

## **1. Vorwort**

Das Berichtsjahr 2006 ist geprägt von zwei Besonderheiten, die über die allgemeinen Aufgaben des Landesbeauftragten hinausgehen: Mir fiel der Vorsitz bei den obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich zu (vgl. Ziff. 18.1 dieses Berichts) und mir wurden die Beratungs- und Kontrollaufgaben nach dem Bremer Informationsfreiheitsgesetz (BremIFG) übertragen, die ebenfalls mit einer Berichtspflicht verbunden sind. Die parlamentarischen Beratungen zum BremIFG und die ersten Schritte zur Umsetzung hatten Vorrang für mich, denn Fehlentwicklungen am Anfang muss man meistens teuer bezahlen. Es lag mir also daran, mehr als das Notwendige zu tun, um das Informationsfreiheitsgesetz in gutes Fahrwasser zu bringen. Da mir hierfür in 2006 kein zusätzliches Budget zur Verfügung gestellt wurde, gingen die Aktivitäten für die Informationsfreiheit zu Lasten des Datenschutzes. Auch der Konferenzvorsitz bei den Datenschutzaufsichtsbehörden verpflichtete mich, neben organisatorischen Aufgaben mehr als sonst alle Datenschutzangelegenheiten im privaten Sektor intensiv zu begleiten, um einen reibungslosen und effektiven Ablauf der beiden Sitzungen in Bremerhaven und Bremen sicherzustellen. Die Ergebnisse und das Feedback der Teilnehmer von Bund und Ländern zeigen, dass sich diese Investition gelohnt hat. Neben den Aufgaben nach dem Informationsfreiheitsgesetz stehen meiner Dienststelle seit Mitte des Jahres weitere neue Belastungen ins Haus: Leider hat sich der Bundesgesetzgeber in 2006 dazu entschieden, mit dem Gesetz zum Abbau bürokratischer Hemmnisse (vgl. Ziff. 18.7 dieses Berichts), auch Mittelstandsentlastungsgesetz genannt, die Regelungen über die Bestellung betrieblicher Datenschutzbeauftragter so zu verändern, dass ich den kleineren und mittleren Unternehmen vermehrt in Datenschutzfragen Hilfestellung leisten muss. Es hat also eine Verlagerung von Aufgaben auf die Datenschutzaufsichtsbehörden der Länder gegeben, die Entlastung der Wirtschaft ist in Teilen durch Belastung des Staates erkauft worden.

Wegen des über die Jahre ständig zunehmenden Einsatzes von elektronischer Kommunikation und Datenverarbeitung und der Erweiterung der Aufgaben meiner Dienststelle bei gleichzeitigem Abbau von Personal bin ich längst schon nicht mehr in der Lage, allen an mich herangetragenen Anforderungen Rechnung zu tragen. Deshalb ist es notwendig, Schwerpunkte zu setzen. Ein Schwerpunkt wird in 2007 die Verlagerung weiterer Teile der elektronischen Datenverarbeitung des Landes Bremen zu Dataport sein (vgl. Ziff. 15.1 dieses Berichts). Dataport ist eine gemeinsame Anstalt öffentlichen Rechts der Länder Bremen, Hamburg, Mecklenburg-Vorpommern und Schleswig-Holstein und wird für diese Länder in unterschiedlichem Umfang als IT-Dienstleister tätig. Mit Gesetz vom 20. Dezember 2005 ist das Land Bremen dem Länderstaatsvertrag zur Errichtung von Dataport beigetreten (Brem.GBl. 2005, S. 615, vgl. 28. JB, Ziff. 15.2). Mit Gesetz vom 19. Dezember 2006 wurde zum 1. Januar 2007 die bremische Niederlassung von Dataport durch Überleitung des Eigenbetriebs Fidatas Bremen gegründet (Brem.GBl. 2006, S. 544). Mitte 2006 begannen die intensiven Beratungen hierzu, die damit einhergehenden datenschutzrechtlichen Fragen wurden von mir begleitet. In 2007 nun steht u. a. die Portierung sämtlicher DV-Verfahren des Bremer Rechenzentrums ID Bremen an. Dieser Prozess bedeutet natürlich auch eine neue Herausforderung für das Technikteam in meinem Hause. Da es sich bei Dataport um ein gemeinsames Rechenzentrum

der genannten vier Länder handelt, kommt neben der räumlichen Entfernung für Prüfungen im Rechenzentrum in Schleswig-Holstein auch noch ein weiterer Abstimmungsbedarf mit den Datenschutzbeauftragten der anderen Länder hinzu. In jedem Fall bedarf der Start intensiver Zusammenarbeit, die ohne den Wechsel nicht entstanden wäre. Andererseits erwarte ich durch die Zusammenarbeit auch Effektivitätssteigerungen. Es bleibt also abzuwarten, zu welcher Seite sich die Waage langfristig neigen wird.

Erstmalig in diesem Jahr wurde die Auditierung eines Verfahrens nach § 7 b des Bremischen Datenschutzgesetzes eingeleitet (vgl. Ziff. 3.1 dieses Berichts). Öffentliche Stellen können nach dieser Vorschrift zur Verbesserung des Datenschutzes und der Datensicherheit ihre Verfahren sowie ihre technischen Einrichtungen durch einen unabhängigen Gutachter prüfen und bewerten lassen (Auditierung). Ziel des Datenschutzaudits ist die Verbesserung des Datenschutzes und der Datensicherheit. Nach erfolgreichem Abschluss sind die Stellen berechtigt, ein Datenschutzgütesiegel zu führen. Wer sich in der Weise um einen hohen Datenschutzstandard im eigenen Hause bemüht, hat dann verdient, dass er dieses Engagement mit einem Gütesiegel seinen Kunden gegenüber zum Ausdruck bringen kann. Ich kann nur dazu auffordern, mehr von dieser Möglichkeit Gebrauch zu machen.

Ausführliche datenschutzrechtliche Stellungnahmen im Rahmen der Gesetzgebungsberatung habe ich insbesondere zu folgenden Gesetzentwürfen des Landes abgegeben: Bremisches Meldegesetz, Bremisches Hochschulreformgesetz, Bremisches Schuldatenschutzgesetz und Bremisches Verfassungsschutzgesetz.

## **1.1 Die obersten Datenschutzaufsichtsbehörden kommen in Bremen zusammen**

Die Vertreter der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich (der so genannte Düsseldorfer Kreis) tagten im Berichtsjahr im Land Bremen, die Frühjahrssitzung fand in Bremerhaven, die Herbstsitzung in Bremen statt. Ich durfte den Vorsitz in dem Gremium führen, was natürlich neben einer intensiven Vorbereitung der Themen mit der Protokollführung, der Pressearbeit und der Vermittlung der Ergebnisse gegenüber der Wirtschaft und ihren Verbänden verbunden ist. Bei der Ausgestaltung des Rahmens haben mich in Bremen der Präsident der Bürgerschaft und in Bremerhaven der Oberbürgermeister tatkräftig unterstützt und so zu einem guten Gelingen der Sitzungstage beigetragen. Neben der Behandlung vieler Einzelfragen (vgl. Ziff. 18.1 dieses Berichts) möchte ich zwei auf der Herbstsitzung in Bremen verabschiedete Beschlüsse hervorheben. Der eine formuliert Voraussetzungen für den datenschutzgerechten Einsatz der Mikrochip-Technologie RFID (vgl. Ziff. 18.2 dieses Berichts), der andere betrifft die Behandlung von Bankdaten im internationalen Zahlungsverkehr durch SWIFT (Society for Worldwide Interbank Financial Telecommunication); eine genauere Darstellung findet sich unter Ziffer 18.3 dieses Berichts. Nicht unerwähnt lassen möchte ich, dass es in der Frühjahrssitzung in Bremerhaven gelungen ist, verbindliche Regelungen aufzustellen, die eine Veröffentlichung der Beschlüsse des Düsseldorfer Kreises erlauben. Dieser Schritt war aus meiner Sicht längst überfällig, auch wenn es wieder ein Stück mehr Arbeit bedeutet. Die Zusammenkunft der Vertreter der obersten Aufsichtsbehörden wurde auch genutzt, um sich aus erster Hand von kompetenten Informatikern und Juristen über neueste Entwicklungen informieren zu lassen. In Bremerhaven nutzte die datenschutz nord GmbH die Gelegenheit, ihre speziellen für den Datenschutz im Internet entwickelten Software-Prüftools vorzustellen. In Bremen stellten Vertreter des Chip-Herstellers Intel ihre Überlegungen bei der Weiterentwicklung von Prozessoren vor und berichteten dann über ihre TET („Trusted Execution Technology“), eine Technologie, um hardwareunterstützt Schutzstandards im Bereich der Identifikation und der Datensicherheit umzusetzen. Technologische Basis hierfür ist ein „Trusted Platform Module“ (TPM), dass in die Chipsätze auf Motherboards integriert werden soll. Unabhängig von damit verbundenen Datenschutzfragen ist feststellbar, dass, ebenso wie zum Beispiel bei der Firma Microsoft, die in der Vergangenheit liegenden öffentlichen Reaktionen auf datenschutzunfreundliche technische Ausgestaltung (vgl. 25. JB, Ziff. 2.5 und 22. JB, Ziff. 18.4) ihre Wirkung gezeigt und zu einem Umdenken in diesen Unternehmen geführt haben.

## **1.2 Vertragsverletzungsverfahren vor dem EuGH**

Im 28. Jahresbericht (vgl. Ziff. 3.1) hatte ich über das von der Europäischen Kommission am 5. Juli 2005 eingeleitete Vertragsverletzungsverfahren gegen die Bundesrepublik Deutschland wegen Verstoßes gegen Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG (EG-Datenschutzrichtlinie) berichtet. Die Europäische Kommission vertritt die Auffassung, die derzeitigen Organisations- und Aufsichtsstrukturen der für die Überwachung der Datenverarbeitung im nicht öffentlichen Bereich zuständigen Kontrollstellen in den Ländern seien nicht mit Gemeinschaftsrecht vereinbar, da die verschiedenen Formen von Fach-, Rechts- und Dienstaufsicht nicht den Anforderungen der verlangten „völligen Unabhängigkeit“ im Sinne des Artikel 28 Abs. 1 Satz 2 der Richtlinie 95/46/EG entsprechen.

Im Laufe dieses Jahres gab es Gespräche zwischen der Europäischen Kommission und der Bundesregierung mit dem Ziel, eine außergerichtliche Lösung herbeizuführen. Diese steht weiter aus. Die EU-Kommission hat daher mit Schreiben vom 15. Dezember 2006 (SG[2006]D/207794) eine mit Gründen versehene Stellungnahme (Nr. 2003/4820) gemäß Artikel 226 des Vertrags zur Gründung der Europäischen Gemeinschaft an die Bundesrepublik Deutschland übermittelt. Darin wird die Bundesrepublik Deutschland aufgefordert, binnen zwei Monaten der Stellungnahme nachzukommen und die völlige Unabhängigkeit der für die Datenverarbeitung nicht öffentlicher Stellen zuständigen Aufsichtsbehörden sicherzustellen. Parallel zu dem Fortgang des Vertragsverletzungsverfahrens dauern die Gespräche an. Im Zusammenhang dieser Gespräche hielt es das Bundesministerium des Innern in seiner Stellungnahme für unabdingbar, die Datenschutzaufsichtsbehörden für den nicht öffentlichen Bereich einer Rechtsaufsicht durch die Landesregierung oder durch eine oberste Landesbehörde zu unterwerfen. Meine Rechtsauffassung zur Situation in Bremen habe ich im 28. Jahresbericht (vgl. Ziff. 3.1) dargelegt, der Rechtsausschuss der Bürgerschaft ist unterrichtet, Aufsichtsmaßnahmen gegenüber der Datenschutzaufsichtsbehörde des Landes hat es in Bremen nicht gegeben.

## **1.3 Zur Entwicklung des Datenschutzes auf internationaler und auf**

### **Bundesebene**

Auf eine Darstellung der Entwicklung des Datenschutzes auf internationaler und auf Bundesebene habe ich im Hauptteil des Berichts weitgehend verzichtet. An dieser Stelle jedoch möchte ich kurz darauf eingehen. Ein zentrales Thema der Sicherheitspolitik war die Terrorismusgefahr. Auf internationaler Ebene stand nach der Entscheidung des Europäischen Gerichtshofes (EuGH) vom 30. Mai 2006 die Überarbeitung des Abkommens zum Abruf der Fluggastdaten von den USA (Ministerium für Heimatschutz) an. Leider hat auch das zweite Abkommen vom Oktober 2006 für den Schutz der Fluggastdaten nur wenig gebracht. Das Pull-Verfahren bleibt zunächst bestehen (vgl. hierzu auch den 27. JB, Ziff. 15.2), auch die weitere Verwendung und die Speicherdauer der Daten bleiben ungewiss. Die Presse berichtete erst jüngst im November, die USA wollten Passagierdaten von Einreisenden 50 Jahre lang speichern. Auch der zur Verfügung gestellte Datensatz mit Daten z. B. über Sitzplatznummer, Zahlungsart, Reisebüro oder Essgewohnheiten ist weiterhin viel zu umfangreich.

Im Spätsommer berichteten seriöse Zeitungen, nachdem Innenminister Schäuble in einer Pressekonferenz ein positives Resümee über den Verlauf der Fußball-WM gezogen habe, dass der Minister mit der Begründung: „Jetzt dürfe man nicht die Hände in den Schoß legen, denn die Terrorgefahr sei während der WM weiter gewachsen“, das Antiterrordateigesetz präsentiert habe. So kam es denn auch. Auf Bundesebene standen die Beratung und Verabschiedung über das Terrorismusbekämpfungsergänzungsgesetz und das Gesetz zum Aufbau einer gemeinsamen Datei von Polizei und Nachrichtendiensten (vgl. Ziff. 9.4 dieses Berichts) an, die beide die Aufgaben und Befugnisse von Polizei und Nachrichtendiensten erweitern. Dabei wurden auch die durch das Terrorismusbekämpfungsgesetz im Jahre 2002 eingeführten Kompetenzen der Nachrichtendienste ohne Änderungen neu aufgelegt. Dabei war in das Gesetz eine Befristung aufgenommen worden, um vor einer Verlängerung die Regelungen einer gründlichen Überprüfung zu unterziehen und ungenutzte Instrumente des Rechtsstaats wieder abzuschaffen (vgl. Ziff. 9.3 und auch 9.16 dieses Berichts). Auch die ständig stark ansteigende Zahl an Telefonüberwachungsmaßnahmen spricht Bände (vgl. Grafik unter Ziff. 22.3 dieses Berichts). Seit dem 11. September 2001 hat es eine Verschärfung der Sicherheitsgesetze gegeben, die in der Geschichte der Bundesrepublik ihresgleichen sucht. Dabei ist es häufig nicht die Praxis, die nach immer neuen Eingriffsgrundlagen sucht, sondern es sind die Innenpolitiker, die bei jedem Vorfall Handlungsfähigkeit beweisen wollen. Ein Kritiker nannte dieses Phänomen jüngst ein dringendes Adoptionsbedürfnis deutscher Politiker für britische Terrorängste. In der Demokratie gibt es ein natürliches Spannungsfeld zwischen Sicherheitsbedürfnis und Freiheitsrechten. Die eine Frage ist, ob die Balance gehalten wird oder ob wir uns rapide in Richtung Überwachungsstaat bewegen. Die andere Frage ist, ob nicht durch unangemessene Maßnahmen der Kampf gegen den Terrorismus erschwert wird. Die vom Bundesverfassungsgericht für verfassungswidrig erklärte Durchführung einer Rasterfahndung ohne konkrete Gefahr (vgl. Ziff. 9.2 dieses Berichts) war solch eine Maßnahme. Sie hat in der Sache faktisch nichts erbracht, wurde aber insbesondere von Betroffenen moslemischen Glaubens als unberechtigtes Misstrauen empfunden

und hat sie gegen den Staat aufgebracht. Auch die Konferenz der Datenschutzbeauftragten des Bundes und der Länder ist in einer EntschlieÙung kritisch auf die Durchführung der Rasterfahndung eingegangen (vgl. Ziff. 19.8 dieses Berichts)

#### **1.4           Schwerpunkte der Begleitung technischer Entwicklungen**

Im privaten Bereich verfolge ich schwerpunktmäßig die Entwicklung bei der Internet-Telefonie, der RFID-Technik (vgl. Ziff. 18.2 dieses Berichts) und die Entwicklung verschiedener DV-Techniken, die in Kraftfahrzeugen zum Einsatz kommen sollen. Beispielhaft sei der in Krankenwagen bei der Feuerwehr Bremen eingesetzte UDS-Speicher erwähnt, dessen Einsatz und Funktionsweise ich bereits im letzten Jahresbericht (vgl. 28. JB, Ziff. 6.3) dargestellt habe. Die Technik arbeitet in der Regel mit GPS und teils auch biometrischen, in jedem Falle mit fahrer- oder eignerbezogenen Daten. Die Daten sollen je nach Anwendung mit einer Dockingstation auslesbar im Fahrzeug selbst gespeichert oder an dritte Stellen via Satellit oder über Handyfrequenzen laufend oder ereignisbezogen übertragen werden. Es ist dabei nicht Aufgabe des Datenschutzes zu überprüfen, wie sinnvoll solche technischen Entwicklungen sind, sondern es ist nur darauf zu achten, wie das informationelle Selbstbestimmungsrecht gewahrt werden kann. Und Wege hierfür konnten bisher immer aufgezeigt werden. Die Datenschutzbeauftragten und die Datenschutzaufsichtsbehörden des Bundes und der Länder haben zur Begleitung dieser Entwicklung eine gemeinsame Arbeitsgruppe eingesetzt, der ich angehöre. Erste Kontakte mit der Autoindustrie und den Zulieferbetrieben hat es im Berichtsjahr gegeben.

## **1.5 Schriftliche Eingaben und telefonische Anfragen von Bürgerinnen und Bürgern**

Im Jahre 2006 erhielt ich erneut eine hohe Zahl von schriftlichen Eingaben von Bürgern, die sich an mich wegen der Verarbeitung ihrer personenbezogenen Daten durch Behörden, Unternehmen oder andere datenverarbeitende Stellen wandten. Im öffentlichen Bereich ging es bei den Eingaben am häufigsten um Fragen aus dem Bereich der inneren Sicherheit, speziell der Polizei. Fast ebenso starken Anteil hatte der Bereich Jugend, Familie und Soziales; wie bereits im Jahr zuvor bezogen sich dabei viele Fragen auf die Datenverarbeitung der BAfG. Eine erhebliche Anzahl Eingaben betrafen auch die Datenverarbeitung im Gesundheitsbereich, hier insbesondere zur Kranken- und Pflegeversicherung.

Im nicht öffentlichen Bereich hatten Eingaben, die den Bereich Internet/Telekommunikation betrafen, den höchsten Anteil. Sehr häufig erhielt ich auch Eingaben zur Videoüberwachung durch Unternehmen und Wohnungseigentümer, zum Arbeitnehmerdatenschutz in den Betrieben und zur Datenverarbeitung der Auskunfteien.

Darüber hinaus bekam ich eine Vielzahl telefonischer Anfragen zu den verschiedenen Bereichen der Datenverarbeitung. Um die Vielfalt dieser Anfragen darzustellen, habe ich einige der Themen aus dem Berichtsjahr in einer Tabelle erfasst (vgl. Ziff. 22.2 dieses Berichts). Die dort aufgeführten Fragen wurden alle telefonisch beantwortet. Insgesamt gesehen stieg die Zahl der Eingaben und Anfragen im Berichtsjahr im Vergleich zum Vorjahr weiter an.

## **1.6 Zur Situation der Dienststelle**

Das Berichtsjahr 2006 war für die Dienststelle mit einigen zum Teil unvorhersehbaren Turbulenzen verbunden, verursacht durch die personelle Situation. Davon war einiges vorhersehbar, anderes kam unerwartet. Vorhersehbar waren die durch Altersteilzeit bedingten Ausfälle, die u. a. zwei von sechs Referaten betreffen. Hinzu kamen weitere nicht planbare Abgänge durch Beurlaubung, Beendigung des Dienstverhältnisses und Abberufung zu einer anderen senatorischen Dienststelle. Ich hatte zwar in den Haushaltsberatungen um einen Ausgleich für die durch die Freistellung für Altersteilzeit bedingten Ausfälle gebeten, der mir aber nicht gewährt wurde. Zu diesem Zeitpunkt war aber die weitere dramatische Entwicklung noch nicht absehbar. Im Laufe des Jahres verschlechterten sich die personellen Ressourcen kontinuierlich. Seit Ende 2006 müssen zwei Referenten die anderen vier Referate mit vertreten. Ein geordnetes Arbeiten ist da natürlich nicht mehr möglich. Wenn ich nicht gleich den Notstand ausgerufen habe, dann nur deshalb, weil auch die Stürme mit orkanartigen Böen immer erst Bremerhaven heimsuchen, bevor sie abgeschwächt in Bremen einfallen. Enttäuschung über mangelnde Unterstützung zur Überbrückung des personellen Engpasses ist schon in der Dienststelle zu verspüren, aber für 2007 gibt es Anzeichen, dass die personelle Situation sich entscheidend verbessern wird. Wichtig ist, mit eingearbeitetem Personal wieder Kontinuität und Effektivität zu erreichen.

## **1.7 Vorträge, Fortbildungsangebot und Kooperationen**

In 2006 führten die Mitarbeiterinnen und Mitarbeiter der Dienststelle wieder mehrere Fortbildungsmaßnahmen durch. Den beim Magistrat der Stadt Bremerhaven Ende 2005 neu bestellten behördlichen Datenschutzbeauftragten bot ich gleich zu Beginn des Berichtsjahres ein Fortbildungsseminar an, das ihrer Einführung in die neue Tätigkeit diene. Außerdem wurde im Aus- und Fortbildungszentrum der bremischen Verwaltung ein Fortbildungsseminar zur „Einführung in das Datenschutzrecht“ gehalten, an dem interessierte Teilnehmer aus allen Bereichen der Verwaltung teilnahmen. Mehrere Vorträge zum Thema „Datenschutzaspekte beim Bürokommunikations- und Archivierungssystem VISkompakt“ und zu der von mir erarbeiteten „Orientierungshilfe zur Erstellung eines Datenschutzkonzeptes“ wurden von den Mitarbeiterinnen und Mitarbeitern der Dienststelle in Workshops für die behördlichen Datenschutzbeauftragten behandelt (vgl. Ziff. 2.1 dieses Berichts).

Vorträge zu den Themen „Konsequenzen aus dem Mittelstandsentlastungsgesetz für den betrieblichen Datenschutz“ und „Informationsfreiheitsgesetz“ hielt ich vor betrieblichen Datenschutzbeauftragten im Erfa-Kreis Bremen/Weser-Ems. Weiterhin kooperierte ich im Berichtsjahr mit dem Virtuellen Datenschutzbüro, dessen Federführung beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein liegt, und der datenschutz nord GmbH. Die Zusammenarbeit mit den Datenschutzbeauftragten des Bundes und der Länder sowie mit den Datenschutzaufsichtsbehörden versteht sich von selbst.