer Verwaltungsanordnung des Senators für Bildung und Wissenschaft zu löschen.

Der Senator für Bildung und Wissenschaft hat in der für die Schulen der Stadtgemeinde Bremen geltenden Richtlinie über die Sicherung, Aufbewahrung und Aussonderung von Schriftgut in den Schulen als Grundsatz festgelegt, dass personenbezogene Daten in nicht automatisierten Dateien und in Akten zu löschen oder zu vernichten sind, wenn ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe nicht mehr erforderlich ist und sie nicht nach dem Bremischen Archivgesetz vom Staatsarchiv übernommen werden (vgl. Pkt. 3.1 der Richtlinie). Aus Punkt 4 der genannten Richtlinie ergeben sich für die in der Schullaufbahnakte aufbewahrten Unterlagen zeitlich gestaffelte unterschiedliche Aufbewahrungsfristen, was bedeutet, dass bestimmte Teile der Akte erheblich länger als andere aufzubewahren sind. Für die keiner längeren Aufbewahrungsfrist unterliegenden Daten bzw. Dokumente ist nach der Richtlinie eine Aufbewahrungsdauer von drei Jahren vorgesehen. Die unterschiedlichen Aufbewahrungsfristen beginnen jeweils am Ende des Schuljahres, in dem der letzte Vorgang in die Akte eingetragen wurde, d. h., der Schüler die Schule endgültig verlässt. Aufbewahrt worden waren von beiden überprüften Schulen mit vollem Umfang auch Akten, in die schon seit mehr als zehn Jahren kein Eintrag mehr erfolgt war, was einen klaren Verstoß darstellt.

Von den Schulen wurden die festgestellten Mängel insbesondere mit Arbeitsüberlastung und Zeitmangel begründet. Aus meiner Sicht können die genannten Gründe aber nicht dazu führen, dem Schutz des Betroffenen dienende datenschutzrechtliche Regelungen außer Acht zu lassen. Die überprüften Schulen haben sich schließlich bereit erklärt, die bei ihnen aufgetretenen Mängel zu beseitigen.

10.4. Forschungsvorhaben und Schulbegleitforschungsprojekte

Mehrmals bin ich im vergangenen Jahr z. B. vom Landesinstitut für Schule und von der Universität Bremen über die geplante Durchführung wissenschaftlicher Forschungsvorhaben und von Schulbegleitforschungsvorhaben unterrichtet und um Stellungnahme gebeten worden. Die Themen der Vorhaben, bei denen Schüler und Schülerinnen in der Regel mit Hilfe von Fragebögen um Angaben gebeten werden, waren dabei erneut sehr unterschiedlicher Art. Während die Erhebungen im Rahmen der Schulbegleitforschung eher der Evaluation und Begleitung des Unterrichts in den Schulen dienten, hatten die wissenschaftlichen Forschungsvorhaben die Erforschung der gesellschaftlichen Situation minderjähriger Schüler und Schülerinnen zum Inhalt. Im Jahre 2001 habe ich u. a. zu Befragungen mit den Themen „Frühfranzösischunterricht bei Grundschülern“, „Erforschung kognitiver Schichten im Bereich der Mechanik (Sek. II)“, „Messung der allgemeinen Lebensqualität“, und „Regionale Mobilität von Auszubildenden und jungen Fachkräften“ Stellung genommen. Auch die Pisa-Studie hat mich noch beschäftigt. Meine Bewertung beschränkt sich im Wesentlichen auf die Organisation und Durchführung des jeweiligen Vorhabens.

Häufig findet das Einwilligungsverfahren keine ausreichende Berücksichtigung bei der Vorbereitung personenbezogener Schülerbefragungen. Sollen Schülerinnen und Schüler ohne ausreichende Einsichtsfähigkeit im Rahmen von Erhebungsvorhaben in den Schulen befragt werden, so müssen deren Erziehungsberechtigte vorher darüber informiert und um die schriftliche Einwilligung in die Datenerhebung bei ihren Kindern und die Weiterverarbeitung der bei ihnen erhobenen Daten gebeten werden. Eine wirksame Einwilligung setzt voraus, dass die Betroffenen über das geplante Vorhaben und über Art, Umfang und Zweck der Nutzung der von ihnen gewünschten Daten umfassend aufgeklärt werden. Die Teilnahme an dem Vorhaben muss den betroffenen minderjährigen Schülern nach der Einwilligung ihrer Eltern freigestellt bleiben. Meine Stellungnahmen enthalten daher oftmals Empfehlungen zur inhaltlichen Gestaltung der Unterrichtungsschreiben zu den Einwilligungserklärungen an die Erziehungsberechtigten sowie zur Gewährleistung der freiwilligen Teilnahme an der Erhebung durch die jeweilige Schülerin bzw. dem jeweiligen Schüler. Bezogen auf das einzelne Vorhaben müssen angemessene Lösungen zur Umsetzung der datenschutzrechtlichen Anforderungen gefunden werden.

Außerdem ist es vielfach erforderlich, Empfehlungen zum Umgang mit den Schülerdaten nach der Erhebung, also während der Auswertungsphase, zu geben. Um Risiken beim Umgang mit dem erhobenen Datenmaterial zu vermeiden, müssen die erhobenen Daten frühestmöglich anonymisiert und die personenbezogenen Daten spätestens nach Erreichung des Forschungszwecks gelöscht werden. Die bei den Schülerinnen und Schülern erhobenen Daten dürfen nur für die jeweilige Erhebung bzw. Untersuchung und nur im Rahmen der erteilten Einwilligung ausgewertet werden. Eine Nutzung der Daten zu anderen Zwecken wäre unzulässig. Geeignete technische und organisatorische Sicherungsmaßnahmen sind für den Umgang mit den erhobenen Daten zu ergreifen. Diesen Grundsätzen entsprechend habe ich die genannten Projekte beraten.

Die bei der Durchführung von Forschungsprojekten in den Schulen zu beachtenden Anforderungen habe ich außerdem in einem von mir herausgegebenen Merkblatt zusammengestellt, das auch in meinem Internet-Angebot verfügbar ist.

11. Finanzen

11.1. Weiterentwicklung des Projektes Chipsmobil

Im letzten Bericht habe ich die Schwerpunkte meiner Projektbegleitung beschrieben (vgl. 23. JB, Ziff. 12.1.). Diese habe ich im Berichtsjahr durch meine Mitwir-

kung in den Arbeitsgruppen „Basiseinrichtung IT-Konzeption“, „Berechtigungskonzept“ und „Datenschutzkonzept“ weiter verfolgt. Folgende konzeptionelle Konkretisierungen wurden erreicht:

Die Sicherheit der Passwortmechanismen von SAP wurde im Rahmen der Arbeitsgruppe „Basiseinrichtung IT-Konzeption“ vom Senator für Finanzen überprüft. Es wurde zugestanden, dass SAP die Passworte in „gehashter Form“ übermittelt und diese Hash-Werte im lokalen Netzwerk mitgelauscht werden könnten. Die von mir benannten Risiken (Abhör- und Replayattacken) wurden als gering eingestuft, da erhebliches Systemwissen erforderlich sei, um solche Angriffe erfolgreich zu starten. Noch unwahrscheinlicher sei es, dass Daten auf dem Transport direkt manipuliert würden. Die Sicherheitsrisiken bei einem Verzicht auf die Verschlüsselung von Passworten und Inhaltsdaten werden vom Senator für Finanzen als beherrschbar eingestuft. Ich habe meine Forderung nach einer systemspezifischen Lösung nicht mehr aufrecht erhalten, weil die mir vom Senator für Finanzen aufgezeigte Perspektive, eine durchgängige Sicherheit für alle über das BVN laufende Arten von Anwendungen und Systemen zur Verfügung zu stellen (VPN mit IPsec und Active Directory mit Kerberos unter Windows 2000), als umfassende Infrastrukturmaßnahme einen höheren Wirkungsgrad hat als eine systemspezifische Lösung. Darüber hinaus sollen entsprechende Komponenten bereits in 2002/2003 zum Einsatz kommen, die somit auch für das Verfahren Chipsmobil nutzbar gemacht werden können.

Das Berechtigungskonzept wurde in der gleichnamigen Arbeitsgruppe im März des Berichtsjahres fertiggestellt. Es befasst sich mit den Berechtigungen innerhalb der Standardsoftware SAP R/3. Es enthält u. a. das von mir geforderte Überwachungsverfahren zur zeitnahen Überprüfung der Korrektheit der Berechtigungsstruktur und beschreibt die Auswertungs- und Informationsmöglichkeiten sowie ein Verbot, diese zu Leistungs- und Verhaltenskontrollen der Mitarbeiter/-innen und zu Auswertungen von Bürgerinformationen zu nutzen. Es definiert hierzu die Sonderrolle „zentrales Auditing“. Als weitere Sonderrollen werden „Entwicklung/Customizing“ definiert, mit deren Möglichkeiten Erweiterungen des Systems und Zusatzentwicklungen möglich sind. Im Rahmen einer Weiterentwicklung des Konzeptes halte ich es für erforderlich zu beschreiben, welchen Organisationsebenen diese definierten Rollen zugeordnet werden und wie eine mögliche Kontrolle der Nutzung der Auswertungstools gestaltet sein könnte. Darüber hinaus ist es erforderlich, den größten Teil der fachbezogenen Rollen, mit denen die Zugriffslogik an den Arbeitsplätzen definiert wird, zu beschreiben. Weiterer Konkretisierungsbedarf besteht z. B. bei der Verknüpfung von bestimmten Rollen mit umfassenden Funktionen wie Downloads, durch die Daten aus dem SAP-System exportiert und mit Hilfe andere Systeme weiterverarbeitet werden können.

Der aktuelle Entwurf des Rahmendatenschutzkonzeptes hat in seinem aktuellen Entwurfsstadium sein Ziel, zentrale Datenschutz- und -sicherungsmaßnahmen in Einzel- und Wechselwirkungen darzustellen, noch nicht erreicht. In seiner bisherigen Fassung macht es eher eine von mir bereits im letzten Berichtsjahr benannte Schwierigkeit deutlich, die darin besteht, eine komplexe Sicherheitsstruktur, die eine Bewertung einer Fülle von Einzelmaßnahmen (u. a. im Berechtigungskonzept, IT-Konzept, Betreiber- und CCC-Betreiberkonzept) und deren Einordnung in ein Gesamtsystem erfordert, darzustellen.

Das Ziel, das Projekt zum 1. Januar 2002 abzuschließen, ist nicht erreicht worden. Derzeit gibt es daher keine Klarheit über den zeitlichen Rahmen, innerhalb dessen die datenschutzrelevanten Konzepte, insbesondere das Rahmendatenschutzkonzept, fertiggestellt werden können.

11.2. Softwareentwicklung FISCUS

Von den Oberfinanzbehörden Deutschlands wurde die Entwicklung einer neue Software für die deutsche Finanzverwaltung unter dem Begriff FISCUS betrieben. Diese kam in letzter Zeit nicht voran bzw. zeigte keine brauchbaren Ergebnisse. Deshalb wurde das Projekt FISCUS nach Beratung in der Finanzministerkonferenz neu konzipiert. Es wurde daraufhin eine FISCUS GmbH gegründet, an der der Bund und die Länder (ohne Bayern) beteiligt sind. Sie hat den Auftrag, eine anwendungsreife Software für die Finanzverwaltung zu entwickeln. Diese

GmbH hat untersucht, welche der bisherigen Module weiter vorangetrieben werden können und welche neu aufgelegt werden müssen. Die Untersuchung hat ergeben, dass der überwiegende Teil der Module neu erstellt werden muss.

Eine kleine Arbeitsgruppe der Landesbeauftragten für den Datenschutz, der auch ich angehöre, hat den Auftrag, die Arbeiten der GmbH datenschutzrechtlich zu begleiten.

11.3. MEDIA@Komm: Einsicht in das Steuerkonto

Eine Lebenslage im Rahmen des MEDIA@Komm-Projektes betraf die Einsicht des Steuerbürgers in sein Steuerkonto. Dieses Steuerkonto enthält neben den Daten über den Steuerbürger insbesondere Hinweise auf Fälligkeiten und Höhe von Steuern.

Diese Anwendung sollte den Betroffenen in die Lage versetzen, jederzeit in sein Steuerkonto auf elektronischem Wege Einsicht zu nehmen. Diese Lebenslage habe ich intensiv mit den Projektträgern beraten. Allerdings wurde dieses Projekt Ende des Berichtsjahres zurückgezogen, da im Rahmen des von Bayern entwikkelten Programms „ELSTER“ (elektronische Steuererklärung, vgl. auch Ziff. 11.4. dieses Berichts) eine ähnliche Anwendung vorbereitet wird. In „ELSTER“ sind bremische Überlegungen, insbesondere zu Sicherheitsfunktionen, eingeflossen.

11.4. Unsicherer Zugriff über Internet auf ELSTER

Im Frühjahr des Berichtsjahres gab es große Presseaufmerksamkeit, weil eine kostenlose Software, mit der deutsche Steuerbürger ihre Einkommensteuerdaten an ihr Finanzamt übermitteln können und die über das Internet von dem Server der Oberfinanzdirektion München herunterladen werden konnte, nicht die erforderliche Sicherheit bot. Unter bestimmten Voraussetzungen war nicht auszuschließen, dass Dritte die Daten beim Transport zum „ELSTER“-Server einsehen bzw. auf ihrem Rechner speichern konnten.

Durch eine Presseerklärung machte ich umgehend alle Steuerbürger auf dieses „Sicherheitsloch“ aufmerksam und empfahl, diese Software — zunächst — nicht zu verwenden. Diese Sicherheitslücke wurde dann nach ca. zwei Wochen geschlossen. Es hatte sich gezeigt, dass keine Software frei von Fehlern ist und immer wieder auf Sicherheitsgefahren getestet werden muss.

12. Wirtschaft und Häfen

12.1. Wahlen zur Arbeitnehmerkammer

Seit Jahren wird ein Weg gesucht, das aufwendige Wahlverfahren zu den Kammerwahlen unter Beachtung des Datenschutzes zu vereinfachen und kostengünstiger zu gestalten.

Nach dem Kammerwahlrecht sind die Arbeitgeber (Unternehmer und Betriebsstätten) von der Arbeitnehmerkammer anzuschreiben und aufzufordern, ihre Arbeitnehmer den Wahlorganen der Arbeitnehmerkammer melden. Die Arbeitnehmerkammer hat jedoch keine eigenen Arbeitgeberdaten. Derartige Daten haben die Finanzbehörden oder die Arbeitsämter in ihren Betriebsstättendateien. Eine Übermittlung dieser Betriebsdaten, die auch in großem Umfang personenbezogene Daten, z. B. über Handwerker, aber auch über private Haushalte, soweit sie Hausangestellte beschäftigen, enthalten, ist nach der Abgabenordnung und nach dem Sozialgesetzbuch nicht zulässig.

Ich habe die Entwicklung des folgenden Verfahrens begleitet. Die Kammerwahlen 2002 sollen auf der Basis eines so genannten Letter-Shop-Verfahrens durchgeführt werden. Die Arbeitsämter Bremen und Bremerhaven werden die Aufforderungsschreiben der Arbeitnehmerkammer — in denen auch auf die gesetzlichen Mitwirkungs- und Mitteilungspflichten hingewiesen wird — an die Betriebsstätten versenden. Es werden somit keine Arbeitgeberdaten an die Arbeitnehmerkammer übermittelt. Nach einer gewissen Zeit soll nochmals an die Meldung erinnert und zusätzlich in den „Amtlichen Bekanntmachungen“ in der Tageszeitung darauf hingewiesen werden.

Die Rückmeldungen ihrer Beschäftigten durch die Arbeitgeber erfolgen ausschließlich an die Wahlorgane der Arbeitnehmerkammer. Die Daten dürfen von der Arbeitnehmerkammer dabei nur zum Zwecke der Durchführung der Wahlen genutzt werden.

13. Bremerhaven

13.1. Nutzung der Haushalts- und Kassen-DV für die Kosten- und Leistungsrechnung

Die Kosten- und Leistungsrechnung (KLR) soll die Transparenz des Aufwandes für ein Produkt (z. B. Zulassung eines Kfz) in der Verwaltung herstellen und das Kostenbewusstsein verstärken. Eine Bezugsgröße sind u. a. die Personalkosten für jedes Produkt. Um diese Kosten festzustellen, ist es erforderlich, die Arbeitsstunden der Mitarbeiter, die an der Erstellung dieses Produktes beteiligt sind, zu ermitteln und auf das einzelne Produkt zu beziehen. Bei großen Beschäftigtengruppen werden die Personalkosten zusammengerechnet und entsprechend auf die Produkte umgelegt. Problematisch wird dieses jedoch, wenn ein Mitarbeiter an der Erstellung verschiedener Produkte beteiligt ist. In diesen Fällen muss zur Kosten- und Leistungsrechnung geklärt werden, wieviel zeitlicher Aufwand für die einzelnen Produkte benötigt wird. Diese Feststellungen sind nur durch entsprechendes Notieren möglich.

In der Bremerhavener Stadtverwaltung sollen für diese Fälle die Zeiterfassungsbögen verwendet werden. Ich habe den Gesamtpersonalrat beim Magistrat dahingehend beraten, die vorgesehene Dienstvereinbarung so zu gestalten, dass die Aufschreibung nur für diesen Zweck verwendet werden darf und auch dann nur, wenn ein Mitarbeiter an der Erstellung verschiedener Produkte beteiligt ist. Mit der Erfassung der Zeitanteile pro Produkt/Mitarbeiter in der jeweiligen Organisationseinheit darf nur ein bestimmter, auf das Datengeheimnis besonders verpflichteter Mitarbeiter betraut werden. Sobald die Daten erfasst und auf Vollständigkeit und Plausibilität überprüft worden sind, werden sie in bereits aggregierter Form an die zentrale Stelle, die für die KLR zuständig ist, übermittelt.

Die Daten erfassende Stelle löscht die Daten nach der Übermittlung. In den Fällen, in denen Plausibilitätsprobleme auftreten, sind die Daten bei Betroffenen, die für das Produkt verantwortlich sind, neu zu erfassen. Hinsichtlich der Personalkostenrechnung werden nicht die echten Personalkosten herangezogen, sondern sog. Standardwerte (in die auch sonstige Allgemeinkosten einbezogen werden), so dass ein weiterer Schutz für das Persönlichkeitsrecht greift.

Diese datenschutzsichernden Maßnahmen wurden in den Entwurf der obengenannten Dienstvereinbarung übernommen. Zum Ende des Berichtsjahres stand die Dienstvereinbarung kurz vor der Unterzeichnung.

13.2. Verweisung

Da es sich anbietet, viele Themen in einem Sachzusammenhang darzustellen, soll an dieser Stelle die Auffindbarkeit von Beiträgen erleichtert werden, die Themen aus Bremerhaven betreffen. Sie finden sich unter Ziff. 1.2. (Internet-Auftritt: www.datenschutz.bremen.de), Ziff. 1.3. (Gründung der „datenschutz nord GmbH“), Ziff. 2.1. (Stadtinformationssystem Bremen (bremen.de), Ziff. 2.3. (Hochschule Bremerhaven), Ziff. 3.5. (Web.Punkte), Ziff. 4.2. (Weitere Themen der Beratungen im Datenschutzausschuss), Ziff. 5.1. (Prüfung der Führung der Personalakten bei verschiedenen Personalstellen), Ziff. 6.3. (Durchführung der Rasterfahndung im Land Bremen), Ziff. 6.10. (Neues DV-System in den Ausländerämtern Bremen und Bremerhaven), Ziff. 6.12.1. (Änderung des Bremischen Meldegesetzes), Ziff. 6.12.2. (Änderung der Bremischen Meldedatenübermittlungsverordnung), Ziff. 6.12.4. (Einwohnerverfahren Meso 96 in Bremerhaven), Ziff. 7.1. (Prüfung des Justiznetzes), Ziff. 9.1. (Vernetzung des Amtes für Jugend und Familie Bremerhaven), Ziff. 10.1. (Internet-Nutzung durch Schulen), Ziff. 12.1. (Wahlen zur Arbeitnehmerkammer), Ziff. 14.10.3. (Verwendung von Vornamen auf Namensschildern der Beschäftigten), Ziff. 14.10.4. (Veröffentlichung von Videoaufnahmen im Internet), Ziff. 14.10.10. (Rasterfahndung durch das BKA bei Versorgungsunternehmen).

14. Datenschutz in der Privatwirtschaft

14.1 Entwicklung des Düsseldorfer Kreises

Auch in diesem Jahr fanden wieder zwei Sitzungen des Düsseldorfer Kreises mit einer Vielzahl von Themen aus verschiedenen Bereichen der Wirtschaft zur Auslegung und Anwendung der Vorschriften des BDSG statt. Neben Berichten aus den Arbeitsgruppen Kredit- und Versicherungswirtschaft, Auskunfteien, Telekommunikation, Tele- und Mediendienste sowie Internationaler Datenverkehr stand wieder die Behandlung einer Vielzahl länderübergreifender Einzelthemen an. An dieser Stelle seien aus dem Spektrum einige genannt wie Datawarehouse — Data Mining und Datenschutz bei Sparkassen, Warndateien im Wohnungswesen, Kundenbindungsprogramme sowie einige der weiter unten näher ausgeführten Punkte, die auch durch Bremen eingebracht wurden, wie etwa die Videoüberwachung in öffentlichen Verkehrsmitteln, das Payback-Rabattkarten-System oder die Nutzung von Rezeptdaten durch Apothekenrechenzentren.

Ein Beratungspunkt galt der Struktur und dem Selbstverständnis des Kreises, u. a. ausgelöst durch die Aufgabe des Vorsitzes im Düsseldorfer Kreis durch das Innenministerium in Nordrhein-Westfalen und die dortige gesetzliche Übertragung der Datenschutzaufsicht auf die Landesbeauftragte für den Datenschutz. Die Mitglieder des Düsseldorfer Kreises, der seit über 20 Jahren — wie der Name schon sagt — in Düsseldorf tagt, haben sich dazu entschlossen, den Vorsitz und damit den Ort der Zusammenkunft im jährlichen Wechsel unter den Ländern rotieren zu lassen. Diese Entscheidung habe ich unterstützt. Beginnend mit Baden-Würtemberg in 2002 soll der Vorsitz in alphabetischer Reihenfolge wahrgenommen werden. Bremen wird somit im Jahre 2006 den Vorsitz inne haben. Auch in anderen Ländern ist die Funktion der Datenschutzaufsicht nach dem BDSG — wie in Bremen schon seit Anbeginn — auf Landesbeauftragte übertragen worden, insbesondere um die von der EG-Datenschutz-Richtlinie geforderte „völlige Unabhängigkeit“ der Datenschutzkontrollinstanz sicherzustellen (vgl. Ziff. 16. dieses Berichts). Wegen dieses Wechsels war es notwendig, auch für die neuen Mitglieder die Verfahrensregeln des Düsseldorfer Kreises als Beratungs- und Abstimmungsgremium in allen Fragen des Datenschutzes im nicht öffentlichen Bereich verbindlich festzulegen.

14.2. Workshop der Datenschutzaufsichtsbehörden

Es fand wieder ein Workshop der Datenschutzaufsichtsbehörden statt, an dem Vertreter von 21 verschiedenen Aufsichtsbehörden teilnahmen. Dieser 7. Workshop stand ganz im Zeichen des novellierten BDSG mit seinen neuen Anforderungen und aktuellen Auslegungs- und Umsetzungsproblemen, auch für die Aufsichtsbehörden. Fast alle Datenschutzaufsichtsbehörden im Bundesgebiet beteiligen sich inzwischen an dem Erfahrungsaustausch, der in Eigenregie veranstaltet wird. Gegenstände des Workshops in Berlin waren:

— Berichte zur angekündigten nächsten Stufe der BDSG-Novelle,

— die Meldepflicht und das neue Verfahrensregister,

— die Neuregelung der Videoüberwachung sowie

— ausgewählte Probleme und Anwendungsfragen.

Auch in diesem Jahr soll wieder ein Workshop durchgeführt werden, weil inzwischen alle Datenschutzaufsichtsbehörden eine derartige Veranstaltung für ihre Arbeit, insbesondere für eine bundeseinheitliche Praxis, für unbedingt erforderlich halten.

14.3. Kooperation mit betrieblichen Datenschutzbeauftragten

Im Berichtsjahr habe ich die bewährte Kooperation mit dem bremischen Erfa-Kreis, in dem sich betriebliche Datenschutzbeauftragte zwecks Meinungs- und Erfahrungsaustausch zusammengeschlossen haben, fortgesetzt. Ich halte diesen Meinungs- und Erfahrungsaustausch zwischen betrieblichen Datenschutzbeauftragten und Datenschutzaufsichtsbehörde vor dem Hintergrund des novellierten BDSG für wichtiger denn je, weil auf diese Weise in unmittelbarem Kontakt

und außerhalb eines förmlichen Prüfungs- und Beratungsgeschehens Datenschutzthemen in einem größeren Kreis von Interessierten erörtert werden können.

14.4. Informationen zum betrieblichen Datenschutzbeauftragten

Aufgrund des novellierten BDSG mit seinen Neuerungen auch für die Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten nach §§ 4 f, 4 g BDSG habe ich Informationen zum betrieblichen Datenschutzbeauftragten entworfen und in mein Internet-Angebot eingestellt. Auf diese Weise hoffe ich, die vielen Anfragen zur Bestellung und zur Tätigkeit eines betrieblichen Datenschutzbeauftragten einfach und ohne große Arbeitsbelastung für mich beantworten zu können. Mit der Information werden u. a. folgende Themen angesprochen:

— Wann muss ein betrieblicher Datenschutzbeauftragter bestellt werden?

— Welche Anforderungen muss der betriebliche Datenschutzbeauftragte erfüllen?

— Welche Stellung hat der betriebliche Datenschutzbeauftragte im Unternehmen?

— Welche Aufgaben hat der betriebliche Datenschutzbeauftragte?

— In welcher Weise kann der betriebliche Datenschutzbeauftragte seine Aufgaben erfüllen?

14.5. Datenschutzprüfungen nach der Novellierung des BDSG

Mit der Novellierung des BDSG haben sich auch für die Datenschutzaufsichtsbehörden wichtige Veränderungen ergeben. Nicht nur der Anwendungsbereich des Gesetzes hat sich geändert (z. B. durch die Veränderungen in der Begrifflichkeit, die Einbeziehung der Videoüberwachung und der Chipkartentechnik, den Einbezug des Datenschutzrechts der anderen EU-/EWR-Mitgliedstaaten im Einzelfall), sondern auch der Aufgabenkatalog und der Befugnisrahmen für die Tätigkeit der Datenschutzaufsichtsbehörden wurden verändert (z. B. zusätzliche Aufgaben, zusätzliche Anzeige- und Unterrichtungsbefugnisse, eigenständiges Strafantragsrecht).

Datenschutzprüfungen sind weiterhin Hauptaufgabe der Datenschutzaufsichtsbehörden, wenngleich der Beratungs- und Informationsaspekt erheblich an Bedeutung zugenommen hat. Für die Prüftätigkeit haben sich starke Veränderungen ergeben (z. B. Wegfall der bisherigen Beschränkungen auf Anlässe oder auf Registerfirmen, Erweiterung des Prüffeldes und dadurch bedingter drastischer Anstieg der möglichen Prüffälle). Dies erfordert ein neues Konzept über das Vorgehen der Datenschutzaufsicht und die Schwerpunkte künftiger Prüftätigkeit.

Anlassprüfungen wird es weiterhin geben. Auslöser derartiger Prüfungen werden wie bisher begründete Eingaben und Beschwerden Betroffener, Hinweise Dritter und eigene Erkenntnisse der Datenschutzaufsichtsbehörden sein. Gegenstand dieser Prüfung sind wie bisher der konkrete Anlass, im Ausnahmefall auch weitere Gesichtspunkte datenschutzrechtlicher Art. Die Verfahrensweise wird sich hier nicht ändern. Die Prüfung des Sachverhaltes sowie anschließende datenschutzrechtliche Würdigung und Ergebnismitteilung an die Beteiligten. Von der Art etwaiger festgestellter Datenschutzverstöße und weiterer Erkenntnisse hängt es ab, wie vor dem Hintergrund der erweiterten Sanktionsmöglichkeiten weiter verfahren wird.

Datenschutzprüfungen ohne Anlass werden mehr und systematischer als bisher Prüfplänen folgen müssen, die möglicherweise regional oder gar bundesweit abgestimmt werden. Eine Schwerpunktbildung ist dabei möglich. Gegenstände sind hier nicht konkrete Anlässe, sondern ggf. auch nur begrenzt die formalen und materiellen Datenschutzerfordernisse. Eine solche Prüfung dürfte wie bisher vorher angekündigt und inhaltlich vorbereitet werden. Die Prüfung selbst erfolgt in aller Regel vor Ort, selbst wenn bestimmte Vor- und Nachbereitungsmaßnahmen schriftlich oder elektronisch durchgeführt werden. Das Ergebnis der Prüfung wird in einem Prüfbericht festgehalten, in den nicht nur die Prüfgegenstände sondern

auch die Feststellungen und datenschutzrechtlichen Bewertungen eingehen. Von der Art etwaiger festgestellter Datenschutzverstöße hängt es auch hier im Wesentlichen ab, wie vor dem Hintergrund der erweiterten Sanktionsmöglichkeiten weiter verfahren werden wird.

Zur Häufigkeit des Prüfens ist zu sagen: Die anlassbezogenen Einzelfallprüfungen müssen auch in Zukunft vollzählig und relativ zeitnah durchgeführt werden, allein schon deshalb, um evtl. rechtliche Schritte seitens der Betroffenen oder seitens der Aufsichtsbehörde einleiten zu können. Bei den Prüfungen ohne Anlass hängt es letztlich von den Ressourcen der Datenschutzaufsichtsbehörde ab, wie viele verantwortliche Stellen mit welcher Intensität in einem bestimmten Zeitraum geprüft werden. Dabei spielen selbstverständlich die Art der jeweils eingesetzten IuK-Technik, ihr Umfang und die zu prüfenden Sachverhalte eine große Rolle. Eine konkrete Zahl läßt sich deshalb schlecht festlegen.

14.6. Umstellung des Registers der meldepflichtigen Stellen

Die Regelungen zur Meldepflicht der nicht öffentlichen verantwortlichen Stellen und damit indirekt auch die Regelungen zur Registerführung der Datenschutzaufsichtsbehörden haben sich durch die Novelle zum BDSG grundlegend geändert. Dabei wurden Meldepflicht und Bestellung eines betrieblichen Datenschutzbeauftragten in Zusammenhang gebracht.

Die Neuregelung sieht als Grundsatz vor, dass automatisierte Verarbeitungen vor ihrer Inbetriebnahme der zuständigen Datenschutzaufsichtsbehörde zu melden sind (§ 4 d Abs. 1 BDSG). Das bedeutet, dass sämtliche DV-Verfahren bzw. DV-Anwendungen, die die Verarbeitung personenbezogener Daten zum Gegenstand haben, gemeldet werden müssen. Die Meldepflicht entfällt jedoch, wenn ein betrieblicher Datenschutzbeauftragter bestellt ist. Die Meldepflicht entfällt ferner, wenn die verantwortliche Stelle personenbezogene Daten für eigene Zwecke erhebt, verarbeitet oder nutzt, hierbei höchstens vier Arbeitnehmer mit der Erhebung, Verarbeitung oder Nutzung beschäftigt werden und entweder eine Einwilligung der Betroffenen vorliegt oder es um die Erfüllung eines Vertrages oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen geht (§ 4 d Abs. 2 und 3 BDSG).

Bei Stellen, die geschäftsmäßig zum Zwecke der Übermittlung oder zum Zwecke der anonymisierten Übermittlung personenbezogene Daten speichern, gilt die Ausnahme von der Meldepflicht nicht (§ 4 d Abs.4 BDSG), d. h., diese Stellen müssen in jedem Fall ihre automatisierten Verarbeitungen bei der zuständigen Datenschutzaufsichtsbehörde melden. Konkret heißt das, dass die Auskunfteien, Adresshandels- und Direktwerbeunternehmen, die Markt- und Meinungsforschungsinstitute etc. ihre automatisierten Verarbeitungen stets bei den Aufsichtsbehörden melden müssen, während die bisher zum Register der Aufsichtsbehörden auch meldepflichtigen Auftragsdatenverarbeiter davon in aller Regel befreit sind.

Der Inhalt der Meldungen wurde ebenfalls stark verändert (§ 4 e BDSG). Während die Meldepflicht des nicht öffentlichen Bereichs bisher im Wesentlichen auf Angaben zur meldepflichtigen Stelle, zum Geschäftszweck der Stelle und der Datenverarbeitung, zum Datenschutzbeauftragten, zur Art der eingesetzten DV-Anlagen und in wenigen Fällen auch zur Art der gespeicherten Daten sowie zu den Datenempfängern und zu den übermittelten Daten beschränkt war, sind nunmehr zusätzlich auch dezidierte Angaben zu den DV-Verfahren, d. h., zu den automatisierten Verarbeitungen und zu den technisch-organisatorischen Sicherungsmaßnahmen zu machen.

Nach § 38 Abs. 2 BDSG führt die zuständige Datenschutzaufsichtsbehörde das Register der nach § 4 d BDSG meldepflichtigen automatisierten Verarbeitungen mit den Angaben nach § 4 e Satz 1 BDSG. Dieses Register kann von jedem eingesehen werden, wobei dieses Einsichtsrecht hinsichtlich der Beschreibung der technisch-organisatorischen Sicherheitsmaßnahmen eingeschränkt ist. Die nicht bei der zuständigen Datenschutzaufsichtsbehörde meldepflichtigen automatisierten Verarbeitungen müssen durch den betrieblichen Datenschutzbeauftragten bzw. — soweit ein solcher nicht bestellt ist — von der verantwortlichen Stelle zugänglich gemacht werden (§ 4 g Abs. 2 BDSG). Das Verarbeitungsregister muss in diesen Fällen bei der Stelle selbst geführt werden.

Aufgrund dieser Neuregelungen und der Tatsache, dass die Regelungen ohne Übergangsfrist in Kraft getreten sind, war ich gezwungen, mein bisheriges Register der meldepflichtigen Stellen relativ schnell und vollständig umzustellen. Parallel zum BDSG-Novellierungsverfahren hatte ich bereits im Vorfeld in Zusammenarbeit mit verschiedenen anderen Datenschutzaufsichtsbehörden mit Vorüberlegungen für ein neues Registerverfahren begonnen (vgl. 23. JB, Ziff. 16.7.1). Unmittelbar nach Inkrafttreten des novellierten BDSG wurden unter meinem Vorsitz die begonnenen Arbeiten wieder aufgenommen und die vorläufig erstellten Unterlagen (Merkblatt zur Meldepflicht, Meldeformulare, Ausfüllhinweise) endgültig fertig gestellt. Ziel der Arbeit war es, möglichst schnell nach Inkrafttreten der neuen Regelungen bundesweit ein einheitliches Register- und Meldeverfahren verfügbar zu machen. Seit dem Sommer des vergangenen Jahres können das Merkblatt zur Meldepflicht, die Meldeformulare und die Ausfüllhinweise aus meinem Internet-Angebot abgerufen werden.

Die Umstellung meines Registers habe ich schrittweise vorgenommen. In einem ersten Schritt habe ich die verantwortlichen Stellen, bei denen ich von einer weiterbestehenden Meldepflicht ausgehen konnte, angeschrieben und um Überprüfung ihrer Meldepflicht gebeten. In einem zweiten Schritt habe ich sodann die übrigen Registerfirmen angeschrieben und um Prüfung ihrer Meldepflicht gebeten. Diese Arbeit ist noch nicht abgeschlossen. Anzunehmen ist, dass hier weitgehend keine meldepflichtigen automatisierten Verarbeitungen vorliegen werden, so dass sich mein Register künftig nur noch auf wenige verantwortliche Stellen mit automatisierten Verarbeitungen bezieht. Dabei ist aber nicht abzusehen, ob kleine Betriebe tatsächlich nicht zur Meldung verpflichtet sind, weil bei ihnen die Ausnahmeregelungen des § 4 d Abs. 2 und 3 BDSG greifen.

14.7. Payback-Verfahren

Im letzten Jahresbericht (23. JB, Ziff. 16.3.) hatte ich über verschiedene datenschutzrechtliche Anforderungen im Zusammenhang mit dem Rabattkartenverfahren „Payback“ berichtet. Diese Fragen betrafen neben einer datenschutzrechtlichen Gestaltung der Einverständniserklärung und der Allgemeinen Geschäftsbedingungen insbesondere die Aufklärung der Inhaber dieser Rabattkarten über die Datenverarbeitung, die Nutzer und die Nutzung dieser Daten, die Verwendung der Daten für Zwecke der Markt- und Meinungsforschung und für Werbemaßnahmen und die Möglichkeiten des Widerrufs der Einwilligung. Das Landgericht München II hat in einem Urteil vom Frühjahr 2001 meine Rechtsauffassung in wesentlichen Teilen bestätigt.

Das Rabattkartenverfahren betreibende Unternehmen unterliegt einer bayerischen Aufsichtsbehörde, die den Datenschutzaufsichtsbehörden nach einem längeren Abstimmungsprozess vor kurzem mitgeteilt hat, welche Anforderungen sie an die veranwortliche Stelle für das Payback-Verfahren stellt. Sollten der Betreiber und die angeschlossenen Partnerfirmen dieses Rabattkartenverfahrens diesen Forderungen zustimmen, so wäre auch meinen wesentlichen Kritikpunkten Rechnung getragen.

14.8. Patientendaten — Apotheken-Rechenzentren — Apotheken-CD

Apotheken leiten Rezepte, die ihnen von Versicherten bei einer gesetzlichen Krankenversicherung vorgelegt werden, in der Regel nicht direkt der jeweiligen Krankenkasse zur Abrechnung zu, sondern nehmen hierfür die Dienste von hierauf spezialisierten berufsständischen oder gewerblichen Rechenzentren in Anspruch. Diese bereiten die ihnen zugeleiteten Rezeptdaten, d. h. die Identitätsdaten von Ärzten und Patienten sowie die verschriebenen Arzneimittel, elektronisch auf, bevor sie sie den jeweiligen Kassen zuordnen und zuleiten. § 300 Abs. 2 SGB V lässt dies ausdrücklich zu.

In letzter Zeit sind die Apotheken-Rechenzentren, auch das in Bremen ansässige für Apotheken in ganz Norddeutschland tätige Norddeutsche Apotheken-Rechenzentrum (NARZ), dazu übergegangen, die Rezeptdaten über den Zweck der Abrechnung mit den Kassen hinaus für andere Zwecke aufzubereiten und die neu strukturierten Daten der jeweiligen Apotheke auf CD oder im Onlineabruf zur Verfügung zu stellen. Das NARZ hatte die so genannte Apotheken-CD allein im

Lande Bremen an etwa 50 Apotheken ausgeliefert. Bei einem Prüfbesuch stellte mir das NARZ die Inhalte der von ihm vertriebenen „Apotheken-CD“ vor. Sie bietet:

— Kopien (Images) der von der jeweiligen Apotheke eingereichten Rezepte zum Zwecke der Rezeptrecherche.

— Versicherten-Datenbank mit Krankenversichertennummern, Verordnungsvolumen und Medikamentenlisten zum Zweck der Beratung der Patienten und zum Ausdruck von Medikamentenlisten zur Vorlage durch die Patienten bei Krankenkassen (Zuzahlungsbescheinigungen) und bei Finanzämtern (Nachweis von Sonderbelastungen).

— Ärzte-Datenbank mit Arztnummern und Verordnungen sowie diversen Funktionen für die Auswertung des Verschreibungsverhaltens der einzelnen Ärzte zum Zweck der Führung von Ärzte-Renn-Statistiken und der pharmazeutischen Beratung von Ärzten.

Die Apotheken, die eine solche CD bezogen, konnten mit ihrer Hilfe auf die gespeicherten Daten auch zu anderen als Abrechnungszwecken zugreifen, ohne dass die betroffenen Patienten zuvor eingewilligt hatten. Auf dem Bildschirm erschien lediglich vor Aufruf der Versicherten-Datenbank ein Hinweis darauf, dass die in ihr erfassten Daten nur mit schriftlicher Einwilligung des jeweiligen Patienten aufgerufen werden dürften und entsprechende Vordrucke auf Anforderung zugeleitet würden. In einer von mir exemplarisch überprüften Apotheke waren Einwilligungen der Kunden nicht eingeholt worden, vielmehr hatte der Apotheker den Vordruck selbst unterzeichnet und dem Rechenzentrum eingesandt.

Ein derartiges Verfahren ist rechtswidrig. Bereits 1999 hatten die obersten Aufsichtsbehörden für den Datenschutz festgestellt, dass die Apotheken und ihre Rechenzentren die Rezeptdaten nur für die Abrechnung mit den Krankenkassen verarbeiten dürfen, für andere Zwecke dagegen bedürfte es der Einwilligung der Betroffenen. Meinem Hinweis auf die Rechtslage entgegnete das NARZ, es stehe im Wettbewerb zu anderen Rechenzentren, die den Apotheken entsprechende Angebote machten, ohne dass die zuständigen Aufsichtsbehörden gegen diese vorgegangen seien. Diese Sachlage veranlasste mich dazu, nicht nur dem NARZ gegenüber, sondern auch bundesweit mit dem Ziel tätig zu werden, möglichst einvernehmlich sowohl eine für die Versicherten datenschutzkonforme als auch für die Rechenzentren und Apotheken akzeptable Lösung wie folgt zu erreichen:

Ich erklärte mich bereit, in Bremen den weiteren Vertrieb einer in Inhalten und Funktionen reduzierten CD vorübergehend zu tolerieren, zugleich drang ich aber darauf, dass das NARZ ein Verfahren entwickeln solle, das technisch und organisatorisch sicherstellt, dass die Betroffenen über die Nutzung ihrer Rezeptdaten zu anderen als den gesetzlich festgelegten Zwecken selbst entscheiden können. Dem ist das NARZ nachgekommen. Zwar vertreibt das NARZ weiterhin CD mit Rezeptdaten, ohne dass die Betroffenen zuvor in die Speicherung ihrer Daten auf der CD eingewilligt hätten. Bevor aber der Apotheker die CD auslesen kann, muss zunächst der Betroffene seine Krankenversichertenkarte durch einen Kartenleser „gezogen“ haben. Dann erscheint auf dem Bildschirm eine Maske, in die differenziert die Einwilligung des Patienten in jede einzelne der Funktionen der CD eingetragen werden kann. Diese Erklärung soll ausgedruckt und vom Patienten unterzeichnet werden. Nachdem schließlich der Apotheker die Abgabe der Einwilligung bestätigt, kann er die entsprechenden Funktionen und Inhalte aufrufen. Auf diese Weise erhält der Patient Gelegenheit, nur die ihm nützlich erscheinenden Funktionen zu erlauben (z. B. Rezeptrecherche oder Ausdruck einer Zuzahlungsbescheinigung für seine Krankenkasse).

Zugleich bemühte ich mich bundesweit im Düsseldorfer Kreis um eine Zustimmung der anderen obersten Aufsichtsbehörden zu dem mit dem NARZ abgestimmten Verfahren mit dem Ziel, dass die anderen Aufsichtsbehörden, in deren Zuständigkeitsgebiet ein Apotheken-Rechenzentrum seinen Sitz hat, ein vergleichbares Verfahren durchzusetzen versuchen. Eine Einigung ist bislang nicht gelungen. Zwar teilt die Mehrheit des Düsseldorfer Kreises meine Rechtsauf-

fassung und ist z. B. in Bayern ein vergleichbares Verfahren zwischen Rechenzentrum und Aufsichtsbehörde abgestimmt worden, doch fand zugleich die Forderung nach Verbesserung und Konkretisierung des vom NARZ entwickelten Verfahrens Unterstützung. Darüber hinaus vertreten der Bundesbeauftragte für den Datenschutz und die Aufsichtsbehörde Nordrhein-Westfalen die Auffassung, auch die Einwilligung der Betroffenen könne die Nutzung ihrer Rezeptdaten für die CD nicht legitimieren.

Zuvor hatte ich im Auftrag des Düsseldorfer Kreises an das Bundesministerium für Gesundheit die Frage gerichtet, ob es der Rechtsauffassung zustimme, die in Rede stehende Verarbeitung von Rezeptdaten sei rechtswidrig, könne aber durch Einwilligung der Betroffenen legitimiert werden. Das Ministerium hatte dem unter Hinweis auf das informationelle Selbstbestimmungsrecht der Betroffenen zugestimmt. Inzwischen hat jedoch der Bundesbeauftragte für den Datenschutz das Ministerium gebeten, seine Stellungnahme unter Hinblick auf die strikte Ablehnung kommerzieller Verwertung von Rezeptdaten seitens der französischen Datenschutzaufsichtsbehörde CNIL zu überdenken.

Zugleich hatte ich — ebenfalls im Auftrag des Düsseldorfer Kreises — die Bundesvereinigung Deutscher Apothekenverbände (ABDA) und die Bundesapothekerkammer angeschrieben, sie auf die Rechtswidrigkeit der Praxis vieler berufsständischer Apotheken-Rechenzentren hingewiesen, Rezeptdaten ohne Einwilligung der Betroffenen auf CD zu speichern und an Apotheken zu vertreiben. Die ABDA hatte hierauf erwidert, sie erachte die kritisierte Praxis mit Hinblick auf die öffentlichen Aufgaben der Apotheken zur Sicherstellung einer ordnungsgemäßen Arzneimittelversorgung der Bevölkerung für rechtmäßig, hat aber Gesprächsbereitschaft signalisiert.

Kürzlich hat mir das NARZ erbetene Ergänzungen und Konkretisierungen des von ihm entwickelten Verfahrens zugeleitet. Diese habe ich allen am Verfahren Beteiligten zugeleitet. Ich erkenne zwar an, dass Schutznormen nicht durch eine einfache Einwilligung ausgehebelt werden können. Ich strebe aber weiterhin an, dass die Aufsichtsbehörden mit den Apotheken-Rechenzentren bzw. der ABDA ein Verfahren abstimmen, das eine Nutzung der auf den CD gespeicherten Rezeptdaten von der Einwilligung der jeweils Betroffenen abhängig macht, zumal die Zugriffe der Apotheken in vielen Fällen im Interesse der Betroffenen liegen dürften und von diesen gesteuert werden können. Ich glaube, davon ausgehen zu können, dass das vom NARZ entwickelte und modifizierte Verfahren nunmehr von allen Beteiligten akzeptiert wird. Andernfalls muss der Gesetzgeber Öffnungsklauseln für anerkannte Zwecke schaffen.

14.9. Datenabruf der Finanzämter bei den Firmen

Am 1. Januar 2002 ist die neue Bestimmung des § 147 Absatz 6 AO (Abgabenordnung) in Kraft getreten. Über diese Rechtsvorschrift habe ich bereits berichtet (23. JB, Ziff. 12.2.) und darauf hingewiesen, dass die Betriebe verpflichtet sind, ihre DV so zu gestalten, dass eine Trennung von steuerrechtlich relevanten Daten und anderen Daten gewährleistet ist. Den Steuerbehörden sind nur die Daten zur Verfügung zu stellen, die steuerrechtlich relevant sind. So haben die verantwortlichen Stellen sicherzustellen, dass die Daten von Kunden und Mitarbeitern, soweit sie für die Steuerverarbeitung nicht vorzuhalten sind, auch ihr nicht übermittelt werden. Mir ist bekannt, dass diese datenschutzrechtlichen Vorkehrungen in vielen Betrieben noch nicht getroffen worden sind bzw. ihnen keine Buchhaltungssoftware zur Verfügung steht, die dieses umsetzt.

14.10. Ausgewählte Prüfergebnisse im nicht öffentlichen Bereich

Neben meiner Beratungstätigkeit (die in diesem Jahr wegen des neuen BDSG und der Neuregelungen in weiteren Rechtsbereichen wie z. B. dem TDG/TDDSG, SignaturG zugenommen hat) und der Bearbeitung von Eingaben und Beschwerden (so genannte Anlassprüfungen) habe ich auch in diesem Jahr wieder mehrere systematische Datenschutzprüfungen mit einem bestimmten Prüfansatz durchgeführt (weitere Prüfungen unter Ziff. 2. dieses Berichts). Einige Prüfungen fanden noch nach alter Rechtslage (BDSG) statt, die Mehrzahl der Prüfung basierte auf dem novellierten BDSG.

14.10.1. Detektei, Rechenzentrum und Wirtschaftsunternehmen

Ich habe eine Detektei, ein privates Rechenzentrum, eine Brauerei, ein Handelsunternehmen (Im- und Export) und ein Kreditberatungsunternehmen geprüft. Bei den genannten Prüfungsfällen ging es um die datenschutzrechtliche Meldepflicht und die Bestellung sowie Tätigkeit eines betrieblichen Datenschutzbeauftragten. Darüber hinaus wurden auch — sofern relevant — die Verpflichtung der Mitarbeiter auf das Datengeheimnis, eine evtl. Auftragsdatenverarbeitung sowie technisch-organisatorische Datensicherungsfragen geprüft.

Gravierende Mängel wurden bei diesen Prüfungen nicht festgestellt. Es wurden jedoch in einzelnen Fällen, wie bei den früheren Prüfungen auch, leichtere Verstöße im Zusammenhang mit der Meldepflicht (z. B. keine oder nur sehr zögerliche Änderungsmeldungen, keine rechtzeitige Abmeldung), der Bestellung des betrieblichen Datenschutzbeauftragten (z. B. fehlende schriftliche Bestellung) sowie der Auftragsdatenverarbeitung (z. B. bei der Gestaltung der Vertragsverhältnisse oder Subauftragsverhältnisse) festgestellt. Förmliche Verfahren (z. B. Abberufungsverlangen des betrieblichen Datenschutzbeauftragten, Anordnung von Maßnahmen nach § 9 BDSG, Bußgeldverfahren) wurden nicht eingeleitet.

14.10.2. Bekanntgabe von Kündigungen in einer Betriebsversammlung

Auf die Anfrage eines Beauftragten für den Datenschutz eines Betriebes, ob es zulässig sei, dass Kündigungen in einer Betriebsversammlung ausgesprochen und damit alle Anwesenden davon in Kenntnis gesetzt würden, habe ich mitgeteilt, dass diese Art der Bekanntgabe personenbezogener Daten nicht zur Zweckbestimmung der Arbeitsvertragsverhältnisse erforderlich ist und schutzwürdige Interessen der von der Kündigung betroffenen Arbeitnehmer erheblich überwiegen. Der betriebliche Datenschutzbeauftragte hat daraufhin erklärt, er habe den Arbeitgeber aufgrund meiner Stellungnahme von einer humanen Vorgehensweise überzeugt und den entsprechenden Mitarbeitern in einem persönlichen Gespräch mitgeteilt, dass sie schriftliche Kündigungen zu erwarten hätten.

14.10.3. Verwendung von Vornamen auf Namensschildern der Beschäftigten

Ich bin von Beschäftigten eines SB-Warenhauses in Bremerhaven darüber informiert worden, dass sie seit Ende des Jahres 2000 Namensschilder tragen müssen, auf denen Vor- und Zunamen der Beschäftigten vermerkt sind. Häufiger seien insbesondere weibliche Beschäftigte unter Nennung ihres Vornamens sozusagen „unflätig“ angesprochen worden. Außerdem wurde die Befürchtung geäußert, Kunden könnten unter Verwendung von Adress- und Telefonbüchern Privatanschriften und Telefonnummern mit den vollständigen Namen verbinden, Kontakt zu den Betroffenen aufnehmen oder die Daten anderweitig missbrauchen. Insoweit würden die schutzwürdigen Interessen der Betroffenen beeinträchtigt. Inzwischen hat der betriebliche Datenschutzbeauftragte der bundesweiten Warenhauskette meinen Vorschlag übernommen, es den Beschäftigten freizustellen, ob sie auch ihren Vornamen auf den Namensschildern tragen wollen.

14.10.4. Veröffentlichung von Videoaufnahmen im Internet

Eine ehemalige Mitarbeiterin einer Firma im Dienstleistungszentrum Grünhöfe in Bremerhaven (DLZ) hat erklärt, ihre Firma habe im Rahmen der Darstellung von Einrichtungen des DLZ auch Videoaufnahmen über ihre Tätigkeit erstellt. Diese Aufnahmen seien ohne ihre Einwilligung im Internet veröffentlicht worden. Die Firma hat auf Anfrage erklärt, der besagte Videofilm sei inzwischen gelöscht worden und nicht mehr im Internet abrufbar. Sie hat weiter zugesagt, in Zukunft derartige Videoaufnahmen nur mit schriftlicher Einwilligung der Betroffenen zu veröffentlichen.

14.10.5. Videoüberwachung in einem Betrieb und einer Betriebshalle

Ein Mitarbeiter eines Zuliefererbetriebes für einen Autohersteller hat erklärt, im Büro würde Videoüberwachung eingesetzt. Außerdem sei der Einsatz in der Betriebshalle beabsichtigt.

Anlässlich einer Prüfung vor Ort erklärte der Firmenleiter, die Videoüberwachung im Büro sei erforderlich, weil bereits einmal Geld aus seinem Schreibtisch gestohlen worden sei. Das Büro müsse aufgrund der Arbeitsabläufe zumindest in den Spätschichten offen sein. Mein Hinweis auf die Anforderungen aus § 6 b BDSG führte dazu, dass zugesichert wurde, die Videoüberwachung im Bürobereich werde nur während der Spätschichten aktiviert, und auch auf den Umstand der Videoüberwachung werde hingewiesen, damit die Arbeitnehmer und Besucher darüber informiert seien.

Die beabsichtigte Videoüberwachung in der Betriebshalle war nach Angaben des Produktionsleiters erforderlich, weil dort Kunststofftanks für Kraftfahrzeuge der Auftragsfirma zur Lieferung aufbereitet würden. Es seien bereits Werkzeug und eine größere Leiter gestohlen worden. Außerdem sei ein Schlauch bzw. anderer Gegenstand in einen Tank gesteckt worden, was zu erheblichen Problemen mit Daimler-Chrysler geführt habe. Die Firma teile sich die Betriebshalle mit anderen Firmen; die Tore sind während der Schichten geöffnet. Da der Videoeinsatz während der Arbeitszeiten eine lückenlose Überwachung der Arbeitnehmer bedeuten würde, überwiegen deren schutzwürdige Interessen. Der Betriebsleiter hat daher zugesagt, die Videoüberwachung mittels einer Zeitschaltuhr nur in den festgelegten Pausenzeiten und am Wochenende außerhalb der Arbeitszeiten zu aktivieren und darauf entsprechend hinzuweisen.

14.10.6. Videoüberwachung im Taxi

Ein Taxiunternehmer der Fachvereinigung Personenverkehr hat den Videoeinsatz in einem Taxi als Modellversuch vorgestellt und um Beratung gebeten. Dazu wurde erklärt, durch den Einsatz der Videoüberwachung im Taxi könnten Gefahren für Leib und Leben der Taxifahrer sowie Überfälle abgewendet werden. Der Unternehmer setze seit mehreren Jahren Videoüberwachung ein und habe seither keine Übergriffe mehr erlebt. Die Videokamera werde nur beim Öffnen der Beifahrertür sowie der hinteren Türen aktiviert. Dabei würden jedesmal fünf Bilder der Fahrgäste aufgenommen. Während der Fahrt sei die Kamera inaktiv. Im Taxi befinde sich das Aufzeichnungsgerät einschließlich einer ausbaufähigen Speichereinheit und über der Windschutzscheibe vor dem Beifahrersitz eine kleine Videokamera. Ein Hinweis auf die Videoanlage ist auf der Windschutzscheibe vor dem Beifahrersitz erkennbar. Nach Angaben des Unternehmers könnten bis zu 1.500 Aufnahmen bei minimaler Auflösung gespeichert werden; danach würde automatisch überschrieben. Je größer die Auflösung sei, desto weniger Aufnahmen könnten gespeichert werden

Im Gebäude der Fachvereinigung steht ein PC, der nach Angaben des Unternehmers mit einer speziellen Software ausgestattet ist. Der Speicher kann aus dem Fahrzeug ausgebaut werden. Nur in Verbindung mit einem speziellen Kabel und der speziellen PC-Software ist die Einsicht in die Aufnahmen möglich. Im Falle strafbarer Handlungen soll der im Fahrzeug befindliche Speicher vom Unternehmer herausgenommen, die Bilder eingesehen, und nur die einschlägigen Bilder des Fahrgastes bzw. Täters sollen ausgedruckt und an die Polizei übergeben werden.

Nach Ablauf des Modellversuchs sei vorgesehen, allen Taxiunternehmern, die der Fachvereinigung Personenverkehr und dem Taxi-Ruf Bremen angehören, die Ausstattung zu ermöglichen. Es handele sich um ca. 250 Unternehmer, die über insgesamt rund 500 Taxen verfügen würden. Jedes eingebaute System solle mit einem Code versehen werden. Eine Liste der Codes solle bei der Zentrale unter Verschluss vorhanden sein und dürfe nur verwendet werden, wenn nach einem Vorfall ein betroffener Taxifahrer den Speicher aus seinem Taxi ausbaut oder seinem Vertreter vorlegt, weil nur diese beiden Personen befugt wären, das System zu bedienen.

Die mir so vorgestellte Videoaufzeichnungsanlage habe ich folgendermaßen bewertet: Die genannten Zwecke der Gefahrenabwehr und Straftatenvermeidung erfüllen die Voraussetzungen nach § 6 b Abs. 1 Nr. 3 BDSG, wonach die Videoüberwachung dann zulässig ist, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist. Dabei dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Um

den Interessen der Betroffenen Rechnung zu tragen, habe ich u. a. folgende Empfehlungen abgegeben:

— Es sollen außen an den Fahrzeugen bzw. den Türen, die den Kontakt auslösen, deutlich sichtbare Hinweisschilder auf die Videoaufzeichnung angebracht werden, so dass der Videoeinsatz schon vor Besteigen des Fahrzeugs vom Fahrgast erkannt werden kann, eine Maßnahme, die zugleich auf mögliche Täter abschreckend wirken dürfte.

— Der PC für die Bildverarbeitung ist so einzurichten, dass gewährleistet ist, dass nur ein bestimmter Personenkreis Zugriff auf diesen Rechner und damit die Software für die Bildverarbeitung und die Bilder selbst hat. Durch eine geeignete Rechtevergabe auf Betriebssystemebene ist der unbefugte Zugriff auf die Bildverarbeitungssoftware, die Bilder und die Verzeichnisse, in denen die Bilder abgelegt werden, zu verhindern. Dazu ist es notwendig, ein geeignetes Betriebssystem einzusetzen. Für die Nutzung der Anwendung und der Bilddaten aus der Videoüberwachung sind dann eigene Benutzerkennungen (Accounts) im Betriebssystem anzulegen, die ausschließlich die Bilder verarbeiten können. Der PC sollte nicht (wie noch beim Modellversuch) unmittelbar an das Internet angeschlossen sein. Für die auf dem Rechner gespeicherten Bilddaten müssen Löschungsfristen festgelegt werden.

— Da im Falle strafbarer Handlungen eine Übertragung der Bilder auf den Rechner erfolgt, sollten die Aufnahmen in den Fahrzeugen in der Regel nicht länger als 24 Stunden aufbewahrt werden. Die Löschungsfrist ist durch entsprechende Programmierung des Aufnahmesystems in den Fahrzeugen zu gewährleisten, z. B. durch eine zeitabhängige Löschung der Daten oder durch die Überschreibfrequenz bei entsprechender Wahl des Bild-Speichervolumens.

Der Taxiunternehmer hat erklärt, er werde die genannten Anforderungen unter Beteiligung der Softwarefirma und dem Hersteller der Anlage umsetzen und mich darüber unterrichten.

14.10.7. Vorlage der Sozialversicherungsausweise durch Lkw-Fahrer

Ein Lkw-Fahrer aus Bremen hat mich darüber unterrichtet, ein Stahlproduzent würde von den Lkw-Fahrern der Lieferfirmen die Vorlage der Sozialversicherungsausweise verlangen. Es sei ein entsprechender Aushang an der Verladestelle auf dem Firmengelände vorhanden.

Auf Nachfrage erklärte die Firma, es handele sich um einen Irrtum. Tatsächlich sei sie nach dem Gesetz zur Bekämpfung der illegalen Beschäftigung im gewerblichen Güterkraftverkehr nur verpflichtet, die Mitführung der Transportlizenzen und bei Fahrern aus Drittländern, die in einem EU-Staat arbeiten, die entsprechende Arbeitsgenehmigung zu überprüfen. Der genannte Aushang sei entfernt worden; die Vorlage der Sozialversicherungsausweise werde nicht mehr verlangt.

14.10.8. Fahrradclub-Umfrage mit Hilfe der Hochschule Bremen

Im Sommer des Berichtsjahres bin ich von einem Fahrradclub gebeten worden, ihn bei der Gestaltung einer Umfrage zu beraten. Im Rahmen eines Studienprojektes sollten Studierende der Hochschule Bremen eine Umfrage durchführen. Es sollten verschiedene Informationen gewonnen werden, u. a. welche Nutzerkreise nach Geschlecht, Alter, Beruf und Einkommen die Angebote des Fahrradclubs nachfragen und welche Radreisegewohnheiten nach Länge der Etappen bei Nutzung eines eigenen Fahrrades bestehen, welches Kartenmaterial benutzt wird und wie viel Geld ausgegeben wird.

Bei meiner Beratung habe ich eine umfassende Aufklärung über den Zweck der Umfrage, die Nutzung der gewonnenen Daten und die Freiwilligkeit der Teilnahme verlangt, auf die Zusicherung der Anonymität bei der Veröffentlichung der Auswertungsergebnisse und die Löschung der Fragebögen hingewirkt sowie Vorschläge für einen Vertrag mit der Hochschule Bremen unterbreitet, die mit der Weiterverarbeitung der erhobenen Daten beauftragt werden sollte.

14.10.9. Fragebogenaktion einer Firma über Berufsschullehrer

Aufgrund einer Eingabe habe ich erfahren, dass eine große Bremer Spedition eine Fragebogenaktion bei Auszubildenden über Lehrer der Berufsschule für Großhandel, Außenhandel und Verkehr durchgeführt hat. Die nach Auswertung gewonnenen personenbezogenen Daten über Lehrer dieser Schule hat sie an andere Firmen weitergegeben.

Die Firma hat den Sachverhalt bestätigt und gleichzeitig bedauert, die Daten weitergegeben zu haben. Sie hat zugesagt, derartige Fragebogenaktionen in Zukunft nicht mehr vorzunehmen. Eine solche Aktion darf nicht hinter dem Rücken der Lehrer durchgeführt werden und ist nur mit Einwilligung der Betroffenen zulässig. Weil nach § 35 Abs. 2 Nr. 1 BDSG unzulässig gespeicherte personenbezogene Daten zu löschen sind, habe ich die Firma aufgefordert, die Löschung vorzunehmen und die Firmen, an die diese Daten übermittelt worden sind, ebenfalls dazu aufzufordern. Die Firma hat dies inzwischen bestätigt.

14.10.10. Rasterfahndung durch das BKA bei Versorgungsunternehmen

Mit Schreiben vom 11. Oktober 2001 hat das Bundeskriminalamt (BKA) den Verband der Elektrizitätswirtschaft angeschrieben und um Übersendung von „Daten über Mitarbeiter und Dritte (männlichen Geschlecht im Alter von 18 bis 40 Jahren), die sich im Firmenbereich bewegen können“ gebeten; mit Firmenbereich waren in diesem Zusammenhang insbesondere die angeschlossenen Elektrizitätsunternehmen gemeint. Bei dieser Datenanforderung für Zwecke der Rasterfahndung bezog sich das BKA auf § 7 BKAG (BKA-Gesetz) als Rechtsgrundlage. Die Erhebung der Daten für die Rasterfahndung ist aber Aufgabe der Polizei der Länder, die in dem Schreiben vom BKA zitierte Rechtsvorschrift gibt ihm keine Befugnis zur Anordnung einer Rasterfahndung. Sie ist lediglich die Befugnisnorm dafür, beim BKA bereits vorhandene Daten miteinander abzugleichen. Diese Aufteilung entspricht der grundgesetzlich festgelegten Aufgabe der Zentralstellenfunktion des BKA.

Da der Verband der Elektrizitätswirtschaft selbst keine eigenen Mitarbeiter im Sinne der Anforderung des BKA beschäftigt, hat der Verband die Datenanforderung des BKA an die angeschlossenen Elektrizitätsversorgungsunternehmen weitergeleitet. Betriebliche Datenschutzbeauftragte von Elektrizitätsversorgungsunternehmen in Bremen und Bremerhaven haben mich nach Eingang des Schreibens über die Anforderung unterrichtet und um eine datenschutzrechtliche Stellungnahme dazu gebeten. Im Vordergrund stand die Frage, ob sie verpflichtet seien, die angeforderten Daten an des BKA zu übermitteln. Da ich keine hinreichende Rechtsgrundlage feststellen konnte, habe ich den Bundesbeauftragten für den Datenschutz um Aufklärung gebeten. Daraufhin wurde mir mitgeteilt, das BKA habe lediglich den Unternehmen eine Datenrasterung und -übermittlung der Daten (Mitarbeiter und Dritter) auf „freiwilliger Basis“ empfohlen. Diese Auslegung der Datenanforderung durch das BKA konnte ich seinem Anschreiben an die Versorgungsunternehmen nicht entnehmen. Darüber hinaus kann nicht das Unternehmen entscheiden, sondern nur der jeweils Betroffene, ob seine Daten auf freiwilliger Basis weitergegeben werden dürfen. Die Unternehmen haben nach ihrer Auskunft die Rechtslage beachtet und zur Wahrung der Schutzrechte ihrer Mitarbeiter und der Externen sich dahingehend entschieden, keine Daten an das BKA weiterzugeben.

15. Entschließungen der Datenschutzkonferenzen im Jahr 2001

15.1. Äußerungsrecht der Datenschutzbeauftragten

(Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001)

Die Datenschutzbeauftragten des Bundes und der Länder sind verpflichtet, Einzelne — wie es die Rechtsprechung des Bundesverfassungsgerichts und die Richtlinie der Europäischen Gemeinschaft zum Datenschutz von 1995 vorsehen — vor rechtswidrigem Umgang mit ihren personenbezogenen Daten wirksam zu schützen. Die damit verbundenen Beratungs- und Kontrollaufgaben verleihen den

Datenschutzbeauftragten ein öffentliches Wächteramt, das die Befugnis einschließt, Behördenverhalten auch im Detail und, soweit der Bedeutung der Sache angemessen, auch unter Bezeichnung der Amtsträgerinnen und Amtsträger öffentlich zu rügen.

Aus gegebenem Anlass wendet sich die Konferenz der Datenschutzbeauftragten des Bundes und der Länder energisch gegen Versuche im Land Sachsen, durch gesetzgeberische Maßnahmen dieses Recht zu beschneiden und die Arbeit des Sächsischen Datenschutzbeauftragten zu behindern.

15.2. Datenschutz bei der Bekämpfung von Datennetzkriminalität

(Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001)

Der Europarat entwirft gegenwärtig zusammen mit anderen Staaten, insbesondere den USA und Japan, eine Konvention über Datennetzkriminalität (Cybercrime-Konvention), die über ihren Titel hinaus auch die automatisierte Speicherung von Daten im Zusammenhang mit anderen Straftaten regeln soll.[1]

Die Datenschutzbeauftragten des Bundes und der Länder verkennen nicht, dass das Internet — ebenso wie andere technische Hilfsmittel — für Straftaten missbraucht wird. Sie teilen daher die Auffassung des Europarats, dass der Kriminalität auch im Internet wirksam begegnet werden muss. Allerdings ist zu beachten, dass sich die weit überwiegende Anzahl der Nutzenden an die gesetzlichen Vorgaben hält. Insoweit stellt sich die Frage der Verhältnismäßigkeit von Maßnahmen, die alle Nutzenden betreffen.

Die Datenschutzbeauftragten des Bundes und der Länder teilen die Auffassung der Europäischen Kommission, dass zur Schaffung einer sichereren Informationsgesellschaft in erster Linie die Sicherheit der Informationsinfrastruktur verbessert werden und anonyme wie pseudonyme Nutzungsmöglichkeiten erhalten bleiben müssen; über Fragen der Bekämpfung der Datennetzkriminalität sollte ein offener Diskussionsprozess unter Einbeziehung der Betreiberinnen und Betreiber, Bürgerrechtsorganisationen, Verbraucherverbände und Datenschutzbeauftragten geführt werden.[2]

Die Konferenz regt eine entsprechende Debatte auch auf nationaler Ebene an und bittet die Bundesregierung, hierfür den erforderlichen Rahmen zu schaffen.

Die Konferenz der Datenschutzbeauftragten fordert die Bundesregierung auf, sich bei der Schaffung von nationalen und internationalen Regelungen zur Bekämpfung von Datennetzkriminalität dafür einzusetzen, dass

— Maßnahmen zur Identifikation von Internet-Nutzenden, zur Registrierung des Nutzungsverhaltens und Übermittlung der dabei gewonnenen Daten für Zwecke der Strafverfolgung erst dann erfolgen dürfen, wenn ein konkreter Verdacht besteht,

— der Datenschutz und das Fernmeldegeheimnis gewährleistet und Grundrechtseingriffe auf das unabdingbare Maß begrenzt werden,

— der Zugriff und die Nutzung personenbezogener Daten einer strikten und eindeutigen Zweckbindung unterworfen werden,

— Daten von Internet-Nutzenden nur in Länder übermittelt werden dürfen, in denen ein angemessenes Niveau des Datenschutzes, des Fernmeldegeheimnisses und der Informationsfreiheit gewährleistet ist sowie verfahrensmäßige Garantien bei entsprechenden Eingriffen bestehen.

---

1 European Committee on Crimes Problems (CDPC), Committee of Experts on Crime in Cyber-Space (PC-CY), Draft Convention on Cyber-crime (PC-CY [2000] Draft No. 25)

2 Mitteilung der Kommission an den Rat, das Europäische Parlament, den Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen vom 26. Januar 2001 — KOM (2000) 890 endgültig

15.3. Datenschutz beim elektronischen Geschäftsverkehr

(Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001)

Die Konferenz wendet sich mit Entschiedenheit gegen Anträge, die gegenwärtig dem Bundesrat zum Entwurf eines Gesetzes zum elektronischen Geschäftsverkehr (BR-Drs. 136/01) vorliegen. Danach sollen Bestands- und Nutzungsdaten bei Telediensten nicht nur an Strafverfolgungsbehörden, sondern auch an Verwaltungsbehörden zur Verfolgung von Ordnungswidrigkeiten und an Nachrichtendienste übermittelt werden. Darüber hinaus sollen die Anbieterinnen und Anbieter zur Speicherung von Nutzungsdaten auf Vorrat für eine mögliche spätere Strafverfolgung verpflichtet werden.

Die Datenschutzbeauftragten weisen darauf hin, dass sich anhand dieser Daten nachvollziehen lässt, wer wann mit wem kommuniziert hat, wer welches Medium genutzt hat und damit wer welchen weltanschaulichen, religiösen und sonstigen persönlichen Interessen nachgeht. Eine pauschale Registrierung jeder Inanspruchnahme von Telediensten zur staatlichen Überwachung greift tief in das Persönlichkeitsrecht der betroffenen Nutzerinnen und Nutzer ein und berührt auf empfindliche Weise deren Informationsfreiheit. Der Bundesrat wird daher aufgefordert, diese Anträge abzulehnen.

15.4. Informationszugangsgesetze

(Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001)

Die Konferenz verfolgt mit Interesse die Bestrebungen des Bundes, ein Informationszugangsgesetz zu schaffen und dem Bundesbeauftragten für den Datenschutz die Aufgaben zur Sicherung des Informationszugangs zu übertragen. Die Bundesregierung nimmt damit die Überlegungen auf, die in Artikel 255 EU-Vertrag und Artikel 42 EU-Grundrechte-Charta zum Ausdruck kommen. Die Konferenz betont, dass das Recht auf informationelle Selbstbestimmung der Einzelnen dem freien Zugang zu behördeninternen, amtlichen Informationen nicht entgegen steht, wenn die Privatsphäre der Betroffenen sowie Betriebsgeheimnisse gesetzlich geschützt bleiben. Die Berichte aus den Ländern Berlin, Brandenburg und Schleswig-Holstein zeigen, dass die datenschutzrechtlichen Gewährleistungen für die informationelle Selbstbestimmung sich mit dem erweiterten Zugangsrecht zu den Informationen öffentlicher Stellen unter der Voraussetzung entsprechender Schutzmechanismen vereinbaren lassen. Die Zusammenführung von Datenschutz- und Informationszugangskontrolle kann diese Gewährleistung institutionell absichern.

15.5. Novellierung des Melderechtsrahmengesetzes

(Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen die Absicht der Bundesregierung, das Melderechtsrahmengesetz im Hinblick auf die neuen Informations- und Kommunikationstechnologien zu modernisieren und einzelne unnötige Meldepflichten abzuschaffen.

1. Allerdings sind aus dem vorliegenden Gesetzentwurf Tendenzen zu erkennen, dass durch den Zusammenschluss mehrerer Melderegister übergreifende Dateien entstehen können, die letztlich sogar zu einem zentralen Melderegister führen würden. Eine solche Entwicklung wäre aus datenschutzrechtlicher Sicht nicht hinnehmbar, weil damit das Recht auf informationelle Selbstbestimmung der Bürgerinnen und Bürger unverhältnismäßig eingeschränkt werden würde.

2. Bereits die bisherige Rechtslage, nach der nahezu jedermann eine einfache Melderegisterauskunft von der Meldebehörde erhalten kann, ist äußerst unbefriedigend. Dies wird dadurch verschärft, dass der Gesetzentwurf — wie in

seiner Begründung ausdrücklich betont wird — nunmehr vorsieht, einfache Melderegisterauskünfte mit Hilfe des Internet durch jedermann auch elektronisch abrufen zu können. Um sich gegen eine unkontrollierte Weitergabe solcher über das Internet zum Abruf bereitgehaltener Daten schützen zu können und weil beim Internet-gestützten Abruf die gesetzlich vorgeschriebene Berücksichtigung der schutzwürdigen Belange Betroffener nicht möglich ist, sollte für die Bürgerin oder den Bürger in diesen Fällen ein ausdrückliches Einwilligungsrecht oder mindestens ein Widerspruchsrecht geschaffen werden. Es handelt sich hier um personenbezogene Daten, die auf der Grundlage einer gesetzlichen Auskunftspflicht erhoben wurden.

3. Auch für öffentliche Stellen sollte in das Gesetz eine Bestimmung aufgenommen werden, wonach bei elektronischen Abrufverfahren über das Internet zur Wahrung der schutzwürdigen Interessen der Betroffenen zumindest Verfahren der fortgeschrittenen elektronischen Signatur gemäß den Regelungen des Signaturgesetzes einzusetzen sind.

4. Nach geltendem Recht ist jede Melderegisterauskunft unzulässig, wenn eine Gefahr für Leben, Gesundheit, persönliche Freiheit oder ähnliche schutzwürdige Belange glaubhaft gemacht wird. Diese Regelung hat sich bewährt. Die Datenschutzbeauftragten treten angesichts des in diesen Fällen bestehenden hohen Schutzbedarfs dem Vorhaben entschieden entgegen, diese Regelung durch eine Risikoabwägung im Einzelfall aufzuweichen.

5. Bislang dürfen Meldebehörden an Parteien, Wählergruppen und andere Träger von Wahlvorschlägen Auskunft über Daten von Gruppen von Wahlberechtigten erteilen, sofern die Wahlberechtigten dieser Auskunftserteilung nicht widersprochen haben. Die Datenschutzbeauftragten bekräftigen ihre bereits in der Vergangenheit erhobene Forderung, gesetzlich zu regeln, dass eine Einwilligung der Betroffenen Voraussetzung für solche Datenweitergaben sein muss. Die bisherige Widerspruchslösung ist in weiten Kreisen der Bevölkerung unbekannt.

6. Außerdem fordern die Datenschutzbeauftragten, die Hotelmeldepflicht abzuschaffen, da die hiermit verbundene millionenfache Datenerhebung auf Vorrat unverhältnismäßig ist.

Bei Enthaltung Thüringens zu Ziffer 6.

15.6. Novellierung des G 10-Gesetzes

(Entschließung der 61. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8./9. März 2001)

Die Datenschutzbeauftragten des Bundes und der Länder sehen mit großer Sorge, dass die Empfehlungen des Rechts- und des Innenausschusses des Bundesrates erhebliche Einschränkungen der Persönlichkeitsrechte der Bürgerinnen und Bürger zur Folge hätten, die über den Gesetzentwurf der Bundesregierung teilweise weit hinausgehen. Die Datenschutzbeauftragten wenden sich insbesondere entschieden dagegen, dass

— die Befugnisse der Nachrichtendienste zur Übermittlung und Verwendung von G 10-Daten an Strafverfolgungsbehörden gegenüber dem Gesetzentwurf noch deutlich erweitert werden sollen, indem Erkenntnisse der Nachrichtendienste u. a. zur Strafverfolgung weit über die Schwerkriminalität hinaus genutzt werden dürften,

— der Verzicht auf die Kennzeichnung von G 10-Daten sogar ohne vorherige Zustimmung der G 10-Kommission zulässig sein und

— die Schwelle dafür, endgültig von der Benachrichtigung Betroffener abzusehen, deutlich herabgesetzt werden soll.

Darüber hinaus kritisieren die Datenschutzbeauftragten des Bundes und der Länder, dass die Bundesregierung mit der Gesetzesnovelle über die Vorgaben des BVerfG hinaus weitere Änderungen im G 10-Bereich erreichen will, die neue grundrechtliche Beschränkungen vorsehen:

— Die Anforderungen an die halbjährlichen Berichte des zuständigen Bundesministers an die PKG müssen so gefasst werden, dass eine wirksame parlamentarische Kontrolle erreicht wird. Dies ist derzeit nicht gewährleistet. Deshalb muss über Anlass, Umfang, Dauer, Ergebnis und Kosten aller Maßnahmen nach dem G 10-Gesetz sowie über die Benachrichtigung der Beteiligten berichtet werden. Die gleichen Anforderungen müssen auch für die Berichte der PKG an den Bundestag gelten.

— Die Neuregelung, nach der auch außerhalb der Staatsschutzdelikte mutmaßliche Einzeltäter und lose Gruppierungen den Maßnahmen nach dem G 10-Gesetz unterliegen sollen, stellt das Trennungsgebot nach Art. 87 Abs. 1 Satz 2 GG weiter in Frage. Ermittlungen von der Eingriffsschwelle eines konkreten Anfangsverdachts zu lösen und nach nachrichtendienstlicher Art schon im Vorfeld zur Verdachtsgewinnung durchzuführen, weitet die Gefahr unverhältnismäßig aus, dass auch gegen Unbescholtene strafrechtlich ermittelt wird.

— Alle Neuregelungen wie z. B. zum Parteienverbotsverfahren, zur Verwendung von G 10-Erkenntnissen bei Gefahren für Leib oder Leben einer Person im Ausland und zu Spontanübermittlungen an den BND müssen befristet und einer effizienten Erfolgskontrolle unterzogen worden.

— Bei der internen Datenverarbeitung durch die Nachrichtendienste ist die Zweckbindung so zu formulieren, dass die erhobenen Daten nicht zur Erforschung und Verfolgung anderer als der in § 3 und § 5 G 10-E genannten Straftaten genutzt werden dürfen.

— Die vorgesehenen Ausnahmen von der vom BVerfG geforderten Kennzeichnungspflicht bei der Übermittlung von Daten, die aus G 10-Maßnahmen stammen, begegnen schwerwiegenden datenschutzrechtlichen Bedenken.

— Im Gesetzentwurf fehlt die Regelung, dass eine Weiterübermittlung an andere Stellen und Dritte nicht zulässig ist. Sie darf nur durch die erhebende Stelle erfolgen. Die Weitergabe von G 10-Daten an andere Dienststellen ist bei der übermittelnden Stelle stets zu dokumentieren und zu kennzeichnen.

— Eine dauerhafte Ausnahme von der Benachrichtigungspflicht ist abzulehnen. Sie würde für die Betroffenen zu einem Ausschluss des Rechtsweges führen.

— Dem BND wird nicht mehr nur die „strategische Überwachung" des nichtleitungsgebundenen, sondern künftig des gesamten internationalen Telekommunikationsverkehrs ermöglicht. Dies setzt den Zugriff deutscher Stellen auf Telekommunikationssysteme in fremden Hoheitsbereichen voraus. Dabei muss sichergestellt werden, dass die Anforderungen des Völkerrechts eingehalten werden.

— Die Überwachung internationaler Telekommunikationsbeziehungen im Falle einer Gefahr für Leib oder Leben einer Person im Ausland (§ 8 G 10-E) ermöglicht sehr intensive Grundrechtseingriffe in großer Zahl und mit einer hohen Dichte, die höher sein kann als bei „strategischen Überwachung" nach § 5 G 10-E. Dies setzt eine hohe Eingriffsschwelle und enge zeitliche Befristungen voraus, die der Entwurf nicht hinreichend vorsieht.

15.7. Anlasslose DNA-Analyse aller Männer verfassungswidrig

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 12. März 2001)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder weist entschieden den Vorschlag zurück, den „genetischen Fingerabdruck" aller Männer zu erheben und rein vorsorglich zu speichern. Die Erhebung personenbezogener Daten ist auch im Rahmen der Strafverfolgung an rechtsstaatliche Grundsätze gebunden. Eine Datenerhebung auf Vorrat, die die Hälfte der Bevölkerung als potentielle Straftäter behandelt, ist verfassungsrechtlich unzulässig. Darüber hinaus erscheint der erwartete Abschreckungseffekt äußerst fragwürdig.

15.8. Veröffentlichung von Insolvenzinformationen im Internet

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 24. April 2001)

Dem Bundestag liegt ein Gesetzentwurf der Bundesregierung zur Änderung der Insolvenzordnung (BT-Drs. 14/5680) vor. Danach sollen gerichtliche Entscheidungen — vor allem in Verbraucherinsolvenzverfahren — künftig auch über das Internet veröffentlicht werden können, um Kosten für Bekanntmachungen in Printmedien zu sparen.

Die Datenschutzbeauftragten des Bundes und der Länder weisen darauf hin, dass Informationen aus Insolvenzverfahren, die in das Internet eingestellt sind, durch die Justiz nicht räumlich begrenzt werden können. Darüber hinaus ist deren Speicherung zeitlich nicht beherrschbar, und die Daten können vielfältig ausgewertet werden. Dies kann dazu führen, dass Dritte, etwa Auskunfteien oder Wirtschaftsinformationsdienste, die Daten auch nach Abschluss eines Insolvenzverfahrens speichern und diese über längere Zeit im Internet verfügbar sind. Die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn würde letztlich auf Dauer beeinträchtigt, wenn sie zeitlebens weltweit abrufbar am Schulden-Pranger stehen.

Der Gesetzgeber muss das Risiko für die betroffenen Verbraucherinnen und Verbraucher, aufgrund einer möglichen Auswertung justizieller Veröffentlichungen im Internet dauerhaft Einbußen bei der Teilnahme am Wirtschaftsverkehr zu erleiden, sorgfältig mit dem Interesse an der beabsichtigten Senkung von Bekanntmachungskosten abwägen. Hierbei ist auch die gesetzgeberische Wertung zu berücksichtigen, dass Personen, für die ein Insolvenzverfahren eröffnet wurde, gerade nicht in das Schuldnerverzeichnis beim Amtsgericht aufgenommen werden. Das Internet bietet im Gegensatz zu einem gerichtlichen Verzeichnis letztlich keine Gewähr, die ordnungsgemäße Pflege und Löschung personenbezogener Daten sicherzustellen, die für die Betroffenen von entscheidender wirtschaftlicher Bedeutung sein können. Die Datenschutzbeauftragten appellieren daher an den Gesetzgeber und an die Justizverwaltungen der Länder, die aufgezeigten Risiken insbesondere für Verbraucherinsolvenzen neu zu bewerten. Die vorgenannten Überlegungen sind im Gesetzgebungsverfahren bisher nicht in ausreichendem Maße berücksichtigt worden. Dabei sollten die Erwägungen des Bundesverfassungsgerichtes im Beschluss vom 9. März 1988 (1 BvL 49/86) zu einem vergleichbaren Sachverhalt einbezogen werden.

Es erscheint zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung. Gerade das Internet bietet neue Chancen und Möglichkeiten, Informationen gezielt nur denen zugänglich zu machen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es gilt deshalb, insbesondere zu untersuchen, ob dem Prinzip der Publizität bei Veröffentlichungen im Internet nicht ein anderer Stellenwert zukommt und wie gravierende Nachteile für die Betroffenen vermieden werden können.

Bevor die geplante Änderung des § 9 InsO verabschiedet wird, ist daher vorrangig zu klären, wie das Recht auf informationelle Selbstbestimmung der Betroffenen besser geschützt werden kann.

Auch in anderen Bereichen wird das Internet bereits genutzt, erprobt oder die Nutzung erwogen, um justizielle Informationen bereitzustellen, z. B. die Handels-, Vereins-, Genossenschafts- und Partnerschaftsregister oder in Zwangsvollstreckungsverfahren. Inwieweit das Internet als Medium der im Ergebnis unbegrenzbaren Informationsverarbeitung datenschutzrechtlich angemessen ist und welches Datenprofil in das Internet eingestellt werden darf, muss differenziert in Übereinstimmung mit dem gesetzlich bezweckten Grad der Publizität der jeweiligen Daten entschieden werden. Jede gesetzgeberische Entscheidung für eine Veröffentlichung über das Internet sollte aber im Hinblick auf deren besondere Risiken regeln, dass Veröffentlichungen befristet sind und dass spezielle Vorkehrungen getroffen werden, um die Identität und die Authentizität zu sichern sowie eine automatische Übernahme der Daten zu verhindern (Kopierschutz).

Sollte sich der Gesetzgeber nach sorgfältiger Abwägung für eine Veröffentlichung über das Internet entscheiden, so muss er die Auswirkungen der Regelung auf Grund aussagefähiger Berichte der Landesjustizverwaltungen überprüfen. Gegenstand dieser Überprüfung muss auch sein, ob die eingetretene Kostensenkung tatsächlich — wie von der Bundesregierung erwartet — einer größeren Anzahl von Schuldnerinnen und Schuldnern den Weg zur Restschuldbefreiung eröffnet hat.

15.9. Terrorismusbekämpfung

(Entschließung anlässlich des Sondertreffens zwischen der 61. und der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 1. Oktober 2001)

Die Datenschutzbeauftragten des Bundes und der Länder unterstützen mit Nachdruck den Kampf des demokratischen Rechtsstaats gegen Terrorismus und organisierte Kriminalität. Sie sind heute zu einem Sondertreffen in Bonn zusammengekommen, um die aktuelle Situation nach den Terroranschlägen zu erörtern. Im politischen Raum werden zahlreiche Forderungen und Vorschläge zur Verbesserung der inneren Sicherheit diskutiert, die auch Auswirkungen auf den Datenschutz haben.

Die Datenschutzbeauftragten weisen darauf hin, dass die Sicherheits- und Strafverfolgungsbehörden zur Terrorismusbekämpfung bereits über weitreichende Befugnisse zur Datenverarbeitung verfügen. So ist z. B. die Rasterfahndung zu Strafverfolgungszwecken generell möglich, in den meisten Ländern auch zur Gefahrenabwehr durch die Polizei. Das Bundesamt für die Anerkennung ausländischer Flüchtlinge kann bereits heute Erkenntnisse über terroristische Aktivitäten an den Verfassungsschutz und die Polizei übermitteln. Auch ist eine effektive Zusammenarbeit zwischen Polizei und Verfassungsschutz durch die geltende Rechtslage gewährleistet; Vollzugsdefizite sind kein Datenschutzproblem. Zu pauschalen Forderungen nach Einschränkung des Bürgerrechts auf Datenschutz besteht deshalb kein Anlass. Die Datenschutzbeauftragten betonen, dass Datenschutz nie Täterschutz war und auch in Zukunft nicht sein wird.

Die Datenschutzbeauftragten sind zu einem offenen und konstruktiven Dialog über etwa notwendige Anpassungen an die neue Bedrohungslage bereit. Sie erwarten, dass sie rechtzeitig beteiligt werden. Die Datenschutzbeauftragten warnen vor übereilten Maßnahmen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger einschränken. Sie sprechen sich dafür aus, alle neu beschlossenen Eingriffsbefugnisse zu befristen und tiefgreifende Eingriffsbefugnisse, damit auch die laufende Rasterfahndung, einer ergebnisoffenen Erfolgskontrolle zu unterziehen.

Bei der künftigen Gesetzgebung sind die grundlegenden Rechtsstaatsprinzipien, das Grundrecht der freien Entfaltung der Persönlichkeit, das Verhältnismäßigkeitsprinzip, die Unschuldsvermutung und das Gebot besonderer gesetzlicher Verwendungsregelungen für sensible Daten selbstverständlich zu beachten. Diese verfassungsrechtlichen Garantien prägen den Rechtsstaat, den wir gemeinsam zu verteidigen haben.

15.10. Datenschutzrechtliche Anforderungen an den „Arzneimittelpass“ (Medikamentenchipkarte)

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2001)

Vor dem Hintergrund der Lipobay-Diskussion hat das Bundesministerium für Gesundheit die Einführung eines „Arzneimittelpasses“ in Form einer (elektronisch nutzbaren) Medikamentenchipkarte befürwortet; auf der Karte sollen alle ärztlichen Verordnungen verzeichnet werden. Damit soll eine größere Transparenz der Arzneimittelverordnungen erreicht werden. Bisher ist nicht ansatzweise belegt, dass die bekannt gewordenen Gefahren für die Patientinnen und Patienten dadurch entstanden sind, dass verschiedene Ärztinnen und Ärzte ohne Kenntnis voneinander unverträgliche Medikamente verordnet hätten. Deswegen ist auch nicht ersichtlich, dass die aufgetretenen Probleme mit einem Arzneimittelpass hätten verhindert werden können.

Aus datenschutzrechtlicher Sicht bestehen erhebliche Bedenken gegen eine Medikamentenchipkarte als Pflichtkarte. Die Datenschutzbeauftragten begrüßen es daher ausdrücklich, dass der Gedanke einer Pflichtkarte fallen gelassen wurde. Die Patientinnen und Patienten würden sonst rechtlich oder faktisch gezwungen, die ihnen verordneten Medikamente und damit zumeist auch ihre Erkrankung bei jedem Arzt- und/oder Apothekenbesuch ohne ihren Willen zu offenbaren. Dies würde eine wesentliche Einschränkung des Arztgeheimnisses bewirken, das auch gegenüber anderen Ärztinnen und Ärzten gilt. Zudem würde sich dadurch das Vertrauensverhältnis, das für die Behandlung und für eine funktionierende Gesundheitsfürsorge insgesamt unabdingbar ist, grundlegend verändern. Darüber hinaus wäre das Einholen einer unbeeinflussten Zweitmeinung nahezu ausgeschlossen.

Die freie und unbeeinflusste Entscheidung der Patientinnen und Patienten über Einsatz und Verwendung der Karte muss gewährleistet werden (Grundsatz der Freiwilligkeit).

Die Datenschutzbeauftragten des Bundes und der Länder haben bereits auf ihrer 47. Konferenz im März 1994 und auf ihrer 50. Konferenz im November 1995 zum freiwilligen Einsatz von Chipkarten im Gesundheitswesen Stellung genommen; deren Zulässigkeit wird dort von verschiedenen Bedingungen zur Sicherung des Persönlichkeitsrechts der Patientinnen und Patienten abhängig gemacht. Grundlegende Voraussetzung ist vor allem die freie Entscheidung der Betroffenen (auch als Versicherte). Sie müssen entscheiden können,

— ob ihre Daten auf einer Chipkarte gespeichert werden,

— welche ihrer Gesundheitsdaten auf die Karte aufgenommen werden,

— welche ihrer Daten auf der Karte wieder gelöscht werden,

— ob sie die Karte bei einem Arzt- oder Apothekenbesuch vorlegen und

— welche ihrer Daten sie im Einzelfall zugänglich machen (die Technik muss eine partielle Freigabe ermöglichen).

Die Verantwortung für die Wahrung der Arzneimittelsicherheit tragen grundsätzlich die Ärztinnen und Ärzte sowie die Apothekerinnen und Apotheker. Sie darf nicht auf die Betroffenen abgewälzt werden. Dies gilt auch, wenn sie von dem „Arzneimittelpass“ keinen Gebrauch machen.

Der Chipkarteneinsatz darf nicht zur Entstehung neuer zentraler Datensammlungen über Patientinnen und Patienten führen.

Datenschutzrechtlich problematisch wäre es, den „Arzneimittelpass“ auf der Krankenversichertenkarte gemäß § 291 SGB V zu implementieren. Eine solche Erweiterung wäre allenfalls vertretbar, wenn die „Funktion Krankenversichertenkarte“ von der „Funktion Arzneimittelpass“ informationstechnisch getrennt würde, so dass die Patientinnen oder Patienten bei einem Arzt- oder Apothekenbesuch nicht gezwungen werden, ihre gesamten Gesundheitsdaten ungewollt zu offenbaren. Ihre Entscheidungsfreiheit, wem gegenüber sie welche Gesundheitsdaten offenlegen, müsste also durch die technische Ausgestaltung der Karte gewährleistet sein.

Die Betroffenen müssen ferner das Recht und die Möglichkeit haben, ihre auf der Chipkarte gespeicherten Daten vollständig zu lesen.

Die Verwendung der Karte außerhalb des medizinischen Bereichs, z. B. durch Arbeitgeberinnen und Arbeitgeber oder Versicherungen, muss gesetzlich verboten und sanktioniert werden.

15.11. Zur gesetzlichen Regelung von genetischen Untersuchungen

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2001)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder konkretisiert ihre Forderungen an Bundestag und Bundesrat, genetische Untersuchungen

am Menschen gesetzlich zu regeln. Geboten sind besondere Regelungen für genetische Untersuchungen zu medizinischen Zwecken, zur Klärung von Identität und Abstammung, im Zusammenhang mit Arbeits- und Versicherungsverhältnissen sowie zu Forschungszwecken. Außer dem „genetischen Fingerabdruck“ für Zwecke der Strafverfolgung — in der Strafprozessordnung bereits normiert — sind typische Anwendungsfelder für genetische Untersuchungen zu regeln. Von besonderer Bedeutung sind das Informations- und Entscheidungsrecht der betroffenen Personen. Die Kernanliegen der Datenschutzbeauftragten sind:

— Stärkung des Selbstbestimmungsrechts durch einen grundsätzlichen Einwilligungsvorbehalt für die Durchführung genetischer Untersuchungen;

— Information und Transparenz für die betroffene Person durch Umschreibung des notwendigen Aufklärungsumfangs;

— Qualität und Sicherheit genetischer Tests durch Arzt- und Zulassungsvorbehalte;

— Schutz von Ungeborenen, Minderjährigen und nicht einsichtsfähigen Personen durch abgestufte Beschränkung zugelassener Untersuchungsziele;

— Gewährleistung des Rechts auf Nichtwissen durch differenzierte Entscheidungs- und Offenbarungsoptionen;

— Verhinderung heimlicher Gentests durch das Gebot der Probennahme direkt in ärztlicher Praxis oder Labor;

— Verhinderung von missbräuchlicher Nutzung genetischer Erkenntnisse im Arbeitsleben und im Versicherungsverhältnis durch ein grundsätzliches Verbot, Gentests oder Testergebnisse zu fordern oder entgegen zu nehmen;

— Selbstbestimmung der Betroffenen auch im Forschungsbereich durch einen grundsätzlichen Einwilligungsvorbehalt bei einzelnen Forschungsprojekten und Proben- und Gendatenbanken;

— Sicherung zuverlässiger Pseudonymisierungsverfahren bei Proben- und Gendatenbanken durch externe Datentreuhänderschaft;

— Hilfe für die Betroffenen durch die Pflicht, im Rahmen der Forschung, individuell bedeutsame Untersuchungsergebnisse mitzuteilen;

— Absicherung der Regelungen durch die Einführung von Straftatbeständen.

Neben diesen bereichsspezifischen Bestimmungen zu den verschiedenen Zwecken genetischer Untersuchungen fordert die Konferenz der Datenschutzbeauftragten eine grundlegende Strafnorm im Strafgesetzbuch, um Gentests ohne gesetzliche Ermächtigung oder ohne die grundsätzlich nur für Zwecke der medizinischen Behandlung oder Forschung wirksame Einwilligung der betroffenen Person zu unterbinden.

Die Datenschutzbeauftragten des Bundes und der Länder verstehen ihre Vorschläge als Anregungen zu anstehenden Gesetzesinitiativen und zur gesellschaftspolitischen Diskussion.

15.12. Zur Lkw-Maut auf Autobahnen und zur allgemeinen Maut auf privat errichteten Bundesfernstraßen

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2001)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert die Bundesregierung auf, bei der technischen Realisierung und bei der anstehenden internationalen Normierung elektronischer Mautsysteme datenschutzrechtliche Anforderungen durchzusetzen.

Das Bundeskabinett hat am 15. August 2001 den Gesetzentwurf für die Einführung eines solchen Mautsystems beschlossen. Ab 2003 ist neben der manuellen

Erfassung der Gebühren ein automatisches System geplant, mit dem eine streckenbezogene Autobahnbenutzungsgebühr (Maut) für Lastkraftwagen erhoben werden soll. Das Bundesministerium für Verkehr, Bau- und Wohnungswesen prüft zurzeit Angebote, die im Ergebnis einer europaweiten Ausschreibung eingegangen sind.

Für das automatische System sollen das Satellitennavigationssystem GPS und die Mobilfunktechnologie genutzt werden. Dadurch werden stationäre Erfassungseinrichtungen entbehrlich. Relativ einfach könnte so das mautpflichtige Straßennetz beispielsweise auf den Bereich der Bundesstraßen ausgedehnt werden. Selbst ein grenzüberschreitender Einsatz derartiger Systeme wäre aus technischer Sicht leicht zu realisieren. Entsprechendes Interesse aus dem benachbarten Ausland ist bereits bekundet worden.

Die verfügbare, im Gesetzentwurf nicht festgeschriebene Technik ermöglicht es prinzipiell, den Fahrweg der Mautpflichtigen detailliert zu dokumentieren und zu archivieren und auf diese Weise exakte Bewegungsprofile zu erstellen. Damit würden die Voraussetzungen geschaffen, dass Systembetreiber und andere nachvollziehen können, wer wann wohin gefahren ist. Die Datenschutzbeauftragten des Bundes und der Länder halten es deshalb für unverzichtbar, elektronische Mautsysteme datenschutzgerecht auszugestalten. Insbesondere ist dafür Sorge zu tragen, dass die Erhebung und Speicherung ausschließlich für Abrechnungszwecke verwendet werden.

Weiterhin ist bei Gestaltung und beim Betrieb der erforderlichen Erfassungs- und Kontrollsysteme das im Bundesdatenschutzgesetz normierte Prinzip der Datensparsamkeit sicherzustellen. Das erfordert den Einsatz von Verfahren, bei denen Mautgebühren vorab entrichtet werden können, ohne dass dafür die Erhebung und Speicherung personenbeziehbarer Daten erforderlich ist.

Insbesondere ist sicherzustellen, dass damit keine oder so wenig personenbezogene Daten wie möglich erhoben, verarbeitet oder genutzt werden. Soweit personenbezogene Daten beispielsweise für Abrechnungs- oder Kontrollzwecke gespeichert werden, sind sie zum frühestmöglichen Zeitpunkt, spätestens jedoch nach Entrichtung der Straßenbenutzungsgebühr beziehungsweise nach Abschluss eines Mauterstattungsverfahrens zu löschen, wenn sie nicht mehr für die Abwicklung des Mautverfahrens oder für erforderliche Kontroll- oder Prüfverfahren benötigt werden.

Bereits 1995 haben die Datenschutzbeauftragten des Bundes und der Länder Anforderungen an Systeme zur automatischen Erhebung von Straßennutzungsgebühren formuliert. Insbesondere die folgenden Aspekte sind nach wie vor aktuell:

— Die Überwachung der Gebührenzahlung darf nur stichprobenweise erfolgen. Die Identität der Mautpflichtigen darf nur dann aufgedeckt werden, wenn tatsächliche Anhaltspunkte dafür bestehen, dass die Gebühren nicht entrichtet worden sind.

— Die Verfahren der Gebührenerhebung und -kontrolle müssen für die Mautpflichtigen durchschaubar sein. Sie müssen sich jederzeit über den Abrechnungsvorgang informieren sowie den eventuellen Kontrollvorgang erkennen können.

— Alle datenschutzrelevanten Systemkomponenten sind so auszugestalten, dass sie weder vom Betreiber noch von anderer Seite beeinträchtigt oder zurückgenommen werden können.

— Es ist sicherzustellen, dass anfallende personenbezogenen Daten von allen beteiligten Stellen vertraulich behandelt werden und einer strikten Zweckbindung unterliegen.

Außerdem liegt ein Gesetzentwurf vor, der zur Erhebung von Mautgebühren an Brücken, Tunneln und Gebirgspässen im Zuge von Bundesautobahnen und Bundesstraßen sowie an mehrspurigen Bundesstraßen mit getrennten Fahrbahnen berechtigt, soweit sie von Privaten errichtet sind. Die Mautpflicht gilt für alle Kraftfahrzeuge. Deshalb muss an der im Entwurf vorgesehenen Barzahlungs-

möglichkeit ohne Verarbeitung personenbezogener Daten unbedingt festgehalten werden. Ihre Ausgestaltung sollte kundenfreundlich erfolgen. Diese Zahlungsweise vermeidet die weitergehende Datenerfassung für alle Mautpflichtigen (Kennzeichen und Bilder der Fahrzeuge). In der zu erlassenden Rechtsverordnung muss deshalb insbesondere sichergestellt werden, dass keine Datenerfassung bei Personen erfolgt, die die Gebühr unmittelbar entrichten.

15.13. Zur „neuen Medienordnung"

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2001)

Bund und Länder beraten gegenwärtig über die Grundzüge einer neuen Medienordnung. Zu den dabei zu beachtenden verfassungsrechtlichen Rahmenbedingungen gehören neben den Gesetzgebungskompetenzen von Bund und Ländern auch die Grundrechte auf Schutz der Privatsphäre und der personenbezogenen Daten, Meinungsfreiheit und Vertraulichkeit der Kommunikation. Diese Rechte müssen in einer neuen Medienordnung durchgängig gewährleistet bleiben.

Angesichts der technischen Entwicklung und der Konvergenz der Medien darf der Grad der Vertraulichkeit nicht mehr allein davon abhängig sein, ob ein Kommunikationsvorgang der Telekommunikation, den Tele- oder den Mediendiensten zugeordnet wird. Vielmehr muss für alle Formen der Kommunikation und der Mediennutzung ein angemessen hoher Schutz gewährleistet werden.

Aus diesem Grund fordert die Konferenz, das Fernmeldegeheimnis nach Art. 10 GG zu einem allgemeinen Kommunikations- und Mediennutzungsgeheimnis weiter zu entwickeln und einfachgesetzlich abzusichern.

Die Konferenz tritt in diesem Zusammenhang dafür ein, die einschlägigen Rechtsvorschriften inhaltlich stärker einander anzugleichen, klarer zu strukturieren und für Nutzende und Anbietende verständlicher zu gestalten.

15.14. Biometrische Merkmale in Personalausweisen und Pässen

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26.1 Oktober 2001)

Im Entwurf eines Terrorismusbekämpfungsgesetzes ist vorgesehen, die Möglichkeit zu eröffnen, in deutschen Personalausweisen und Pässen neben dem Lichtbild und der Unterschrift weitere biometrische Informationen wie zum Beispiel Fingerabdrücke, Handgeometrie, Gesichtsgeometrie u. a. aufzunehmen. Auch die Verwendung genetischer Daten wird nicht ausgeschlossen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass diese Maßnahme schon allein wegen des technischen und zeitlichen Aufwandes, der mit der Einführung derartiger Dokumente verbunden wäre, keinen kurzfristigen Beitrag zur Lösung der mit dem internationalen Terrorismus derzeit verbundenen Probleme leisten kann, zumal Ausländerinnen und Ausländer, die sich in Deutschland aufhalten, nicht erfasst werden.

Die Nutzung biometrischer Merkmale in Personalausweisen und Pässen sowie die damit verbundenen Folgeprobleme (zum Beispiel Art und Ort der Speicherung von Referenzdaten; Vermeidung von Überschussinformationen) werfen eine Vielzahl schwieriger Fragen auf, die einer ausführlichen Diskussion bedürfen. Die zuständigen Stellen werden hierzu aufgefordert, die Notwendigkeit und die rechtlichen und technischen Einzelheiten einer Realisierung dieser Maßnahmen darzulegen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist bereit, sich unter diesen Voraussetzungen mit der Frage zu befassen, ob und wie es möglich ist, mit Hilfe geeigneter zusätzlicher Merkmale in Identifikationspapieren deren Missbrauch zu verhindern, ohne dabei die Grundsätze des Datenschutzes zu verletzen.

15.15. Freiheits- und Persönlichkeitsrechte dürfen bei der Terrorismusbekämpfung nicht verloren gehen

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2001)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass zahlreiche Vorschläge in der gegenwärtigen Debatte um notwendige Konsequenzen aus den Terroranschlägen vom 11. September 2001 die erforderliche sachliche und verantwortungsbewusste Abwägung mit den grundgesetzlich geschützten Freiheits- und Persönlichkeitsrechten der Einzelnen vermissen lassen.

Der Entwurf eines Terrorismusbekämpfungsgesetzes und der Antrag der Länder Baden-Württemberg, Bayern und Hessen im Bundesrat zur wirksamen Bekämpfung des internationalen Terrorismus und Extremismus (BR-Drs. 807/01) übertreffen die in der Entschließung der Konferenz vom 1. Oktober 2001 geäußerte Befürchtung, dass übereilt Maßnahmen ergriffen werden sollen, die keinen wirksamen Beitrag zur Terrorismusbekämpfung leisten, aber die Freiheitsrechte der Bürgerinnen und Bürger unangemessen einschränken.

Gegenwärtig wird ohne Rücksicht auf das grundrechtliche Übermaßverbot vorgeschlagen, was technisch möglich erscheint, anstatt zu prüfen, was wirklich geeignet und erforderlich ist. Außerdem müsste der Frage nachgegangen werden, ob es nicht in den Geheimdiensten und in der Strafverfolgung Vollzugsdefizite gibt. Dabei müsste auch untersucht werden, welche Resultate die vielen Gesetzesverschärfungen der letzten Jahre gebracht haben.

Persönlichkeitsrechte haben über ihre grundrechtssichernde Wirkung hinaus — mit den Worten des Bundesverfassungsgerichts — auch Bedeutung als „elementare Funktionsbedingung eines auf Handlungs- und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlich demokratischen Gemeinwesens".

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert daher sehr eindringlich an alle Beteiligten, nicht Persönlichkeitsrechte vorschnell und ohne die gebotene sorgsam abwägende Prüfung über die bereits bestehenden Eingriffsmöglichkeiten hinaus dauerhaft einzuschränken und so den Ausnahmezustand zur Norm zu erheben.

Alle neu erwogenen Maßnahmen müssen sich daran messen lassen, ob sie für eine wirkungsvolle Bekämpfung des Terrorismus wirklich zielführend und erforderlich sind und ob sie den Verfassungsgrundsatz der Verhältnismäßigkeit einhalten. Einseitiges Streben nach einer umfassenden Sicherheit darf nicht den bisherigen gesellschaftlichen Konsens über die wertsetzende Bedeutung bürgerlicher Freiheits- und Persönlichkeitsrechte so überlagern, dass es in unserem Land zu einer langwirkenden Verschiebung zugunsten staatlicher Überwachung und zu Lasten freier und unbeobachteter Aktion, Bewegung und Kommunikation der Bürgerinnen und Bürger kommt.

Wesentliche im BMI-Entwurf eines Terrorismusbekämpfungsgesetzes enthaltene Eingriffsmöglichkeiten führen zwangsläufig dazu, dass eine Vielzahl völlig unbescholtener Einzelpersonen zentral erfasst oder verdeckt in Datenerhebungen einbezogen werden, ohne dass eine konkrete Verdachts- oder Gefahrenlage verlangt wird. Zugleich werden Auskunftspflichten und Ermittlungskompetenzen in einer Weise ausgedehnt, dass Eingrenzungen verloren gehen, die aus rechtsstaatlichen Gründen unverzichtbar sind.

Der Verfassungsschutz soll künftig zur Erfüllung aller seiner Aufgaben von den Banken die Kontenbewegungen, von den Luftverkehrsunternehmen alle Reisedaten und von den Post- und Telekommunikationsunternehmen alle Informationen darüber erhalten können, wer von wem Post erhalten und wann mit wem telefoniert hat. All dies soll ohne Wissen der Betroffenen erfolgen und bis zu 15 Jahren gespeichert werden.

Die geplante Befugnis des BKA, Vorermittlungen ohne Anfangsverdacht im Sinne der StPO zu ergreifen, führt zu Eingriffen in das Persönlichkeitsrecht, die weit über das verfassungsrechtlich Zulässige hinausreichen und das tradierte System der Strafverfolgung sprengen. Dies verschiebt die bisher klaren Grenzen zwi-

schen BKA und Verfassungsschutz sowie zwischen Gefahrenabwehr und Strafverfolgung. Ohne jeden Anfangsverdacht soll das BKA künftig Daten über nicht näher eingegrenzte Personenkreise erheben dürfen. Dies kann im Prinzip jede Bürgerin und jeden Bürger betreffen, ohne dass sie sich auf die Schutzmechanismen der Strafprozessordnung verlassen können.

Auch die Vorschläge der Länder enthalten unvertretbare Einschränkungen von grundgesetzlich geschützten Rechtspositionen. So soll die Gefahrenschwelle für den verdeckten Einsatz technischer Mittel in Wohnungen übermäßig abgesenkt werden. Telekommunikationsunternehmen und Internetprovider sollen gesetzlich verpflichtet werden, Verbindungsdaten (zum Beispiel über den Besuch einer Website oder einer Newsgroup) länger zu speichern, als diese zu Abrechnungszwecken benötigt werden, um sie Sicherheitsbehörden zur Verfügung zu stellen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern, dass neue Eingriffsbefugnisse nicht pauschal ausgerichtet, sondern zielgenau auf konkrete Gefährdungssituationen im terroristischen Bereich zugeschnitten und von vornherein befristet werden. Eine unabhängige Evaluierung nach festgelegten Fristen ist unerlässlich, um Geeignetheit und Erforderlichkeit für die Zukunft sachgerecht beurteilen zu können.

15.16. Grundsätze zur Übermittlung von Telekommunikationsverbindungsdaten

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2001)

Die Bundesregierung hat den Gesetzentwurf für eine Nachfolgeregelung zu § 12 FAG vorgelegt, der eine Reihe datenschutzrechtlich positiver Ansätze enthält. Der Bundesrat hat sich demgegenüber in seiner Stellungnahme für eine Regelung ausgesprochen, die wesentlichen datenschutzrechtlichen Anforderungen nicht gerecht wird. Die Datenschutzbeauftragten des Bundes und der Länder lehnen den Vorschlag des Bundesrates entschieden ab.

Sie halten es für nicht vertretbar, Auskünfte über zurückliegende Aktivmeldungen von Mobiltelefonen auch bei reinem Stand-by-Betrieb zu erteilen und Diensteanbieter zur Aufzeichnung von Telekommunikationsverbindungsdaten eigens für Zwecke der Strafverfolgung zu verpflichten.

Auch die vom Bundesrat vorgeschlagene Regelung des § 18 a BVerfSchG zur Übermittlung von Telekommunikationsverbindungsdaten an die Verfassungsschutzbehörden halten die Datenschutzbeauftragten des Bundes und der Länder für nicht akzeptabel. Sie fordern eine deutliche Klarstellung im Wortlaut des Gesetzes, dass Verbindungsdaten an den Verfassungsschutz nur dann übermittelt werden dürfen, wenn tatsächliche Anhaltspunkte für den Verdacht bestehen, dass jemand eine in § 3 Abs. 1 G 10 genannte Straftat plant, begeht oder begangen hat oder sonst an gewalttätigen Bestrebungen oder sicherheitsgefährdenden Tätigkeiten teilnimmt. Eine Übermittlung der Verbindungsdaten für den gesamten Aufgabenbereich des Verfassungsschutzes ginge dagegen erheblich zu weit.

Ferner halten es die Datenschutzbeauftragten für geboten, hinsichtlich der Kennzeichnung und Zweckbindung der Daten, der Mitteilungen an Betroffene und der parlamentarischen Kontrolle einen dem G 10 möglichst gleichwertigen Standard zu gewährleisten.

Die Bundesregierung und der Deutsche Bundestag werden gebeten, diese datenschutzrechtlichen Mindestanforderungen im weiteren Gesetzgebungsverfahren zu berücksichtigen.

15.17. EUROJUST — Vorläufer einer künftigen europäischen Staatsanwaltschaft?

(Entschließung der 62. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 25./26. Oktober 2001)

Der Europäische Rat hat im Herbst 1999 in Tampere die Einrichtung einer gemeinsamen Stelle EUROJUST zur justiziellen Zusammenarbeit beschlossen. EUROJUST soll zur Bekämpfung der schweren organisierten Kriminalität eine sach-

gerechte Koordinierung der nationalen Staatsanwaltschaften erleichtern und die strafrechtlichen Ermittlungen unterstützen sowie die Erledigung von Rechtshilfeersuchen vereinfachen. Zusätzlich beschloss der Rat im Dezember 2000 die Einrichtung einer vorläufigen Stelle zur justiziellen Zusammenarbeit, PRO-EUROJUST genannt, die am 1. März 2001 ihre Arbeit aufgenommen hat. Diese Stelle soll bis zur Einrichtung von EUROJUST die Zusammenarbeit der Ermittlungsbehörden auf dem Gebiet der Bekämpfung der schweren grenzüberschreitenden Kriminalität verbessern und die Koordinierung von Ermittlungen anregen und verstärken. Ein Beschluss des Rates über die Einrichtung von EUROJUST soll bis Ende des Jahres 2001 verabschiedet werden.

Die Aufgabenstellung von EUROJUST führt möglicherweise dazu, dass eine europäische Großbehörde heranwächst, die Daten nicht nur über verdächtige Personen, sondern auch über Opfer und Zeugen sammeln soll, und damit zwangsläufig tiefgreifende Eingriffe in Bürgerrechte vornehmen würde. In diesem Falle käme als Grundlage für EUROJUST nur eine Konvention in Betracht, da für künftige Grundrechtseingriffe durch EUROJUST eine demokratische Legitimation notwendig wäre.

Mit Blick auf die sensiblen personenbezogenen Daten, die von EUROJUST erhoben, verarbeitet und genutzt werden sollen, und unter Berücksichtigung der eigenen Rechtspersönlichkeit von EUROJUST sind umfassende Datenschutzvorschriften erforderlich. Diese müssen sowohl Regelungen zur Verarbeitung, Speicherung, Nutzung, Berichtigung, Löschung als auch zum Auskunftsanspruch des Betroffenen sowie zu einer Kontrollinstanz von EUROJUST enthalten.

Nach Auffassung der Datenschutzbeauftragten des Bundes und der Länder sind folgende datenschutzrechtliche Anforderungen an EUROJUST zu stellen:

— Informationsaustausch mit Partnern

Der Informationsaustausch mit Partnern sollte EUROJUST dann erlaubt sein, wenn er zur Erfüllung seiner Aufgaben erforderlich ist. Bei Weiterleitung dieser Daten an Drittstaaten und -stellen ist die Zustimmung des Mitgliedstaates einzuholen, von dem diese Daten geliefert wurden. Sind personenbezogene Daten betroffen, so muss grundsätzlich eine Übereinkunft zwischen EUROJUST und der Partnerstelle über den Datenschutzstandard getroffen werden. Nur in absoluten Ausnahmefällen, die einer restriktiven Regelung bedürfen, sollte eine Datenübermittlung auch bei Fehlen einer solchen Vereinbarung zulässig sein.

— Verarbeitung personenbezogener Daten

Der Katalog der personenbezogenen Daten, die automatisiert verarbeitet werden dürfen, ist streng am Maßstab der Erforderlichkeit und an den Aufgaben von EUROJUST zu orientieren. Eine zusätzliche Öffnungsklausel, die letztlich die Speicherung aller Daten zulassen würde, ist abzulehnen. Eine Verarbeitung der Daten von Opfern und Zeugen darf, wenn überhaupt erforderlich, nur unter einschränkenden Bedingungen vorgenommen werden.

— Ermittlungsindex und Dateien

Der Ermittlungsindex sollte so ausgestaltet sein, dass es sich um eine reine Vorgangsverwaltung handelt. Sofern zusätzlich Arbeitsdateien geführt werden, sind sie genau zu bezeichnen.

— Auskunftsrecht

Wenn EUROJUST Daten verarbeitet, die ursprünglich von einem Mitgliedstaat geliefert wurden, handelt es sich im Ergebnis um Daten von EUROJUST. Insofern ist ein eigener Auskunftsanspruch von Betroffenen gegenüber EUROJUST unverzichtbar. Für den Fall, dass im Strafverfolgungsinteresse oder aus sonstigen Gründen des Gemeinwohls von einer Auskunft an den Betroffenen abgesehen werden soll, muss eine Abwägung mit den Interessen des Betroffenen an einer Auskunftserteilung vorangegangen sein.

— Änderung, Berichtigung und Löschung

Es sollte auch eine Regelung zur Sperrung von Daten ausgenommen werden, die dazu führt, dass Daten unter bestimmten Voraussetzungen nicht gelöscht, sondern lediglich gesperrt werden.

— Speicherungsfristen

Sofern Daten nach Ablauf bestimmter sonstiger Fristen zu löschen sind, z. B. nach Ablauf der Verjährungsfrist einzelner Mitgliedstaaten, sollte sich die Speicherungsfrist bei EUROJUST nach der Frist des Mitgliedstaates richten, in dem sie am kürzesten ist, um eine mögliche Umgehung nationaler Löschungsfristen zu vermeiden. Die Prüffristen sollten zwei Jahre betragen und auch für Folgeprüfungen nicht länger sein.

— Datensicherheit

Erforderlich sind konkrete Vorschriften zur Datensicherheit. Um den Text des Beschlusses nicht zu überfrachten, könnte eine Regelung entsprechend Art. 22 der Verordnung EG 45/2001 oder § 9 BDSG vorgesehen werden.

— Gemeinsame Kontrollinstanz

Die Erforderlichkeit einer gemeinsamen Kontrollinstanz für EUROJUST muss außer Frage stehen. Die Unabhängigkeit dieser gemeinsamen Kontrollinstanz ist bereits durch die personelle Zusammensetzung zu gewährleisten. Sowohl für die EUROJUST-Mitglieder als auch das Kollegium müssen die Entscheidungen der gemeinsamen Kontrollinstanz bindender Charakter haben.

— Rechtsschutz

Dem Betroffenen ist ein angemessener Rechtsschutz gegenüber EUROJUST zu gewähren. Es sollte festgelegt werden, welche nationale oder supranationale Gerichtsbarkeit für Klagen auf Auskunft, Löschung, Berichtigung und Schadensersatz zuständig ist.

— Rechtsetzungsbedarf

Zur Erfüllung seiner Aufgaben muss EUROJUST Auskünfte über strafrechtliche Ermittlungsverfahren einholen. Nach geltendem Recht (§ 474 StPO) können die Ermittlungsbehörden der Bundesrepublik Deutschland derartigen Ersuchen nicht stattgeben.

Darüber hinaus bedarf der Zugriff des deutschen EUROJUST-Mitglieds auf das Bundeszentralregister und auf das Zentrale Staatsanwaltschaftliche Verfahrensregister einer eindeutigen gesetzlichen Grundlage.

16. EU-Kommission zur Unabhängigkeit der Datenschutzkontrollstellen

Die EU-Kommission — Generalinspektion Binnenmarkt — hat auf eine Anfrage zur Unabhängigkeit der Datenschutzkontrollstellen mit Schreiben vom 11.09.2001 unter anderem folgendes geantwortetet:

„Die ... aufgeworfene Frage der völligen Unabhängigkeit der Kontrollstellen im Bereich des Datenschutzes, wie von Artikel 28 der Datenschutzrichtlinie 95/46/EG gefordert, ist in der Tat von zentraler Bedeutung für eine effiziente Anwendung des nationalen Datenschutzrechts zum Wohle aller Bürger.

.....

Die Richtlinie selbst verlangt, dass die Kontrollstellen ihre Aufgaben „in völliger Unabhängigkeit“ wahrnehmen. In den gegenwärtigen Erweiterungsverhandlungen drängt die Kommission die Beitrittskandidaten beispielsweise, bei der Umsetzung des „acquis communautaire“ darauf zu achten, dass diese Kontrollstellen als solche keinerlei Weisungen unterworfen sind, dass ihre Entscheidung nicht durch politische Instanzen beeinflusst oder abgeändert werden können und dass die Bestellung ihres Leiters nicht ausschließlich durch die Exekutive erfolgt. Überlegungen, die bereits auf internationaler Ebene diskutiert werden, könnten ebenfalls für die Diskussion in Deutschland hilfreich sein. Der Entwurf des Zusatzprotokolls zur Konvention 108 des Europarates verlangt in wörtlicher Übereinstimmung mit der Richtlinie „völlige Unabhängigkeit“ der Kontrollstellen und der erläuternde Bericht zum Zusatzprotokoll nennt als Elemente, die diese Unabhängigkeit ausmachen können, folgende Umstände:

— Zusammensetzung der Kontrollstelle

— Art und Weise der Ernennung ihrer Mitglieder

— Bedingungen zur Beendigung des Amtes

— Zuweisung ausreichender Mittel an die Kontrollstelle

— Keine Anweisungen oder Einmischungen von außen bei der Beschlussfassung.“

17. Anhang

17.1. Auswahl von Berichten in Tageszeitungen/Zeitschriften im Land Bremen im Jahr 2001

Datum	Zeitung	Titel/Inhalt
16.01.	taz Bremen	**Viel Aufwand — wenig Erfolg?** Die Telefonüberwachung durch die Polizei .....
17.02.	Bremer Nachrichten	**Rabattmarken unter die Lupe nehmen** Bremer Datenschützer will „Payback“ prüfen lassen
20.02.	Weser Kurier	**„Zu neuer Technologie gehört Datenschutz“** Einführung neuer Technologien in die Verwaltung
20.02.	taz bremen	**Private Datenschützer kommen** Datenschutzbehörde will private Aufträge haben
22.02.	Weser Kurier	**Sven Holst soll fortan in Bremen die Daten schützen** Landtag wählte einstimmig den neuen Landesbeauftragten
06.03.	Bremer Nachrichten	**Bremen setzt auf Einnahmen aus einer Datenschutz GmbH** Wirtschaft soll demnächst für Beratungen zur Kasse gebeten werden ...
08.03.	Weser Kurier	**„Nackte Frau“ macht Unternehmen zu schaffen** Neues E-Mail-Virus zerstört Dateien und Teile des Windows-Betriebssystems
18.03.	Weser Report	**Gastkommentar: Kein Volk von Verdächtigen** Von Henning Scherf
21.03.	Weser Report	**Unser Wissen ist grenzenlos** Creditreform erteilt Auskünfte aller Art/Datenschutzgesetz wird bald geändert
22.03.	Nordsee Zeitung	**Spannend ist es geblieben** Sven Holst ist zum neuen LfD ernannt worden
22.03.	taz bremen	**Die Steuerlücke im Netz** Panne in der Finanzverwaltung: Abgabe der Steuererklärung über „Elster“
22.03.	Weser Kurier	**Datenschutz mit Homepage** Der LfD Sven Holst ist jetzt auch im Internet erreichbar
22.03.	Weser Kurier	**Chip zieht auch in Bremer Karte ein** Ab 2002 Automaten in allen Straßenbahnen und Bussen
30.03.	Weser Kurier	**Observierung von Kleingärten unterbrochen** Fragebogen-Überwachung mit Folgen: Datenrechtliche Probleme sollen noch mal geprüft werden
31.03.	Weser Kurier	**Kein Sorglospaket vom Datenschutz** Landesbeauftragter legt Bericht vor
31.03.	Nordsee Zeitung	**Kritik an Patienten-Datei** Vorlage des Jahresberichts
02.04.	BILD Zeitung	**Klinik-Skandal** Patienten-Daten im Lager-Computer

03.04.	BILD Zeitung	**Neuer Baby-Test bringt Gewissheit** Münchener Labor bietet Vaterschaftstests an
03.04.	Nordsee Zeitung	**Datenschutz-Mängel auf „bremerhaven.de“** LfD kritisiert auch Videokamera in VGB-Bussen
05.04.	taz bremen	**Besser geht‘s immer** Datenschützer Holst legt Bericht vor
18.04.	Weser Kurier	**Zusätzliches Auge für mehr Sicherheit im Taxi** Modellversuch mit digitalen Kameras ...
26.04.	Die Welt/Bremen	**Datenschutz wird immer wieder neu erfinden** Neuer Amtsleiter Sven Holst wurde offiziell eingeführt
26.04.	Nordsee Zeitung	**Holst in Amt eingeführt** Neuer Landesbeauftragter für den Datenschutz
28.04.	Bremer Anzeiger	**Auf dem Weg ins virtuelle Rathaus** Experten diskutieren in Bremen über die Chancen der digitalen Signatur
07.05.	Die Welt/Bremen	**Mamma-Screening wartet noch** Die zwei Jahre dauernden Untersuchungen starten in den nächsten Wochen
09.05.	Weser Kurier	**Grundbuch auf EDV umgestellt** Notare haben vom Büro aus Zugriff
10.05.	Die Welt/Bremen	**Der Gang zu den Archiven des Amtsgerichts gehört der Vergangenheit an** Henning Scherf führt in Bremen das elektronische Grundbuch ein
24.05.	Weser Kurier	**Streit um heimliche Vaterschaftstests** Datenschützer sieht Persönlichkeitsrechte verletzt
30.05.	Weser Kurier	**Angst vor Missbrauch von Daten eine Hürde** Verbraucher kaufen erst zögernd über das Internet
12.06.	Nordsee Zeitung	**Senat streicht das Kompetenzzentrum** TTZ-Institut auf Eis gelegt ...
13.06.	Nordsee Zeitung	**Empörung über den Senat** Landesregierung legt Bremerhavener Projekte auf Eis
15.06.	Nordsee Zeitung	**Abgeordnete korrigieren Senat** Seestadt-Projekte sollen entgegen dem Beschluss der Landesregierung umgesetzt werden
21.06.	taz bremen	**Internet aus der Steckdose?** Bremer Stromversorger hält sich zurück ...
05.07.	Weser Kurier	**Akteneinsicht statt Geheimniskrämerei** Grüner Gesetzesentwurf — Ziel: Transparente Verwaltung
29.08.	Bremer Anzeiger	**Hacker knackten Bremer Server** „bremen.online“ erstmals offline
22.09.	Weser Kurier	**Von Herz, Schmerz und Kettenbriefen** Aktionen für angeblich todkranke Kinder .....
21.09.	Kreiszeitung Syke	**Trotz Terrors: Kein Überwachungsstaat** Bremens Datenschützer Sven Holst warnt vor vorschnellen Einschränkungen der Freiheit
26.09.	taz bremen	**Virtuelles Rathaus ohne Briefgeheimnis** Einweihung des neuen Info-Zentrums im Foyer der Bremer Bürgerschaft

15.10.	taz bremen	**Krankendaten:** Aufbewahren!/Gewerkschafter fordern Regelung für Konkursfall
17.10.	taz bremen	**Raster ohne Richter** Koalition will Rasterfahndung ohne Richterbeschluss einführen
18.10.	Weser Kurier	**Datenschützer für Richtervorbehalt** ... Rasterfahndung im Bremischen Polizeigesetz
18.10.	taz bremen	**Polizeigesetz — Watschen aus BHV** DSB Sven Holst rügt die Bremer Rasterfahndung
24.10.	Weser Report	**Ausweis mit Fingerabdruck?** Pro & Contra (Sigmar Gabriel/Sven Holst)
25.10.	taz bremen	**Regelung mit „Gerümpel“** Böse sieht im Meldegesetz nur „Zwischenschritt“
25.10.	taz bremen	**Nicht ohne Verdacht** E. Kempf vom Deutschen Anwaltverein begründet Kritik der etablierten Justizverbände an Schilys Plänen
25.10.	Weser Kurier	**Bürgerschaft kurz & bündig** INPOL — neu — Fahndungsprobleme
25.10.	Weser Kurier	**Freie Akteneinsicht umstritten** Grüne und SPD wollen „Gläserne Verwaltung“
26.10.	Weser Kurier	**Bürgerschaft hebt Rasterfahndung ins Polizeigesetz**
26.10.	taz bremen	**Jetzt darf Bremen rastern** „Schläfer“-Fahndung und Wegweisung ist Gesetz
27./ 28.10.	taz bremen	**Warnung vor Otto-Katalog** Datenschützer Sven Holst schlägt Alarm
30.10.	Weser Kurier	**Im Menschen zu lesen, bringt keine innere Sicherheit** Zum Sicherheitspaket II — Biometrische Merkmale
02.11.	BREMER	**The days after** Bremen nach dem 11. September, was sagt der LfD dazu
02.11.	Weser Kurier	**Scouts auf der Datenautobahn** Projekt „Web.Punkte“ bietet Internetservice für Schule und Stadtteil
02.11.	Weser Kurier	**Das Netzwerk kannten wir schon vorher** Ehemaliger Geheimdienstkoordinator Schmidbauer beklagt Versäumnisse im Kampf gegen den Terrorismus
05.11.	Die Welt/Bremen	**Neues Zentrum für Datenschutz** Gütesiegel für Internet-Anbieter geplant
28.11.	Delmenhorster Kreisblatt	**Die Daten sollen laufen, nicht die Bürger** Fachtagung zum Thema „e-Government“ im Bremer Rathaus
31.12.	Die Welt/Bremen	**Neuer Zugriff auf Meldedaten für die Steuerfahndung**

17.2. Liste des verfügbaren Informationsmaterials

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

Folgende Informationsmaterialien können beim

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

angefordert werden:

18. Jahresbericht 1995, Bürgerschafts-Drs. 14/272	(Restexemplare)
19. Jahresbericht 1996, Bürgerschafts-Drs. 14/627	(Restexemplare)
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)

Broschüre „Mobilfunk und Datenschutz“

Broschüre „Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet“

Broschüre „Datenschutz in der Freien Hansestadt Bremen“ (Gesetzestexte und Informationen)

Broschüre „Datenschutz bei WindowsNT“

Broschüre „Datenschutzfreundliche Technologien“

Broschüre „Datenschutz bei der Nutzung von Internet und Intranet“

Broschüre „Vom Bürgerbüro zum Internet“

Faltblatt „Der betriebliche Datenschutzbeauftragte“

Faltblatt „Handels- und Wirtschaftsauskunfteien“

BfD-Info 1 - Bundesdatenschutzgesetz — Text und Erläuterungen
(voraussichtlich Ende April 2002 verfügbar)

BfD-Info 2 - Der Bürger und seine Daten

BfD-Info 3 - Schutz der Sozialdaten

BfD-Info 4 - Der behördliche Datenschutzbeauftragte

BfD-Info 5 - Datenschutz und Telekommunikation

17.3. Index

Druck: Anker-Druck Bremen