

1. Vorwort

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

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

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

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

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

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

1.1 Novellierung BremDSG abgeschlossen

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

1.2 Selbstverteidigung im Internet

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

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

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

1.3 Indiskretionen bei Themen in den Untersuchungsausschüssen

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

1.4 Verfaxtes Fax

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

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

1.5 Miles and More

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

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

1.6 Zur Europäischen Dimension des Datenschutzes

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

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

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

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

1.7 Zur Situation der Dienststelle

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

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

1.8 Öffentlichkeitsarbeit und Presseresonanz

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

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

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

1.9 Von meiner Dienststelle durchgeführte Fortbildungsmaßnahmen

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

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

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

1.10 Eingabenschwerpunkte

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

1.11 Kooperationen

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

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

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

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

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

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

1.12 Technik-Splitter

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

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

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

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

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

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

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

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

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



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

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

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

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

1.14 Informationsfreiheitsgesetz

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

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

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

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

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

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

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

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

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

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

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

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

1.15 Mit den Änderungen im Bremischen Datenschutzgesetz Erreichtes

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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