23. Jahresbericht

des Landesbeauftragten für den Datenschutz

Hiermit erstatte ich der Bürgerschaft (Landtag) und dem Präsidenten des Senats über das Ergebnis der Tätigkeit im Jahre 2000 den 23. Jahresbericht zum 31. März 2001 (§ 33 Abs. 1 Bremisches Datenschutzgesetz - BrDSG). Redaktionsschluss für die Beiträge war der 31. Januar 2001. Ich war bemüht, alle bis dahin eingehenden Äußerungen zu berücksichtigen.

Sven Holst

(Landesbeauftragter für den Datenschutz)

Inhaltsverzeichnis

1. Vorwort

Der Jahresbericht enthält nur einen Teil des gesamten Spektrums der Tätigkeiten der Dienststelle. Viele Projekte aus den vergangenen Berichten werden noch betreut, ohne dass sie Erwähnung finden, andere sind noch nicht so weit gediehen, eine Darstellung würde noch zu rudimentär wirken. Die im Bericht aufgegriffenen Themen sind nicht nur Schwerpunktbereiche, sondern zum Teil sollen sie die Facetten und Bandbreite der Arbeit wiedergegeben. Der der Bürgerschaft und dem Senat vorzulegende Bericht enthält zugleich auch immer Elemente der Darstellung für die Bürger. Sie fordern regelmäßig nach Erscheinen den Bericht bei mir an. Die Leser sind angesichts des Berichtsumfangs wie in den vergangenen Jahren gehalten, sich das herauszusuchen, was sie interessiert und sollten die Artikel lesen, deren Themen in ihren Lebensbereichen zum Tragen kommen.

Als Trost für die berufstätigen Leser sei angemerkt, dass die eingereichten Beiträge um rund ein Drittel gekürzt oder gestrichen wurden. Gleichwohl wünschte ich mir an der einen oder anderen Stelle eine noch konzentriertere Darstellung. Zur Verbesserung beabsichtige ich in Abstimmung mit Bürgerschaft und Senat im Rahmen der gesetzlichen Bestimmungen ein neues Modell zu entwickeln.

Das vergangene Jahr ist noch von einem schwerpunktmäßigen Einsatz der Kapazitäten im öffentlichen Sektor geprägt. Diese Gewichte werden sich mit der Novellierung des BDSG in Richtung Privatwirtschaft verschieben. Der Bericht läßt erkennen, dass neben den Beratungen zur Gestaltung technischer Systeme auch eine verstärkte Prüftätigkeit im technischen Bereich z. T. durch Online-Prüfungen zu verzeichnen ist. Alle, auch die nichttechnischen Prüfungen machen deutlich, dass in nicht unerheblichem Umfang noch Maßnahmen zur Verbesserung des Datenschutzes zu ergreifen sind. Im Wesentlichen kann positiv festgestellt werden, dass im Gegensatz zu früheren Zeiten die Energien der geprüften Stellen nicht mehr darauf verwandt werden den Datenschutz möglichst fernzuhalten, sondern darauf gerichtet sind den Empfehlungen zur Verbesserung des Datenschutzes Rechnung zutragen.

1.1. I love you-Virus

Im Frühjahr 2000 verbreitete sich binnen kürzester Zeit – von den Philippinen kommend nach Europa und schließlich weltweit - das "I love you-Virus“ und blockierte die Netze und Rechner. Ein immenser wirtschaftlicher Schaden wurde verursacht. Auch die Bremer Verwaltung war in erheblichem Maße betroffen. Noch Tage, nachdem der Angriff erkannt und bekannt war, tauchte das als Anhang an eine E-Mail versandte Virus immer wieder neu in bereits "gereinigten" Verwaltungsnetzen auf. Einzelne Mail-Server wurden mehrere Wochen vom Netz genommen.

Der Vorfall macht deutlich, wie verletzlich die Informationsgesellschaft ist. Die Reaktion der Politik nach dem Vorfall mit erhöhtem Strafrechtsschutz (vgl. BR-Drs. 275/00) dürfte

eher von fragwürdigem Erfolg sein. Besser wäre es, den Datenschutz zu erhöhen. Nur mit hohen Sicherheitsstandarts kann ein ausreichendes Schutzniveau erreicht werden. Datenschutz ist auch Datensicherheit, ist der Schutz vor nicht erlaubten Einwirkungen. Wenn nicht rechtzeitig in Datenschutz und -sicherheit investiert wird, können die Versäumnisse in Folge weit mehr Kosten verursachen oder gar den wirtschaftlichen Ruin bedeuten.

1.2. Neue Trends und die Bedrohungen des informationellen Selbstbestimmungsrechts

Die Entwicklung auf dem Gebiet der Medien und der IuK-Technik (Informations- und Kommunikationstechnik) ist rasant. Dies machen einige Zahlen deutlich, die ich diesem Bericht beifüge (vgl. Ziff. 16.8.). Unterstützt wird dieser weltweite Prozess auch durch verschiedene Initiativen der EU (vgl. Ziff. 16.8.). Es mag sich der Leser fragen, was hat diese Entwicklung mit dem Land Bremen zu tun. Nun, ich betrachte es als meine Aufgabe, die in Bremen lebenden Bürgerinnen und Bürger in ihrem Bestreben zu unterstützen, ihr informationelles Selbstbestimmungsrecht zu wahren und zu schützen. Daher muss der Landesbeauftragte für den Datenschutz für die "global villages“ Bremen und Bremerhaven den Blick über die Landesgrenzen hinaus und in die Zukunft richten, um diesem Anspruch gerecht werden zu können. Einige Schlaglichter des Jahres 2000 seien an dieser Stelle eingefangen, einige bevorstehende Entwicklungen angesprochen.

Computerprotagonisten sehen bereits jetzt, dass mit der Vernetzung von Computern durch das Internet nur ein erster Schritt getan ist. So sagte Bill Gates, “99 Prozent der großen Internet-Applikationen müssen noch geschrieben werden“. Sie sollen PC, größere Server und mobile Endgeräte miteinander umfassend verbinden. Einige sehen im XML-Standart, eine Universalsprache für Datenaustausch, den Schlüssel zur universellen Vernetzung unterschiedlichster Quellen mit PC, Fernseher, Mobiltelefon und Taschencomputer.

Gewaltigen Datenmengen, die durchs Internet transportiert werden, stellen alles bisher Dagewesene in den Schatten. Was hier mittlerweile von E-Commerce-Unternehmen bewältigt werden muss, sei einmal anhand eines der größten Online-Buchhändler dargestellt: Die Web-Site wurde im letzten Jahr monatlich von 15 Millionen Surfern besucht. Von diesen Besuchern werden Nutzerprofile angelegt, um ihren Weg durch die Site und ihr Kaufverhalten zu verfolgen und zu speichern, damit ihnen beim nächsten Besuch gleich auf der ersten Seite maßgeschneiderte Angebote präsentiert werden können. Zu diesen enormen Datenmengen kommen noch die herkömmlichen Transaktionsdaten wie Bestellungen, Stornierungen, Reklamationen und Passwortänderungen hinzu. Welche Dimensionen das Datenvolumen insgesamt bei allen E-Commerce- Unternehmen in den nächsten Jahren annehmen wird, ist kaum vorstellbar, gehen doch konservative Schätzungen davon aus, dass in diesem Jahrzehnt jährlich 50 Millionen neue Internetnutzer hinzukommen werden. Zugleich muss gesehen werden, dass spätestens im

Moment einer Bestellung die gespeicherten Verbraucherprofile personenbezogen zugeordnet werden können. Diese Informationen selbst lassen sich weiter vermarkten. So ist bekannt, dass Kreditkartenunternehmen in den USA die äußerst informativen Datenspuren ihrer Kunden verkaufen. Berichten zufolge soll es branchenüblich sein, dass große Unternehmen sich über Bewerber für einen höheren Posten bereits im Vorfeld aussagekräftige Persönlichkeitsprofile von namhaften Kreditkartenunternehmen besorgen. Gebranntmarkt quasi mit einem geheimen Stempel tritt ein solcher Bewerber seinen Weg an. Nicht viel anders ergeht es dem Verbraucher, wenn er bei einem Versandhaus bestellt oder um einen Kredit nachsucht; die wenig durchschaubaren "Scorewerte“ begleiten ihn (vgl. auch Ziff. 16.4. des Berichts).

Auch das WAP (Wireless Application Protokoll) verdient ein Augenmerk des Datenschutzes. Allerdings ist im Moment noch keine Euphorie auszumachen. WAP ist zur Enttäuschung vieler nicht das angekündigte mobile farbenfrohe Internet, sondern die Datendienste fürs Handy wurden schon mit dem Videotext im Fernsehenkanal verglichen. Bisher sollen in Deutschland rund 2000 Seiten abrufbar sein, wovon zahlreiche Seiten bisher nur aus der Überschrift bestehen. Auch der Zugang ist sehr mühsam und von Provider zu Provider verschieden; komplizierte Eingaben bei E-Commerce-Anwendungen werden ebenso beklagt wie hohe Gebühren. Auf eine systematische Prüfung habe ich daher verzichtet. Die diesjährige Cebit wird allerdings voraussichtlich einen neuen Anlauf nehmen und neue WAP-Dienste anbieten, die mit der Ortsbestimmung des Nutzers (z. T. Meter genau) verbunden ist. Hier ist aus Sicht des Datenschutzes sicherzustellen, dass der Handy-Nutzer selbst entscheiden kann, ob und wann das Handy seinen Standort an Provider und Dienstanbieter übermittelt. WAP kommt allerdings auch geschäftlich zum Einsatz. So werden Unternehmensdaten außerhalb der sicheren Unternehmensumgebung erstellt. Mitarbeiter übertragen von ausgelagerten Arbeitsplätzen z. B. Kundendaten von Laptops via Handy an die Firmenrechner. Hier empfiehlt es sich, eine WAP-fähige Anti-Virensoftware für WAP-Gateways einzusetzen.

Eine weitere schnurlose Technik bahnt sich unter dem Namen "Bluetooth“ an, eine Entwicklung des sog. "Mobile-Computing", die es ermöglicht, mittels Radiowellen mit kurzer Reichweite verschiedene Endgeräte mit drahtloser Übertragungstechnik zu verbinden. Angriffspunkt ist hier die eventuelle Abhörmöglichkeit. Ähnliche Technik wird z. Zt. laut Zeitungsberichten an der Uni Bremen durch das Technologiezentrum Informatik (TZI) getestet. In zwei bis drei Jahren sollen Funkstrecken den gesamten Campus miteinander verbinden. Mit 10 Megabit können die Daten übertragen werden, eine Verbindungsqualität, die selbst für Videokonferenzen ausreicht.

Ein weiterer neuer Berufszweig hat sich entwickelt, der sog. "Infobroker". Hierbei handelt es sich um Rechercheprofis, die im Auftrag Dritter in Archiven und Datenbanken Jagd auf Daten im Web machen. Die Aufgabe scheint dabei eher einem Spitzel zu gleichen, der heimlich in die Privatheit eindringt. Dass es dabei häufig um personenbezogene Daten

geht, liegt auf der Hand. Auch hier zeigt sich, dass das Datenschutzprinzip der Datenvermeidung die beste Antwort ist.

Eine zur Einschränkung für Kinder entwickelte nicht abschaltbare Internet-Software auf dem Familien-PC entwickelte sich zum Boomerang, erlaubte sie doch nicht nur das Verhalten der Kinder im Internet, sondern auch das Verhalten der Eltern zu überwachen.

Eine absolute Sicherheit gibt es nicht, das machte im letzten Jahr ein Hackereinbruch deutlich. Trotz aller Sicherheits- und Verschlüsselungstechniken, die seit Jahren mit großem Aufwand eingesetzt werden, gelang es ins Rechenzentrum von Microsoft einzubrechen und geheimgehaltene Quellcodes auszuspionieren. Der Einbrecher schickte einen sog. "Wurm" oder "Trojaner" in die Firma. Das Programm baut eine Verbindung des infizierten Rechners ins Internet auf und ermöglicht so den Export von Daten. Auch wenn in diesem Falle nur technische Daten ausgelesen wurden, wird doch deutlich, dass Unternehmen mit personenbezogen Daten ebenso getroffen werden können.

Im März 2000 startete ein Fernsehsender unter dem Titel "Big Brother“ ein Medienspektakel, bei dem 10 Männer und Frauen in eine gemeinsame Wohnung eingesperrt dem Voyeurismus vieler Fernseh- und Internetnutzer preisgegeben wurden. Mit der unverantwortlichen Inszenierung wurden die Schamgrenzen beim Eindringen in den sensiblen Bereich der Wohnung bagatellisiert. Mit der Sendung wird ein gesellschaftliches Bewusstsein gefördert, wonach die Persönlichkeitssphäre nur noch wenig wert ist. Indirekt wird zugleich suggeriert, das durch Art. 13 GG geschützte Grundrecht auf Unverletzlichkeit der Wohnung sei überholt. Mit der Sendung wurde zugleich Anschauungsunterricht nachgeliefert, warum Datenschutzbeauftragte gegen den "Großen Lauschangriff" erbitterten Widerstand geleistet haben und weshalb sie sich der Zulassung von polizeilichen Videokameras in Privatwohnungen widersetzt haben. Zum Glück machen neuere Meinungsumfragen deutlich, dass der überwiegende Teil der Bevölkerung im Persönlichkeitsschutz ein sehr hohes Gut sieht.

Das Thema "Videoüberwachung" nahm auch in 2000 wieder breiten Raum ein (vgl. Ziff. 6.1.3., 15.1.3., 15.1.5. und 17.1. dieses Berichts) und wird noch an Brisanz zunehmen. Mit der Videoüberwachung (Video- und Webcams) sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Kamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung der Bilder sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die Bearbeitungs- und Verwendungsmöglichkeiten abschätzen. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und demokratischen Gemeinwesen insgesamt. Alle Menschen haben grundsätz-

lich das Recht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras beobachtet, aufgezeichnet oder ins Internet übertragen wird.

Zusammenfassend lässt sich feststellen: Der Einsatz automatisierter Datenverarbeitung birgt weiterhin ein erhebliches Gefahrenpotential für die Privatsphäre der Bürgerinnen und Bürger. Mehr denn je haben sich Datennetze und Computer in allen Bereichen des Lebens ausgebreitet. Die Entwicklung geht dabei so dramatisch schnell voran, dass wir kaum noch wirklich beurteilen können, wie abhängig unsere Gesellschaft mittlerweile von der IuK-Technik ist. Dabei ist die Entwicklung so vielfältig und vielschichtig, dass wir immer häufiger an die Grenzen der Beeinflussbarkeit der verschiedenen Entwicklungen stoßen. Darüber hinaus sind die Grenzen so fließend, dass zum Teil schon nicht mehr genau zwischen realer und virtueller Welt unterschieden werden kann. Längst sind bei der Datenverarbeitung auch die Grenzen zwischen öffentlicher Verwaltung und Privatwirtschaft verwischt. Weder sind die Daten im privaten Bereich weniger sensibel als im staatlichen Bereich, noch sind die in der Wirtschaft eingesetzen DV-Anlagen moderner, als die der Verwaltung. Häufig bedienen sich beide Bereiche der gleichen Hard- und Software und der gleichen Instrumente und Methoden. Der Zwang zur Kostenenreduzierung und Modernisierung hat gleichzeitig zum massiven Einsatz der automatisierten Datenverarbeitung in der Verwaltung beigetragen.

Die Coputertechnologie ist in alle Lebensbereiche eingedrungen. Beim Einkaufen, Bezahlen, Reservieren mittels Chip- und Magnetstreifenkarten, in digitalen Netzen, durch Teilnahme an Online-Diensten, national und international, überall fällt eine Fülle personenbezogener Daten an. Diese elektronischen Spuren sind geeignet, Persönlichkeitsprofile über den Einzelnen zu bilden. Die moderne IuK-Technik ermöglicht es, Daten in weltweit verteilten Rechnersystemen zu verarbeiten. Weltumspannende Datennetze schaffen die Voraussetzungen, um verschiedene Datensammlungen zusammenzuführen, nach unterschiedlichsten Gesichtspunkten zu durchsuchen und das Verhalten einzelner zu analysieren.

Auch wenn de eine oder andere Neuentwicklung auf dem Computermarkt neue Chancen für den Schutz der Privatheit bieten, so bleibt doch unter dem Strich richtig, dass mit der beschriebenen Entwicklung auch die Risiken für das informationelle Selbstbestimmungsrecht beständig gewachsen sind. Der Datenschutz bleibt daher die notwendige Antwort auf die Risiken der Computertechnik für das EU- und verfassungsrechtlich garantierte Recht auf informationelle Selbstbestimmung.

1.3. Vorbereiteter Internet-Auftritt

Die Arbeiten zur Erstellung einer eigenen Homepage sind weitestgehend abgeschlossen. Die Seite wird künfttig unter www.bremen.datenschutz.de sowie www.datenschutz.bremen.de abrufbar sein. Das Layout orientiert sich an der Seite bremen.de. Das Angebot wird technisch gesehen aus einem Frame bestehen, auf dem sämtliche Steuerungsfunktionen untergebracht sind und es wird XML-fähig sein, ein For-

mat, das die Volltextsuche erleichtert. Das Angebot wird in einigen Bereichen aus dynamisch erzeugten Webseiten bestehen, die tagesaktuell gepflegt werden können und z. B. besonders für Presseerklärungen geeignet sind. Die inhaltliche Struktur der Hompage wird u. a. die Bereiche "Tipps für Bürger“, "Infomationen - Jahresberichte“, "Recht“, "Technik“, "Datenschutzausschuss der Bremischen Bürgerschaft“ und "Aktuelles" enthalten. Für die Bürger werden u. a. Formulare zum Download und Ausdruck bereitstellt. Die Seite ist mit den Angeboten anderer Datenschutzbeauftragte, insbesondere dem "Virtuellen Datenschutzbüro“ verlinkt.

Ich habe dem Datenschutzausschuss das Projekt im Oktober 2000 vorgestellt; er ist mit dem Konzept und Präsentation einverstanden.

1.4. Serviceorientierte Verwaltung

Verwaltungsreform, Bürgerämter, Bürgerbüros, Bürgerkommune, Service-Center und Call-Center sowie Internet-basierte Verwaltungsdienstleistungen sind die neuen Stichworte, unter die sich die Umgestaltung der Verwaltung zusammenfassen lässt. Eine Arbeitsgruppe der Datenschutzbeauftragten der Länder - an der ich mich beteiligt habe - hat für diesen Bereich ihre Vorschläge für einen sicheren Datenschutz zusammengetragen und in einer Broschüre veröffentlicht, die in meiner Dienststelle angefordert werden kann. Der Inhalt der Broschüre ist auch im Internet abrufbar. Folgende Themen werden dort behandelt:

- Multifunktionaler Service (Bürgeramt, Bürgerbüro, Bürgerladen und Kundencenter)
- Call-Center
- Informationsangebote öffentlicher Stellen im Internet
- Interaktive Verwaltung
- Bürgerkarte
- Elektronische Auskunft, Akteneinsicht und Bürgerbeteiligung
- Auslagerung von Verwaltungsfunktionen.

1.5. Zur Situation der Dienststelle

Der amtierende Landesbeauftragte für den Datenschutz hatte sich am 31.12.1999 aus seinem Amt verabschiedet, die Wiederbesetzung der Stelle konnte im Berichtszeitraums nicht abgeschlossen werden. Mit der Entscheidung des Senats vom 06. Februar 2001 zeichnet sich in dieser Frage ein Ende ab. (Nach Redaktionsschluss wurde ich am 21. Februar 2001 von der Bremischen Bürgerschaft gewählt.) Bedingt durch die Unsicherheit der Entscheidung des Senats konnten längst überfällige Umstrukturierungsmaßnahmen im Berichtsjahr nicht getroffen werden. Hinzu traten weitere personelle Abgänge. Damit sind zwar die Zielzahlen des PEP (Personalentwicklungsprogramm) erreicht, da aber die Anforderungen an die Dienststelle nicht geringer wurden, konnten die Arbeitsergebnisse nur gehalten werden, indem de einzelnen Beschäftigten zum Teil in erheblichem Umfang Mehrarbeit leisteten, die noch im kommenden Jahr abzubauen sein wird. Ich denke, der

Bericht macht die Leistungsfähigkeit der Dienststelle sowie die Vielfalt und Bandbreite des Tätigkeitsspektrums deutlich, auch wenn gerade die Erledigung der vielen, den Landesbeauftragten für den Datenschutz erreichenden Bürgeranfragen und Beschwerden, die oft auch eine Aufklärung vor Ort - häufig daher verbunden mit Fahrten nach Bremen - erfordern, nicht so deutlich zum Ausdruck kommen.

Ich habe das letzte Jahr genutzt, alle Haushaltspositionen auf Einsparmöglichkeiten hin zu untersuchen. Durch harte Verhandlungen oder Wechsel des Vertragspartners konnte ich in einer Reihe von Positionen günstigere Bedingungen oder sogar rückwirkend eine Gutschrift erreichen. Auf der anderen Seite ist absehbar, will sich der Landesbeauftragte für den Datenschutz nicht aus dem Verbund der Bremer Verwaltung verabschieden, dass sich bereits im kommenden Jahr - auch wegen des Standortes - Kostensteigerungen in einzelnen Haushaltsbereichen abzeichnen. So wird es unbedingt erforderlich sein, eine Standleitung für die Datenübertragung nach Bremen einzurichten. Auch die neuen Bahntarife und erhöhte Heizölkosten werden zu Buche schlagen. Im Berichtsjahr konnten in nur sehr eingeschränktem Umfang technische Fortbildungsmaßnahmen genehmigt werden, um die Haushaltsanschläge nicht zu überschreiten. Angesichts der raschen technischen Entwicklung und der Vielzahl der mit technischem Sachverstand von der Dienststelle zu beratenden Projekte und zu kontrollierenden Verfahren ist eine permanente Fortbildung eine notwendige Voraussetzung für die Aufgabenerfüllung.

1.6. Eingabenschwerpunkte und Öffentlichkeitsarbeit

Ein bedeutender Teil der von mir zu erfüllenden Aufgaben ist die Bearbeitung von Bürgereingaben. Sie bezogen sich zu ungefähr gleichen Teilen auf die Verarbeitung personenbezogener Daten im öffentlichen und im nicht-öffentlichen Bereich. Während die Eingaben im öffentlichen Bereich insbesondere die Verarbeitung personenbezogener Daten durch die Polizei, die Sozialverwaltung und Einrichtungen des öffentlichen Gesundheitsdienstes betrafen, bezogen sie sich im nicht-öffentlichen Bereich insbesondere auf Fragen des Arbeitsnehmerdatenschutzes und die Datenverarbeitung von Kreditinstituten, Versicherungsgesellschaften, Auskunfteien und in zunehmendem Maße auf Internet-Provider.

Die Eingaben waren nicht selten Anlass für umfangreiche Datenschutzüberprüfungen, deren Zahl - trotz der geringeren Personaldecke - notwendigerweise im Berichtszeitraum ebenfalls zunahm.

Mehrere Fortbildungsveranstaltungen und Vorträge zu aktuellen Themen des Datenschutzes wurden außerdem wieder in Wirtschaft und Verwaltung durchgeführt. Ein Schwerpunkt hierbei waren Veranstaltungen bei Einrichtungen im Sozialbereich und des öffentlichen Gesundheitswesens. Auch die Presse griff - oft nach Pressemitteilungen - aktuelle Datenschutzthemen auf. Exemplarisch genannt seien Berichte der Bremer Presse wie "Abgehört wird auch im Internet“, "„Der gläserne Mensch“, "Keine Weitergabe von Daten an rechtsradikale Parteien“, "Datenschützer warnt vor Kunden-Observa-

tionen“, "Menschen werden Objekt fremder Einflussnahme“, "Big Brother auf dem Weg zum Sielwall“, "Lauschangriff: Keine Wanzen in der guten Stube“, "Videoüberwachung: Allheilmittel oder Gift für Freiheitsrechte“, "Webcams, Datenschützer besorgt“ oder "Der gläserne Student“.

1.7. Kooperation mit anderen Datenschutzbehörden

Die Zusammenarbeit und der Erfahrungsaustausch findet für den öffentlichen Bereich unter den Datenschutzbeauftragten von Bund und Ländern statt und für den privaten Bereich unter den Datenschutzaufsichtsbehörden.

Die Konferenz der Datenschutzbeauftragten tagte in Hannover und Braunschweig unter Vorsitz des Niedersächsischen Datenschutzbeauftragten. Die wichtigsten Themen finden sich in den Konferenzbeschlüssen wieder (vgl. Ziff. 17. dieses Berichts). Die obersten Datenschutzaufsichtsbehörden der Länder trafen sich zweimal in Düsseldorf. Die hier erzielten Ergebnisse werden jeweils in einem Protokoll festgehalten, das nicht veröffentlich wird, die Beschlüsse des "Düsseldorfer Kreises“ schaffen aber für die Datenschutzkontrollen der Aufsichtbehörden eine einheitliche Grundlage für die Anwendung der Vorschriften des Bundesdatenschutzgesetzes (BDSG) im nicht-öffentlichen Bereich. Einige der Themen finden sich unter Ziff. 16. dieses Berichts. Auf der Ebene der Aufsichtsbehörden findet in der Regel einmal im Jahr ein Workshop statt, wo alle Teilnehmer einen Themenbereich vorbereiten. In beiden Bereichen (öffentlich und nicht-öffentlich) findet die Zusammenarbeit auch auf der Ebene von fachspezifischen Arbeitskreisen statt, an denen sich i. d. R. jeweils nur ein Teil der Länder beteiligen.

1.8. Ausblick

Die Anpassung der Vorschriften des BDSG an die EU-Datenschutzrichtlinie wird höchste Zeit, wird doch seit Ende des Berichtsjahrs die Einleitung eines Vertragsverletzungsverfahren durch die Europäische Kommission geprüft. Nunmehr wird für Ende Mai 2001 das Inkrafttreten des neuen BDSG erwartet. Daraus resultierend kann spätestens dann auch zügig mit der Novellierung des Bremischen Datenschutzgesetzes (BrDSG) begonnen werden. Die Entwicklungen in Bezug auf Polizeigesetz und Meldegesetz sind in 2000 nicht so schnell vorangekommen, wie ich noch im letzten Bericht gemutmaßt habe die parlamentarischen Beratungen werden in 2001 aufgenommen werden.

Des weiteren ist demnächst vom Bund der Entwurf eines Arbeitnehmerdatenschutzgesetzes zu erwarten. Der dafür zuständige Referatsleiter im Bundesarbeitsministerium hatte im Berichtsjahr dem Arbeitskreis Personalwesen der Datenschutzbeauftragten des Bundes und der Länder die Grundzüge des Entwurfs dargelegt und erklärt, neben bereichsspezifischen Regelungen über die Verarbeitung von Arbeitnehmerdaten werde der Gesetzentwurf im Hinblick auf die Informations- und Kommunikationsfreiheit Regelungen zur Nutzung von E-Mail und Internet am Arbeitsplatz vorsehen. Die nähere Ausgestaltung dieser Regelungen bleibe Betriebsvereinbarungen vorbehalten.

Die Präsenz des Landesbeauftragten für den Datenschutz mit einer Homepage im Internet (vgl. Ziff. 1.3. dieses Berichtes) wird ebenso wie die vom BDSG übertragenen neuen Aufgaben weitere Arbeit (z. B. Bürgereingaben zu Videoüberwachung und Chip-Karten) nach sich ziehen und zu Schwerpunktverlagerungen führen. Die Vielzahl der Automatisationsprojekte der Verwaltung in Bremen und Bremerhaven ist dem Bericht zu entnehmen, die meisten sind noch nicht abgeschlossen und bedürfen weiterer Begleitung. Hinzu kommen neue Projekte. Schon jetzt ist absehbar, dass die völlige Neustrukturierung der DV der Polizei (Vorgangsbearbeitung und INPOL-neu) umfangreiche Datenschutzberatung und -begeitung verlangen wird.

Auf dem Weg zu einer Informations- und Kommunikationsgesellschaft werden zunehmend auch technische Aspekte des Datenschutzes eine entscheidende Rolle spielen. Überall wo IuK-Technologie zur Verarbeitung personenbezogener Daten eingesetzt wird, sind technische, organisatorische und personelle Maßnahmen erforderlich, um eine missbräuchliche oder zweckentfremdete Nutzung der Daten zu vermeiden. Eine wichtige Aufgabe kann dabei von der Technik selbst übernommen werden, wenn es gelingt, in größerem Rahmen technische Systeme auch im Interesse des Datenschutzes zu entwickeln und einzusetzen. Verschlüsselungs- und Annonymisierungstechniken oder sog. Webwasher, (z. B Filter gegen Bugs, Banner, Privecyverletzungen oder Cookies) sind nur Beispiele für diese Entwicklung, die letztlich noch weiter gehen wird, wenn erst erkannt wird, dass der Datenschutz selbst auch ein Zukunftsmarkt sein wird. Jedenfalls belegen die Meinungsumfragen zum Datenschutz u. a. auch, dass alle Generationen dem Datenschutz einen hohen Stellenwert einräumen. Datenschutz wird damit zu einem Qalitätsmerkmal. Diesen Prozess gilt es aktiv zu unterstützen.

2. Telekommunikation, Teledienste und Medien

2.1. Novellierung des Telekommunikations-, Teledienste- und Medienrechts

2.1.1. Telekommunikations-Datenschutzverordnung

Nach langen Diskussionen hat das Bundeskabinett am 22. November 2000 eine neue Telekommunikations-Datenschutzverordnung (TDSV) beschlossen, die seit 21. Dezember 2000 in Kraft ist. Die TDSV musste aufgrund von Vorgaben des Telekommunikationsgesetzes (TKG), aber auch aufgrund bestehender EU-Richtlinien geändert werden und löst die aus dem Jahre 1996 stammende Verordnung ab. Zuvor wurden in kleinen Runden mit den Telekommunikationsreferenten der Wirtschaftsministerien – unterstützt durch eine konzertierte Zusammenarbeit der Datenschutzbeauftragten – strittige Punkte erörtert. Auch ich habe mich an dieser Diskussion beteiligt. Der Bundesrat befasste sich am 29. September 2000 mit der TDSV.

Trotz erheblicher Kritik der Datenschutzbeauftragten wurde durch die Neufassung der TDSV die Frist zur Speicherung von Verbindungsdaten drastisch von bisher 80 Tagen auf sechs Monate ab Rechnungsversand ausgedehnt. Obwohl diese Form der Vorratsspeicherung einen unnötigen Eingriff in das grundrechtlich geschützte Fernmeldegeheimnis darstellt, wurde mit der erhöhten Speicherfrist dem Interesse der Strafverfolgungsbehörden Rechnung getragen, für künftige Abfragen mehr Datenmaterial zur Verfügung zu haben. Aus Sicht der Datenschutzbeauftragten werden damit die Daten aller Nutzer von Telekommunikationsdiensten in die Fahndung mit einbezogen.

Darüber hinaus wurde das Wahlrecht von Kunden auf Löschung von Verbindungsdaten dahingehend eingeschränkt, dass diese Option nur noch gegenüber dem Anbieter ausgeübt werden kann, der die Rechnung verschickt. Auf die Speicherung von Verbindungsdaten anderer Call-by-Call-Anbieter hat der Kunde keinen Einfluss mehr.

2.1.2. Teledienstedatenschutzgesetz

Das Informations- und Kommunikationsgesetz (IuKDG) mit dem Teledienstedatenschutzgesetz (TDDSG) als wesentlichen Bestandteil ist zusammen mit dem Mediendienste-Staatsvertrag (MDStV) der Länder seit mehr als dreieinhalb Jahren in Kraft. Beide Regelungen stellen für die Datenschutzbeauftragten ein sehr effektives Mittel zur Kontrolle von Teledienten dar. Aufgrund der europäischen E-Commerce-Richtlinie, der geplanten Novellierung des BDSG und dem damit zusammenhängenden Harmonisierungsbedarf sowie aufgrund der Dynamik der technischen Entwicklungen besteht jedoch nunmehr gesetzgeberischer Handlungsbedarf. Diesen hat die Bundesregierung in ihrem Bericht an den deutschen Bundestag über die Erfahrungen und Entwicklungen bei den neuen Informations- und Kommunikationsdiensten ausführlich dargelegt (BT-Drs. 14/1191).

Ein Gesetzentwurf zur Änderung des Teledienstedatenschutzgesetzes liegt inzwischen vor. Dabei geht es neben dem erwähnten Harmonisierungsbedarf im wesentlichen um folgende Aspekte:

- **Konkretisierung des Geltungsbereichs:** Das TDDSG soll nur noch im Verhältnis von Anbietern und Nutzern von Telediensten gelten. Personenbezogenen Daten, die zur Steuerung von Geschäftsprozessen innerhalb oder zwischen Unternehmen oder öffentlichen Stellen verarbeitet werden, fallen nicht mehr in den Anwendungsbereich des TDDSG.
- **Verbesserung der Gesetzessystematik:** Die im Gesetz enthaltenen Grundsätze, Pflichten und Erlaubnistatbestände sind übersichtlicher zugeordnet.
- **Präzisierung der Einwilligung:** Die bisherigen engen gesetzlichen Erlaubnisse für Einwilligungslösungen werden in dem Gesetzentwurf mit dem Ziel konkretisiert, die bestehenden Rechtsunsicherheiten zu beseitigen.

- **Breitere Anwendung der elektronischen Einwilligung:** Die Vorkehrungen, die der Diensteanbieter für eine elektronische Einwilligung zu treffen hat, werden an die Entwicklung im elektronischen Rechtsverkehr angepasst.
- **Verhinderung des Missbrauchs von Telediensten:** Um den Zugriff auf rechtswidrige Inhalte besser verfolgen zu können, wird ein neuer Erlaubnistatbestand zur Nutzung von personenbezogenen Daten für Zwecke der Strafverfolgung eingeführt. Dieser erlaubt die Protokollierung von Internetaktivitäten einzelner Verdächtiger, jedoch keine Vollprotokollierung der Internetaktivitäten sämtlicher Kunden.
- **Begriffliche Abgrenzung:** Es erfolgt eine begriffliche Abgrenzung der Nutzungsdaten im TDDSG und der Verbindungsdaten in der TDSV.
- **Einführung von Sanktionen:** In Ergänzung zum BDSG werden nunmehr auch die wichtigsten Pflichten der Anbieter bußgeldbewährt.

2.2. Prüfung von Internet-Providern

Wer im Internet surft oder elektronische Post verschickt, hinterlässt dort zahlreiche, mehr oder weniger personenbeziehbare Datenspuren, einige davon bei den Internet-Providern, die den Zugang zum Internet herstellen und das sogenannte "Web-Hosting" betreiben. Zwar sind im Land Bremen zurzeit keine bundesweit agierenden Marktführer ansässig, dennoch gibt es einige Provider, über die zumindest in Bremen und Bremerhaven zahlreiche Benutzer Internetdienste in Anspruch nehmen. Vier davon habe ich im Berichtszeitraum geprüft.

Das Ergebnis verdeutlicht erhebliche datenschutzrechtliche Defizite. Sämtliche geprüften Provider erhoben und verarbeiteten personenbezogene Nutzungs- und Stammdaten über das gesetzlich erlaubte Maß hinaus. Die teilweise sehr komplexen und nicht immer transparenten gesetzlichen Regelungen waren den meisten Providern nicht in ausreichendem Umfang bekannt und wurden folglich nicht umgesetzt. Die Allgemeinen Geschäftsbedingungen bzw. Benutzerordnungen enthielten kaum Hinweise auf das Nutzungsverbot rechtswidriger Inhalte und waren zumindest in dieser Hinsicht überarbeitungsbedürftig. Auch waren die Mail- und Web-Server nicht in ausreichender Weise vor Attacken aus dem Internet gesichert.

2.2.1. Universität Bremen

Das Zentrum für Netze (ZfN) der Universität Bremen stellt sowohl den Studenten als auch den Mitarbeitern der Universität einschließlich der Institute einen z. Zt. noch kostenlosen Internetzugang, ein Postfach auf dem Mail-Server sowie Kapazität auf ihrem Web-Server zur Verfügung. Diese Angebote werden von ca. 19 000 Personen genutzt; zahlreiche Institute sowie der Fachbereich Informatik haben zusätzlich eigene Mail- und Web-Server im Einsatz. Da dieser Teledienst nicht nur den eigenen Mitarbeitern der Universität,

sondern auch Dritten angeboten wird, unterliegt die Universität damit dem Teledienstegesetz (TDG) und dem Teledienstedatenschutzgesetz (TDDSG).

Für die Universität Bremen ist der Domänenname *uni-bremen.de* reserviert. Fachbereiche und der Universität angeschlossene Institute und Einrichtungen können beim ZfN Subdomänen beantragen. Die Zahl der Subdomänen beträgt mehr als 300. Das ZfN führt eine entsprechende "Who-is-Datei".

Web-Hosting: Neben den offiziellen Seiten der Universität verwaltet das ZfN noch Web-Seiten von Hochschulinstituten, sofern diese keinen eigenen Web-Server betreiben, sowie von Studierenden. Dieses Web-Hosting ist sowohl ein Teledienst für eigene universitäte Zwecke als auch ein Teledienst für Dritte. Verantwortlich für das inhaltliche Angebot der Universität einschließlich der Fachbereiche ist gemäß § 5 Abs. 1 TDG die Leitung der Universität. Für fremde Inhalte, die die Universität Bremen zur Nutzung bereithält, ist sie gemäß § 5 Abs.2 TDG jedoch dann verantwortlich, wenn sie von den rechtwidrigen Inhalten Kenntnis erlangt.

Auf die jeweilige Verantwortung der Institute sowie der Studierenden wird zwar in der Benutzerordnung kurz hingewiesen. Auch existiert ein Hinweis auf die Bedingungen, unter denen das Leistungsangebot des ZfN genutzt werden kann. In der Benutzerordnung fehlen jedoch Hinweise auf das TDG sowie eine Auflistung der in § 8 Abs. 1 Mediendienste-Staatsvertrag (MDStV) genannten rechtswidrigen Inhalte. Eine Überarbeitung der Benutzerordnung ist daher für das Jahr 2001 vorgesehen.

Sofern Informationen über die Veröffentlichung rechtwidriger Inhalte vorliegen, geht das Zentrum für Netze diesen Hinweisen nach. Eine regelmäßige Überprüfung der Seiten sowie Stichproben fanden jedoch nicht statt. Die Universität Bremen hat eine regelmäßige stichprobenartige Durchsicht der persönlichen Homepages von Studierenden und Mitarbeitern auch mit dem Ziel angekündigt, dass der gemäß § 6 TDG geforderten Anbieter- bzw. Impressumspflicht verstärkt nachgekommen wird.

Die Zugriffe auf den Web-Server der Universität Bremen werden bezogen auf die IP-Nummer des Abrufenden 30 Tage gespeichert. Nach 30 Tagen werden die Protokolle zu Statistiken aggregiert. Diese Praxis widerspricht § 6 TDDSG, wonach ein Diensteanbieter personenbezogene Daten über die Inanspruchnahme von Telediensten frühestmöglich zu löschen hat, sofern es sich nicht um Abrechnungsdaten handelt. Zwar sind nach § 4 Abs. 4 TDDSG Nutzungsprofile bei Verwendung von Pseudonymen zulässig, wenn die Nutzungsprofile nicht mit Daten über den Träger des Pseudonyms zusammengeführt werden. IP-Adressen sind jedoch nur dann pseudonym, wenn sie dynamisch vergeben werden. Sofern ein Internetbenutzer mit statischen IP-Adressen arbeitet, ist es relativ problemlos möglich, den jeweiligen Benutzer zu ermitteln.

Da jedoch bei der Speicherung von Nutzungsprofilen kaum zwischen pseudonymen und nicht-pseudonymen bzw. dynamischen und statischen IP-Adressen differenziert werden kann, habe ich der Universität Bremen empfohlen, auf die Speicherung der IP-Adresse

vollständig zu verzichten und die IP-Adressen in den Protokolldatensätzen auf die jeweilige Class-C-Adresse zu aggregieren. Die Universität Bremen hat zugesagt, das jetzige Protokollierungsverfahren entsprechend zu überarbeiten.

Internetzugang und persönliches Postfach: Auf schriftlichen Antrag wird Studierenden sowie Mitarbeitern der Universität und der Institute sowohl ein Internetzugang als auch ein persönliches Postfach eingerichtet.

Der Internetzugang und das persönliche Postfach können sowohl aus dem Campusnetz mit seinen 1500 Rechnern als auch vom Heimarbeitsplatz aus benutzt werden. Dieser Einwahlservice steht 24 Stunden zur Verfügung. Auf dem hierfür benötigten Radius-Server werden Einwahlprotokolle erstellt, die Auskunft geben über Einwahldatum und -uhrzeit, über die jeweilige Benutzerkennung sowie die dynamisch vergebenene IP-Adresse einschließlich der Portnummer. Die Protokolle, die aufgrund des kostenlosen Zugangs nicht zu Abrechnungszwecken benötigt werden, wurden bislang 30 Tage aufbewahrt.

Da die Protokolldaten über die Vermittlung des Internetzugangs nicht ohne Einwilligung des Benutzers gespeichert werden dürfen, soll eine entsprechende Einwilligungslösung auch in die neu zu gestaltende Benutzerordnung aufgenommen werden. Gleichwohl sollen die Vermittlungsdaten spätestens nach einer Woche im ZfN gelöscht werden.

Die Anbindung des Campusnetzes an das Internet wird über das Deutsche Forschungsnetz (DFN) realisiert. Hierüber wird auch der Internetzugang für sämtliche an das Landesbreitbandnetz angeschlossenen Unternehmen und Organisationen hergestellt. Sämtliche DFN-Verbindungen wurden bislang ebenfalls personenbeziehbar protokolliert, obwohl die Datensätze lediglich für statistische Auswertungen benötigt werden. Demnächst werden die Protokolle nur noch temporär und im technisch erforderlichen Rahmen personenbeziehbar gespeichert und anschließend aggregiert!

Sicherheit des Campus-Netzes: Die Sicherheit des Campus-Netzes ist z. Zt. noch unzureichend. Weder existiert ein zentraler Firewall zur Absicherung des Universitätsnetzes, noch wird ein sogenanntes "Intrusion Detection System" zur Erkennung von Hackerangriffen eingesetzt. Zudem stehen – dies wurde bei einem von mir durchgeführten Online-Sicherheitscheck sehr deutlich – auf den internetweit erreichbaren Servern zahlreiche Dienste zur Verfügung, die potentiell Angriffen aus dem Internet ausgesetzt sind, ohne dass dies vom ZfN bemerkt würde.

Aufgrund dieser Sicherheitsrisiken hat die Universität Bremen zugesichert, ein umfassendes Sicherheitskonzept für das Campus-Netz zu erarbeiten, das u. a. den Aufbau eines Firewallsystems vorsieht. Zudem sollen auf den Servern nur diejenigen Ports netzweit verfügbar sein, die für elektronische Post und Internetzugriff benötigt werden. Sämtliche anderen Dienste sollen durch Einsatz eines Filterprogramms nur noch speziellen Rechnern zur Verfügung gestellt werden.

2.2.2. Bürgernetz Bremerhaven

Die Seestadt Bremerhaven bietet den Bürgern der Region seit Frühjahr 2000 auf der Basis des Stadtinformationssystems *bremerhaven.de* einen Internetzugang sowie eine E-Mail-Adresse an. Vereinen und Initiativen wird zudem die Möglichkeit eröffnet, Internetseiten unter dem Angebot von bremerhaven.de zu veröffentlichen. Das gesamte Angebot wird zurzeit von ca. 1500 Personen genutzt.

Betreiber des Stadtinformationsdienstes ist die Firma mcb multimedia-centrum bremerhaven, während der Mail-Server von der NordCom und die Web-Server von der Datenverarbeitungszentrale des Magistrats administriert werden. Inhaltlich verantwortlich für das Internetangebot der Seestadt Bremerhaven ist der Pressesprecher des Magistrats.

Stadtinformationssystem bremerhaven.de: Auf den Web-Servern wurden sämtliche Zugriffe IP-Nummern-bezogen protokolliert und zu statistischen Zwecken längere Zeit aufbewahrt. Da dies § 6 TDDSG widerspricht, wurde auf meinen Hinweis hin auf die Speicherung der IP-Adresse verzichtet. Es werden nunmehr lediglich aggregierte Protokolle über die Häufigkeit der Zugriffe geführt.

Darüber hinaus habe ich empfohlen, in einer sogenannten Privacy Policy dem Internetbenutzer Informationen darüber zu geben, in welchem Umfang personenbezogene Daten im Rahmen von *bremerhaven.de* gespeichert werden.

Internetzugang und elektronisches Postfach: Die Anmeldung für einen Internetzugang einschließlich E-Mail-Adresse erfolgt mittels Formular, dass auch online unter *bremerhaven.de* verfügbar ist. Neben Angaben zur Person wird der Kunde aufgefordert, darüber Auskunft zu geben, ob er Internetkunde der Nordcom, TelefonKunde der NordCom, Kunde der Städtischen Sparkasse Bremerhaven, Abonnent der Nordsee-Zeitung oder Nutzer des Homebanking-Programms StarMoney ist. Diese Felder waren Plichtfelder, die mit der Anmeldung zum Bürgernetz ausgefüllt werden mussten.

Da gemäß § 6 Abs. 1 TDDSG personenbezogene Daten über die Inanspruchnahme von Telediensten nur zu Abrechnungs- oder Vermittlungszwecken erheben werden dürfen, habe ich gefordert, auf die genannten Pflichtfelder zu verzichten. Das entsprechende Web-Formular wurde daraufhin modifiziert; die Daten werden nunmehr auf freiwilliger Basis erhoben.

Die Bedingungen, unter denen der Internetzugang genutzt werden kann, regeln die Geschäftsbedingungen. Diese waren jedoch sehr allgemein gehalten und hinsichtlich des Datenschutzes wenig aussagekräftig. Auf meine Anregung hin wurden die Geschäftsbedingungen überarbeitet und präzisiert.

Der Internetzugang wird über einen Radius-Server vermittelt; die jeweiligen IP-Adressen werden dynamisch vergeben. Welche IP-Adressen zu welcher Zeit an welchen Account vergeben wurden, wird auf dem Radius-Server längere Zeit protokolliert. Da personenbezogene Daten über die Inanspruchnahme dieses Teledienstes gemäß § 6 Abs. 1 TDDSG

nur erhoben und verarbeitet werden dürfen, soweit es für die Vermittlung des Internetzugangs erforderlich ist, habe ich den Magistrat aufgefordert, die Daten gemäß § 6 Abs. 2 TDDSG frühestmöglich zu löschen. Die NordCom hat sich hierzu als Betreiber der Server bereit erklärt.

Netzsicherheit: Es existiert keine Firewall zur Absicherung der NordCom- und Magistrats-Server. Hierdurch stehen internetnetweit sämtliche auf den jeweiligen Servern installierten Dienste zur Verfügung. Dies ist aus datenschutzrechtlicher Sicht problematisch, da diese Rechner weltweit attackiert werden können. Auf meine Forderung hin hat sich der Magistrat bereit erklärt, eine Firewall sowie ein sogenanntes Intrusion Detection Systems zu installieren.

2.2.3. Internationale Stadt Bremen/isb GmbH

Im Herbst letzten Jahres habe ich die Firma isb GmbH geprüft, die neben ihrer Providertätigkeit noch als Betreiber der Internetseite is-bremen.de agiert. Auch bei isb wurden erheblich mehr Daten über die Internetnutzung gespeichert als zulässig. Darüber hinaus sind die Server nicht ausreichend vor missbräuchlichen Attacken aus dem Internet heraus gesichert.

Internationale Stadt Bremen *is-bremen.de:* Zugriffe auf die Web-Server der isb GmbH, darunter auch Internetzugriffe auf die Seiten von is-bremen.de, werden IP-Nummernbezogen gespeichert. Da dies – wie bereits erwähnt – zumindest im Hinblick auf statisch vergebene IP-Adressen unzulässig ist, habe ich empfohlen, vollständig auf die Speicherung von IP-Adressen zu verzichten. isb hat sich bereit erklärt, die Aufzeichnung der Zugriffe zu anonymisieren, sobald die Transferleistungen des Servers mit den Kunden abgerechnet ist. Ein manueller Eingriff in den Programmcode des Web-Servers wurde mit dem Hinweis abgeleht, dass der Programmieraufwand angesichts regelmäßiger Updates des Servers nicht realisierbar sei. Die Kunden von isb hätten ohnehin nur Zugriff auf die anonymisierten Statistiken.

Internetzugang und persönliches Postfach: Die Bedingungen, unter denen der Internetzugang und das persönliche Postfach genutzt werden können, werden in den Kundenverträgen und den allgemeinen Geschäftsbedingungen geregelt. Auf meine Anregung hin wurden die allgemeinen Geschäftsbedingungen dahingehend erweitert, dass auf die Impressumspflicht hingewiesen wird. Darüber hinaus habe ich empfohlen, die Kunden auf die Möglichkeit hinzuweisen, dass bei isb zum Surfen im Internet Pseudonyme benutzt werden können.

Der Internetzugang wird über einen Radius-Server vermittelt. Ich habe kritisiert, dass auf diesem Server protokolliert wird, wer zu welcher Zeit unter welcher IP-Adresse im Internet agiert hat. Isb hat diese Forderung aufgegriffen und wird künftig auf die Speicherung der IP-Adresse verzichten.

Netzsicherheit: Auf den isb-Servern waren zahlreiche TCP/IP-Ports erreichbar, die von Außenstehenden zu Attacken genutzt werden können. Um die Gefahr einer missbräuchlichen Nutzung dieser Ports zu reduzieren, habe ich isb aufgefordert, die verfügbaren Ports auf das erforderliche Maß zu beschränken. Auch sollte das Netz der isb durch Einsatz einer Firewall zusätzlich geschützt werden.

isb hat sich leider weder bereit erklärt, die internetweit verfügbaren Ports zu reduzieren noch einen Firewall zum Schutz der Server zu installieren. Ich habe daraufhin isb nochmals ausdrücklich aufgefordert, die Sicherheit der eigenen Server zu verbessern. Eine Antwort von isb steht noch aus.

2.2.4. Vossnet Communications GmbH

Im Januar 2000 habe ich die Providertätigkeit der Firma Vossnet geprüft, die zur damaligen Zeit u. a. als bundesweiter Stromanbieter aufgrund ihrer Geschäftspraktiken ins Gerede gekommen war. Leider hatte die Firma Vossnet aufgrund von Zahlungsschwierigkeiten drei Tage vor dem Prüftermin ihre Tätigkeit als Internetprovider eingestellt und eine Lübecker Firma veräußert, die bereits seit Herbst letzten Jahres auch als TK-Dienstleister für die Firma Vossnet tätig war. Da auch die entsprechenden Rechner gleich mit veräußert wurden, bezog sich die Prüfung schwerpunktmäßig auf die noch bei der Firma Vossnet verbliebenen Bestandsdaten sowie auf organisatorische Rahmenbedindungen.

Trotz Aufgabe des Onlinedienst-Geschäftszweiges waren von Vossnet noch sämtliche Bestandsdaten der Kunden gespeichert – auch Daten solcher Kunden, mit denen seit langem kein Vertragsverhältnis mehr bestand und gegenüber denen auch keine Forderungen mehr existierten. Zwar war das Kündigungsdatum eingetragen, der entsprechende Kundendatensatz war jedoch nicht gelöscht worden. Ich habe Vossnet daraufhin aufgefordert, die Bestandsdaten sämtlicher Kunden mit aufgelöstem Vertragsverhältnis unverzüglich zu löschen, gegenüber denen keine Forderungen mehr existieren.

Der Verkauf des Onlinedienst-Geschäftszweiges blieb in den ersten Tagen für die Kunden unbemerkt. Da die Lübecker Firma bereits seit längerem als TK-Dienstleister für Vossnet tätig war, konnte trotz des Wechsels die Einwahl weiterhin über die gleiche Einwahlnummer erfolgen wie bisher. Über den Wechsel des Diensteanbieters wurden die Kunden erst nach einigen Tagen per Brief informiert. Hierin wurden die Kunden u. a. auf die Webseite der Lübecker Firma mit der Bitte verwiesen, ihre Bestandsdaten – geschützt durch ihren Benutzernamen und Passwort – zu prüfen und entsprechend zu aktualisieren. Sämtliche Bestandsdaten der Onlinedienst-Kunden (Adresse einschließlich Konto-Verbindung) waren mit dem Verkauf des Geschäftszweiges von der Firma Vossnet an die Lübecker Firma übermittelt worden. Die Vertragsübergabe an Dritte war in Ziff. 9 der Allgemeinen Geschäftsbedingungen geregelt, die dem Kunden das Recht einräumte, im Falle einer Vertragsübergabe sofort den Vertrag zu kündigen.

Die Übermittlung sämtlicher Bestandsdaten von Onlinekunden an die Firma in Lübeck stellt einen Verstoß gegen § 28 Abs.1 BDSG dar. Zwar ist es zur Wahrung berechtigter Interessen der speichernden Stelle zulässig, Bestandsdaten von Kunden an ein Unternehmen zu übermitteln, an das der jeweilige Geschäftsbereich veräußert worden ist. Eine unzulässige Übermittlung stellt jedoch die Weitergabe von Kundendaten dar, mit denen überhaupt kein Vertragsverhältnis mehr existiert.

Zudem fiel bei der Prüfung negativ auf, dass Vossnet weder einen betrieblichen Datenschutzbeauftragten bestellt hatte, obwohl dort ehemals 60 Mitarbeiter – zahleiche mit Zugriff auf Kundendaten – beschäftigt waren, noch der Meldung zum Register gemäß § 32 BDSG nachgekommen war. Eine Verpflichtung der Mitarbeiter auf das Datengeheimnis war ebenso unterblieben.

3. Datenschutz durch Technikgestaltung und -bewertung

3.1. Bremisches Verwaltungsnetz

3.1.1. Online-Prüfung des Bremischen Verwaltungsnetzes

Im Sommer letzten Jahres habe ich mittels Onlinetests die Sicherheit des Bremischen Verwaltungsnetzes (BVN) sowie der hieran angeschlossenen Server der Bremer Kommunikationstechnik (BreKom) sowie der Informations- und Datentechnik Bremen (ID Bremen) geprüft. Getestet wurde die Erreichbarkeit und Verfügbarkeit von Rechnern und Diensten des BVN von einem normalen Arbeitsplatz-PC meiner Dienststelle aus, die ebenfalls über einen Anschluss an das Bremische Verwaltungsnetz verfügt. Da die Online-Prüfung mit den Standard-Zugriffsrechten eines BVN-Anwenders durchgeführt wurde, sind die aus der Prüfung gewonnenen Prüferkenntnisse typisch für das gesamte Netz; die im Rahmen der Prüfung aufgedeckten Lesezugriffe wären von fast jedem Arbeitsplatz der bremischen Verwaltung, der an das BVN angeschlossen ist, möglich gewesen. Dies gilt umso mehr, als frei verfügbare Prüfwerkzeuge und Windows NT-Ressourcen benutzt wurden.

Die Sicherheit des Bremischen Verwaltungsnetzes wird in starkem Maße durch die zentrale Struktur des Netzes geprägt, die lediglich Zugriffe der Ämter auf die zentralen Server der BreKom und der ID Bremen zulässt. Dass Querzugriffe der Ämter auf andere BVN-Standorte nicht möglich sind, fiel bei der Online-Attacke positiv auf.

Erfreulich war ebenfalls die Tatsache, dass die Server der ID Bremen BVN-seitig durch den Einsatz eines Firewall abgesichert sind und somit keine Zugriffe möglich waren, die über das erlaubte Maß hinausgingen. Im Gegensatz hierzu erwiesen sich allerdings die zentralen Server der Bremer Kommunikationstechnik als attackierbar, da der Zugriff hierauf nicht durch einen Firewall kontrolliert wurde. Die netzweite Erreichbarkeit der BreKom-Rechner war umso problematischer, als auf den geprüften Rechnern zahlreiche

TCP/IP-Ports verfügbar waren, die für weitere gezielte Attacken hätten genutzt werden können. Im Einzelnen ist zu berichten:

- Bei den im Test ermittelten telnet-, ftp- und netbios-Ports bestand das Risiko, durch Ausprobieren der jeweiligen Passwörter – unterstützt durch sogenannte Passwort-Cracker – missbräuchlich Zugriff auf die jeweiligen Rechner zu erhalten. Bei schnellen Netzwerkverbindungen, die während des Tests allerdings nicht zur Verfügung standen, hätten pro Stunde mehr als 10 000 Passwörter per Brute-Force-Attacke ausprobiert werden können, so dass es nur eine Frage der Zeit gewesen wäre, bis Passwörter automatisch ermittelt worden wären. Brute-Force-Attacken richten sich vor allem gegen die Administratorkennung, die nach mehrmaligen Fehlversuchen nicht deaktiviert werden kann.

- Der Netbios Session Service kann domainübergreifend dazu genutzt werden, um Informationen über freigegebene Verzeichnisse und Benutzerkonten auf Rechnern zu erhalten. Beispielsweise war es im Verlauf des Online-Tests möglich, sämtliche ca. 200 Benutzerkennungen auf dem zentralen Mail-Server der BreKom zu ermitteln. Diese Informationen sind für gezielte Attacken recht hilfreich, da von vielen Benutzern Standard-Passwörter verwendet werden.

- Der Zugriff auf den Finger-Dienst zahlreicher BVN-Router ermöglichte es, Auskunft über die aktuell im BVN vermittelten Anwender zu erhalten. Diese Informationen geben nicht nur Informationen über das Nutzungsverhalten zahlreicher Behördenmitarbeiter, sondern können auch wiederum für weitere Attacken verwendet werden.

Um die missbräuchliche Nutzung der Ports zu reduzieren, habe ich in meinem Prüfbericht gefordert, die verfügbaren Ports auf das erforderliche Maß zu beschränken. Darüber hinaus sollte zum Schutz der BreKom-Server vor BVN-internem Missbrach ein zusätzlicher Firewall seitens der Bremer Kommunikationstechnik installiert werden.

Beide Forderungen sind sowohl von der BreKom als auch vom Senator für Finanzen als Betreiber des Bremischen Verwaltungsnetzes sehr konstruktiv als wesentliche Maßnahme zur Verbesserung der internen Netzsicherheit aufgegriffen worden. Die netzweit verfügbaren Ports wurden von der BreKom bereits während der Prüfungsphase erheblich eingeschränkt. Eine Firewall zum internen Schutz der BreKom-Server wird ab Frühjahr 2001 aufgebaut. Hierdurch ist es möglich, von zentraler Stelle aus die Erreichbarkeit von Maschinen und Diensten für das BVN zu steuern sowie kontinuierlich die Einhaltung der Sicherheitsrichtlinien zu überprüfen. Damit wurde meinen Anregungen im Prüfbericht voll und ganz Rechnung getragen.

3.1.2. Elektronische Post in der bremischen Verwaltung

Bereits im letzten Jahr (vgl. 22. JB, Ziff. 3.4.) hatte ich ausführlich über den Einsatz elektronischer Post in der bremischen Verwaltung berichtet und u. a. abschließende Regelungen sowie Verschlüsselungsmaßnahmen gefordert. Dies war auch Gegenstand der

Beratungen im Datenschutzausschuss. Mittlerweile hat der Senatur für Finanzen einen Richtlinienentwurf zum Einsatz elektronischer Post vorgelegt, der – auf einer Richtlinie des deutschen Städtetages aufbauend – detailliert auf Vertretungsregelungen und Verschlüsselungsmaßnahmen eingeht.

Der Entwurf ist nicht zuletzt Ergebnis einer teilweise kontroversen, aber konstruktiven Diskussion aller in der Arbeitsgruppe "Sicherheit im Bremischen Verwaltungsnetz" vertretenen Akteure. Dabei stand zum einen das Interesse der Verwaltung an flexiblen Vertretungsregelungen im Vordergrund, die auch bei Abwesenheit des Empfängers (Urlaub, Krankheit) ein Weiterleiten der E-Mail ermöglichen. Zum anderen galt es, die Datenschutzinteressen sowohl der betroffenen Bürger als auch der Beschäftigten zu berücksichtigen, elektronische Post weitgehend vertraulich über das Bremische Verwaltungsnetz (BVN) zu übertragen und auf den Mail-Servern bei Bedarf verschlüsselt zu speichern. Im Verlauf der Diskussion wurden vor allem folgende Probleme deutlich:

- Sofern die dienstlich zur Verfügung gestellten individuellen Postfacher auch für private Zwecke genutzt werden dürfen oder eine private Nutzung geduldet wird, liegt ein Telekommunikationsdienst vor, der Dritten zur Verfügung gestellt wird. Ein solcher Telekommunikationsdienst unterliegt gemäß § 85 Telekommunikationsgesetz (TKG) dem Fernmeldegeheimnis. Folglich dürften Inhalte von Postfächern, die auch privat genutzt werden, nur von den Empfängern selbst gelesen werden. Ein Weiterleiten der elektronischen Post an einen Vertreter wäre dann nur bei Einwilligung des Postfach-Eigentümers möglich.
- Elektronische Post, die mit benutzerbezogenen, signaturgesetzkonformen Zertifikaten verschlüsselt worden ist, kann nur von dem Benutzer selbst entschlüsselt werden. Da ein solches Zertifikat nicht dupliziert werden kann, wäre bei Verlust des Zertifikates bzw. bei Verlust des Trägermediums die Nachricht nicht mehr zu entschlüsseln. Ein mit einem Gruppenschlüssel bzw. einem serverbasierten Zertifikat codiertes Dokument wäre dagegen rückholbar.
- Die intern für die bremische Verwaltung angestrebte Verschlüsselungslösung sollte möglichst kompatibel sein mit der chipkartenbasierten Lösung des MEDIA@Komm-Projekts, d. h. die X.509-Zertifikate sollen sowohl softwarebasiert als auch hardwarebasiert verwendet werden können.

Die nunmehr im Entwurf vorliegende Richtlinie versucht diese Aspekte durch folgende Regelungen zu berücksichten:

- Für dienstliche Postfächer ist die private Nutzung unzulässig. Private elektronische Post soll ausschließlich über Postfächer auf speziellen Internet- oder Intranet-Servern verschickt werden.
- Pro Dienstelle werden ein zentrales Postfach für die Poststelle, personenbezogene Postfächer sowie bei Bedarf Postfächer für einzelne Organisationseinheiten oder Arbeitsgruppen eingerichtet.

- Bei vorhersehbarer Abwesenheit (Urlaub, Dienstreisen) hat jeder Mitarbeiter zu veranlassen, dass neu eingehende Post automatisch an den Vertreter weitergeleitet wird oder ein automatischer Antworttext an den Absender geschickt wird, in dem auf die Abwesenheit des Empfängers hingewiesen wird. Bei längerer nicht vorhersehbarer Abwesenheit sind Mechanismen umzusetzen, die den Zugriff des Vertreters auf das Postfach des Abwesenden ermöglichen.
- Bis zur Einführung der digitalen Signatur sollen nur solche Dokumente per E-Mail versandt werden, die keinen besonderen Formvorschriften oder Zugangsvoraussetzungen unterliegen.
- Die Übermittlung sensibler Daten mittels E-Mail ist nur unter Einsatz geeigneter Verschlüsselungsverfahren zulässig. Damit eine Stellvertretung gewährleistet wird, soll zukünftig zur Verschlüsselung ausschließlich ein Gruppen-Zertifikat der Dienststelle bzw. des Servers eingesetzt werden. Die derzeit genutzte Verschlüsselung mit einem dem Benutzer persönlich zugeordneten Verschlüsselungszertifikat (z. B. bei Verfahren wie PuMa und SEKT) soll zukünftig durch ein solches Gruppen-Zertifikat der Dienststelle bzw. des Servers abgelöst werden.

Der skizzierte Entwurf der Richtlinie berücksichtigt datenschutzrechtliche Überlegungen und wird gerade mit den Behörden der bremischen Verwaltung abgestimmt. Ich gehe davon aus, dass die Grundgedanken des jetzigen Entwurfs weitgehend in die Endfassung übernommen werden. Der Senator für Finanzen arbeitet zurzeit an der technischen Umsetzung der vorgeschlagenen Verschlüsselungsvariante.

3.2. Verwaltungsnetz des Magistrats der Seestadt Bremerhaven

Die Datenverarbeitungszentrale des Magistrats hat in den letzten beiden Jahren komplett sämtliche Großrechner-Anwendungen erfolgreich auf Client-Server-Verfahren umgestellt. Die Grundlage hierfür bildet ein modernes Verwaltungsnetz mit einem Novell Directory Service (NDS) als Verzeichnisdienst. Auf den Arbeitsplatz-PC wird Windows NT als Betriebssystem eingesetzt, auf den Servern sowohl Novell Netware als auch Windows NT.

Obwohl die Umstellung von meiner Dienststelle soweit wie möglich begleitet wurde, gelang es nicht immer, bereits mit der Einführung der neuen Verfahren datenschutzkonforme Lösungen umzusetzen. Dies galt insbesondere hinsichtlich der Sicherheit des Magistratsnetzes. Umstritten waren zunächst folgende Punkte:

- Elektronische Post ist an gut 1100 Arbeitsplätzen verfügbar, ohne dass die Möglichkeit besteht, die Nachrichten zu verschlüsseln. Der Aufbau einer von mir geforderten Verschlüsselungsinfrastruktur wurde zunächst als zu aufwändig eingeschätzt, insbesondere die hiermit verbundene Schulung sämtlicher Anwender. Mittlerweile ist der Aufbau einer X.509-Verschlüsselungsinfrastruktur vorgesehen, die konform ist zu der im MEDIA@Komm-Projekt (vgl. 22. JB, Ziff. 3.1. u. in diesem Bericht Ziff. 3.1.2. u. 3.4.) realisierten Chipkartenlösung.

- An zahlreichen Arbeitsplätzen steht ein Internetzugang zu Verfügung, ohne dass die lokal verfügbaren sensiblen personenbezogenen Daten ausreichend gesichert wären. Um zu verhindern, dass diese Daten aus dem Magistratsnetz heraus unbemerkt ins Internet versendet werden, habe ich gefordert, entweder getrennte Arbeitsumgebungen auf den Windows NT-Client einzurichten oder Terminal-Server einzusetzen (vgl. 22. JB, Ziff. 3.4.4.). Seit Anfang des Jahres existieren nunmehr zwei Pilotprojekte zur Erprobung von Terminal-Servern sowohl auf Windows NT- als auch auf einer Linux-Plattform. Anfang 2001 ist ebenfalls ein geeignetes Einsatzkonzept für Windows NT verabschiedet worden, das den Administratoren praxisrelevante Hinweise für eine ordnungsgemäße und sichere Installation der Server und Client gibt.

- Mit Ausnahme von Verfahren des Sozialamts werden sämtliche Client-Server-Verfahren des Magistrats in einer gemeinsamen NDS (Novell Directory Service) verwaltet. Die Daten der jeweiligen Verfahren werden in sogenannten Containern gespeichert. Während die Administration der NDS durch einen Magistratsadministrator mit sehr umfassenden Superuserrechten erfolgt, werden die Container durch Bereichsadministratoren verwaltet. In einigen Ämtern, beispielsweise im Gesundheitsamt oder im Jugendamt werden die Bereichsadministratoren von der speichernden Stelle selbst gestellt. In anderen Fällen wird die Bereichsadministration im Auftrag der Ämter von der Datenverarbeitungszentrale wahrgenommen (z. B. beim Amt für Arbeitsmarktpolitik).

  Das Datenschutzproblem bestand nunmehr darin, dass zum einen nicht nur der Magistratsadministrator, sondern auch die Bereichsadministratoren mit Zugriffsrechten ausgestattet sind, die es ihnen ermöglichen, auf Daten des gesamten Magistratsnetzes bzw. auf die Daten der jeweiligen Container bzw. Bereiche zuzugreifen; zum anderen wurde seitens der Datenverarbeitungszentrale sowohl die Magistrats- als auch die Bereichsadministration lediglich von zwei Personen durchgeführt, so dass die angestrebte arbeitsteilige Administration des Magistratsnetzes faktisch nicht funktionierte. Mit der Benennung weiterer Bereichsadministratoren im Baubereich, im Bereich des Ordnungsamtes, im Personal- und Organisationsamt und im Bereich der Stadtkämmerei wurde dieses Problem Ende des letzten Jahres insoweit reduziert, als zumindest keine bereichsübergreifenden Zugriffe von Systemadministratoren auf sensible Daten mehr möglich sind.

War der Kraftakt der Umstellung im Bremerhavener Magistratsnetz zunächst geprägt durch rein technische Fragestellungen, bei der der Datenschutz nicht immer den entsprechenden Stellenwert erhielt, befindet sich die Datenverarbeitungsphase nach deren Aussage mittlerweile in einer Konsolidierungsphase, in der nunmehr auch nicht-technische Aspekte im Detail geregelt und umgesetzt werden. Mit der Verabschiedung zweier RichtInien zum Einsatz von Windows NT sowie zur NDS-Administration wurden unter engagierter Mithilfe des neuen behördlichen Datenschutzbeauftragten die grundlegenden

Voraussetzungen für eine datenschutzgerechte Ausgestaltung der Fachverfahren geschaffen.

3.3. ID Bremen

Zur Privatisierung der ID Bremen und dem in diesem Zusammenhang erstellten Datenschutzkonzept habe ich bereits im letzten Jahresbericht (Ziff. 3.3.) ausführlich Stellung genommen. Einer der zentralen Eckpfeiler des Datenschutzkonzepts stellte seinerzeit die Gründung einer Aufsichtführenden Stelle beim ID Bremen Eigenbetrieb dar, die sämtliche Verfahren der ID Bremen GmbH, in denen sensible Daten hoheitlich verarbeitet werden, hinsichtlich einer ordnungsgemäßen Datenverarbeitung kontrollieren sollte.

Diese Aufsichtführende Stelle habe ich gegen Ende des Jahres geprüft. Die Aufsicht über die ID Bremen GmbH umfasst laut Datenschutzkonzept schwerpunktmäßig die Großrechneradministration mittels RACF, die Arbeitsvorbereitung, die Druckausgabe sowie die Verfahrensentwicklung einschließlich der Übergabe in die Produktion.

Insgesamt wurde bei der Prüfung jedoch deutlich, dass die Arbeitsteilung zwischen der ID Bremen GmbH und der Aufsichtführenden Stelle nicht in dem Umfang umgesetzt worden ist, wie sie seinerzeit im Sicherheitskonzept festgelegt wurde. Die Aufsichtführende Stelle ist zu einem Großteil der Tätigkeit direkt an der Umsetzung des Sicherheitskonzepts beteiligt und hat umfangreiche Aufgaben übernommen, die normalerweise von der ID Bremen GmbH zu erledigen wären. Ein wesentlicher Schwerpunkt der Tätigkeit hat sich dabei auf die Gebäudesicherheit bezogen. Konzeptionell wurden Umbaumaßnahmen begleitet sowie eine neue Zugangskontrollregelung für die Räumlichkeiten entwickelt. Auch war die Aufsichtführende Stelle für das Einrichten neuer Benutzer ebenso zuständig wie für Änderungen der Zugriffsrechte. Die Aufsichtführende Stelle kontrollierte sich damit selbst.

Im Interesse einer ordnungsgemäßen Arbeitsteilung zwischen der ID Bremen GmbH und der Aufsichtführenden Stelle habe ich gefordert, dass die RACF-Benutzerverwaltung von der ID Bremen GmbH durchgeführt wird. In diesem Sinne ist es positiv, dass nunmehr ein Ansprechpartner seitens der ID Bremen GmbH zur Verfügung steht, der diese Tätigkeiten übernommen hat. Die Aufsichtführende Stelle sollte sich dagegen auf ihre eigentliche Aufsichtsfunktion konzentrieren und die im Sicherheitskonzept aufgeführten Revisionsaufgaben regelmäßig durchführen. Die Ergebnisse sollten regelmäßig in Quartalsberichten dokumentiert und den Auftraggebern mitgeteilt werden.

Um die Revison sachgerecht durchführen zu können, benötigt die "Aufsichtführende Stelle" geeignete Auditing- und Controlling-Werkzeuge. Zwar stehen mit den sogenannten SMF-Störungsmeldungen und RCD-Jobprotokollen entsprechende Hilfsprogramme zur Verfügung. Diese sind jedoch im Hinblick auf regelmäßige Revisionszyklen noch verbesserungsfähig. Die ID Bremen beabsichtigt, verbesserte Tools bereitzustellen.

Bei der Prüfung fiel zudem auf, dass die Kontrolle der RACF-Administration ebenso wie die RACF-Administration über Arbeitsplatz-PC erfolgt, die über einen Internetzugang verfügen. Der gleichzeitige Zugriff auf das Internet und den MVS-Großrechner ist äußerst problematisch. Es besteht die Gefahr, dass verdeckte Programmfunktionen bzw. Trojanische Pferde auf dem lokalen Rechner ausgeführt werden, die es ermöglichen, Außenstehenden Remote-Zugriff über den PC und somit auch über den Großrechner einschließlich der RACF-Administration zu verschaffen. Ich habe empfohlen, den Internetzugang im ID Bremen generell über einen Terminal-Server zu realisieren, der – durch Firewall getrennt – außerhalb des Hausnetzes des ID Bremen installiert wird. Sämtliche sicherheitskritischen Internetdienste sollten hierüber ausgeführt werden, so dass Webseiten oder Inhalte von elektronischer Post lediglich in Form einer Grafik vom Terminal-Server an den jeweiligen Arbeitsplatz-PC übertragen werden. Da der Terminal-Server die eigentliche Datenverarbeitung übernimmt, können auch keine unerwünschen Fehlfunktionen auf dem Arbeitsplatz-PC zur Ausführung gelangen. Um Restrisiken zu vermeiden, wird die ID Bremen die RACF-Administration zunächst über Stand-alone-Konsolen betreiben, der Einsatz von Terminal-Servern wird geprüft. Damit ist eine befriedigende Lösung erreicht.

Die Verträge mit den Kunden der ID Bremen GmbH enthielten darüber hinaus keine Klauseln hinsichtlich der seitens der ID Bremen getroffenen technisch-organisatorischen Sicherheitsmaßnahmen. Zudem wurde nicht auf die Revisionstätigkeit der "Aufsichtführenden Stelle" hingewiesen. Auf meine Anregung hin werden nunmehr entsprechende Regelungen in die Verträge aufgenommen, damit den Kunden der ID Bremen ein Mindest-Sicherheitsstandard einschließlich einer unabhängigen Kontrolle durch die "Aufsichtführende Stelle" vertraglich garantiert wird.

3.4. MEDIA@Komm

Die Präsenz von Städten und Gemeinden im Internet wächst. Gleichwohl ist die bisherige Entwicklung über das Niveau von Informationsangeboten kaum hinausgegangen. Der breite Durchbruch zur rechtsverbindlichen Interaktion in elektronischen Netzen auf Basis der digitalen Signatur steht noch aus. Hier setzt das Projekt MEDIA@Komm an, auf das ich bereits im letzten Jahresbericht ausführlich eingegangen bin.

Zur Umsetzung des MEDIA@Komm-Projekts wurde im Herbst 1999 eigens die "bremen online services" (bos) gegründet. In den nächsten zwei Jahren wird bos 70 rechtsverbindliche Geschäftsprozesse mit 26 privaten und öffentlichen überregionalen Dienstleistern gebündelt in Form von Lebenslagen anbieten.

Die lebenslagenübergreifenden Themen "rechtliche Einschätzung der bos-Geschäftsfelder", "bos-Plattform" und "elektronischer Laufzettel" sowie zum Probebetrieb seit September 2000 nehme ich im Folgenden ausführlicher Stellung.

Geschäftsfelder von bos: bos ist als nicht-öffentliche Stelle anzusehen, soweit sie eigene personenbezogene Daten verarbeitet und nutzt. Im Verhältnis zur bremischen

Verwaltung tritt bos hauptsächlich als eigener Datenverarbeiter (eigene speichernde Stelle) mit spezifischen Dienstleistungsfunktionen auf; bos ist bis auf einige Ausnahmen nicht Auftragnehmerin im Rahmen eines DV-Auftragsverhältnisses. Datentransferleistungen zwischen bos und der bremischen Verwaltung stellen also Übermittlungsvorgänge dar.

bos übernimmt eine Providertätigkeit, die als Teledienst dem Teledienstgesetz (TDG) und somit auch dem Teledienstedatenschutzgesetz (TDDSG) unterliegt. Soweit an die Allgemeinheit gerichtete Informations- und Kommunikationsdienste angeboten bzw. zur Nutzung bereitgehalten werden (z. B. Allgemeine Verwaltungshinweise, Amtliche Bekanntmachungen u. Mitteilungen), gilt der Mediendienstestaatsvertrag (MDStV).

bos-Plattform: Informationstechnisch werden die Dienstleitungen über eine zentrale Plattform realisiert, die von bos betrieben wird. Die Transaktionen basieren auf dem Online Services Computer Interface Standard (OSCI), der mit dem Bankenstandard für Internetbanking HBCI vergleichbar ist und von bos aufgrund fehlender Standards zur Abwicklung von Geschäftsvorfällen eigens für MEDIA@Komm entwickelt wurde.

Die Dienstleistungen werden über das Internet über die Adresse **www.bremen.de** offeriert und durchgeführt. Die Rechtssicherheit wird durch eine signaturgesetzkonforme digitale Signatur gewährleistet.

Die bos-Plattform soll folgende Funktionen haben:

- Bereitstellung von Formularen auf einem Formularserver,
- Empfang der gemäß Signaturgesetz (SigG) signierten und verschlüsselten Formularinhalte in Form von OSCI-Nachrichten,
- Entschlüsselung der Absender- und Empfängerinformationen der OSCI-Nachricht,
- Generierung eines sogenannten Laufzettels, auf dem Verbindungsinformationen protokolliert werden,
- Überprüfung der OSCI-Nachrichten auf syntaktische und in Einzelfällen auch auf semantische Richtigkeit,
- Zahlungsabwicklung von Dienstleitungen,
- Einfügen von Bezahlinformationen in den Laufzettel der OSCI-Nachricht,
- Entschlüsselung der Inhaltsdaten und Änderung des Satzaufbaus von OSCI-Nachrichten, soweit dies für die Anpassung der OSCI-Nachrichten an die Anforderungen des Zielsystems erforderlich ist,
- Archivierung offener Geschäftsvorfälle in verschlüsselter Form,
- Zielgerichtete Weiterleitung der OSCI-Nachrichten an den Empfänger, wobei die Inhaltsdaten der OSCI-Nachricht verschlüsselt übertragen werden.

Der Bürger authentisiert sich gegenüber der bos-Plattform durch ein Challenge-Response-Verfahren. Der hierfür auf Seiten des Bürgers benötigte Schlüssel ist auf einer Chipkarte hinterlegt (ab 2002 auf der EC-Karte). Gegenüber der Chipkarte authentisiert sich der Bürger nochmals mittels PIN; diese ist nicht identisch mit der PIN, die bei der

Benutzung von Geldautomaten oder Electronic Cash eingegeben werden muss. Nach erfolgreicher Authentisierung wird ein Sitzungsschlüssel mit einer Länge von 128 Bit erzeugt, mit dem die übertragenen Daten verschlüsselt werden.

Die von bos übermittelten OSCI-Pakete werden von den jeweiligen Fachverfahren der Meldestelle (DEMOS) und der Kfz-Zulassungsstelle (FAZIT) nicht direkt weiterverarbeitet. Es ist daher datenverarbeitungs-technisch erforderlich, die Originaldatensätze dieser beiden Fachverfahren teilweise zu spiegeln und die beiden Datensätze regelmäßig zu synchronisieren.

Die angestrebte (Teil-)Spiegelung von Datensätzen verbleibt weiterhin in der Verantwortung der jeweils speichernden Stelle (Meldestelle bzw. Kfz-Zulassungsstelle). Auch die gespiegelten Datensätze werden beim ID Bremen im Auftrag verarbeitet.

Um Plausibilitäten am Original-Datensatz durchführen zu können, benötigt bos einzelfallbezogenen Zugriff auf die gespiegelten DEMOS- und FAZIT-Datenbestände. Dieser Online-Zugriff ist im Vergleich zu der sonstigen Tätigkeit von bos ebenfalls als Auftragsdatenverarbeitung anzusehen. Entsprechende Auftragsverhältnisse werden von bos eingegangen.

Elektronischer Laufzettel: Um in Streitfällen die Übermittlung signaturgesetzkonformer elektronischer Formulare nachweisen zu können, werden elektronische Laufzettel generiert, die über den Transport hinaus bei bos aufbewahrt werden sollen; ein weiteres Exemplar erhält der Empfänger. Auf den Laufzetteln werden u. a. die Absender- und Empängerschlüssel, das Absendedatum sowie im Falle von Zahlungen ein von der Landeshaushaltsstelle vergebenes Kassenzeichen gespeichert.

Die längerfristige Speicherung von Laufzetteln bei bos ist aus datenschutzrechtlicher Sicht nicht unproblematisch, da Nutzungsdaten gemäß § 6 Abs. 1 TDDSG nur erhoben und verarbeitet werden dürfen, um dem Nutzer die Inanspruchnahme des Teledienstes zu ermöglichen. Eine über den Transportzeitraum hinausgehende Speicherung von Laufzetteln ist daher nur dann zulässig, sofern der Laufzettel direkter Bestandteil des Teledienstes "*Übertragen von signaturgesetzkonformen Formularen*" ist.

Aus dieser Interpretation ergibt sich jedoch nicht die Befugnis, die elektronischen Laufzettel beliebig lange speichern zu dürfen, nur um im Falle von Rechtsstreitigkeiten den Transport eines elektronischen Formulars zweifelsfrei nachweisen zu können. Da gemäß § 6 Abs. 2 TDDSG Nutzungsdaten frühestmöglich, spätestens unmittelbar nach Ende der jeweiligen Nutzung zu löschen sind, käme eine Speicherung der Laufzettel nur solange in Betracht, wie der eigentliche Verwaltungsvorgang noch nicht abgeschlossen ist. Ich habe daher vorgeschlagen, die elektronischen Laufzettel zu löschen, sobald die Übertragung der elektronischen Formulare nicht mehr strittig ist und durch andere Belege seitens beider Kommunikationspartner indirekt bewiesen werden kann.

Pilotbetrieb ab September 2000: Seit September 2000 läuft der Pilotbetrieb mit Geschäftsvorfällen aus verschiedenen Lebenslagen. Da bei den Anwendern zur Zeit noch

keine Möglichkeit vorhanden ist, OSCI-Formulare zu erkennen, werden die Formulare zunächst auf der bos-Plattform entschlüsselt und in einem für den Anwender lesbaren Format weiterversendet. Solange die Inhaltsdaten nicht von bos gespeichert und lediglich umformatiert werden, bestehen gegen diese Vorgehensweise im Pilotbetrieb keine grundsätzlichen datenschutzrechtlichen Bedenken.

3.5. Windows 2000

Der Einsatz des Betriebssystems Windows 2000 ist im zurückliegenden Jahr in vielen Unternehmen weiter vorangeschritten; dies gilt auch für die bremische Verwaltung. Es haben zwei Workshops zu diesem Thema stattgefunden, an denen auch ein Beschäftigter meiner Dienststelle auf Einladung des Senators für Finanzen teilgenommen hat.

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

Unabhängig von der Datenschutzentscheidung, die mit einem solchen zentralen Verzeichnisdienst verbunden ist, sind mit dem Einsatz einer "Active Directory" auch ganz konkrete sicherheitstechnische Probleme verbunden, da sich der Geltungsbereich der Domänen (Arbeitsgebiete) auf wesentlich größere Organisationsbereiche als bisher erstreckt. Während beispielsweise in der bremischen Verwaltung bislang ca. 200 Domänen eingerichtet sind, würde sich dort bei Einsatz einer Active Directory die Anzahl der Domänen auf einige wenige beschränken. Anstelle der ehemaligen NT-Domänen würden sogenannte Organisationseinheiten (Org.Unit-OU) treten, zwischen denen – im Gegensatz zu einer NT-Lösung mit mehreren Domänen – permanent Vertrauensstellungen mit OU-übergreifendem Zugriff existieren. Die bisherigen NT-Barrieren auf Domänenebene müssen statt dessen durch eine strikte Vergabe der Zugriffsrechte auf OU-Ebene ersetzt werden. Dies kann in großen Unternehmen und Verwaltungen ein erhebliches administratives Risiko darstellen. Ein weiterer Nachteil von Active Directories besteht darin, dass Passwortrichtlinen nur verzeichnisübergreifend gelten und nicht in einzelnen Organisationseinheiten (OU), in denen besonders sensible Daten verarbeitet werden, besonders verschärft werden können. Darüber hinaus richtet Windows 2000 standardmäßig zwischen allen Domänen transitive (gegenseitige) Vertrauensstellungen ein. Traut also Domäne A der Domäne B und Domäne B der Domäne C, dann traut auch Domäne A der Domäne C.

Für das Administrieren (Vergabe von Rechten, Einrichten von Benutzerkonten) der Domänen gibt es, wie unter Windows NT, die Gruppe der Administratoren. Durch die Vertrauensstellungen der Domänen untereinander ergibt es sich aber nicht automatisch, dass ein Administrator einer Domäne Rechte auf allen anderen Domänen hat. Eine Ausnahme bilden hier die Administratoren der Stamm-Domäne (Root-Ebene), sie sind in

einer speziellen Gruppe, den Organisations-Admins. Die Organisations-Admins bekommen automatisch die Berechtigung, sich in allen Domänen der Gesamtstruktur mit unbeschränktem Zugriff anzumelden.

Da der Einsatz eines Active Directory aufgrund des internen Abstimmungsprozesses auch einen erheblichen personellen und technischen Aufwand bedeuten würde, wurde der Einsatz von Active Directories in der bremischen Verwaltung zunächst zurückgestellt. Vorab sollen Erfahrungen mit Active Directories aus anderen Städten auf Wirtschaftlichkeits- und Datenschutzaspekte genauer geprüft werden.

Trotz der Risiken, die mit Active Directories verbunden sind, ist der Einsatz von Windows 2000 als Server-Betriebssystem zu empfehlen, weil dieses Betriebssystem eine Reihe zusätzlicher Funktionen ausweist, die zur Sicherheit von Netzen beitragen können:

- Das Dateisystem EFS (Encryption File System) erlaubt den Benutzern, Daten oder ganze Verzeichnisse auf lokalen Datenträgern online zu verschlüsseln. Dies ist beispielsweise bei Verlust von Wechselplatten oder bei Diebstahl des Gerätes ein entscheidener Vorteil gegenüber Windows NT. Realisiert wird der Schutz mit Hilfe einer auf öffentlichen Zertifikaten basierenden Verschlüsselung unter Nutzung der CryptoAPI-Architektur von Windows 2000. Die Dateien werden mit einem schnellen symmetrischen Verschlüsselungsalgorithmus verschlüsselt, der einen nach dem Zufallsprinzip erzeugten Schlüssel zur Datenverschlüsselung (Files Encryption Key – FEK) verwendet. Da EFS eng mit dem Dateisystem NTFS verknüpft ist, ist die Verschlüsselung der Daten transparent, d. h. der berechtigte Benutzer kann die Daten im Klartext lesen. Die Daten liegen nur dann in verschlüsselter Form vor, wenn die Daten in ein externes Dateisystem kopiert oder von einem unberechtigten Benutzer aufgerufen werden.
- Windows 2000 ermöglicht nicht nur die Authentifzierung der Benutzer gegenüber einem Domänen Controller, sondern unterstützt auch umgekehrt Identitätsnachweise bestimmter Netzwerkdienste gegenüber dem Benutzer. Für beide Arten der Authentifzierung verwendet Windows 2000 das Sicherheitsprotokoll Kerberos, Version 5. Kerberos v5 setzt zum Verschlüsseln von Kennwörtern kryptografische Mechanismen ein; somit werden Kennwörter nicht als Klartext sondern verschlüsselt über Netzwerkleitungen gesendet.
- Um die Integrität, Authentifizierung und Vertraulichkeit von Netzwerkdaten zu gewährleisten unterstützt Windows 2000 das Internet Protocol Security (IPSec). IPSec gestattet die Verschlüsselung (Ende-zu-Ende-Verschlüsselung) der Datenübertragung auf der Netzwerkschicht und eignet sich zur Absicherung von Client-Server-Anwendungen bzw. zum Sichern von Server-Verbindungen. Zum Verschlüsseln der Paketdaten wird der DES-Algorithmus (Data Encryption Standard) oder der 3DES-Algorithmus (Dreifach-Data Encryption Standard) verwendet. Es handelt sich hier um

symmetrische Verschlüsselungsalgorithmen, die die Daten in Blöcken von 64 Bit (Bei 3DES wird jeder Block dreimal verarbeitet) verschlüsselt.

- Die Zertifikatsdienste von Windows 2000 ermöglichen den Aufbau einer Schlüssel-Infrastruktur (Publik Key Infrastructure – PKI), die dazu genutzt werden kann, bei Bedarf einen großen Kreis von Benutzern zu authentifizieren und diesen Benutzern verschlüsselte und signierte Daten zuzuschicken. Zertifikatbasierte Prozesse unter Windows 2000 verwenden X.509v3 als standardmäßiges Zertifikatsformat.
- Im Gegensatz zu Windows NT 4.0 ist der Terminal-Server integraler Bestandteil des Betriebssystems Windows 2000. Programme können per Terminal-Server zentral ausgeführt werden, so dass auf dem Client die Inhalte der Anwendung nur grafisch dargestellt werden. Da auf dem Client keine aktiven Programmkomponenten ausgeführt werden, reduziert sich nicht nur die Virengefahr. Auch die Gefährdung des internen Netzes durch Trojanische Pferde ist damit weitgehend ausgeschlossen. Der Einsatz eines Terminal-Servers eignet sich besonders für Arbeitsplätze, an denen sowohl auf sensible Daten als auch auf Internetdienste zugegriffen wird. Statt lokal über einen Browser auf Internetseiten oder elektronische Postfächer zuzugreifen, werden lediglich Bildschirminhalte mit einem Terminal-Server synchronisiert.

3.6. Veranstaltungs-Management-System der Landesvertretung Bremen

Im Berichtszeitraum hat die Landesvertretung Bremen in Berlin mich über den geplanten Einsatz eines Veranstaltungs-Management-Systems informiert. Meine aus dem vorgelegten Feinkonzept und Pflichtenheft abgeleiteten Empfehlungen zur Beschränkung der Zugriffsregelung auf den Zuständigkeitsbereich der Beschäftigten, die Vernichtung von erstellten Listen durch Aktenvernichter sowie die Festschreibung von Löschfristen wurden in vollem Umfang umgesetzt. Am Jahresende wurde das überarbeitete Konzept zugesandt.

4. Bürgerschaft - Die Arbeit des Datenschutzausschusses

4.1. Ergebnisse der Beratung des 22. Jahresberichts

Bericht und Antrag des Datenschutzausschusses vom 19. Februar 2001 zum 22. Jahresbericht des Landesbeauftragten für den Datenschutz vom 31. März 2000 (Drs. 15/266) und zur Stellungnahme des Senats vom 26. September 2000 (Drs. 15/472)

- **Bericht**

Die Bürgerschaft (Landtag) hat in ihrer Sitzung am 11. Mai 2000 den 22. Jahresbericht des Landesbeauftragten für den Datenschutz und in ihrer Sitzung am 11. Oktober 2000 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 beziehungsweise des Magistrats der Stadt Bremerhaven angehört. Die wesentlichen Beratungsergebnisse sind nachfolgend aufgeführt. Daraus ist u. a. ersichtlich, dass bei der Planung und Weiterentwicklung von DV-Verfahren datenschutzrechtliche Aspekte häufig vernachlässigt werden. Der Datenschutzausschuss fordert den Senat in diesem Zusammenhang auf, künftig die jeweiligen Datenschutzkonzepte zeitgleich mit der DV-Entwicklung zu erstellen.

Die Textziffern in den verwendeten Überschriften entsprechen denen des 22. Jahresberichts.

Elektronische Post in der bremischen Verwaltung (Tz. 3.4): Die elektronische Post gewinnt in der bremischen Verwaltung immer mehr an Bedeutung. Sämtliche Dienststellen verfügen über Sammelpostfächer und an fast einem Drittel der 12.000 Bildschirmarbeitsplätze sind individuelle Postfächer eingerichtet. Die Erprobungsphase ist praktisch abgeschlossen. Richtlinien für den dauerhaften Betrieb der elektronischen Post liegen bisher nicht vor.

Das Problem in datenschutzrechtlicher Hinsicht besteht zurzeit darin, dass de elektronische Post unverschlüsselt übertragen wird. Vor Aufnahme des Echtbetriebes sind Regelungen für alle Anschlussteilnehmer im bremischen Verwaltungsnetz auszuarbeiten, die den Datenschutz ausreichend berücksichtigen. Dabei erfordert die vertrauliche Übertragung von elektronischer Post den Aufbau einer Verschlüsselungsinfrastruktur, die unter anderem verträglich ist mit flexiblen Abwesenheits- und Vertretungsregelungen. Weiter ist bei den Regelungen zu berücksichtigen, dass private E-Mails in individuellen Postfächern der bremischen Verwaltung dem Fernmeldegeheimnis nach § 85 des Telekommunikationsgesetzes unterliegen.

Der Datenschutzausschuss geht davon aus, dass alsbald eine E-Mail-Richtlinie vorgelegt werden wird, die eine Lösung der aufgezeigten Fragen beinhaltet.

Richtlinien zur Telefonüberwachung (Tz. 6.2.1): Bereits im 19. Jahresbericht (1997) hat der Landesbeauftragte für den Datenschutz als Ergebnis einer Prüfung der Telefonüberwachungsmaßnahmen durch die Polizei festgestellt, dass ein Erlass von 1971 und die Richtlinie von 1990 zur Überwachung des Fernmeldeverkehrs für Zwecke der Strafverfolgung aufgrund zwischenzeitlich eingetretener Veränderungen überholt sind. Ausgelöst durch die Einführung digitaler Übertragungstechniken in den Telefonnetzen, kam es auch bei der Polizei zu organisatorischen und technischen Veränderungen. Der Datenschutzbeauftragte hat aufgrund seiner Prüfergebnisse dem Senator für Inneres, Kultur und Sport empfohlen, den geänderten Bedingungen durch eine entsprechende Überarbeitung der Durchführungsbestimmungen zur Telefonüberwachung Rechnung zu tragen.

Wie bei der Beratung dieser Angelegenheit im Datenschutzausschuss bekannt geworden ist, ist ein die Telefonüberwachung regelnder Erlass im November 2000 in Kraft getreten. Hierbei handelt es sich jedoch lediglich um einen Rahmenerlass. Die Details der Telefonüberwachung sollen in Richtlinien geregelt werden, die der Senator für Inneres, Kultur und Sport zwischenzeitlich dem Landesbeauftragten für den Datenschutz zur Abstimmung zugeleitet hat.

Der Datenschutzausschuss geht davon aus, dass eine einvernehmliche und zufrieden stellende Lösung der datenschutzrelevanten Probleme bis zum 30. Juni 2001 gefunden wird.

Mängel bei der Übermittlung von Meldedaten an die Parteien vor der Bürgerschaftswahl (Tz. 6.3.2): Der Datenschutzausschuss ist mit dem Landesbeauftragten für den Datenschutz und dem Senat der Auffassung, dass die Bremerhavener Meldebehörde dadurch, dass sie die Daten aller Wahlberechtigten an eine Partei weitergegeben hat, gegen das Bremische Meldegesetz verstoßen hat.

Der Ausschuss begrüßt, dass der Senator für Inneres, Kultur und Sport der mehrfach erhobenen Forderung des Ausschusses, Vorkehrungen dahingehend zu treffen, dass Daten aus den Melderegistern nicht an Parteigliederungen außerhalb Bremens weitergegeben werden dürfen, durch das In-Kraft-Setzen eines entsprechenden Erlasses nachgekommen ist. Er hält es weiterhin für sachdienlich, dass die Empfänger bei der Übermittlung der Daten ausdrücklich auf die Zweckbindung und die Löschungs-verpflichtung hingewiesen werden.

Die Frage, ob die Weitergabe von Daten aus dem Melderegister künftig von der vorherigen Zustimmung der Betroffenen abhängig gemacht werden soll oder ob die so genannte Widerspruchslösung weiterhin vorzuziehen ist, hat den Ausschuss bereits anlässlich der Beratung des 21. Jahresberichts des Landesbeauftragten für den Datenschutz beschäftigt. Sie wird regelmäßig akut, wenn sich Bürger wegen der Übermittlung ihrer Meldedaten an politische Parteien und Wählergruppen im Zusammenhang mit Wahlen beschweren. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat einen Beschluss des Inhalts gefasst, dass das informationelle Selbstbestimmungsrecht der Betroffenen sich besser wahren ließe, wenn die Widerspruchslösung durch eine Einwilligungslösung ersetzt würde. Die Vertreterin der Fraktion Bündnis 90/Die Grünen im Datenschutzausschuss schließt sich dieser Auffassung an. Die den Fraktionen von SPD und CDU angehörenden Mitglieder im Ausschuss halten dagegen an der Widerspruchslösung fest. Auch sie verkennen nicht, dass bei der Einwilligungslösung ein Großteil der Beschwerden gar nicht erst auftreten würde. Die Koalitionsfraktionen sind gleichwohl mit dem Senat der Auffassung, dass das Informationsbedürfnis von Parteien und Wählergruppen so bedeutsam ist, dass demgegenüber Beschwerden von Bürgern über den Zugang von Informationsmaterial einzelner Parteien zu vernachlässigen sind. Deshalb wird die nach dem Bremischen Meldegesetz bestehende Möglichkeit, der Weitergabe von Daten zu widersprechen, als angemessen und ausreichend angesehen. Auch der Um-

stand, dass alle anderen Landesmeldegesetze die Widerspruchslösung enthalten, spricht dafür, die jetzige Regelung im Bremischen Meldegesetz beizubehalten.

Im Übrigen hat der Senator für Inneres, Kultur und Sport gegenüber dem Ausschuss erklärt, dass bei der aufgrund der anstehenden Novellierung des Meldegesetzes notwendig werdenden Neugestaltung der Formulare darauf geachtet werde, die Rubrik, die der Bürger im Falle eines Widerspruchs ankreuzen müsse, auffälliger zu gestalten, damit sie nicht übersehen werden könne.

Auslegung des Wählerverzeichnisses (Tz.6.4.2): Der Ausschuss begrüßt, dass der Senat der Forderung des Landesbeauftragten für den Datenschutz, Sperrvermerke bei der Erstellung des Wählerverzeichnisses zu berücksichtigen, durch die Änderung der Bremischen Landeswahlordnung vom 25. März 1999 nachgekommen ist. Danach dürfen Daten von Wahlberechtigten, die mit Sperrvermerken versehen sind, weil durch das Bekanntwerden der Daten zum Beispiel eine Gefahr für Leben, Gesundheit oder andere schutzwürdige Belange erwachsen kann, nicht mit dem Wählerverzeichnis öffentlich ausgelegt werden. Der Ausschuss erwartet durch die Novellierung des Bundeswahlrechts weitere Verbesserungen für den Datenschutz der Wähler.

Stand des elektronischen Einbürgerungsverfahrens (Tz. 6.6.2): Bei Einbürgerungsverfahren wird vom Senator für Inneres, Kultur und Sport ein elektronisches Dokumentations- und Vorgangsbearbeitungsverfahren eingesetzt, das unter anderem dazu dient, Standard-Vordrucke und Standard-Schreiben herzustellen und immer wiederkehrende persönliche Daten, wie zum Beispiel Namen und Anschrift, automatisch einzufügen. An einem Datenschutzkonzept fehlt es bisher.

Der Ausschuss geht davon aus, dass ein solches Konzept entsprechend der Erklärung des Vertreters des Innenressorts vor dem Ausschuss bis zum 31. März 2001 vorliegen wird.

DV-Entwicklung bei JUDIT (Tz. 7.1), DV-Entwicklung in der Justizvollzugsanstalt (Tz. 7.4), E-Mail-Server bei JUDIT (Tz. 7.5): Nach den Feststellungen des Landesbeauftragten für den Datenschutz werden im Bereich der Justiz-Dienstleistungen (JUDIT) insbesondere infolge der Einrichtung eines "JUDIT-Synergiezentrums" umfangreiche Änderungen bei der Vernetzung und beim Einsatz von Hardware und Software erforderlich. Ein Datenschutzkonzept gibt es bisher nicht. Dasselbe gilt für den E-Mail-Anschluss der Justizbehörden und für das Netz des Ärztlichen Dienstes in der Justizvollzugsanstalt.

Der Datenschutzausschuss erwartet, dass entsprechend der von dem Vertreter des Senators für Justiz und Verfassung vor dem Ausschuss abgegebenen Erklärung, Datenschutzkonzepte für alle drei Bereiche bis zum 31. März 2001 vorliegen werden.

Anforderung von Sozial- und Ausländerakten durch das Rechnungsprüfungsamt (Tz. 14.1.1): Das Rechnungsprüfungsamt der Stadt Bremerhaven forderte gezielt jeweils eine Akte der Ausländer- und der Sozialbehörde einer bestimmten Person an. Der Landesbeauftragten für den Datenschutz, der vom Magistrat zu diesem Vorgang um

Stellungnahme gebeten wurde, äußerte vor dem Hintergrund, dass bei den angeforderten Akten keine haushaltsrechtlichen Vorschriften zu prüfen waren, die Befürchtung, dass eine Nutzung der Daten außerhalb der Zuständigkeit des Rechnungsprüfungsamts nicht völlig ausgeschlossen werden könne.

Der Magistratsdirektor der Stadt Bremerhaven hat den Datenschutzausschuss darüber informiert, dass zurzeit geprüft werde, ob im Zusammenhang mit dem vom Landesbeauftragten für den Datenschutz geschilderten Vorgang möglicherweise Dienstpflichten verletzt worden sind. Er hat weiterhin erklärt, es werde gegenwärtig diskutiert, die Dienstanweisung für das Rechnungsprüfungsamt, die neben der Rechnungsprüfungsordnung Kompetenzen und Arbeitsweise des Rechnungsprüfungsamtes regele, inhaltlich zu verändern. In diesem Zusammenhang sei zu überlegen, ob auch das Recht des Rechnungsprüfungsamts, Akten anzufordern, präzisiert werden müsste, um möglichen Missbräuchen künftig entgegenzuwirken.

Der Datenschutzausschuss geht davon aus, dass er entsprechend der Ankündigung des Vertreters des Magistrats über den Fortgang in dieser Angelegenheit informiert wird.

- **Antrag**

Die Bürgerschaft (Landtag) möge beschließen:

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

4.2. Weitere Themen der Beratungen im Datenschutzausschuss

Darüber hinaus hat sich der Datenschutzausschuss mit folgenden Themen beschäftigt:

- Mamma-Screening-Projekt am ZKH St.-Jürgen-Straße
- Fly-Line
- Digitale Signatur
- Verbraucherbefragung durch die Lifestyle AG
- Videoüberwachung bei stationärer Pflege in Altersheimen und in Großwohnanlagen
- Novellierung des Landespolizeigesetzes
- Bremerhavener Verwaltungsnetz
- Bericht der Verwaltung über Möglichkeiten der Kontrolle missbräuchlicher Arzneimittelverrechnungen
- Problematik des Datenschutzes beim Projekt MEDIA@Komm
- Einrichtung einer Internet-Homepage des LfD
- Datensammlung der Telefonanbieter über die Kunden
- Entschlüsselung des menschlichen Genoms
- Nebentätigkeitsanzeigen im Weser-Kurier
- Hacker bei Microsoft
- Novellierung des Landesmeldegesetzes
- Virtuelles Datenschutzbüro (www.datenschutz.de)
- Konferenz der DSB - Kinderpornografie auf Internetseiten

Der Ausschuss, der gewöhnlich im Haus der Bürgerschaft öffentlich tagt, führte eine Sitzung in Bremerhaven durch. Er hat sich regelmäßig über den Stand der Besetzung der Stelle des Landesbeauftragten für den Datenschutz unterrichten lassen.

5. Personalwesen

5.1. Prüfung des Personalabrechnungsverfahrens KIDICAP 2000

Im 20. Jahresbericht habe ich unter Ziff. 11.5. über die Einführung eines neuen Bezügeabrechnungsverfahrens berichtet. Unter Ziff. 8.4. des 21. Jahresbericht habe ich darüber informiert, dass ein mit mir abgestimmtes Datenschutzkonzept vorliegt. Dies habe ich zum Anlass genommen, im Berichtszeitraum die Umsetzung der im Datenschutzkonzept genannten technischen und organisatorischen Maßnahmen zu überprüfen. Geprüft wurden die auf KIDICAP 2000 zugreifenden Organisationseinheiten, deren Aufgabenzuständigkeit und die daraus resultierenden Zugriffsberechtigungen. Des weiteren wurden die getroffenen technischen Maßnahmen (z. B. Zugang zu Hard- und Software, Protokolleinstellungen, Verschlüsselungs-Software für Clients mit offenen Diskettenlaufwerken, Virenschutz etc.) zum Datenschutz für Betriebssystem (Server und Client) sowie das Fachverfahren KIDICAP 2000 festgestellt und bewertet sowie die Umsetzung der mit Schreiben vom 15. März 2000 durch den Senator für Finanzen bekannt gegebenen und für verbindlich erklärten Richtlinie für Einzelplätze/ Server/ lokale Netzwerke - Aufbau, Installation und Sicherheitseinstellungen für Windows NT-Server/NT-Workstation - (NT-Security-Guideline) überprüft.

Bei der Prüfung habe ich u. a. festgestellt, dass derzeit noch keine Virenschutzsoftware auf dem Server implementiert ist. Zum Prüfzeitpunkt wurde an einem Konzept für den Einsatz von Virenschutzsoftware gearbeitet und der Einsatz nach Konzepterstellung vorgesehen. Die Protokolleinstellungen auf dem Server entsprachen nicht den im Datenschutzkonzept angegebenen. Da die technisch eingestellte Löschung von Protokolldaten, die älter als 180 Tage sind, wegen eines Softwarefehlers von Windows NT nicht umgesetzt werden kann, befanden sich noch alle Protokolldaten seit Einsatz des Servers (1998) im System. Ich habe angeregt, die Protokolldaten in regelmäßigen Abständen manuell zu löschen. Das Datenschutzkonzept sieht vor, die offenen Diskettenlaufwerke der Clients, auf denen personenbezogene Daten verarbeitet werden zu sperren oder eine Verschlüsselungs-Software bereitzustellen. Zum Prüfzeitpunkt fand eine Software-Evaluation für ein geeignetes kostengünstiges Produkt statt.

Das Datenschutzkonzept für das Fachverfahren KIDICAP 2000 ist in Bezug auf "Fehlerbereinigungen" und "Lesezugriffe der Abschnittsleitung" zu aktualisieren. Die Ziffer 4.5. des Datenschutzkonzeptes sieht vor, im Rahmen der Eingabekontrolle die Online-Dateneingaben in KIDICAP zu protokollieren. Während der Prüfung habe ich festgestellt, dass eine Sachbearbeiterin Zugriff auf die Protokolldaten der Erfassung von Beschäftigen ausserhalb ihres Aufgabenbereiches hatte. Die Erfassungsdaten beinhalten u. a. die

Sachbearbeiter-Nummer, Datum und Uhrzeit. Der überprüften Stelle war diese Zugriffsmöglichkeit nicht bekannt und sie sagte zu, hier die Zugriffsregelungen zu überarbeiten. Über die Löschung der zu Revisionszwecken gespeicherten Protokolldateien nach 5 Jahren konnte von Performa Nord keine Aussage getroffen werden, da die Protokolldaten bei der ID Bremen erhoben und verwaltet werden. In meinem Prüfbericht habe ich 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. Da die Maßnahmen Änderungen erfordert, die ausreichend getestet werden müssen, habe ich der Umsetzung bis Jahresende 2000 zugestimmt. Ich gehe davon aus, dass meine aus den Prüfergebnissen resultierenden Empfehlungen, die ich Performa Nord zugesandt habe umgesetzt werden und ich über die Durchführung informiert werde.

Im Rahmen der Prüfung wurde bekannt, dass andere Stellen einen Anschluss an das Verfahren KIDICAP erhalten haben und die Datenschutzmaßnahmen in deren örtlichen Datenschutzkonzepten beschrieben werden müssen. Ich habe die zuständigen Stellen angeschrieben und diese Konzepte angefordert. Einige Antworten stehen noch aus, andere Datenschutzkonzepte konnten bereits abgestimmt werden.

5.2. Übertragung der Beihilfe- und Kindergeldsachbearbeitung

Das Personalamt des Magistrats der Stadt Bremerhaven hat bei mir angefragt, welche Anforderungen bei der Übertragung der Beihilfe- und Kindergeldsachbearbeitung durch die Städtische Sparkasse Bremerhaven an das Personalamt des Magistrats zu beachten sind.

Ich habe dem Personalamt erklärt, dass es hierüber keine speziellen datenschutzrechtlichen Regelungen gibt. Die Sparkasse ist nach dem Sparkassengesetz für öffentlich-rechtliche Sparkassen im Lande Bremen eine rechtsfähige Anstalt des öffentlichen Rechts und unterliegt der Aufsicht des Senators für Finanzen. Sie ist insoweit wie das Personalamt öffentliche Stelle i. S. des § 1 Abs. 2 BrDSG. Es handelt sich also um eine Aufgabenübertragung von einer öffentlichen Stelle auf eine andere, für die die gleichen personalrechtlichen Vorschriften gelten.

Zur Sicherstellung der Auskunfts- und Einsichtsrechte der Beschäftigten der Sparkasse habe ich empfohlen, den Umfang der übertragenen Aufgaben einschließlich der Einhaltung der jeweils geltenden Datenschutzbestimmungen vertraglich festzulegen. Darüber hinaus sollte die Sparkasse ihre Beschäftigten ausdrücklich darüber informieren, dass ihre Kindergeld- und Beihilfeakten nunmehr beim Personalamt geführt werden und sie dort ihre Auskunfts- und Einsichtsrechte wahrnehmen können. Soweit die Kindergeld- und insbesondere die Beihilfeanträge über die Hauptstelle der Sparkasse an die zuständige Stelle des Magistrats weitergeleitet werden (z. B. Geburtsurkunden der Kinder, Zusammenstellung von Aufwendungen, Rechnungen, Rezepte, Heil- und Kostenpläne

usw.), sollen diese nur in einem verschlossenen Umschlag von der Hauptstelle der Sparkasse weitergeleitet werden.

5.3. Erstellung von Stunden- und Materialnachweisen

Ich bin darüber unterrichtet worden, dass die Hausverwalter und Haushandwerker der Studentenwohnheime des Studentenwerks Bremen tägliche Stunden- und Materialnachweise zu erstellen haben. Danach sind alle Tätigkeiten (Büroarbeiten, Telefonate, Reparaturen aller Art) zeitlich lückenlos zu benennen. Die Beschwerdeführer hielten diese Aufzeichnungen nicht für erforderlich und vermuteten, dass diese zu einer umfassenden und permanenten Leistungs- und Verhaltenskontrollen verwendet würden.

Das Studentenwerk hat auf meine Anfrage erklärt, die von den Beschäftigten zu erstellenden Stunden- und Materialnachweise dienten ausschließlich der Ermittlung und Feststellung von Ansprüchen gegenüber Mietern und ehemaligen Mietern und würden nur zu diesem Zweck geführt.

Eine Dokumentation war also nur für diese Zwecke erforderlich. Da jedoch nur bei bestimmten Schäden Regressansprüche entstehen, sind die Arbeitsanweisung und das zu verwendende Formular auf meine Anregung hin überarbeitet worden. Danach werden nur noch handwerklichen Tätigkeiten und deren Zeitaufwand aufgenommen.

5.4. Hinweis bei Anzeigepflichten Versorgungsberechtigter

Ein Versorgungsempfänger fragte mich, ob er der zuständigen Stelle (Performa Nord) zur Berechnung seiner Pension auch die Einkünfte seiner Frau mitteilen muss. Er berief sich auf den Hinweis in seinem Pensionsbescheid, wonach er verpflichtet sei, weitere Einkommensarten - auch des Ehegatten - mitzuteilen.

Performa Nord hat auf Anfrage dargelegt, Einkünfte des Ehegatten seien deshalb anzugeben, weil sie Änderungen des Familienzuschlages nach § 50 Abs. 1 Beamtenversorgungsgesetz bewirken können. Daraufhin habe ich vorgeschlagen, dieses in den Hinweisen aufzunehmen, was inzwischen erfolgt ist.

5.5. Besetzung einer Chefarztstelle im Krankenhaus

Im vergangenen Jahr wurde ich über Probleme bei der Besetzung einer Chefarztstelle im Bremerhavener Zentralkrankenhaus Reinkenheide informiert. Es wurde mitgeteilt, dass zu schützende persönliche Daten einer Bewerberin nicht nur an alle im Krankenhaus tätigen Chefärzte weitergegeben würden, sondern auch an die Öffentlichkeit gelangt seien. Die Mitteilung erfolgte vor dem Hintergrund, dass über das Verfahren und über die Bewerberin mit Angaben zu ihrer Person auch in Zeitungen und Fachzeitschriften berichtet worden war.

Die Überprüfung des Sachverhalts ergab, dass in dem Krankenhaus bei der Besetzung von Chefarztstellen bislang stets so verfahren worden war, dass die Chefarztkonferenz

des Krankenhauses, an der alle 16 Kliniken und Institute mit ihren ärztlichen Leitern beteiligt sind, am Stellenbesetzungsverfahren mitwirkten und ein Votum abgaben. Hierfür erhielten alle Chefärzte Kopien der vollständigen Bewerbungsunterlagen der einzelnen Bewerber, u. a. auch Zeugnisse und Lebensläufe.

Eine Rechtsgrundlage für die Mitwirkung der Chefärztekonferenz an Stellenbesetzungsverfahren gibt es nicht. Nach den Bestimmungen des Ortsgesetzes über den Betrieb des Zentralkrankenhauses Reinkenheide der Stadt Bremerhaven (Krankenhausbetriebsgesetz) trifft der Krankenhausausschuss der Bremerhavener Stadtverordnetenversammlung u. a. die Entscheidung über die Bestellung der leitenden Ärzte/Ärztinnen des Krankenhauses. Aus der Verfassung für die Stadt Bremerhaven ergibt sich, dass der Krankenhausausschuss zu seinen Beratungen Vertreter des Krankenhauses hinzuziehen kann. Aus datenschutzrechtlicher Sicht ist darüber hinaus zu beachten, dass auch in Verfahren zur Besetzung leitender Stellen die Verarbeitung personenbezogener Bewerberdaten auf das erforderliche Maß beschränkt bleiben muss. Gerade auch diese Anforderung dient der Vermeidung des missbräuchlichen Umgangs mit personenbezogenen Daten.

Ich kritisierte im vorliegenden Fall die Weiterleitung der Bewerbungsunterlagen an alle ärztlichen Leiter des Krankenhauses und forderte dieses für künftige Fälle auf, die Bekanntgabe von Bewerberdaten auf das erforderliche Maß zu beschränken. Das Krankenhaus teilt meine Auffassung, dass der Umfang der bisherigen Bekanntgabe unverhältnismäßig war. Es gelang schließlich in Abstimmung mit dem Krankenhausausschuss eine Verfahrensänderung, die vorsieht, dass zur Besetzung von Chefarztstellen künftig nur noch die Meinung einiger weniger ärztlicher Leiter des Krankenhauses, deren Beteiligung tatsächlich erforderlich ist, eingeholt wird und eine Abgabe von Kopien der Bewerbungsunterlagen an die Chefärzte nicht mehr erfolgt, weil die notwendigen Informationen durch Einsichtnahme gewonnen werden können.

5.6. Verschlüsselung von Datenträgern bei PuMa

Bereits 1997 (vgl. 19. JB, Ziff. 8.1.3.) habe ich über die fehlende Verschlüsselung für das Verfahren PuMa (Personalverwaltung und -management) und 1999 (vgl. 21. JB, Ziff. 8.2.) über die fehlende Verschlüsselungs-Software auf PuMa-Sachbearbeitungs-Clients mit offenen Diskettenlaufwerken berichtet. Zu Beginn des Berichtszeitraumes wurde dies Thema im Datenausschuss behandelt und es wurde eine akzeptable Lösung erzielt. Der Senator für Finanzen hat das Produkt PGP-Disk vorgeschlagen, das die Verschlüsselungsfunktionalitäten ermöglicht. Nach einem Test in meinem Hause habe ich dem Einsatz zugestimmt. Mit einer Freeware-Version des Produktes werden bereits die monatlich aktualisierten Daten für die Dienststellen verschlüsselt. Für die Installation auf den einzelnen Arbeitsplatzrechnern sind die Lizenzen bestellt und die Implementierung erfolgt derzeit.

6. Inneres

6.1. Polizeibereich

6.1.1. Prüfung des DNA-Analyseverfahrens

Zur Vorbereitung und Durchführung einer Prüfung habe ich drei Besuche bei beteiligten Dienststellen der Polizei Bremen durchgeführt. Ich habe die von der Polizei mir zur Verfügung gestellten Materialien in die Prüfung miteinbezogen und habe ergänzend Akten der Staatsanwaltschaft beigezogen, um einen Eindruck über das zwischengeschobene staatsanwaltschaftliche und gerichtliche Verfahren zu bekommen. Die Prüfung ist noch nicht abgeschlossen und bezog sich zunächst auf die Datenverarbeitung bei der Polizei, an dieser Stelle soll daher nur ein Zwischenbericht gegeben werden.

Zu den rechtlichen Voraussetzungen: Mit dem Strafverfahrensänderungsgesetz vom 17. März 1997 wurde erstmals die Untersuchung von molekulargenetischem Material für Zwecke der Strafverfolgung gesetzlich bestimmt (§ 81 e StPO). Voraussetzung für eine molekulargenetische Untersuchung ist eine richterliche Anordnung. Mit ihr muss auch die/der zu beauftragende Sachverständige bestimmt werden (§ 81 f StPO). Anfang 1998 wurde durch Errichtungsanordnung beim BKA eine Zentrale DNA-Analyse Datei eingerichtet. Am 07. September 1999 schließlich wurde mit dem DNA-Identitätsfeststellungsgesetz (DNA-IFG) die StPO um § 81 g ergänzt, um auch in zukünftigen Strafverfahren eine Identitätsfeststellung zu ermöglichen. Eine Erfassung kommt nach dieser Vorschrift in Fällen von Straftaten erheblicher Bedeutung, insbesondere eines Verbrechens, eines Vergehens gegen die sexuelle Selbstbestimmung, einer gefährlichen Körperverletzung oder einer Erpressung in Betracht. Mit der Bundesrats-Drs. 780/00 wird z. Zt. eine weitere Ergänzung der DNA Regelungen bei Spuren beabsichtigt.

Zu den DNA-Untersuchungsansätzen: DNA-Analysen werden von Spuren mit DNA-Material erstellt, bei denen der Täter noch nicht bekannt ist. DNA-Material wird außerdem bei aktuellen Kriminalfällen untersucht, bei denen ein Tatverdacht gegen eine bestimmte Person besteht. Schließlich werden DNA-Analysen in so genannten "Altfällen" vorgenommen. Hierbei handelt es sich um solche DNA-Analysen, die bei Verurteilten, die sich auch noch in Haft befinden können, vorgenommen werden. Bei ihnen werden die molekular-genetische Untersuchungen von Körperzellen zum Zwecke der Identitätsfeststellung in künftigen Strafverfahren vorgenommen.

Die Verfahrensschritte: Kriminalfälle, in denen eine DNA-Analysen in Frage kommt, können in verschiedenen polizeilichen Kommissariaten anfallen. Zunächst wird geprüft, ob bereits durch eine andere Polizeidienststelle eine DNA-Untersuchung für die Person beantragt oder durchgeführt worden ist. Dazu wird eine INPOL-Anfrage gemacht. Findet sich in INPOL bislang kein Eintrag, wird der Staatsanwaltschaft ein Antrag auf Erlass einer richterlichen Anordnung vorgeschlagen. Die Polizei verbindet ihren Vorschlag mit einer Kriminalprognose. Die Staatsanwaltschaft entscheidet u. a. nach Prüfung der poli-

zeilichen Prognosen die Antragstellung auf einen richterlichen Beschluss. Gibt der Richter dem Antrag statt, wird der richterlichen Beschluss (§ 81 f StPO) der beantragenden Polizeidienststelle mitgeteilt. Nach Erfassung in Kriminalaktennachweis (KAN) und in INPOL wird ein pseudonymisierter Untersuchungsantrag an die bezeichneten Sachverständigen, bzw. die Untersuchungsdienststelle bei der Polizei Bremen zusammen mit der DNA-Probe weitergeleitet. Der pseudonymisierte Persondatensatz besteht aus dem ersten Buchstaben des Nachnamen, dem Vornamen und dem vierstelligen Geburtsjahr. Jede Probe wird zweimal untersucht. Das Ergebnis der Labordaten (sog. Alelen) wird auf einem PC der Untersuchungsdienststelle gespeichert. Das Ergebnis wird weiterhin handschriftlich auf dem pseudonymisierte Antragsbogen vermerkt und an die einreichende Polizeidienststelle zurückgegeben. Der dortige Sachbearbeiter deanonymisiert den Meldebogen, indem er die personenbezogenen Daten ergänzt. Dieser Meldebogen wird nunmehr zur Erfassung der Alelen in INPOL weitergegeben. Die Alelen bestehen aus zwei mal fünf Ziffernpaaren. Dabei wird vor Übernahmen zunächst geprüft, ob in INPOL bereits ein identischer Datensatz gespeichert ist.

Zum Stand der Arbeiten: Insgesamt sind im Lande Bremen rund 10.000 Personendatensätze als sog. "Altfälle" zur retrograden Erfassung gem. § 81 g StPO daraufhin zu überprüfen, ob auf Grund der gesetzlichen Bestimmungen eine DNA-Analyse durchgeführt werden muss und eine Erfassung der Datensätze in INPOL zu erfolgen hat. Das BKA hat der Polizei bereits 1999 durch einen Abgleich der Haftdatei INPOL mit dem Bundeszentralregister (BZR) einen Datenbestand von ca. 2000 Personendatensätzen auf einer CD-ROM übermittelt. Die CD-ROM kann aber zur Zeit nicht bearbeitet werden, weil in der zuständigen Polizei-Dienststelle keine Datenbanklizenz für Access und auch keine Anwendungskenntnisse vorhanden sind. Auch die organisatorische Zuständigkeit für die Bearbeitung ist nicht geklärt. Bei der Staatsanwaltschaft Bremen sollen sich nach Auskunft der Polizei weitere (rund 8000) personenbezogenen Datensätze befinden, die die Staatsanwaltschaft selbst bearbeiten will und für die die Staatsanwaltschaft insoweit dann auch die Kriminalprognose selbst erstellen muss (Näheres, vgl. Protokoll der Fragestunde der Bürgerschaft am 13. September 2000, S. 1570 f.). Wieviele Altfälle insgesamt bereits bearbeitet wurden, ließ sich bei der Prüfung nicht feststellen. Nur der gesamte Bestand der nach DNA-Analyse erfassten Personendatensätze konnte ermittelt werden. Danach hat das Land Bremen bislang 319 Personendatensätze und 61 Spurendatensätze jeweils mit den zugehörigen DNA-Untersuchungsergebnis in INPOL eingestellt (Stand 24. Januar 2001). Eine erstaunlicher Langmut bei der Umsetzung der Regelungen, war doch der Druck auf den Gesetzgeber im Jahre 1996, DNA-Regelungen rasch zu erlassen so immens, dass kaum Zeit war, die datenschutzrechtlichen Implikationen ausreichend zu erörtern. Dass im Gesetzgebungsverfahren mit heißer Nadel gestrickt wurde, machen auch die mehrfachen gesetzlichen Nachbesserungen deutlich.

Bewertung einiger Punkte: Die polizeiliche Bearbeitungsweise war ausweislich der untersuchten Akten äußerst unterschiedlich. Dies gilt zum einen für die zum Teil recht gering ausfallenden, formularmäßig vorbereiteten Prognosebegründungen (" Wegen des

beigefügten BZR-Ausdruckes besteht der begründete Verdacht, dass gegen ihn/sie auch künftigen Strafverfahren von erheblicher Bedeutung zu führen sind"), zum anderen fand sich in zwei Fällen keine Prognose, sondern nur jeweils ein von der Polizei ausgefülltes und vom Betroffenen unterzeichnetes Formular "Belehrung und Einverständniserklärung". In der Hälfte der geprüften Akten wurde ein Formular mit Einwilligungserklärung verwandt. Das Formular enthält u. a. die Passagen: *"Darf die Polizei eine Speichelprobe nehmen und untersuchen? Ja, sie darf: Das DNA-Identitätsstellungsgesetz verpflichtet die Polizei dazu, bei Ihnen eine Speicherprobe zu nehmen und Sie zu untersuchen. Diese Maßnahme ist vergleichbar mit einer erkennungsdienstlichen Behandlung, bei der Sie fotografiert und Ihnen die Fingerabdrücke abgenommen werden."* Weiter unten in dem Formular ist eine Rubrik enthalten, in der die/der Betroffene einer Speichelprobe und/ oder der molekular-genetische Untersuchung ausdrücklich und aus freiem Willen zustimmt. Die Passagen lautet: *"Diese Belehrung habe ich verstanden. Ich stimme einer* ***O*** *Speichelprobe,* ***O*** *Molekulargenetische Untersuchung ausdrücklich aus freiem Willen zu (Zutreffendes ist anzukreuzen)."*

Für die Prognose ob ein Täter auch künftigen Straftaten begehen wird, sind alle verfügbaren Erkenntnisse beizuziehen und in jedem Einzelfall zu bewerten. Dies hat die Entscheidung des Bundesverfassungsgerichts zur DNA-Analyse (vgl. Beschluss vom 14. Dezember 2000 2 BvR 1741/99 u. a.) deutlich gemacht. Hier sind aufgrund meiner Feststellungen bei der bisherigen Prüfung Nachbesserungen bei allen Verfahrenbetreibern angezeigt. Auch die zitierte Passagen zur Zulässigkeit der Speichelprobe ist zu beanstanden, denn eine solche Aufklärung ist für den Betroffenen mindestens aus zwei Aspekten bedenklich. Zum einen wird hier über die Intensität des Eingriffs getäuscht, denn dass eine molekular genetische Analyse nicht mit den genannten Maßnahmen nach § 81 b StPO vergleichbar ist, zeigt schon der Richtervorbehalt bei der DNA-Analyse. Eine richterliche Entscheidung ist bei den weniger intensiven Maßnahmen wie Lichtbild und ED-Behandlung zum Zwecke des Erkennungsdienstes gerade nicht vorgesehen. Durch die Formulierungen wird somit beim Betroffenen eine falsche Vorstellung über die Qualität seiner Einwilligung erzeugt. Gerade zu grob falsch ist auch die oben zitierte Formulierung, wonach die Polizei verpflichtet sein soll, eine Speichelprobe zu nehmen und diese zu analysieren. Diese Äußerung könnte von der Polizei erst nach richterlicher Entscheidung getroffen werden. Sie beeinträchtigt vielmehr den Betroffenen in seiner Entscheidungsfreiheit, veranlasst ihn zu glauben, er willige in eine ohnehin unausweichliche polizeiliche Maßnahme ein. Schließlich ist in den geprüften Fällen retrograder Erfassung eine Einwilligung in die molekulargenetische Untersuchung entbehrlich und irreführend, weil sie nur bei vorliegen einer entsprechenden Prognose durch den Richter angeordnet werden kann. Zwar lag in allen geprüften Fällen vor Durchführung der DNA-Analyse eine richterliche Entscheidung vor, um aber Missverständnisse zu vermeiden, sollte auf sie ganz verzichtet werden. Das Formular ist daher insoweit umfassend zu überarbeiten.

In Bremen werden auch aktuell molekular-genetische Untersuchungen in vielen Fällen an die KTU (Kriminaltechnische Untersuchungsstelle) vergeben. § 81 f Abs. 2 StPO be-

stimmt, dass mit der Durchführung der Untersuchung nur solche Sachverständigen zu beauftragen sind, die der ermittlungsführenden Behörde nicht angehören oder einer Organisationseinheit angehören, die von der Ermittlung führenden Dienststelle organisatorisch und sachlich getrennt ist. Alle ermittlungsführenden Kommissariate und die KTU unterstehen der gleichen Polizeidirektion. Unter Zugrundelegung des materiellen Behördenbegriffs bestehen daher Bedenken, ob der genannten Vorschrift in ausreichenden Maße Rechnung getragen wird. Ich habe hierzu um Stellungnahme gebeten.

Die in § 81 f Abs. 2 S. 3 StPO gesetzlich angeordnete Anonymisierung des zu untersuchenden Materials soll dadurch erreicht werden, dass die Speichelproben zusammen mit einem Meldebogen an die KTU geben werden, aus dem die Identität der Betroffenen nicht ersichtlich ist. In der Praxis soll es schon vorgekommen sein, dass vollständig ausgefüllte Meldebogen bei der KTU eingegangen sind. Diese habe darauf nach eigenem Bekunden den Meldebogen mit Probe unbearbeitet an die einreichende Dienststelle zurückgegeben. Solche Fehler mögen bei dauerhafter Einübung nicht wieder auftreten, sind aber im Verfahren angelegt. Ich habe daher verfahrenstechnische Vorschläge zur Verbesserung und zur Vermeidung entsprechender Fehler gemacht.

Meinen Prüfberichte habe ich erst Anfang 2001 der Polizei Bremen zugeleitet. Eine Stellungnahme konnte daher nicht erwartet und auch nicht berücksichtigt werden.

6.1.2. Gen-Phantombild

Der Presse war zu entnehmen, dass sich das Bundeskriminalamt für ein neuentwickeltes Verfahren der DNA-Analyse interessiere, das genetische Merkmale von ethnischen Bevölkerungsgruppen herausfiltern kann. Da ich davon ausgehe, dass die DNA-Analyse lediglich im nichtkodierenden Bereich für Zwecke der Strafverfolgung zum Einsatz kommen soll, hatte ich Zweifel ob dieser Ansatz bei den fraglichen Verfahren noch gewährleistet sei. Ich bat daher den BfD um Aufklärung. Dieser wandte sich an das BKA und berichtete, dass das BKA mitgeteilt habe, die Anzahl entsprechender Studien sei derzeit noch zu gering, um die Wertigkeit für den Ermittlungsbereich definieren zu können.

6.1.3. Videoüberwachung

Die technische Entwicklung im Bereich der Videoüberwachung und -aufzeichnung macht so rasante Fortschritte, wie es kaum vorstellbar ist. Dabei denken die meisten Bürger bei dem Begriff "Videoüberwachung" an die Technik, die Ihre private Videokamera zur Aufzeichnung familiärer Ereignisse mitbringt. Moderne Videokameras mit hochauflösender Optik, verbunden mit Computern und Datenübertragungsnetzen sind mit nichten hiermit vergleichbar. Die Videoüberwachung wird für die unterschiedlichsten Zwecke und Aufgabenfelder verwendet. Dementsprechend vielfältig und groß sind auch die sich daraus ergebenden Gefahren und Risiken für das Recht auf informationelle Selbstbestimmung.

Ein weitgehend technisch unbeobachteter Aufenthalt in der Öffentlichkeit muss erhalten bleiben. Deshalb ist eine intensive Videoüberwachung der Öffentlichkeit, wie es einige

Gemeinden in England praktizieren, abzulehnen. Videoüberwachung darf nicht flächendeckend und allgegenwärtig eingesetzt werden. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch videotechnisch gewonnener Daten .

Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen. Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen. Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

Auch die einschlägige Rechtsprechung sieht die Videoüberwachung grundsätzlich als einen Eingriff in das von Art 2 GG verfassungsrechtlich geschützte allgemeine Persönlichkeitsrecht. Sie kommt zum Tragen, wenn auf den Bildern einzelne Personen zu erkennen sind oder die Bilder Rückschlüsse auf sachliche oder persönliche Verhältnisse natürlicher Personen erlauben (z. B. Kfz-Kennzeichen). Der staatliche Eingriff in dieses Recht bedarf daher in jedem Fall einer gesetzlichen Grundlage. Dies gilt auch, wenn eine Videoüberwachung ohne Aufzeichnung erfolgt. Die Betroffenen können nämlich regelmäßig nicht erkennen, ob es sich um eine Videoüberwachung mit oder ohne Aufzeichnung handelt. Die Rechtsprechung geht bei dieser Lage davon aus, dass die Betroffenen in ihrem natürlichen Verhalten beeinträchtigt werden und sich wie bei einer Videospeicherung verhalten.

Die Datenschutzbeauftragten des Bundes und der Länder sahen sich angesichts der massiven politischen Diskussion über die Einführung der Videoüberwachung im öffentlichen Raum für polizeilichen Zwecke genötigt, an diese Grundsätze zu erinnern. Dabei entwickelt sich eine Debatte gelegentlich so, dass nicht mehr die Befürworter eines Eingriffs in Grundrechte den Beweis antreten müssen warum massive technikunterstützte Eingriffe in in Grundrechte erforderlich sind, sondern dass die Verteidiger von Grundrechten wie Bürgerrechtler und Datenschützer begründen müssen, worin die Gefahren der Videoüberwachung liegen könnten. Die Datenschutzbeauftragten des Bundes und der Länder haben ihre kritische Position zur Einführung der Videoüberwachung in einem Beschluss (vgl. Ziff. 17.1. in diesem Bericht) bekräftigt. Darüber hinaus wurde im November 2000 eine Konferenz zu den Grenzen und Risiken der Videoüberwachung in Schwerin durchgeführt. Die Ergebnisse hat der dortige Landesbeauftragte für den Datenschutz in einer Broschüre zusammengefasst.

6.1.4. Einsatzverwaltungs- und Lagebilddatei der Polizei Bremen

Durch einen Hinweis habe ich von dem geplanten Einsatz einer Einsatzverwaltungs- und Lagebilddatei (ELPOL) erfahren. Auf Nachfrage hat mich die Polizei über den geplanten Einsatz informiert, mir die als Excel'97-Anwendung eigenprogrammierte Software vorgeführt und mir die Errichtungsanordnung gem. § 36 Bremischen Polizeigesetz, Dienstanweisung sowie Programmbeschreibung zur Stellungnahme vorgelegt.

ELPOL soll das bisherige Tagebuch auf den Revieren ablösen und die Daten aller Vorgänge einer Wache enthalten. Der Einsatz von ELPOL ist bis zur flächendeckenden Einführung eines landesweiten Vorgangsbearbeitungssystems vorgesehen. Es werden u. a. folgende Datenfelder erfasst: Registriernummer, Dienstnummer und die Dienstgruppe des zuständigen Beamten, Angaben zu Tatort, -zeit und Daten für statistische Zwecke. Die komprimierten Daten jeder Wache werden täglich per Mail über CISCO-Router verschlüsselt an die zuständige Polizeiinspektion übermittelt und dort zusammengeführt.

Nach Durchsicht der übermittelten Konzepte habe ich neben einigen redaktionellen Änderungen meine Empfehlungen mitgeteilt. So sollte die nicht vorgesehene Teilauswertung der Registriernummer nicht nur organisatorisch sondern auch technisch unterbunden werden, um eine Auswertung nach Dienstnummer bzw. -gruppe nicht zu ermöglichen. Für Abfragen sollte ein Passwortschutz programmtechnisch umgesetzt werden. Eine verbindliche Festlegung von möglichen Auswertungen und der dazu berechtigten Personen sowie die Definition von Löschfristen sollen in das Konzept aufgenommen werden.

Bezüglich der möglichen Auswertungen hat die Polizei erklärt, in nächster Zeit einen abschließenden Katalog zu erarbeiten und ein Verfahren für anlassbezogene Auswertungen vorzuschlagen. Da die Aufbewahrung der Daten 5 Jahre beträgt, das Programm aber nur für einen Zeitraum von ca. 23 Jahren als Zwischenlösung eingesetzt werden soll, sind keine Löschfristen definiert worden, da nicht abzusehen ist, ob der derzeitige Datenbestand in das Vorgangsbearbeitungssystem übernommen werden kann. Für das dann vorgesehene Vorgangsbearbeitungssystem soll ein automatisiertes Löschverfahren umgesetzt werden. Ansonsten sind meine Anregungen umgesetzt und in die entsprechenden Unterlagen eingearbeitet worden.

6.1.5. Zugriffsprotokollierung bei der Polizei

Im Jahr 1998 (vgl. 20. JB, Ziff. 12.4.) habe ich über das Ergebnis einer Überprüfung der Speicherungspraxis für die Protokolldaten des Verfahrens ISA-D (Informationssystem Anzeigen Dezentral) berichtet. Auf der Festplatte waren alle seit Einsatz des Verfahrens erhobenen Protokolldaten im Jahre 1993 gespeichert. Inzwischen sind alle Protokolldaten, die älter als 6 Monate sind auf der Festplatte gelöscht. Die Einhaltung der Löschfrist von 6 Monaten wird durch den Einsatz einer automatisierten Routine sichergestellt.

Die Daten der letzten zwei Jahre werden auf Magnetbändern gesichert und nach Ablauf der Aufbewahrungsfrist durch Überspielen des Bandes gelöscht.

Problematisiert wurde damals die Aufbewahrung der Sicherungsbänder im Zuständigkeitsbereich der DV. Ich habe angeregt, die Sicherungsbänder bei dem behördlichen Datenschutzbeauftragten auszulagern und so die Einhaltung des Vier-Augen-Prinzips zu gewährleisten. Die Polizei begründet die Lagerung der Sicherungsbänder im DV-Bereich damit, das im Falle eines Datenverlustes schnell auf den gesicherten Datenbestand zugegriffen werden kann. Die Einhaltung des Vier-Augen-Prinzips wird jetzt durch ein Antragsverfahren für die Auswertung des Datenbesstandes bei dem behördlichen Datenschutzbeauftragten gewährleistet. Über durchgeführte Auswertungen wird ein Nachweis für die Einhaltung der Vorgaben erbracht. Ich habe dieses Verfahren akzeptiert.

6.1.6. INPOL-neu, die weitere Entwicklung

Im Jahr 1999 (vgl. 21. JB, Ziff. 9.4.) habe ich die Umstrukturierung von INPOL-neu und die daraus resultierenden Auswirkungen auf die polizeiliche Informationsverarbeitung im Lande Bremen dargelegt. Den Sachstand der Entwicklung habe ich letztes Jahr (vgl. 22. JB, Ziff. 6.2.2.) fortgeschrieben und über den Diskussionsstand zum Thema Auftragsdatenverarbeitung durch das BKA und die noch nicht erfolgte Stellungnahme des Bundesbeauftragten für den Datenschutz berichtet.

Im Berichtszeitraum habe ich mich zweimal über die Entwicklung und Umsetzung von INPOL-neu und über die Evaluation eines polizeilichen Vorgangsbearbeitungssystems informiert.

Geplant ist jetzt eine auf vier Jahre begrenzte Landesdatenhaltung beim BKA. Das bedeutet, dass es beim BKA INPOL-neu Bund und INPOL-neu Land geben wird, wobei in INPOL-neu Land INPOL-relevante und sonstige Daten gespeichert werden sollen. Ob beim BKA eine strikte Trennung in zwei Datenbanken vorgesehen ist oder welche anderen technischen Lösungen angestrebt werden, ist noch nicht bekannt. Vorgesehen ist eine länderbezogene Abschottung der Daten, wobei über bilaterale Verträge die Einsicht in Daten anderer Länder möglich sein soll. Innerhalb dieser vier Jahre soll geprüft werden, ob eine Änderung des BKA-Gesetzes erfolgen soll.

Mitte des vergangenen Jahres wurde mir der Vertragsentwurf der "Rahmenvereinbarung über die Auftragsdatenverarbeitung der Länder beim BKA" ausgehändigt. Über den Rahmenvertrag und dessen Inhalte wird derzeit noch diskutiert. Die in diesem Zusammenhang stehende Auftragsdatenverarbeitung durch das BKA wurde vor der letzten Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Oktober 2000 durch eine Entschließung (vgl. Anlage, Ziff. 17.6.).

Ab 15. April 2001 startet der Parallelbetrieb für das "Manual ¾" (Personendateien werden auf das neue System überspielt und Abfragen werden an das neue System gerichtet). Das Ende des Parallelbetriebes ist für den 15. Oktober 2001 vorgesehen. Anschließend

werden die übrigen BKA-Dateien in einer harten Migration in das neue System übernommen (hier gibt es keinen Parallelbetrieb).

Die ganze Entwicklung steht unter ständigem Zeitdruck. Auch von den Datenschutzkollegen anderer Länder höre ich Klagen über die kurzen Anpassungsfristen. Es ist jedenfalls nicht auszuschließen, dass es in einzelnen Fällen frequentiell zu erheblichen Beeinträchtigungen der polizeilichen Arbeit kommen kann.

Auswirkungen in Bremen: Laut Aussage der Polizei Bremen definiert die Bundesarbeitsgruppe Einführung "INPOL-neu" Zeitvorgaben, die von Bremen nicht eingehalten werden können. Wenn für Bremen eine Minimallösung (zentrale Erfassung mit Qualitätssicherung) umgesetzt wird, sind Mehrfach- bzw. zusätzliche Eingaben erforderlich. Ein erhöhter Bearbeitungsaufwand bei einer zentralen Erfassung würde dadurch entstehen, dass die INPOL-neu-Dialoge Fallkenntnisse voraussetzen. Kurz vor Redaktionsschluss habe ich erfahren, das der Bremer Senat die Einführung von INPOL und die Anschaffung eines Vorgangsbearbeitungssystems beschlossen hat.

Die Datenstruktur von INPOL-Land enthält alle in ISA vorhandenen Datenfelder. In Bremen sollen die in INPOL-Land vorhandenen Daten redundant gehalten werden, um die Schnittstellen zur Staatsanwaltschaft und zum Einwohnermeldeverfahren zu erhalten. Alle bisherigen Einzeldateien sollen zentralisiert werden.

Die Software-Evaluation (vgl. 22. JB, Ziff. 6.2.3.) für ein neues polizeiliches Landesinformationssystem ist abgeschlossen. Für ein bereits in Mecklenburg-Vorpommern eingesetztes Produkt zur Vorgangsbearbeitung liegt eine Machbarkeitsstudie vor, eine Entscheidung über den Einsatz steht noch aus. Die Software ist bei der Polizei Bremen zu Testzwecken und zur Feststellung des Anpassungsbedarfes installiert.

Sowohl die Einführung von INPOL-neu wie auch die Einführung eines neuen Vorgangsbearbeitungssystem erfordern eine zeitnahe Schulung der Poliezeibeamten zum Einsatztermin, da die korrekte Dateneingabe und die adäquate Nutzung der Abfragen über die Qualität der in den Systemen gespeicherten Daten und die Gewährleistung des Datenschutzes entscheiden. Dies muss gewährleistet sein.

6.1.7. Schengener Informationssystem

Das Schengener Informationssystem (SIS) ist das gemeinsame Informationssystem der Staaten, die das Schengener Durchführungsabkommen (SDÜ) anwenden. Neben Deutschland haben Frankreich, Belgien, Holland, Luxemburg, Italien, Spanien, Portugal, Dänemark, Schweden, Finnland, Österreich und Griechenland ein Abkommen geschlossen um die Binnengrenzkontrollen abzuschaffen oder zumindest stark zu reduzieren, dafür aber die Kontrollen zu Drittstaaten zu verstärken. Damit alle Grenzkontrollstellen an den Außengrenzen ausreichend mit Informationen versorgt werden, ist das Schengener Informationssystem (SIS) eingerichtet worden. In das SIS werden Informationen zu Per-

sonen und Sachen eingestellt, auf das die übrigen Nationalstaaten in online-Zugriff haben.

Die personenbezogenen Daten, die in das System eingestellt werden sind Daten zu Personen, die

- zur Festnahme mit dem Ziel der Auslieferung ausgeschrieben sind,
- vermisst werden oder
- die zur verdeckten Fahndung (d. h. deren Grenzübertritt nur registriert wird) ausgeschrieben sind.

Ferner werden Sachen (Fahrzeuge, Waffen, Schriftstücke, Banknoten usw.) gespeichert, die gestohlen, unterschlagen oder sonst abhanden gekommen sind.

Mit der Einrichtung des SIS wurde gleichzeitig eine gemeinsame Kontrollinstanz für den Schutz personenbezogener Daten eingerichtet. Sie prüft die Anwendung des SDÜ und kontrolliert die technische Unterstützungseinheit (SIS). Jeder Staat entsendet zwei Vertreter. Deutschland wird durch den Bundesbeauftragten für den Datenschutz und den Hessischen Datenschutzbeauftragten vertreten.

Bürger - ganz gleich aus welchem Staat der Welt - haben aus dem SDÜ besondere Rechte. Dieses sind insbesondere:

- Recht auf Auskunft über die im SIS zu ihrer Person gespeicherten Daten,
- Recht auf Berichtigung unrichtiger Daten oder das Recht auf Löschung unrechtmäßig gespeicherter Daten,
- Recht auf Einleitung eines Verfahrens bei Gericht oder den zuständigen Stellen, um die Berichtigung oder Löschung der Informationen oder Schadensersatz zu erreichen und
- Recht auf Überprüfung der gespeicherten Daten und deren Nutzung.

Betroffene, deren Daten im SIS gespeichert sind, können sich an mich oder direkt an die obengenannten nationalen Datenschutzbehörden wenden. Die Überprüfung der Ausschreibung bzw. die Speicherung im SIS erfolgt auf der Grundlage des geltenden Rechts des Staates, der die Daten gespeichert hat. Die Kontrollinstanz wird über das Ergebnis der Überprüfung bzw. ob dem Antrag des Betroffenen stattgegeben wurde, unterrichtet.

6.1.8. Hilfeleistungsgesetz

Der Senator für Inneres hat mir im Spätsommer des Berichtsjahres den Entwurf eines Hilfeleistungsgesetzes übersandt. Hierzu habe ich eine Stellungnahme abgegeben. Dieses Gesetz soll das Brandschutzgesetz und das Rettungsdienstgesetz ablösen und Regelungen für den Katastrophenschutz treffen. Dabei sollen die Aufgaben- und Befugnissnormen neu gestaltet und einheitliche datenschutzrechtliche Vorschriften geschaffen werden. In den Gesetzen zum Brandschutz und dem Rettungsdienst waren bereits datenschutzrechtliche Vorschriften enthalten, die als Vorlage für das neue Gesetz

dienten, allerdings waren zum Teil Vereinheitlichungen und klare Zweckbegrenzungen zu treffen.

Ein besonderes Problem in diesem Zusammenhang stellte die Nutzung von Daten aus dem Bereich des Rettungsdienstes für ein neu einzuführendes Qualitätsmanagement dar. Denn einerseits sind Daten besonders zu schützen, die dem Arztgeheimnis unterliegen und anderseits ist es ein berechtigtes Interesse des Rettungsdienstes einen qualitativ hochwertigen und effektiven Rettungsdienst zum Wohle der Bürger zu unterhalten. Dieses Qualitätsmanagement wird nach diesem Entwurf in die Zuständigkeit und Verantwortung des "Ärztlichen Leiters Rettungsdienst" gestellt. Zur Erfüllung dieser Aufgabe ist er auch befugt, medizinische Daten von bremischen Krankenhäusern entgegenzunehmen und zu verarbeiten, die durch den bremischen Rettungsdienst betreut wurden. Nur auf diese Weise ist es möglich, festzustellen, ob die Rettungsmaßnahmen, die Ausbildung und die technische Ausstattung des Rettungsdienstes den hohen Anforderungen an einen Rettungsdienst gerecht werden.

6.1.9. Errichtungs- und Feststellungsanordnungen

Gem. § 36 BremPolG sind bei der Anlage personenbezogener Sammlungen durch die Polizei, Richtlinien darüber zu erlassen, unter welchen Voraussetzungen derartige Sammlungen eingerichtet werden dürfen. Die Errichtungs- oder Feststellungsanordnungen haben u. a. Regelungen zu enthalten über Rechtsgrundlage und Zweck der Sammlung, den aufzunehmenden Personenkreis, die Art und Übermittlung der zu speichernden Informationen sowie über die Dauer der Aufbewahrung. Im Berichtszeitraum habe ich wieder eine Reihe solcher Anordnungen erhalten und dazu Stellungnahmen abgegeben. An dieser Stelle sei beispielshaft die Errichtungsanordnung zur Einführung des Verfahrens MALATOK erwähnt. Diese vom BKA entwickelte Datenbankanwendung soll der Polizei ermöglichen die polizeilichen Erkenntnissen aus dem Bereich Menschenhandel strukturiert zu erfassen, um die verarbeiteten Daten einer Analyse zu unterziehen und mit diesen Erkenntnissen präventiv und repressiv tätigwerden zu können. Für die Abgabe einer Stellungnahmen ist es dabei in der Regel notwendig, im unmittelbaren Kontakt mit der Polizei die verfolgten Ziele und Auswertungsstrukturen zu erörtern, um zu einem datenschutzrechtlich korrekten Ergebnis zukommen.

6.2. Verfassungsschutzbereich

6.2.1. Entwurf eines neuen Bremischen Verfassungsschutzgesetzes

Der mir im Frühjahr vom Senator für Inneres übersandte Entwurf eines Gesetzes über den Verfassungsschutz im Lande Bremen enthielt insbesondere Regelungen zur Aufgabenerweiterung und zur Beschränkung der Bürgerrechte auf Auskunft und Akteneinsicht.

Ich habe in meiner Stellungnahme vom Juli 2000 davon abgeraten, den Verfassungsschutz mit der Bekämpfung von Gefahren zu betrauen, sondern es beim Schutz der freiheitlichen demokratischen Grundordnung und Schutz des Bestandes und der Sicherheit des Bundes und der Länder zu belassen. Daraus folgend sollte es bei der Aufgabe des Landesamtes für Verfassungsschutz (LfV) verbleiben, Nachrichten und Informationen zu sammeln und an die zuständigen Behörden zu übermitteln, damit diese dann rechtzeitige zur Gefahrenabwehr tätig werden können. Der Verfassungsschutz selbst sollte gerade nicht Gefahrenabwehr im Sinne von Gefahrenvereitelung wahrnehmen. Dem LfV stehen nämlich keine eigenen exekutiven Mittel zur Verfügung, um einer entdeckten akuten Gefahr präventiv entgegenwirken zu können. Ich habe in diesem Zusammenhang darauf aufmerksam gemacht, dass das LfV bisher nicht verpflichtet ist, Informationen über erkannte Gefahren oder Straftaten an die zuständigen Stellen weiterzugeben. Eine Änderung würde daher verschiedene auch datenschutzrechtliche Implikationen mit sich bringen. Auch bedürfe es bei der Zuweisung derselben Aufgabe an zwei Stellen einer festgelegten Sachleitungsbefugnis. All dies würde den datenschutzrechtlichen Prinzip der Funktionstrennung und der zweckgebundenen Erhebung von Daten zuwiderlaufen. Weiter habe ich daraufhingewiesen dass die im Gesetzentwurf vorgesehene Bildaufzeichnung in Wohnungen in Art. 13 GG keine Entsprechung findet. Auch bei den bewährten Regelungen der Auskunft im BrDSG sollte es bleiben. Ich habe den Eindruck, dass der Gesetzentwurf zur Zeit nicht weiterverfolgt wird.

6.2.2. Auskunft über Daten bei Sicherheitsbehörden

Bürger haben gemäß § 19 des BrDSG generell ein Auskunfts- und Akteneinsichtsrecht über ihre Daten, die von öffentlichen Stellen verarbeitet werden. Hiervon wurden aber Sicherheitsbehörden unter bestimmten Voraussetzungen ausgenommen. Zeitweilig bestand daher insbesondere beim Verfassungsschutz Unsicherheit, in welchem Umfang Auskünfte zu erteilen sind. In meinem 10. Jahresbericht (S. 10 unten) habe ich auf ein Urteil des OVG Bremen aus dem Jahre 1987 hingewiesen, das sich mit dem Auskunftsverweigerungsrecht der Sicherheitsbehörden aus § 19 BrDSG befasst. In dem zitierten Urteil hat das OVG Bremen entschieden, dass die Sicherheitsbehörden bei ihren Ablehnungen eine Abwägung zu treffen haben zwischen dem Geheimhaltungsinteresse der speichernden Stelle und dem evtl. vorliegenden besonderen Interesse des Auskunftsbegehrenden und die Entscheidung begründen müssen.

Mit seinem Beschluss vom 10. Oktober 2000 (1 BvR 586/90 und 1 BvR 673/90) hat das Bundesverfassungsgericht in zwei anderen Fällen die Abwägungs- und Begründungsverpflichtung und somit die in Bremen entwickelte Linie bestätigt.

Ich habe den Beschluss des Bundesverfassungsgerichts zum Anlass genommen, das Landesamt für Verfassungsschutz in Bremen auf das Urteil des Bundesverfassungsgerichts hinzuweisen. Das LfV hat mir mitgeteilt, dass es seit der OVG-Entscheidung so verfährt.

6.2.3. Fernmeldegeheimnis und Kontrolle

Das Bundesverfassungsgericht (ich berichtete im 22. JB, Ziff. 2.1.) hat mit seiner Entscheidung vom 14. Juli 1999 (BVerfGE 100, 313 ff.) im Bereich der vom Bundesnachrichtendienst durchgeführten strategischen Überwachung einige Bestimmungen des Gesetzes zu Artikel 10 Grundgesetz (G 10) beanstandet und dem Gesetzgeber zur Herstellung eines verfassungsmäßigen Zustandes eine Frist bis zum 30. Juni 2001 aufgegeben. Um diesen Beanstandungen Rechnung zu tragen hat die Bundesregierung einen Entwurf zum G 10 (BR-Drs. 54/01) vorgelegt, die Beratungen dazu haben die Datenschutzbeauftragten begleitet.

Kernpunkte der Forderungen der Datenschutzbeauftragten an dem neuen G 10 sind insbesondere:

- Keine Erweiterung des Katalogs der Überwachungsbefugnisse,
- eine konsequente Zweckbindung der erhobenen Daten, keine Datenübermittlung für andere Aufgabenfelder des Antragstellers und deren besondere Kennzeichnung als hochsensible Daten,
- eine generelle Benachrichtigung der Betroffenen nach Einstellung der G 10-Maßnahme,
- eine Regelung zur Gewährleistung einer wirksamen Kontrolle der nach G 10 erhobenen Daten durch die G 10-Kommission und den zuständigen Datenschutzbeauftragten und
- eine Evaluierung der G 10-Maßnahmen durch parlamentarische Kontrollorgane.

Für das Land bedeutsam ist eine Bestimmung im neuen G 10-Gesetz, nach der die Landesgesetzgeber die parlamentarische Kontrolle für die G 10-Maßnahmen in ihren Ländern, den Vorschriften des Bundes anpassen müssen. Danach ist eine wirksame Kontrolle zu installieren, die nicht nur die Entscheidung über die G 10-Anordnung hat, sondern auch die gesamte Datenerhebung, Verarbeitung und Nutzung der durch die G 10-Maßnahmen gewonnen Daten, einschließlich der Entscheidungen über die Mitteilung an Betroffene kontrolliert und begleitet. Gleiches gälte auch für die laufende Evaluierung des G 10-Instrumentariums. Ich bin gern bereit an der Ausgestaltung der Regelung mitzuwirken.

6.3. Meldewesen

6.3.1. Änderung des Melderechtsrahmengesetzes

Im Berichtszeitraum ist das Melderechtsrahmengesetz (MRRG) des Bundes mit Folgewirkung auch für Bremen geändert worden (2. Gesetz zur Änderung des MRRG vom 28. August 2000). Mit dieser Gesetzesänderung soll die Qualität der kommunalen Melderegister, d. h. ihre Richtigkeit und Vollständigkeit verbessert werden, indem z. B. erwei-

terte Ermittlungsbefugnisse der Meldebehörden und besondere Unterrichtungsverpflichtungen dritter Behörden eingeführt werden. Hintergrund dieser Novellierung ist die anstehende neue Volkszählung, die nicht mehr als statistische Primärerhebung bei allen Betroffenen, sondern als Sekundärstatistik aus vorhandenen Verwaltungsregistern wie z. B. dem Melderegister durchgeführt werden soll, mit stichprobenweisen primärstatistischen Ergänzungen d. h. Datenerhebungen bei Betroffenen (genauer, vgl. 22. JB, Ziff. 6.4.1.).

Derzeit wird in Bundesinnenministerium eine dritte Novelle zur Änderung des MRRG vorbereitet, erste Arbeitsentwürfe liegen vor. Ich bin in diese Diskussion derzeit noch nicht einbezogen. Nach meinem Kenntnisstand würden diese Änderungen sehr weitreichende Folgen für die der Meldepflicht unterliegenden Einwohner haben. So soll z. B. das Melderegister für online-Zugriffe durch jedermann (Internet) geöffnet werden, was die bisher auf Einzeleinwohner beschränkte einfache Melderegisterauskunft und die eingeschränkte Befugnis zur Datenübermittlung an Adressbuchverlage erheblich ausweiten würde. Wenn dies politisch so gewollt sein sollte, ist die Frage nach Sinn und Zweck des Melderegisters bei bußgeldbewehrter Meldepflicht neu zu stellen und damit auch die Frage, ob ein solcher Eingriff in das informationionelle Selbstbestimmungsrecht zur Befriedigung privater Interessen zulässig ist.

6.3.2. Änderung des Bremischen Meldegesetzes

Im Berichtsjahr wurde der von Bürgerschaft und Datenschutzausschuss wiederholt geforderte Entwurf eines Bremischen Meldegesetzes von der Innenbehörde vorgelegt. Ich habe dazu Stellung genommen. Mit dem Entwurf sind einige datenschutzrechtliche Verbesserungen des Melderechts verbunden. Einige meiner Anregungen sind übernommen worden, in einer Reihe von Punkten wurde meinen Vorschlägen nicht gefolgt. An dieser Stelle sollen einige Forderungen dargestellt werden:

Ich habe die Erweiterung der Datenspeicherung von bisher "Mitglied einer öffentlich-rechtlichen Religionsgesellschaft“ auf "die Zugehörigkeit zu jedweder Religionsgemeinschaft", in Frage gestellt. Nur bei öffentlich-rechtlichen Religionsgemeinschaften stellt dieses Datum ein steuerrelevantes Datum dar. In den übrigen Fällen ist nicht nachgewiesen, wofür dieses Merkmal eine melderechtliche Relevanz hat. Ich habe daher vorgeschlagen, es bei der alten einschränkenden Regelung zu belassen.

Der Senators für Inneres, Kultur und Sport lehnte diesen und eine Reihe anderer Vorschlägen mit der Begründung ab, man wolle nicht von den Vorgaben des Melderechtsrahmengesetzes (MRRG) abweichen, um möglichst eine einheitliche Regelung des Melderechts in den Ländern sicherzustellen. Dieses Argument der Einheitlichkeit nach dem Melderechtsrahmengesetz hätte das Innenressort dann aber auch in den Fällen gegen sich gelten lassen, in denen es mit seinen landesseitigen Regelungen von den Vorgaben des Melderechtsrahmengesetzes mit einem erweiterten Datensatz oder Meldeverfahren abweicht.

Das gilt z. B. für die vom Entwurf vorgeschlagenen Änderungen des Meldeverfahrens bei Mietverhältnissen. Die Regelungen (§ 3 Abs. 2 Nr. 6; § 14 und § 20 des Entwurfs) stellen partiell zwar eine datenschutzrechtliche Verbesserung des Verfahrens gegenüber dem bisher geltenden Recht dar, gleichwohl ist zu fragen, ob Mieter weniger vertrauenswürdig sind als Eigentümer einer Wohnung oder eines Hauses und daher einer Kontrolle durch den Vermieter und der Preisgabe ihrer Daten an den Vermieter unterworfen werden müssen. Einige Länder verzichten sogar vollständig auf eine Regelung zur Kontrollpflicht des Vermieters und beschränken die nach MRRG vorgesehene Mitwirkungspflicht auf die nach § 20 BremMG vorgesehene Auskunftspflicht des Vermieters.

Auch die Regelungen zur Hotelmeldepflicht (§ 26 Abs. 2 des Entwurfs) vermögen mich - auch wenn das Melderechtsrahmengesetz entsprechendes vorsieht - aus datenschutzrechtlicher Sicht nicht zu überzeugen. Einer privaten Stelle wird die Erhebung von Daten für öffentliche Aufgaben übertragen. Durch die vorgesehenen Regelungen wird der Hotelier quasi zur "Ersatzmeldestelle". Er wird per Gesetz verpflichtet, die Daten seiner Hotelgäste aufzunehmen und für ein Jahr aufzubewahren. Bei Ausländern muss er sich darüber hinaus den Ausweis zeigen lassen. Einmal davon abgesehen, dass ich diese Regelung unter dem Gesichtspunkt des EU-Rechts für fraglich halte, allenfalls können als sogenannte Kompensation für Schengen "die Nicht-EG-Bürger“ in diese Passvorlagepflicht genommen werden, überzeugt mich die vorgeschlagene Regelung auch aus anderen Gründen nicht. Ein melderechtlich relevanter Vorgang ist für die Meldebehörde mit der Hotelmeldepflicht nicht verbunden, sie erhält diese Daten nicht, sondern die Daten werden für die Kontrolle durch die Polizei vom Hotelgewerbe ein Jahr lang vorgehalten. Nach allem Anschein handelt es sich daher um eine Datenerhebung rein für polizeiliche Zwecke. Diese bedürfte deshalb keiner Regelung im Melderecht, sondern im Polizeigesetz insbesondere die Zweckbindung der Daten müsste bei den polizeirechtlichen Vorschriften geregelt werden.

Hinsichtlich der Regelungen zur Übermittlung von Meldedaten an politische Parteien (§ 33 Abs. 1 des Entwurfs) habe ich an die Entschließung der Konferenz der Datenschutzbeauftragten erinnert, die fordert, die Meldedaten an politische Parteien nur mit Einwilligung der Betroffenen zuzulassen. Es ist bekannt, dass sich die Bürger insbesondere über die Datenübermittlung an rechtsradikale Parteien im Vorfeld von Wahlen beschweren. In der Innendeputation ist erklärt worden, dass die zukünftigen Meldeformulare einen verbesserten Hinweis auf die Widerspruchsmöglichkeit enthalten sollen. Die Widerspruchslösung reicht bei vielen Jungwählern jedoch nicht aus, weil diese i. d. R. noch bei ihren Eltern wohnen und daher von der auf den Meldeformularen abgedruckten Widerspruchsregelung keine Kenntnis erlangen.

Die in § 17 Abs. 5 und 6 des Entwurfes vorgesehenen Möglichkeiten, im Rahmen des Anmeldungsverfahrens im elektronischen Wege Daten der Meldebehörde mitzuteilen, ist unter dem Gesichtspunkt der Bürgerfreundlichkeit und der Effizienz der Verwaltung zu

begrüßen. Anliegen des Datenschutzes dabei kann es nicht sein, diesen Weg mit Steinen zu pflastern, sondern möglichst einfach aber auch sicher zu gestalten.

Es ist noch nicht abschließend erkennbar, wie der Bundesgesetzgeber diese Materie im Melderechtsrahmengesetz festlegen wird. Solange der gesamte Komplex der elektronischen Anmeldung in allen seinen Facetten noch nicht abschließend durchdrungen ist (dies gilt nicht nur für die unmittelbare Beziehung Bürger-Meldebehörde, sondern auch für den gesamten Weg der Daten über Provider und Plattformen), habe ich empfohlen, nur die Regelungen ins Meldegesetz aufzunehmen, die datenschutzrechtliche Grundsätze regeln und absehbar Bestand haben werden. Hierzu zählt, dass die Daten auf dem Weg vom Bürger zur Meldebehörde und umgekehrt (gilt auch für die kostenfreie Bestätigung nach § 17 Abs. 6 BremMG-E) bei der Übertragung gegen unbefugte Kenntnisnahme nach dem jeweiligen technischen Stand hinreichend geschützt sind (Verschlüsselung), dass Identität und Authentizität der jeweiligen Kommunikationspartner zweifelsfrei bzw. signaturgesetzkonform ermittelt werden können (z. B. Chipkarten). Weiter steht außer Frage, dass durch hinreichende technische Vorkehrungen sichergestellt sein muss, dass das Melderegister vor missbräuchlichen Zugriffen, Manipulationen oder sonstigen Attacken aus Kommunikationsnetzen wie dem Internet geschützt sein muss (z. B. Firewall).

Ich habe empfohlen, diese Grundlinien in das Gesetz aufzunehmen. Detailfragen des Verfahrens hingegen, die sich je nach technischem Stand auch ändern können, können dagegen in einer Rechtsverordnung verankert und von mir dann in diesem Zusammenhang beraten werden. Soweit sich im weiteren Verlauf der Verfahren herausschälen sollte, dass weitere Festlegungen vom Gesetzgeber selbst aufgestellt werden müssen, kann dies aus meiner Sicht im Zuge einer späteren Novellierung nachgebessert werden. Der Entwurf entspricht in Bezug auf die elektronische Anmeldung diesen Vorschlägen in wesentlichen Punkten.

Nach Abschluss der Vorberatungen wurde mir Mitte Januar 2001 Gelegenheit gegeben, die offenen Punkte in der Innendeputation vorzutragen.

6.3.3. Änderung der Bremischen Meldedatenübermittlungsverordnung

Im Berichtsjahr erhielt ich mehrere Vorschläge zur Änderung der Bremischen Meldedatenübermittlungsverordnung (z. B. regelmäßige Übermittlungen an die Kataster- und Vermessungsverwaltung, die Amts- und Landgerichte, die Sozialverwaltung, Datenabgleiche des Bremischen Krebsregisters mit dem Melderegister) zur Stellungnahme. Ich habe zu allen Vorschlägen Stellung genommen. Ein Punkt, nämlich die regelmäßige Übermittlung von Meldedaten an die Sozialverwaltung/Sozialämter wurde seitens der Innendeputation im Berichtsjahr realisiert. Hierzu hatte es im Vorfeld der Beratungen der Innendeputation eine Abstimmung mit mir gegeben, dabei sind meine Vorschläge praktisch vollständig von der Fachbehörde aufgegriffen worden. Die Verordnung zur Ände-

rung der Bremischen Meldedatenübermittlungsverordnung wurde noch im Dezember im Gesetzblatt der Freien Hansestadt Bremen verkündet (BremGBl. S. 451 vom 19. Dezember 2000) und ist seit dem in Kraft.

6.3.4. Neues DV-Verfahren Meso 96 bei der Meldebehörde Bremerhaven

Im Berichtszeitraum hat die Meldebehörde Bremerhaven das neue DV-Verfahren Meso 96 (= Meldebehördensoftware), worüber ich im Vorjahr berichtet habe (22. JB, Ziff. 6.3.3.), in Betrieb genommen. Dieses Verfahren löst das frühere, technisch und organisatorisch veraltete Großrechnerverfahren für den Meldebereich ab. Das neue Windows-basierte Client-Server-Verfahren umfasst in seiner Funktionalität neben dem eigentlichen Meldewesen auch Komponenten für die Bereiche Pass- und Ausweiswesen, Wahl (Wählerverzeichnis) und Statistik.

Bei der Meldebehörde Bremerhaven habe ich im Berichtsjahr eine Datenschutzprüfung durchgeführt. Meine Prüfung bezog sich dabei nur auf einen Teil des Meso 96-Verfahrens und ist noch nicht abgeschlossen. Bei der Überprüfung der regelmäßigen Datenübermittlungen, Datenabrufe und Datenabgleiche musste ich z. T. erhebliche Abweichungen von den rechtlichen Vorgaben feststellen. Diese Abweichungen lagen z. B.

- in der Unklarheit oder gar völligen Unzulässigkeit der zugelassenen Datenübermittlungen (Datenkataloge),
- in der fehlenden Übersicht der an das Melderegister angeschlossenen Terminals/Rechner und berechtigten Mitarbeiter,
- in der unzulänglichen Protokollierung der Registeraktivitäten und dem Fehlen einer aktuellen Dokumentation des Verfahrens und
- in der Unvollständigkeit der mir mitgeteilten regelmäßigen Datenübermittlungen (unvollständige Übersicht),
- im fehlenden Datenschutz- und Datensicherungskonzept für das Subnetz Meldewesen.

Ich habe dem Magistrat der Stadt Bremerhaven das Ergebnis in einem Prüfbericht mitgeteilt und um Abhilfe gebeten. Daraufhin wurden seitens des Magistrats und seitens des Softwareherstellers Veränderungen am Meso 96 - Verfahren und an den DV-Programmen zugesagt. Anfang November fand ein weiteres Prüfgespräch beim Magistrat über den Stand der Anpassung und die offenen Punkte statt. Dabei zeigte sich, dass zwar einige Punkte erledigt wurden, andere aber noch offen sind.

Anfang dieses Jahres erhielt ich neben dem Anwenderhandbuch zum Meso 96 - Verfahren neue überarbeitete Informationen zu den regelmäßigen Datenübermittlungen, Datenabrufen und Datenabgleichen. Weitere Informationen wie z. B. eine Datensatz- und Datenbankbeschreibung zur Überprüfung der Datensätze, eine Übersicht der auf das Melderegister zugreifenden externen, nicht zur Meldebehörde gehörenden Terminals/Rechner. Details zur Wahl- und Statistikkomponente oder zum sog. APOL-Verfahren

der Polizei, mit dem u. a. auf das Melderegister zugegriffen werden kann, erhielt ich noch nicht. Diese Informationen sind mir allerdings zugesagt worden. Nach Durchsicht beabsichtige ich meine Prüfungen fortzusetzen.

6.4. Statistik

6.4.1. Volkszählung 2001

Die Vorbereitungen zu einer neuen Volkszählung (vgl. auch 22. JB, Ziff. 6.4.1.) wurden im Berichtszeitraum fortgesetzt. Geplant ist ein Methodenwechsel, bei dem anstelle einer direkten Befragung der Betroffenen vorhandene Verwaltungsdatenbestände wie z. B. die Melderegister und die Dateien der Bundesanstalt für Arbeit ausgewertet werden. Die mit dem Methodenwechsel verbundenen neuen Verfahren und Strukturen müssen vorbereitet und in Tests erprobt werden.

Die erforderliche Rechtsgrundlage soll durch das Gesetz zur Vorbereitung eines registergestützten Zensus (Zensusvorbereitungsgesetz) geschaffen werden, dessen Entwurf im Berichtsjahr erarbeitet und zwischen dem Bund und den Ländern abgestimmt wurde. Anfang dieses Jahres hat das Bundeskabinett den Gesetzentwurf beschlossen und das Gesetzgebungsverfahren eingeleitet.

Der Gesetzentwurf sieht Testerhebungen zur Prüfung der Qualität der Melderegister und der Dateien der Bundesanstalt für Arbeit sowie die Überprüfung statistischer Verfahren und Methoden vor. Er ordnet Testerhebungen auf Stichprobenbasis bei den Meldebehörden und der Bundesanstalt für Arbeit sowie eine Gebäude- und Wohnungsstichprobe in ausgewählten Gemeinden an. Daneben erfolgt eine Befragung von Personen, die in den für die Stichprobenerhebung ausgewählten Gebäuden wohnen, um die Qualität und Validität der Registerdaten und statistischen Verfahren zu überprüfen. Diese direkte Befragung ist nur für die Erprobungsphase vorgesehen, sie soll bei einem künftigen registergestützten Zensus entfallen.

Ich habe gegenüber dem Innensenator in meiner Stellungnahme zu dem Gesetzentwurf darauf hingewiesen, dass aus datenschutzrechtlicher Sicht der technisch-organisatorischen Sicherung der Abläufe und Datenflüsse sowie der konsequenten Beachtung des funktionellen Trennungsgebots zwischen amtlicher Statistik und Verwaltungsvollzug (Fachbehörden - Statistische Ämter/Erhebungsstellen) besondere Bedeutung zukommt. Daher verbieten sich z. B. Datenrückflüsse an die Fachbehörden zur Überprüfung der Richtigkeit von Angaben. Wie auch bei anderen amtlichen Statistiken müssen die erhobenen Daten in besonders abgeschotteten Bereichen der statistischen Ämter verarbeitet und zum frühestmöglichen Zeitpunkt anonymisiert bzw. gelöscht werden (statistische Geheimhaltungspflicht). Da Personen auch direkt befragt werden sollen, müssen diese und die Öffentlichkeit über die vorgesehene Erhebung frühzeitig und ausreichend aufgeklärt werden. Schließlich müssen auch bei einer Testerhebung der Umfang der zu erhebenden Daten und die Auskunftspflicht auf das erforderliche Maß beschränkt bleiben.

6.4.2. Versorgungsstatistik

Der Bundesminister des Innern beabsichtigt, für die Erstellung des 2. Versorgungsberichts der Bundesregierung Informationen über die Dienstunfähigkeit von Beamten zu erheben. Jeweils einzelfallbezogen sollen dem Bundesinnenministerium vom Bund und den Ländern in anonymer Form insbesondere Angaben über den Grund der Dienstunfähigkeit, die Reaktivierung, die begrenzte Dienstfähigkeit, die Höhe des Ruhegehaltssatzes sowie das Ruhen von Erwerbseinkommen mitgeteilt werden. Liegen ihr nicht alle erforderlichen Daten vor, so soll die für die Mitteilung an das Bundesinnenministerium zuständige Stelle Angaben zu Gründen einer Versetzung des Beamten in den Ruhestand auch bei anderen Stellen erheben können. Insbesondere sollen die fehlenden Daten von Stellen zur Verfügung gestellt werden, die mit der ärztlichen Begutachtung des Beamten beauftragt sind. Zuständige Stelle für die Mitteilung an den Bundesminister des Innern ist im Lande Bremen der Senator für Finanzen.

Die bundesweit geplante Datenerhebung vom Bundesminister des Innern sollte als Geschäftsstatistik durchgeführt werden. Diese Zuordnung entsprach nicht den damit verbundenen Gesetzesregelungen. Geschäftsstatistiken sind grundsätzlich bei der Stelle zu führen, bei der die für die Statistik benötigten Einzelangaben bei der Aufgabenerfüllung anfallen. Um eine Geschäftsstatistik handelt es sich daher nicht, wenn hierfür Einzelangaben bei einer anderen Stelle oder von dieser Stelle sogar noch bei einer anderen Einrichtung erhoben und an die statistikführende Stelle übermittelt werden. Die vorgesehene bundesweite Datenerhebung dagegen stellt eine Sekundärstatistik dar, für die es einer bundesgesetzlichen Grundlage bedarf. Ohne eine derartige Grundlage wäre die beabsichtigte Erhebung unzulässig. Meiner Bitte wegen der fehlenden Rechtsgrundlage das bereits begonnene Datenerhebungsverfahren auszusetzen, kam der Senator für Finanzen nicht nach.

Die Regierungsfraktionen des Deutschen Bundestages haben das geschilderte Problem erkannt und dann im Oktober des vergangenen Jahres in den Deutschen Bundestag den Entwurf eines Gesetzes zur Neuordnung der Versorgungsabschläge eingebracht, der auch eine Regelung über die Mitteilungspflicht für Datenerhebungen und -übermittlungen für den Versorgungsbericht enthält. Der Gesetzentwurf entspricht noch nicht in vollem Umfang datenschutzrechtlichen Anforderungen.

6.4.3. Hochbaustatistik

Die gebotene Trennung von amtlicher Statistik und Verwaltungsvollzug erwies sich auch im Hinblick auf die Umsetzung des novellierten Hochbaustatistikgesetzes als problematisch. Die Bestimmmungen des Gesetzes sehen für die verschiedenen Teilerhebungen der Hochbaustatistik Auskunftspflichten u. a. auch für die Bauherren vor. Verfahrensmäßig werden die Erhebungen in Bremen und Bremerhaven so durchgeführt, dass die Bauordnungsämter die Bauherren auffordern, den von ihnen einzureichenden Unterlagen die ausgefüllten statistischen Erhebungsbögen beizufügen. Obgleich die statistischen

Erhebungsbögen von den Baubehörden für die Beurteilung des Bauvorhabens und die Bearbeitung des Bauantrags nicht benötigt werden, sind die Bögen ein Teil der Erklärungen, die vom Bauherrn gegenüber der Bauverwaltung gemacht werden sollen. Die Bauordnungsämter erhalten also von Daten der Bauherren Kenntnis, die sie zur Erfüllung ihrer Aufgaben nicht benötigen.

Das Bauantragsverfahren ist in Bremen darüber hinaus auch ein Teil des MEDIA@Komm-Projekts. Im Rahmen der Lebenslage "Bau eines Hauses“ ist vorgesehen, dass der Bauherr den statistischen Erhebungsbogen dem zuständigen Bauordnungsamt übermittelt. Außerdem sollen die im Bauantrag und im Statistikbogen angegebenen statistischen Daten vor der Weiterleitung an das Statistische Landesamt gemeinsam in einem automatisierten Verfahren aufbereitet werden.

Ich machte den Senator für Bau und Umwelt zum bestehenden und zum geplanten automatisierten Verfahren darauf aufmerksam, dass der Bauherr nach den Bestimmungen des Hochbaustatistikgesetzes gegenüber dem Statistischen Landesamt und nicht gegenüber den Bauordnungsämtern auskunftspflichtig ist. Beide Verfahren bedürfen einer raschen Veränderung. Für den Bauherren muss deutlich werden, dass er die gewünschten statistischen Angaben auch direkt gegenüber dem Statistischen Landesamt machen kann. Im Bauantragsformular sollte ausdrücklich darauf hingewiesen werden, dass es dem Bauherrn freisteht, ob er den ausgefüllten statistischen Erhebungsbogen dem Bauantrag beifügt oder direkt an das Statistische Landesamt sendet. Meine Rechtsauffassung zur Auslegung der Gesetzesbestimmungen wird auch von anderen Landesdatenschutzbeauftragten geteilt. Eine Antwort seitens des Senators für Bau und Umwelt, ob er zu den notwendigen Verfahrensänderungen bereit ist, steht trotz mehrfacher Anschreiben noch aus.

6.5. Änderung des Wahlrechts

Der Bundesgesetzgeber hat einen Entwurf zur Änderung des Bundeswahlgesetzes (BT.Drs. 14/3764) vorgelegt, der ein bereits seit Jahren erkanntes datenschutzrechtliches Problem beseitigen soll. Dieses Problem besteht darin, dass viele Wähler ihre Sicherheit und Anonymität beeinträchtigt sehen, weil andere Bürger wegen des bisherigen Einsichtsrecht in die Wählerverzeichnisse Kenntnis über persönliche Verhältnisse erlangen können.

Nach dem Gesetzesentwurf bleibt es zwar bei der Erstellung der Wählerverzeichnisse, aber Einsicht auf die Daten hat nur der betroffene Bürger selbst um festzustellen, ob er ordnungsgemäß eingetragen ist. Hätte er Bedenken gegen das Wahlrecht eines anderen Bürgers, so müsste er seine Bedenken gegenüber der auslegenden Behörde schriftlich oder zur Niederschrift äußern. Die Wahlbehörde bzw. die Wahlorgane hätten die Bedenken zu prüfen. Diese neue Regelung würde eine Reihe von Beschwerden von Bürgern aus Anlass der öffentlichen Auslegung der Wählerverzeichnisse vermeiden.

6.6. AsylCard

In den letzten Jahren (vgl. 17. JB, Ziff. 9.2.4. oder 22. JB, Ziff. 6.6.1.) habe ich über die AsylCard (Chipkarte für Asylbewerber) berichtet. An dieser Stelle soll nur kurz über den Fortgang des Projektes unterrichtet werden.

Nach den mir vorliegenden Informationen hat die Bund-Länder-Arbeitsgruppe einen Stufenplan des Bundesinnenministers diskutiert. In der Arbeitsgruppe sind der Bund und die Länder Baden-Württemberg, Brandenburg, Bayern, Mecklenburg-Vorpommern, Niedersachsen und Nordrhein-Westfalen vertreten und wollen einen Pilotversuch zur Einführung der AsylCard starten.

In der ersten Stufe ist der Ersatz der Aufenthaltsgestattung als bundeseinheitliches Ausweisdokument (Ausweisfunktion) durch eine scheckkartenähnliche Plastikkarte mit hohem Sicherheitsstandard (analog EU-Führerschein) geplant. Alle auf der Karte aufgebrachten Daten sind auch visuell lesbar. Die zweite Stufe sieht zusätzlich das Aufbringen eines Mikroprozessorchips mit digitalisiertem Daumenabdruck, zur eindeutigen Identifizierung des Asylbewerbers vor. Diese bedarf jedoch - wenn nicht nur eine freiwillige Teilnahme vorgesehen wird - einer Änderung der entsprechenden Rechtsnormen.

Die Einführung der Stufen 3 und 4 ist noch fraglich. Sie sehen zusätzlich die Errichtung eines Hintergrundsystems vor, in dem alle Daten der Verwaltungsvorgänge und der AsylCard in einem sog. Backsystem gehalten und ständig abgeglichen werden. Die Einrichtung eines solchen Hintergrundsystems bedarf einer umfassenden rechtlichen Absicherung. Hinzu kommen erhebliche finanzielle Aufwendungen für alle Beteiligten. Weiter ist die Implementierung sog. optionaler Funktionen für die Länder und Kommunen geplant.

Bremen nimmt nicht teil und wartet die Ergebnisse des Pilotversuchs ab.

6.7. Gewerbemeldedaten im Internet

Ein Adressbuchverlag beabsichtigt im Internet die Gewerbemeldedaten, die er gemäß § 14 Abs. 8 Gewerbeordnung erhält im Internet zu veröffentlichen. Begründung für diese Veröffentlichung ist die Unterstützung einer gemeinnützigen Ausbildungsplatzsuchhilfe für Jugendliche, durch die eine schnelle Verknüpfung vom "Gewerbeadressbuch“ zum ausbildungswilligen Betrieb hergestellt werden könnte. Die Veröffentlichung der Gewerbemeldedaten im Internet stellt jedoch im Verhältnis zur Veröffentlichung im Gewerbeadressbuch in gedruckter Form eine andere Qualität dar. Einerseits ist ein weltweiter Zugriff möglich und andererseits können diese Daten im Internet durch Verknüpfung, Vervielfältigung und Nichtpflege (keine Berichtigung oder Löschung) ein unkontrollierbares Eigenleben entfalten. Aus diesem Grund halte ich die geplante Veröffentlichung der Gewerbemeldedaten im Internet derzeit rechtlich für unzulässig.

Anders verhält es sich für den Fall, dass die betroffenen Gewerbetreibenden in die Veröffentlichung einwilligen. Deshalb habe ich vorgeschlagen, bei den Betrieben, die dem

Verlag bereits bekannt sind die Einwilligung direkt einzuholen. Für alle zukünftigen Fälle habe ich vorgeschlagen, dass die Gewerbemeldestelle bereits bei der Anmeldung eines Betriebes eine entsprechende Einwilligung einholt. Diese Einwilligung könnte allerdings auch widerrufen werden. Ich bin der Auffassung, dass die Mehrzahl der Gewerbetreibenden der Veröffentlichung nicht ablehnend gegenüber steht, allerdings sind genauso Fälle denkbar, in denen einer Veröffentlichung nicht zugestimmt wird.

6.8. Ermittlungsgruppe Schwarzarbeit

Aspekte der Arbeit der Ermittlungsgruppe Schwarzarbeit werden unter Ziff. 16.6. des Berichts behandelt.

6.9. Eingaben

Auch im vergangenen Jahr bin ich wieder einer Reihe von Bürgereingaben und Anfragen in allen hier genannten Bereichen, insbesondere aber auch in Bezug auf die polizeiliche Datenverarbeitung nachgegangen. Dabei konnte ich den Bürgern teilweise bei ihrer Rechtswahrnehmung helfen indem ich zum Beispiel Löschungen in polizeilichen Informationssystemen erreicht habe. Ich konnte sie bei der Wahrnehmung ihrer Auskunftsrechte unterstützen oder aber auch Ihnen bestätigen, dass die von der Polizei erteilten Auskünfte und die festgesetzten Löschfristen den gesetzlichen Regelungen entsprechen.

7. Justiz

7.1. Postkontrolle im Insolvenzverfahren

Verzweifelt wandte sich eine Bürgerin an mich, die als Bürgin in die Zahlungsunfähigkeit geraten war und sich einem Insolvenzverfahrens unterzogen hatte. Im Rahmen eines Insolvenzverfahren wird ein Insolvenzverwalter oder Treuhänder bestellt, dem es in der Regel auch obliegt, alle an den Insolvenzschuldner gerichteten Schriftstücke zu öffnen und einzusehen.

Die Bürgerin beklagte sich nun darüber, dass alle an sie gerichtete Post, auch die Post z. B. von Gerichten und ihres Anwalts, wie auch ihre Telefonrechnung vom Treuhänder geöffnet und mit gelesen werde. Dieser setzte noch auf die Post den Stempel "Vom Treuhänder" und werfe die an sie gerichteten Briefe wieder in den Postbriefkasten ein. Dieses Verfahren führte zu verschiedenen Problemen und irritierte scheinbar die Postboten. Unter anderem sei die Post vom Büro des Treuhänders unverschlossen an die Beschwerdeführerin weitergeleitet worden. Auch zu anderen Unregelmäßigkeiten sei es gekommen. Am belastendsten empfand aber die Beschwerdeführerin, dass häufig an sie gerichtete Post an den Absender zurück gehe. Weil die Post sie nicht erreicht habe, sei es dadurch zu nichtbezahlten Rechnungen gekommen und infolgedessen zu weiteren Beeinträchtigungen, wie Mahngebühren, Kündigung einer Versicherungspolice oder Anschlusssperre des Telefonanschlusses. Durch die Rücksendung der Briefe mit der Stem-

pelung durch den Treuhänder wäre darüber hinaus aber auch den Absendern bekannt geworden, dass die Beschwerdeführerin einem Insolvenzverfahren unterliege.

Da der Treuhänder auch auf mehrfaches Bitten der Beschwerdeführerin hin sein Verfahren nicht ändern wollte, habe ich mich an das Amtsgericht gewendet, das den Treuhänder bestellt hatte und habe dieses um Unterstützung gebeten.

Das Amtsgericht ist der Sache nachgegangen und der Präsident des Amtsgerichts Bremen hat in seiner Stellungnahme mitgeteilt, dass er wegen der allgemeinen Bedeutung der Sache auch die übrigen Insolvenzverwalter und Treuhänder nach deren Handhabung der Postkontrolle befragt habe. Ihm sei dabei ausnahmslos bestätigt worden, das alle nicht die Insolvenzmasse betreffenden Sendungen nach erfolgter Einsicht unverzüglich in einem neuen Umschlag und neu frankiert an die Post zur Weiterleitung an den Empfänger herausgeben würden, wobei die Umschläge lediglich den Aufdruck "Vom Insolvenzverwalter" bzw. "Treuhänder" und gegebenenfalls vereinzelt noch "zustellen trotz Postsperre" tragen, um eine Beförderung und Aushändigung an den Empfänger überhaupt möglich zu machen. Ohne einen entsprechenden Aufdruck würden die Briefe wiederum zum Insolvenzverwalter bzw. Treuhänder zurücklaufen.

Der Präsident des Amtsgerichts Bremen hat zugesichert, dass er diese einheitliche Handhabung auch beim Treuhänder der Beschwerdeführerin sicherstellen werde. Der Beschwerdeführerin konnte somit geholfen werden, sie hat die geänderte Praxis mir gegenüber bestätigt.

7.2. Gerichtliche Bekanntmachungen und Register im Internet

Im Rahmen der Behandlung des obengenannten Falles wurde mir auch die Absicht bekannt, die Veröffentlichungen der Gerichte in Insolvenzverfahren künftig nicht mehr in den Printmedien sondern im Internet zu veranlassen. Ich habe auf die eindeutige Regelung in § 9 Insolvenzordnung (InsO) hingewiesen, nach der die öffentliche Bekanntmachung in dem für amtliche Bekanntmachungen des Gerichts bestimmten "Blatt" zu erfolgen hat. Eine Veröffentlichung im Internet würde darüber hinaus einen Eingriff in das informationelle Selbstbestimmungsrecht der Betroffenen darstellen, der weit über die bisher vorgesehene lokale Veröffentlichung hinausgeht.

Der Justizsenator, der meine Rechtsauffassung insoweit teilt, machte mich aber darauf aufmerksam, dass die Bundesregierung eine Änderung der Insolvenzordnung in die kritisierte Richtung beabsichtige. Danach sei vorgesehen, die Regelung der öffentlichen Bekanntmachung in § 9 InsO dahingehend zu erweitern, dass eine öffentliche Bekanntmachung auch in einem "für das Gericht bestimmtes elektronisch betriebenes Informationsverarbeitungssystem" (Internet) vorgenommen werden könne. Diese Überlegung wurde vor allem mit Kostengründen gerechtfertigt. Durch eine ausschließliche Internetveröffentlichung sollen vor allem Verbraucher entlastet werden, bei denen die Eröffnung eines Insolvenzverfahren nicht selten an den Bekanntmachungskosten scheitert.

Die Verfahrenskosten zu senken ist sicherlich wünschenswert, es ist jedoch zu bedenken, dass es wegen des unbeschränkten räumliche Nutzungsbereichs des Internet und wegen der gleichfalls unbegrenzten Möglichkeiten der Selektionen und elektronischen Zusammenstellungen der Daten aus dem Internet, die Informationen über den Schuldner im Ergebnis nicht zurückholbar preisgegeben werden. Dies könnte, insbesondere wegen der im Internet ständig wachsenden Anzahl an Auskunfteien und Wirtschaftsinformationsdiensten dazu führen, dass die Daten auch lange nach Abschluss eines Insolvenzverfahrens nicht rückholbar jederzeit im Internet verfügbar sind und so die mit der Insolvenzordnung bezweckte Chance der Schuldner auf einen wirtschaftlichen Neubeginn letztlich auf Dauer beeinträchtigt werden.

Gerade das Internet bietet neue Chancen und Möglichkeiten, die Informationen gezielt nur an die heranzutragen, die es angeht. Gerade hier sind neue Wege möglich, die mit herkömmlichen Medien nicht erreicht werden konnten. Es erscheint mir daher zu einfach, die Informationen im Internet in gleicher Weise abzubilden wie in der Zeitung, einer Gerichtstafel oder durch Aushang am schwarzen Brett. Es sollte daher geprüft werden, ob nicht der mit einer öffentlichen Bekanntmachung verfolgte Zweck auch mit einem Abrufverfahren erreicht werden kann. Auch ist nicht nachvollziehbar, warum der Insolvenzschuldner nicht wissen soll, wer sich für seine Daten interessierte. Auch hier könnte im Internet eine verfahrensseitige Verbesserung gegenüber einer Veröffentlichung in Printmedien erzielt werden. Ich hoffe, dass diese Überlegungen im Gesetzgebungsverfahren noch geprüft werden.

Auch bei den anderen von den Gerichten geführten Verzeichnissen, wie Handels-, Vereinsregister unter Schuldnerverzeichnis sind im Einzelnen Überlegungen anzustellen, welche neuen Möglichkeiten mit der Internetnutzung verbunden sind und auch hierdurch Verbesserungen für den Datenschutz der Betroffenen erreicht werden können.

7.3. Beratung von Justizvorschriften und Bürgereingaben

Im Berichtsjahr hat es wieder eine Reihe von Beratungen verschiedener Justizvorschriften gegeben, an dieser Stelle zu nennen sind z. B. MiStra, GBO, StPO, StrafVollzG. An den Diskussionen unter den Vertretern der Datenschutzbeauftragten habe ich mich beteiligt, soweit die Federführung zu einzelnen Vorschriften bei der Justizverwaltung einzelner Länder lag, habe ich auf eine Stellungnahme gegenüber dem Senator für Justiz und Verfassung verzichtet.

Bürgereingaben richteten sich auf Fragen der Datenverarbeitung durch die Gerichte, z. B. Bekanntgaben bei Zwangsversteigerungen oder die Speicherung von Daten im staatsanwaltschaftlichen Informationssystem. Alle Eingaben konnten zur Zufriedenheit der Betroffenen erledigt werden.

8. Gesundheit und Krankenversicherung

8.1. SAP-Prüfung in zwei Krankenhäusern

Im Herbst letzten Jahres habe ich den Einsatz des SAP-Moduls IS-H in Bremerhaven im Zentralkrankenhaus Reinkenheide (ZKR) und in Bremen im Zentralkrankenhaus Links der Weser (ZKH LdW) geprüft, vorab einige wesentliche Ergebnisse:

- Während im ZKR auch das Modul IS-H*MED (Industry Solution-Hospital) zur Dokumentation der ärztlichen Behandlung und der Pflege eingesetzt wird, beschränkt sich im ZKH LdW der Einsatz von IS-H bislang auf die Aufnahme von Patienten und auf die Abrechnung von Leistungen. Allerdings sollen im ZKH LdW gleichfalls in Kürze ärztliche Behandlung und Pflege mit Hilfe von IS-H*MED in digitalisierter Form gespeichert werden. Deshalb habe ich seine Leitung vorsorglich darauf hingewiesen, dass dann die unten unter Ziff. 8.1.1. für die Dokumentation im ZKR dargestellten Gesichtspunkte zu berücksichtigen seien.
- Im ZKR wies das SAP-Berechtigungskonzept den gravierenden Mangel auf, dass insgesamt 111 Nutzer, darunter interne und externe Nutzer vorwiegend aus dem nichtmedizinischen Bereich überwiegend ohne sachlichen Grund Vollzugriff auf alle gespeicherte Patientendaten hatten. Auf mein Betreiben hin schränkte das ZKR den Kreis auf 15 Nutzer ein, erklärte sich aber zu einer weiteren Reduzierung nicht bereit (Ziff. 8.1.1.).
- Im ZKH LdW war zwar die Zahl der SAP_ALL-Berechtigten mit 17 gleichfalls höher als aus meiner Sicht zu vertreten. Das ZKH LdW hat aber erklärt, die Zahl weiter zu reduzieren (Ziff. 8.1.2.).
- SAP stellt kein Archivierungssystem bereit, das eine den Vorgaben des Bremischen Krankenhausdatenschutzgesetzes (KHDSG) genügende Sperrung von Patientendaten nach Abschluss der Behandlung vorsieht - ein Defizit, das auch die Datenschutzbeauftragten anderer Länder konstatiert haben. Das ZKH Bremen-Nord hingegen will ein gesetzeskonformes Archivierungssystem einsetzen.

8.1.1. Zentralkrankenhaus Reinkenheide

Patientenverwaltungs- und -dokumentationssystem IS-H: Das Modul IS-H wird im ZKR in der Patientenverwaltung und -aufnahme, in der Notfallambulanz, im Zentrum Ambulantes Operieren, in der Radiologie, im OP-Bereich sowie auf 8 Stationen eingesetzt. Es dient nicht nur zur Abrechnung der Krankenhausleistungen, sondern mit Hilfe von IS-H*MED auch zur Dokumentation. Das ZKR ist bislang das einzige kommunale Krankenhaus im Lande Bremen, das IS-H auch für die Dokumentation von ärztlicher Behandlung und Pflege einsetzt.

Im ZKR haben Krankenhausärzte lesenden Zugriff auf alle in IS-H gespeicherten Daten von derzeitigen und früheren Patienten des ZKR und schreibenden Zugriff auf die medi-

zinischen Daten der Patienten, die in ihrer jeweiligen Fachabteilung behandelt werden. Pflegekräfte haben lesenden Zugriff auf alle Daten derzeitiger Patienten des ZKR und schreibenden Zugriff auf die Stammdaten aller Patienten.

Diese Zugriffsstruktur wird nicht den Regelungen gerecht, die das Bremische Krankenhausdatenschutzgesetz (KHDSG) für die Verarbeitung von Patientendaten in den Krankenhäusern im Lande Bremen getroffen hat:

- Nach § 3 Abs.2 KHDSG wird die abteilungsübergreifende Weitergabe bzw. der abteilungsübergreifende Abruf von Patientendaten als deren Übermittlung qualifiziert, die nur nach Maßgabe des § 4 Abs.1 KHDSG zulässig ist. Dies bedeutet, dass z. B. eine Übermittlung zur Durchführung einer Mit- oder Nachbehandlung zulässig ist, soweit die Übermittlung hierfür erforderlich ist und der Patient oder die Patientin nichts anderes bestimmt hat.

- Nach § 6 Abs.2 KHDSG sind Patientendaten in Krankenakten nach Abschluss der Behandlung zu sperren. Die Sperrung ist zu dokumentieren. Zur Erschließung der Akten ist ein Aktennachweis zu führen, zu dem kein direkter Zugriff anderer Bereiche besteht. Die Sperrung darf nur aufgehoben werden für die Durchführung einer Behandlung, mit der die frühere Behandlung in einem medizinischem Sachzusammenhang steht, zur Behebung einer Beweisnot, für eine nach § 4 Abs. 1 KHDSG zulässige Übermittlung oder wenn der Patient oder die Patientin eingewilligt hat. Die Aufhebung der Sperrung ist zu begründen. Diese Vorschriften gilt unmittelbar zwar nur für den Umgang mit in Krankenakten gespeicherten Patientendaten, nicht für den Umgang mit automatisiert gespeicherten Daten. Eindeutig aber ist der Wille des Gesetzgebers, Zugriffe auf durch andere Abteilungen erhobene Patientendaten und auf nach Abschluss der Behandlung archivierte Patientendaten zu erschweren.

Das KHDSG trat 1989 in Kraft - d. h. lange vor Beginn der digitalisierten Behandlungsdokumentation im Krankenhaus - und gilt seitdem in im wesentlichen unveränderter Fassung. Informationssysteme wie ISH*MED bieten im völligen Gegensatz zum Regelsystem des KHDSG von ihrer Logik her unbegrenzte Zugriffsmöglichkeiten. Bereits 1989 wollte der Gesetzgeber dem Grenzen setzen: Nach § 6 Abs. 3 KHDSG ist mit Abschluss der Behandlung die Möglichkeit des Direktabrufs von automatisiert gespeicherten Daten zu sperren. Diese Vorschrift ist direkt anwendbar, da nach § 3 Abs. 2 KHDSG Patientendaten von einer Fachabteilung zur anderen übermittelt werden und folglich der abteilungsübergreifende Zugriff ein Direktabruf i. S. des § 14 BrDSG ist.

Angesichts dieser Diskrepanz zwischen der Entscheidung des Gesetzgebers einerseits und informationstechnischer Entwicklung sowie Handlungszwängen im Krankenhaus andererseits habe ich - dem ZKR folgende Vorschläge zur Ausgestaltung der Zugriffsstruktur in ISH* MED unterbreitet:

- Wird der Patient während einer aktuellen Behandlung von einer anderen Fachabteilung mitbehandelt oder in eine andere Fachabteilung verlegt, so sollte Voraus-

setzung für den Zugriff durch den mit- oder nachbehandelnden Arzt sein, dass der erstbehandelnde Arzt die Daten freigibt. Akzeptabel könnte auch sein, dass die erstbehandelnde Fachabteilung die mit- oder nachbehandelnde Abteilung als solche "einträgt". Dies könnte die Freigabe der Daten im Einzelfall ersetzen.

- Wird ein Patient nach seiner Entlassung ein weiteres Mal im selben Krankenhaus, aber in einer anderen Fachabteilung behandelt, so sollte der aktuell behandelnde Arzt Zugriff auf den Stammdatensatz haben, aus dem erkennbar ist, ob und wann, der Patient früher schon im ZKR behandelt worden ist. Dann kann der behandelnde Arzt mit Einwilligung des Betroffenen die gesperrte Dokumentation der abgeschlossenen Behandlung einsehen. Ein eigenes Zugriffsrecht der Pflegekräfte auf die ärztliche Dokumentation abgeschlossener Behandlungen sollte i. d. R. ausgeschlossen sein.

Das ZKR hat mit der Begründung, man verfüge nicht über ein digitales Archivsystem, es abgelehnt, Patientendaten nach Abschluss der Behandlung zu sperren. Man plane derzeit auch nicht, ein solches System zu beschaffen. Dies kann ich nicht als sachliche Begründung bewerten, sondern lediglich als schlichte Weigerung, gesetzliche Anforderungen umzusetzen. Inwieweit im übrigen die Regelungen des § 6 Abs. 2 und 3 KHDSG unter den Bedingungen moderner DV-Technik anzupassen sind, ohne jedoch seinen Grundgedanken aufzugeben, dass auch krankenhausintern Patientendaten weder unbegrenzt noch unbefristet verfügbar sein dürfen, bleibt einer Prüfung durch den Senator für Gesundheit vorbehalten.

Systemadministration: Die Administration des SAP-Systems im ZKR - durchgeführt durch 3 Mitarbeiter der Abteilung Informatik - entsprach nicht den Anforderungen, die an eine ordnungsgemäße Datenverarbeitung gestellt werden. Es gab keine Trennung zwischen "Test- und Produktivmandant": Sämtliche Mitarbeiter, die Zugriff auf den Testmandant haben, besaßen auch Zugriffsrechte für das Produktivsystem. Es gab keinen Hauptverantwortlichen für das Basissystem einschließlich des Berechtigungskonzepts.

Ich habe gefordert, dass ein Berechtigungs-, Administrations- und Freigabekonzept erstellt und umgesetzt wird, das sich an folgenden organisatorischen Rahmenbedingungen orientiert:

- Es sollten getrennte Test- und Produktionsumgebungen eingerichtet werden. Der Transport von der Test- in die Produktivumgebung sollte durch entsprechende Transportaufträge erfolgen.
- Sog. ABAP/4-Programme sowie Rechteänderungen sollten nur auf schriftlichen Antrag der jeweiligen Fachverantwortlichen hin freigegeben werden.
- Benutzerstammdatensätze sollten durch einen Benutzeradministrator, Profile und Berechtigungen durch einen Berechtigungsadministrator verwaltet werden. Die Aufgabe des Aktivierungsadministrators kann von dem Benutzeradministrator in Personalunion übernommen werden.

- Die Fachmodule sollten von Moduladministratoren betreut werden, die keine privilegierten Zugriffsrechte für das Basissystem besitzen.

Das ZKR hat daraufhin im Oktober 2000 getrennte Test- und Produktionsumgebungen eingerichtet. Ein entsprechenden Freigabeverfahren befindet sich zur Zeit in Arbeit. Die beiden letztgenannten Forderungen konnten nach Aussage des ZKR aufgrund der personellen Lage der Informatikabteilung nicht umgesetzt werden.

Berechtigungskonzept: Zur Verwaltung des SAP-Berechtigungskonzepts wird im ZKR seit einiger Zeit der Profilgenerator eingesetzt. Hiermit wurden hauptsächlich die auf den Stationen benötigten Profile für das Pflegepersonal und die Ärzte erstellt, so dass sich dieser Teil des Berechtigungskonzepts als transparent darstellt. Darüber hinaus existierten jedoch noch weitere Profile, die ohne Profilgenerator erstellt wurden. Zahlreichen Personen (insgesamt 111 Benutzerkennungen, u. a. für das Lager, das Labor, die Wirtschaftsabteilung, die Radiologie, die Aufnahme sowie Kennungen für externe Unternehmensberater) waren jedoch zum Zeitpunkt der Prüfung nicht nur ihre für die Benutzung des jeweiligen Moduls benötigten Profile zugeordnet, sondern darüber hinaus auch das Profil SAP_ALL, das einem Generalschlüssel entspricht und zum schreibenden Zugriff auf sämtliche SAP-Daten einschließlich der medizinischen Daten berechtigt.

Derart viele Kennungen mit Superuser-Berechtigung stellen einen äußerst gravierenden Verstoß gegen § 2 Abs. 1 KHDSG, wonach Mitarbeiter des Krankenhauses nur soweit auf Patientendaten zugreifen dürfen, wie es für ihre jeweilige rechtmäßige Aufgabenerfüllung erforderlich ist, aber auch gegen § 3 Abs. 1, 2, § 4 Abs. 1 und § 6 Abs. 1 - 3 KHDSG dar. Nichtmedizinischen Abteilungen dürfen nur dann Zugriffsrechte auf medizinische Daten eingeräumt werden, wenn die besonderen Begrenzungen des § 3 Abs. 4 KHDSG Beachtung finden. Planungs-, Wirtschaftlichkeits- und Organisationuntersuchungen dürfen danach grundsätzlich nur mit anonymisierten Daten durchgeführt werden; eine Ausnahme bildet die gesetzliche Diagnosestatistik. Der Zugriff Externer auf Patientendaten ist allenfalls soweit im Einzelfall unbedingt erforderlich und nach Freigabe durch die EDV-Abteilung tolerierbar.

Darüber hinaus sind zahlreiche ZKR-Kennungen im Besitz des kritischen Profils SAP_NEW, das sämtliche zusätzlichen Berechtigungsobjekte enthält, die für Releasewechsel benötigt werden, um weiterhin die Anwendung problemlos ohne Einschränkung der Zugriffsrechte nutzen zu können.

Wegen der erheblichen Bedeutung des datenschutzrechtlichen Verstoßes habe ich das ZKR aufgefordert, den Kreis der SAP_ALL-Berechtigten unverzüglich auf das erforderliche Maß zu beschränken. Angesichts des Ausmaßes der festgestellten Mängel ist das gesamte Berechtigungskonzept einer vollständigen Revision zu unterziehen. Dies gilt insbesondere für diejenigen Profile, die noch nicht per Profilgenerator erstellt worden seien. Folgende Gestsltungsaspekte sind zu beachten:

- Es sollen möglichst keine redundanten Berechtigungen vergeben werden, d. h. Berechtigungen sollen sich nur auf ein Profil beziehen und nicht auf mehrere Profile. Die Vergabe nicht-redundanter Berechtigungen verbessert die Transparenz des Berechtigungskonzepts, da von einer Berechtigungsänderung nicht mehrere Profile zugleich betroffen sind.
- Es sollen möglichst keine Sammelprofile vergeben werden. Sammelprofile, die ihrerseits wiederum aus Sammelprofilen bestehen, sollen zu Gunsten der Transparenz auf jeden Fall vermieden werden.
- In der Produktionsumgebung sollen keine Standard-Profile zum Einsatz kommen.
- In der Produktionsumgebung solle vor allem das Standard-Profil SAP_NEW nicht zum Einsatz kommen. Die im Standard-Profil SAP_NEW enthaltenen Berechtigungen sollen in die bestehenden Profile integriert werden.
- Reports sollen in der Regel nicht mit Hilfe der Transaktion sa38 ausgeführt werden, sondern durch Aufruf eines Transaktionscodes. Berechtigungen zum Aufruf einzelner Transaktionen können über Programmberechtigungsgruppen definiert werden, die SAP jedoch standardmäßig nicht zur Verfügung stellt.

Das ZKR hat inzwischen erklärt, es habe die SAP-Berechtigungen auf dieser Grundlage überarbeitet. Redundante Berechtigungen oder Sammel- oder SAP-Standardprofile würden nicht mehr verwendet. Allerdings musste ich den Informationen des ZKR entnehmen, dass noch immer insgesamt 15 SAP_ALL-Berechtigungen vergeben sind. Auch diese Zahl ist entschieden zu hoch. Insbesondere ist es unzulässig, dass externe Berater/Wartungstechniker per SAP_ALL vollständigen Schreib- und Lesezugriff auf alle im System gespeicherten Patientendaten haben.

8.1.2. Krankenhaus Links der Weser

Patientenverwaltungs- und -dokumentationssystem IS-H: Bislang wird im ZKH LdW das Modul IS-H in der zentralen Aufnahme, die zugleich Abrechnungsabteilung ist und auf zahlreichen Stationen eingesetzt. Während in der zentralen Aufnahme-/ Abrechnungsabteilung der in § 301 SGB V für die Abrechnung mit den gesetzlichen Krankenkassen vorgegebene Datensatz, d. h. auch die Einweisungs- und die Entlassungsdiagnose gespeichert werden, werden auf den Stationen jeweils der Tag der Aufnahme, der Operation, der Entlassung und von Nachbehandlungen sowie die jeweilige Abteilung, dagegen keine Diagnosen gespeichert. Zugriff auf den Stations-PC hat das gesamte Stations-Personal.

Die im IS-H-Modul verarbeiteten Daten werden nach Abschluss der Behandlung bzw. nach erfolgter Abrechnung nicht archiviert und damit auch nicht gesperrt, sondern sind weiterhin wie vorher im Direktzugriff verfügbar. Dies verstößt gegen § 6 Abs. 3 KHDSG, wonach nach Abschluss der Behandlung der Direktzugriff zu sperren ist, soweit Patientendaten in automatisierten Verfahren mit der Möglichkeit des Direktabrufs gespeichert

werden. Ich habe daher gefordert, dass das für 2001 geplante digitalisierte Patientenarchiv die gesetzlichen Festlegungen berücksichtigt.

Administrationskonzept: Das SAP-System des ZKH LdW wird durch zwei Mitarbeiter der EDV-Abteilung administriert. Diese teilen sich die Zuständigkeit für die Module IS-H sowie FI, CO und MM (Finanz, Controlle, Materialwirtschaft) einerseits und für das Basissystem einschließlich des Berechtigungskonzepts andererseits. Sog. ABAP/4-Programme werden nur auf schriftlichen Antrag der jeweiligen Fachverantwortlichen entwickelt und freigegeben. Eine Trennung zwischen Test- und Produktivmandant erfolgt jedoch nicht. Ich habe daher das ZKH LdW aufgefordert, ein Berechtigungs- und Administrationskonzept zu erstellen und umzusetzen, das sich an den oben unter Ziff. 8.1.1. formulierten Rahmenbedingungen orientiert.

Das ZKH LdW hat inzwischen eine getrennte Test- und Produktionsumgebung mit entsprechenden Transportaufträgen eingerichtet. Benutzerstammdatensätze einerseits und Profile und Berechtigungen andererseits werden arbeitsteilig administriert. Die Aufgaben des Aktivierungsadministrators werden vom Berechtigungsadministrator in Personalunion wahrgenommen.

Berechtigungskonzept: Insgesamt existierten 17 Kennungen, denen das Profil SAP_ALL zugeordnet war. Neben den Mitarbeitern der EDV-Abteilung waren die Leiter der Finanzbuchhaltung und der Materialwirtschaft und externe Siemens- und SAP-Mitarbeiter mit privilegierten Zugriffsrechten ausgestattet. Darüber hinaus war 17 Kennungen die Berechtigung ISH-ALL zugewiesen, die den Zugriff auf sämtliche IS-H-Daten ermöglicht. Hierunter befinden sich sämtliche Mitarbeiter der Aufnahme- und Abrechnungsabteilung, der betriebliche Datenschutzbeauftragte und externe Berater/Wartungstechniker. 12 Kennungen waren im Besitz des Profils SAP_NEW.

Inzwischen hat sich das ZKH LdW bereit erklärt, die Anzahl der SAP-ALL-Berechtigten auf drei Personen zu reduzieren. Für regelmäßige Systemadministrationsaufgaben werden spezielle Profile eingerichtet. Externe Mitarbeiter sollen jedoch weiterhin im Einzelfall Zugriff auf Echtdaten erhalten; nach Beendigung der SAP-Einführung werden deren Kennungen gelöscht. Die Zugriffsrechte der Finanzbuchhaltung und Materialwirtschaft werden auf das erforderliche Maß beschränkt.

Auch wurde die Zahl der ISH_ALL-Berechtigten auf das erforderliche Maß eingeschränkt. Nach dem nächsten Releasewechsel werden die SAP_NEW-Berechtigungen - wie ich gefordert habe - in die bestehenden Profile integriert. Schließlich soll das Berechtigungskonzept einer regelmäßigen halbjährlichen Revision unterzogen werden, in deren Rahmen die oben unter Ziff. 8.8.1.3. aufgeführten Gestaltungsaspekte berücksichtigt werden.

8.2. Aufdeckung von Unregelmäßigkeiten bei der Abrechnung von Gesundheitsleistungen

Immer wieder wird über Ärzte, Apotheker und/oder Angehörige anderer Heilberufe berichtet, die bei den gesetzlichen Krankenkassen zu Unrecht Leistungen abrechnen. In diesem Zusammenhang wird auch der Vorwurf erhoben, die für Verhinderung, Aufdeckung und Verfolgung zuständigen Stellen wie die Krankenkassen selbst, die Kassen(zahn)ärztlichen Vereinigungen, die Heilberufskammern, die Apothekenaufsicht oder Polizei und Justiz gingen nicht energisch und effektiv genug vor. Dann wird häufig zu der Entschuldigung gegriffen, man wolle ja handeln, werde aber durch den Datenschutz an der Aufklärung gehindert. So geschah es im Berichtsjahr auch in Bremen.

Ich sah mich deshalb veranlasst, den für die Verhinderung bzw. Aufdeckung ungerechtfertigter Leistungsabrechnung zuständigen Stellen und dem Datenschutzausschuss der Bremischen Bürgerschaft zu erläutern, welche Befugnisse das geltende Recht zur Verarbeitung der Daten von Leistungserbringern und von Patienten in diesem Zusammenhang bereitstellt und welche nicht. Es gelang, in einem durch den Senator für Arbeit, Frauen, Gesundheit, Jugend und Soziales koordinierten Diskussionsprozess Konsens zwischen den Beteiligten herzustellen: Die Krankenkassen - und damit auch die von ihnen gemeinsam eingerichtete Pharmazeutische Beratungs- und Prüfstelle - dürfen Arzneimittelverordnungen zum Zweck der Prüfung ihrer Leistungspflicht auswerten. Bei Verdacht auf Unregelmäßigkeiten dürfen sie auch Polizei, Staatsanwaltschaft sowie Ärztekammer und Apothekerkammer einschalten und ihnen soweit erforderlich Sozialdaten übermitteln. Allerdings dürfen sie dies nur in eigener Entscheidung zur Erfüllung ihrer eigenen Aufgaben tun. Voraussetzung für die Übermittlungsbefugnis ist weiter, dass die Krankenkassen einen konkreten Verdacht hegen. Falls die Identität der einzelnen betroffenen Versicherten ohne Belang ist, dürfen die übermittelten Daten ihn nicht erkennen lassen. Die Überlassung ganzer Datenbestände zur freien Auswertung wäre unzulässig. Das Ergebnis der Beratungen zu diesem Punkt im Datenschutzausschuss wurde der Gesundheitsdeputation mitgeteilt.

8.3. Daten zur Abrechnung von Methadon-Substitution

Ärzte, die Drogenabhängigen als Ersatz (Substitution) für die Droge Methadon verabreichen, müssen deren Daten unabhängig vom normalen Abrechnungsverfahren für Arzneiverschreibungen der Kassenärztlichen Vereinigung (KV) und der Krankenkasse melden, bei der die Betreffenden versichert sind (meist die AOK). Dort waren auf diese Weise über die Jahre brisante Datensammlungen einer Randgruppe entstanden und dies ohne eindeutige gesetzliche Grundlage und ohne klare Zweckbestimmung oder Speicherungsdauer. 1995 (vgl. 17. JB, Ziff. 13.1.3.) wurde auf die vereinte Intervention der Datenschutzbeauftragten von Bund und Ländern hin durch die Spitzenverbände der gesetzlichen Krankenversicherung und die Kassenärztliche Bundesvereinigung die Verarbeitung der Daten Methadon-Substituierter präzisiert. Insbesondere waren die Daten-

kataloge dem jeweiligen Verarbeitungszweck angepasst worden. So sollten die Kassen nur noch die Daten erhalten, die erforderlich waren, damit sie Fälle von mehrfacher Substitution eines Patienten durch mehrere Ärzte feststellen konnten. Die KV Bremen teilte mir außerdem mit, nunmehr nach Beendigung der Substitution eines Patienten die ihn identifizierenden Daten unverzüglich löschen zu wollen.

Leider mußte ich festzustellen, dass die KV Bremen ihre Zusage, die Meldedaten nach Substitutionsende zu löschen, zu keinem Zeitpunkt eingelöst hat. Vielmehr hat sie seit Beginn der Methadon-Substitution kontinuierlich eine Art Register aller Substituierten im Lande Bremen aufgebaut. Eine Löschungsprozedur oder Speicherfrist wurde mir trotz mehrfacher Anfrage nicht genannt. Dies ist ein Verstoß gegen § 84 SGB X, der die Löschung von Sozialdaten verlangt, sobald sie für die gesetzlichen Aufgaben nicht mehr benötigt werden. Anders als die KV Bremen hat mir die AOK Bremen/ Bremerhaven mitgeteilt, sie lösche die automatisiert gespeicherten Meldedaten mit Ablauf eines Jahres, die Antragsvordrucke mit Ablauf von zwei Jahren nach Substitutionsende. Ich habe der KV vorgeschlagen, entsprechend zu verfahren.

Leider wurden auch die getroffenen Vereinbarungen von den Spitzenverbänden einseitig zurückgenommen. Der Bundesbeauftragte für den Datenschutz tritt dem entgegen, die Verhandlungen sind aber noch nicht abgeschlossen.

8.4. Bremisches Gesetz zur Änderung gesundheitsrechtlicher Vorschriften

Der Senat hat der Bremischen Bürgerschaft/Landtag am 09. Januar 2001 den Entwurf für ein Gesetz zur Änderung gesundheitsrechtlicher Vorschriften (Drs. 15/584) zugeleitet. Mit dem Entwurf strebt er für drei Landesgesetze Änderungen an, die z. T. von erheblicher datenschutzrechtlicher Relevanz sind:

8.4.1. Gesetz über den Öffentlichen Gesundheitsdienst

Es soll eine Rechtsgrundlage geschaffen werden für die Verarbeitung von Daten zum Zwecke von Maßnahmen der gesundheitlichen Prävention. Anlass gab das in diesem Bericht unter Ziff. 8.5. dargestellte Projekt zum Brustkrebs-Screening.

Die in 1999 zwischen Gesundheitsressort und Senatskommission für das Personalwesen abgeschlossene Vereinbarung über amtsärztliche Untersuchungen von Beamten im Zusammenhang mit ihrer Versetzung in den Ruhestand wegen Dienstunfähigkeit, gegen die ich Bedenken angemeldet hatte (vgl. 22. JB, Ziff. 5.2.), soll gleichfalls gesetzlich abgesichert werden. Anders als bislang in § 23 Abs. 4 ÖGDG (Gesetz über den öffentlichen Gesundheitsdienst) geregelt, sollte - so zunächst der Entwurf - der Amtsarzt dem öffentlichen Arbeitgeber neben dem Ergebnis der Untersuchung auch die wesentlichen Feststellungen, auf denen das Untersuchungsergebnis beruht, mitteilen. Es gelang mir, diese weitgehende Regelung auf das vom Beamtenrechtsrahmengesetz vorgegebene Ausmaß zu begrenzen. Die das Ergebnis tragenden Feststellungen sollen nunmehr nur im Ein-

zelfall auf Anforderung und nur soweit verhältnismäßig und erforderlich in einem gesonderten verschlossenen Umschlag übermittelt werden. Die übermittelten Daten unterliegen einer strengen Zweckbindung. Die zu untersuchende Person ist vor der Untersuchung auf deren Zweck und das Ausmaß der erlaubten Übermittlungen hinzuweisen.

8.4.2. Gesetz über das Leichenwesen

Im Gesetz über das Leichenwesen soll die Rechtsgrundlage dafür geschaffen werden, dass die von den Ärzten ausgestellten Todesbescheinigungen durch eine vom Gesundheitsressort beauftragte Stelle in einer als Bremer Mortalitätsindex bezeichneten Datenbank gespeichert und für Zwecke der Verwaltung und der Forschung vorgehalten werden.

8.4.3. Bremisches Krebsregistergesetz

Aus der Fülle der Änderungen, deren datenschutzgerechte Ausgestaltung ich im einzelnen mit dem Gesundheitsressort intensiv erörtert habe, will ich nur einige herausgreifen:

- Bei Widerspruch eines Patienten dagegen, dass sein Arzt seine Daten an das Register meldet, darf bislang zu statistischen Zwecken lediglich die Tatsache eines Widerspruchs gemeldet werden. Künftig sollen trotz des Widerspruchs außerdem auch die Identitätsdaten und die Diagnose gemeldet werden dürfen, dies aber nur zu dem Zweck, dass bereits vorhandene oder zukünftig eingehende Meldungen, etwa von Pathologen, denen der Widerspruch nicht bekannt war oder ist, gelöscht werden können. Die Identitätsdaten sollen in diesem Fall in irreversibel verschlüsselter Form gespeichert werden.

- Auf Empfehlung des Gesundheitsressorts akzeptiert es die Vertrauensstelle des Bremer Krebsregisters, wenn Kliniken ihre Meldungen nicht auf den Dokumentationsbögen abgeben, sondern statt dessen mit Einwilligung ihrer Patienten die für die nachbehandelnden Ärzte bestimmten Arztbriefe/ Entlassungsberichte einreichen. Ich hatte dies deshalb kritisiert, weil dadurch mehr als die gesetzlich vorgesehenen Daten übermittelt würden. Künftig soll die Praxis ausdrücklich erlaubt sein, immerhin soll – wofür ich mich eingesetzt habe - festgeschrieben werden, dass dieses Verfahren nur dann zulässig ist, wenn die meldende Stelle außerstande ist, die Dokumentationsbögen auszufüllen (etwa wegen Überlastung der Klinikärzte) und dass die Arztbriefe nur für die Erfassung des gesetzlichen Datensatzes genutzt und danach unverzüglich vernichtet werden müssen.

- Die Registerstelle, die darauf beschränkt ist, die bei ihr nicht personenbezogen gespeicherten medizinischen Daten im Rahmen ihrer gesetzlichen Aufgaben auszuwerten, soll künftig an epidemiologischer Forschung teilnehmen können. Ich habe erreicht, dass bei Beteiligung der Registerstelle Voraussetzung für die Herstellung des Personenbezugs das gesetzlich vorgeschriebene Verfahren beachtet wird, also zuvor die Vertrauensstelle über den jeweils behandelnden Arzt die Einwilligung des einzel-

nen betroffenen Patienten eingeholt haben muss. Außerdem soll die Registerstelle die ihr darauf hin durch die Vertrauensstelle übermittelten Identitätsdaten nur für das in der Genehmigung des Gesundheitsressorts bezeichnete Forschungsvorhaben verwenden. Auf diese Garantien habe ich Wert gelegt.

8.5. Bremer Projekt zum Brustkrebs-Screening

In der Stadtgemeinde Bremen sollen im Verlauf der Jahre 2001 und 2002 alle Frauen im Alter von 50 - 70 Jahren, dies sind etwa 70.000 Frauen, zu einer Mammographie-Untersuchung eingeladen werden. Im 22. Jahresbericht hatte ich unter Ziff. 8.2. die Grundzüge dieses Projekts dargestellt, für das Bremen neben den Regionen Wiesbaden-Rheingau-Taunus und Weser-Ems in einer bundesweiten Ausschreibung im September 1999 den Zuschlag erhalten hatte. Ich hatte danach kritisch angemerkt, dass noch keine der beteiligten Stellen zwecks Klärung datenschutzrechtlicher Fragen, geschweige denn mit dem Entwurf eines Datenschutzkonzepts an mich herangetreten war. Anfang September des Berichtsjahrs war es dann für den angekündigten Starttermin des Screening im Januar 2001 zu spät, zumal das Projekt zunehmend Gegenstand öffentlicher Auseinandersetzungen wurde und eine Fülle schwieriger und beispielhafter datenschutzrechtlicher Probleme aufwirft.

Im folgenden gebe ich eine knappe Zusammenfassung der wichtigsten datenschutzrechtlichen Aspekte des Projekts, der sich darauf beziehenden Erörterungen und deren derzeitige Ergebnisse. Die medizinischen und gesundheitspolitischen Argumente pro und contra, die öffentlich diskutiert werden, zu bewerten und zu kommentieren, ist nicht meine Aufgabe. Die öffentlichen Kontroverse um das Projekt, die große Zahl der betroffenen Frauen sowie Ausmaß und Dauer der geplanten Verarbeitung sensibler Gesundheitsdaten haben mich aber veranlasst, das Projekt besonders intensiv zu begleiten. In diesem Rahmen habe ich nicht nur das Projekt selbst, sondern auch den Datenschutzausschuss und den Ausschuss für die Gleichberechtigung der Frau, die ZGF, den Gesundheitssenator, das Gesundheitsamt Bremen und Abgeordnete beraten. Auch mit den Datenschutzbeauftragten der anderen beteiligten Länder habe ich mich abgestimmt.

Projektdesign, erste Fassung: freiwillige Reihenuntersuchung und langfristige Evaluation durch Vergleich der Lebenserwartung für Teilnehmerinnen und Nichtteilnehmerinnen: Das Projekt in der mir zunächst zur Bewertung vorgelegten Fassung bestand aus dem eigentlichen **Screening-Programm**, d. h. dem Angebot an alle 50 - 70jährigen Frauen in der Stadtgemeinde, sich freiwillig einer Mammographie zu unterziehen. Die hierfür benötigten Daten und weitere Daten auch aus dem Melderegister sollten zu einer langfristig angelegten **Evaluation** der Lebenserwartung der Teilnehmerinnen im Vergleich zur Lebenserwartung der am Projekt nicht teilnehmenden Frauen genutzt werden.

Für die Einladung zur Reihenuntersuchung sollte die Meldebehörde einer noch zu gründenden Einladungsstelle des Projekts Namen, Anschriften und andere Meldedaten der

Frauen übermitteln, die zur Altersgruppe der 50 - 70jährigen gehören. Diese Stelle sollte dann die Einladungen verschicken, d. h. den Adressatinnen einen Termin zur Reihenuntersuchung bei der eigentlichen Screening-Stelle vorschlagen. Die in der Screening-Stelle erhobenen medizinischen Daten, insbesondere die Mammographien, sollten dann zur weiteren Befundung und Auswertung an eine dem Zentralkrankenhaus Sankt-Jürgen-Str. angegliederte Stelle übermittelt werden.

Die Daten aller angeschriebenen Frauen, auch der Frauen, die die Einladung, obleich noch ein zweites Mal eingeladen, nicht wahrgenommen bzw. ausdrücklich ihrer Ablehnung Ausdruck gegeben hatten, sollten langfristig durch die Einladungsstelle weiter gespeichert werden.

Man dachte daran, bei den Frauen zugleich mit der schriftlichen Erklärung, zur Teilnahme an der Reihenuntersuchung, ihr Einverständnis in die weitere langfristige Speicherung und in die Auswertung sowohl ihrer Meldedaten als ihrer bei der Untersuchung erhobenen Gesundheitsdaten einzuholen. Mit der Erklärung verbunden wäre die Einwilligung insbesondere in Abgleiche dieser Daten mit Daten aus Krebsregistern, aus Melderegistern und aus Todesbescheinigungen (in Bremen künftig Mortalitätsindex). Die Meldedaten der Nichtteilnehmerinnen sollten langfristig gespeichert und gleichfalls für die genannten Abgleiche genutzt werden.

Datenschutzrechtliche Bedenken gegen das Projektdesign, erste Fassung: In einer ersten Stellungnahme habe ich erhebliche Bedenken gegen das Projekt vortragen und in wesentlichen Punkten Änderungen empfohlen. Wichtig war es dabei die Vermengung zwischen Daten, die für die Durchführung des Brustkrebs-Screenings benötigt werden und den Daten, die für die Begleitforschung erforderlich sind, aufzuheben und bei der datenschutzrechtlichen Beurteilung nach den verschiedenen Zwecken zu differenzieren.

Am einfachsten wäre es gewesen, wenn die Meldebehörde im Auftrag und auf Kosten des Projekts die Einladungen versandt hätte. So hätte das Projekt von der Identität der Frauen, die das mit der Einladung verbundene Angebot nicht wahrgenommen hätten, gar keine Kenntnis erhalten. Dagegen wurde eingewandt, man benötige Namen, Anschriften und Geburtsdaten aller eingeladenen Frauen zur Organisation der Untersuchungstermine, zur Vermeidung von ärgerlichen Mehrfach- oder Fehleinladungen und zur vollständigen Erfassung der Zielgruppe.

Dem musste ich entgegenhalten, die Meldebehörde dürfe auf Grund der melderechtlichen Regelungen die abverlangten Datensätze nur einer öffentlichen Stelle übermitteln, die sie zur Erfüllung ihrer gesetzlichen Aufgaben benötige. Andernfalls dürfe die Meldebehörde nur einen eingeschränkten Datensatz übermitteln, vorausgesetzt, es bestehe ein öffentliches Interesse an dem mit dem Projekt angestrebten Nutzungszweck. Zudem sei im Einzelfall eine durch die Meldebehörde anerkannte Übermittlungssperre zu beachten.

Ich schlug vor, anders als vorgesehen, die Erklärung der eingeladenen Frauen, an der Untersuchung teilnehmen zu wollen, abzutrennen von ihrer Einwilligung in die Verarbei-

tung ihrer Daten zu Zwecken der oben dargestellten langfristigen Evaluation. Vor der Untersuchung und in Unkenntnis von deren Ergebnis könne die einzelne Frau eine sinnvolle Entscheidung hierüber noch nicht treffen. Zudem musste ich auf § 7 des Bremischen Krebsregistergesetzes hinweisen, der in Übereinstimmung mit den entsprechenden Gesetzen anderer Bundesländer die Übermittlung von im Krebsregister erfassten Daten in personenbezogener Form zu Forschungszwecken nur dann erlaubt, wenn zuvor über den behandelnden Arzt das Einverständnis der einzelnen registrierten Patientin eingeholt worden ist. Eine langfristeige Speicherung und Nutzung der Daten für Forschungszwecke ohne Einwilligung der Betroffenen wäre nicht möglich.

Reihenuntersuchung zur Prävention: eine öffentliche Aufgabe: Auch der Senator für Gesundheit erkannte, dass eine Übermittlung umfangreicher Daten für Zwecke gesundheitlicher Prävention nur auf einer ausreichenden gesetzlichen Grundlage stattfinden kann. Die Abeilung hat die nachstehend aufgeführten Regelungen ausführlich mit mir beraten. In Art. 1 Nr. 4 seines Entwurfs für ein Gesetz zur Änderung gesundheitsrechtlicher Gesetze, über das ich oben unter Ziff. 8.4. berichtet habe, strebt der Senat an, dass in einem neuen § 15 des Gesetzes über den Öffentlichen Gesundheitsdienst (ÖGDG)

- die Durchführung von Maßnahmen der Prävention, unter denen er insbesondere Screening-Verfahren wie das in Rede stehende Projekt versteht, zur Aufgabe des Öffentlichen Gesundheitsdienstes erklärt wird,
- mit derartigen Maßnahmen beauftragte Stellen, soweit erforderlich einen abschließend aufgeführten Satz von Meldedaten, insbesondere Namen, Anschrift und Geburtsdatum, der von der jeweiligen Maßnahme betroffenen Personen bei der Meldebehörde erheben dürfen,
- hierzu auch die Daten gehören, die für die Feststellung erforderlich sind, ob eine der genannten Personen ihren Namen geändert hat, verzogen oder verstorben ist und
- der Senator für Gesundheit durch Rechtsverordnung eine bestimmte Stelle mit der Durchführung einer bestimmten Maßnahme der Prävention beauftragen kann.

In der amtlichen Begründung heißt es dazu,

- damit werde die Grundlage für die Erhebung der für die Einladung zu einer Präventionsmaßnahme erforderlichen Meldedaten geschaffen,
- die für die Einladung erforderlichen Daten von Teilnehmerinnen einschließlich der bei der Untersuchung erhobenen Gesundheitsdaten dürften für weitere Zwecke im Rahmen der Maßnahme der Prävention (insbesondere für die Übermittlung zur Befundung) nur verwendet werden, wenn die betroffene Person hierin eingewilligt habe. Weitere Datenübermittlungen bedürften neuer Einwilligungserklärungen.
- die Einladungsdaten der Personen, die an der Screening-Maßnahme nicht teilnehmen, seien zu anonymisieren.

Projektdesign, neue Fassung: Inzwischen hat die Projektleitung in Reaktion auf die vielfältig geäußerte Kritik und auf den dargestellten Gesetzentwurf ein neues Konzept vorgelegt:

- Die neue Projektbeschreibung beschränkt sich auf das eigentliche Screening-Projekt mit seinem Angebot einer freiwilligen Reihenuntersuchung. Die langfristige Evaluation wird nicht mehr thematisiert.

- Nach Abschluss eines Einladungsverfahrens sollen die in der Einladungsstelle des Projekts hierfür gespeicherten Meldedatensätze der Frauen, die ihre Einladungen nicht wahrgenommen haben, anonymisiert werden, d. h. die Bestandteile des Datensatzes, durch die auf die Identität einzelner Frauen geschlossen werden könnte, sollen gelöscht werden. Es können dann nur noch statistische Auswertungen vorgenommen werden. Dies hat zur Folge, dass diese Frauen zur vorgesehenen zweiten Untersuchung und schon vorher bei Umzug in einen Stadtteil, in dem die Einladungen später verschickt werden, erneut eingeladen werden. Man will aber eine erneute Einladung von Frauen, die ausdrücklich abgelehnt haben teilzunehmen oder die ausdrücklich die Speicherung ihrer Daten abgelehnt haben, vermeiden. Zu diesem Zweck will man ihre Meldedaten über einen Hash-Code unwiderruflich verschlüsselt auf einem besonderen Datenträger speichern. Auf diese Weise sollen beim Import neuer Meldedaten aus der Meldebehörde die sie identifizierenden Bestandteile der Datensätze der ablehnenden Frauen automatisch "weggefiltert“ werden, sodass sie nicht personenbeziehbar gespeíchert und folglich auch nicht eingeladen werden. Zusätzlich will man aber zur Vermeidung von Neueinladungen eventuell eingehende Widerspruchsschreiben aufbewahren.

- Nach wie vor ist vorgesehen, mit der Annahme der Einladung die Einwilligung in die weitere Auswertung personenbezogener Meldedaten bzw. der bei der Untersuchung gewonnenen medizinischen Daten zu verbinden. Dies gilt insbesondere für die Übermittlung der bei der Mammographie erhobenen medizinischen Daten, insbesondere der Röntgenaufnahme, an die Befundungsstelle.

- Dagegen ist das Konzept insoweit geändert worden, als es berücksichtigt, dass personenbezogene Daten von im Krebsregister erfassten Frauen dem Projekt nur übermittelt werden dürfen, nachdem die Vertrauensstelle des Krebsregisters über den behandelnden Arzt der einzelnen Betroffenen deren Einwilligung eingeholt hat.

Datenschutzrechtliche Bewertung des Projektdesign, neue Fassung: Ein Teil der datenschutzrechtlichen Bedenken ist damit ausgeräumt, einige wichtige Arbeitsschritte sind in Kooperation mit dem Projekt selbst und mit dem Gesundheitsamt Bremen, das das Einladungsverfahren durchführen wird, noch zu erledigen:

- Über das Ausmaß der Übermittlung von Meldedaten seitens der Meldebehörde an das Projekt besteht weiterhin Unklarheit. Meldebehörde und ich gehen davon aus, dass über zwei Jahre hinweg nach und nach "portionsweise“ die Daten der vom Pro-

jekt erfassten Frauen aus den Stadtteilen übermittelt werden sollen, die als nächst eingeladen werden sollen. Für die Nacheinladung nach vier Wochen sollen die Daten einmal aktualisiert werden. Dagegen erwartet das Projekt alle vier Wochen die aktualisierten Daten der erfassten Frauen aus allen Stadtteilen. Es wird zu klären sein, in welchem Umfang Datenübermittlungen für die Durchführung des Screening-Projekts erfroderlich sind. Nach § 15 des Entwurfs zum § 15 ÖGDG ist dies Voraussetzung für die Übermittlung der Meldedaten.

- Bedenken bestehen gegen die Aufbewahrung der Schreiben, in denen Frauen die Speicherung ihrer Meldedaten bzw. ihre Teilnahme am Screening ausdrücklich ablehnen. Sobald ein technischer Filter verhindert, dass sie nochmals eingeladen werden, ist die Aufbewahrung nicht mehr erforderlich und führt zu unnötigen Datenschutzrisiken.
- Das Informationsblatt und die Einwilligungserklärungen für die eingeladenen Frauen sind noch nicht abgestimmt. Sie müssen unter anderem auch datenschutzrechtlichen Anforderungen genügen.
- Die Datenschutzgesetze geben vor, vor Beginn der Datenverarbeitung die technischen Sicherheitsvorkehrungen festzulegen. Ein entsprechendes Konzept ist mir noch nicht zur Abstimmung vorgelegt worden.

Fazit: Der erste Fehler wurde gemacht, als die Kassen ein Projekt in Auftrag gaben, ohne vorher in einer Machbarkeitsstudie ein Datenschutzkonzept entwickelt zu haben. Auf Risiken habe ich rund ein Jahr vor dem geplanten Projektstart hingewiesen. Aber auch die sonstigen insbesondere frauen- und gesundheitspolitischen Implikationen wurden wohl unterschätzt. Auch wenn ich an dieser Stelle nicht verhehlen will, dass es keine Freude bereitet, immer neue Varianten des Projekts unter datenschutzrechtlichen Aspekten zu beraten, so habe ich doch mein Möglichstes gegeben, um in einem datenschutzrechtlich gesicherten Rahmen die Fortentwicklung der Prozesse zeitnah zu begleiten.

8.6. Vernetzung des Gesundheitsamtes Bremen

Das Gesundheitsamt Bremen setzt zur Zeit ca. 240 miteinander vernetzte PC in seinen Abteilungen ein. Darüber hinaus ist der Zugang zum Bremer Verwaltungsnetz (BVN) realisiert, womit jeder Arbeitsplatz E-Mail- und internetfähig ist. Das gesamte Netz liegt hinter der Firewall der BreKom. Damit werden wie in anderen Verwaltungen die derzeitigen technischen Möglichkeiten für die interne und externe Kommunikation sowie für die Dokumentation des Amtes genutzt. Angesichts der Verarbeitung z. T. hoch sensibler dem Arztgeheimnis unterliegender Gesundheitsdaten sind allerdings hohe Anforderungen an die technischen Vorkehrungen zum Schutz vor unbefugten Zugriffen sowohl Interner als auch Externer zu stellen. Für diese Fragen gibt es vorbildliche gesetzliche Regelungen,

deren technische Umsetzung beim Gesundheitsamt Bremen zum Teil noch Schwierigkeiten bereiten. Dazu im einzelnen:

Interne Regelungen zur Abschottung von Beratungsdaten: In jüngster Zeit sind mehrere aufeinander abgestimmte Regelungen in Kraft getreten, die besondere Schutzvorkehrungen anordnen:

- Das **Bremische Gesetz über den öffentlichen Gesundheitsdienst (ÖGDG)** von 1995 verlangt sicherzustellen, dass personenenbezogene Daten nur für die jeweiligen Aufgabenbereiche verwendet werden dürfen. Insbesondere ist die Trennung zu gewährleisten zwischen bei freiwilligen Beratungen erhobene Daten und solchen, die bei der Ausübung von Überwachungs- und Zwangsmaßnahmen erhoben werden.
- Das neue **Gesetz über Hilfen und Schutzmaßnahmen (PsychKG)** bei psychischen Krankheiten vom 22. Dezember 2000 unterwirft die zum Zwecke der Erfüllung von Aufgaben nach diesem Gesetz erhobenen Daten einer im Vergleich zum BrDSG und zum ÖGDG besonders strengen Zweckbindung, d. h. die Daten psychisch Kranker dürfen für andere Zwecke nur bei deren Einwilligung verarbeitet werden oder wenn eine gegenwärtige Gefahr für Leib oder Leben der betroffenen Person oder Dritter nicht anders abgewendet werden kann.
- Die auf der Grundlage des ÖGDG erlassene **Verordnung über die Verarbeitung personenbezogener Daten im Öffentlichen Gesundheitsdienst** vom Dezember 1999 i.d.F. des neuen PsychKG verlangt in Ausführung beider zitierter Gesetze, dass die durch Sozialpsychiatrische Dienste bei der freiwilligen Beratung erhobenen Daten von den Daten getrennt zu speichern sind, die im Rahmen von ihrer Natur nach nicht freiwilligen Schutzmaßnahmen erhoben werden. Die Daten dürfen nur zusammengeführt werden, wenn die Zweckänderung nach der oben dargestellten strengen Regelung des neuen PsychKG zulässig ist.

Mehrfach habe ich in schriftlichen Stellungnahmen darauf hingewiesen, dass im Netz die neuen rechtlichen Vorgaben für die abteilungsinterne Abschottung von Beratungsdaten des Sozialpsychiatrischen Dienstes durch technische Vorkehrungen umzusetzen sind. Bisher leider ohne durchschlagenden Erfolg.

Abschottung der einzelnen Abteilungen untereinander: Unterschiedlichste sensible Aufgabenbereiche (insbesondere der sozialpsychiatrische Dienst) sind laut ÖGDG im Rahmen dieser Netzstruktur strikt voneinander abzugrenzen. Für den Bereich der internen Abschottung ist es dringend erforderlich, den abteilungsübergreifenden E-Mail-Verkehr zu regeln (Löschungen, Attachments (Anhang zum Anschreiben), Verwaltung der individuellen Postfächer, Outlook-Einstellungen, Vetretungsregelungen, Sicherheit auf der Netzstrecke etc.). Diese Notwendigkeit wurde bereits vom Gesundheitsamt im September 1998 anerkannt, aber noch nicht umgesetzt.

Für das Netz des Gesundheitsamtes sind mir verschiedene Entwürfe eines Datenschutzkonzeptes vorgelegt worden. Der letzte Entwurf ist um die Beschreibung der Sicherheitsfeatures, der sich im Netz befindlichen PC ergänzt worden. Die Konfiguration soll gemäß Datenschutzkonzept entsprechend der Security-Guideline des TUI-Referates vorgenommen worden sein. Damit wäre eine angemessene Datensicherung für die Workstations im Netz erreicht.

Insgesamt offen bleibt neben dem nicht kontrollierbaren E-Mail-Verkehr die Steuerung der Daten über andere Exportschnittstellen (div. Laufwerke etc.). Ohne technische und organisatorische Regelungen ist an dieser Stelle nicht sichergestellt, dass die rechtlich vorgeschriebene Abschottung zwischen den einzelnen Bereichen des Gesundheitsamtes angemessen gewährleistet ist. Meinem mit Schreiben vom 19. Oktober 2000 erbetenem Ergänzungswunsch zum Datenschutzkonzept um Richtlinien zur Programmierung von Datenbankanwendungen ist bis zum letzten Konzept vom Januar 2001 ansatzweise entsprochen worden. Wesentliche Verfahrensmerkmale, die einen kontrollierbaren Ablauf gewährleisten würden, fehlen jedoch. Dazu gehören u. a. verbindliche Zulässigkeitskriterien für die Eigenentwicklung, Festlegung der fachlichen und technischen Verantwortung für den Einsatz, institutionalisierte interne Kontrollen, Kriterien zur Progammfreigabe, Dokumentationen der Programmierung und Programmpflege.

Die zentrale Administration hat neben der Datenbankprogrammierung umfassende Rechte im Netz, die den Zugriff auf den gesamten Datenbestand des Gesundheitsamtes ermöglichen. Auch die Verwaltung der Workstations in den Abteilungen erfolgt durch die für das gesamte Gesundheitsamt zuständige zentrale Administration. Um die Abschottung der einzelnen Abteilungen des Gesundheitsamtes auch technisch im Bereich der Administration umzusetzen, habe ich zuletzt im Oktober 2000 den Vorschlag gemacht, abteilungsbezogene Domänenadministratoren zu installieren und somit einen ersten Schritt in Richtung der Verteilung der Administrationsaufgaben auf verschiedene Rollen (vgl. Security-Guideline Stand 3/00) zu gehen.

Damit könnte ein abteilungsübergreifender Zugriff auf die Datenbestände auf technische Notfälle begrenzt werden. Die Umsetzung dieses Vorschlages ist nach Aussage des Gesundheitsamtes aus Gründen des dafür erforderlichen Know-How und in der Praxis entstehende erhebliche Mehrarbeit der Administration nicht vorgesehen. Vorgeschlagen wurde vom Gesundheitsamt der Aufbau einer wirksamen Kontrollmöglichkeit der zentralen EDV-Koordination.

Meinem vor diesem Vorschlag erbetenen Wunsch, das Konzept um Protokollierungsrichtlinien, Auswertungen und Organisation der Revision zu ergänzen, wurde jedoch nicht entsprochen. Insgesamt sind vor dem Hintergrund der komplexen technischen Infrastruktur und der strengen rechtlichen Anforderungen in wesentlichen Bereichen keine ausreichenden Maßnahmen getroffen worden.

Abschottung gegenüber Zugriffen Externer: Weiter muss das Netz mit starken technischen Maßnahmen gegen externe Angriffe geschützt werden. Aufgrund der Sensibilität

der Daten im Gesundheitsamt ist es nicht ausreichend, allein auf die Sicherheitsmechanismen der BreKom-Firewall zu setzen. Es ist vielmehr notwendig, lokal zusätzliche Maßnahmen einzusetzen (vgl. 22. JB, Ziff. 3.4.4.).

Ich habe das in einem Beratungsgespräch im Mai 2000 erläutert. In dem mir vorgelegten aktuellen Konzept wird nun der Einsatz eines Proxy-Servers, über den mittels Terminaldienste der Zugang zum Internet abgesichert werden soll, angekündigt. Ich gehe bei dem vorhandenen Gefährdungspotential davon aus, dass diese Planung im ersten Halbjahr dieses Jahres umgesetzt wird.

8.7. Transparenzgesetz - Pseudonymisierung in der Gesetzlichen Krankenversicherung

Am 4. November 1999 verabschiedete der Deutsche Bundestag das Gesetz zur Gesundheitsreform 2000. Das Gesetz verfolgte das Ziel, den gesetzlichen Krankenkassen eine ausreichende Datengrundlage für die Prüfung der Abrechnungen von ärztlichen Leistungen sowie von deren Wirtschaftlichkeit und Qualität zur Verfügung zu stellen. Zur Wahrung der Persönlichkeitsrechte der Versicherten hatte man im Gesetzentwurf den von Datenschutzseite vorgetragenen Vorschlag aufgenommen, die Abrechnungs- und Leistungsdaten zuvor dergestalt zu pseudonymisieren, dass der Bezug auf einzelne Versicherte verhindert wurde, es sei denn, in gesetzlich bestimmten Fällen werde durch eine Stelle außerhalb der Krankenkassen das Pseudonym aufgehoben. Leider scheiterte diese Regelung anschließend an der Ablehnung der zustimmungsbedürftigen Teile des Gesetzesbeschlusses durch die Mehrheit des Bundesrates.

Bereits in meinem letzten Jahresbericht (vgl. 22. JB; Ziff. 8.8.) konnte ich darüber berichten, das Bundesministerium für Gesundheit wolle in einem neuen Anlauf versuchen, die Datenbasis der Krankenkassen und den Datenschutz für die Versicherten zugleich zu verbessern. Inzwischen hat über mögliche Inhalte eines Gesetzes zur Verbesserung der Datentransparenz in der gesetzlichen Krankenversicherung ein erster Informationsaustausch zwischen Ministerium und Datenschutzbeauftragten stattgefunden. Bedauerlich ist, dass - wohl auf Einwände der Krankenkassen hin - das Vorhaben aufgegeben worden ist, diesen von vornherein nur pseudonymisierte Daten zur Verfügung zu stellen. Die Krankenkassen sollen für die Abrechnungsprüfung von allen Leistungserbringern außer den niedergelassenen Ärzten - insoweit verbleibt diese Aufgabe bei den Kassen(zahn)ärztlichen Vereinigungen - die Daten weiterhin versichertenbezogen erhalten. Allerdings sollen nach Abschluss der Abrechnungsprüfung die Daten pseudonymisiert werden und grundsätzlich nur in dieser Form für weitere Zwecke genutzt werden dürfen. Damit scheint zwar eine anspruchsvolle Lösung für Datenschutz durch Technik vorerst vom Tisch zu sein, immerhin aber besteht die Aussicht, bestimmte Verbesserungen zu erreichen, sofern präzise gesetzliche Bestimmungen Zeitraum und Zwecke der Nutzung versichertenbezogener Daten durch die Krankenkassen auf das unerlässliche Maß begrenzen.

8.8. Datenschutzrechtliche Konsequenzen der Entschlüsselung des menschlichen Genoms

Bereits in 1989 haben die Datenschutzbeauftragten von Bund und Ländern zur Analyse der menschlichen Erbanlagen ihre Position klargemacht, dass es gilt, die freie Selbstbestimmung des Einzelnen zu wahren und das Recht des Einzelnen auf Nichtwissen zu respektieren. Sie forderten gesetzliche Vorgaben insbesondere für Genomanalysen in der pränatalen Diagnostik, im gerichtlichen Verfahren, im Arbeitsverhältnis und im Versicherungswesen. Die Konferenz der Datenschutzbeauftragten hat im Berichtsjahr in einer Entschließung (vgl. Ziff. 17.9. des Berichts) diese Position noch einmal bekräftigt. Allein der "genetische Fingerabdruck“ zur Identitätsfeststellung im Strafverfahren hat bisher eine gesetzliche Regelung gefunden. Die Anwendung von Verfahren zur Entschlüsselung menschlicher Erbanlagen, insbesondere von Krankheitsrisiken hat zwar auch längst begonnen, unterliegt aber noch keinen verbindlichen von den Beteiligten anerkannten Regeln.

Die Enquete-Kommisssion des Deutschen Bundestages "Recht und Ethik der modernen Medizin" ist in Vorbereitung der anstehenden parlamentarischen Entscheidungen auch an die Datenschutzbeauftragten herangetreten. Die Konferenz der Datenschutzbeauftragten hat eine Arbeitsgruppe zur Genomanalyse eingesetzt, die ihre Arbeit aufgenommen hat. Ich beteilige mich daran. Der Senatorin für Gesundheit die dieses Jahr den Vorsitz in der Gesundheitsministerkonferenz hat, habe ich einen Informationsaustausch vorgeschlagen. Dieser Vorschlag ist auf positive Resonanz gestoßen.

9. Jugend, Soziales und Arbeit

9.1. Elektronische Fallakte in der Jugendhilfe

Die Aktenführung in der Jugendhilfe im Amt für Soziale Dienste Bremen dient zur Unterstützung der MitarbeiterInnen in der praktischen Arbeit, aber auch für Zwecke der Planung und des Controlling. Sie soll digitalisiert werden, später sollen auch die Akten der anderen Sozialen Dienste mit einbezogen werden. Bereits im letzten Jahr (vgl. 22. JB, Ziff. 9.1.) hatte ich über die datenschutzrechtlichen Aspekte des Vorhabens berichtet, es begegnet keinen grundsätzlichen Bedenken. Bei dem Projekt ist zu beachten, dass auch amtsintern persönliche Schweigepflichten von MitarbeiterInnen gelten. Auch Klientendaten genießen einen vergleichbaren besonderen Vertrauensschutz nach §65 SGB VIII. Ich hatte daher die Verwaltung insbesondere darauf hingewiesen, dass dieser Vertrauensschutz die Speicherung bestimmter Datenkategorien ausschließt bzw. die Eröffnung von Zugriffen anderer MitarbeiterInnen/Abteilungen auf diese Daten verbietet. Dies gilt etwa für Mitteilungen persönlicher Verhältnisse, die KlientInnen im Rahmen eines Beratungsgesprächs machen, die aber nicht Gegenstand eines Antrags auf eine kostenwirksame Maßnahme werden.

Da das im Sommer 2000 als Grundlage der Ausschreibung vorgelegte Pflichtenheft "Elektronische Fallakte“ hierzu keine ausreichenden Aussagen machte, soll das Pflichtenheft um eine Präambel ergänzt werden, die auf der Grundlage von in Abstimmung mit mir vor einigen Jahren erarbeiteten Dienstanweisungen des Amtes für Soziale Dienste Datenschutzvorgaben enthält, die auch auf die Nutzung der Elektronischen Fallakte übertragbar sind. Der Vorgang ist noch nicht abgeschlossen.

9.2. Rechnungsprüfung und -abwicklung von Leistungen der Krankenhilfe in Bremen durch einen externen Dienstleister

Nicht nur in Bremen, sondern bundesweit wird in Sozialämtern daran gedacht, mit der Abwicklung von Leistungen der Krankenhilfe an Sozialhilfeempfänger und an Asylbewerber, d. h. mit der Prüfung und Abgeltung der Rechnungen von Ärzten und Angehörigen anderer Heilberufe, externe Dienstleister zu beauftragen. Dies liegt nahe, da hier ein spezielles, nicht in der Sozialhilfeverwaltung, sondern in der gesetzlichen Krankenversicherung vorhandene Kenntnisse gefragt sind. Das Sozialressort trat bereits zu Beginn des Jahres 1999 an mich mit der Frage heran, ob es datenschutzrechtlich zulässig sei, eine Krankenkasse zu beauftragen. Ich wies das Ressort darauf hin, es komme darauf an, ob Gegenstand der Beauftragung

- die selbständige Erfüllung der gesetzlichen Aufgabe selbst oder aber
- nur eine unterstützende Datenverarbeitung ohne eigenen Beurteilungs- und Entscheidungsspielraum (der beim öffentlichen Sozialhilfeträger verbleibe) sein solle.

Im ersten Fall handelte es sich um eine Funktionsübertragung, die einer - bislang fehlenden - gesetzlichen Grundlage bedürfte. Im zweiten Fall handelte es sich um Datenverarbeitung im Auftrag, die nach Maßgabe des § 80 SGB X bereits jetzt zulässig ist.

Das Ressort legte mir im März 2000 das Angebot eines bestimmten, für Sozialhilfeträger in anderen Bundesländern im Rahmen von Prüfung und Abwicklung von Leistungen der Krankenhilfe bereits tätigen gewerblichen Dienstleisters aus Nordrhein-Westfalen vor. Eine Bewertung der Unterlagen auf der Grundlage von Kriterien, die mit Datenschutzbeauftragten anderer Länder abgestimmt waren, ergab, dass Gegenstand des Angebots die Erledigung gesetzlicher Aufgaben war. Der Anbieter wollte zur Gänze die Sachbearbeitung übernehmen. Es war nicht erkennbar, ob das Ressort ihm hierfür Vorgaben machen würde, die jeden eigenen Entscheidungs- und Beurteilungsspielraum des Auftragnehmers ausschließen und die Regelung von Zweifelsfällen dem Auftraggeber vorbehalten würden. Kürzlich legte mir das Ressort zusammen mit einem unter Vorbehalt meiner Zustimmung bereits abgeschlossenen Vertrag mit dem Dienstleister den Entwurf einer Prüfanweisung für den Auftragnehmer vor, die dessen Vorgehen bei der Prüfung ihm eingesandter Rechnungen festlegt. Rechnungen, die danach nicht abzuwickeln sind, sollen an den Auftraggeber weitergereicht werden. Zudem will das Ressort eine Clearingstelle einrichten, an die die Rechnungssteller sich in Zweifelsfällen wenden können, etwa wenn sie mit der Entscheidung des Auftragnehmers nicht zufrieden sind. Ich habe dem

Ressort signalisiert, dass eine Auftragsvergabe unter diesen Konditionen akzeptabel ist, vorausgesetzt, der Auftraggeber erkennt die Prüfanweisung, seine Pflicht, unklare Rechnungen weiterzureichen und die Aufgaben der Clearingstelle verbindlich an.

Inzwischen hat aber die nordrhein-westfälische Datenschutzbeauftragte in ihrer Eigenschaft als Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich die Datensicherheit bei dem Dienstleister geprüft. Ich beabsichtige daher erst nach Kenntnis des Prüfberichts eine abschließende Stellungnahme abzugeben.

9.3. Datenaustausch zur Bekämpfung illegaler Beschäftigung

Im 21. Jahresbericht unter Ziff. 13.1. und im 22. Jahresbericht unter Ziff. 9.3. hatte ich über die Vorstellungen des Senators für Arbeit berichtet, einen bremischen Informationsverbund zur Bekämpfung illegaler Beschäftigung in Gestalt einer zentralen Datei einzurichten. Angesichts des Zögerns wichtiger Beteiligter wie der Arbeitsämter, der Justiz und des Stadtamtes, aber auch von Bedenken, ob das geltende Recht eine ausreichende Grundlage für einen funktionierenden Verbund biete, beantragte der Senat gemeinsam mit der niedersächsischen Landesregierung im Bundesrat, die Bundesregierung zu bitten, gesetzliche Maßnahmen zu prüfen, durch die die an der Bekämpfung illegaler Beschäftigung beteiligten Stellen verpflichtet werden, ihre Erkenntnisse unverzüglich weiterzuleiten und untereinander Auskünfte zu erteilen. Insbesondere solle die Bundesregierung rechtliche und organisatorische Hindernisse beseitigen, die dem erforderlichen Datenaustausch im automatisierten Abrufverfahren entgegenstehen, z. B. durch Änderung des § 79 SGB X. Schließlich wird gefordert, durch Änderung des § 31 AO statt der bisherigen Befugnis zur Durchbrechung des Steuergeheimnisses eine Auskunftspflicht einzuführen. In seiner Sitzung am 29. September 2000 nahm der Bundesrat diesen Antrag an (BR-Drs. 396/00).

Es bleibt abzuwarten, zu welchen Gesetzesinitiativen diese Entschließung in Zukunft führen wird. Die Fülle bereits geltender Unterrichtungspflichten und Auskunftsbefugnisse legt den Gedanken nahe, dass diese doch erst einmal ausgeschöpft und die daraus gewonnenen Erfahrungen nachvollziehbar dokumentiert und ausgewertet werden sollten, bevor weitere, insbesondere das Sozialgeheimnis und das Steuergeheimnis weiter aushöhlende Regelungen getroffen werden. Auch im Lande selbst können noch Verbesserungen erreicht werden (vgl. Ziff. 16.6. des Berichts).

10. Bildung

10.1. Internet-Nutzung durch Schulen

In meinem letzten Jahresbericht (22. JB, Ziff. 10.3.) hatte ich über die Internet-Nutzung durch Schulen berichtet und auf wichtige datenschutzrechtliche Anforderungen hingewiesen. Diese Anforderungen hatte ich den Schulbehörden und Schulen im Lande Bremen

zugeschickt in der Erwartung, eine landesweit abgestimmte Auffassung in dieser Frage zu erreichen.

Der Senat hatte in seiner Stellungnahme zu meinem Bericht (vgl. BB-Drs. 15/472 v. 26. September 2000) meine Initiative begrüßt und darauf hingewiesen, dass der Senator für Bildung und Wissenschaft das Landesinstitut für Schule (LIS) für die Organisation der Umsetzung dieser Anforderungen in den Schulen einbezogen hat.

Bei der im März des Berichtsjahres begonnenen Diskussion meines Anforderungspapiers beim Senator für Bildung und Wissenschaft war vereinbart worden, noch vor den Sommerferien des Berichtsjahres beim LIS in Bremen einen Workshop mit den Webmastern der Schulen unter meiner Beteiligung zu veranstalten, auf dem mein Anforderungspapier diskutiert werden sollte. Leider ist es zu dieser Veranstaltung bis heute nicht gekommen.

Außerdem war vereinbart worden, die Überlegungen zur Internet-Nutzung durch Schulen in Form einer Orientierungshilfe allen Schulen im Lande zur Verfügung zu stellen und verbindlich zu machen. Eine solche Orientierungshilfe liegt bis heute nicht vor.

Ferner sollte der Musterentwurf einer Internet-Nutzungs-Ordnung für die Schulen erarbeitet werden, die als Grundlage für den Erlass entsprechender Ordnungen in den Schulen dienen könnte. Auch hierzu gibt es bis heute keine Vorlage.

Ich habe den Senator für Bildung und Wissenschaft im Herbst des Berichtsjahres an seine Zusagen erinnert. Leider hat es bisher keine Reaktionen gegeben. Ich werde daher im Frühjahr 2001 eine neue Initiative starten.

10.2. Internationale Grundschul-Leistungs-Untersuchung

Am Ende des vergangenen Jahres erhielt ich umfangreiche Unterlagen über die auch in Bremen geplante "Internationale Grundschul-Leistungs-Untersuchung" (PIRLS/IGLU). Diese Untersuchung soll in Bremen ergänzt werden um zusätzliche Analysen und Untersuchungsinstrumente sowie eine Vergleichsuntersuchung zwischen voller Halbtagsschule und verlässlicher Grundschule. Am Projekt PIRLS/IGLU sollen in Bremen nach den mir übersandten Unterlagen insgesamt 37 Grundschulen (4. Jahrgangsstufen) teilnehmen, an der Vergleichsuntersuchung die 14 vollen Halbtagsschulen und 12 repräsentativ ausgewählte verlässliche Grundschulen. Die Haupttestphase für Bremen liegt im Mai 2001.

In einer ersten Stellungnahme habe ich weitergehende Informationen zur konkreten Durchführung des Vorhabens in Bremen und Bremerhaven erbeten. Auf meine datenschutzrechtlichen Anforderungen zur Durchführung von Forschungsprojekten in einem Merkblatt, insbesondere auch zur Freiwilligkeit der Teilnahme, zur Einwilligung in die Datenerhebung und die nachfolgende Datenverarbeitung und zur möglichst umfassenden Aufklärung und Transparenz für alle Beteiligten und die Schulgremien habe ich aufmerksam gemacht. Mit einer analogen Anwendung der beim PISA-Projekt (einer weiteren internationalen Schulvergleichsuntersuchung, vgl. 22. JB., Ziff. 10.1.) gefundenen Daten-

schutzregelungen habe ich mich grundsätzlich einverstanden erklärt. Die Gespräche in dieser Sache sind noch nicht abgeschlossen.

11. Bau, Verkehr und Umwelt

11.1. Änderung der Liegenschaftsdatenübermittlungsverordnung

§ 23 Abs. 7 Vermessungs- und Katastergesetz ermächtigt den Senator für das Bauwesen (jetzt: Der Senator für Bau und Umwelt), durch Rechtsverordnung die zur Durchführung dieses Gesetzes erforderlichen Vorschriften über das Verfahren bei der Einrichtung von automatisierten Verfahren zu erlassen. Diese Vorschrift wird durch die Liegenschaftsdatenübermittlungsverordnung (LieDÜV) ausgeführt.

Die LieDÜV vom 27. Januar 1995 ist am 30. November 2000 erneut geändert worden (BremGBl. S. 447). Nunmehr erhalten der Gutachterausschuss für Grundstückswerte, öffentlich bestellte Vermessungsingenieure, das Amt für Straßen und Verkehr und der Senator für Wirtschaft und Häfen jeweils eine Datenabrufbefugnis aus dem automatisierten Liegenschaftskataster zu den in der LieDÜV jeweils genannten Zwecken.

Ich wurde rechtzeitig beteiligt und habe festgestellt, dass die in § 10 Abs. 7 Vermessungs- und Katastergesetz genannten Voraussetzungen vorliegen. Ich habe daher keine Bedenken gegen die Änderung der LieDÜV geäußert.

11.2. Prüfung des Wohngeldverfahrens

Für die Bearbeitung von Wohngeldfällen ist von der ID Bremen die neue Software "BREWOG" für den Einsatz in Bremen und Bremerhaven erstellt und im August 1999 in Betrieb genommen worden. Ich wurde rechtzeitig informiert und habe die mir vorgelegten Entwürfe eines Datenschutzkonzeptes und einer Dienstanweisung beraten. Im Sommer 2000 lagen die mit mir abgestimmten Konzepte vor und ich habe den Einsatz des Verfahrens im Herbst 2000 beim Amt für Wohnung und Städtebauförderung in Bremen geprüft.

Prüfthemen waren u. a. die folgenden im Datenschutzkonzept festgeschriebenen organisatorischen und technischen Maßnahmen zur Gewährleistung des Datenschutzes:

- Organisationseinheiten, die auf die Software zugreifen und deren Zugriffsberechtigungen,
- Schulungen der MitarbeiterInnen,
- Umsetzung der Richtlinie für Einzelplätze/Server/lokale Netzwerke - Aufbau, Installation und Sicherheitseinstellungen für Windows NT-Server/NT-Workstation - (NT-Security-Guideline), Vorhandensein von Dateibeschreibung und Geräteverzeichnis, eingesetzte Hard- und Software,
- Anschluss der Clients an das Großrechnerverfahren bei der ID Bremen,
- Protokollierung,
- Virenschutzsoftware und

- Löschung von Textdateien.

Als Prüfergebnis habe ich festgestellt, dass die Systemadministration durch Kenntnis des Administrationspasswortes Zugriff auf das Fachverfahren nehmen kann. Hier muss die in der Dienstanweisung beschriebene organisatorische Trennung von Systemadministration und Datenbankadministration (Fachverfahren) technisch umgesetzt werden. Die in der NT-Security-Guideline genannten Datenschutzmaßnahmen sind für den Einsatz von Personaldatenverbeitungs-Systemen erstellt worden, sollen aber auch hier getroffen werden, da die Sensibilität der in dem Verfahren zu verarbeitenden Daten der von Personaldaten entspricht. Das Amt für Wohnung und Städtebauförderung hat die Umsetzung der NT-Security-Guideline bis zum Jahresende zugesagt. Die auf den Servern vorhandene Virenschutzsoftware wurde zum Prüfzeitpunkt vierteljährlich aktualisiert. Angesichts der schnellen Verbreitung von neuen Viren habe ich hier wenigstens ein monatliches Update der Virenschutzsoftware empfohlen.

Meine Verbesserungsvorschläge sind umgesetzt worden. Die Aktualisierung der Virenschutzsoftware auf den Servern erfolgt sogar wöchentlich.

Weiter ist eine differenzierte Zugriffsberechtigung nicht umgesetzt worden, da die insgesamt fast 60 Sachbearbeiter uneingeschränkten Zugriff auf den gesamten Wohngeldbestand, unabhängig von ihrem jeweiligen Aufgabenbereich, haben. Begründet wird dies mit der Erforderlichkeit für die Bearbeitung von "Wohngemeinschaftsfällen". Auf eine von mir problematisierte regelmäßige Rückstandsstatistik wird bis auf Weiteres verzichtet. Die Umsetzung der differenzierten Zugriffsregelung ist laut Aussage der geprüften Stelle derzeit nicht leistbar. Dieser Punkt wird noch geklärt.

11.3. Videoüberwachung in öffentlichen Verkehrsmitteln

Bei den im Lande Bremen ansässigen öffentlichen Verkehrsunternehmen, der Bremer Straßenbahn AG (BSAG) und der Verkehrsgesellschaft Bremerhaven (VGB) habe ich angefragt, ob dort in den Fahrzeugen eine Videoüberwachung der Fahrgäste stattfindet bzw. geplant ist.

Die BSAG hat erklärt, sie führe keine Videoüberwachung von Fahrgästen in ihren Fahrzeugen durch. Auch sei deren Einführung nicht geplant. Darüber hinaus war der Presse zu entnehmen, dass Polizeibeamte eine Woche in Bussen und Bahnen der BSAG unterwegs waren, um das Sicherheitsgefühl der Fahrgäste zu erhöhen. Aufgrund der positiven Resonanz seitens der Beschäftigten und der Fahrgäste werde die Polizei die Aktion voraussichtlich ab Frühjahr kontinuierlich fortsetzen.

Dagegen hat die VGB erklärt, sie setze in vier Gelenkbussen Videoüberwachungsanlagen ein, weil in diesen Bussen die Vandalismusschäden erheblich ausgeprägter seien als in den anderen Bussen. Die Vandalismusschäden seien seit dem erstmaligen Probeeinsatz der Überwachungsanlagen im Jahre 1997 zurückgegangen. Außerdem sei das Sicherheitsempfinden der Fahrgäste erheblich gestiegen, wie eine Umfrage unter

den Fahrgästen erbracht habe. Gelegentlich seien auch in Bremerhaven Polizeibeamte in den Bussen mitgefahren, allerdings seien die Kosten hierfür zu hoch. Beabsichtigt sei daher, alle Gelenkbusse mit Videokameras auszustatten.

Die Videoanlage werde beim Anlassen des Motors mit dem Zündschlüssel automatisch aktiviert und beim Abstellen beendet. Sie verfüge über einen Ringspeicher; die Aufzeichnungen würden nach 24 Stunden automatisch überspielt und insoweit gelöscht werden.

Eine Auswertung werde dann vorgenommen, wenn der Fahrer Vandalismusschäden feststelle. Dann werde die Kassette von einem der beiden Zugriffsberechtigten aus der im Bus befindlichen Anlage herausgenommen und in der Betriebshalle ausgewertet. Dort befinde sich in einem Raum ein PC als Auswertungsstation, auf die nur der Einsatzleiter und ein weiterer Mitarbeiter Zugriff hätten.

Die Besichtigung eines mit einer Videoanlage ausgestatteten Gelenkbusses hat ergeben, dass die Videoanlage im vorderen oberen Teil des Busses hinter einer Abdeckhaube montiert ist. Im Bus befinden sich insgesamt vier Videokameras, die als halbrunde dunkle Halbkugeln erkennbar sind. Die Videolinsen überwachen alle zugänglichen Bereiche des Busses, nur der Fahrerraum sei ausgespart. An den Türen und im Bus befinden sich Schilder in einer Größe von ca. 10 x 10 cm, die auf die Videoüberwachung hinweisen und mit dem Logo der VGB versehen sind.

Im Berichtsjahr sei erstmalig eine 24-Stunden-Aufzeichnung herausgenommen worden, weil ein Fahrgast eine Fensterscheibe eingeschlagen habe. Von dem Täter seien Bildausdrucke angefertigt worden, die der Kriminalpolizei (Kripo) zur Strafanzeige zugestellt worden seien. Durch die Ermittlungen der Kripo sei die Identität des Täters festgestellt worden, und die VGB habe Schadensersatzforderungen gegen diese Person erhoben. Ob die Bilder zur Ergreifung des Täters beigetragen haben, ist nicht bekannt.

Nach dieser Bestandsaufnahme habe ich die VGB auf die derzeit ungenügende Rechtslage hingewiesen (BGH-Urteil vom 25. April 1995 - Az.: VI ZR 272/94 KG und §6 b BDSG-Entwurf) und die Beratungsergebnisse einer Arbeitsgruppe der Datenschutzbeauftragten der Länder mitgeteilt. Die Arbeitsgruppe hat folgende Voraussetzungen festgelegt, unter denen der Einsatz von Videoüberwachung in öffentlichen Verkehrsmitteln möglich ist:

- Die Videoüberwachung dient der sicheren Beförderung der Fahrgäste oder der Verhinderung von Eigentumsstörungen (Gewährleistung der öffentlichen Sicherheit), ist zu diesem Zweck erforderlich und beeinträchtigt die Rechte der Fahrgäste auf informationelle Selbstbestimmung nicht unverhältnismäßig.
- In geeigneten Fällen verbleibt den Fahrgästen in der Regel die Entscheidung, unbeobachtet zu fahren. Dazu wird z. B. ein Bereich in den Verkehrsmitteln nicht von Kameras erfasst.

- Es werden rechtzeitig organisatorische Vorkehrungen für konkrete Gefahrenlagen getroffen, um bei einer Beobachtung zur Sicherheit der Fahrgäste eingreifen zu können.
- Eine Aufzeichnung erfolgt, wenn ein Anlass dazu besteht, etwa weil Ereignisse festgestellt werden, die die Gewährleistung der Sicherheit beinträchtigen.
- Die Auswertung aufgezeichneter Bilder wird zweckentsprechend und nur durch die dazu befugten Personen vorgenommen. Nicht benötigte Bilder werden unverzüglich gelöscht.
- Auf die Beobachtung und auf die Aufzeichnung sowie auf die verantwortliche Stelle (Angabe der Telefonnummer) wird deutlich sichtbar hingewiesen. Bei personenbezogener Auswertung werden die betroffenen Personen grundsätzlich benachrichtigt.
- Die notwendigen Sicherheitsmaßnahmen sind in einer Betriebsanweisung festgelegt.
- Die Überwachung wird nicht auf einmal, sondern schrittweise eingeführt. Dabei werden die Datenschutzvorkehrungen kontinuierlich überprüft und bewertet. In regelmäßigen Zeitabständen wird festgestellt, ob die Überwachung noch erforderlich ist.

Inzwischen hat die VGB mit dem Betriebsrat eine Vereinbarung abgeschlossen, die zwar nur die Vertragsverhältnisse der VGB mit ihren Mitarbeitern und nicht die mit den Fahrgästen tangiert. Gleichwohl berücksichtigt die Betriebsvereinbarung die vorgenannten Kriterien, wenn auch nicht vollständig.

Beispielsweise befinden sich in den Bussen keine unbeobachteten Bereiche. Hierzu hat die VGB erklärt, es müssten insbesondere die Ein- und Ausstiege und zwar auch in Fahrernähe videoüberwacht werden, weil dies bei Übergriffen auf den Fahrer zu Beweiszwecken erforderlich sei. Außerdem habe ich verlangt, größere als 10 x 10 cm und besser als bisher sichtbare Hinweise auf die Videoüberwachung der VGB anzubringen.

Ich habe die VGB daher gebeten, mich darüber zu unterrichten, wenn neue Hinweise angebracht werden sollen und in regelmäßigen Abständen (jährlich) zu prüfen, ob der Umfang der Videoüberwachung noch erforderlich ist und ob nicht doch bestimmte Bereiche in den Bussen "videofrei" bleiben können. Im Übrigen behalte ich mir vor, in absehbarer Zeit den Videoeinsatz zu überprüfen und auf seine Erforderlichkeit hin zu bewerten.

11.4. Entwurf eines Gesetzes über die Vergabe von Bauaufträgen

Der Senator für Bau und Umwelt hat mir den vorgenannten Entwurf zur Stellungnahme zugeleitet. Darin sollen für öffentliche Bauaufträge im Sinne des Gesetzes gegen Wettbewerbsbeschränkungen (GWB) Vergabegrundsätze und der Umfang der von den Unternehmern zu erbringenden Nachweise geregelt werden.

Ich habe dem Senator für Bau und Umwelt mitgeteilt, dass die Regelung hinsichtlich der zu erbringenden Nachweise nur dann eine ausreichende Rechtsgrundlage zur Erhebung personenbezogener Daten über Unternehmer und ggf. ihre Arbeitnehmer ist, wenn bei der Ausführung die Vorgaben des § 10 Abs. 2 Bremisches Datenschutzgesetz (Datenerhebung grundsätzlich beim Betroffenen mit seiner Kenntnis) beachtet werden.

In diesem Zusammenhang habe ich die senatorische Dienststelle auf den Entwurf einer Verwaltungsvorschrift zur Vermeidung und Bekämpfung der Korruption in der Verwaltung (VV), vorgelegt von der Antikorruptionsstelle (AKS) des Senators für Finanzen, hingewiesen.

Nach der VV sind besondere Bestimmungen für das öffentliche Auftragswesen vorgesehen, insbesondere

- Schaffung einer Melde- und Informationsstelle für Vergabestellen beim Senator für Finanzen
- Anfragen daraus durch die Vergabestellen und
- der Ausschluss vom Wettbewerb bis zu sechs Monaten.

Weil Bremen ein Gesetz über die Vergabe von Bauaufträgen aufgrund des § 97 Abs. 4 GWB schaffen will, habe ich angeregt, die Verarbeitung personenbezogener Unternehmerdaten dort zu regeln. Dem soll nunmehr entsprochen werden. Ich habe auch angeregt, eine Regelung zum Ausschluss vom Wettbewerb bei Korruption zu schaffen. Der Senator für Finanzen hat mitgeteilt, es sei die Einbringung eines Registergesetzes für ein Bundeszentralregister über den Bundesrat beabsichtigt, so dass es zunächst bei der Regelung für eine Melde- und Informationsstelle für Vergabestellen in der VV bleiben soll.

11.5. Veröffentlichung einer Prüfungsmitteilung im behördeneigenen Netz

Ich bin darauf hingewiesen worden, das der Bremer Baubetrieb eine interne vorläufige Prüfungsmitteilung des Bundesrechnungshofs im "Mitarbeiter-Informationssystem" (MIS) im behördeneigenen Netz veröffentlicht hat. Die Prüfungsmitteilung ist von der Oberfinanzdirektion Bremen an den Bremer Baubetrieb versandt und mit einem Vermerk versehen worden, der darauf hinweist, dass eine Veröffentlichung der Mitteilung an Dritte unzulässig ist und nur an Stellen bzw. Personen weitergeleitet werden darf, die dazu Stellung zu nehmen haben. Die Prüfungsmitteilung enthält eine Vielzahl personenbezogener Daten über Beschäftigte und sonstige Beteiligte an den geprüften Bauvorhaben. Durch die Veröffentlichung haben ca. 200 Beschäftigte des Bremer Baubetriebes die Möglichkeit zur Kenntnisnahme, den Bericht auszudrucken und beliebig damit zu verfahren erhalten.

Der Bremer Baubetrieb hat mitgeteilt, er habe die interne Veröffentlichung noch am selben Tage meines Schreibens aus dem MIS herausgenommen.

12. Finanzen

12.1. Chipsmobil

Der Senator für Finanzen hat vom Senat den Auftrag zur Erneuerung des bremischen Haushalts-, Kassen- und Rechnungswesens (HKR) erhalten. Zur Umsetzung dieses Auftrags wurde das Projekt CHIPSMOBIL (Controlling, Haushalt, Integration, Planung, Standard, Modular, Online, Buchführung, Informatik, Logistik) aufgesetzt. Meine grundsätzlichen datenschutzrechtlichen Anforderungen habe ich bereits im letzten Bericht (vgl. 22. JB, Ziff. 21.1.) dargestellt.

Während der schwerpunktmäßig in diesem Berichtsjahr abgearbeiteten Phase 2 des Projektes wurden Projektziele konkretisiert und die konzeptionellen Grundlagen geschaffen, die in den folgenden Projektphasen umgesetzt werden sollen (Business Blueprints).

Von den in dieser Phase erarbeiteten Fachkonzepten, die sich insbesondere mit der Dokumentation der Organisationsstruktur und der Definition der Geschäftsprozesse beschäftigen, war ich neben der Qualitätssicherung in folgenden Arbeitsgruppen vertreten bzw. habe entsprechende Schwerpunkte gesetzt:

- Kosten- und Leistungsrechnung und Controlling
- Basiseinrichtung IT-Konzeption
- Berechtigungskonzept
- Datenschutzkonzept.

Die Konzeptionen dieser Fachbereiche bilden zusammen mit dem noch zu erstellenden CCC- (Customer Competence Center) und Betreiberkonzept wesentliche Grundlagen einer datenschutzgerechten Systemgestaltung

Kosten- und Leistungsrechnung (KLR) und Controlling: Die KLR dient der Erzielung von Kostentransparenz und der Erreichung eines kostenbewussten Handelns bei den Beschäftigten in der Verwaltung und den Eigenbetrieben und ist Grundlage für die Budgetierung von Mitteln sowie zur Leistungsverrechnung gegenüber Kostenträgern (vgl. 21. JB, Ziff. 17.3.).

Das Modul, das zur Kosten- und Leistungsrechnung bzw. zum Controlling in CHIPSMOBIL enthalten ist, bereitet in diesem Projekt datenschutzrechtliche Probleme.

Während das im 21. Jahresbericht beschriebene Verfahren darauf abstellte, die KLR in dezentralen Einrichtungen zu nutzen, ist nunmehr im Rahmen des Projektes CHIPSMOBIL eine zentrale oder eine weitgehend zentrale KLR (in KLR-Service-Centern) vorgesehen. Da die KLR notwendigerweise auf die Originaldaten zugreifen muss, würde sie einen umfassenden Blick auf alle rechnungsrelevanten Daten der Freien Hansestadt Bremen haben. Damit hätte, um nur ein Beispiel zu nennen, die zentrale KLR die Möglichkeit ihren Fokus auf die Bürger -soweit sie Schuldner oder Gläubiger sind- zu richten und damit einen übergreifenden Einblick in deren Verhalten zu gewinnen. In intensiven

Gesprächen mit den zuständigen Projektverantwortlichen sind die datenschutzrechtlichen Belange erörtert worden. Es ist nunmehr in dem Blueprint zur KLR festgeschrieben, dass die KLR so eingerichtet wird, dass personenbezogene Daten (bzw. das entsprechende Feld) weder bei den Debitoren noch bei den Kreditoren dargestellt werden.

Basiseinrichtung IT-Konzeption: Die datenschutzrechtlichen Schwerpunkte lagen hier

- bei der Beurteilung der Sicherheit der von SAP zur Verfügung gestellten Passwortmechanismen und
- bei der Sicherung der Vertraulichkeit der Daten, die über das Bremer Verwaltungsnetz transportiert werden.

Bei den Passwortmechanismen stellte sich insbesondere die Frage, ob die Verschlüsselung der Passworte über den von SAP zur Verfügung gestellten Hash-Algorithmus als angemessen sicher einzustufen ist. Angemessen sicher heißt hier, mit welchem Aufwand durch vorstellbare Attacken auf das Bremer Verwaltungsnetz (insbesondere Abhör-und Replayattacken) ausgelesene Hashwerte von Passworten auf die Originalpassworte zurückgerechnet oder als Hashwert wiederverwendet werden können und wie groß das Gefährdungspotential für die zu schützenden Daten dann wäre. Eine abschließende Bewertung dieses Problems konnte bis Redaktionsschluss nicht erfolgen. Hiervon hängt aber ab, ob der Authentifikationsdialog zu verschlüsseln ist.

Ich halte eine starke Authentifizierung insbesondere zur Absicherung des durch die Berechtigungsstruktur vorgegebenen Handlungsrahmens im System für erforderlich. Da die Daten im SAP-System im Klartext über das Netz übertragen werden, halte ich darüber hinaus die Bereitstellung einer Möglichkeit für erforderlich, sensible Inhaltsdaten zu verschlüsseln. Dies wäre u. a. durch die Bereitstellung eines Zusatzproduktes über die SNC-Schnittstelle (Secure network communications) von SAP zur Ankopplung externer Sicherheitsprodukte möglich.

Sowohl die Benutzerauthentifizierung als auch die über Netzverbindungen übertragenen sensiblen personenbezogenen Daten könnten so mithilfe kryptographischer Methoden geschützt werden. Aber auch andere Verschlüsselungsverfahren, wie der Rückgriff für die Verschlüsselung der Daten von der Benutzerschnittstelle (SAPGUI) zum Server auf die in Windows 2000 bereits integrierte SNC von Kerberos sowie eine Router-zu-Router-Verschlüsselung auf IP-Ebene durch VPN-Technologie (IPSEC) wären denkbar und werden momentan diskutiert.

Berechtigungskonzept: Das SAP/R3-Berechtigungskonzept ermöglicht den Schutz vor unzulässigen Zugriffen auf Daten, Transaktionen und Programme. Hierfür ist es erforderlich, enge und trennscharfe Definitionen erforderlicher Rollen im System vorzunehmen. Datenschutzrechtlich sind zwei Ebenen dieser Struktur zu betrachten:

Festlegungen in den einzelnen Fachbereichen: Hier geht es um die Festlegung, welche AnwenderInnen welche Aufgaben im System vornehmen dürfen. Das definierte Ziel in dem zuletzt mir vorliegenden Entwurf des bremischen Berechtigungskonzeptes

(Version 1.4) ist es, Berechtigungsmatrixen zu erstellen, die durch die Fachabteilungen verifiziert werden. Der Zuschnitt der Rollen (vergebene Berechtigungen) muss dem Aufgabenvolumen entsprechen.

Organisation der Berechtigungsadministration: Hierzu bestehen die Möglichkeiten, eine zentrale Organisation innerhalb eines Basisbereiches oder eine Zuordnung von Teilbereichen der Administration an dezentrale Stellen vorzunehmen. Im Rahmen der von der Arbeitsgruppe favorisierten dezentralen Struktur wird die Zuordnung einer zentral angelegten Systemnutzung zu einem bestimmten Berechtigungsprofil in der Fachabteilung eigenverantwortlich vorgenommen. Ein Vier-Augen-Prinzip soll hierbei ein transparentes und kontrolliertes Verfahren sicherstellen. Berechtigungsänderungen sollen dann an einer zentralen Stelle auf Anforderungen der Fachabteilungen vorgenommen werden. Die Meldung dieser Anforderungen unterliegt dann einem klar vorgegebenen Verfahren, das adäquate Kontrollmechanismen zur Überprüfung der Rechtmäßigkeit der Anforderungen enthält.

Für die Verwaltung von Berechtigungen schlägt SAP selbst ein Sechs-Augen-Prinzip vor, d. h. die Wahrnehmung der erforderlichen Funktionen durch drei verschiedene Rollen: Den Benutzerverwalter (legt Benutzerstammsätze fest), den Berechtigungsverwalter (legt Profile und Berechtigungen an und pflegt sie) und den Aktivierungsverwalter (aktiviert Profile und Berechtigungen). Das momentan favorisierte Modell im Berechtigungskonzept dezentralisiert neben der Aktivierung von Profilen und Berechtigungen auch noch deren Verknüpfung mit den zentral angelegten Benutzerstammsätzen.

Sowohl die inhaltliche Rollenaufteilung als auch die Teildezentralisierung der Verwaltungsaufgaben stellt ein datenschutzgerechtes Verfahren dar. Wesentlich für die Organisation eines ordnungsgemäßen Ablaufes sind darüber hinaus noch folgende Definitionen:

Es ist eine systemübergreifende Festlegung der Administrationsrechte und Sonderrollen (wie z. B. SAP*, S-Develop, DDIC etc.) zu treffen, denn mit ihnen sind umfassende Veränderungsrechte im System verbunden.

Ein Überwachungsverfahren ist einzurichten, über das die Korrektheit der Berechtigungsstruktur im System jederzeit unter bestimmten Selektionsaspekten überprüft werden kann und das bereits bei der automatisierten Generierung von Berechtigungen und Profilen durch den Profilgenerator möglicherweise zu umfangreiche oder redundant vergebene Berechtigungen abfängt. Weiter sind Schutzmechanismen für das vom System angebotene Audit-System (AIS) vorzusehen. Es sind nämlich Auswertungen außerhalb der SAP-Berechtigungsstruktur möglich. Satzaufbau, Selektions-und Sortierkriterien müssen transparent von der Revision definiert werden.

Insgesamt sind die Berechtigungen für Reports (Auswertungen über den Datenbestand) in der Form einschränkend zu handhaben, damit es an keiner Stelle zu zentralen personenbezogenen Auswertungen kommen kann.

Datenschutzkonzept: Die mit mir im Rahmen der Arbeitsgruppe zur Erstellung des Berechtigungskonzeptes entwickelte erste Grundstruktur enthält im Wesentlichen die o. g. Aspekte.

Darüber hinaus halte ich es aufgrund der komplexen Struktur des Gesamtprojektes für erforderlich, zentrale Datenschutz- und -sicherungsmaßnahmen in ihren Einzel- und Wechselwirkungen insgesamt darzustellen. Das bedeutet insbesondere, die Einzelmaßnahmen der Arbeitspakete Berechtigungsstruktur, IT-Konzept und CCC-Betreiberkonzept (in dem u. a. die Organisation der Systementwicklung, Absicherung des Qualitätssicherungssystems, innerhalb dessen mit Produktionsdaten gearbeitet wird, über denen keine Berechtigungsstruktur liegt) gesamtübersichtlich darzustellen.

Da die SAP-Sicherheit sich lediglich auf die Anwendungsebene bezieht (Anwendungsmodule, R/3 Berechtigungssystem) und damit nur einen Teilbereich der Sicherheitsstruktur abdeckt, bedeutet es auch, die Ebenen der Kommunikation (Netzwerk, Firewall, SAP-Router), die Datenbank (Zugangskontrolle zu den Verwaltungsfunktionen der Datenbank) und die zugrunde liegenden Betriebssysteme zu betrachten.

Die endgültige Abwägung der Verhältnismäßigkeit der von mir zu fordernden technischen Maßnahmen kann noch nicht eindeutig erfolgen, da bisher keine Risikoanalyse unter Einbeziehung der beteiligten Systemkomponenten und deren Interaktion erfolgt ist.

Vor dem Hintergrund deshalb nicht abschließbar zu bewertender Risiken habe ich an den Senator für Finanzen im Rahmen der von mir begleiteten Gremien die Erwartung fomuliert, dieser Unsicherheit mit einem entsprechend hohen Schutzniveau zu begegnen. Darüber hinaus habe ich empfohlen, bereits im Verlauf des Projektes zu prüfen, ob entsprechende gesetzliche Grundlagen verändert werden müssen.

12.2. Abgabenordnung

Auskunft und Einsicht in Steuerakten: Die Abgabenordnung (AO) enthält keine eindeutigen Regelungen über die Auskunft und die Einsicht in Akten der Steuerverwaltung. Gemäß § 91 i. V. m. §364 AO können die Steuerbehörden dem Betroffenen Einsicht in ihre Steuerakte nach pflichtgemäßen Ermessen gewähren. Ein solcher Einsichtsantrag ist demnach nicht von vornherein unzulässig. Bei der Ausübung des Ermessens hat die Behörde einen weiten Entscheidungsrahmen, sie darf von dem Ermessen jedoch nicht fehlerhaft Gebrauch machen und keine sachfremden Argumente anführen.

Im Berichtszeitraum habe ich in zwei Fällen Bürger über ihre rechtliche Situation unterrichtet, die daraufhin selbständig von ihren Rechten Gebrauch gemacht haben. In einem Fall hat mich der Auskunftsbegehrende von dem Erfolg seiner Bemühungen unterrichtet.

Es wäre wünschenswert, wenn für die Steuerverwaltung die gleichen Rechtsvorschriften über die Akteneinsicht und die Auskunft wie für andere Verwaltungszweige (einschl. der Polizei) gelten würden. Ich unterstütze daher die darauf gerichteten Bemühungen der Bundesregierung.

Führung von Fahrtenbüchern durch Ärzte: Über die Verpflichtung der Ärzte zur umfassenden Dokumentation ihrer Fahrten zur steuerlichen Abgrenzung von privaten Fahrten zu geschäftlichen Fahrten und der damit einhergehenden Durchbrechung der ärztlichen Schweigepflicht habe ich schon früher berichtet (vgl. 20. JB, Ziff. 18.2.).

Nach Intervention der Datenschutzbeauftragten in Bund und Ländern hat das Bundesfinanzministerium seinen damaligen Erlass revidiert. Der neue Erlass schreibt zwar weiterhin vor, dass die Ärzte zur umfassenden Dokumentation verpflichtet sind, allerdings mit der Maßgabe, dass die Patientendaten in einem Extraverzeichnis geführt werden können, mit dem die Fahrtenbuchaufzeichnungen bei einer Betriebsprüfung vervollständigt werden können.

Automation und Steuerverwaltung: Im Zuge der DV-technischen Fortentwicklung in Wirtschaft und Verwaltung wurde die AO (§ 147 Abs. 6 AO) im letzten Jahr angepasst. Diese Änderung erfolgte durch Artikel 7 des Steuersenkungsgesetzes vom 26. Okt. 2000 (BGBl. S. 1460). Ab dem 1. Januar 2002 wird es den Steuerbehörden möglich sein, während der Aufbewahrungsfirst von steuerrechtlichen Unterlagen (Buchführungsunterlagen) von Unternehmen, die ihre Buchhaltung auf DV-Systemen verarbeiten und archivieren, zu verlangen, dass die Unterlagen jederzeit verfügbar, unverzüglich lesbar gemacht und maschinell auswertbar sind. Darüber hinaus ist den Betriebsprüfern im Rahmen der Außenprüfung das Recht einzuräumen, die Datenverarbeitungssysteme des Betriebes zu benutzen, Daten nach ihren Vorgaben auszuwerten und gespeicherte Unterlagen auf maschinell verwertbaren Datenträgern vom Betrieb zu erhalten.

Diese Rechtsänderung erfordert in vielen Betrieben eine rechtzeitige Trennung der Daten in den eigenen DV-Systemen, damit "nicht-steuerrechtliche“ Daten (reine Personaldaten, Entwicklungsdaten usw.), die auf DV-Systemen auch gespeichert sind, nicht in die DV-Systeme der Steuerverwaltung übertragen werden.

Steuerdatenabrufverordnung: Die Steuerdatenabrufverordnung, die auf Grund von § 30 Abs. 6 AO seit Jahren überfällig ist, soll auf Vorschlag des bremischen Finanzsenators im Hinblick auf das Forschungsprojekt MEDIA@Komm um die Möglichkeit des Abrufs der eigenen Steuerdaten durch den Steuerschuldner (oder seines Bevollmächtigten) ergänzt werden. Dafür ist es aus Sicht des Datenschutzes erforderlich, eine ausreichende Daten- und Authentitätssicherung durch eine qualifizierte elektronische Signatur und sichere Übertragungen zu gewährleisten.

12.3. FIDATAS Bremen "Ein neuer Eigenbetrieb"

Die Freie Hansestadt Bremen beabsichtigt einen neuen Eigenbetrieb mit dem Namen FIDATAS Bremen zu errichten. Dieser Eigenbetrieb soll als DV-Dienstleistungseinrichtung für die Finanzbehörden gegründet werden. Gleichzeitig wird der "Rest“eigenbetrieb der ID Bremen (siehe Ziff. 3.3. des 22. JB) in FIDATAS übertragen und übernimmt dessen Aufgaben in Bezug auf die ID Bremen GmbH als "Aufsichtsführende Stelle“. Der

neue Eigenbetrieb wird örtliche Finanzbehörde und für die Aufgabenerfüllung nach §2 Abs. 2 des Finanzverwaltungsgesetzes zuständig.

Damit wird die "Automationsabteilung“ der ehemaligen Oberfinanzdirektion in den Eigenbetrieb überführt.

Durch diese rechtliche Konstruktion wird die Datenverarbeitung für Hoheitsbereiche (z. B. Steuern und Justiz) wieder näher an die Verwaltung angelehnt. In die Entwicklung war ich beratend mit einbezogen. Diese Rechtsform wird von mir ausdrücklich begrüßt, weil die Verantwortlichkeiten und die Kontrolle eindeutiger geregelt sind. Gleichwohl werde ich nach Aufnahme des Betriebes eine eingehende Prüfung bezüglich der Abschottung der einzelnen Verfahren vornehmen.

12.4. Bremer Investitions-Gesellschaft

Die Bremer Investions-Gesellschaft mbH (big) ist die Dachgesellschaft der (land)bremischen Fördergesellschaften (wie z. B. Wirtschaftsförderungsgesellschaft (WfG) oder Bremerhavener Gesellschaft für Investitionsförderung und Stadtentwicklung (BIS). Bereits zum Zeitpunkt der Gründung der big wurde erkannt, dass zur Aufgabenerfüllung der big und ihrer zahlreichen Töchter eine leistungsfähige DV-Infrastruktur erforderlich sei. Diese ist erforderlich, um die Daten des erheblichen Fördervolumens zu verarbeiten und mit anderen Stellen auszutauschen.

Im Sommer letzten Jahres ist die big an mich herangetreten, um ein Datenschutzkonzept für die vielfältigen Arbeitsschritte in der big und ihren Töchtern zu erstellen. In diesem Zusammenhang habe ich ihr datenschutzrechtliche Hinweise für eine Gestaltung der Datenverarbeitung und den Betrieb des big-Rechenzentrums gegeben. Es handelt sich um ein komplexes System, dass umfassende organisatorische Abgrenzungen und entsprechende technische Umsetzungen erfordert. Die Arbeiten sind noch nicht abgeschlossen.

12.5. Kampfhunde, kupierte Hunde und ihre Halter

Hunde spielten im Berichtszeitraum aus zwei verschiedenen Gesichtspunkten datenschutzrechtlich eine Rolle.

Kampfhunde und Steuergeheimnis: Aufgrund der publizierten Vorfälle mit Kampfhunden kam es zu der besonderen Fragestellung, ob die Identität des Hundehalters nach einem Schadensfall durch die Steuerverwaltung (in Bremen dem Finanzamt Bremen-Mitte) offenbart werden darf. Gemäß § 30 Abgabenordnung der für alle Steuerarten gilt, war auch die Identität des Steuerpflichtigen (Halter des Hundes) geschützt. Für eine Offenbarung war keine Befugnisnorm vorhanden.

Diesem Umstand hat der Gesetzgeber in Bremen Rechnung getragen und in § 3 Abs. 1 Nr. 1 des Bremischen Abgabengesetzes eine entsprechende Rechtsnorm (BremGBl. Nr. 47 vom 27. Sept. 2000) eingefügt, die die Offenbarung der Daten des Halters eines

Hundes (Name und Anschrift) durch den Steuerbeamten an Behörden und Schadensbeteiligte zulässt, wenn ein Schaden durch den Hund eingetreten ist.

Kupierte Hunde: Ein Hundezüchter außerhalb des Landes Bremen beschwerte sich darüber, dass die Veterinärbehörde Bremen, die u. a. für den Tierschutz zuständig ist, Daten an die zuständige Tierschutzbehörde an seinem Wohnsitz übermittelt habe. Diese Daten hatte das bremische Veterinäramt erhalten, als es bei einer Prüfung anlässlich einer Hundeschau in Bremen auf den Hund des Hundezüchters traf, der eine kupierte Rute gehabt hat. Das Kupieren der Rute von Hunden ist nach dem Tierschutzgesetz i. d. F. vom 25. Mai 1998 (BGBl. S. 1105) grundsätzlich verboten. Aus diesem Grunde war die bremische Tierschutzbehörde auch zur Erhebung - und da sie für den Hundehalter räumlich nicht zuständig war - auch zur Übermittlung an die Tierschutzbehörde des Wohnsitzes des Hundehalters befugt. Ob die Ausnahmetatbestände des § 6 Tierschutzgesetzes, der in bestimmten Fällen das Kupieren der Rute zulässt auch auf den Hund des Eingebers zutrifft, kann nur die zuständige Tierschutzbehörde feststellen. Datenschutzrechtlich war das Verhalten der bremischen Tierschutzbehörde nicht zu beanstanden.

13. Wirtschaft und Häfen: Neues Bremisches Hafenbetriebsgesetz

2001 ist das neue Bremische Hafenbetriebsgesetz vom 21. November 2000 (BremGBl S. 437) in Kraft getreten. Dieses Gesetz löst das bisherige Hafengesetz ab. Eine Überarbeitung war erforderlich, weil durch die strukturelle Fortentwicklung in den bremischen Häfen und die Veränderung der Zuständigkeiten die bisherige Rechtsvorschrift in großen Teilen hätte neuformuliert werden müssen. Gleichzeitig wurden zwei Aufgabenfelder (Seeschiffassistenz und Beleihung von Dritten mit der Erhebung von Abgaben) neu gestaltet.

Das neue Bremische Hafenbetriebsgesetz hat die datenschutzrechtlichen Standards erhalten. Die bereichsspezifischen Rechtsvorschriften sind nicht geändert worden. Auch in den Entwürfen der neuen Hafenordnung und der Hafeninformatonsverordnung sind keine wesentlichen Veränderungen enthalten. Meine frühzeitige Beteiligung an den verschiedenen Rechtsvorschriften ist positiv zu erwähnen.

14. Radio Bremen: Rundfunkgebühreneinzug

Gegenstand meiner Prüftätigkeit war im abgelaufenen Jahr auch die Durchführung des Staatsvertrags über die Rundfunkgebühren (RfGebStV). Veranlasst zur Überprüfung sah ich mich u. a. durch Anfragen und Eingaben aus Bremen und Bremerhaven. Die Bürger verwunderten sich insbesondere darüber, dass sie von der mit dem Rundfunkgebühreneinzug beauftragten Gebühreneinzugszentrale (GEZ) wegen der Erfüllung ihrer Gebührenpflicht angeschrieben worden waren. Die Bürger erklärten, sie hätten ihre Gebühren korrekt bezahlt oder aber sie seien gar nicht gebührenpflichtig.

Die Überprüfung verschiedener Eingaben ergab, dass die Petenten ihre Zuschriften im Rahmen sog. Mailing-Aktionen der GEZ erhalten hatten, von denen insbesondere Personen betroffen sind, die nur ein Hörfunk- aber kein Fernsehgerät oder aber gar kein Empfangsgerät bei der GEZ angemeldet haben. Den übersandten Anschreiben waren von der GEZ Fragebögen beigefügt worden, in denen die Betroffenen Angaben zu ihrer spezifischen häuslichen Situation machen sollten. Neben den Fragen enthielten die Fragebögen auch einen Hinweis, auf eine für die Betroffenen bestehende Auskunftsverpflichtung, die sich aus § 4 Abs. 5 RfGebStV ergebe. Auch der Inhalt der Anschreiben selbst erweckte den Eindruck, als seien die Betroffenen zur Auskunft verpflichtet.

Unbeachtet bei den stets an große Personengruppen gerichteten Mailing-Aktionen blieb, dass Voraussetzung für die Pflicht zur Erteilung von Auskünften nach § 4 Abs. 5 RfGebStV das einzelfallbezogene Vorliegen konkreter Anhaltspunkte beim Rundfunkteilnehmer oder aber einer anderen Person dafür ist, dass ein Rundfunkempfangsgerät zum Empfang bereitgehalten wird und nicht oder nicht umfassend entsprechend der Anzeigepflicht bei der Landesrundfunkanstalt bzw. der GEZ angezeigt worden ist. Konkrete Anhaltspunkte für einen Verstoß gegen die Anzeigepflicht wurden bei den mir zugestellten Eingaben nicht dargelegt, eine Auskunftsverpflichtung war nach meiner Auffassung deshalb nicht gegeben.

Außerdem stieß bei mir auch der Umfang der Angaben auf Kritik, die mit den übersandten Fragebögen erhoben werden sollten. Nach § 4 Abs. 5 RfGebStV darf nur Auskunft über diejenigen Tatsachen verlangt werden, die Grund, Höhe und Zeitraum der Gebührenpflicht betreffen. Eine negative Auskunftspflicht, d. h. eine Auskunftspflicht über das Nichtvorhandensein von Geräten, wie sie die den Betroffenen übersandten Fragebögen enthielten, ergibt sich hieraus - auch nach der Auffassung anderer Landesdatenschutzbeauftragter - nicht. Wird kein gebührenpflichtiges Gerät betrieben, so besteht aus meiner Sicht für den Bürger keine Verpflichtung, dieses der Landesrundfunkanstalt bzw. der GEZ anzuzeigen oder aber hierüber nach § 4 Abs. 5 RfGebStV Auskunft zu erteilen.

Ich habe gegenüber Radio Bremen eine grundlegende Veränderung der für die Mailing-Aktionen verwendeten Anschreiben und Fragebögen angeregt. Während Radio Bremen sich für eine Veränderung der verwendeten Formulare aufgeschlossen zeigte, allerdings nicht isoliert vorgehen wolle, vertrat der Sender hinsichtlich des Umfangs des Auskunftsanspruchs wie die übrigen Rundfunkanstalten die Auffassung, dass vom Rundfunkteilnehmer auch Angaben darüber zu machen seien, ob und in welchen Zeiträumen kein Rundfunkgerät zum Empfang bereitgehalten worden ist.

Die konträre Rechtsauslegung könnte durch Klarstellung der rechtlichen Regelungen oder durch die Rechtsprechung aufgelöst werden.

Weitere Eingaben erhielt ich im Hinblick auf die für Radio Bremen tätigen Rundfunkgebührenbeauftragten und ihre umfangreichen Datenkenntnisse. Die Gebührenbeauftragten erhalten von der GEZ im Auftrag Radio Bremens umfangreiches Listenmaterial mit Daten über die gemeldeten Rundfunkteilnehmer. Zu ihren Aufgaben gehört es u. a.

Rundfunkteilnehmer zur Anmeldung der von ihnen betriebenen Empfangsgeräte sowie zur Zahlung von Rundfunkgebühren zu veranlassen.

Aus datenschutzrechtlicher Sicht ist zu kritisieren, dass es für die Übermittlung der Daten an die Gebührenbeauftragten keine ausreichende Rechtsgrundlage gibt. Ich regte gegenüber Radio Bremen an, neben einer Begrenzung des den Beauftragten zur Verfügung gestellten Datenmaterials auf den tatsächlich erforderlichen Umfang in die Tätigkeitsvereinbarung mit den Gebührenbeauftragten eine Passage hinsichtlich des Datenschutzes und der Überlassung von Teilnehmerdaten aufzunehmen. Außerdem empfahl ich zur Vermeidung eines evtl. Datenmissbrauchs weitere Regelungen zum sachgerechten Umgang mit Teilnehmerdaten in die Tätigkeitsvereinbarung aufzunehmen. Radio Bremen sagte eine wohlwollende Überprüfung der Angelegenheit zu.

Insgesamt gesehen, wurde aus den von mir bearbeiteten Bürgereingaben deutlich, dass sich aus dem bestehenden System der Erhebung von Rundfunkgebühren für das informationelle Selbstbestimmungsrecht des betroffenen Bürgers Probleme ergeben können. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat in ihrer Sitzung am 12. und 13. Oktober 2000 in Braunschweig im Zusammenhang mit der Diskusion um eine Neuregelung der Rundfunkfinanzierung einen Beschluss gefasst, in dem sie die Bundesländer auffordert, bei einer Neuordnung der Rundfunkfinanzierung ein Modell zu Grunde zu legen, dass sich stärker als das bisherige an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert (vgl. Ziff. 19.9. des JB).

15. Bremerhaven

Da es sich anbietet, viele Themen in einem Sachzusammenhang darzustellen, soll an dieser Stelle nur die Auffindbarkeit erleichtert werden. Die nachfolgend aufgezählten Gliederungspunkte betreffen Themen aus Bremerhaven, sie finden sich unter Ziff. 2.2.2. "Bürgernetz Bremerhaven", 3.2. "Verwaltungsnetz des Magistrats der Seestadt Bremerhaven", 5.5. "Besetzung einer Chefarztstelle im Krankenhaus", 6.3.2. "Neues DV-Verfahren Meso 96 bei der Meldebehörde Bremerhaven", 8.1.1. "Zentralkrankenhaus Reinkenheide", 11.2. "Prüfung des Wohngeldverfahrens" und 11.3. "Videoüberwachung in öffentlichen Verkehrsmitteln".

16. Datenschutz in der Privatwirtschaft

16.1. Datenschutz für Beschäftigte

16.1.1. Datenerhebung mittels Bewerbungsfragebogen

Im Rahmen eines Bewerbungsverfahrens wurde einem Bewerber ein Fragebogen ausgehändigt, in dem u. a. nach dem Empfang von Arbeitslosengeld/-hilfe und Sozialhilfe gefragt wurde.

Aufgrund meiner Anfrage beim Arbeitgeber, zu welchem Zweck diese Daten erforderlich sind, hat er den Fragebogen überarbeitet, so dass diese Angaben nicht mehr erhoben werden.

16.1.2. Datenverarbeitung durch den Betriebsarzt

Der Betriebsrat eines Metall verarbeitenden Betriebes hat mich gebeten, den Entwurf einer Betriebsvereinbarung hinsichtlich der Datenverarbeitung durch den Betriebsarzt zu prüfen und insbesondere darzulegen, ob der Betriebsarzt befugt ist, Daten über die Krankenkasse, die private Telefonnummer und den Hausarzt der Beschäftigten zu erheben. Fraglich ist auch, ob es sich hierbei um die Daten aller Beschäftigten oder nur derjenigen handeln darf, die Vorsorgeuntersuchungen unterliegen. Des Weiteren hat er mich gebeten darzulegen, ob der Betriebsarzt befugt ist, personenbezogene Daten an den Arbeitgeber weiterzuleiten bzw. welche Anforderungen an die Anonymisierung der Daten zu stellen sind.

Aus datenschutzrechtlicher Sicht sind folgende Problemkreise zu unterscheiden:

Allgemeines zur Datenerhebung und zum Personenkreis: Für die Datenverarbeitung des Betriebsarztes kommt hier § 3 Abs. 1 Nr. 2 Arbeitssicherheitsgesetz (ASiG) in Betracht. Danach hat der Betriebsarzt insbesondere die Arbeitnehmer zu untersuchen, arbeitsmedizinisch zu beurteilen und zu beraten sowie die Untersuchungsergebnisse zu erfassen und auszuwerten. Außerdem hat er nach § Abs. 1 Nr. 3 Buchstabe c Ursachen von arbeitsbedingten Erkrankungen zu untersuchen, die Untersuchungsergebnisse zu erfassen und auszuwerten und dem Arbeitgeber Maßnahmen zur Verhütung dieser Erkrankungen vorzuschlagen.

Dieses Gesetz enthält keine Regelungen, wie er die dafür erforderlichen Daten erheben darf. Also ist hier der allgemeine Grundsatz gemäß § 28 Satz 2 BDSG anwendbar, wonach die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden müssen. Nach diesem Grundsatz sind die Daten grundsätzlich bei dem Betroffenen mit seiner Kenntnis zu erheben. Nur in eng begrenzten Ausnahmefällen ist eine Erhebung ohne seine Mitwirkung zulässig, z. B. wenn eine andere Rechtsvorschrift dies vorsieht (§ 13 Abs. 2 BDSG).

Als andere Rechtsvorschrift käme auch eine Betriebsvereinbarung in Frage (Rechtsprechung des Bundesarbeitsgerichts). Eine weitere Ausnahme wäre gegeben, wenn der Betriebsarzt nicht in der Lage ist, die Daten bei den Arbeitnehmern zu erheben, weil er keine Kenntnis darüber hat, welche Arbeitnehmer sich Vorsorgeuntersuchungen zu unterziehen haben.

Beim Arbeitgeber darf er daher nur die Arbeitnehmerdaten erheben, die zur dienstlichen Erreichbarkeit der Arbeitnehmer erforderlich sind, die Vorsorgeuntersuchungen unterliegen oder die sich direkt an ihn zwecks Beratung gewandt haben. Er benötigt nicht die Daten aller Beschäftigten des Betriebes.

Erhebung des Datums "Krankenkasse": Nach § 15 Abs. 2 Sozialgesetzbuch VII (SGB VII) können die Unfallversicherungsträger Vorschriften über vom Unternehmer zu veranlassende arbeitsmedizinische Untersuchungen erlassen und nach Nr. 5 dieser Vorschrift hierfür auch die Erhebung, Verarbeitung und Nutzung des Datums "zuständige Krankenkasse" vorsehen. Nach dem mir zugesandten Formular "Arbeitsmedizinische Vorsorgeuntersuchungen" wird diese Angabe verlangt. Soweit das Formular vom zuständigen Unfallversicherungsträger (Berufsgenossenschaft) per Unfallverhütungsvorschrift erlassen worden ist, ist die Erhebung durch den Betriebsarzt aufgrund dieser Rechtsvorschrift zulässig.

Nach dem vorgenannten Grundsatz von Treu und Glauben kann der Betriebsarzt dieses Datum entweder bei dem Arbeitnehmer mit seiner Kenntnis oder wenn eine Betriebsvereinbarung es erlaubt, dieses Datum aus einem Personaldatenverarbeitungssystem erheben. Allerdings darf das Datum nur in die vorgesehene ärztliche Bescheinigung aufgenommen werden.

Erhebung des Datums "Private Telefonnummer": Grundsätzlich ist die private Telefonnummer nicht für die Aufgaben des Betriebsarztes erforderlich, so dass sie nur mit Einwilligung des Arbeitnehmers erhoben werden darf. Denkbar könnte sein, dass ein Arbeitnehmer einmal im Einzelfall für den Betriebsarzt außerhalb der Arbeitszeit erreichbar sein muss. Darauf sollte er den Arbeitnehmer hinweisen, der seinerseits dann ohne jeden Zweifel freiwillig entscheiden können muss, ob er dem Betriebsarzt seine private Telefonnummer geben will oder nicht. Eine Aufnahme dieses Datums in das DV-System des Betriebsarztes ist ebenfalls nur mit Einwilligung des Arbeitnehmers zulässig. Die Löschung dieses Datums muss erfolgen, wenn der dafür genannte Zweck entfallen ist.

Erhebung von Daten über den Hausarzt: Auch diese Daten sind für die Aufgaben des Betriebsarztes nicht erforderlich. Allerdings könnte der Betriebsarzt im Rahmen einer Beratung des Arbeitnehmers anregen, sich mit dessen Hausarzt in Verbindung zu setzen, um insoweit die Behandlung durch den Hausarzt zu unterstützen. In einem solchen Einzelfall muss der Betriebsarzt den Arbeitnehmer über den Zweck informieren, damit dieser ohne jeden Zweifel freiwillig entscheiden kann, ob er dem Betriebsarzt Name und Anschrift seines Hausarztes mitteilen und ihn von der ärztlichen Schweigepflicht entbinden will.

Die Einwilligung bedarf nach § 4 Abs. 1 BDSG der Schriftform. In der Einwilligungserklärung muss der Zweck für die wechselseitige Entbindung von der Schweigepflicht gegenüber Hausarzt bzw. Betriebsarzt präzise benannt werden. Eine Aufnahme in das DV-System des Betriebsarztes ist in gleicher Weise nur aufgrund der schriftlichen Einwilligung des Arbeitnehmers zulässig. Sobald die Daten des Hausarztes für den in der Erklärung zur Schweigepflichtentbindung genannten Zweck nicht mehr erforderlich sind, müssen sie beim Betriebsarzt gelöscht werden.

Datenübermittlung an den Arbeitgeber durch den Betriebsarzt: Nach § 8 Abs. 1 ASiG haben die Betriebsärzte die Regeln der ärztlichen Schweigepflicht zu beachten.

Insoweit ist § 203 Abs. 1 Nr. 1 Strafgesetzbuch beachtlich, wonach sich strafbar macht, wer unbefugt ein fremdes Geheimnis offenbart, das ihm als Arzt anvertraut oder sonst bekannt geworden ist. Eine Befugnis des Betriebsarztes, personenbezogene Daten ohne Einwilligung der untersuchten Arbeitnehmer an den Arbeitergeber zu übermitteln, ergibt sich ausschließlich aus den einschlägigen Vorschriften über Vorsorgeuntersuchungen nach § 15 SGB VII, z. B. zu Durchschriften der Bescheinigungen über Vorsorgeuntersuchungen.

Auswertungen des Betriebsarztes und deren Weiterleitung an den Arbeitgeber: Nach § 3 Abs. 1 c) ASiG hat der Betriebsrat u. a. die Aufgabe, Ursachen von arbeitsbedingten Erkrankungen zu untersuchen, die Untersuchungsergebnisse zu erfassen und auszuwerten und dem Arbeitgeber Maßnahmen zur Verhütung dieser Erkrankungen vorzuschlagen. Eine besondere Einschränkung enthält die Vorschrift nicht. Gleichwohl darf der Betriebsarzt nur die Auswertungen vornehmen, die für die Erfüllung seiner Aufgaben nach diesem Gesetz erforderlich sind.

Das Gesetz enthält keine Befugnis des Betriebsarztes, die im Rahmen seiner Auswertungen verarbeiteten personenbezogenen Untersuchungsdaten an den Arbeitgeber zu übermitteln. Die Untersuchungs- bzw. Auswertungsergebnisse dürfen daher nur anonymisiert an den Arbeitgeber weitergeleitet werden. Daten gelten dann als anonymisiert, wenn ein Personenbezug nicht mehr herstellbar ist.

16.1.3. Betriebsvereinbarung zur Videoüberwachung im Betrieb

Der Betriebsrat eines Speditionsbetriebs im Hafen hat mich um Beratung zu einer im Betrieb vorgesehenen Videoüberwachung gebeten. Zweck der Videoüberwachung ist die Durchsetzung eines absoluten Rauchverbots (Ausnahme in den Sozialräumen), um dadurch Brandgefahren abzuwehren, die den Feuerversicherungsschutz und die Zulassung zur Londoner Börse gewährleisten sollen.

Durch die Videoüberwachung werden die Persönlichkeitsrechte der Arbeitnehmer und Kunden berührt. Hierzu habe ich auf die anstehende Regelung des § 6b Bundesdatenschutzgesetz verwiesen. Zur Wahrung der Persönlichkeitsrechte der Arbeitnehmer habe ich empfohlen, eine Betriebsvereinbarung abzuschließen, die folgende Anforderungen enthalten muss:

Neben dem Zweck zur Erforderlichkeit der Videoüberwachung müssen die zu überwachenden Bereiche präzise festgelegt werden. Die Kameras dürfen nur auf diese Bereiche programmiert und positioniert werden. In den Bereichen müssen deutlich erkennbare Hinweisschilder angebracht werden, damit überwachte Personen von der Videoüberwachung und -aufzeichnung rechtzeitig Kenntnis nehmen können.

Um Missbrauchsmöglichkeiten auszuschließen bzw. zumindest erheblich zu erschweren, sollten der Zugriff durch die dazu berechtigten Personen nur nach dem "Vier-Augen-Prin-

zip" zulässig sein, z. B. durch die Benutzung von zwei Passwörtern etc. und Auswertungen protokolliert werden.

Des Weiteren sollten die Daten bereits nach 24 Stunden automatisch gelöscht werden, wenn keine Vorkommnisse eingetreten sind, die eine rechtmäßige Verwertung erforderlich machen. Eine Verwendung des Videoüberwachungssystems zu Zwecken der Leistungskontrolle ist auszuschließen.

16.1.4. Überwachung der Mitarbeiter beim "Surfen" im Internet

Unternehmen fragten bei mir an, in welchem Umfang sie ihre Mitarbeiter beim "Surfen" überwachen dürfen, ohne gegen geltendes Recht zu verstoßen.

Ich habe den Unternehmen mitgeteilt, dass normenklare gesetzliche Regelungen zur Überwachung von Mitarbeitern beim "Surfen" im Internet durch den Arbeitgeber derzeit nicht bestehen. Es ist jedoch beabsichtigt, noch in dieser Legislaturperiode des Deutschen Bundestages ein Arbeitnehmerdatenschutzgesetz zu schaffen. Aus diesem Grunde gilt für die Verarbeitung von Arbeitnehmerdaten derzeit nur die Vorschrift des § 28 BDSG.

Nach § 28 Abs. 1 Nr. 2 BDSG ist die Verarbeitung personenbezogener Daten zulässig, soweit sie zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Daraus ergibt sich bei der Überwachung der Mitarbeiter beim "Surfen" im Internet, dass abgewogen werden muss zwischen den berechtigten Interessen des Arbeitgebers und den schutzwürdigen Interessen der Mitarbeiter.

Es empfiehlt sich, in einer Betriebsvereinbarung festzulegen, ob und ggf. zu welchem Zweck, in welchem Umfang durch wen eine Datenverarbeitung stattfinden darf. Die Betriebsvereinbarung muss die genannte Abwägung sowie weitere gesetzliche Anforderungen beachten. Insbesondere gilt dies, wenn den Mitarbeitern erlaubt bzw. nicht ausdrücklich untersagt wird, Internet und E-Mail auch privat zu nutzen.

Nach meinen Erfahrungen wird ein Verbot privater Nutzung nicht vollständig einzuhalten sein. Außerdem kann niemand verhindern, dass über die persönlichen E-Mail-Adressen nicht nur betriebliche sondern auch private E-Mails eingehen. Jedenfalls dann, wenn den Mitarbeitern die private Nutzung erlaubt wird, werden insoweit Teledienste und Telekommunikationsdienstleistungen durch den Arbeitgeber geschäftsmäßig erbracht, so dass sowohl das Teledienstedatenschutzgesetz (TDDSG) und der Mediendienste-Staatsvertrag als auch die einschlägigen Vorschriften über das Fernmeldegeheimnis nach dem Telekommunikationsgesetz (TKG) einzuhalten sind, nämlich §§ 3 Nr. 5, 85 TKG. Der Arbeitgeber nimmt gegenüber dem Arbeitnehmer Provider-Funktionen wahr, da das Vermitteln von Internetdiensten zu privaten Zwecken als ein geschäftsmäßiges Erbringen von Diensten für Dritte zu werten ist.

Daraus ergibt sich, dass der Arbeitgeber weder protokollieren darf, auf welche Internetseiten die einzelnen Beschäftigten zugegriffen haben, noch stichprobenhafte Mitschnitte von aufgerufenen Seiten machen darf. Es sind lediglich Statistiken über die Nutzungshäufigkeit einzelner Seiten zulässig. Erst wenn hierüber bemerkbar wird, dass auf rechtswidrige Seiten aus dem Unternehmensnetz heraus zugegriffen wird, sollte im Einvernehmen mit der Personalvertretung eine mitarbeiterbezogene Protokollierung für einen begrenzten Zeitraum aktiviert werden.

16.1.5. Videoüberwachung am und im Gebäude

Ein Betroffener als Arbeitnehmer einer Einrichtung, die in einem Gebäude als Mieterin untergebracht ist, wandte sich gegen den Einsatz von Videokameras, die an und in dem Gebäude (in den Flureingängen) angebracht sind. Dadurch sei die perfekte Überwachung und Analyse der Verhaltensweisen Einzelner möglich.

Nach Besichtigung der Videoüberwachung vor Ort und der Erörterung mit dem Eigentümer des Gebäudes habe ich ihn darauf hingewiesen, dass derzeit keine gesetzliche Erlaubnis zum Einsatz von Videoüberwachung bestehe, hierzu jedoch die Rechtsprechung des Bundesgerichtshofs (BGH) zu beachten sei (s. a. 21. JB, Ziff. 16.1. zu Videoüberwachung in Großwohnanlagen).

Nach Abwägung der berechtigten Interessen des Eigentümers, Einbrüchen vorbeugen zu wollen und den schutzwürdigen Interessen der Besucher des Gebäudes, in dem sich mehrere Einrichtungen befinden, hat der Eigentümer meinen Vorschlag akzeptiert, die Videoüberwachung im Eingangsbereich nur noch nach den Geschäftszeiten vorzunehmen. Die Kameras an den Außenwänden werden so ausgerichtet, dass sie nur die direkte Hauswand abbilden.

Dagegen sind die Videokameras in den Flureingängen Türöffnungssysteme, die nur dann aktiviert werden, wenn jemand dort klingelt und Einlass begehrt.

16.1.6. Sicherung gesundheitsrelevanter Daten bei Beendigung eines Betriebes

Ausgangslage: Im Jahre 1997 hat sich der damalige Betriebsrat der Vulkanwerft Bremen i. K. an mich gewandt und angefragt, welche Möglichkeiten beständen, umfangreiche im Betrieb befindliche gesundheitsrelevante Unterlagen, die Rückschlüsse auf die gesundheitlichen Belastungen der Beschäftigten und ehemaligen Beschäftigten ermöglichen, nach Beendigung des Betriebes zu sichern (s. a. 20. JB, Ziff. 20.7.).

Es handelt sich dabei im Wesentlichen um folgende Unterlagen, die teilweise beim Konkursverwalter und beim Betriebsrat vorhanden sind:

- Durchschriften der Unfallanzeigen und Anzeigen von Berufskrankheiten,
- Arbeitsbereichsanalysen,

- Messprotokolle (Lärm, Asbest, Staub, Lösemittel, Kühlschmierstoffe, Schweißuntersuchungen, Strahlenschutz),
- Chemische Reinigung "Hautallergien",
- Schadstoffkataster,
- Betriebsanweisungen zu Arbeitsschutz und zur Arbeitssicherheit,
- Prüfprotokolle für Kräne und andere Fahrzeuge,
- Schulungen der Mitarbeiter, Listen der Ersthelfer und Sicherheitsbeauftragten,
- Analysen bemerkenswerter Unfälle,
- Vorsorgeuntersuchungen und Gesundheitsakten sowie
- sonstige Personalakten.

Der damalige Betriebsrat hielt die Sicherung dieser Unterlagen für erforderlich, weil die Beschäftigten bzw. ehemaligen Beschäftigten ihre Rechtsansprüche, insbesondere gegenüber der Berufsgenossenschaft, verlieren könnten, wenn die Unterlagen vernichtet werden.

Auch wenn nicht alle diese Unterlagen personenbezogene Daten über Beschäftigte bzw. ehemalige Beschäftigte enthalten, kann im Zusammenwirken mit dem jeweiligen Betroffenen und der Hinzuziehung seiner sonstigen Personalakten eruiert werden, welcher Gesundheitsbeeinträchtigung er ausgesetzt war, obwohl er während seiner Beschäftigungszeit keinen Arbeitsunfall hatte oder bei ihm keine Berufskrankheit festgestellt worden ist.

Weil zumindest insoweit der Personenbezug herstellbar ist, ist die weitere Verwendung (Sicherung oder Vernichtung) dieser Unterlagen nach Beendigung des Betriebes auch datenschutzrechtlich zu bewerten.

Datenschutzrechtliche Situation bei Beendigung des Betriebes: Die Verarbeitung personenbezogener Arbeitnehmerdaten im Rahmen der Zweckbestimmung des Arbeitsverhältnisses ist nach § 28 Abs. 1 Nr. 1 Bundesdatenschutzgesetz (BDSG) zulässig, soweit die Daten in oder aus Dateien verarbeitet werden.

Mit der Beendigung der Tätigkeit des Bremer Vulkan enden alle Arbeitsverhältnisse mit den Beschäftigten. Dies hat grundsätzlich zur Folge, dass die zu diesem Zweck gespeicherten Daten nach § 35 Abs. 2 Nr. 3 BDSG zu löschen sind. Allerdings tritt an Stelle der Löschung nach § 35 Abs. 3 BDSG eine Sperrung der Daten, soweit u. a.

- einer Löschung gesetzliche, satzungsmäßige oder vertragliche Aufbewahrungsfristen entgegenstehen oder
- Grund zu der Annahme besteht, dass durch eine Löschung schutzwürdige Interessen des Betroffenen beeinträchtigt würden.

Für Daten, die nicht in oder aus Dateien verarbeitet werden, gelten analog die allgemeinen Bestimmungen der §§ 611, 242 Bürgerliches Gesetzbuch (BGB). Daraus ergeben sich Nebenpflichten des Arbeitgebers bzw. Konkursverwalters, die Rechtsgüter des Arbeitnehmers zu wahren. Zu den Rechtsgütern des Arbeitnehmers dürfte insbeson-

dere sein Rechtsanspruch auf Leistungen gegenüber der Berufsgenossenschaft gehören, der ihm aus gesundheitlichen Belastungen am Arbeitsplatz entsteht.

Zu prüfen war daher, welche Pflichten der Berufsgenossenschaft und dem Konkursverwalter zur Einhaltung dieser Vorschriften insbesondere hinsichtlich der gesundheitsrelevanten Unterlagen obliegen.

Berufsgenossenschaft

Der Konkursverwalter hat erklärt, Unterlagen, die der Berufsgenossenschaft zustehen, seien dieser zugänglich gemacht worden. Die Berufsgenossenschaft war nach Angaben des damaligen Betriebsrats jedoch nicht bereit, weitere als die nach § 193 Abs. 1 Sozialgesetzbuch VII (SGB VII) vorgesehenen Unterlagen (Unfallanzeigen und Anzeigen von Berufskrankheiten) zu übernehmen.

Dies befremdet insbesondere deshalb, weil die übrigen Unterlagen nach Angaben des Gewerbeaufsichtsamtes Bremen nach § 18 Abs. 3 Gefahrstoffverordnung und den Unfallverhütungsvorschriften (UVV) "Umgang mit krebserzeugenden Gefahrstoffen" VBG 113 (§ 4), "Vorsorgeuntersuchung" VBG 100 (§ 14) und "Lärm" VBG 121 (§ 7) dem zuständigen Unfallversicherungsträger auszuhändigen sind.

Konkursverwalter als Rechtsnachfolger des Arbeitgebers: Dem Konkursverwalter habe ich mitgeteilt, dass er nach § 6 Abs. 2 Konkursordnung (KO) das Verwaltungs- und Verfügungsrecht über die Konkursmasse ausübt, zu der auch die Personalakten einschließlich der gesundheitsrelevanten Unterlagen gehören. Insoweit obliegt es ihm, insbesondere die schutzwürdigen Interessen der ehemaligen Beschäftigten zu wahren.

Hierzu hat der Konkursverwalter erklärt, die Personalakten und arbeitsmedizinischen Untersuchungsergebnisse/Krankenakten müssten wegen etwaiger Verjährungsfristen teilweise bis zu 30 Jahren aufbewahrt werden. Er wisse, dass manche Betriebe i. K. die Personalakten den Betroffenen ausgehändigt haben.

Demzufolge würden in Absprache mit dem Betriebsrat und der Metallberufsgenossenschaft die arbeitsmedizinischen Unterlagen dem jeweils betroffenen Mitarbeiter direkt ausgehändigt werden. Unterlagen, die nicht abgeholt werden, würden den jeweiligen Personalakten zugeordnet und gemeinsam mit diesen archiviert. Wo diese letztendlich nach Beendigung der Tätigkeit des Konkursverwalters aufbewahrt werden sollen, sei nicht geklärt, möglicherweise bei einer treuhänderischen Stelle.

Archivierung nach Beendigung der Tätigkeit des Konkursverwalters: Aufgrund dieser unbefriedigenden Situation ist Anfang 1999 zwischen dem Konkursverwalter und dem Verein "Arbeit und Zukunft" mit meiner Beteiligung vertraglich vereinbart worden, dass der Verein die gesundheitsrelevanten Unterlagen zu treuen Händen zum Verbleib übernimmt. Die Daten dürfen hierbei nur für die Wahrung der Rechte (Auskunft, Berichtigung, Löschung oder Sperrung) sowie anderer schutzwürdiger Belange der Betroffenen und unter den Voraussetzungen des § 35 BDSG verarbeitet werden.

Seit der Übergabe der Unterlagen hat der Verein zahlreiche ehemalige Beschäftigte beraten. In vielen Fällen war es nur aufgrund dieser Unterlagen und mit Hilfe des Vereins möglich, Rechtsansprüche gegenüber der Berufsgenossenschaft geltend zu machen. Diese Arbeit des Vereins ist jedoch gefährdet, weil sie bisher nur auf ABM-Basis erfolgte und zum 31. März 2001 ausläuft, wenn keine weitere Lösung gefunden wird.

Forderungen zur langfristigen Sicherung der Daten: Aus diesem Grunde halte ich es für wichtig, dass sowohl in diesem Fall als auch in allen anderen Konkursfällen zur Wahrung der schutzwürdigen Interessen auf Auskunft, Berichtigung, Löschung oder Sperrung der von Konkursen betroffenen Beschäftigten die erforderliche Sicherung und Archivierung gesundheitsrelevanter Unterlagen, die mehrere Beschäftigte betreffen und daher nicht dem Einzelnen ausgehändigt werden können, durch eine treuhänderische Stelle gewährleistet wird.

Als Beispiel kann hier die Sicherung und Archivierung des Gesundheitswesens Wismut genannt werden. Nach § 7 Abs. 3 Gesetz zur Regelung von Vermögensfragen der Sozialversicherung im Beitrittsgebiet werden Akten, Dateien oder Archive des Gesundheitswesens Wismut, die nicht auf einen Sozialversicherungsträger übergegangen sind, Eigentum der Bundesrepublik Deutschland. Die Übertragungsvorschrift soll sicherstellen, dass diese Daten in ihrem Bestand erhalten werden. Sie werden von der Bundeanstalt für Arbeitsmedizin, einer öffentlichen Stelle des Bundes, verwaltet.

Die Bundesregierung beabsichtigt, noch in dieser Legislaturperiode den Entwurf eines Gesetzes über den Arbeitnehmerdatenschutz vorzulegen. Im Zuge der Beratungen hierzu wird auf die Schaffung einer Regelung hinzuwirken sein, die die Unterlagen aus dem Arbeitsverhältnis nach Beendigung eines Betriebes zur Wahrung der schutzwürdigen Interessen der Betroffenen sicherstellt. Hierauf habe ich das zuständige Referat im Bundesministerium für Arbeit bereits hingewiesen.

Allerdings ist nicht absehbar, wann eine derartige Regelung zu erwarten ist. Aus diesem Grunde sollte in Bremen eine Lösung gefunden werden, die die gesundheitsrelevanten Unterlagen der Vulkanwerft i. K. nachhaltig sichert und archiviert.

16.1.7. Schufa-Selbstauskunft zur Vorlage beim Arbeitgeber

Der Betriebsrat eines Sicherheitsunternehmens hat angefragt, ob der Arbeitgeber berechtigt ist, von Bewerbern und Mitarbeitern Schufa-Selbstauskünfte zu verlangen.

Die in der Schufa-Selbstauskunft enthaltenen personenbezogenen Daten werden in oder aus Dateien verarbeitet, so dass sich die Erhebung dieser Daten durch den Arbeitgeber nach § 28 Abs. 1 Bundesdatenschutzgesetz (BDSG) richtet. Nach § 28 Abs. 1 Satz 2 BDSG müssen die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden.

Dieser Grundsatz wird durch die ständige Rechtsprechung des Bundesarbeitsgerichts (BAG) zur Datenerhebung im Bewerbungsverfahren konkretisiert und ist auf das laufende Arbeitsverhältnis übertragbar.

Der BAG-Rechtsprechung zufolge richtet sich der Umfang der Befugnis zur Datenerhebung durch den Arbeitgeber danach, ob er ein berechtigtes, billigenswertes und schutzwürdiges Interesse an der Datenerhebung hat und ob ein schutzwürdiges Interesse des Arbeitnehmers an dem Ausschluss der Erhebung überwiegt. Insoweit bedarf es einer Abwägung der gegeneinander stehenden Rechtsgüter.

Es war daher zu klären, welche Eignungs- bzw. Zuverlässigkeitsvoraussetzungen bei dem Arbeitnehmer vorliegen müssen, um Aufgaben im Sicherheitsdienst ordnungsgemäß erfüllen zu können und ob hierfür die Vorlage einer Schufa-Selbstauskunft erforderlich ist.

Unbestritten dürfte sein, dass der Arbeitnehmer eines solchen Dienstleistungsunternehmens u. a. nicht "überschuldet" sein darf. Demzufolge ist der Arbeitgeber befugt, in diesem Zusammenhang stehende Fragen zu stellen, die der Arbeitnehmer richtig zu beantworten hat.

Fraglich ist jedoch, ob der Arbeitgeber die Vorlage einer Schufa-Selbstauskunft verlangen darf. Nach dem bei mir geführten Register nach § 32 BDSG werden bei der Schufa folgende personenbezogenen Daten gespeichert:

- Aufnahme und Abwicklung von Geld- und Warenkrediten,
- Einrichtung von Girokonten, Kreditkartenkonten und Dauerkonten des Handels.
- Bei Krediten gleichermaßen den Kreditnehmer, Mitschuldner oder Bürgen mit Kreditbetrag, Laufzeit und vertragsgemäßen Abwicklung (z. B. vorzeitige Rückzahlung oder Laufzeitverlängerung).

Ferner werden Daten aufgrund nicht vertragsgemäßem Verhaltens, gespeichert, z. B.

- Kündigung nach Verzug,
- Inanspruchnahme einer vertraglich vereinbarten Lohnabtretung,
- beantragter Mahnbescheid bei unbestrittener Forderung,
- Vollstreckungsmaßnahmen, Wechselprotest, Scheckkartenmissbrauch und Scheckrückgabe mangels Deckung gespeichert

Außerdem werden Daten aus den öffentlichen Schuldnerverzeichnissen der Amtsgerichte gespeichert.

Aus der vorgenannten Aufzählung dürften lediglich die Daten aus den öffentlichen Schuldnerverzeichnissen der Amtsgerichte für die Prüfung der Eignung und Zuverlässigkeit der Arbeitnehmer bei Sicherheitsdiensten erforderlich sein. Zur Erlangung dieser Daten bedarf es aber keiner Schufa-Auskunft.

Da die Schufa-Selbstauskunft jedoch - soweit vorhanden - alle vorgenannten Daten beinhaltet, würde der Arbeitgeber bei Vorlage der Schufa-Selbstauskunft darüber hinaus

Daten erhalten, die für den vorgenannten Zweck nicht erforderlich sind. Ein Verlangen zur Vorlage der Schufa-Selbstauskunft ist daher nicht zulässig.

16.1.8. Einzelgebührennachweise über Telefongespräche der Arbeitnehmer

Ein Betriebsrat fragte an, ob der Arbeitgeber befugt ist, bei seinem Telekommunikationsunternehmen Einzelgebührennachweise über Telefongespräche der Arbeitnehmer zu erheben. Die Geschäftsleitung habe erklärt, auch überprüfen zu wollen, in welchem zeitlichen Umfang die Arbeitnehmer während der Arbeitszeit private Telefongespräche führen.

Soweit es sich bei den Einzelgebührennachweisen ausschließlich um dienstliche Telefongespräche der Arbeitnehmer handelt, gilt die Bestimmung des § 6 Abs. 7 Telekommunikationsdiensteunternehmen-Datenschutzverordnung, die insoweit auf § 10 Abs. 1 Gesetz über die Regulierung der Telekommunikation und des Postwesens beruht. Die Datenverarbeitung betrifft zunächst das Vertragsverhältnis des Telekommunikationsunternehmens mit der jeweiligen Firma.

Gleichwohl hat der Gesetzgeber erkannt, dass dadurch unmittelbar in die Vertragsverhältnisse der Arbeitnehmer mit dem Arbeitgeber eingegriffen wird. Er setzt daher in dieser Regelung die vorherige Beteiligung und damit die Mitbestimmung des Betriebsrats und die Information der Arbeitnehmer voraus.

Die Befugnis des Arbeitgebers zur Datenerhebung ist außerdem nur unter den Voraussetzungen des § 28 Abs. 1 Satz 2 Bundesdatenschutzgesetz (BDSG) zulässig. Danach müssen die Daten nach Treu und Glauben und auf rechtmäßige Weise erhoben werden. Hieraus folgt, dass bei jeder Datenerhebung zwischen den berechtigten Interessen des Arbeitgebers daran und den schutzwürdigen Interessen der Arbeitnehmer am Ausschluss der Datenerhebung abzuwägen ist.

Der Arbeitgeber hat durchaus ein berechtigtes Interesse, dass die Telefonnutzung wirtschaftlich erfolgt. Dagegen haben die Arbeitnehmer aus ihrem Recht auf informationelle Selbstbestimmung ein schutzwürdiges Interesse, nicht unverhältnismäßig oder lückenlos überwacht zu werden.

Daraus folgt, dass z. B. eine stichprobenartige Überprüfung zur Wirtschaftlichkeit der dienstlichen Telefongespräche durch den Arbeitgeber als angemessen angesehen werden kann. Hierbei sind zunächst Überprüfungen ohne Personenbezug vorzunehmen.

Wie eingangs erwähnt, gelten diese Regelungen und Grundsätze nur für ausschließlich dienstliche Telefongespräche. Es muss also ausgeschlossen sein, dass private Telefongespräche geführt werden. Das gleiche gilt auch, wenn eine getrennte Aufzeichnung dienstlicher und privater Telefongespräche z. B. mittels jeweils anderer Wahlnummern vorgenommen wird.

Wenn keine getrennte Speicherung der Verbindungsdaten vorgenommen wird und private Telefongespräche geführt werden dürfen, erbringt der Arbeitgeber hinsichtlich der privaten Telefongespräche für die Arbeitnehmer Telekommunikationsdienste i. S. des § 3 Nr. 5 Telekommunikationsgesetz (TKG). Danach ist das geschäftsmäßige Erbringen von Telekommunikationsdiensten das nachhaltige Angebot von Telekommunikation einschließlich des Angebots von Übertragungswegen für Dritte mit oder ohne Gewinnerzielungsabsicht.

Daten über private Telefongespräche unterliegen somit dem Fernmeldegeheimnis nach § 85 TKG. Es umfasst den Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche (§ 85 Abs. 1 TKG).

Insoweit ist der Arbeitgeber zur Wahrung des Fernmeldegeheimnisses verpflichtet und hat insbesondere die Vorschriften der §§ 85, 87 und 89 TKG zu beachten. Diese gesetzlichen Vorschriften verbieten es dem Arbeitgeber, ohne Einwilligung der betroffenen Arbeitnehmer Einzelgebührennachweise über private Telefongespräche zu erheben.

16.2. Weitergabe von Mitgliederdaten

Ein Mitglied eines Verbandes im Sozialbereich hat sich dagegen gewandt, dass der Verband seine Daten an eine Versicherung übermittelt hat, obwohl er der Weitergabe ausdrücklich widersprochen hat. Auf Anfrage erklärte der Verband, es bestehe mit der Versicherung ein Gruppenversicherungsvertrag. Aus diesem Grunde erhalte die Versicherung die Daten, die für einen Besuch der Mitglieder erforderlich seien.

Ich habe der Versicherung mitgeteilt, dass dieses Verfahren unzulässig sei, weil dadurch das Widerspruchsrecht der Mitglieder gegen die Übermittlung ihrer Daten unberücksichtigt bleibt. Die Versicherung hat daraufhin erklärt, alle Mitglieder würden nunmehr darauf hingewiesen, dass ein Besuch der Versicherung bevorsteht und dafür die Mitgliederdaten an die Versicherung übermittelt werden sollen. Dem könne jedoch widersprochen werden. Bei Widersprüchen würden keine Mitgliederdaten an die Versicherung übermittelt.

16.3. Elektronische Kunden- und Rabatt-Karten

Im letzten Jahr erhielt ich eine Reihe von Eingaben und Anfragen die sich auf die Gewährleistung des Datenschutzes bei den sog. Rabatt-Cards (z. B. Payback) bezogen. Rabatt-Cards werden von verschiedenen Teilnehmerunternehmen mit eigener Kennung herausgegeben. Die Unterlagen (Flyer, Allgemeine Teilnahmebedingungen, Antragsformulare usw.) dieser Teilnehmerunternehmen sind inhaltlich gleich gestaltet. Teilnehmerunternehmen bei der Payback-Card sind z. B. die Firmen: Real-Kauf, Kaufhof, DEA, Europcar, Apollo-Optik.

Seit Einführung der Karte reißen die Nachfragen von besorgten Bürgerinnen und Bürgern und der Presse bei den Datenschutzaufsichtsbehörden nicht ab. Das liegt daran, dass weder die Einverständniserklärung noch die Allgemeinen Geschäftsbedingungen hinreichend deutlich machen wer über welche Daten verfügt und wo und von wem, welche Daten verarbeitet werden. Auch ist nicht klar: Werden die Daten über die gekauften Waren zusammen mit den personenbezogenen Daten der Kundinnen und Kunden für alle Zeit gespeichert und weiterverarbeitet? Welche Daten werden personenbezogen zwischen den Partnerunternehmen ausgetauscht? Was sind die in den Geschäftsbedingungen genannten "Mailings“, und welche personenbezogene Daten werden hierfür verarbeitet?

Zweifel bestehen, ob die unklare Einverständniserklärung, die die Kundinnen und Kunden abgeben müssen, den Anforderungen des Bundesdatenschutzgesetzes (§ 4 Abs. 2 BDSG) entspricht. Der Teilnehmer wird nämlich weder eindeutig über Umfang und Zweck der Speicherung und die vorgesehene Datenübermittlung (welche Daten werden an Partnerunternehmen weitergegeben) hinreichend unterrichtet.

Was dem Kunden häufig nicht klar ist: Selbst bei Barzahlung wird er beim Kauf mit Rabattkarte eindeutig identifizierbar. Die Daten ermöglichen, das Kaufverhalten über mehrere Produktbereiche und Unternehmen hinweg personenbezogen auszuwerten. Aus der Verarbeitung persönlicher und kaufmännischer Daten kann zu jedem Teilnehmer ein Profil gebildet werden, das den Verbraucher zum "gläsernen Kunden“ macht.

Erforderlich ist eine klare Aufklärung der Kundinnen und Kunden, was mit ihren Daten in welchen Verarbeitungsphasen gemacht wird: Wenn das informationelle Selbstbestimmungsrecht gewahrt bleiben soll, müssen sie selbst entscheiden können, was mit ihren Daten geschieht. Wenn es den Unternehmen wirklich nur um die Kundenbindung geht, wie erklärt wird, sollten die Kunden wenigstens eine Variante wählen können, die es ihnen ermöglicht, nur Rabattpunkte zu sammeln, ohne dass es zu einer weiteren Verarbeitung ihrer Daten zu anderen Zwecken kommt.

Zur Klärung dieser Fragen habe ich die zuständige Datenschutzaufsichtsbehörde um Prüfung und Mitteilung ihrer datenschutzrechtlichen Bewertung gebeten. Diese Prüfung ist noch nicht abgeschlossen.

Im übrigen werde ich die weitere Entwicklung auf diesem Gebiet der Kunden-/Freundschafts-/ oder Rabatt-Kartensysteme, insbesondere nach Aufhebung des Rabattgesetzes, kritisch im Auge behalten.

16.4. Auskunfteien

Auch in diesem Berichtsjahr erhielt ich wieder eine Vielzahl von Anfragen und Eingaben zur Verarbeitung personenbezogener Daten durch die Auskunfteien. Die Bürger beklagten sich über die Erhebung, Speicherung und Übermittlung ihrer Daten, die Nichtbeachtung der Benachrichtigungspflicht und die Nichterfüllung ihres Auskunftsanspruchs.

So beschwerte sich in einem Fall eine Bürgerin darüber, dass von einer Auskunftei grundlos und somit ohne Vorliegen eines berechtigten Interesses über sie Daten an ein ihr nicht bekanntes Unternehmen übermittelt worden seien. Die von mir durchgeführte Prüfung ergab, dass die Auskunftei über die Petentin Mitte Juni des vergangenen Jahres Auskünfte an ein Teppichhandelsunternehmen erteilt hatte, bei dem die Petentin Waren, die nach ihrer Auslieferung per Rechnung (Zahlung nach Erhalt) bezahlt werden sollten, bestellt hatte. Bemängelt wurde von mir in diesem Fall insbesondere, dass die Betroffene nicht unverzüglich, sondern erst zwei Monate nach der Datenübermittlung von der Auskunftei benachrichtigt worden war. Das BDSG (§ 33 Abs. 1 S. 2) verlangt von den Auskunfteien eine Benachrichtigung direkt bei der erstmaligen Datenübermittlung und nicht erst Monate danach.
In einem anderen Fall beklagte sich ein Bürger darüber, dass ihm die Schufa nur unzureichende Auskünfte über die zu seiner Person gespeicherten Daten erteilt habe. Nur zufällig habe er bei seinem Kreditinstitut den über ihn von der Schufa errechneten und in seiner Selbstauskunft nicht aufgeführten Score-Punktwert erfahren. Die von ihm angeschriebene Schufa habe sich geweigert, ihn in ausreichender Weise über den errechneten und an seine Bank übermittelten Score-Punktwert und die damit verbundene Bonitätsrisikoquote zu informieren. Konkrete Informationen, die für den ermittelten Score-Wert maßgeblich gewesen sind, seien ihm trotz seiner Aufforderung nicht mitgeteilt worden. Diese Eingabe macht die mangelnde Transparenz des Schufa-Scoring-Verfahrens und die Notwendigkeit deutlich, den Betroffenen auch über dieses Verfahren und die ihm zugrunde liegenden Sachverhalte besser zu informieren.

Wie bereits im letzten Jahr (vgl. 22. JB, Ziff. 16.7.6.) erläutert, werden beim Schufa-Scoring-Verfahren mit mathematisch-statistischen Methoden sog. Score-Werte ermittelt, die den einzelnen Betroffenen dann zur Beurteilung ihrer Kreditwürdigkeit zugeordnet und an die Kreditgeber übermittelt werden. Da bei den Anschlusskunden der Schufa unterschiedliche Kriterien für die Einschätzung des Kreditrisikos maßgebend sind, fließen bei der Schufa - abhängig vom Vertragspartner - jeweils andere Merkmale des Betroffenen in die Berechnung des Score-Wertes ein, was zu verschiedenartigen Ergebnissen führt. Das Verfahren ist insbesondere wegen seiner mangelnden Transparenz für die Betroffenen bei den Obersten Datenschutz-Aufsichtsbehörden auf heftige Kritik gestoßen.

Ein weiteres Problem im Zusammenhang mit dem Schufa-Scoring-Verfahren hat die Obersten Datenschutzaufsichtsbehörden beschäftigt, die Tatsache nämlich, dass die Einholung von Selbstauskünften nach § 34 BDSG zu einer Verschlechterung des Scoring-Werts eines Betroffenen führt. Die Bundes-Schufa begründete diese Tatsache damit, dass die Selbstauskunft in 80% der Fälle als "wirtschaftliches Führungszeugnis“ beim Wohnungs- oder Arbeitsplatzwechsel oder etwa bei der Anschaffung eines Kraftfahrzeugs genutzt werde und der Einfluss auf den Score-Wert somit sachlich begründet sei. Die Obersten Datenschutz-Aufsichtsbehörden äußerten hiergegen erhebliche Bedenken, denn schließlich wird ein gesetzlich geschütztes Recht in Anspruch genommen. Aufgrund

dieser Bedenken erklärte sich die Schufa schließlich bereit, ihr Verfahren dahingehend umzustellen, dass Selbstauskünfte künftig nicht mehr in die Score-Wert-Ermittlung einfließen.
Abschließend erörtert wurde im vergangenen Jahr zwischen den Obersten Datenschutz-Aufsichtsbehörden, der Schufa und den Banken die Neufassung der Schufa-Klausel. Sie enthält nunmehr auch den zugesagten Hinweis auf das Scoring-Verfahren. Auf Anregung der Obersten Datenschutzaufsichtsbehörden will die Schufa die Bürger noch genauer als bisher über ihr Scoring-Verfahren informieren. Auch das Schufa-Merkblatt der Kreditwirtschaft soll überarbeitet und um Informationen zum Scoring-Verfahren angereichert werden.
Erörtert wurde in der AG Auskunfteien ferner die Erteilung von Auskünften durch die Schufa bei e-commerce-Geschäften. Angaben, die der Auskunftei ansonsten zur Identitätskontrolle dienen, müssen bei diesen Geschäften von den Vertragspartnern nicht unbedingt gemacht werden. Hieraus ergeben sich für die Erteilung von Auskünften über einen potentiellen Kunden durch die Schufa Schwierigkeiten bei der Identifikation des Betroffenen. Die Identifikation eines Betroffenen könnte auch über die Nummer seines Girokontos vorgenommen werden, sofern der Käufer/Besteller diese angibt, um am Lastschriftverfahren teilnehmen zu können. Von der Schufa werden in ihrem Datenbestand schätzungsweise zwei Drittel aller in Deutschland bestehenden Girokonten geführt. Nach ausführlicher Diskussion in der AG Auskunfteien bestand schließlich Einigkeit, dass, sofern die Identifikation eines Betroffenen über die Girokonto-Nummer möglich ist, von der Schufa auch Auskünfte bei e-commerce-Geschäften erteilt werden dürfen. Ist eine Identifikation nicht möglich, sollen keine Auskünfte erteilt werden.

16.5. Kreditwirtschaft

16.5.1. Bezahlen im Internet mit digitalem Geld

Das Bestellen von Büchern und anderen Waren über das Internet hat in den letzten Jahren enorm zugenommen. Bezahlt wird dabei häufig mit Kreditkarten, wobei die Kartennummer zunehmend per SSL-Protokoll (Secure Socket Layer) verschlüsselt übertragen wird. Eine andere Möglichkeit besteht darin, Lastschriften zu erzeugen, die per Handy authentisiert werden. Aufgrund der relativ hohen Kosten, die beim Kauf mit Kreditkarten oder per Handy anfallen, eignen sich diese Zahlungsarten allerdings noch nicht zum Bezahlen niederwertiger Güter oder einfacher Dienstleistungen. Das Bezahlen von Informationen, Zeitschriftenartikeln und Programmen, die über das Internet auf den lokalen PC geladen werden, erfordert den Einsatz digitalen Geldes, das sowohl kostengünstig, manipulationssicher als auch - vergleichbar mit Bargeld - anonym ist. Diese drei Ziele lassen sich jedoch schwer gleichermaßen umsetzen.

Während beim herkömmlichen Handel mit teuren Gütern die Betrugsmöglichkeit dadurch eingeschränkt wird, dass beide Partner ihre Identität bewusst preisgeben, erfolgt die Bezahlung niederwertiger Güter traditionell anonym mittels Bargeld. Das Betrugsrisiko ist

aufgrund des niedrigen Warenwerts und aufgrund der Anwesenheit beider Handelspartner recht gering. Die Echtheit des Bargelds wird zudem an Ort und Stelle überprüft.

Der betrugsfreie Tausch von Ware und Geld gestaltet sich bei elektronischem Geld dagegen wesentlich schwieriger. Falls zuerst das Geld übertragen wird, riskiert der Kunde, im Voraus für etwas zu bezahlen, das er anschließend in der erwarteten Form nicht erhält. In umgekehrter Reihenfolge (nach dem Grundsatz: "zuerst die Ware, dann das Geld“), kann sich der Dienstleister nicht unbedingt darauf verlassen, dass der Kunde auch bezahlt. Das Problem wird noch verschärft, wenn der Kunde seinen Namen und seine Adresse nicht mitteilen und vielmehr anonym bleiben möchte.

Der Wunsch der Kunden nach Anonymität auch im Internet ist jedoch verständlich. Personenbezogene Daten, die beim Bezahlen mit elektronischem Geld entstehen, können zu detaillierten Nutzungs- bzw. Kundenprofilen ausgewertet werden. Auch die Speicherung des Zeitpunkts der Zahlung kann Auskunft über individuelle Gewohnheiten bei der Internetnutzung geben. Erfreulicherweise gibt es seit einiger Zeit jedoch Verfahren, die dieses Problem durch das Zwischenschalten von neutralen Instanzen verringern.

Beispielsweise greift das von einer deutschen Großbank herausgegebene Cybercash-Verfahren bei der Verrechnung der elektronischen Geldeinheiten zusätzlich auf Treuhänder zurück. Der Käufer bezahlt die Ware oder Dienstleistung zunächst beim Treuhänder per Kreditkarte, wobei die Kartennummer verschlüsselt übertragen wird. Der Treuhänder überweist das Geld anschließend auf traditionellem Wege an den Händler. Dadurch bleibt der Käufer gegenüber dem Verkäufer unbekannt, sofern keine Lieferanschrift für bestellte Waren benötigt wird. Der Treuhänder kennt dagegen vom Kunden nur dessen Kreditkartennummer, die er zum Abgleich seiner Solvenz bei der Kreditkartengesellschaft benötigt. Name und Anschrift des Kunden sind auch dem Treuhänder unbekannt; diese kennt nur die Kreditkartengesellschaft. Die Anonymität des Kunden kann somit nur dann aufgehoben werden, wenn Händler, Bank und Treuhänder ihre jeweiligen (Teil-)Datensätze miteinander verknüpfen.

Das Bezahlen per Internet ist seit letztem Jahr auch mit der Geldkarte des deutschen Kreditwesens möglich. Die Geldtransaktionen können nunmehr vom heimischen PC, sofern dieser mit einem zertifizierten Chipkartenleser ausgestattet ist, per Internet direkt von der Geldkarte des Kunden zum Händler übertragen werden. Trotz deutlicher Kritik der Datenschutzbeauftragten werden sämtliche Zahlungstransaktionen einschließlich Kaufdatum und Kaufzeit jedoch in sogenannten Evidenzzentralen über lange Zeiträume gespeichert, obwohl dies aus sicherheitstechnischer Sicht nicht unbedingt notwendig wäre. Da die Transaktionsdatensätze hauptsächlich zu Buchungszwecken gespeichert werden, ist zu hoffen, dass langfristig auf derartige Schattenkonten verzichtet wird und nur noch Schattensalden - wie das bereits bei der österreichischen EC-Karte praktiziert wird - gespeichert werden (vgl. genauer nachfolgenden Beitrag unter Ziff. 16.5.2. des Berichts).

Vollständige Anonymität des Kunden wird zur Zeit durch das Ecash-Verfahren garantiert, das vom niederländischen Kryptologen David Chaum entwickelt worden ist und von der Deutschen Bank in einem Pilotversuch getestet wurde. Um mit Ecash zu zahlen, muss der Käufer zunächst seine elektronische Geldbörse auf seinem privaten PC mit elektronischen Münzen laden, die er von seiner Bank zu Lasten seines Girokontos erhält. Für jede elektronische Münze werden auf dem heimischen PC zufällige Seriennummern erzeugt. Diese werden anschließend von der Bank verdeckt signiert und damit für echt erklärt. Die signierten Münzen werden über das Internet an den Händler übertragen; dieser lässt die Münze online von der ausstellenden Bank auf Echtheit überprüfen, ohne dass dabei die Identität des Kunden ermittelt werden kann.

Die beschriebenen Verfahren sind zusammen mit weiteren Verfahren im Februar 2001 auf einem Workshop in Potsdam vorgestellt und erörtert worden, der vom Arbeitskreis Medien der Datenschutzbeauftragten des Bundes und der Länder veranstaltet wurde. Bei der Zusammenstellung von Bewertungskriterien sowie bei der Auswahl der Verfahren habe ich mit den Datenschutzbeauftragten von Hamburg und Thüringen zusammengearbeitet.

16.5.2. Datenschutzrechtliche Beurteilung des Systems GeldKarte

Wie berichtet, hatte ich es federführend übernommen die datenschutzrechtlichen und -technischen Fragen im Zusammenhang mit dem Einsatz der Geldkarte aufzubereiten. Hier die wesentlichen Ergebnisse:

Grundsätze

Die Datenschutzaufsichtsbehörden lassen sich bei der Beurteilung und den Empfehlungen zum Einsatz der GeldKarte u. a. davon leiten, dass

- die Nutzung soweit wie möglich anonym bzw. pseudonym gestaltet werden sollte,
- dem Prinzip der Datensparsamkeit weitestgehend Rechnung getragen werden sollte,
- nach erfolgreicher Abwicklung die beim Zahlvorgang angefallenen Daten möglichst bald gelöscht werden sollten,
- die anfallenden Daten einer engen Zweckbindung unterliegen sollten und daher nur für die Zahlungsabwicklung genutzt werden dürfen und
- die Erstellung von karten- oder personenbezogenen Verbraucherprofilen ausgeschlossen sein soll.

Nach dem Besuch einer "Evidenzzentrale" (Rechenzentrum) der Kreditwirtschaft und unter Berücksichtigung der von der Kreditwirtschaft schriftlich und mündlich erteilten Auskünfte sowie nach Auswertung der auf CD-ROM zur Verfügung gestellten "Schnittstellenspezifikation", bin ich zu folgenden Ergebnissen:

Allgemeines

- Das Zahlungssystem "GeldKarte" gewährleistet durch seine verteilte Datenverarbeitungsstruktur einen weitgehenden Schutz gegen die unberechtigte Zusammenführung der mit einer GeldKarte getätigten Zahlungsvorgänge.
- Ein einzelnes Kreditinstitut hat über die von ihm einem Kunden oder Dritten herausgegebene GeldKarte unmittelbar keine Kenntnisse über die einzelnen mit einer solchen GeldKarte vorgenommen Bezahlvorgänge. In den jeweiligen Evidenzzentralen (Kundenevidenzzentrale/ Händlerevidenzzentrale) werden Kartennummer und Salden (sog. Schattensaldo) sowie einzelne Umsätze separat gespeichert. Die bei einer Kundenevidenzzentrale geführten Schattensalden lassen keine Aussage über einzelne Bezahlvorgänge zu. Die bei den Händlerevidenzzentralen eingereichten nach festgelegten Zeiträumen archivierten Umsatzdaten eröffnen nur in begrenztem Umfang und mit erheblichem technischen Aufwand die Möglichkeit einer kartenbezogenen Zusammenführung von Umsatzdaten.
- Zu jeder Karte gibt es eine Evidenzzentrale, die alle mit dieser Karte getätigten Transaktionen über viele Jahre nachweist. Nach Aussage der Kreditwirtschaft geschieht dies, um gesetzlichen Aufbewahrungsfristen zu genügen.
- Im Rahmen der Verwendung der GeldKarte kommt es sowohl zu weitgehend anonymen, zu pseudonymen aber auch personenbezogenen Datenverarbeitungsvorgängen. Eine weitestgehend anonyme Form der Nutzung gewährleistet eine mit Bargeld aufgeladene GeldKarte ohne Bindung an ein Bankkonto, wenn Ausgabe und Clearing ohne Personenbezug erfolgen. In Fällen, in denen eine kontogebundene Karte (z. B. EC-Karte mit Geldkartenfunktion) verwendet wird oder eine kontoungebundene Karte gegen ein Konto mit einem Geldbetrag geladen wird, schwächt sich dieser Effekt ab, weil Datenspuren gespeichert werden, die eine Depseudonymisierung z. B. beim bezogenen Kontoinhaber möglich machen können.

Evidenzzentralen

- Die Evidenzzentralen gewährleisten den Datenaustausch zwischen den angeschlossenen Kredditinstituten und überwachen die Abrechnung in Bezug auf Händler und Kunden. Sie übernehmen dabei überwiegend Prüfungen, die zum Ziel haben, die Sicherheit des Zahlungsverkehrs zu gewährleisten.
- Das Risiko einer besonderen Kumulierung von kartenbezogenen Daten ergibt sich in den Fällen, in denen eine Evidenzzentrale sowohl die Funktion der Händlerevidenzzentrale (HEZ), der Kundenevidenzzentrale (KEZ) und der Ladezentrale für verschiedene Kreditinstitute wahrnimmt und gleichzeitig im Auftrag einzelner Kreditinstitute auch noch die Kontoführung für die Geldkarteninhaber durchführt. Die Kreditwirtschaft hat in diesem Zusammenhang darauf hingewiesen, dass die genannten Funktionen organisatorisch und technisch streng voneinander getrennt sind.
- Die Datenschutzaufsichtsbehörden empfehlen hier grundsätzlich ein Verbot kartenbezogener Auswertungen bei den Evidenzzentralen in den entsprechenden Verein-

barungen sicherzustellen. Soweit hiervon Ausnahmen erforderlich sind, sollten diese festgelegt werden. In diesem Falle sollte auch das Zusammenwirken der verschiedenen Funktionen innerhalb einer Evidenzzentrale, wie auch das Zusammenwirken der verschiedenen Evidenzzentralen untereinander geregelt werden. Hierbei sollte neben dem Anlass die Entscheidungsebene festgelegt werden. Auch eine Dokumentation und Protokollierung des Vorgang ist vorzusehen.

- Nicht verkannt werden darf, dass insbesondere die langen Aufbewahrungsfristen der gespeicherten Daten bei den Evidenzzentralen eine kartenbezogene Auswertung auch lange zurückliegender Vorgänge ermöglichen (Historie). Diesen Umstand hat allerdings nicht die Kreditwirtschaft zu vertreten. Die Datenschutzaufsichtsbehörden wollen sich daher dafür verwenden, dass die kartenbezogene Protokollierung von Zahlungsvorgängen mit der GeldKarte, wenigstens solange sie im Bereich von kleinen Beträgen angesiedelt sind, erheblich verkürzt wird.

- Die Tätigkeit der Evidenzzentralen ist als Auftragsdatenverarbeitung zu qualifizieren. Die Kreditinstitute verfügen über personenbezogene Daten, die im Rahmen der Nutzung von Geldkarten von Evidenzzentralen im Auftrag der Institute verarbeitet werden. Weiter ist zu berücksichtigen, dass unter bestimmten Umständen im Einzelfall auch bei den Evidenzzentralen personenbeziehbare Datenverarbeitung stattfinden kann. Es macht z. B. keinen gravierenden Unterschied, ob die Kontonummer oder die Kartennummer der GeldKarte als Ordnungskriterium verwendet wird, weil sie verbunden mit der Bankleitzahl des Kreditinstituts z. B. in Fällen einer kontogebundenen EC-Karte oder bei der Rückzahlung des Betrages einer defekten GeldKarte in der Regel dem Kontoinhaber zugeordnet werden kann. Die Evidenzzentralen sind in die "Vereinbarung des institutsübergreifenden Systems GeldKarte" eingebunden. Die Evidenzzentralen haben keinerlei eigenen Entscheidungsspielraum, wie und in welchem Umfang die einzelnen Daten zu verarbeiten sind. Vielmehr zwingt das gesamte System der GeldKarte zu einem starren, nicht variablen Verarbeitungsablauf. Nach Auskunft der besuchten Evidenzzentrale ist diese in einzelnen Fällen auf Anforderung der Kreditinstitute verpflichtet, die zugehörigen Kundendaten zu übermitteln. Insbesondere aber würde eine Qualifizierung der Datenverarbeitung durch die Evidenzzentrale als "Funktionsübertragung" dazu führen, dass dann eine Übermittlung von Daten durch die Kreditinstitute an die Evidenzzentralen vorläge, die eine Durchbrechung des Bankgeheimnisses mit sich brächte, die einer ausdrücklichen Einwilligung durch den Karteninhaber bedürfte. Die Qualifizierung als Datenverarbeitung im Auftrag hingegen bedürfte insoweit keiner besonderen Legitimation durch den Kunden.

- Von der Kreditwirtschaft festzulegen ist auch, wer für welche Verarbeitung der Daten in den verschiedenen Evidenzzentralen Auftraggeber, d. h. speichernde Stelle im Sinne des BDSG ist, und wer für die Verarbeitung - insgesamt oder aufgeteilt - verantwortlich im Sinne der Datenschutzrichtlinie der EU ist. Eine Beauftragung kommt

dabei nur durch ein Kreditinstitut in Betracht, eine Beauftragung durch Händler oder Kunden ist auszuschließen. Zu überlegen ist, ob eine Aufteilung der Verantwortlichkeit nach Funktionskreisen erfolgen kann, d. h. für alle Kundendaten bei der Evidenzzentrale (KEZ) ist das Kundenkreditinstitut, bzw. das kartenemittierende Institut verantwortlicher Auftrageber, für alle vom Händler bei einer Evidenzzentrale (HEZ) eingereichten Daten hingegen ist das für den Händler kontoführende bzw. die Händlerkarte herausgebende Kreditinstitut des Händlers verantwortlich. Im Rahmen des Auftragsverhältnisses darf das jeweilige Kreditinstitut in der Regel nur dann eine kartenbezogene Auskunft über die in den Evidenzzentralen gespeicherten Daten verlangen, wenn und soweit dies für die Klärung eines vom Karteninhaber (Kunden- oder Händlerkarte) vorgetragenen Reklamationsfalles erforderlich ist.

Händlerterminal

- Zu der von den Datenschutzaufsichtsbehörden geäußerten Befürchtung, im Händlerterminal könne eine Verknüpfung der GeldKarte-Daten mit anderen in der Karte des Kunden oder beim Händler gespeicherten Daten kommen, hat die Kreditwirtschaft erklärt, dass die Händler nur solche GeldKarten-Terminals einsetzen dürfen, die von der Kreditwirtschaft zugelassen seien. Eine solche systemfremde Nutzungsmöglichkeit sei deshalb nicht eröffnet. Durch die "technische Herrschaft" der Kreditwirtschaft über die Systemkomponenten beim Händler seien Datensicherheit und -integrität hinreichend gewahrt. Soweit diese Voraussetzungen auch in Zukunft bestehen bleiben, ist hierin einen ausreichenden Schutz zu sehen.

- Dabei zu berücksichtigen ist auch, dass es Aufgabe der Händler ist, selbst dafür Sorge zu tragen, dass den Bestimmungen der Datenschutzgesetze Rechnung getragen wird. Da aber auch die Schnittstellenspezifikation für die EC-Karte mit Chip (GeldKarte) dahingehend falsch verstanden werden kann, "dass Umsatzdaten vor der Einreichung bei der Evidenzzentrale vom Händler bearbeitet werden dürfen“ wäre ein Hinweis darauf wünschenswert, dass die Daten nur zur Abwicklung des Bezahlvorgangs verwendet werden dürfen und auch beim Händler eine kartenbezogene Auswertung, aufgrund der Nutzungsbedingungen (Zweckbindung) nicht erfolgen darf. Die Kreditwirtschaft hat dazu erklärt, dass die Formulierung aus der Spezifikation ausschließlich darauf abziele, keine speziellen Datenformate für die Weiterleitung der Umsatzinformationen innerhalb von Händlersystemen vorzuschreiben und die Verwendung unterschiedlicher Datenformate sowie Übertragungswege zu ermöglichen.

- Weiter muss ausgeschlossen sein, dass Daten aus der "Bezahlfunktion“ der GeldKarte auch für eine kartenbezogene Zusammenführung mit Daten aus sog. "Zusatzanwendungen" genutzt werden .

Unterrichtungs- und Auskunftsrechte der GeldKarten-Inhaber, u. a.

- Bisher ist keine Information bekannt, die hinreichend deutlich und in allgemein verständlicher Form darüber aufklärt, auf welchen Wegen die Daten transportiert wer-

den, an welchen Stellen Daten kartenbezogen gespeichert werden und wie lange sie aufbewahrt werden. Dies ist aber erforderlich, um eine transparente Datenverarbeitung sicherzustellen. Die als "Bedingungen für die Verwendung der EC-Karte" von der Kreditwirtschaft herausgegebenen Erläuterungen enthalten hierzu keine Ausführungen.

- Auch ist nicht klar, ob und in welchem Umfang die Kreditwirtschaft Auskunftsansprüche von Kunden über zu ihrer Karte gespeicherte Daten befriedigen will. Auch dies sollte festgelegt werden. Es sollte bestimmt werden, von wem und in welchem Umfang Auskunftsersuchen von GeldKartenbesitzern entsprochen werden soll. Dies sollte den Kunden bekanntgegeben werden.

- Schließlich ist zu prüfen, wie eine Auszahlung des Kartenbetrages bei Defekt einer kontoungebundenen GeldKarte ohne Bekanntgabe von Namen und Bankverbindung sichergestellt werden kann. Die Kreditwirtschaft hat in diesem Zusammenhang darauf hingewiesen, dass einzelnen Instituten, die den Bankverlag als Kundenevidenzzentrale nutzen, ein Online-System ermöglicht, den Wert einer GeldKarte zu ermitteln und auszuzahlen,

Entsprechende Bewertungen und Empfehlungen sind der im ZKA (Zentraler Kreditausschuss) vertretenen Kreditwirtschaft nach vorheriger Diskussion zugeleitet worden. Eine Antwort lag bei Redaktionsschluss noch nicht vor.

16.5.3. Datenschutzrechtliche Beurteilung des elektronischen Fahrscheins

Im letzten Bericht (vgl. 22. JB, Ziff. 16.7.3.) habe ich über das bei der Bremer Straßenbahn AG (BSAG) begonnene Pilotprojekt "Einführung des elektronischen Tickets“ berichtet und das Verfahren für den Fahrscheinerwerb, die Datenspeicherung und -weiterleitung von der Karte bis zur Evidenzzentrale beschrieben.

Die Laufzeit des ursprünglich bis Dezember 1999 befristeten Pilotprojekts wurde bis zum 31. Dezember 2000 verlängert. Der im letzten Jahresbericht angekündigte Meinungsaustausch fand wie geplant im Februar 2000 mit Vertretern der BSAG, des Bundesverbandes deutscher Banken und des Systemhauses debis statt. Diskussionsgrundlage waren meine ausgearbeiteten Vorschläge zur Verbesserung des Datenschutzes und zur Datensicherheit. Folgende Ergebnisse wurden dabei erzielt:

- Erweiterte Lesefunktion für Kunden

  Der Nutzer muss sich jederzeit über die auf seiner Karte gespeicherten Daten im Fahrscheinverzeichnis informieren können. Da das gesamte Fahrscheinverzeichnis für den Kunden mit einem Taschenkartenleser lesbar ist, sehe ich die Anforderung als erfüllt an.

- Schaffung gezielter Löschmöglichkeiten durch Kunden

Im Moment wird jeweils der in der Reihe erste abgelaufene Fahrschein mit einem neuen Fahrschein überschrieben. Daher können eine ganze Reihe abgelaufener Fahrscheine auf der Karte gespeichert bleiben. Hierfür besteht auch aus Sicht der Verkehrswirtschaft keine Notwendigkeit. Technisch besteht grundsätzlich die Möglichkeit, abgelaufene Tickets durch Überschreiben zu löschen. Inwieweit die Möglichkeit automatisierter oder gezielter Löschungen praktisch umsetzbar ist, wird von den Projektpartnern überprüft. Soweit dies nicht realisiert werden kann, ist wenigstens eine manuelle Löschmöglichkeit am Terminal vorzuhalten.

- Eingeschränkter Lesezugriff durch Kontrolleur

  Die BSAG muss nicht nur von ihr ausgestellte Fahrscheine lesen. Es gibt Fahrausweise mit Übergangstarifen (DB-Nahverkehrssystem) oder Fahrausweise von anderen Verkehrsunternehmen, die im Verkehrsverbund gelten. Durch technische Vorkehrungen ist daher anzustreben, dass bei Fahrscheinkontrollen nur auf die auf der GeldKarte gespeicherten Daten Zugriff genommen werden kann, die für die jeweils aktuelle Fahrt von Bedeutung sind. Der Lesezugriff des Kontrolleurs sollte daher auf die Fahrkarten beschränkt sein, die die Fahrberechtigung der kontrollierten Fahrt nachweisen. Soweit Fahrten im Verbund erfolgen, bedeutet dies auch den Zugriff auf die Verbundfahrkarte (z. B. Gültigkeit von DB-Fahrkarten für Busse regionaler Verkehrsbetriebe). Weiter sollte der Lesezugriff des Kontrolleurs auf gültige Tickets beschränkt werden. So wird verhindert, dass auf alte oder nicht der Kontrolle unterliegende Fahrscheine Zugriff genommen wird.

- Kurze fahrscheinbezogene Speicherung der Chip-ID beim Verkehrsbetrieb, Auswertung des pseudonymisierten Datenbestandes und frühzeitige Anonymisierung der Daten

  Nach Abwicklung des Vertragsverhältnisses, Ablauf des Tickets, Ablauf der von der BSAG festzulegenden Reklamationsfrist und finanziellen Abwicklung des Vertrages muss eine Löschung der kartenbezogenen Daten beim Verkehrsbetrieb erfolgen. Ich sehe in der Ersetzung der Kartennummer eine Möglichkeit, sicherzustellen, dass nachträglich kein Personenbezug mehr herstellbar ist. Es wird von der BSAG geprüft, mit welchem Aufwand eine Ersetzung der Kartenfolgenummer in den Datensätzen erfolgen kann. Nur wenn kein Personenbezug hergestellt werden kann, darf die BSAG über einen längeren Zeitraum die Daten für statistische Auswertungen speichern.

- Kurze Löschfristen in den externen Terminals und Klärung der Aufbewahrung der Bezahldateien bei der BSAG

  Die in den Terminals gespeicherten Daten zur Übertragung an die BSAG werden nach erfolgreicher Datenübertragung in den mobilen Terminals gelöscht. Transaktionsbezogene Daten werden nach erfolgreicher Übertragung an die jeweiligen Knoten gelöscht. Im BSAG-Einreicher-Terminal werden die Bezahltransaktionsdaten

schnellstmöglich nach Erhalt der Zahlung, spätestens jedoch nach drei Monaten gelöscht.

- Datenschutzrechtliche Verantwortung

  Die datenschutzrechtliche Verantwortung wird im Echtbetrieb vertraglich durch die BSAG geregelt.

- Löschung der Projektdaten

  Bei Übergang in den Echtbetrieb werden die Kriterien des Echtbetriebes auf die Daten des Probebetriebes ausgedehnt.

- Vertragliche Wartung

  Es werden vertragliche Regelungen zur Wartung getroffen werden.

- Schaffung umfassender Aufklärungsmöglichkeiten der Kunden

  Es wurde bereits im Flyer bei Pilotbeginn informiert. Es soll für die Kunden ein Informationsblatt bereitgestellt werden, das über die Funktionsweise und Datenverarbeitung der Karten grundsätzlich aufklärt und Hinweise auf Reklamationsmöglichkeiten enthält.

- Keine Vorteile bei Nutzung kontogebundener Karten

  Die BSAG erklärte, es finde keine Ungleichbehandlung statt von Personen, die eine kontogebundene GeldKarte einsetzen und solchen, die eine kontoungebundene benutzen.

Die Vertreter vom Bundesverband dt. Banken und des Systemhauses debis erklärten sich in dem Gespräch im Februar bereit, insbesondere die Möglichkeit der praktischen Umsetzung für eine gezielte Löschmöglichkeit durch den Kunden sowie die Möglichkeit der Beschränkung für den Lesezugriff des Kontrolleurs nur auf Fahrkarten des eigenen Verkehrsbetriebes bzw. der Verbundteilnehmer zu prüfen. Dabei gingen die Teilnehmer davon aus, dass dies in der AG Kreditwirtschaft mit den Vertretern des Zentralen Kreditausschusses (ZKA) erfolgen solle, denn der elektronische Fahrschein ist eine Zusatzanwendung auf der von der Kreditwirtschaft herausgegebenen GeldKarte.

Ich habe daher einen unter den Datenschutz-Aufsichtsbehörden abgestimmten Katalog mit Vorschlägen zur Verbesserung des Datenschutzes im Juli 2000 dem ZKA übersandt. In der letzten Sitzung der AG Kreditwirtschaft im September 2000 wurde von Seiten des ZKA nunmehr unerwartet darauf hingewiesen, dass der zuständige Ansprechpartner für die Umsetzung der Vorschläge zur Verbesserung des Rechts auf informationelle Selbstbestimmung zum Datenschutz und zur Datensicherheit die jeweiligen Verkehrsbetriebe seien. Aus diesem Grunde habe ich die bereits am 28. Februar 2000 besprochenen Vorschläge im Oktober 2000 nochmals in schriftlicher Form der BSAG mitgeteilt. Die BSAG teilte mir mit, dass auch für sie die Aussage, dass nun die jeweiligen Verkehrsbetriebe Ansprechpartner für die Umsetzung der Vorschläge zur Verbesserung der datenschutz-

rechtlichen Anforderungen seien, unerwartet erfolgte. Die BSAG hat umgehend Kontakt mit dem entsprechenden Sachbearbeiter des ZKA aufgenommen, um die Angelegenheit voranzubringen. BSAG und ZKA befinden sich derzeit noch in Abstimmungsgesprächen und wollen mich nach Abschluss der Gespräche über das Ergebnis unterrichten. Des Weiteren sollen die abgestimmten Vorschläge mit dem Verbund deutscher Verkehrsunternehmen (VdV) besprochen werden.

16.6. Weitergabe von Inserentendaten durch die Presse

Im Oktober des Berichtsjahres erhielt ich eine Eingabe von Bürgern aus dem Bremer Umland. Sie hatten von der Ermittlungsgruppe Schwarzarbeit des Stadtamtes einen Anhörungsbogen erhalten, in dem ihnen vorgeworfen wurde, sie hätten Ordnungswidrigkeiten begangen, da sie in einer Bremer Tageszeitung für die Erbringung von handwerklichen Leistungen geworben hätten, ohne in die Handwerksrolle der zuständigen Handwerkskammer eingetragen zu sein. Ihnen wurde in den Schreiben Bußgelder angedroht.

Die Daten hatte sich das Stadtamt bei der Zeitung besorgt, in der die Annonce erschienen war. Ein Bremer Boulevardblatt titulierte in diesem Zusammenhang: "Bremer Zeitung verrät ihre eigenen Anzeigenkunden". Die betroffenen Bürgerinnen hatten für einen Familienangehörigen jeweils eine Anzeige aufgegeben, in der unter der Angabe einer Telefonnummer für die Verlegung von Laminatfußboden geworben wurde.

Gemäß § 4 des Gesetzes zur Bekämpfung der Schwarzarbeit (SchwArbG) begeht eine Ordnungswidrigkeit, wer für die selbständige Erbringung handwerklicher Dienst- oder Werkleistungen durch Anzeigen in Zeitungen, Zeitschriften oder anderen Medien oder auf andere Weise wirbt, ohne pflichtgemäß in die Handwerksrolle eingetragen zu sein. Eine solche Ordnungswidrigkeit kann mit einer Geldbuße bis zehntausend Deutsche Mark geahndet werden.

§ 1 i. V. m. § 18 der Handwerksordnung legt fest, welche Dienst- und Werkdienstleistungen in die Handwerksrolle einzutragen sind. Die Leistung "Verlegen von Laminatfußboden" gehört nach Prüfung durch die zuständige Handwerkskammer nicht dazu. Dies stellte die Ermittlungsgruppe erst nachträglich fest. Eine Datenanfrage bei der Zeitung wäre bereits unter diesem Gesichtspunkt überflüssig gewesen. Hinzu kam, dass im konkreten Fall die Ermittlungshandlungen gegen die Anzeigenaufgebenden in die falsche Richtung ging, weil nach dem Wortlaut des Gesetzes nur der Anbieter einer Dienst- oder Werkleistung ordnungswidrig handeln kann. Die Ermittlungsgruppe Schwarzarbeit hätte ihre Handlungen auf den konkreten Anbieter - der seine Telefonnummer angegeben hat - lenken müssen.

Wie verhält es sich aber generell mit entsprechenden Auskunftsersuchen der Ermittlungsgruppe Schwarzarbeit. Zum einen ist bei Anzeigen mit Angabe einer Telefonnummer der Telekommunikationsbetreiber gemäß § 4 Abs. 3 SchwArbG verpflichtet, Namen und Anschrift des Inhabers des Telefonanschlusses bekanntzugeben. Diese Angaben kann aber nur die Handwerkskammer verlangen, nicht hingegen die Ermittlungs-

gruppe Schwarzarbeit, da diese keine gesetzliche Zuständigkeit hat. Bei Anzeigen mit Chiffre kann je nach Zuständigkeit die Handwerkskammer oder die Ermittlungsgruppe Schwarzarbeit sich an das Presseorgan wenden und Auskunft verlangen, welche Person die Annonce aufgegeben hat. Das ist durch Rechtsprechung gesichert, sie gilt allerdings nur in Fällen von Chiffreanzeigen, nicht in Fällen in denen eine Telefonnummer oder Adresse angegeben ist. Bei meinen datenschutzrechtlichen Untersuchungen ist darüber hinaus klar geworden, dass noch nicht alle gesetzlichen Möglichkeiten zur Schaffung von Zuständigkeiten (§ 4 Abs.1 SchwArbG) für die Ermittlungsgruppe Schwarzarbeit geschaffen worden sind, so dass mangels Befugnis auch in diesem Bereich z. Zt. keine Auskünfte eingeholt werden dürfen.

Ich habe im Rahmen meiner Prüfung habe ich den Eindruck gewonnen, dass die Ermittlungsgruppe Schwarzarbeit die vielfältigen Varianten der gesetzlichen Regelungen noch nicht hinreichend vergegenwärtigt hat. Ich habe daher mit dem Stadtamt vereinbart, dass Regelungen getroffen werden, die den rechtlichen Rahmen, in dem die Ermittlungsgruppe Schwarzarbeit agieren darf, festlegen.

Das betroffene Presseorgan habe ich darüber unterrichtet, dass die Rechtsprechung und Kommentierung den Medien in Bezug auf Daten von Inserenten grundsätzlich keinen besonderen Schutz zugesteht. Anders sieht es bei der Wahrnehmung redaktioneller Tätigkeit aus, hier gelten die von der Strafprozeßordnung gewährten Zeugnisverweigerungsrechte. Es bestehen daher keine grundsätzlichen datenschutzrechtlichen Bedenken, wenn von Seiten der Presse in einem geordneten Verfahren die erforderlichen Daten an die für die Bekämpfung der Schwarzarbeit zuständigen Stellen herausgegeben werden. Es dürfen allerdings nur dann Daten an das Stadtamt herausgegeben werden, wenn hinreichende Tatsachen vorliegen, um ein Ermittlungsverfahren einzuleiten. Um feststellen zu können, ob diese Voraussetzungen vorliegen, wie auch zur eigenen Dokumentation des Handelns, empfiehlt es sich in der Regel nur in einem geordneten schriftlichen Verfahren unter Berücksichtigung der Verfahrensregelungen Auskünfte zu erteilen.

16.7. Meldepflichtige Stellen

16.7.1. Statistische Übersicht - Entwicklung und Ausblick

Die Zahl der Stellen, die mir zum Register nach § 32 BDSG gemeldet sind, hat sich im Berichtszeitraum wiederum leicht erhöht. Insgesamt weist das Register Anfang Januar 2001 150 Stellen gegenüber 140 Stellen im Vorjahr aus. Davon befinden sich 122 Stellen in Bremen und 28 Stellen in Bremerhaven. Der regionale Schwerpunkt liegt also wie bisher in Bremen. Die Mehrzahl der angemeldeten Stellen ist dem Bereich der Auftragsdatenverarbeiter, insbesondere den DV- und TK-Dienstleistungsanbietern zuzuordnen.

Das Register nach § 32 BDSG ist für mich kein Selbstzweck. Ursprünglich war es in erster Linie gedacht zur Information der Öffentlichkeit, heute ist es vor allem Grundlage und wesentliche Orientierung für meine Prüftätigkeit nach § 38 Abs. 2 BDSG.

Die Entwicklung im Bereich der Informations- und Kommunikationstechnik, die Dezentralisierung der Datenverarbeitung, die Auslagerung betrieblicher Funktionen, insbesondere auch der DV-Aktivitäten sowie neuartige DV-, Tele- und TK-Dienstleistungen führen zu häufigen Änderungen im Register. Registeränderungen ergeben sich auch dadurch, dass ich - ohne gesetzlich dazu verpflichtet zu sein - Betriebe, bei denen ich aufgrund von Handelsregistereintragungen oder von Branchenzuordnungen eine Meldepflicht vermute, anschreibe und um Prüfung ihrer Meldepflicht (deren Nichtbefolgung ja bußgeldbewehrt ist) bitte. Bei einigen angeschriebenen Betrieben ergibt sich, z. T. auch aufgrund örtlicher Feststellungen, tatsächlich, dass meldepflichtige Tätigkeiten ausgeübt werden, die dann zu einer Registereintragung führen.

Einzelheiten zum Stand des Registers zeigt die nachfolgende Übersicht:

Art der Tätigkeit	**insgesamt**	**Bremen**	**Bremerhaven**
Speicherung personenbezogener Daten zum Zwecke der Übermittlung (insgesamt)	**6**	**4**	**2**
Auskunfteien	4	3	1
Adressverlage/Adresshändler	2	1	1
Speicherung personenbezogener Daten zum Zwecke der anonymisierten Übermittlung (insgesamt)	**4**	**4**	**-**
Markt- u. Meinungsforschung	4	4	-
Verarbeitung oder Nutzung personenbezogener Daten im Auftrag (insgesamt)	**140**	**114**	**26**
Datenerfassung	6	6	-
Dienstleistung/Rechenzentren	103	82	21
Mikroverfilmer	4	4	4
Mailboxdienste/Provider	13	9	4
Datenlöschung/Datenträgervernichtung	6	6	-
Call-Center	8	7	1
Gesamt	**150**	**122**	**28**

Stand: 01. Januar 2001

Die Meldepflicht der nicht-öffentlichen Stellen gegenüber den Datenschutzaufsichtsbehörden wird sich sowohl was den Kreis der verpflichteten Stellen als auch was den Inhalt der Meldung anbetrifft aufgrund des neuen BDSG erheblich verändern. Das bedeutet, dass sich auch der Registerinhalt und die Registerführung der Datenschutzaufsichtsbehörden ändern werden. Die Zahl der gemeldeten Stellen dürfte nach den derzeitigen Vorstellungen der BDSG-Novelle drastisch zurückgehen, während sich die meldepflichtigen Angaben künftig inhaltlich ändern und erheblich ausweiten werden (Verfahrensregister). Das bisherige Registerverfahren muss umgestellt und der Datenbestand in bereinigter Form übergeleitet werden. Auch die Verfahrensweise zur Führung des Registers und zur Einsichtnahme in das Register müssen neu gestaltet werden. Ich erwarte, dass das neue BDSG und damit die geänderten Regelungen zur Meldepflicht und damit zur Registerführung demnächst in Kraft treten werden.

Beim 6. Workshop der Datenschutzaufsichtsbehörden im Herbst letzten Jahres nahmen die geplante Neugestaltung der Meldepflicht nach dem neuen BDSG und die künftige

Registerführung der Datenschutzaufsichtsbehörden einen breiten Raum ein. Hierzu wurde ein neues Meldeformular mit Merkblatt zur Meldepflicht nebst zwei Entscheidungsbäumen (zur Meldepflicht und zur Bestellung eines betrieblichen Datenschutzbeauftragten) entwickelt und von den Teilnehmern erörtert. Dieses Formular samt Merkblatt und Entscheidungsbäumen habe ich auch dem Düsseldorfer Kreis vorgestellt. Nach Verabschiedung des neuen BDSG sollen diese Unterlagen endgültig fertiggestellt und dann nach Möglichkeit von allen Datenschutzaufsichtsbehörden im Bundesgebiet einheitlich verwendet werden. Außerdem habe ich vor, diese Unterlagen im Internet verfügbar zu machen.

16.7.2. Ergebnisse der Registerprüfungen

Ich habe im Berichtsjahr bei insgesamt vier nach § 32 BDSG meldepflichtigen Stellen einfache Registerprüfungen nach § 38 Abs. 2 BDSG durchgeführt. Zusätzlich habe ich aufgrund einer Beschwerde und wegen öffentlicher Berichte in der Presse Anfang 2000 eine Datenschutzprüfung bei einem bremischen Internet-Provider durchgeführt, bei der ich auch die Umsetzung der Regelungen des Teledienstedatenschutzgesetzes (TDDSG) geprüft habe; vgl. hierzu die Nummer 3.5.4 in diesem Bericht.

Bei den einfachen Registerprüfungen nach § 38 Abs. 2 BDSG überprüfe ich lediglich das Bestehen der Meldepflicht nach § 32 BDSG sowie die Richtigkeit der Meldung, die Bestellung und Tätigkeit des betrieblichen Datenschutzbeauftragten nach den §§ 36 f. BDSG, die Verpflichtung der Mitarbeiter auf das Datengeheimnis gemäß § 5 BDSG und ggf. die Beachtung der für die DV- Servicebetriebe geltenden Regelungen zur Auftragsdatenverarbeitung nach § 11 BDSG. Technisch-organisatorische Sicherungsmaßnahmen, die Umsetzung der datenschutzrechtlichen Betroffenenrechte sowie die Zulässigkeit der personenbezogenen Datenverarbeitung werden hierbei nicht geprüft, dies bleibt gesonderten Prüfungen vorbehalten. Hierbei ist darauf hinzuweisen, dass die Zulässigkeit der personenbezogenen Datenverarbeitung, die bei den mir gemeldeten Auftragsdatenverarbeitern stattfindet, von den jeweiligen Auftraggebern datenschutzrechtlich zu verantworten ist. Der Auftragnehmer darf die Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten.

Bei meinen Prüfungen habe ich auch dieses Jahr wieder Mängel feststellen müssen. Die wesentlichen Mängel lagen wieder im Bereich der Registermeldungen (z. B. fehlende Meldung, Aktualität der Meldung), beim betrieblichen Datenschutzbeauftragten (z. B. fehlende bzw. nicht-formgerechte Bestellung, Bündelung mehrerer Funktionen, mangelhafte Aufgabenerfüllung), bei den Verpflichtungen der Mitarbeiter auf das Datengeheimnis und bei der Gestaltung des Vertragsverhältnisses zur Auftragsdatenverarbeitung. Bei dem geprüften Internet-Provider habe ich in allen Prüfpunkten Mängel feststellen müssen.

16.7.3. Bußgeldverfahren

Gegen eine Werbeagentur habe ich ein Bußgeldverfahren wegen Verstoßes gegen die Meldepflicht nach § 32 BDSG eingeleitet; dieses Verfahren war am Ende des Berichtsjahres noch nicht abgeschlossen.

16.8. EU-Initiativen und Verbreitung neuer IuK-Technik

- **EU-Initiativen**

Folgende EU-Richtlinien sollen bis Ende 2000 beschlossen werden: Copyright im Internet, Rechte und Pflichten im elektronischen Handel (E-Commerce), elektronische Unterschrift, Datenschutz in der EU und bei transatlantischer Internet-Nutzung.

Die Mitgliedsstaaten sollen bis Ende 2000 die lokalen Telefonnetzzugänge der Telekom-Gesellschaften liberalisieren, um die Kosten des Internet-Zugangs deutlich zu senken.

Die Mitgliedsstaaten sollen bis Ende 2001 alle Schulen mit einem Internet-Zugang ausstatten. Alle Lehrer sollten bis Ende 2002 Internet-geschult sein und allen Bürger bis Ende 2005 die Internet-Grundbegriffe nähergebracht werden.

Bis Ende 2000 sollen alle öffentlichen Ausschreibungen in der EU ab dem vorgeschriebenen Volumen im Internet zugänglich sein.

Die wichtigsten europäischen Universitäten sollen mit einem High-Speed-Datennetz untereinander verbunden werden. Bislang läuft ihre Kommunikation nicht selten über die USA wegen der besseren Kapazität der Datenkanäle.

Die EU-Kommission entwickelt eine Strategie gegen Kriminalität und Betrug im Internet (Cyber-Crime).

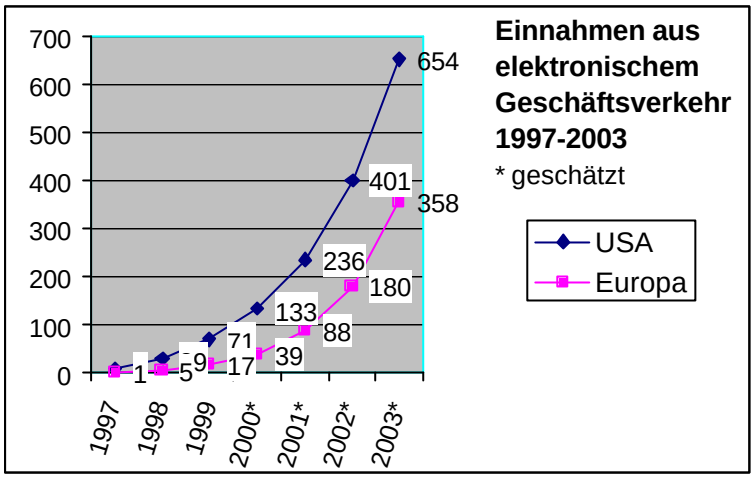
Die EU-Kommission will Mitte Juli bei der entscheidenden internationalen Konferenz den Domänen-Namen ".eu" am Ende von Internet-Adressen durchsetzen.

Die EU soll einen einheitlichen Befähigungsnachweis für Experten der Informationstechnologie (IT) einführen, um dem Arbeitskräfteengpass entgegenzuwirken.

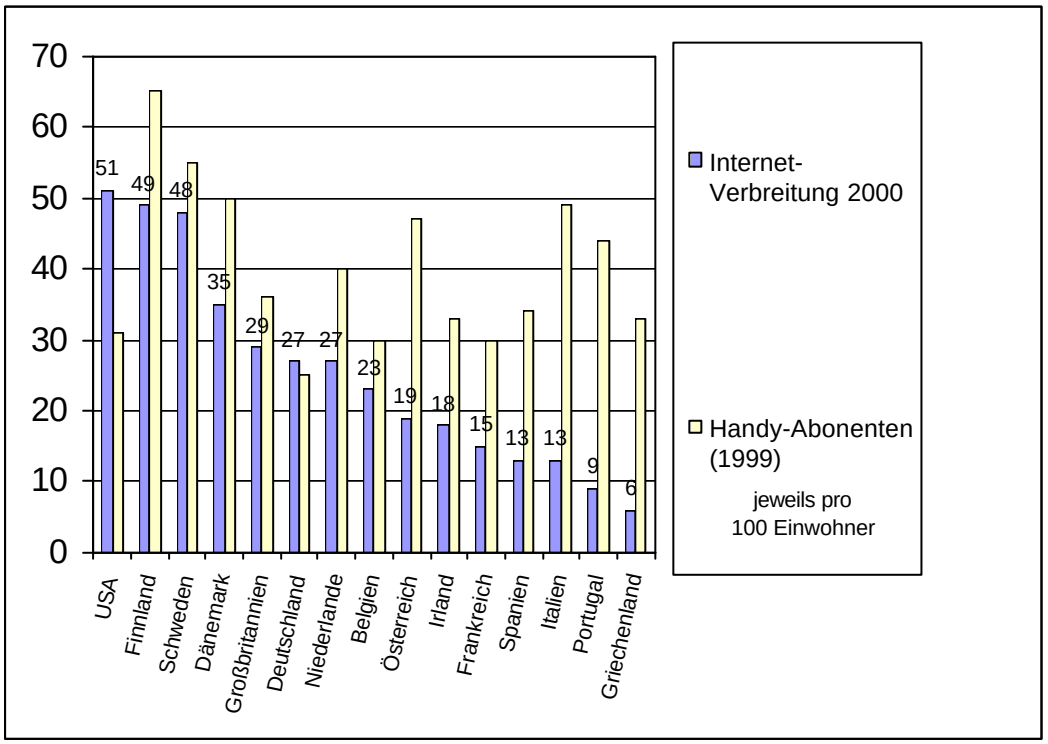
Die Mitgliedsstaaten sollen bis Ende 2000 der Europäischen Investitionsbank ermöglichen, zusätzliches Risikokapital für junge IT-Firmen bereitzustellen.

Alle Vorschläge: europa.eu.int/comm/information_society/eeurope/index_en.htm

- **e-commerce-Entwicklung**



- **Internet und Handy**



17. Die Entschließungen der Datenschutzkonferenzen im Jahr 2000

17.1. Risiken und Grenzen der Videoüberwachung

(Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000)

Immer häufiger werden Videokameras eingesetzt, die für Zwecke der Überwachung genutzt werden können. Ob auf Flughäfen, Bahnhöfen, in Ladenpassagen, Kaufhäusern oder Schalterhallen von Banken oder anderen der Öffentlichkeit zugänglichen Einrichtungen, überall müssen Bürgerinnen und Bürger damit rechnen, dass sie auf Schritt und Tritt offen oder heimlich von einer Videokamera aufgenommen werden. Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder sieht darin die Gefahr, dass diese Entwicklung zu einer Überwachungsinfrastruktur führt.

Mit der Videoüberwachung sind besondere Risiken für das Recht auf informationelle Selbstbestimmung verbunden. Weil eine Videokamera alle Personen erfasst, die in ihren Bereich kommen, werden von der Videoüberwachung unvermeidbar völlig unverdächtige Menschen mit ihren individuellen Verhaltensweisen betroffen. Erfassung, Aufzeichnung und Übertragung von Bildern sind für die Einzelnen in aller Regel nicht durchschaubar. Schon gar nicht können sie die durch die fortschreitende Technik geschaffenen Bearbeitungs- und Verwendungsmöglichkeiten abschätzen und überblicken. Die daraus resultierende Ungewissheit, ob und von wem sie beobachtet werden und zu welchen Zwecken dies geschieht, erzeugt einen latenten Anpassungsdruck. Dies beeinträchtigt nicht nur die grundrechtlich garantierten individuellen Entfaltungsmöglichkeiten, sondern auch das gesellschaftliche Klima in unserem freiheitlichen und

demokratischen Gemeinwesen insgesamt. Alle Menschen haben das Grundrecht, sich in der Öffentlichkeit zu bewegen, ohne dass ihr Verhalten durch Kameras aufgezeichnet wird.

Daher müssen

- eine strenge Zweckbindung,
- eine differenzierte Abstufung zwischen Übersichtsaufnahmen, dem gezielten Beobachten einzelner Personen, dem Aufzeichnen von Bilddaten und dem Zuordnen dieser Daten zu bestimmten Personen
- die deutliche Erkennbarkeit der Videoüberwachung für die betroffenen Personen,
- die Unterrichtung identifizierter Personen über die Verarbeitung ihrer Daten
- sowie die Löschung der Daten binnen kurzer Fristen

strikt sichergestellt werden.

Jede Einrichtung einer Videoüberwachung sollte der datenschutzrechtlichen Vorabkontrolle unterzogen werden. Das heimliche Beobachten und Aufzeichnen, die gezielte Überwachung bestimmter Personen sowie die Suche nach Personen mit bestimmten Verhaltensmustern müssen grundsätzlich verboten sein. Ausnahmen müssen im Strafprozessrecht und im Polizeirecht präzise geregelt werden. Videoüberwachung darf nicht

großflächig oder flächendeckend installiert werden, selbst wenn jeder Einsatz für sich gesehen gerechtfertigt wäre. Auch ein zeitlich unbegrenzter Einsatz ohne regelmäßige Erforderlichkeitsprüfung ist abzulehnen. Der Schutz der Freiheitsrechte erfordert überdies, dass heimliches Aufzeichnen und unbefugte Weitergabe oder Verbreitung von Aufnahmen ebenso strafbewehrt sein müssen wie der Missbrauch video-technisch gewonnener - insbesondere biometrischer - Daten und deren Abgleiche.

Dies bedeutet:

1. Bei einer gesetzlichen Regelung der Videoüberwachung durch öffentliche Stellen dürfen Einschränkungen nur aufgrund einer klaren Rechtsgrundlage erfolgen, die dem Grundsatz der Verhältnismäßigkeit Rechnung trägt.
    - Die Voraussetzungen einer Videoüberwachung und der mit ihr verfolgte Zweck müssen eindeutig bestimmt werden. *Dafür kommen - **soweit nicht überwiegende schutzwürdige Belange von Betroffenen entgegenstehen** - unter anderem in Betracht:*
        - *die Beobachtung einzelner öffentlicher Straßen und Plätze oder anderer öffentlich zugänglicher Orte, auf denen wiederholt Straftaten begangen worden sind, solange tatsächliche Anhaltspunkte dafür bestehen, dass dort weitere Straftaten begangen werden (Kriminalitätsschwerpunkte) und mit der Beobachtung neben der Sicherung von Beweisen eine Präventionswirkung erreicht werden kann; der Grundsatz der Verhältnismäßigkeit ist dabei strikt zu beachten. Ungezielte Verlagerungsprozesse sollten vermieden werden.*
        - *für die Verkehrslenkung nur Übersichtsaufnahmen,*
        - *der Schutz öffentlicher Einrichtungen im Rahmen der ordnungsbehördlichen Gefahrenabwehr, solange eine besondere Gefahrenlage besteht.*
        - Maßnahmen im Rahmen des Hausrechts dürfen den grundsätzlich unbeobachteten Besuch öffentlicher Gebäude nicht unverhältnismäßig einschränken.
    - Die Videoüberwachung ist für die Betroffenen durch entsprechende Hinweise erkennbar zu machen.
    - Bildaufzeichnungen sind nur zulässig, wenn und solange sie zum Erreichen des verfolgten Zweckes unverzichtbar sind. Die Anlässe, aus denen eine Bildaufzeichnung ausnahmsweise zulässig sein soll, sind im einzelnen zu bezeichnen. Die Aufzeichnungen sind unverzüglich zu löschen, wenn sie hierzu nicht mehr erforderlich sind oder überwiegende schutzwürdige Belange von Betroffenen entgegenstehen.
    - Werden die Aufnahmen einer bestimmten Person zugeordnet, ist diese zu benachrichtigen, sobald der Zweck der Speicherung dadurch nicht gefährdet wird.
    - Zur Prüfung der Normeffizienz ist festzulegen, dass das jeweils zuständige Parlament jährlich über die angeordneten Maßnahmen, soweit sie mit einer Speicherung der erhobenen Daten verbunden sind, und die mit ihnen erreichten Ergebnisse unterrichtet wird.

Bei der Videoüberwachung muss in besonderer Weise den Grundsätzen der Datensparsamkeit und Datenvermeidung Rechnung getragen werden. Die Chancen, die die modernen Technologien für die Umsetzung dieser Grundsätze, insbesondere für die Reduzierung auf tatsächlich erforderliche Daten bieten, sind zu nutzen.

2. Der Gesetzgeber ist auch aufgefordert, für die Videoüberwachung durch Private Regelungen zu schaffen, die den für die optisch-elektronische Beobachtung durch öffentliche Stellen geltenden Grundsätzen entsprechen. Dabei muss sichergestellt werden, dass optisch-elektronische Systeme, die die Identifizierung einzelner Personen ermöglichen, nur zur Abwehr von Gefahren für Personen und zum Schutz gewichtiger privater Rechte eingesetzt werden dürfen. Die privatrechtlichen Regelungen zum Schutz des eigenen Bildes durch das Vertragsrecht, das Deliktsrecht, das Besitz- und Eigentumsrecht, das Kunsturheberrecht und die dazu ergangene Rechtsprechung reichen nicht aus.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder erwartet, dass die Gesetzgeber bei der Novellierung der Datenschutzgesetze und anderer Gesetze diese Grundsätze berücksichtigen.

Die kursiv gedruckte Passage wurde bei Stimmenthaltung der Datenschutzbeauftragten der Länder Brandenburg, Bremen, Mecklenburg-Vorpommern und Nordrhein-Westfalen angenommen.

17.2. Für eine freie Telekommunikation in einer freien Gesellschaft

(Entschließung der 59.Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000)

Umfang und Intensität der Eingriffe in das von Art. 10 Grundgesetz geschützte Fernmeldegeheimnis haben in den letzten Jahren deutlich zugenommen. Ursächlich hierfür sind zum einen folgende Aspekte:

- **Erhebliche Zunahme der Telekommunikationsvorgänge**

  Die Zahl der Telekommunikationsvorgänge hat sich vervielfacht. Darüber hinaus werden neben dem traditionellen Telefon neue Kommunikationsmöglichkeiten wie Fax und PC-Fax, das Mobiltelefon, E-Mail und mail-boxen sowie das Internet genutzt.

  - **Stark angestiegener Umfang und wesentlich verbesserte Aussagequalität der Daten**
    - Die digitale Datenverarbeitung ermöglicht detaillierte Auswertungen großer Datenmengen.
    - Die Datenverarbeitungsnetze bieten mehr und mehr aussagekräftige Bestandsdaten, wozu auch E-Mail-Adresse, IP-Nummer oder domain name gehören. So können sich bei Mitgliedschaft in geschlossenen Netzen sogar Rückschlüsse auf Lebensanschauungen oder bestimmte Problemlagen ergeben, z. B. bei der Mitgliedschaft in bestimmten Interessengemeinschaften, etwa Aids-Selbsthilfegruppen.

- Die Verbindungsdaten geben in der Regel Auskunft, wer wann mit wem wie lange und wie häufig kommuniziert hat; werden fremde Geräte verwendet, geraten Unbeteiligte in Verdacht.
- Aus den Nutzungsdaten von Tele- und Mediendiensten lassen sich Rückschlüsse auf Interessengebiete und damit auf persönliche Eigenheiten und das Verhalten der Nutzenden ziehen.
- Mobiltelefone ermöglichen schon im Stand-by-Modus die Bestimmung ihres Standorts.

- **Erleichterte Kenntnisnahme und Weiterverarbeitung dieser Daten**

  Die wesentlich erweiterten und einfacher nutzbaren technischen Möglichkeiten erlauben es, an verschiedenen Orten gespeicherte Daten zur Kenntnis zu nehmen und zu verarbeiten.

- **Entwicklung des Internets zum Massenkommunikationsmittel**

  Über das Netz werden immer mehr Alltagsgeschäfte abgewickelt: Wahrnehmung verschiedenartiger Informationsangebote, Erledigung von Bankgeschäften, Buchung von Reisen oder Bestellung von Waren und Dienstleistungen in virtuellen Kaufhäusern (e-commerce). Dadurch fallen immer mehr auswertbare Informationen über Lebensgewohnheiten und Bedürfnisse der Bürgerinnen und Bürger an.

- **Schwer durchschaubare Rechtslage**

  Die Zersplitterung der Regelungen in Strafprozess-, Telekommunikations- und Multimediarecht machen diese wenig transparent und schwer anwendbar.

Zum anderen ist dieser größere, leichter auswert- und verarbeitbare Datenpool wachsenden Zugriffswünschen der Sicherheitsbehörden im weitesten Sinn auf nationaler und internationaler Ebene ausgesetzt:

- Die Zahlen der Telekommunikations-Überwachungsanordnungen in den letzten Jahren sind kontinuierlich angestiegen: *1995: 3667, 1996: 6428, 1997: 7776, 1998: 9802*
- Immer mehr Straftatbestände wurden als Grund für eine Telekommunikationsüberwachung in § 100 a der Strafprozessordnung (StPO) einbezogen - der Katalog wurde seit Einführung 11 mal erweitert und damit bis heute nahezu verdoppelt. Neue Erweiterungen sind im Gespräch.
- Die Telekommunikationsanbieter werden verpflichtet, technische Einrichtungen zur Umsetzung der Überwachungsanordnungen zu installieren und Kundendateien für Abfragen durch die Sicherheitsbehörden vorzuhalten zur Feststellung, mit welchen Anbietern verdächtige Personen einen Vertrag haben. Diese Verpflichtung wurde auch auf die Anbieter nicht gewerblicher Netze ausgedehnt und kann nach dem Gesetzeswortlaut auch Hotels, Betriebe, Behörden oder möglicherweise sogar Krankenhäuser betreffen.
- Ein europäischer Anforderungskatalog für Überwachungsmöglichkeiten unter dem Namen "ENFOPOL", befasst sich u. a. mit der Frage, welchen Anforderungen die

Netzbetreiber bzw. Diensteanbieter genügen müssen, damit die auf der Grundlage nationaler Ermächtigungsgrundlagen zulässige Telekommunikationsüberwachung technisch durchführbar ist. Die G8-Staaten haben noch weitergehende Beschlüsse gefasst.

Forderungen zur Gewährleistung der freien Telekommunikation

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat bereits 1996 ein Positionspapier erarbeitet. Vor diesem Hintergrund fordert die Konferenz:

- Freie Telekommunikation ist unabdingbar für eine freiheitliche demokratische Kommunikationsgesellschaft. Sie wird durch das Fernmeldegeheimnis geschützt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichts zu den verdachtslosen Abhörmaßnahmen des BND (BVerfG, Urt. v. 14.7.1999, 1 BvR 2226/94 u. a.) auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird. Die Geltung des Fernmeldegeheimnisses ist deshalb auch für den Bereich der Tele- und Mediendienste ausdrücklich klarzustellen.
- Notwendig ist eine bürgerrechtsfreundliche technische Infrastruktur nach dem Grundsatz der Datenvermeidung und dem Datensparsamkeitsprinzip. Dabei ist der Einsatz datenschutzfreundlicher Technologien besonders zu fördern. Anonyme und pseudonyme Nutzungsmöglichkeiten müssen nach dem Vorbild des Teledienstedatenschutzgesetzes als Pflichtangebote vorgehalten werden. Die Nutzung dieser Angebote darf nicht von der Speicherung von Bestandsdaten abhängig gemacht werden. Eine Vorratshaltung von Daten Unverdächtiger über den Betriebszweck hinaus zu Zwecken der Verfolgung eventueller, noch gar nicht absehbarer zukünftiger Straftaten ist als Überwachung auf Vorrat abzulehnen.
- Notwendig ist deshalb ein zusammenfassendes, in sich schlüssiges System von Regelungen staatlicher Eingriffe in das Kommunikationsverhalten, das dem besonderen Gewicht des Grundrechts auf eine unbeobachtete Telekommunikation unter Beachtung der legitimen staatlichen Sicherheitsinteressen Rechnung trägt.
- Als Grundlage hierfür ist eine Evaluierung der bestehenden Eingriffsregelungen nach objektiven, nicht zielorientierten Maßstäben vorzunehmen hinsichtlich Effektivität auf der einen und Eingriffsumfang auf der anderen Seite. Eine gesetzliche Berichtspflicht über Anlass, Verlauf, Ergebnisse und Anzahl der Betroffenen ist auch für Telekommunikationsüberwachungen einzuführen. Dass auch Unverdächtige von Abhör- und Kontrollmaßnahmen betroffen sein können, ist dabei besonders zu berücksichtigen.
- Der aus der Frühzeit der analogen Fernsprechtechnik stammende § 12 Fernmeldeanlagengesetz, der die Herausgabe von Verbindungsdaten vergangener, nach bestrittener Rechtsprechung sogar zukünftiger Telekommunikationsvorgänge ohne Beschränkung auf schwerere Straftaten ermöglicht, muss wegen der erheblich höheren Aussagefähigkeit der digitalen Verbindungsdaten und des damit verbundenen Eingriffs in das Fernmeldegeheimnis zügig durch eine weniger weit reichende Regelung in der StPO ersetzt werden.

- Die Anforderungen aus dem bereits zitierten Urteil des Bundesverfassungsgerichts zur Telekommunikationsüberwachung sind unverzüglich umzusetzen.
- Die Ausweitung der Mitwirkungspflichten bei Überwachungsmaßnahmen auf Nebenstellenanlagen in Hotels, Krankenhäusern oder Betrieben wäre unverhältnismäßig. Es muss deshalb verbindlich klargestellt werden, dass die Betreiber dieser Nebenstellenanlagen nicht zur Bereitstellung entsprechender technischer Einrichtungen verpflichtet werden. Das Eckpunktepapier des Bundesministeriums für Wirtschaft und Technologie, das als Grundlage für einen Entwurf der Telekommunikations-Überwachungverordnung dient und nach verschiedenen Gruppen von Betreibern differenziert, ist dazu ein erster Schritt. Auch muss möglichst durch eine Gesetzesänderung verhindert werden, dass die Verpflichtung, Kundendateien zu führen, auch für die o. g. Nebenstellenanlagen gilt. Darüber hinaus dürfen Anbieter von Guthabenkarten zur Mobiltelefonie nicht dazu verpflichtet werden, Identifikationsdaten ihrer Kunden, die sie für betriebliche Zwecke nicht benötigen, ausschließlich für Zwecke der Strafverfolgungsbehörden und der Nachrichtendienste zu erheben und zum Abruf bereitzuhalten.
- Die Beachtung des Fernmeldegeheimnisses erfordert zwingend die Verschlüsselung von elektronischen Mitteilungen in offenen Netzen. Das Eckpunktepapier der Bundesregierung zur deutschen Kryptopolitik, das eine Kryptoregulierung ablehnt, ist ein wichtiger Schritt in die richtige Richtung. Gewerbliche Telekommunikationsdienstleister sollten gesetzlich verpflichtet werden, die Möglichkeit der verschlüsselten Kommunikation kostenlos zu unterstützen.
- Berufsgruppen, die besonderen Verschwiegenheitspflichten unterliegen, wie Ärztinnen und Ärzte, Anwältinnen und Anwälte, Psychologinnen und Psychologen, bedürfen besonders im Interesse ihrer Klientel eines umfassenden Schutzes ihrer Telekommunikation.
- Straftaten gegen den Schutz der Privatsphäre ist wirksamer entgegenzutreten. Notwendig sind z. B. die Prüfung eines Verbots des freien Verkaufs von Abhörtechnik, eine Verbesserung der Strafverfolgung im Bereich illegaler Abhörmaßnahmen und eine Verschärfung des strafrechtlichen Schutzes des Fernmeldegeheimnisses.

17.3. Data Warehouse, Data Mining und Datenschutz

(Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000)

Mit der ständig zunehmenden Leistungsfähigkeit der Informations- und Kommunikationstechnik wächst die Menge gespeicherter personenbezogener Daten in Wirtschaft und Verwaltung weiter an. Zunehmend kommen automatisierte Verfahren zum Einsatz, die das gesammelte Datenmaterial effektiv verwalten und analysieren. Im "Data Warehouse" werden alle verwendbaren Daten in einem einheitlichen Datenpool losgelöst von ihrer ursprünglichen Verwendung zusammengeführt. "Data Mining" bietet Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten

Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen.

Diese Entwicklung schafft neben Vorteilen neue Gefahren und Risiken für das Grundrecht auf informationelle Selbstbestimmung und für den Schutz der Privatheit: Persönlichkeitsprofile, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherung sind befürchtete Gefahren.

Die Konferenz der Datenschutzbeauftragten weist auf Folgendes hin:

- Nach dem grundrechtlichen Gebot der Zweckbindung dürfen personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarungen verwendet werden. Eine personenbezogene Speicherung in einem allgemein verwendbaren Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck und stellt eine Speicherung auf Vorrat ohne Zweckbindung dar. Personenbezogene Daten, die bei der öffentlichen Verwaltung vorhanden sind, sind in ihrer Zweckbestimmung grundrechtlich geschützt und dürfen nicht für unbestimmte Zwecke in einem "Daten-Lagerhaus" gesammelt werden.
- Eine Zweckänderung ist nur mit Einwilligung der Betroffenen zulässig, nachdem diese über die Tragweite der Einwilligung aufgeklärt worden sind. Eine Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist deswegen unwirksam.
- Gestaltung und Auswahl von Datenverarbeitungs-Systemen haben sich an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten. Anonyme und pseudonyme Verfahren sind datenschutzrechtlich unbedenklich.
- Verfahren sind so zu gestalten, dass die Betroffenen hinreichend unterrichtet werden, damit sie jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen können. Sie haben insbesondere das Recht, eine erteilte Einwilligung jederzeit zurückzuziehen.
- Die gesetzlichen Speicherfristen, nach deren Ablauf die Daten zwingend archiviert oder gelöscht werden müssen, sind strikt zu beachten. Deswegen ist die Einrichtung von permanenten "Daten-Lagerhäusern" rechtswidrig.
- Die Europäische Datenschutzrichtlinie spricht grundsätzlich jeder Person das Recht zu, keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden (Art. 15). "Data Mining" ist ein Instrument, das für solche Entscheidungen herangezogen werden kann.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ruft die Hersteller und Anwender von "Data Warehouse"- und "Data Mining"-Verfahren dazu auf, solchen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

17.4. Konsequenzen aus dem Urteil des Bundesverfassungsgerichtes zu den Abhörmaßnahmen des BND

(Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000)

Das Bundesverfassungsgericht hat für die Verwendung von Daten, die aus der Fernmeldeüberwachung gewonnen wurden, deutliche Schranken gezogen, die weit über den Gegenstand des Verfahrens hinaus bedeutsam sind.

Das Gericht betont die Bedeutung des Fernmeldegeheimnisses zur Aufrechterhaltung einer freien Telekommunikation, die eine Grundvoraussetzung der Informationsgesellschaft darstellt. Dieses Grundrecht erstreckt sich nach dem Urteil des Bundesverfassungsgerichtes zu den verdachtslosen Abhörmaßnahmen des BND auf jede Verwendung von Kommunikationsdaten bis hin zur Löschung, gleich welche Kommunikationstechnik genutzt wird (Telefon, E-Mail, Telefax, Internet-Abrufe o.ä.).

Die Anforderungen des Urteils müssen auch Konsequenzen für Fallgestaltungen, bei denen personenbezogene Daten durch Maßnahmen erlangt werden, die in ihrer Art und Schwere einer Beschränkung des Fernmeldegeheimnisses gleichkommen, insbesondere etwa bei einer Erhebung durch Abhören und Aufzeichnen des nicht öffentlich gesprochenen Wortes mit dem Einsatz technischer Mittel.

Die Anforderungen aus dem Urteil sind unverzüglich umzusetzen:

- Zur Sicherung der Zweckbindung der erlangten Daten und für die Kontrolle ihrer Verwendung muss ihre Herkunft aus Eingriffen in das Fernmeldegeheimnis oder vergleichbaren Eingriffen durch eine entsprechende Kennzeichnung nach der Erfassung auch bei den Übermittlungsempfängern erkennbar bleiben.
- Die erlangten Daten müssen bei allen speichernden Stellen unverzüglich gelöscht werden, wenn sie nicht mehr erforderlich sind - es sei denn, der Rechtsschutz der Betroffenen würde dadurch verkürzt. Die Praxis von Verfassungsschutzämtern, nicht (mehr) erforderliche Daten, wenn sie sich in Unterlagen befinden, nicht zu schwärzen, kann - zumindest bei Daten, die durch Eingriffe in das Fernmeldegeheimnis oder vergleichbare Eingriffe erlangt wurden - nicht mehr aufrechterhalten werden. Um die Notwendigkeit einer späteren Schwärzung zu vermeiden, sollten bereichsspezifischen Vernichtungsregelungen bereits bei der Aktenführung Rechnung getragen werden.

  Die Vernichtungspflicht ist im Licht von Art. 19 Abs. 4 GG zu verstehen. Danach sind Maßnahmen unzulässig, die darauf abzielen oder geeignet sind, den Rechtsschutz der Betroffenen zu vereiteln. Eine Löschung oder Vernichtung ist nach einem Auskunftsantrag bei allen personenbezogenen Daten unzulässig. Zudem sind personenbezogene Daten, die durch die o.g. Maßnahmen erlangt wurden, nach einer Unterrichtung der Betroffenen für einen angemessenen Zeitraum - ausschließlich zum Zweck der Sicherung des Rechtsschutzes - aufzubewahren.
- Überwachte Personen müssen von Eingriffen unterrichtet werden, sobald dadurch der Zweck der Maßnahme nicht mehr gefährdet wird; dies gilt auch für weitere Be-

troffene, es sei denn, überwiegende schutzwürdige Belange der überwachten Person stehen dem entgegen (Schutz vor unnötiger Bloßstellung).

Wie bei Eingriffen in das Fernmeldegeheimnis ist dies auch bei anderen verdeckten Maßnahmen Voraussetzung dafür, dass die Betroffenen von den ihnen zustehenden Rechten Gebrauch machen können, und daher von Art. 19 Abs. 4 GG geboten. Speicherfristen können die Unterrichtungspflicht nicht beseitigen, irrelevante Daten sind umgehend zu löschen.

Damit sind Regelungen z. B. in Landesverfassungsschutz- und Polizeigesetzen nicht zu vereinbaren, wonach eine Unterrichtung der Betroffenen über Datenerhebungen, die in ihrer Art und Schwere einem Eingriff in das Fernmeldegeheimnis gleichkommen, unterbleibt, wenn sich auch nach fünf Jahren nicht abschließend beurteilen lässt, ob eine Gefährdung des Zweckes des Eingriffes ausgeschlossen werden kann.

Zusätzlich zur unbefristeten Benachrichtigungspflicht ist eine Mitteilung an die Datenschutzkontrollstelle für den Fall vorzusehen, dass die Unterrichtung der Betroffenen länger als fünf Jahre zurückgestellt wird.

- Der Umgang des Verfassungsschutzes mit personenbezogenen Daten, die in Durchbrechung des Fernmeldegeheimnisses erhoben worden sind, ist durch eine unabhängige Datenschutzkontrollstelle lückenlos zu überprüfen.
- Eine Kontrolllücke bei personenbezogenen Daten, die durch G 10-Maßnahmen erlangt wurden, wäre verfassungswidrig. Das Bundesverfassungsgericht hat hervorgehoben, dass Art. 10 GG eine umfassende Kontrolle durch unabhängige und an keine Weisung gebundene staatliche Organe und Hilfsorgane gebietet.
- Die Kontrolle muss sich auf den gesamten Prozess der Erfassung und Verwertung der Daten einschließlich der Benachrichtigung - bei Datenübermittlungen auch bei den Datenempfängern - erstrecken.
- Der Gesetzgeber sollte festlegen, dass die Übermittlung der Daten, die Prüfung der Erforderlichkeit weiterer Speicherung sowie die Durchführung der Vernichtung und Löschung der Daten aus G 10-Maßnahmen zu protokollieren sind.
- Für eine effektive Kontrolle sind die zuständigen Stellen personell und sachlich angemessen auszustatten.

Die Ausführungsgesetze zum G 10 müssen hinsichtlich der Kontrolle eindeutig sein. Es ist klarzustellen, inwieweit die G 10-Kommissionen auch für die Kontrolle der weitergehenden Datenverarbeitung zuständig sind oder inwieweit die Kontrolle von den Datenschutzbeauftragten wahrzunehmen ist.

17.5. Strafverfahrensänderungsgesetz 1999 (StVÄG 1999)

(Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000)

Die Datenschutzbeauftragten des Bundes und der Länder begrüßen es, dass mit dem Entwurf für ein Strafverfahrensänderungsgesetz 1999 die Strafprozessordnung endlich

die seit fast zwei Jahrzehnten überfälligen datenschutzrechtlichen Regelungen erhalten soll. Sie stellen jedoch fest, dass der nunmehr vorliegende Gesetzesbeschluß des Bundestages nicht alle wichtigen Forderungen des Datenschutzes erfüllt.

Darüber hinaus will der Bundesrat das Datenschutzniveau weiter absenken und hat auch zu diesem Zweck den Vermittlungsausschuss angerufen. Zu kritisieren ist, dass

- Zeuginnen und Zeugen auch bei Straftaten ohne erhebliche Bedeutung durch Öffentlichkeitsfahndung im Fernsehen oder Internet gesucht werden können,
- Zweckbindungen präventivpolizeilicher Daten, darunter auch der Erkenntnisse aus verdeckten Datenerhebungsmaßnahmen, wie z. B. einem Großen Lauschangriff oder einem Einsatz verdeckter Ermittler, völlig aufgehoben werden, so dass sie uneingeschränkt zur Strafverfolgung genutzt werden können,
- umgekehrt aber auch Informationen aus Strafverfahren über die Gefahrenabwehr hinaus uneingeschränkt zur Gefahrenvorsorge genutzt werden können,
- nicht am Verfahren beteiligte Dritte schon bei "berechtigtem Interesse" Einsicht in Strafverfahrensakten bekommen können.

Die Datenschutzbeauftragten des Bundes und der Länder sehen den verfassungsrechtlich gebotenen Ausgleich zwischen Persönlichkeitsschutz und Interessen der Strafverfolgungsbehörden nicht mehr als gewährleistet an, falls die Vorschläge des Bundesrates Eingang in die Strafprozessordnung finden sollten. Die Datenschutzbeauftragten fordern daher den Vermittlungsausschuss auf, die Änderungsanträge zurückzuweisen. Stattdessen sind Regelungen in der Strafprozessordnung vorzusehen, die geeignet sind, bei einer effektiven Strafverfolgung die Persönlichkeitsrechte der Betroffenen angemessen zu gewährleisten.

17.6. Unzulässiger Speicherungsumfang in "INPOL-neu" geplant

(Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000)

Das Bundeskriminalamt und die Polizeien der Bundesländer konzipieren seit geraumer Zeit unter der Bezeichnung "INPOL-neu" eine Fortentwicklung des gemeinsamen Informationssystems. Inzwischen steht der Beginn der schrittweisen Einführung des neuen Datenaustauschsystems kurz bevor.

Das Informationssystem INPOL wirft in vielfacher Hinsicht datenschutzrechtliche Probleme auf. Die Datenschutzbeauftragten des Bundes und der Länder haben mehrfach aus konkretem Anlass darauf hingewiesen, dass nicht jede mit den heutigen technischen Möglichkeiten realisierbare oder mit polizeifachlicher Erforderlichkeit begründete Verarbeitung personenbezogener Daten zulässig ist. Bereits bei der Konzeption des INPOL-Systems muss vielmehr dafür Sorge getragen werden, dass in das Recht der Bürgerinnen und Bürger auf informationelle Selbstbestimmung nur soweit eingegriffen wird, wie dies im Rahmen der Erforderllichkeit für die polizeiliche Aufgabenerfüllung durch Rechtsvorschriften erlaubt wird.

Es besteht jedoch Grund zu der Sorge, dass es bei der Neugestaltung des INPOL-Systems zu falschen Weichenstellungen mit der Folge unzulässiger Verarbeitung personenbezogener Daten kommt. Die zu befürchtende Fehlentwicklung liegt darin, dass das Bundeskriminalamt und die Landeskriminalämter planen, künftig im Bundes-Kriminalaktennachweis (KAN) die "gesamte kriminelle Karriere" jeder Person abzubilden, die aus Anlass eines INPOL-relevanten Delikts erfasst ist. Es sollen in diesen Fällen auch Daten über solche Straftaten gespeichert und zum Abruf bereit gehalten werden, die weder von länderübergreifender oder internationaler noch von besonderer Bedeutung sind.

§ 2 Abs. 1 BKAG beschränkt die Zuständigkeit des BKA (als Zentralstelle des polizeilichen Informationssystems) sowohl im präventiven als auch im repressiven Bereich auf "Straftaten mit länderübergreifender, internationaler oder erheblichen Bedeutung". Der Wortlaut ist eindeutig. Anknüpfungspunkt und Gegenstand der Einteilung in INPOL-relevante Informationen einerseits und INPOL-irrelevante Informationen andererseits sind die "Straftaten", nicht die einzelne Person und auch nicht das "Gesamtbild einer Person". Der Gesetzeswortlaut bildet die Grenze der Auslegung; eine über den Wortsinn hinausgehende Anwendung verstößt gegen das Gesetz. Daher ist es unzulässig, die Frage der INPOL-Relevanz unabhängig von der konkreten einzelnen Straftat zu beurteilen. Vielmehr dürfen im Bundes-KAN nur Informationen zu solchen Straftaten verarbeitet werden, die im Einzelfall die in § 2 Abs. 1 BKAG aufgestellte Bedeutungsschwelle überschreiten.

Die Datenschutzbeauftragten des Bundes und der Länder fordern das Bundesinnenministerium und die Innenministerien der Länder auf, von der geschilderten KAN-Erweiterung abzusehen.

17.7. Auftragsdatenverarbeitung durch das Bundeskriminalamt

(Entschließung zwischen der 59. und 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder)

Im Rahmen der Neukonzeption des polizeilichen Informationssystems INPOL ist geplant, neben bundesweit verfügbaren Verbunddaten auch Landesdatenbestände im Wege der Auftragsdatenverarbeitung logisch getrennt in der INPOL-Datenbank zu speichern. Zudem sollen aufgrund bilateraler Absprachen landesspezifische Informationen in bestimmtem Umfang gespeichert werden können und ebenso gegenseitige Zugriffe einzelner Länder auf die Datenbestände ermöglicht werden.

§ 2 Abs. 5 des Bundeskriminalamtgesetzes lässt grundsätzlich eine Unterstützung der Länder bei deren Datenverarbeitung auf Ersuchen, also in Einzelfällen, zu. Diese Vorschrift kann auch herangezogen werden, wenn aufgrund besonderer Dringlichkeit, wie gegenwärtig bei der Realisierung von INPOL-neu, eine zeitlich befristete Auftragsdatenverarbeitung von Landesdaten geplant ist. Hierzu sind Ende vergangenen Jahres entsprechende Beschlüsse des Arbeitskreises und der Innenministerkonferenz gefasst worden.

Diese Entwicklung birgt aus der Sicht der Datenschutzbeauftragten die Gefahr, dass weitere Beschlüsse folgen werden, die die dauerhafte Speicherung von Landesdaten beim BKA begründen; bereits jetzt sind Tendenzen deutlich, die zentralisierte Speicherung der Daten auch zur Erleichterung der gegenseitigen Zugriffe auf Landesdaten zu nutzen.

Die Notwendigkeit der zentralen Datenspeicherung beim Bundeskriminalamt wird im Wesentlichen mit Kosten- und Zeitargumenten begründet. Diese sind jedoch aus datenschutzrechtlicher Sicht nicht geeignet, eine Erweiterung der zentralen Datenverarbeitung beim Bundeskriminalamt zu begründen.

Die dauerhafte zentrale Datenhaltung beim BKA würde die informationelle Trennung von Landesdaten und Verbunddaten aufweichen; die in § 2 Abs. 1 BKA-Gesetz statuierte Schwelle, dass nur Daten über Straftaten von länderübergreifender, internationaler oder sonst erheblicher Bedeutung beim BKA verarbeitet werden dürfen, würde schleichend umgangen.

Eine dauerhafte zentrale Landesdatenhaltung beim Bundeskriminalamt beinhaltet eine neue, bei der augenblicklichen Rechtslage unakzeptable Qualität polizeilicher Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder fordern dazu auf, die für die Datenverarbeitung beim Bundeskriminalamt gesetzlich gezogenen Grenzen strikt zu beachten. Sie appellieren an die Innenminister/-senatoren von Bund und Ländern, an den bisherigen Beschlüssen festzuhalten und die Polizeien der Länder, wie ursprünglich geplant, aufzufordern, unverzüglich eigene Datenverarbeitungsverfahren zu entwickeln. Bis zur Realisierung dieser Verfahren könnte allenfalls eine übergangsweise Lösung als Auftragsdatenverarbeitung unter Wahrung datenschutzrechtlicher Anforderungen ermöglicht werden. Daneben steht das Angebot des Bundeskriminalamtes, kostenlos Software von INPOL-neu zur Verfügung zu stellen. Diese Lösung würde auch das vorgetragene Kostenargument entkräften.

17.8. Effektive parlamentarische Kontrolle von Lauschangriffen durch aussagekräftige jährliche Berichte der Bundesregierung

(Entschließung der Datenschutzbeauftragten des Bundes und der Länder vom 26. Juni 2000)

Die Bundesregierung hat den Bundestag jährlich über die nach Art. 13 Abs. 3 GG zur Strafverfolgung eingesetzten "Großen Lauschangriffe" zu unterrichten. § 100 e StPO konkretisiert die Berichtspflicht dahingehend, dass die Bundesregierung aufgrund von Mitteilungen der Staatsanwaltschaften der Länder den Bundestag über Anlass, Umfang, Dauer, Ergebnis und Kosten der Maßnahmen zu unterrichten hat.

Diese Berichte sollen eine laufende parlamentarische Kontrolle dieser mit intensiven Grundrechtseingriffen verbundenen Maßnahmen ermöglichen. Der Bundestag soll auf-

grund der Berichte in die Lage versetzt werden, die Angemessenheit und Eignung der Maßnahmen zu überprüfen.

Diesen Anforderungen wird der erste von der Bundesregierung vorgelegte Bericht nicht in vollem Umfang gerecht. So wurde nur die Gesamtzahl der von der Anordnung Betroffenen erfasst, wobei zwischen Beschuldigten und nicht beschuldigten Wohnungsinhabern unterschieden wird.

Nach § 100 e Abs. 1 StPO muss über den Umfang der Maßnahme berichtet werden. Hierzu zählt die Angabe über die Anzahl aller von der Maßnahme betroffenen Personen, nicht nur der in der gerichtlichen Anordnung genannten. Von dem "Großen Lauschangriff" ist jeder betroffen, dessen gesprochenes Wort in der Wohnung abgehört wird. Er greift auch in die grundrechtlich geschützten Rechte der am Verfahren Unbeteiligten, wie z. B. unverdächtige Familienangehörige, Bekannte, Besucherinnen und Besucher sowie sonstige Personen, die nicht selbst Wohnungsinhaber sind, ein. Dem wollte der Gesetzgeber mit der Einführung der Berichtspflicht Rechnung tragen.

Die Beschränkung der Berichtspflicht auf Wohnungsinhaber und Beschuldigte gibt nicht den wirklichen Umfang der von der Maßnahme betroffenen Personen wieder. Somit erfüllt sie den Zweck der im Grundgesetz vorgesehenen Berichtspflicht nicht.

Darüber hinaus wäre es wünschenswert, wenn - wie in den "Wire-tap-Reports" der USA - die Anzahl der abgehörten Gespräche und die Anzahl der Gespräche, die mit dem Ermittlungsverfahren in Zusammenhang stehen, die Art der betroffenen Räume (Geschäftsräume, Wohnung, Restaurant etc.), die Anzahl und Dauer der angeordneten Verlängerungen der Maßnahme, die Zahl der Verhaftungen, Anklageerhebungen und Verurteilungen, zu denen die Maßnahme beigetragen hat, angegeben werden.

Die Länder haben nach Art. 13 Abs. 6 Satz 3 GG eine gleichwertige parlamentarische Kontrolle zu gewährleisten. Die oben genannten Forderungen gelten deshalb gleichermaßen bzw. in entsprechender Weise für die den Landesparlamenten vorzulegenden jährlichen Berichte über die nach § 100 c Abs. 1 Nr. 3 StPO durchgeführten Maßnahmen bzw. über die von der Polizei zur Gefahrenabwehr veranlassten "Großen Lauschangriffe".

17.9. Datenschutzrechtliche Konsequenzen aus der Entschlüsselung des menschlichen Genoms

(Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000)

Bei der Entschlüsselung des menschlichen Genoms sind in den letzten Monaten wohl entscheidende Durchbrüche gelungen. Für mehr als 20, oft vererbliche Krankheiten sind bereits Gentests zu erwerben, mit denen in Labors analysiert werden kann, ob eine Erkrankung vorliegt bzw. in welchem Umfang ein Erkrankungsrisiko besteht. Viele dieser Krankheiten sind allerdings bisher nicht heil- oder behandelbar.

Gentechnische Untersuchungen beim Menschen eröffnen den Zugang zu höchstpersönlichen und hochsensiblen Informationen in einem Maße, das die Intensität bisheriger personenbezogener Informationen ganz erheblich übersteigt. Durch den genetischen Ein-

blick in den Kernbereich der Privatsphäre, etwa in Gesundheitsdisposition, Anlagen der Persönlichkeitsstruktur oder den voraussichtlichen Lebensverlauf, entsteht eine ganz neue Qualität des Wissens und des Offenlegens von persönlichsten Daten. Sowohl für die Betroffenen als auch für dritte Personen, insbesondere Familienangehörige, ist es von entscheidender Bedeutung, ob und inwieweit sie selbst und wer außer ihnen von den Ergebnissen Kenntnis bekommt. Davor steht die Frage, ob und aus welchen Anlässen überhaupt genetische Untersuchungen am Menschen vorgenommen werden dürfen. Zur informationellen Selbstbestimmung gehört auch das Recht auf Nichtwissen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder fordert, dass für die Zulässigkeit gentechnischer Untersuchungen beim Menschen und für den Umgang mit den dabei gewonnenen Informationen sehr schnell klare und verbindliche Prinzipien entwickelt werden, um auch die informationelle Selbstbestimmung in diesem Kernbereich zu sichern und zugleich eine "genetische Diskriminierung" bei der Gewinnung oder Verwendung genetischer Informationen, etwa im Arbeitsverhältnis oder beim Abschluss von Versicherungsverträgen zu verhindern. Auf der Grundlage dieser und in der "Entschließung über Genomanalyse und informationelle Selbstbestimmung" vom 26. Oktober 1989 formulierten Grundsätze wird die Konferenz an der Ausgestaltung mitwirken.

Die Datenschutzbeauftragten erinnern an ihre Grundsätze aus der Entschließung von 1989 bezüglich der Genomanalyse:

1. Die Genomanalyse darf grundsätzlich nur auf freiwilliger Basis nach umfassender Aufklärung der Betroffenen vorgenommen werden; ausgenommen sind Straf- und Abstammungsverfahren.
2. Die jederzeit widerrufliche Einwilligung muss sich auch auf die weitere Verwendung der gentechnischen Informationen erstrecken. Im Falle eines Widerrufs sind die gewonnnen Informationen zu löschen oder an den Betroffenen herauszugeben.
3. Jede Genomanalyse muss zweckorientiert vorgenommen werden. Es ist diejenige genomanalytische Methode zu wählen, die keine oder die geringste Menge an Überschussinformationen bringt. Überschussinformationen sind unverzüglich zu vernichten.
4. Es ist zu prüfen, inwieweit genomanalytische Untersuchungsmethoden einer staatlichen Zulassung bedürfen. Für DNA-Sonden ist dies jedenfalls zu bejahen.
5. Die Genomanalyse im gerichtlichen Verfahren muss auf die reine Identitätsfeststellung beschränkt werden; es dürfen keine genomanalytischen Methoden angewandt werden, die Überschussinformationen zur Person liefern. Die Nutzung der Genomanalyse im Strafverfahren setzt eine normenklare gesetzliche Ermächtigung voraus. Präzise Regelungen müssen u. a. sicherstellen, dass genomanalytische Befunde einer strengen Zweckbindung unterworfen werden.
6. Im Arbeitsverhältnis sind die Anordnung von Genomanalysen oder die Verwendung ihrer Ergebnisse grundsätzlich zu verbieten. Ausnahmen bedürfen der gesetzlichen

Regelung. Eine bloße Einwilligung des Arbeitnehmers ist wegen der faktischen Zwangssituation, der er im Arbeitsleben häufig unterliegt, nicht ausreichend.

7. Genomanalysen im Versicherungswesen sind grundsätzlich nicht erforderlich und mit dem Prinzip der Versicherungen, Risiken abzudecken und nicht auszuschließen, unvereinbar. Dies sollte durch eine Klarstellung im Versicherungsvertragsgesetz deutlich gemacht werden.
8. Im Rahmen der pränatalen Diagnostik dürfen nur Informationen über das Vorhandensein oder Fehlen von Erbanlagen erhoben werden, bei denen eine Schädigung heilbar ist oder die zu einer so schwerwiegenden Gesundheitsschädigung des Kindes führen würden, dass ein Schwangerschaftsabbruch straffrei bliebe.

   Reihenuntersuchungen an Neugeborenen dürfen sich nur auf solche Erbkrankheiten erstrecken, die bei frühzeitiger Erkennung eines genetischen Defekts geheilt oder zumindest spürbar therapeutisch begleitet werden können.

   Die Eltern müssen nach umfassender fachkundiger Beratung in voller Freiheit über die Anwendung genomanalytischer Methoden entscheiden können. Jegliche Beeinflussung, insbesondere jeder individuelle und gesellschaftliche Druck, muss vermieden werden.

Die informationelle Selbstbestimmung Dritter, zu der auch das Recht auf Nichtwissen gehört, muss berücksichtigt werden. Demnächst werden nicht nur - wie bisher - Gensequenzen aufgedeckt und verglichen, sondern auch die mit dem Genom verbundenen Wirkungszusammenhänge für die menschliche Gesundheit und für die Persönlichkeitsstruktur entschlüsselt werden können.

17.10. Vom Bürgerbüro zum Internet
Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung

(Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000)

Bei der Modernisierung der öffentlichen Verwaltung soll insbesondere die Dienstleistungs- und Serviceorientierung verbessert werden. Dazu sollen unter anderem Dienstleistungen in multifunktionalen Servicecentern (Bürgeramt, Bürgerbüro, Bürgerladen, Kundencenter) gebündelt und die Möglichkeiten der modernen Informations- und Kommunikations-Technik intensiver genutzt werden (Information, Kommunikation und Transaktion über das Internet, Einrichtung von Call-Centern).

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder unterstützt alle Bemühungen, den Kontakt von Bürgerinnen und Bürgern mit den Verwaltungen schneller, einfacher, effektiver und insbesondere transparenter zu machen. Die Datenschutzbeauftragten erklären daher ihre ausdrückliche Bereitschaft, solche Entwicklungsprozesse konstruktiv zu begleiten.

Es ist aber unerlässlich, dass bei allen Lösungen eine sichere und vertrauliche Kommunikation zwischen Verwaltung und Bürgern sowie ein angemessener Schutz personen-

bezogener Daten gewährleistet wird. Nur Serviceangebote, die dem Recht auf informationelle Selbstbestimmung gerecht werden, nützen letztlich sowohl Bürgerinnen und Bürgern als auch der Verwaltung selbst.

Eine Arbeitsgruppe der Konferenz der Datenschutzbeauftragten des Bundes und der Länder erarbeitet deshalb Empfehlungen zum Datenschutz für eine serviceorientierte Verwaltung. Diese Empfehlungen sollen den Verwaltungen helfen, bei der Verbesserung ihrer Dienstleistungs- und Serviceorientierung den Forderungen nach Datenschutz und Datensicherheit gerecht zu werden. Diese Empfehlungen werden demnächst veröffentlicht und entsprechend der rechtlichen und technischen Entwicklung fortgeschrieben.

17.11. Datensparsamkeit bei der Rundfunkfinanzierung

(Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000)

Die Finanzierung des öffentlich-rechtlichen Rundfunks ist derzeit Gegenstand öffentlicher Diskussion in der Politik und unter den Rundfunkanstalten selbst. Erörtert wird hierbei auch, ob die Erhebung von Rundfunkgebühren, die an das "Bereithalten eines Rundfunkempfangsgerätes" anknüpfen, im Hinblick auf veränderte Gerätetechniken und bestehende Mängel im Verfahren modifiziert oder durch andere Finanzierungsformen ersetzt bzw. ergänzt werden sollte.

Künftig wird kaum noch überschaubar sein, welche Geräte zum Rundfunkempfang geeignet sind. Über die eigentlichen Fernseh- und Rundfunkgeräte hinaus ist dies bereits heute beispielsweise mit Personalcomputern, die über einen Internetzugang verfügen, oder mit bestimmten Mobiltelefonen möglich. In naher Zukunft werden neue Technologien wie UMTS weitere Empfangsmöglichkeiten eröffnen. Sofern der Besitz derartiger multifunktionaler Geräte zum Kriterium für die Rundfunkgebührenpflicht gemacht wird, würde das zu einer erheblichen Ausweitung von Datenabgleichen führen. Schon das gegenwärtig praktizierte Gebühreneinzugsverfahren erfordert in großem Umfang die Verarbeitung personenbezogener Daten. Nach den Angaben der Rundfunkanstalten meldet ein signifikanter Teil der Rundfunkteilnehmerinnen und -teilnehmer trotz der Verpflichtung hierzu seine Geräte nicht an. Um möglichst alle Gebührenpflichtigen zu erfassen, nutzen die Rundfunkanstalten Daten aus dem Melderegister, vom privaten Adresshandel und setzen vor Ort Rundfunkgebührenbeauftragte ein, die einzelne Haushalte aufsuchen. Damit wird in unverhältnismäßiger Weise in das Recht auf informationelle Selbstbestimmung vieler gesetzestreuer Bürgerinnen und Bürger eingegriffen.

Die Datenschutzbeauftragten des Bundes und der Länder fordern die Bundesländer auf, einer Neuordnung ein Modell zu Grunde zu legen, das sich stärker als das bestehende System der Rundfunkfinanzierung an den Prinzipien der Datenvermeidung, Datensparsamkeit und Dezentralisierung orientiert. Nach ihrer Überzeugung lässt sich die verfassungsrechtlich gebotene Staatsferne und Funktionsfähigkeit des öffentlich-rechtlichen Rundfunks auch mit anderen, das Recht auf informationelle Selbstbestimmung weniger

stark einschränkenden Finanzierungsmodellen als dem derzeit praktizierten gewährleisten.

17.12. Entschließung zur Novellierung des BDSG

(Entschließung der 60. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 12./13. Oktober 2000)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder appelliert an Bundestag und Bundesrat, das Gesetzgebungsverfahren eines novellierten Bundesdatenschutzgesetzes zügig und ohne Abstriche zum Abschluss zu bringen. Damit wird die längst überfällige Anpassung des deutschen Datenschutzrechts an die Vorgaben der EG-Richtlinie vorgenommen. Die Novelle enthält verschiedene innovative Ansätze, insbesondere das Gebot zur Datenvermeidung und Datensparsamkeit bei der Systemgestaltung (Systemdatenschutz - § 3a E-BDSG) und die Einführung des Datenschutzaudit (§ 9a), die von den Datenschutzbeauftragten schon seit langem befürwortet werden.

Sowohl der Systemdatenschutz als auch das Datenschutzaudit werden die Durchsetzung datenschutzfreundlicher Lösungen im Wettbewerb erleichtern und tragen auf diese Weise zur Selbstregulierung des Marktes bei. Das Datenschutzaudit fügt sich in de bewährten Strukturen des betrieblichen Datenschutzes ein und ermöglicht es den Unternehmen, datenschutzkonforme Angebote und Verhaltensweisen nachprüfbar zu dokumentieren und damit einen Wettbewerbsvorsprung zu gewinnen.

Die Konferenz fordert den Bundesrat auf, die Aufnahme des Datenschutzaudit in das BDSG nicht zu blockieren. Sie geht weiter davon aus, dass die angekündigte zweite Stufe der Novellierung des BDSG noch in dieser Legislaturperiode realisiert wird, und erklärt ihre Bereitschaft, hieran konstruktiv mitzuwirken.

18. 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: 0471/9 24 61-0
Telefax: 0471/9 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	(vergriffen)
21. Jahresbericht 1998, Bürgerschafts-Drs. 14/1399	(vergriffen)
22. Jahresbericht 1999, Bürgerschafts-Drs. 15/266	(Restexemplare)

Broschüre "Mobilfunk und Datenschutz"
Broschüre "Orientierungshilfe zu Datenschutzfragen des Anschlusses von Netzen der öffentlichen Verwaltung an das Internet"
Faltblatt "Der betriebliche Datenschutzbeauftragte"
Faltblatt "Handels- und Wirtschaftsauskunfteien"
Faltblatt "Was Sie über die Schufa wissen sollten"
Broschüre "Datenschutz in der Freien Hansestadt Bremen" (Gesetzessammlung)
Broschüre "Datenschutz bei Windows NT"
Broschüre "Datenschutzfreundliche Technologien"
Broschüre "Datenschutz bei der Nutzung von Internet und Intranet"
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

19. Index