BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG
18. Wahlperiode

Drucksache 18/606
11.04.08

Der Hamburgische Datenschutzbeauftragte

An den
Präsidenten der Hamburgischen Bürgerschaft

Betr.: Tätigkeitsbericht des Hamburgischen Datenschutzbeauftragten über die Berichtsperiode 2006/2007

Gemäß § 23 Absatz 3 Satz 2 des Hamburgischen Datenschutzgesetzes übersende ich der Bürgerschaft meinen Tätigkeitsbericht über die Berichtsperiode 2006/2007.*****

Dem Senat leite ich meinen Tätigkeitsbericht gleichzeitig zu.

Lubomierski

* Verteilt nur an die Abgeordneten der Bürgerschaft.

Das Bundesverfassungsgericht
hat am 27. Februar 2008,
25 Jahre nach seinem Volkszählungsurteil,
entschieden:

Das Grundrecht auf Gewährleistung der Integrität und Vertraulichkeit informationstechnischer Systeme ist anzuwenden, wenn die Eingriffsermächtigung Systeme erfasst, die personenbezogene Daten des Betroffenen in einem Umfang und in einer Vielfalt enthalten können, dass ein Zugriff auf das System es ermöglicht, einen Einblick in wesentliche Teile der Lebensgestaltung einer Person zu gewinnen oder gar ein aussagekräftiges Bild der Persönlichkeit zu erhalten. **Eine solche Möglichkeit besteht beim Zugriff auf Personalcomputer.** Nicht nur bei einer Nutzung für private Zwecke, sondern auch bei einer geschäftlichen Nutzung lässt sich aus dem Nutzungsverhalten regelmäßig auf persönliche Eigenschaften oder Vorlieben schließen.

Der Gesetzgeber hat dieses Grundrecht zu achten und von derartigen Zugriffen abzusehen.

21. Tätigkeitsbericht 2006/2007 HmbDSB

Der Hamburgische Datenschutzbeauftragte

Tätigkeitsbericht

2006/2007

21. Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten
zugleich
Tätigkeitsbericht der Aufsichtsbehörde
für den nicht-öffentlichen Bereich
2006 / 2007

vorgelegt im März 2008

Hartmut Lubomierski
(Redaktionsschluss: 31. Dezember 2007)

Diesen Tätigkeitsbericht können Sie abrufen unter
www.datenschutz.hamburg.de

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Klosterwall 6 (Block C) · 20095 Hamburg · Tel. 428 54 40 40 · Fax 428 54 40 00
mailbox@datenschutz.hamburg.de

Auflage: 1.500 Exemplare

Druck: Lütcke & Wulff, 20097 Hamburg

INHALTSVERZEICHNIS

Vorbemerkung

Das Persönlichkeitsrecht und die Privatsphäre der Bürgerinnen und Bürger waren in den beiden Berichtsjahren weiteren Gefährdungen und Angriffen sowohl von Seiten des Staates als auch von Seiten der Wirtschaft ausgesetzt.

Die berufliche aber auch private Nutzung von Computer, Internet und Handy ist Alltagswirklichkeit und hat für die Lebensführung vieler Bürger eine zentrale Bedeutung gewonnen. Die enorm gestiegene Verbreitung und Leistungsfähigkeit der Computer und der Telekommunikationsgeräte sowie ihre Vernetzung mit dem Internet eröffnen neue Möglichkeiten der Persönlichkeitsentfaltung, bewirken aber auch neue Persönlichkeitsgefährdungen.

Der Staat nutzt die heute nahezu unbegrenzten Datenspeicherungskapazitäten, um sich Ausforschungsmöglichkeiten über das Kommunikationsverhalten der Bürger zu erschließen, die noch vor wenigen Jahren undenkbar waren. Mittels der seit dem 1. Januar 2008 in Kraft getretenen verdachtsunabhängigen Vorratsdatenspeicherung können Ermittlungsbehörden künftig die Kommunikationsbeziehungen aller Bürger und ihre Internetnutzung für ein halbes Jahr zurückverfolgen.

Per heimlicher Online-Durchsuchung der Personalcomputer der Bürger wollen Polizei und Verfassungsschutz durch Manipulation und Infiltration dauerhaft unbemerkten Zugriff auf alle elektronisch gespeicherten Daten nehmen, um dadurch Einblick in wesentliche Teile der privaten Lebensgestaltung der Bürger zu gewinnen bis hin zu einer Bildung von Verhaltens- und Kommunikationsprofilen.

Die Wirtschaft versucht, durch Scoring-Verfahren die Kunden in ihrem Zahlungsverhalten, insbesondere in ihrer Kreditwürdigkeit, berechenbar zu machen, sie weigert sich aber, für die Kunden Transparenz zu solchen Bewertungsverfahren herzustellen. Über Kundenbindungssysteme sammeln die Unternehmen Verbraucherdaten, um Kundenprofile erstellen und den Kunden ganz individuell mit Werbung überziehen zu können. Die Erweiterung der zentralen Datenbestände bei Auskunfteien und die branchenübergreifende Bereitstellung dieser Informationen für eine Vielzahl von Unternehmen gefährden nachhaltig das Recht auf informationelle Selbstbestimmung der Verbraucher.

Internet-Suchmaschinen spielen für die Informationsbeschaffung in fast allen Bereichen der Wirtschaft und der Verwaltung aber ebenso auch im privaten Bereich eine immer wichtigere Rolle. Dabei führt die Nutzung von Suchmaschinen zu hohen Risiken. Ein Internetsurfer, der intensiv auf die Nutzung von Suchmaschinendiensten setzt, hinterlässt permanent digitale Spuren, die nicht nur für die Werbewirtschaft sehr wertvoll sind. Die Suchabfragen sowie die Klicks auf Treffer und kontextbezogene Anzeigen offenbaren beispielsweise, für welche Produkte sich der Nutzer interessiert, welche Käufe in nächster Zeit anstehen, welche Vorlieben bestehen. Werden weitere Dienste wie

E-Mail, Bezahlfunktion, Toolbar (Werkzeugleiste für den Internetexplorer und Firefox), Newsreader, Blogs und Routenplaner in das Suchmaschinenangebot integriert und alle Nutzeraktivitäten protokolliert, verfügt der Suchmaschinenbetreiber über ein komplettes Persönlichkeitsprofil des Nutzers. Ein Großteil der Daten, die der Staat erst mittels Vorratsdatenspeicherung und Online-Durchsuchung des Computers zu erlangen sucht, sammelt sich auf diese Weise automatisch beim Suchmaschinenbetreiber an. Ob und wie diese Daten genutzt werden, entzieht sich jeder Kenntnis und Kontrolle der Betroffenen. Insbesondere, wenn der Suchmaschinenbetreiber seinen Sitz außerhalb der EU hat, ist auch eine Kontrolle der Datenverarbeitung durch die Datenschutzaufsichtsbehörde nicht möglich.

Sowohl staatliche Stellen als auch Wirtschaftsunternehmen versuchen, die jeweils für sie bestehenden datenschutzrechtlichen Begrenzungen zu überwinden, indem sie sich über das Instrument der Einwilligung, die sie dem Bürger, dem Kunden oder Vertragspartner abverlangen, Datenverarbeitungsmöglichkeiten erschließen, für die es keine gesetzlichen Grundlagen gibt. Auf die datenschutzrechtliche Problematik, mittels Einwilligung in Datenverarbeitungen die dafür bestehenden gesetzlichen Zulässigkeitsvoraussetzungen zu übersteigen, wird nachstehend (1.) vertieft eingegangen. Die datenschutzrechtliche Einwilligung muss als Instrument der freien Selbstbestimmung auf die Fälle begrenzt werden, in denen tatsächlich Entscheidungsfreiheit besteht.

„Wo aber Gefahr ist, wächst das Rettende auch." (Hölderlin)

Das Bundesverfassungsgericht hat 25 Jahre nach seinem legendären Volkszählungsurteil in seiner Entscheidung vom 27. Februar 2008 zum Verbot von Online-Durchsuchungen von Computern den Schutz des Persönlichkeitsrechts vor den neuen Gefährdungen im Computer- und Internet-Zeitalter gestärkt und festgestellt, dass das allgemeine Persönlichkeitsrecht auch die Vertraulichkeit und Integrität informationstechnischer Systeme gewährleistet. Dieses Grundrecht bewahrt den persönlichen und privaten Lebensbereich des Grundrechtsträgers vor staatlichem Zugriff im Bereich der Informationstechnik auch insoweit, als auf das informationstechnische System insgesamt zugegriffen wird und nicht nur auf einzelne Kommunikationsvorgänge oder gespeicherte Daten.

Mit seiner Entscheidung vom 11. März 2008 zum Verbot der automatisierten Kfz-Kennzeichenerfassung hat das Bundesverfassungsgericht einen Riegel vor eine Ausweitung von verdachtsunabhängigen Kontrollen und Überwachungsmaßnahmen und den Aufbau von Überwachungsstrukturen geschoben. Die Bürger haben grundsätzlich das Recht, sich im öffentlichen Raum frei und unbeobachtet und unerfasst zu bewegen. Sie müssen sich darauf verlassen können, dass gegen sie keine Überwachungsmaßnahmen ergriffen werden, wenn sie dafür keinen Anlass gegeben haben. Der Mensch darf nicht zum Objekt permanenter und verhaltenslenkender Überwachung werden. Po-

lizeiliche Überwachung des Bürgers darf nicht zu einer „Alltagserscheinung“ werden. Polizeiliche Eingriffe „ins Blaue hinein“ lässt die Verfassung nicht zu.

In seiner Entscheidung vom 23. Februar 2007 zur Videoüberwachung im öffentlichen Raum hat das Bundesverfassungsgericht festgestellt, dass der mit einer Videoüberwachung verbundene intensive Eingriff in das Persönlichkeitsrecht der Bürger nicht auf die allgemeinen Regelungen zur Datenerhebung im Datenschutzrecht gestützt werden kann. Diese Normen enthalten keine ausreichend bestimmten Vorgaben für die Videoüberwachung, um als Ermächtigungsgrundlage für den Grundrechtseingriff in Betracht zu kommen. Das Gebot der Erforderlichkeit kann allein die behördliche Praxis nicht hinreichend anleiten oder Kontrollmaßstäbe bereitstellen, weil die Ausrichtung auf ein näher beschriebenes Normziel fehlt. Anlass, Zweck und Grenzen der Videoüberwachung muss der Gesetzgeber selbst festlegen.

Leider bedurfte es erst dieser deutlichen Feststellungen des Bundesverfassungsgerichts, damit die Grundrechte und der Persönlichkeitsschutz in Deutschland wieder Geltung gewinnen. Die Regierungen und Parlamente haben in Deutschland in letzter Zeit häufig die notwendige Selbstdisziplin zur Achtung der Grundrechte der Bürger nicht aufgebracht. Es bleibt zu hoffen, dass künftig die Politiker und Parlamente zur Wahrung der Grundrechte zurückfinden, damit nicht immer erst das Verfassungsgericht die Notbremse ziehen muss.

Die Vorgaben des Bundesverfassungsgerichts müssen auch in Hamburg beachtet und umgesetzt werden. Ich habe mich deshalb im Hinblick auf die bevorstehende 19. Wahlperiode der Bürgerschaft mit den nachstehenden Empfehlungen zur Verbesserung des Datenschutzes in Hamburg an Bürgerschaft und Senat gewandt:

Empfehlungen an die Bürgerschaft als Gesetzgeber:

- Keine Änderung des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) dahingehend, dass eine über die Regelung des § 10 a Absatz 1 Satz 1 hinausgehende präventive Telekommunikationsüberwachung möglich ist.
- Keine Änderung des PolDVG und des Hamburgischen Verfassungsschutzgesetzes zur Ermöglichung von Online-Durchsuchungen durch das Landeskriminalamt und das Landesamt für Verfassungsschutz sowie keine Ausweitung sonstiger heimlicher und verdachtsunabhängiger Kontroll- und Überwachungsmaßnahmen.
- Änderung des PolDVG und des Hamburgischen Verfassungsschutzgesetzes dahingehend, dass bei allen heimlichen und verdeckten Überwachungs- und Ermittlungsmaßnahmen der unantastbare Kernbereich privater Lebensgestaltung gewahrt wird, d.h. schon die Erhebung/Er-

fassung von Daten muss unterbleiben, wenn der Kernbereich privater Lebensgestaltung berührt sein könnte.

- Änderung des PolDVG dahingehend, dass die Vorschrift über die automatisierte Kfz-Kennzeichenerfassung (§ 8 Absatz 6) gestrichen oder entsprechend den Vorgaben der Entscheidung des Bundesverfassungsgerichts vom 11. März 2008 eingeschränkt bestimmt und normenklar gefasst wird, d.h. Beschränkung auf die Abwehr schwerwiegender Rechtsgutverletzungen, kein anlassloser Einsatz, keine Verfolgung von Ordnungswidrigkeiten.
- Ergänzung des Hamburgischen Datenschutzgesetzes um eine normenklare, bestimmte aber restriktive Regelung für die Videoüberwachung von öffentlichen Dienstgebäuden einschließlich Schulen (entsprechend den Vorgaben des Bundesverfassungsgerichts vom 23. Februar 2007), jedoch keine Zulassung einer Videoüberwachung von sonstigem öffentlichen Raum außerhalb der polizeilichen Videoüberwachung gemäß § 8 Absatz 2 PolDVG. (Keine neue Einrichtung von Videoüberwachungsanlagen für öffentliche Gebäude vor Inkrafttreten der erforderlichen gesetzlichen Regelung.)
- Änderung des Hamburgischen Strafvollzugsgesetzes und des Hamburgischen Maßregelvollzugsgesetzes dahingehend, dass eine Videoüberwachung von Hafträumen ausgeschlossen ist.
- Änderung des Hamburgischen Datenschutzgesetzes (§ 10a) dahingehend, dass alle hamburgischen Behörden verpflichtet sind, einen behördlichen Datenschutzbeauftragten zu bestellen (Von der Kann-Vorschrift, von der nicht Gebrauch gemacht wird, zur Muss-Vorschrift).
- Keine Änderung des Hamburgischen Datenschutzgesetzes (§§ 11 und 11a) dahingehend, dass auf das Rechtsverordnungserfordernis für die Einrichtung automatisierter Abrufverfahren sowie gemeinsamer automatisierter Dateien verzichtet oder ein automatisiertes Abrufverfahren für Stellen außerhalb der Verwaltung zugelassen wird, wenn nicht durch gesetzliche Regelungen ein unvermindert hoher Datenschutz durch zusätzliche technische und organisatorische Maßnahmen gewährleistet und für Abrufe durch Stellen außerhalb der Verwaltung eine strikte Zweckbindung und die Kontrolle durch den Hamburgischen Datenschutzbeauftragten sichergestellt wird.

Empfehlungen an Senat und Behörden:

- Beschränkung der polizeilichen Videoüberwachung auf Reeperbahn und Hansaplatz (Ausweitung allenfalls nach vorheriger unabhängiger Evaluierung und vorheriger Erstellung einer Risikoanalyse).
- Erhöhung der Sicherheit der IT-Infrastruktur für die hamburgischen Behörden durch Ausrichtung auf den Standard des IT-Grundschutzes des

Bundesamtes für Sicherheit in der Informationstechnik (BSI) und Bereitstellung der dafür erforderlichen Haushaltsmittel.

- Keine Zuverlässigkeitsüberprüfungen durch Polizei und Verfassungsschutz von Teilnehmern an Großveranstaltungen ohne gesetzliche Grundlage allein auf Einwilligungsbasis. Ggf. Hinwirken auf eine bundeseinheitliche Rechtsgrundlage für Zuverlässigkeitsüberprüfungen.

Die aufsichtsbehördliche Tätigkeit der Dienststelle des Hamburgischen Datenschutzbeauftragten wurde 2007 dadurch besonders geprägt, dass der Hamburgische Datenschutzbeauftragte 2007 den Vorsitz im Düsseldorfer Kreis, dem Zusammenschluss der Obersten Aufsichtsbehörden zur Kontrolle des Datenschutzes in der Privatwirtschaft, ausübte. In den beiden in Hamburg stattfindenden Sitzungen des Düsseldorfer Kreises wurden wichtige Entscheidungen zu Gunsten des Datenschutzes in der Wirtschaft getroffen.

So wurde u.a. beschlossen,

- dass Auskunfteien sog. Positivdaten zu Privatpersonen – das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben – nur erheben dürfen, wenn der Betroffene ausdrücklich darin eingewilligt hat,
- dass Versandhandelsunternehmen personenbezogene Daten über das vertragsgemäße Zahlungs- und Geschäftsabwicklungsverhalten ihrer Kunden an Auskunfteien zur Nutzung für deren eigene Geschäftszwecke nur weitergeben dürfen, wenn ihre Kunden ausdrücklich darin eingewilligt haben,
- dass ein Unternehmen Umzugsadressen seiner Kunden an andere Unternehmen zur weiteren Übermittlung dieser Adressänderungen an angeschlossene Unternehmen zum Zwecke des Adressabgleichs nur übermitteln darf, wenn die Betroffenen ausdrücklich darin eingewilligt haben.

In diesen Fällen besteht für die Betroffenen eine tatsächliche Entscheidungsfreiheit, ob sie die jeweilige Einwilligung erteilen wollen, ohne dass die Nichterteilung der Einwilligung für sie sie negative Folgen hätte. (Siehe dazu die Ausführungen unter 1. Datenschutzrechtliche Einwilligungen)

Ferner wurde beschlossen:

- dass eine telefonische Mahnung durch Computeranruf unzulässig ist, weil eine hohe Gefahr besteht, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und damit personenbezogene Daten einem Dritten unbefugt offenbart werden,
- dass die Nutzung der Privatadresse des Arbeitnehmers zum Zwecke der Versendung einer Zeitschrift eines Arbeitgeberverbandes unzulässig ist.

Bei unseren anlassfreien Unternehmensprüfungen stellten wir teilweise gravierende Datenschutzmängel fest. Nach unseren Erfahrungen aus den vergangenen Jahren haben wir verstärkt den Schutz der personenbezogenen

Daten in den konkreten Datenverarbeitungsprozessen kontrolliert. Dabei legten wir großen Wert auf die Prüfung der Rechtmäßigkeit der Erhebung und Verarbeitung – insbesondere Übermittlung – personenbezogener Daten. Unser Ziel ist es, mehr Transparenz für die betroffenen Kunden, letztlich aber auch für die Unternehmensleitungen zu erzeugen. Obwohl das Datenschutzrecht in erster Linie eine Selbstkontrolle der Wirtschaft vorsieht, belegen die bei unseren Prüfungen festgestellten datenschutzrechtlichen Mängel, dass eine Kontrolle durch die Aufsichtsbehörde notwendig ist. Trotz knapper personeller Ressourcen werden wir daher weiterhin anlassfreie Unternehmensprüfungen durchführen.

Auch in den letzten zwei Jahren haben sich viele Bürgerinnen und Bürger schriftlich, per E-Mail, telefonisch und auch persönlich an uns gewandt, da sie der Ansicht waren, bei der Verarbeitung ihrer persönlichen Daten durch Behörden oder Unternehmen in ihren Rechten verletzt worden zu sein. Unsere Beratung und Einschaltung führte ganz überwiegend zu befriedigenden Ergebnissen.

Zahlreiche Beschwerden zeigen aber, dass eine Vielzahl von Unternehmen die Ausübung insbesondere von Auskunftsrechten und von Werbewidersprüchen der Bürger schlicht ignoriert und erst die Einschaltung der Aufsichtsbehörde bewirkt, dass die Ansprüche der Bürger erfüllt werden. Dieser mangelnde Wille der Unternehmen, die datenschutzrechtlichen Vorschriften einzuhalten und die berechtigten Ansprüche der Bürger zu erfüllen, ist nicht hinnehmbar. Wir werden auch künftig von den Unternehmen die direkte Erfüllung der den Bürgern im Bundesdatenschutzgesetz gewährten Rechte einfordern.

1. Datenschutzrechtliche Einwilligungen – Wege aus der Sackgasse

1. Informationelle Selbstbestimmung

Wer in voller Sachkenntnis freiwillig persönliche Daten preisgibt oder über die Verwendung seiner Daten durch Dritte bestimmt, übt sein Grundrecht auf informationelle Selbstbestimmung aus (Bundesverfassungsgericht, Volkszählungsurteil von 1983). Er macht von seinem Freiheitsrecht aus Art.1 (Menschenwürde) und Art.2 (allgemeines Persönlichkeitsrecht) Gebrauch. Dazu kann er einer Behörde die persönlichen Daten selbst offenbaren (Realakt) oder die Einwilligung geben, sich die Daten bei einer anderen Stelle zu beschaffen (rechtsgeschäftliche Erklärung). Es geht um die Befugnis, grundsätzlich selbst darüber zu bestimmen, wer was über einen weiß.

Dies ist die Idealvorstellung, die auch dem § 4 Bundesdatenschutzgesetz (BDSG) und § 5 Hamburgisches Datenschutzgesetz (HmbDSG) zugrunde liegt. In der Realität wird dieses hehre Gut freiheitlicher Selbstbestimmung

über die persönlichen Daten von zwei Entwicklungen in seinen Grundfesten erschüttert: Zum einen gehen staatliche Stellen und Wirtschaftsunternehmen dazu über, Lücken in der gesetzlichen Legimitation zur Datenverarbeitung dadurch zu überbrücken, dass sie von den Betroffenen Einwilligungen abfordern. Zum anderen sind Umfang und Sprache der Einwilligungserklärungen häufig so komplex, dass sie die Aufnahmefähigkeit und -bereitschaft der Betroffenen überfordern. Das Ergebnis ist dasselbe: Statt einer selbstbestimmten Entscheidung, anderen den Umgang mit den eigenen Daten zu gestatten, verkümmert die Einwilligung zur Fiktion, wird entweder zur Unterwerfung oder zur unverstandenen Formalie. Datenschutzpolitisch muss es darum gehen, das Institut der Einwilligung wieder auf seinen grundrechtlichen Selbstbestimmungskern zu konzentrieren, seinen freiheitsrechtlichen Gehalt zu retten.

§ 4 BDSG sowie § 5 HmbDSG und entsprechende Vorschriften der anderen Landesdatenschutzgesetze stellen die Einwilligung gleichberechtigt neben eine gesetzliche Regelung, die die Datenverarbeitung ausdrücklich zulässt oder vorschreibt. Das BDSG bezieht diese beiden Ermächtigungs-Alternativen – Gesetz oder Einwilligung – sowohl auf den öffentlichen, staatlichen Bereich als auch auf den nicht öffentlichen Bereich, die private Wirtschaft.

Versteht man die datenschutzrechtliche Einwilligung als rechtsgeschäftliche Willenserklärung (Simitis BDSG § 4a RN 20), dann erscheint weniger der privatrechtliche Bereich als vielmehr der öffentliche, staatliche Anwendungsbereich der Einwilligung begründungsbedürftig. Denn während im Privatrechtsverkehr solche Willenserklärungen und Geschäfte unter rechtlich Gleichen die normale Handlungsform darstellen, ist dies im öffentlichen Bereich die Ausnahme. Nicht durch individuelle Verträge, Willenserklärungen, Angebot und Annahme handelt der Staat, sondern in der Regel durch allgemein verbindliche gesetzliche Regelungen, durch Verwaltungsakte, einseitige Festsetzungen.

Während das private Unternehmen im Geschäftsverkehr selbst Grundrechte wahrnimmt (z.B. die Berufsfreiheit und das Eigentumsrecht), ist der Staat, die öffentliche Stelle den Grundrechten unmittelbar unterworfen. Art.1 Abs.3 GG stellt klar, dass dies für alle drei Staatsgewalten gilt. Die „vollziehende Gewalt“, der gegenüber eine datenschutzrechtliche Einwilligung überhaupt nur in Betracht kommt, agiert dabei ihrerseits als hoheitliche Eingriffsverwaltung, als Leistungsverwaltung, in Form des Verwaltungsprivatrechts oder rein fiskalisch. Für die ersten beiden Arten staatlichen Handelns ist die direkte Grundrechtsbindung unbestritten.

2. Einwilligungen in der Eingriffsverwaltung

Der hoheitliche Staat greift durch seine Polizei-, Aufsichts-, Fach-, Ausländer- und andere Behörden in die Freiheitsrechte der Bürgerinnen und Bürger ein. Er darf dies nach der Formulierung der Grundrechte nur aufgrund eines formel-

len Gesetzes. Dieses hat Ziel und Aufgabe der öffentlichen Stelle zu bestimmen und muss den Grundrechtseingriff im Einzelfall durch ein höherwertiges Allgemeininteresse rechtfertigen. Das bedeutet auch, dass die Eingriffe so grundrechtsfreundlich wie möglich ausfallen müssen. Die Eingriffsregelung muss verhältnismäßig sein. Zum Grundrecht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht deswegen gefordert, dass die Eingriffe in „bereichsspezifischen" Regelungen genau umschrieben werden. Die Flut von spezialgesetzlichen Detailnormierungen – auch als „Verrechtlichungsfalle" kritisiert – hat hier ihren Ursprung.

Wenn aber Aufgabe und konkrete Maßnahmen der Eingriffsverwaltung von Verfassungs wegen gesetzlich fixiert werden müssen, dann fragt sich, wo noch Spielraum bleibt für eine rechtsgeschäftliche Erklärung wie die datenschutzrechtliche Einwilligung. Es ist nicht davon auszugehen, dass die Verfassung einen inhaltlichen Widerspruch zulassen will zwischen allgemeingültigen Anforderungen an das Staatshandeln zum einen und der Ausübung des Grundrechts durch den einzelnen Betroffenen zum anderen: Eine individuelle Erweiterung der hoheitlichen Befugnisse über den gesetzlich vorgegebenen Rahmen hinaus würde den grundrechtlichen Gesetzesvorbehalt aushebeln, die Gewaltenteilung und Kompetenzverteilung im Grundgesetz konterkarieren und möglicherweise auch das Gleichbehandlungsgebot verletzen.

Vermisst z.B. die Polizei in der Praxis bestimmte rechtliche Handlungsmöglichkeiten zur Erfüllung ihrer Sicherheitsaufgaben, so hat sie dies an den grundrechtsgebundenen Gesetzgeber heranzutragen. Eine Einwilligung der Betroffenen in eine neue belastende hoheitliche Maßnahme kann den Gesetzesvorbehalt weder verdrängen noch ersetzen. Unmittelbar einsichtig ist dies, wenn die Polizei gegen eine Mehrzahl von Personen vorgehen müsste und will, aber hierzu keine Rechtsgrundlage hat. Die Einwilligung Einzelner kann die Polizei nicht zum Handeln gegenüber allen Personen legitimieren. Die Polizei ist aus Art.3 GG an das Gleichbehandlungsgebot gebunden. Das gilt auch für Eingriffe, die letztlich auf einer Initiative der Betroffenen selbst beruhen.

Aus diesen Gründen ist das Verfahren der Zuverlässigkeitsüberprüfung im Rahmen der sogenannten Akkreditierung bei Großveranstaltungen – Fußballweltmeisterschaft, G8-Gipfel und ähnliches – nicht zulässig (unten 8.4): Dieses Verfahren sieht vor, dass Gewerbetreibende, Besucher, Aktive darin einwilligen, dass das Landeskriminalamt und der Verfassungsschutz ihre Zuverlässigkeit überprüfen und das Ergebnis dem Veranstalter mitteilen. Spezifische gesetzliche Aufgabenzuweisungen und Datenverarbeitungsermächtigungen hierzu fehlen. Eine Ablehnung der Einwilligung hat die Verweigerung des Zutritts zur Folge – mit möglicherweise existentiellen beruflichen Konsequenzen. Freiwillig ist eine solche Einwilligung daher nicht. Damit ist sie nach § 4 a BDSG auch nicht wirksam. Die Verantwortung für staatliches Handeln auf den Betroffenen selbst zu übertragen, ist ein untauglicher Versuch.

Eine datenschutzrechtliche Einwilligung zur Ermächtigung öffentlicher Stellen der Eingriffsverwaltung ist letztlich nur denkbar, wenn sie nichts mit der hoheitlichen Aufgabe selbst zu tun hat. Insoweit handelt die Stelle dann nicht als Eingriffsbehörde. So ließe sich konstruieren, dass eine Polizeiwache sich für Namen und Adresse ihrer Besucher interessiert, um ihnen eine noch im Druck befindliche Aufklärungs- und Vorbeugungsbroschüre zukommen zu lassen. Entscheidend wäre, dass dieser Zweck mitgeteilt wird und eine Ablehnung der gewünschten Angaben keinerlei negative Konsequenzen hat, also wirklich freiwillig erfolgen kann.

Eine Zwitterstellung nehmen gesetzliche Vorschriften ein, die selbst die Einholung einer Einwilligung vorschreiben und den staatlichen Eingriff – die Verarbeitung der Betroffenendaten – ausdrücklich von ihr abhängig machen. So verhält es sich etwa mit den namensbezogenen Meldungen zum Hamburger Krebsregister und der Datenverarbeitung dort: § 2 des Hamburgischen Krebsregistergesetzes fordert hierzu die Einwilligung des Patienten, verlangt eine entsprechende Aufklärung und regelt Ausnahmen für einwilligungslose Meldungen. Die Ablehnung der Einwilligung hat keinerlei Konsequenzen für die medizinische Behandlung, der Patient kann über die Datenverwendung wirklich frei bestimmen.

Ein anderes Beispiel ist der 2005 neu eingeführte § 81 h Strafprozessordnung: Reihengentests z.B. zur Ermittlung eines Sexualstraftäters aus einer größeren Bevölkerungsgruppe (z.B. Nachbarschaft) wurden zuvor ausschließlich aufgrund von Einwilligungen vorgenommen. § 81 h StPO stellt dies nun auf eine gesetzliche Grundlage: Sie schreibt nicht nur die Einholung der Einwilligung vor, sondern legt auch formale Verfahren, Aufklärungserfordernisse und Zweckbindungen zum Schutze der Betroffenen fest. Problematisch bleibt hier jedoch die Freiwilligkeit der Einwilligung: Wer Speichelentnahme und DNA-Test verweigert, macht sich verdächtig und setzt sich weiteren Ermittlungen aus. Es wäre besser (und ehrlicher) gewesen, die nach festen Kriterien zu bestimmende Personengruppe zur Duldung von Speichelentnahme und DNA-Test zu verpflichten. Wie § 81 c StPO zeigt, sind dem Strafverfahrensrecht körperliche Untersuchungen ohne Einwilligung an „anderen Personen als Beschuldigten“ keineswegs fremd.

3. Einwilligungen in der Leistungsverwaltung

Trotz einer anderen Grundkonstellation gelten die vorstehenden Prinzipien auch für die Leistungsverwaltung: Zwar hat der Gesetzgeber hier im Rahmen des Sozialstaatsprinzips ein weites Gestaltungsermessen. Hat er sich aber zu einer staatlichen Leistungsgewährung für bestimmte Lebenssituationen entschlossen, hat er die materiellen Voraussetzungen und die dafür erforderlichen Angaben der Antragsteller / Begünstigten eindeutig zu umschreiben. Die Angaben der betroffenen Person sind also streng gebunden an den Zweck festzu-

stellen, ob und ggf. in welcher Höhe ein Anspruch auf die staatliche Leistung besteht. Über das Gleichbehandlungsgebot gilt dies grundsätzlich auch für Leistungen, die das Gesetz in das Ermessen der Verwaltung stellt oder die ohne eine spezielle Gesetzesgrundlage nur auf einer Haushaltsentscheidung beruhen. Die Datenoffenbarung der Betroffenen ist hier weniger eine freiwillige rechtsgeschäftliche Einwilligungserklärung als vielmehr die Wahrnehmung einer Obliegenheit oder Mitwirkungs"pflicht", um die Antragsvoraussetzungen zu erfüllen (vgl. § 60 Sozialgesetzbuch – SGB – I). Die Selbstbestimmung liegt in der Entscheidung, einen Leistungsantrag zu stellen; die Datenoffenbarung ist die logische Folge.

Auch hier bilden die gesetzlichen Vorgaben und Förderungsbedingungen einschließlich der erforderlichen Datenverarbeitung abschließende Regelungen, die nicht über individuelle Einwilligungen ausgeweitet werden dürfen. Im Bereich der massenweisen, allgemeinverbindlichen und auf Gleichbehandlung ausgerichteten Leistungsverwaltung ist – jedenfalls im Regelfall – kein Platz für individuelle Lösungen. Die Grundrechtsausübung (Einwilligung) eines Einzelnen kann die Grundrechtsausübung anderer jedenfalls nicht präjudizieren. Einzelentscheidungen der am Gleichbehandlungsgebot orientierten Leistungsverwaltung sind nicht sinnvoll und würden die Leistungsaufgabe verfehlen. So wäre eine Frage an die Leistungsempfänger, wozu sie den „zum Lebensunterhalt" erhaltenen Geldbetrag ganz konkret verwenden werden, auch dann zu kritisieren, wenn die Freiwilligkeit der Antwort außer Frage steht. Sie würde die gesetzliche Aufgabe überschreiten und wäre auch nicht repräsentativ.

Die enge Zweckbindung gilt streng genommen auch für Einwilligungserklärungen in Form von Schweigepflichtentbindungen, wie sie etwa das Versorgungsamt, das Sozialamt, das Gesundheitsamt von den Antragstellern abfordern: Es geht um die Obliegenheit des Antragstellers, die zur Antragsbegründung erforderlichen Informationen beizubringen. Die Einwilligung in die direkte Kontaktaufnahme zwischen Amt und Arzt dient lediglich der Abkürzung des Kommunikationsvorgangs. Das Grundrecht auf informationelle Selbstbestimmung, an das die Leistungsverwaltung gebunden ist, gibt dem Antragsteller das Recht, die Unterlagen auch selbst bei seinen Ärzten zu beschaffen, ohne dem Amt gegenüber eine Schweigepflichtentbindung für den Arzt zu erklären. Ein unverhältnismäßiger Mehraufwand dürfte dem Amt nicht entstehen: In beiden Varianten muss es festlegen, welche medizinischen Informationen es von den Ärzten benötigt. Der Betroffene kann nicht über den erforderlichen Umfang, wohl aber über den Weg der Information frei entscheiden. Holt er die Unterlagen selbst beim Arzt ab, bleibt er auch „Herr" der Datenoffenbarung gegenüber dem Amt.

Im Bereich der gesetzlichen Krankenversicherung hat das Bundessozialgericht den Vorrang der gesetzlichen Regelungen vor einer Einwilligung höchstrichterlich bestätigt (19.TB 6.1): Zur Abrechnung von Krankenhauskosten um-

schreibt § 301 SGB V abschließend die Befugnis des Krankenhauses zur Datenübermittlung an die Krankenkasse. Die Krankenkasse darf zusätzliche Informationen über den Patienten auch nicht über eine Einwilligung der versicherten Person abfordern.

Auch Arbeitsagentur oder ARGE dürfen im Rahmen ihrer Aufgabenerfüllung ALG II-Empfängerinnen und -Empfänger nicht über Motive und Lebenssituationen befragen, selbst wenn die Betroffenen insoweit auf die Freiwilligkeit der Angaben hingewiesen werden. Die Nähe zur Leistungsgewährung verbietet solche Datenerhebungen, wenn sie personenbezogen erfolgen.

Sehr problematisch ist es auch, die Leistungsgewährung von der Einwilligung abhängig zu machen, dass die Verwaltung die anspruchsbegründenden Angaben automatisiert weiterverarbeiten darf. So müssen Hamburger Eltern, die für ihr Kind Lernmittelfreiheit beantragen, vorab zustimmen, dass z.B. die Angabe der Kinderzahl oder die Bescheinigung der Arbeitsagentur in die Lehrer- und Schülerdatei LUSD eingestellt wird. Das Einwilligungsformular enthält den Hinweis, dass die Erklärung nicht abgegeben werden muss, aber „die Schule in diesem Fall die Förderberechtigung oder Gebührenermäßigung regelmäßig nicht anerkennt". Von einer freien Entscheidung kann hier kaum gesprochen werden. Nach längeren Diskussionen konnte die Schulbehörde überzeugt werden, dass die gewünschte Regelung in die Schuldatenschutzverordnung aufzunehmen, also eine entsprechende Ermächtigungsgrundlage zu schaffen ist.

Denkbar ist eine datenschutzrechtliche Einwilligung auch hier nur bei klarer Trennung von der gesetzlichen Aufgabe und bei tatsächlicher Freiwilligkeit. So könnte man sich eine eigenständige Fragebogenaktion vorstellen, mit der ein Sozialamt die Zufriedenheit seiner „Dauerkunden" mit dem Personal ermitteln will. Wenn die befragten Personen die Antworten ohne irgendeine Konsequenz ablehnen können, ist auch eine personenbeziehbare Erhebung zulässig, z. B. um eine spätere gezielte Nachfrage zu ermöglichen.

4. Einwilligungen im Verwaltungsprivatrecht

Handelt die vollziehende Gewalt in privatrechtlicher Organisationsform – z. B. als Großaktionär oder Anteilseigner einer GmbH –, kann sie damit entweder staatliche Aufgaben der Daseinsvorsorge erfüllen (Verwaltungsprivatrecht im engeren Sinne) oder Erwerbswirtschaft betreiben. Zumindest im erstgenannten Fall wird nach herrschender Rechtsauffassung eine „Flucht ins Privatrecht" dadurch vermieden, dass die direkte Grundrechtsbindung auch hier erhalten bleibt.

Für die datenschutzrechtliche Einwilligung bedeutet das zumindest, dass auch im Rahmen (verwaltungs)privatrechtlicher Verträge und Einwilligungsabforderungen in besonderem Maße auf den Selbstbestimmungsspielraum der Betroffenen, auf die Freiwilligkeit der Entscheidung, geachtet werden muss.

Kompliziert, aber relevant ist das Problem, ob die privatrechtliche Form die handelnde Behörde oder Stadt zu einer „nicht öffentlichen Stelle“ macht, die ausschließlich und direkt nach dem 3. Abschnitt des BDSG (nicht öffentlicher Bereich) zu beurteilen ist. Dies gilt nach § 2 Abs.1 Satz 2 HmbDSG für Hamburg uneingeschränkt. Dagegen bleibt eine Bundesbehörde, die in privatrechtlicher Organisation Aufgaben der öffentlichen Verwaltung wahrnimmt und eine beherrschende Stellung einnimmt, datenschutzrechtlich eine öffentliche Stelle. Andererseits sind auch öffentlich-rechtlich organisierte Einrichtungen (z.B. Körperschaften des öffentlichen Rechts wie das Universitätsklinikum Hamburg-Eppendorf) dann wie nicht öffentliche Wirtschaftsunternehmen zu behandeln, wenn sie sich am Wettbewerb beteiligen. Diese gesetzlichen Regelungen werden jedoch die verfassungsrechtliche Grundrechtsbindung der öffentlichen Hand nicht lösen können. In der Praxis kann sich diese aber gegebenenfalls nur über die sogenannte mittelbare Drittwirkung der Grundrechte bei der Auslegung der §§ 28 ff. BDSG (Datenverarbeitung im nicht öffentlichen Bereich) realisieren (siehe dazu unten 6.).

5. Einwilligungen bei fiskalischem Verwaltungshandeln

Bei fiskalischem Handeln agiert die öffentliche Verwaltung privatrechtlich – zumeist als Käuferin, Verkäuferin oder Auftraggeberin in Bezug auf staatliches Eigentum (Beschaffungswesen, Liegenschaftsverwaltung). Die Verarbeitung personenbezogener Daten ist in der Regel dem jeweiligen Rechtsgeschäft immanent oder folgt aus ihm. Sie wird vom Willen zum Vertragsschluss umfasst. Die direkte Grundrechtsbindung fiskalischer Verwaltung ist umstritten, wird aber da anzunehmen sein, wo mittelbar auch öffentliche Aufgaben erfüllt werden – etwa bei der gezielten Vergabe von Liegenschaftsgrundstücken an weniger wohlhabende Käufergruppen. Jedenfalls bleibt die Verwaltung – anders als im Verwaltungsprivatrecht – öffentliche Stelle. Trotz der privatrechtlichen Geschäfte sind deswegen die Landesdatenschutzgesetze bzw. der 2. Abschnitt des BDSG mit den erhöhten datenschutzrechtlichen Anforderungen anzuwenden und nicht der 3. Abschnitt des BDSG, der für die Wirtschaft und andere nicht öffentliche Stellen gilt.

So hätte die Hamburger Liegenschaftsverwaltung die §§ 16, 13 HmbDSG (Übermittlung von öffentlichen an nicht öffentliche Stellen) anwenden müssen, als sie ihre Erbbaugrundstücke an die betroffenen Erbbauberechtigten verkaufen wollte (unten 11.1). Mangels Rechtsgrundlage hätte sie ihre Vertragspartner um Einwilligung bitten oder ihnen jedenfalls Gelegenheit zum Widerspruch geben müssen, bevor sie einem Makler die Personalien der Betroffenen übermittelte. Die Betroffenen wären auch in ihrer Entscheidung frei gewesen, die Übermittlung ihrer Daten an einen Dritten abzulehnen, z.B. wenn sie einen Grundstückskauf überhaupt ablehnten.

6. Einwilligungen im Privatrechtsverkehr

Informationsaustausch und Datenverarbeitung im nicht öffentlichen Bereich – im wirtschaftlichen und gesellschaftlichen Leben – sind zumeist eng verbunden mit Verträgen und Geschäftsbeziehungen „unter rechtlich Gleichen". Auch die Einwilligung als rechtsgeschäftliche Erklärung unterliegt dieser Vorstellung von Privatautonomie und Gleichstellung – eine Idealvorstellung, die in der Realität an Grenzen stößt.

Das „Recht auf informationelle Selbstbestimmung entfaltet als Norm des objektiven Rechts seinen Rechtsgehalt auch im Privatrecht" (Bundesverfassungsgericht, Beschluss vom 11.7.2007). Es wirkt im nicht öffentlichen Bereich auf zweierlei Weise: Zum einen ist nach Art.1 Abs.3 GG bereits der Gesetzgeber zivilrechtlicher Normen an die Grundrechte gebunden und muss bei Grundrechtsgefährdungen Schutzgesetze erlassen. Dies ist der Grund für die Datenschutzgesetze, hier für das BDSG, 3. Abschnitt. Zum anderen ist bei der Auslegung von zivilrechtlichen Generalklauseln und unbestimmten Rechtsbegriffen die Wertentscheidung der Verfassung, die in den Grundrechten zum Ausdruck kommt, zu berücksichtigen (mittelbare Drittwirkung der Grundrechte).

Einwilligungen stehen nach dem Wortlaut des § 4 BDSG auch im nicht öffentlichen Bereich gleichberechtigt neben den gesetzlichen Datenverarbeitungsermächtigungen der §§ 28 ff. BDSG. Kann – anders als die grundrechtsgebundene Verwaltung – ein Unternehmen deswegen beliebig wählen zwischen der Berufung auf die gesetzliche Verarbeitungsbefugnis in § 28 BDSG und der Einholung einer Einwilligung? Dies würde bedeuten, dass alle gesetzlichen Anforderungen an die Datenverarbeitung – von der Zweckbestimmung und -bindung über die Einschränkung der Zweckänderungstatbestände bis zur Spezialregelung für Werbung und Markt- oder Meinungsforschung – disponibel sind und über eine Einwilligung außer Kraft gesetzt werden können. Hinsichtlich der Verarbeitung von besonders sensiblen Arten personenbezogener Daten (z.B. zur Gesundheit) lässt der Gesetzgeber genau dies in § 28 Abs. 6 BDSG tatsächlich zu: Die gesetzlichen Datenverarbeitungs-Restriktionen gelten nur, „soweit nicht der Betroffene nach Maßgabe des § 4a Abs.3 eingewilligt hat". In Bezug auf die weniger riskante „normale" Verarbeitung personenbezogener Daten kann dann nichts anderes gelten.

Steht eine individuelle Einwilligung demnach den gesetzlichen Schutzvorschriften für den Betroffenen gleich, muss jedoch – auch wegen der mittelbaren Drittwirkung der Grundrechte -sichergestellt werden, dass der vom Gesetzgeber anerkannte Schutzbedarf der Betroffenen auf andere Weise berücksichtigt wird. Dies kann nur über entsprechend hohe Anforderungen an eine wirksame Einwilligung erfolgen. Die in § 4a BDSG genannten Bedingungen – vor allem die „freie Entscheidung" und die Hinweise auf den Verarbeitungszweck – müssen so erfüllt werden, dass sich ein externer Schutz des Einwilli-

genden erübrigt. In der Realität bedeutet das vor allem: Die Freiheit des Betroffenen, die Einwilligung zu verweigern, ohne negative Folgen befürchten zu müssen, ist ernst zu nehmen.

7. Einwilligungen zum Zweck der Vertragserfüllung

Setzt die Erfüllung eines Vertrages – z.B. die Lieferung von Ware gegen Rechnung – eine Verarbeitung personenbezogener Daten voraus, dann wird sie von den rechtsgeschäftlichen Willenserklärungen umfasst. Die freie Entscheidung bezieht sich auf das Geschäft insgesamt. Ist es gewollt, ist auch die dafür erforderliche Datenverarbeitung gewollt.

Diese alltägliche Situation bildet § 28 Abs.1 Nr.1 BDSG ab: Die Datenverarbeitung, die der Zweckbestimmung eines Vertragsverhältnisses dient, ist – ohne Einwilligung – gesetzlich zugelassen. Die Einholung einer Einwilligung (in die Datenverarbeitung) ist in diesen Fällen kontraproduktiv: Sie ist nicht nur unnötig, sondern suggeriert auch eine Entscheidungsfreiheit, die nicht besteht. Denn wenn der Betroffene nicht einwilligt (oder die Einwilligung später widerruft), gilt dennoch die gesetzliche Regelung. Es wäre widersinnig, bei einer Lieferung gegen Rechnung dem Käufer das Recht einzuräumen, seine (Liefer-)Adresse und die (Beleg-)Daten der Banküberweisung zu verheimlichen.

Im Kern geht es jedoch auch um etwas anderes: Die Vereinbarungen zwischen Geschäftspartnern sollten so gestaltet sein, dass Erhebung, Speicherung und Nutzung von personenbezogenen Daten zur Vertragserfüllung angemessen und erforderlich sind. Es sollen nur solche personenbezogenen Informationen vom Vertragspartner verlangt werden, die in einem inneren Zusammenhang mit den Vertragsleistungen stehen, sie erst ermöglichen. Die Datenverarbeitung wird zum immanenten Teil des Vertrages; sie könnte auch in den Vertragstext selbst aufgenommen werden. Eine gesonderte datenschutzrechtliche Einwilligung macht keinen Sinn. Von ihr ist abzusehen. Dies fordert gerade auch das Recht auf informationelle Selbstbestimmung: Der Betroffene sollte nicht über die Relevanz seiner Einwilligungserklärung getäuscht werden.

Allerdings kann durchaus umstritten sein, wo im konkreten Fall die Grenze der Erforderlichkeit der Datenverarbeitung und des inneren Zusammenhangs mit der Vertragserfüllung verläuft: Wie weit reicht der Vertragszweck z.B. bei Datenerhebungen zur Kreditwürdigkeit des Kunden? Bezieht der Vertragszweck auch die Übermittlung von Kundendaten an die SCHUFA mit ein – ist sie also gesetzlich legitimiert? Dies wird man bei Bankgeschäften anders beurteilen müssen als bei Lieferungen auf Nachnahme (Bezahlung bei Empfang der Ware) oder bei der Vermietung von Wohnraum.

Im Arbeitsrecht hat die Rechtsprechung weitgehend festgelegt, welche Bewerberdaten für den Arbeitsvertragszweck erforderlich sind und wo das Frage-

recht des Arbeitgebers seine Grenze findet. Diese darf auch nicht durch eine gesonderte individuelle Einwilligung überschritten werden – z.B. um eine genetische Untersuchung zur Ermittlung von Krankheitsanlagen zu ermöglichen, die in der Zukunft vielleicht einmal zu einem Arbeitsausfall führen könnten.

8. Einwilligungen zur Wahrung berechtigter Interessen

Bezieht sich der Inhalt der Einwilligung nicht auf die Zweckbestimmung eines Vertrages, sondern auf andere berechtigte Interessen desjenigen, der um die Einwilligung bittet, scheint dagegen der Spielraum für eine freiwillige Selbstbestimmung eher gegeben. Immerhin ist denkbar, dass beide Seiten ihre Interessen – jenseits des Vertragsgegenstandes – gleichberechtigt abwägen und dann eine freie Entscheidung treffen. Diese könnte in Form einer Einwilligung ihren Niederschlag finden.

Dennoch: Auch die gesetzliche Regelung in §§ 28 Abs.1 Nr.2, Abs.3; 29 BDSG sieht für die „Wahrung berechtigter Interessen" eine Abwägung mit den schutzwürdigen Interessen der Betroffenen vor. Sie gibt eine gesetzliche Datenverarbeitungsermächtigung – und zwar unabhängig davon, ob sich die beiden Seiten einigen können oder nicht. Die Einholung einer Einwilligung ist deswegen grundsätzlich nicht erforderlich. Ist klar, dass das Interesse der Stelle gegenüber möglichen Interessen des Betroffenen überwiegt, dann gilt die gesetzliche Datenverarbeitungsermächtigung des § 28 Abs.1 Nr.2 BDSG. Eine gesonderte Einwilligung ist auch hier überflüssig und kontraproduktiv, weil sie eine freie Selbstbestimmung nur vortäuscht. Denn wird die Einwilligung verweigert oder widerrufen, ist doch wieder die gesetzliche Grundlage für die Datenverarbeitung zu prüfen und – nach entsprechender Interessenabwägung – als Verarbeitungsermächtigung gültig. Auch in diesen Fällen ist deswegen – neben der gesetzlichen Ermächtigung – für eine eigene Einwilligung in die Verarbeitung personenbezogener Daten kein Raum.

Schwieriger noch als bei der Datenverarbeitung zur Vertragserfüllung ist die Abgrenzung des von § 28 Abs.1 Nr.2 BDSG abgedeckten Ermächtigungsbereichs. Deswegen mag im Einzelfall eine Einwilligung auch dann in Betracht kommen, wenn die abstrakt-pauschalierende Abwägung im Rahmen des § 28 Abs. 1 Nr. 2 BDSG zu keinem eindeutigen Ergebnis führt, da in dieser typisierenden Betrachtung für individuelle Besonderheiten einzelner Betroffener kein Platz ist. Das Korrektiv für diese Überwälzung der Verantwortung von der Daten verarbeitenden Stelle auf die (einwilligende) betroffene Person muss dann jedoch darin liegen, dass der Betroffene die Einwilligung ablehnen kann, ohne den Vertrag zu gefährden.

Die Reichweite der gesetzlichen Ermächtigung ist z.B. zweifelhaft bei der Frage, welche Daten ein Vermieter von einem Mietinteressenten bei einer Auskunftei abfragen darf bzw. welche Daten die Auskunftei im Rahmen von § 29 BDSG an den Vermieter übermitteln darf (unten 24.3). Soweit die allgemein-

abstrakte Abwägung zwischen den Vermieter- und den Mieterinteressen die Datenverarbeitung noch als angemessen erscheinen lässt, kann sie auf § 28 bzw. § 29 BDSG gegründet werden. Eine Einwilligung in eine darüber hinausgehende Datenerhebung und Übermittlung wäre zwar denkbar, aber mangels Freiwilligkeit unwirksam, weil im Ergebnis die Vermietung von ihr abhängig gemacht würde.

9. Einwilligungen in Allgemeinen Geschäftsbedingungen

Im alltäglichen Geschäftsleben werden nicht selten Einwilligungen im Rahmen von Allgemeinen Geschäftsbedingungen (AGB) abgefordert – unabhängig davon, ob ihr Zweck in der Vertragserfüllung (oben 7.), in der Wahrung berechtigter Interessen (oben 8.) oder in zusätzlichen Wünschen des Verwenders liegt. Unternehmen wollen sich absichern für den Fall, dass die gesetzlichen Ermächtigungen nach den §§ 28 ff. BDSG für die begehrte Datenverarbeitung nicht ausreichen. Mit der Abforderung einer Einwilligung überträgt das Unternehmen in diesen Fällen die Verantwortung für die Rechtmäßigkeit der Datenverarbeitung von sich auf die betroffene Person: Zweifel an der Gesetzmäßigkeit sollen durch die Alternative „Einwilligung“ verdrängt werden.

Meist geht es um die Verarbeitung von Daten zur Kreditwürdigkeit, um den Schutz vor Schäden durch den Kunden oder um die Weiterverwendung von personenbezogenen Daten zu Werbezwecken. Ein angestrebter Versicherungsschutz, eine Kontoeröffnung werden oft nur erreicht, wenn der betroffene Kunde die AGB und die damit verbundene Einwilligungserklärung unterschreibt. (Dass AGB-Verwender zuweilen den Abschluss eines AGB-Vertrages mit Datenverarbeitungsklausel sowohl als „Einwilligung“ als auch für gesetzlich legitimiert ansehen, zeigt der unten unter 26.1. beschriebene Fall.)

Mit dem Sinn der Einwilligung nach § 4a BDSG, mit der individuellen Ausübung der informationellen Selbstbestimmung, hat dies regelmäßig nichts mehr zu tun. Eine „freie Entscheidung“ ist Illusion.

Deswegen bedarf es grundsätzlich einer Entscheidung darüber, ob der gesetzliche Ermächtigungsbereich für die gewünschte Datenverarbeitung ausreicht oder nicht, mit anderen Worten: ob sich das Unternehmen noch im Bereich des berechtigten Eigeninteresses bewegt, das die Interessen des Betroffenen überwiegt. Ist dies so, gilt das Gesetz und haben („prophylaktische“) Einwilligungserklärungen keinen Platz. Erst wo dieser Bereich überschritten ist, das abstrakt-typisierende schützwürdige Interesse der Betroffenen also überwiegt, ist der Bereich der Einwilligungen eröffnet. Eine Einwilligungserklärung mag hier auch als AGB-Teil angefügt werden. Wirksamkeitsvoraussetzung ist jedoch, dass der Betroffene über Erteilung oder Ablehnung frei entscheiden kann, ohne den Vertrag zu gefährden.

Dafür ist in der Regel dort Raum, wo es für den AGB-Verwender nicht entscheidend darauf ankommt bzw. wo die Einwilligung auch im Interesse des Betroffenen sein kann – etwa bei der Weiterverwendung von Kundendaten zu Werbezwecken, bei der Erhebung und Weitergabe von Positivdaten durch Auskunfteien (unten 24.1) oder bei der Weitergabe von Umzugsdaten von Versandhauskunden an Adresshändler (unten 26.2).

Wo es jedoch um elementare Geschäftsinteressen wie die Zahlungsfähigkeit und Kreditwürdigkeit, das Risiko des Eintritts der Leistungspflicht oder den Schutz vor Täuschung und Missbrauch durch den Vertragspartner geht, kann die Datenverarbeitung zur Wahrung der eigenen Interessen kaum vom Willen des Vertragspartners abhängig gemacht werden. Hier wird der AGB-Verwender – im Rahmen der Vorgaben des § 307 BGB – grundsätzlich durch die Varianten der §§ 28 ff. BDSG zur Datenverarbeitung ermächtigt. Einwilligungen in diesem Bereich wären nicht nur überflüssig, sondern zumeist auch wegen fehlender Freiwilligkeit unwirksam.

Die jahrelangen und noch immer nicht beendeten Diskussionen zwischen Datenschutzaufsicht und Versicherungswirtschaft um die Einwilligungsklauseln in Antragsformularen (unten 22.2, 20.TB 20.1) und um die Schufa-Klauseln bei Kontoeröffnung (unten 23.1) zeigen sehr deutlich: Die Debatte wird nicht um die Anforderungen an eine freie Entscheidung des Versicherungsnehmers geführt, sondern um die Angemessenheit und Zumutbarkeit der von der Versicherungswirtschaft bzw. den Auskunfteien wie der Schufa gewünschten Datenerhebungen und -übermittlungen. In Wahrheit geht es darum, ob die Klauseln noch als Vertragszweckerfüllung oder zur Wahrung des überwiegenden Versichererinteresses gesetzlich legitimiert sind oder nicht. Wären die Voraussetzungen des § 4a BDSG – insbesondere eine freie Entscheidung ohne Nachteile – erfüllt, würden sich die inhaltlichen Auseinandersetzungen erübrigen: Der Kunde hätte die freie Wahl, ihm nicht genehme Übermittlungen an Warn- und Hinweisdateien, Schufa-Abfragen usw. einfach abzulehnen, ohne auf den Versicherungsschutz oder ein Konto verzichten zu müssen.

In einem Punkt hat nach einer Entscheidung des Bundesverfassungsgerichts der Gesetzgeber gehandelt: Gemäß § 213 Versicherungsvertragsgesetz haben die AGB dem zukünftigen Versicherten nun das Recht einzuräumen, zwischen einer einmaligen Schweigepflichtentbindung „auf Vorrat“ und einer jeweils im konkreten Leistungsfall zu erteilenden Schweigepflichtentbindung zu wählen (vgl. unten 22.1). (Die Einwilligungserklärung selbst wird auch hier nicht vom Datenschutzrecht, sondern von der strafbewehrten ärztlichen Schweigepflicht, § 203 StGB, verlangt.)

Neben gesetzlichen Vorgaben und der gerichtlichen AGB-Kontrolle nach den §§ 305 ff. BGB prüfen auch die Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich die Datenverarbeitungsregelungen in AGB auf Angemessenheit und Interessensausgleich. Sie sollten nur dort „Einwilligungs-

klauseln“ zulassen, wo der Ermächtigungsbereich der §§ 28, 29 BDSG verlassen wird, das schutzwürdige Interesse der Betroffenen also die berechtigten Interessen der Daten verarbeitenden Stelle überwiegt. Dies setzt eine klare Grenzziehung und Entscheidung voraus. Für die Geschäftsbedingungen von Versicherern und Banken ist nach unserer Auffassung darüber hinaus die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) mit dafür verantwortlich, dass zumindest das in § 28 BDSG formulierte Datenschutzniveau – insbesondere die ausreichende Berücksichtigung der Betroffeneninteressen – in den AGB eingehalten wird.

10. Einwilligungen in freier Selbstbestimmung

Aus dem Vorstehenden ergibt sich insgesamt, dass sowohl für staatliche Stellen als auch für privatrechtliche Unternehmen der Spielraum zur Abforderung von Einwilligungen viel kleiner ist, als die Verwaltung und Geschäftswelt derzeit praktiziert. Eine Einwilligung, die nicht nur notgedrungen eine formale Mitwirkungspflicht erfüllt, sondern tatsächlich Ausübung der (grundrechtlichen) Selbstbestimmung ist, setzt Entschlussfreiheit voraus. Der Lackmustest dafür ist die Frage nach den Folgen einer Einwilligungsverweigerung.

Diese Freiheitsspielräume gibt es durchaus – aber weniger in der Routine des Verwaltungshandelns oder des Massengeschäfts, sondern eher in einzelnen Projekten, bei besonderen Fragestellungen, individuellen Zwecksetzungen oder zusätzlicher, ergänzender Informationsverarbeitung. So können – um Fälle aus der täglichen Praxis zu nennen – Krankenhauspatienten außerhalb des Behandlungsvertrages gefragt werden, ob sie zur Planung einer Serviceverbesserung freiwillig ihre Religionszugehörigkeit oder ihre Staatsangehörigkeit angeben möchten; ein Nein hat auf die Behandlung keinen Einfluss. Ein Kaufhaus kann seine Kunden bitten, die Postleitzahl ihres Wohnortes zu nennen, um den Einzugsbereich zu ermitteln; der Kunde ist frei, dem zu folgen. Lehrer können ihre Schüler/innen und deren Eltern darum bitten, Schulleistungen und Berufswünsche der jungen Leute an eine private Beratungs- und Vermittlungsfirma weitergeben zu dürfen; eine Verweigerung bleibt ohne Nachteile. Dasselbe gilt für die oben unter 9. genannten Datenverarbeitungen geringerer Relevanz für den AGB-Verwender.

Ein großer Bereich für freiwillige Einwilligungsentscheidungen ist die Forschung. Niemand wird gezwungen, seine personenbezogenen Daten Wissenschaftlern für Forschungszwecke zur Verfügung zu stellen. Viele Menschen haben umgekehrt sogar ein Interesse daran, mit den eigenen Daten zu Erkenntnisfortschritten beizutragen. Die Entscheidung für oder wider hängt oft vom konkreten Forschungsziel ab.

Nur erwähnt, aber nicht vertieft werden soll, dass in all diesen Fällen, in denen eine freiwillige Einwilligung möglich und sachgerecht ist, neben der ausreichenden Information über den Einwilligungsgegenstand die gesetzlichen

Formerfordernisse und Hinweispflichten zu beachten sind: Schriftlichkeit, besondere Hervorhebung bei einer Verbindung mit anderen Erklärungen, ausdrückliche Bezugnahme auf besondere Arten personenbezogener Daten, § 4a BDSG. § 5 Abs.2 HmbDSG fordert darüber hinaus, dass die öffentliche Stelle auf Möglichkeit und Folgen hinweist, die Einwilligung zu verweigern und zu widerrufen. Bei Geschäften über das Internet gelten schließlich Besonderheiten wie Eindeutigkeit der Willensbekundung, Protokollierungspflicht und jederzeitige Abrufbarkeit des Einwilligungstextes, § 13 Abs.2 Telemediengesetz.

11. Einwilligungen in Kenntnis des Sachverhalts

Eine Einwilligung ist nur wirksam, wenn der Einwilligende weiß, „worauf er sich einlässt". Er benötigt Informationen über den Zweck der Datenverarbeitung und über die Folgen einer Ablehnung der Einwilligung, § 4a BDSG (informed consent). Für die Hamburger Verwaltung fordert § 5 Abs.2 HmbDSG im Einzelnen, dass Gegenstand, Inhalt und Umfang der Datenverarbeitung, die Art der Daten, die Übermittlungsempfänger und die Speicherungsdauer „klar und verständlich" bezeichnet werden.

Gerade im Bereich der Forschung, aber auch im Geschäftsverkehr wird die Bitte um eine Einwilligung aber nicht selten auch mit komplizierten, in Bürokraten- oder Juristendeutsch abgefassten Aufklärungstexten verbunden. Hier wäre weniger manchmal mehr. Soll die Einwilligung stärker auf ihre Funktion als freie Grundrechtsausübung konzentriert werden, dann dürfen auch die Verständnismöglichkeiten und „Verarbeitungskapazitäten" der Einwilligenden nicht überfordert werden.

Der Entwurf eines Gendiagnostikgesetzes sieht nicht nur verschiedene Gegenstände für die Einwilligungsentscheidung selbst vor, sondern auch einen ausführlichen Katalog von elf obligatorischen Aufklärungspunkten – darunter Angaben zur Herkunft der Forschungsmittel, zu vorgesehenen Kooperationspartnern, zur Bewertung durch die Ethikkommission, zur kommerziellen Verwertung erzielter Forschungsergebnisse. Nur wenige Patienten, die vor einer Krebsoperation um eine Einwilligung in die genetische Untersuchung ihrer Tumorzellen gebeten werden, dürften Verständnis für solche Detailinformationen aufbringen, vgl. unten 14.7.

Andererseits muss es speziell Interessierten ermöglicht werden, alle für sie wichtigen Entscheidungsgrundlagen zu erhalten. Diesen widersprüchlichen Anforderungen an die Aufklärung für eine Einwilligung ist praktisch nur in einem mehrstufigen Verfahren zu begegnen: Eine einfache, auf das Wesentliche beschränkte Grundinformation ist je nach Wunsch der Betroffenen um weitere Angaben und Aufklärungen zu ergänzen. Dem sollte auch die schriftliche Projektinformation Rechnung tragen. Auch Datenschützer neigen nicht selten dazu, das Interesse und auch die Aufnahmebereitschaft der Betroffenen an Einzelheiten von Forschungsprojekten zu überschätzen. Im legitimen Be-

streben, die Menschen nicht zum Objekt von Forschung und zum Opfer von „Übertölpelungen“ werden zu lassen, wird zuweilen die Anforderung an die Kenntnis des Sachverhalts, an die Konkretisierung des Einwilligungsgegenstandes übersteigert und so die subjektive Selbstbestimmungsfreiheit eher eingeschränkt als gefördert.

12. Fazit

Um die datenschutzrechtliche Einwilligung als Instrument freier Selbstbestimmung zu stärken, muss ihr Anwendungsbereich auf die Fälle konzentriert werden, die tatsächlich Entscheidungsfreiheit bieten. Dies setzt im konkreten Einzelfall ein Verhältnis „unter Gleichen“ voraus. Im Bereich der Eingriffs-, aber auch der Leistungsverwaltung ist dies in aller Regel nicht gegeben. Der Staat darf die gesetzliche Aufgabenzuweisung und Verfahrensfestlegung nicht durch eine Einwilligung ausdehnen. Im nicht öffentlichen Bereich kommen Einwilligungen erst dort in Betracht, wo die gesetzlichen Ermächtigungen des BDSG enden. Im privatrechtlichen Massengeschäft müssen die staatliche Aufsicht und die Inhaltskontrolle der Allgemeinen Geschäftsbedingungen für datenschutzgerechte Austauschbeziehungen sorgen. Danach bleiben für eine wirksame Einwilligung nur noch eher individuelle, besondere Fallkonstellationen übrig, in denen es dem Betroffenen keinerlei Nachteile bringt, eine erbetene Einwilligung zu verweigern. Diese etwa in der Forschung zu findenden Bereiche müssen ihrerseits vor einer Überfrachtung von Aufklärungs- und Informationsanforderungen geschützt werden. Der Einzelne soll seine freie Entscheidung auf der Grundlage treffen können, die er selbst für ausreichend hält. Dies erreichen mehrstufige Informationsangebote nach den Bedürfnissen der Betroffenen.

2. Informations- und Kommunikationstechnik

2.1 E-Government – Technik muss dem Recht folgen

Bei E-Government-Projekten müssen die datenschutzrechtlichen Rahmenbedingungen stärker beachtet werden.

Auch in diesem Berichtszeitraum hat sich der Hamburgische Datenschutzbeauftragte intensiv mit den Projekten zum E-Government auseinandergesetzt. Dabei ist unsere Handlungsleitlinie, kundenorientierte und datenschutzgerechte Lösungen zu finden. Die beschlossene EU-Dienstleistungsrichtlinie wird dem E-Government-Prozess einen zusätzlichen Schub geben und die Rahmenbedingungen nachhaltig prägen. Nach der Richtlinie muss es ab 2009 möglich sein, IT-gestützt direkt mit den zuständigen Behörden aller übrigen EU-Mitgliedstaaten zu kommunizieren. In die verstärkte elektronische Kommu-

nikation werden neben Behörden vermehrt auch Akteure außerhalb der Verwaltung einzubinden sein.

Vor dem Hintergrund seiner Erfahrungen bei der Begleitung zahlreicher E-Government-Projekte und in Anbetracht der veränderten Rahmenbedingungen hat der HmbDSB zum E-Government-Strategiebericht 2007/2008 des Senats (Bürgerschaftsdrucksache 18/6908) zwei grundlegende Problembereiche aufgezeigt, die es in Zukunft verstärkt zu beachten gilt:

Zum einen besteht das Problem, dass der Strategieansatz für die E-Government-Neuorientierung auf Kommunikationsstrukturen und Datenaustausche ausgerichtet ist, denen in vielen Fällen die Bestimmungen des Hamburgischen Datenschutzgesetzes entgegenstehen. Die fehlende Rechtsgrundlage kann jedoch nicht durch den verständlichen Wunsch nach „Verwaltungsmodernität", durchgängiger Online-Nutzung und „medienbruchfreier Kommunikation" ersetzt werden. Die Projekte müssen deshalb aus rechtsstaatlichen Gründen nach dem Prinzip „Die Technik folgt dem Recht" gestaltet werden. Das bedeutet: Entweder basiert die technische Ausgestaltung der E-Government-Vorhaben auf der bestehenden Rechtslage, oder es müssen notwendige Rechtsänderungen frühzeitig vor Einführung neuer Verfahren herbeigeführt werden, etwa wenn durch leistungsstärkere Technik neue , insbesondere automatisierte Verarbeitungsabläufe eröffnet werden sollen.

Schon in der Vergangenheit musste der Hamburgische Datenschutzbeauftragte in folgenden Fallgruppen rechtliche Hinweise geben und fehlende Ermächtigungsgrundlagen einfordern, so dass eine frühestmögliche Klärung der nachstehenden Fragen auch aus wirtschaftlichen Gründen geboten ist:

- Das Hamburgische Datenschutzgesetz verbietet, soweit nicht gesonderte spezialgesetzliche Ermächtigungen bestehen, einen automatisierten Abruf von personenbezogenen Daten durch private Dritte, wenn es sich dabei nicht um ihre eigenen Daten als Betroffene handelt (§ 11 Abs. 4 HmbDSG). Diese Fragestellung wird vor allem bei Adressaten berührt, die regelmäßig professionell mit der Verwaltung Kontakt haben, wie z.B. Architekten, Rechtsanwälte, Notare, Autohändler oder Vermessungsbüros, und denen elektronische Zugangskanäle zur Verwaltung geschaffen werden sollen. Aber auch in allen Fällen von Outsourcing muss dies beachtet werden, wenn nämlich ehemals öffentliche, nunmehr aber in privater Rechtsform agierende Stellen für ihre Aufgabenwahrnehmung Daten von Bürgern weiterhin aus Dateien der Verwaltung abrufen wollen.

- Werden automatisierte Abrufe für andere Behörden eingerichtet oder sollen Daten gemeinsam aus einer Datei genutzt werden, ist regelmäßig zu prüfen, ob für diese Art der Verarbeitung schon eine Rechtsgrundlage besteht oder noch eine Rechtsverordnung zu erlassen ist (§§ 11,11a HmbDSG).

- Bei länderübergreifender Verarbeitung personenbezogener Daten (vgl. 17.1 Metropolregion) ist in diesen Fällen der vorherige Abschluss eines Staatsvertrages erforderlich, soweit nicht eine ausreichende bundesgesetzliche Regelung besteht oder geschaffen wird.

Werden diese datenschutzrechtlichen Anforderungen nicht rechtzeitig erfüllt, ist die Datenverarbeitung unzulässig.

Zum anderen haben die Nutzer von E-Government-Angeboten die berechtigte Erwartung, dass die angebotenen Verfahren sicher sind. Die strategische Planung muss sich daher auch auf den Bereich der Sicherheit und ihre Fortentwicklung erstrecken. Durch umfassende technische und organisatorische Sicherheitsmaßnahmen werden nicht nur die personenbezogenen Daten im erforderlichen Umfang geschützt, sondern diese Maßnahmen wirken zugleich für die Nutzer vertrauensbildend und sichern somit die Akzeptanz.

Neben der Vertraulichkeit spielt insbesondere die Authentizität bei einer allein technisch vermittelten Behördenkommunikation eine erhebliche Rolle. Die elektronische Signatur kann hierbei zu einer wesentlichen Verbesserung beitragen. Der Hamburgische Datenschutzbeauftragte hatte bereits in seinem 19. Tätigkeitsbericht 2002/2003 auf die Erforderlichkeit einer sicheren Authentisierung beim E-Government hingewiesen. Trotz der Ankündigung des Senats in der Mitteilung an die Bürgerschaft (Bürgerschaftsdrucksache 18/4965), das HamburgGateway im Jahr 2006 diesbezüglich zu erweitern, steht die Signatur für eine sichere Authentisierung im HamburgGateway bisher lediglich theoretisch für Firmennutzer zur Verfügung. Sie wird jedoch nach wie vor von keinem E-Government-Verfahren genutzt. Offen ist auch noch, wann diese Form der Authentisierung für private Nutzer freigegeben wird. Wir werden auch in Zukunft darauf achten, dass das Interesse nach zügiger Ausweitung des E-Government-Angebotes nicht zu einer Senkung des Sicherheitsniveaus führt, sondern vielmehr darauf hinwirken, dass Datenschutz als „Türöffner“ für neue Kommunikationsformen begriffen wird.

2.2 BlackBerry: Daten bei Führungskräften unzureichend geschützt

Mit den festgelegten Einsatzbedingungen für BlackBerry-Geräte vernachlässigt die Finanzbehörde Anforderungen der Datensicherheit und des Datenschutzes.

Seit Sommer 2007 können insbesondere Führungskräfte der hamburgischen Verwaltung ihre E-Mails, Termine und elektronischen Dokumente auf ein dienstliches BlackBerry-Gerät weiterleiten, dass zugleich als Mobilfunk-Gerät nutzbar ist. Die ca. 180 Nutzer bleiben dadurch auch außerhalb ihres Büros erreichbar und können so über den jeweils aktuellen dienstlichen Informationsstand verfügen. Da auf den mobilen IT-Geräten auch sensible personenbezogene Daten verarbeitet werden, sind damit jedoch zusätzliche Risiken verbun-

den, die die Vertraulichkeit der Daten besonders gefährden. Diese Geräte werden typischer Weise auf Tagungen und Besprechungen, in Zügen und Hotels genutzt. Es ist daher besonders wichtig, dass in diesen ungeschützten Umgebungen keine unberechtigten Personen Einsicht in die vertraulichen Daten nehmen können. Auch die Finanzbehörde bewertet die Eintrittswahrscheinlichkeit eines daraus entstehenden Schadens als hoch. Obwohl die Gefährdung durch die mobile Nutzung also weit höher ist als an Arbeitsplatzrechnern, wurden in die Nutzungsbedingungen für BlackBerry, die die Finanzbehörde festgeschrieben hat, aber nicht einmal die normalen Schutzmaßnahmen übernommen. Während Arbeitsplatzrechner spätestens 30 Minuten nach der letzen Nutzung automatisch gesperrt werden, bleiben unbenutzte BlackBerry-Geräte zwei Stunden offen. In einem unbeobachteten Moment kann dann jeder Einblick in die Daten nehmen. Gegen diese Bedrohung greifen auch nicht die sonst getroffenen Sicherheitsmaßnahmen der BlackBerry-Geräte, die in einer aktuellen Fraunhofer-Studie positiv bewertet werden. Gegen diese Bedrohung greift nur die Festlegung einer kurzen Zeitspanne für die automatische Zugriffsperrung.

Auch die Anforderungen an das Passwort, das zur Aktivierung des Geräts eingegeben werden muss, entsprechen nicht dem bisherigen Stand. Aufgrund unserer kritischen Stellungnahme hat die Finanzbehörde nicht die Sicherheitsmaßnahmen für BlackBerry entsprechend der Passwort-Richtlinie angepasst, sondern die Möglichkeit einer Lockerung der Richtlinie für diese Geräte geschaffen.

Die Finanzbehörde ignoriert damit zahlreiche Studien, die aufzeigen, dass gerade mobile Geräte vermehrt Angriffsziele sein werden. Obwohl der Finanzbehörde die Erfahrungen und Einsatzregelungen solcher Geräte in anderen Organisationen und Ländern bekannt sind, setzt sie sich in ihrer Risikoanalyse nicht in dem erforderlichen Maße damit auseinander, so wie es eine fundierte Risikoanalyse verlangt.

Dies betrifft auch den besonderen Dienst, dass sich BlackBerry-Nutzer sogar ihre privaten E-Mails eines privaten E-Mail-Accounts auf ihr BlackBerry weiterleiten lassen können. Entgegen den Vorgaben der PC-Richtlinie wird dabei die zentrale Firewall der FHH umgangen. Dieses zusätzliche Risiko wird von der Finanzbehörde in Kauf genommen, obwohl mit diesem Service keine dienstliche Nutzung verbunden ist.

Die von der Fraunhofer-Gesellschaft positiv bewerteten grundlegenden technischen Schutzmaßnahmen für BlackBerry werden durch die von der Finanzbehörde festgelegten Einsatzbedingungen konterkariert mit der Wirkung, dass insgesamt eine datenschutzgerechte Nutzung nicht gewährleistet ist. Wir haben die Behörde daher aufgefordert, hier weitere Schutzmaßnahmen zu treffen.

2.3 Unzulässiger Test mit Originaldaten

Beim Massentest für automatisierte Bankauszahlungen an BAföG-Empfänger wurde bei Dataport gegen Sicherheitsvorschriften und die Freigabe-Richtlinie verstoßen.

Um die Wirksamkeit von Maßnahmen zur Verbesserung der Performance zu testen, wurde bei Dataport im Januar 2006 ein Test des SAP-Zahlverfahrens BAföG mit Originaldaten durchgeführt. Dadurch kam es kurzzeitig zu ungerechtfertigten Auszahlungen in Höhe von über 3 Mio. Euro. Ein Auftrag der Fachlichen Leitstelle für diesen Testlauf lag nicht vor. Mit dieser Vorgehensweise wurde massiv gegen die datenschutzrechtlichen Anforderungen an Testverfahren verstoßen:

- Für das SAP-Zahlverfahren wurde kein Testdatenbestand generiert und gepflegt, obwohl dies für den Test eines Verfahrens erforderlich und in der Freigaberichtlinie festgeschrieben ist. Dort heißt es unter Ziffer 5.1.3: „Software und DV-Verfahren sind mit systematisch entwickelten Fallkonstellationen (Testdaten) nach einem vorgegebenen Testplan, aus dem das gewünschte Ergebnis hervorgeht, zu überprüfen.“ Tests mit Originaldaten sind nur ergänzend unter den in Ziffer 5.1.4 festgeschriebenen Voraussetzungen zulässig, die nicht gegeben waren.
- Für den Test wurde ein früherer Produktionsdatenbestand verwendet, obwohl dies nach den Bestimmungen über die Auftragsdatenverarbeitung gem. § 3 Abs. 1 HmbDSG nicht zulässig war.
- Die als Testdaten genutzten früheren Produktionsdaten befanden sich seit Januar 2005 auf dem Test-Fileserver. Selbst wenn die Erstellung der Kopie zum damaligen Zeitpunkt zulässig gewesen wäre, hätte die Kopie unmittelbar nach der Nutzung zu Testwecken gelöscht werden müssen. Die unverzügliche Löschung nach dem Test 2005 war jedoch unterblieben.

Diese gravierenden Verstöße gegen die datenschutzrechtlichen Vorschriften wurden vom Hamburgischen Datenschutzbeauftragten beanstandet.

Dataport hat den Vorfall in einem internen Bericht systematisch aufgearbeitet. In Abstimmung mit dem HmbDSB sind technische und organisatorische Maßnahmen vorgesehen, die gewährleisten sollen, dass derartige Verstöße zukünftig verhindert werden. Dazu gehören:

- Aufbau eines Testdatenbestandes,
- ein Test mit Originaldaten wird nur durchgeführt, wenn die Anforderungen der Freigabe-Richtlinie erfüllt werden; dies wird revisionssicher dokumentiert,
- die Umsetzung des Berechtigungs- und Zugriffskonzepte für die genutzten Systeme und das SAP-Verfahren werden geprüft und erforderliche Anpassungen vorgenommen.

Obwohl die Forderungen zusätzlicher technischer und organisatorischer Maßnahmen von Dataport anerkannt sind, bleibt zum Redaktionsschluss dieses Tätigkeitsberichts festzustellen, dass nach wie vor kein anonymisierter Datenbestand existiert und die Revision des Zugangs- und Berechtigungssystems noch nicht abgeschlossen ist. Dabei belegt die Auszahlung von über 3 Mio. Euro, die nur aufgrund günstiger Umstände vollständig zurückgerufen werden konnte, welche gravierenden Schäden durch die hier aufgezeigten Verstöße entstehen können.

Da die datenschutzrechtlichen Anforderungen beim Testen auch bei anderen Fachverfahren wie z.B. bei der Öffentlichen Rechtsauskunfts- und Vergleichsstelle (ÖRA) und beim Verfahren zur Bearbeitung von Verkehrsordnungswidrigkeiten sowie im Zuge der Fusion der Landesunfallkasse Hamburg nicht konsequent eingehalten wurden, wird der HmbDSB auch in Zukunft Tests mit Originaldaten kritisch prüfen.

2.4 Dokumentenverwaltung ELDORADO

Der Umstieg auf die elektronische Dokumentenverwaltung erfordert eine intensive Auseinandersetzung mit den bisherigen Prozessen zur Aktenführung, um die Schutzwürdigkeit personenbezogener Akteninhalte in jeder Verarbeitungsphase des elektronischen Verfahrens angemessen berücksichtigen zu können.

Mit der Vereinbarung nach § 94 HmbPersVG über die Einführung der elektronischen Dokumentenverwaltung sowie der IT-Richtlinie ELDORADO wurden für die Behörden und Ämter verbindliche und einheitliche Vorgaben für die Einrichtung von ELDORADO-Verfahren geschaffen. Im Berichtzeitraum wurde zudem mit der Finanzbehörde eine Risikoanalyse für das bei Dataport betriebene Verfahren ELDORADO abgestimmt. Der Anwendungsbereich dieser Risikoanalyse umfasst jedoch nicht Verfahren, in denen Akten geführt werden, für die besondere datenschutzrechtliche oder sonstige gesetzliche Anforderungen gelten.

Diese Verfahren müssen von den jeweiligen Behörden und verantwortlichen Stellen gesondert betrachtet und es müssen ggf. ergänzende Schutzmaßnahmen getroffen werden.

Die zentrale technische Bereitstellung des Dokumentenverwaltungssystems entbindet die für die Datenverarbeitung verantwortlichen Stellen (§ 4 Abs. 3 HmbDSG) somit nicht von ihrer datenschutzrechtlichen Verantwortung. Vor der Entscheidung über die Einführung des Verfahrens und die Aufnahme von Akten in die ELDORADO- Aktenverwaltung ist eine Analyse der in den Akten enthaltenen personenbezogenen Daten erforderlich.

Erst auf dieser Basis kann geprüft werden, ob und unter welchen Voraussetzungen Akten digital verarbeitet werden können.

Die Ermittlung und Kenntnis der Akteninhalte und ihre Zuordnung zu Schutzbedarfsstufen ist zudem Voraussetzung für die Erstellung eines datenschutzgerechten Zugriffskonzeptes.

Die Verantwortlichkeiten und Berechtigungen für das Verfahren sowie der Zugriff auf die Anwendung und Daten müssen von der verantwortlichen Daten verarbeitenden Stelle festgelegt und entsprechend der IT-Richtlinie ELDORADO revisionssicher protokolliert werden.

Eine revisionssichere Protokollierung umfasst neben der Erstellung eines Zugriffskonzeptes und der Dokumentation der personenbezogenen Zuordnung von Benutzerkennungen auch die Protokollierung der Einrichtung von Berechtigungen sowie jeder Änderung von Berechtigungsprofilen im System. Eine entsprechend von uns geforderte systemseitige Protokollierung wird geschaffen.

Personenbezogene Daten sind von der Daten verarbeitenden Stelle grundsätzlich zu löschen, wenn ihre Speicherung unzulässig oder ihre Kenntnis für die Daten verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich ist (§ 19 Abs. 3 HmbDSG). Archivwürdige Unterlagen bilden hier eine – im Hamburgischen Archivgesetz gesondert geregelte – Ausnahme.

Nach dem Hamburgischen Archivgesetz sind nicht mehr benötigte Unterlagen fortlaufend auszusondern und dem Staatsarchiv anzubieten. Das entsprechende Aussonderungsverfahren zur Anbietungspflicht beinhaltet somit regelmäßig eine Erforderlichkeitsprüfung (Erforderlichkeit für die Aufgabenfüllung, Archivierungsfristen etc.). Daher sind nicht nur die Dokumente aus den Verfahren der Behörden und Ämter zu löschen, die als archivwürdig bewertet und abgeliefert wurden. Dies gilt vielmehr insbesondere auch für die personenbezogenen Unterlagen, für welche die Archivwürdigkeit verneint wurde. Diese sind gem. § 19 Abs. 3 HmbDSG aus den Verfahren der Behörden und Ämter zu löschen.

Da eine weitere Speicherung in diesen Fällen datenschutzrechtlich unzulässig wäre, muss bei der Aufnahme von Unterlagen in die elektronische Dokumentenverwaltung gewährleistet sein, dass personenbezogene Daten, die für die verarbeitende Stelle zur Erfüllung ihrer Aufgaben nicht mehr erforderlich sind – unter Berücksichtigung der Anbietungspflicht gegenüber dem Staatsarchiv – datenschutzgerecht gelöscht werden können und gelöscht werden. Aussonderung und Löschung sollen künftig durch den Einsatz eines Aussonderungsmoduls und den Umstieg auf neue Speichermedien unterstützt werden. Wir werden uns für eine datenschutzgerechte Umsetzung einsetzen.

2.5 Verschlüsselte E-Mails in der hamburgischen Verwaltung

Sensible Daten werden jetzt auch bei der Staatsanwaltschaft verschlüsselt per Mail versandt. Viele behördliche Arbeitsplätze, an denen sensible Daten ver-

arbeitet werden, sind jedoch immer noch nicht mit der Erweiterten Sicherheit ausgestattet.

Der Hamburgische Datenschutzbeauftragte hat wiederholt darauf hingewiesen, dass sensible personenbezogene Daten nur verschlüsselt vermailt werden dürfen. Dies ist in der §94er-Vereinbarung „Bürokommunikation" verbindlich festgeschrieben. Dort ist gleichzeitig die allgemeine Regel enthalten, dass bei der schriftlichen Kommunikation bevorzugt E-Mail genutzt wird. Die Ausstattung an den Arbeitsplätzen lässt eine Verschlüsselung aber noch nicht flächendeckend zu.

Zwar gibt es einzelne Bereiche, die im Berichtszeitraum die Zahl der Arbeitsplätze, die mit der „Erweiterten Sicherheit" ausgestattet sind, deutlich erhöht haben. Aufgrund unserer Bemühungen wurde nach langer Erörterung etwa die Staatsanwaltschaft mit den erforderlichen Zertifikaten ausgestattet, so dass die hochsensiblen Daten im Verfahren „Berichtswesen in Strafsachen" nunmehr verschlüsselt versendet werden (vgl. 20. TB. 1.6). Insgesamt stagniert jedoch die Anzahl der erteilten Zertifikate, so dass lediglich ca. 15 % der FHHinfoNET-Nutzer verschlüsselt mailen können. Das entspricht einem Anteil von ca. 1/3 der Arbeitsplätze, an denen sensible personenbezogene Daten verarbeitet werden.

Vor dem Hintergrund, dass der Senat in seinem E-Government-Strategiebericht 2007/2008 (vgl. Drucksache 18/6908) zu Recht davon ausgeht, dass E-Mail und andere IT-Anwendungen heute fester Bestandteil fast aller Bereiche des Lebens geworden sind und die wirtschaftliche Entwicklung einer Region oder einer Stadt insgesamt von deren IT-Durchdringung abhängt, ist es nicht nachvollziehbar, warum im Berichtszeitraum die Anzahl der Zertifikate für die Erweiterte Sicherheit nicht deutlich erhöht wurde. Trotz der Ankündigung der Senatsvertreter im Unterausschuss Datenschutz der Bürgerschaft Anfang 2007, dass nun sukzessive weitere Arbeitsplätze mit den Sicherheitsmaßnahmen ausgestattet würden, ist hier kein wesentlicher Fortschritt zu verzeichnen.

Der Bedarf, verschlüsselt zu mailen, kann dabei zum einen durch die sensiblen personenbezogenen Daten entstehen, die bei der Bewältigung der Fachaufgabe verarbeitet werden. Zum anderen entsteht der Bedarf auch durch die Anforderung, dass die Mitarbeiter in eigener Angelegenheit etwa mit ihrer Personalabteilung bzw. dem Zentrum für Personaldienste elektronisch kommunizieren oder aber die Kommunikation mit dem Vorgesetzten z.B. im Rahmen des Beurteilungsverfahrens zum Teil elektronisch abläuft. In der Regel sollten daher alle ESARI-Arbeitsplätze mit der Erweiterten Sicherheit ausgestattet werden, da zukünftig bei fast allen PC-Arbeitsplätzen der FHH der Bedarf an einer verschlüsselten Mail-Kommunikation besteht. Nur wenn die Mitarbeiter auch tatsächlich die Möglichkeit der verschlüsselten Kommunikation haben, können sie ihre Verantwortung sachgerecht wahrnehmen.

2.6 Prüfung des FHH-Netzes

Eine Überprüfung der Sicherheit des FHH-Netzes hat gravierende Mängel administrativer und konzeptioneller Art aufgezeigt. Erste Maßnahmen wurden durch Dataport getroffen, strukturelle Konsequenzen müssen folgen.

Die Datenverarbeitungs-Infrastruktur der Freien und Hansestadt Hamburg war bereits häufig Gegenstand unserer Tätigkeitsberichte (zuletzt 20. TB, 1.6 und 19. TB, 3.4 und 3.6). Unsere dabei vorgebrachte Kritik an dem Umgang mit IT-Sicherheit und die damit verbundenen Verbesserungsvorschläge stießen dabei regelmäßig auf eine Abwehrhaltung seitens der Finanzbehörde. Diese Position wurde unter anderem mit dem Hinweis untermauert, dass es in der Vergangenheit keine Sicherheitsvorfälle gegeben habe und daher die bereits getroffenen Maßnahmen offenbar ausreichend seien.

Vor dem Hintergrund dieser Auseinandersetzungen haben wir eine systematische Untersuchung der tatsächlich im FHH-Netz getroffenen Sicherheitsmaßnahmen durchgeführt. Die Prüfung sollte Antworten auf zwei Fragenbereiche geben:

- Wie gut sind die Daten und Infrastrukturen der verschiedenen Behörden voneinander abgeschottet bzw. wie wirksam sind die getroffenen Maßnahmen?
- Werden unregelmäßige bzw. unzuständige Zugriffe und Sicherheitsverletzungen überhaupt bemerkt?

Um den Feststellungen eine möglichst umfassende Aussagekraft zu verleihen, wurde die Prüfung von einem Standard-ESARI-Gerät aus durchgeführt, das wie alle anderen PCs in das lokale Netz beim Hamburgischen Datenschutzbeauftragten eingebunden war. Das verwendete Benutzerkonto war mit keinen besonderen Privilegien ausgestattet.

Dennoch gelang es unter Verwendung von frei verfügbaren Software-Werkzeugen, von dort aus eine Vielzahl von Ressourcen in anderen Teilen des FHH-Netzes zu identifizieren und auf dort gespeicherte Inhalte zuzugreifen. Dazu gehörten auch erhebliche Mengen sensibler personenbezogener Daten. Wir haben aus datenschutzrechtlicher Sicht folgende Maßnahmen gefordert, um die Mängel zu beheben und die damit verbundenen Risiken für die verarbeiteten personenbezogenen Daten zu reduzieren:

- Dateien bzw. Freigaben müssen von ihren Zugriffsrechten her auf die erforderlichen Nutzer bzw. Gruppen beschränkt werden.
- Informationen, die nicht für die Allgemeinheit zugänglich sein sollen, müssen gegen unberechtigte Kenntnisnahme geschützt sein.
- Passwörter dürfen nicht im Klartext auf Datenträgern gespeichert werden.
- Standard-Passwörter und -kennungen müssen nach Installation eines Systems auf individuelle Werte verändert werden.

- Drucker und andere vergleichbare Geräte (Scanner, Faxgeräte), die im Netzwerk eingebunden sind, sind gegen Missbrauch zu sichern.
- Die Router-Filterung muss enger ausgelegt werden.
- Es sind wirksame technische und organisatorische Mechanismen zu implementieren, die gewährleisten, dass außergewöhnliche Vorkommnisse im Netzwerk oder auf Servern erkannt und aufgeklärt werden.
- Die Empfehlungen des Secorvo-Gutachtens (lokale Firewall, Terminal-Server) sind umgehend umzusetzen, um die Risiken externer Zugriffe zu begrenzen.
- Das FHH-Netz ist in Hinblick auf die Trennung der verschiedenen speichernden Stellen sowohl innerhalb als auch außerhalb der FHH zu rekonzipieren.
- Das Passwort für die lokale Administration darf nicht ermittelbar sein.
- Der Betrieb von ftp-Servern mit anonymer Zugangsmöglichkeit ist auf die erforderlichen Fälle zu begrenzen.
- Den Benutzern sollte ein einfach zu bedienendes Werkzeug zur Verfügung gestellt werden, mit denen Passwörter oder andere Zugangsdaten sicher verwaltet werden können.
- Sämtliche DNS-Server im FHH-Netz sollten so konfiguriert werden, dass keine unautorisierten Zone Transfers möglich sind.

Die Finanzbehörde und Dataport haben unsere Feststellungen und Forderungen anerkannt und eine Reihe von Sofortmaßnahmen ergriffen, um immanente Sicherheitslücken zu schließen. Darüber hinaus sind jedoch auch strukturelle Änderungen erforderlich, um eine dauerhafte und nachhaltige Verbesserung der Sicherheit zu erreichen. Hierzu gehört eine Orientierung auf das Grundschutzkonzept des BSI (siehe 2.10), sowohl für die FHH als auch für Dataport. Ein solcher Schritt wird dazu beitragen, das Vertrauen in das sichere Funktionieren des FHH-Netzes auf eine nachprüfbare Basis zu stellen.

Zudem ist die konsequente und rasche Umsetzung des Projekts „Zentralarchitektur für Basisinfrastruktur“ (ZaBi) bei Dataport erforderlich. Detaillierte Informationen über dieses Projekt sind uns zugesagt worden.

2.7 Übergabe des IuK-Netzes der Polizei an Dataport

Die Polizei Hamburg übergibt seit 2005 sukzessive ihr selbst betriebenes Netzwerk für die eingesetzte PC-Hardware an den IT-Dienstleister Dataport, ohne den datenschutzrechtlichen Anforderungen zu entsprechen. Es bestehen erhebliche Bedenken, ob die derzeitigen Datenschutz- und Datensicherheitsstandards des Dienstleisters ausreichen, den Schutzbedarf für das Polizeinetz zu gewährleisten.

Bereits 2005 wurde von der Polizei Hamburg, der Finanzbehörde und Dataport der Beschluss gefasst, das Polizeinetz von der Polizei zu Dataport zu verlagern. Eine rechtzeitige Beteiligung des Hamburgischen Datenschutzbeauftragten wäre erforderlich gewesen. Die Absicht der Übergabe des Polizeinetzes an Dataport wurde dem Hamburgischen Datenschutzbeauftragten aber erst 2007 zufällig bekannt. Wir erhielten dann auf unsere Nachfrage im Juli 2007 von der Polizei dazu mündliche Informationen und erst seitdem wurde in den zahlreichen Datei-Errichtungsanordnungen, die nach dem Gesetz über die Datenverarbeitung der Polizei auch dem Hamburgischen Datenschutzbeauftragten vorzulegen sind, der Standort des Servers bei Dataport ausgewiesen. Dabei ist nicht nur die unterlassene Korrektur des Serverstandorts zu bemängeln. Vielmehr hätte die Polizei nach dem Hamburgischen Datenschutzgesetz bereits vor der mit einer Verlagerung verbundenen wesentlichen Änderung der automatisierten Verfahren Vorabkontrollen, sog. Risikoanalysen, durchführen und dem Hamburgischen Datenschutzbeauftragten vorlegen müssen. Daneben war für die verlagerten Anwendungen die Verfahrensbeschreibung zu ändern, in der die technischen und organisatorischen Maßnahmen zur Beherrschung der festgestellten Gefahren festzulegen sind. Die Datenbank des Verfahrens CRIME war bereits im Oktober 2005 zu Dataport verlagert worden, aber erst im Dezember 2007 wurde für dieses Verfahren aus anderem Anlass die Risikoanalyse und die Verfahrensbeschreibung überarbeitet. Für andere Anwendungen liegen bislang keine geänderten Risikoanalysen und Verfahrensbeschreibungen vor.

Die Ergebnisse der Prüfung des Behörden-Computernetzes (siehe 2.6) sowie der Abschlußbericht zum Basissicherheitscheck FHH-Netz (siehe 2.10) machen deutlich, dass der Übergang des separaten Polizeinetzes in das von Dataport betriebene länderübergreifende, nur schwach segmentierte Netz mit hohen Risiken behaftet sein kann. Im Abschlußbericht zum Basissicherheitscheck heißt es: „Darüber hinaus ist das FHH-Netz nicht grundschutzkonform, so dass die polizeiliche Datenverarbeitung die Anforderungen der derzeit geltenden Polizeirichtlinien nicht erfüllt."

Die Übernahme des Polizeinetzes sehen wir nach diesen Ergebnissen kritisch.

Die möglichen Vorteile einer Netzübergabe wären sorgfältig mit den hohen Anforderungen des Datenschutzes und der Datensicherheit im Bereich der Polizei abzuwägen gewesen. Die Polizei Hamburg ist verpflichtet, den Hamburgischen Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben zu unterstützen; diese Unterstützung umfasst insbesondere die Auskunft zu Fragen und Einsicht in alle Unterlagen. Aber weder konnten uns Dokumente über den erforderlichen Abwägungsprozess vorgelegt, noch konnte er uns sonst nachvollziehbar erläutert werden. Es ist uns nicht verständlich, wie die Entscheidung über eine Weichenstellung dieses Ausmaßes ohne vorherige systematische Abwägung getroffen werden konnte.

Wir erwarten, dass die Polizei Hamburg die laufende Diskussion über eine Neuausrichtung der strategischen Sicherheitskonzeption des FHH-Netzes nutzt, ihre spezifischen Sicherheitsanforderungen durchzusetzen, so dass die Verlagerung des Polizeinetzes doch noch mit einem positiven Ergebnis vollzogen werden kann.

2.8 FHHPortal – Vertrauliche Informationen offen zugänglich !?

Um die Zusammenarbeit innerhalb der Verwaltung technisch besser unterstützen zu können, hat die Finanzbehörde das Projekt FHHPortal aufgelegt. Zugriffsberechtigungen sind so unübersichtlich, dass alle Intranet-Benutzern sogar vertrauliche Informationen mit einem Klick einsehen konnten.

Viele Dokumente entstehen arbeitsteilig. Dazu gehört auch, dass Veränderungen an den Versionen zu Konzepten und Teilergebnissen verfolgt und bewertet werden müssen. Besprechungen müssen terminiert und die erforderlichen Unterlagen bereitgestellt werden. Um diesen Prozess zu verbessern, hat die Finanzbehörde die bisherige Bürofunktionalität um dass „FHH-Portal“ erweitert. Auf der Basis der Microsoft SharePointPortal-Technologie wurde diese Unterstützung realisiert und für die Nutzung in der hamburgischen Verwaltung freigegeben.

Zum Schutz der Vertraulichkeit und Akzeptanz ist dabei von besonderer Bedeutung, dass nur die jeweils berechtigten Nutzer die bereitgestellten Informationen einsehen können. Zwar können die Zugriffsrechte sehr differenziert vergeben werden. Doch wer im Ergebnis wirklich Zugriff erhält, ist für den Nutzer kaum transparent. Dadurch entstehen gerade zu Nutzungsbeginn sowie bei gelegentlicher Nutzung schnell Fehler, die dazu führen können, dass selbst Dokumente mit sensiblen Inhalten für alle Intranet-Nutzer zugänglich gemacht werden. So wurden einzelne Dokumente erst nach direkten Hinweisen des HmbDSB vor unberechtigter Nutzung geschützt. Es ist daher zwingend geboten, die Nutzer generell in die Lage zu versetzen, dass die gut gemeinten Instrumente auch datenschutzgerecht genutzt werden. Hierzu hat der HmbDSB konkrete Ansatzpunkte aufgezeigt:

- Default-Einstellungen sollten so vorgenommen werden, dass die Zugriffsberechtigungen für neue Dokumente und Seiten nicht automatisch vererbt werden, sondern die erforderlichen Zugriffsberechtigungen bewusst vergeben werden.
- Ein Ersteller neuer Seiten und Dokumente sollte sich eine Übersicht anzeigen lassen können, welche Personen aufgrund der gewählten Einstellungen Zugriffsberechtigungen haben.
- Arbeitsplatzwechsel, die geänderte Zugriffsberechtigungen zur Folge haben, müssen technisch so unterstützt werden, dass nicht der jeweilige

Besitzer der Dokumente bzw. Seiten derartige personelle Veränderungen im Blick haben muss.

- Wenn verschiedene Daten verarbeitende Stellen gemeinsame Dateien nutzen, sind sowohl die rechtlichen Voraussetzungen nach § 11a HmbDSG als auch die erforderlichen technischen und organisatorischen Maßnahmen wie u.a. eine Protokollierung der Abrufe zu schaffen.

Vor einer weiteren Ausweitung der produktiven Nutzung, insbesondere bei der Verwendung sensibler personenbezogener Daten, ist es dringend geboten, die noch ausstehende Projektarbeit nachzuholen und vor dem flächendeckenden Einsatz eine entsprechende Ergänzung bzw. Konfiguration vorzunehmen. Das FHH-Portal sollte nicht erst beim Kunden reifen, sondern die Freigabe sollte diese Reife gerade belegen.

2.9 Passwort Self Service

Im Rahmen der weiteren Zentralisierung der IT-Administration führte die Finanzbehörde 2007 für die standardisierten Bildschirmarbeitsplätze der Behörden den Passwort Self Service ein.

Bis vor kurzem konnte sich ein PC-Nutzer, der sein Passwort vergessen hatte oder dessen Account nach 5 Fehleingaben automatisch gesperrt wurde, an seinen lokalen Administrator wenden, der ein neues Passwort vergab, das der Nutzer bei seiner ersten Anmeldung am eigenen PC durch ein eigenes Passwort ersetzen musste. Im Zuge der Zentralisierung der IT-Administration bei Dataport sind die Stellenanteile der Behörden für die lokale IT-Administration weitgehend gestrichen bzw. gekürzt worden. Um dennoch eine Identifizierung des Nutzers und damit eine berechtigte Passwort-Rücksetzung sicherzustellen, wurde der Passwort Self Service (PSS) eingeführt. Das Verfahren ermöglicht es einem Nutzer, über eine Web-Anwendung im Intranet der FHH sein Passwort selbst zurückzusetzen, sofern er sich zuvor für dieses Verfahren angemeldet hat. Dabei hat er von 10 Fragen mit teilweise trivialem Charakter („Geburtsname der Mutter“) 3 Fragen zu beantworten. Die Antworten werden einwegverschlüsselt gespeichert. Sofern nun für den Nutzer der Bedarf entsteht, sein Passwort zurückzusetzen, muss er sich an einen Kollegen aus dem eigenen Arbeitsbereich wenden und an dessen PC den Passwort Self Service aufrufen. Nach korrekter Beantwortung der ausgewählten Fragen kann der Nutzer dann ein neues Passwort für seinen eigenen PC eingeben.

Im Rahmen der Abstimmungsgespräche mit der Finanzbehörde haben wir, neben weiteren Forderungen, auch Wert darauf gelegt, dass dieses – am fremden Arbeitsplatz – erstellte Passwort nur einen Übergangscharakter haben kann, da ein Ausspähen nicht ausgeschlossen werden kann. Es ist umgehend am eigenen PC durch ein neues Passwort zu ersetzen. Wichtig war uns auch, dass die Nutzung des PSS nur innerhalb der eigenen Organisationseinheit

möglich ist. Nach wie vor halten wir eine Ausweitung des Fragenkatalogs und die Definition von individuellen Fragen durch den Nutzer für wünschenswert.

2.10 Basissicherheitscheck des FHH-Netzes

Ein unabhängiges Gutachten hat sich mit der Sicherheit des FHH-Netzes vor dem Hintergrund anerkannter Standards befasst. Darin werden erhebliche Defizite benannt und eine Neuausrichtung der strategischen Sicherheitskonzeption empfohlen.

Im Auftrag der Finanzbehörde hat das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) im Herbst 2007 eine interne Auditierung der Sicherheit des FHH-Netzes durchgeführt. Dieser Beauftragung waren langjährige Diskussionen zwischen dem Hamburgischen Datenschutzbeauftragten und der Finanzbehörde über die Frage vorausgegangen, welches Sicherheitsniveau das FHH-Netz bietet. Während die Finanzbehörde argumentierte, dass das Netz aufgrund seines einheitlichen Betriebs durch Dataport und seiner guten Außensicherung als insgesamt sicher gelten könne, haben wir auf Defizite im Bereich des Sicherheitsmanagements, der inneren Segmentierung und der Transparenz verwiesen und zusätzliche Sicherheitsmaßnahmen gefordert, etwa zum verschlüsselten Versand von E-Mails (vgl. 20. TB, 1.6).

Mit der Erstellung des Audits war daher das Ziel verbunden, eine abschließende Grundlage für weitergehende Empfehlungen zu schaffen, die sowohl von der Finanzbehörde als auch vom Hamburgischen Datenschutzbeauftragten anerkannt wird.

Das Gutachten ist als internes Audit in der Form eines Basis-Sicherheitschecks erstellt worden. Im Rahmen der IT-Grundschutz-Konzepte des Bundesamts für Sicherheit in der Informationstechnik (BSI) muss geprüft werden, welche Standard-Sicherheitsmaßnahmen bereits umgesetzt sind und wo noch Defizite bestehen. Hierzu werden Interviews mit den Verantwortlichen und stichprobenartige Kontrollen durchgeführt. Dies wird als Basis-Sicherheitscheck bezeichnet. Das Gutachten dokumentiert zum einen den bereits erreichten Stand der Sicherheit im FHH-Netz und listet zum anderen die Abweichungen von den Standardvorgaben des IT-Grundschutzes sowie daran anknüpfende Empfehlungen auf.

Die wesentlichen Aussagen des Audits lauten (Auszug):

- Zahlreiche relevante Standardsicherheitsmaßnahmen insbesondere im Firewall-System und dem zentralen Verzeichnisdienst ActiveDirectory sind bereits umgesetzt.
- Die vorhandene technische Infrastruktur des FHH-Netzes bietet eine gute Grundlage, um weitere nach dem Stand der Technik erforderliche Sicherheitsmaßnahmen umzusetzen.

- Die eingesetzte Methode zur Risikoanalyse stellt nicht sicher, dass Risiken umfassend und mit Maßnahmen vergleichbarer Stärke behandelt werden, so dass wesentliche Sicherheitsmaßnahmen nicht betrachtet und umgesetzt werden.
- Die Umsetzung der festgelegten Sicherheitsmaßnahmen wird nicht sichergestellt – Protokollkonzeption, Protokollierung und Protokollrevision sowie Auditierung und IT-Revision fehlen entweder vollständig oder sind unzureichend.
- Festgelegte Sicherheitsmaßnahmen sind nicht ausreichend transparent.
- Für die Netzinfrastruktur des FHH-Netzes fehlt es an einer einheitlichen Zuständigkeit für die Konzeption und Umsetzung der festgelegten Sicherheitsmaßnahmen, so dass die Umsetzung des geplanten Sicherheitsniveaus gefährdet ist.
- Die logische Segmentierung des FHH-Netzes ist angesichts der Zahl der angeschlossenen Nutzer und Systeme in Teilen unzureichend.
- Technische Standardsicherheitsmaßnahmen sind teilweise nicht umgesetzt.
- Die Mängel führen dazu, dass das FHH-Netz durch Innentäter oder menschliche Fehlhandlungen hochgradig verwundbar ist. Die gefundenen technischen Sicherheitslücken können darüber hinaus für Angriffe von Außen auf den im Rahmen eines anderen Sicherheitsgutachtens bereits 2006 aufgezeigten Wegen genutzt werden.

Das Audit befasst sich auch mit dem Prozess der Integration des Netzes der Polizei in das FHH-Netz (siehe 2.7). Es kommt dabei zu dem Schluss, dass die bislang eingesetzte Verschlüsselung wegfallen wird, ohne dass es zugleich ein Konzept für ihre Wiedereinführung gibt. Dadurch wird zum einen die Sicherheit der polizeilichen Datenverarbeitung abgesenkt und zum anderen das Erreichen des insbesondere in diesem Bereich erforderlichen Grundschutzniveaus erschwert.

Entsprechend der Vereinbarung mit der Finanzbehörde, das Gutachten als gemeinsame Grundlage für die künftige Bewertung der Sicherheit im FHH-Netz zu verwenden, sehen wir weiteren Handlungsbedarf. Das Gutachten ist ein guter Ausgangspunkt für den Eintritt der FHH in ein modernes Sicherheitsmanagement, das anerkannten Standards entspricht. Die BSI-Grundschutz-Konzeption bietet sich hierfür in besonderer Weise an. Auf diesem Weg werden wir die Finanzbehörde nach Kräften unterstützen.

2.11 Online-Durchsuchung

Die Datenschutzbeauftragten bekräftigen ihre ablehnende Haltung zu Online-Durchsuchungen. Bedenken bestehen sowohl in verfassungsrechtlicher als auch in technischer Hinsicht.

Die Konferenz der Datenschutzbeauftragten der Länder und des Bundes hat sich in zwei Beschlüssen kritisch zu den Plänen staatlicher Zugriffe auf private Computer geäußert (der Beschluss vom Oktober 2007 ist in Auszügen wiedergegeben).

Neben den erheblichen verfassungsrechtlichen Problemen hätte ein solches Instrument auch aus technischer Sicht fatale Folgen. Während es einerseits öffentliche Aufgabe ist, die Sicherheit in der Informationstechnik zu fördern – hierfür ist auf Bundesebene vorrangig das Bundesamt für Sicherheit in der Informationstechnik (BSI) zuständig –, entsteht im Zusammenhang mit Online-Durchsuchungen ein staatliches Eigeninteresse an Sicherheitslücken, die sich für diesen Zweck ausnutzen lassen. Für das allgemeine Vertrauen in die IT-Sicherheit einerseits und das Sicherheitsniveau andererseits hätte dies erhebliche negative Auswirkungen.

Besonders alarmierend sind in diesem Zusammenhang Ideen, die für die Online-Durchsuchung erforderliche Software als Bestandteil der Kommunikation des Bürgers mit staatlichen Stellen im Rahmen des E-Government zu platzieren. Den gemeinsamen Anstrengungen der Verwaltungen und der Datenschutzbeauftragten für sichere, vertrauenswürdige E-Government-Lösungen (siehe 2.1) ist mit solchen Vorschlägen wohl kaum gedient.

Nein zur Online-Durchsuchung

Der Computer hat im täglichen Leben der meisten Menschen eine zentrale Bedeutung für die Aufbewahrung und Gestaltung privatester Informationen, wie Fotografien, Reiseberichte, Tagebuchaufzeichnungen, persönliche Briefe, Eindrücke, Vorstellungen und Gefühle. Die heimliche Online-Durchsuchung führt deshalb zu erheblichen Eingriffen in Grundrechte (informationelles Selbstbestimmungsrecht, Unverletzlichkeit der Wohnung, Telekommunikationsgeheimnis usw.). Die Installation von Überwachungssoftware etwa mit Hilfe des Internets oder die Versendung von E-Mails unter dem Namen einer anderen Behörde wird erwogen, sogar das unbemerkte Eindringen in Wohnungen zu diesem Zweck wird nicht ausgeschlossen.

Es steht fest, dass sich der unantastbare Kernbereich privater Lebensgestaltung bei Online-Durchsuchungen durch technische Mittel bei der Datenerhebung nicht schützen lässt. Ein automatisierter Kernbereichsschutz ist somit nicht realisierbar.

Derzeit wird zwar versichert, dass der Einsatz nur auf die Bekämpfung des Terrorismus sowie die Verfolgung schwerster Straftaten und insgesamt auf wenige Fälle beschränkt wird. Die Erfahrungen zeigen aber, dass solche Beschränkungen nicht von langer Dauer sein werden.

Zudem ist davon auszugehen, dass Terrorverdächtige Mittel und Wege finden werden, durch geeignete Gegenmaßnahmen eine erfolgreiche Online-Durchsuchung zu verhindern. Die heimliche Online-Durchsuchung führt deshalb voraussichtlich nicht zu mehr Sicherheit, aber sicher zur Einschränkung der Freiheit.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen daher ihre im Rahmen der 73. Konferenz im März 2007 erhobene Forderung an die Bundesregierung, die Landesregierungen und die Parlamente, auf die Einführung der repressiven und präventiven Online-Durchsuchung zu verzichten.

DATENSCHUTZ IM ÖFFENTLICHEN BEREICH

3. Behördliche Datenschutzbeauftragte

Da insbesondere die Fachbehörden es weiterhin unterlassen, behördliche Datenschutzbeauftragte zu bestellen, muss das Hamburgische Datenschutzgesetz dahingehend geändert werden, dass die Bestellung von behördlichen Datenschutzbeauftragten auch in Hamburg zur Pflicht wird.

Behördliche Datenschutzbeauftragte üben eine wichtige Funktion bei der Durchsetzung und Verbesserung des Datenschutzes in den Behörden aus. Zu ihren Aufgaben gehört es insbesondere, auf die Umsetzung und Einhaltung der Vorschriften über den Datenschutz hinzuwirken, die erforderlichen Verfahrensbeschreibungen zu führen und die von den Behörden vor der Einführung von automatisierten Datenverarbeitungsprozessen zu erstellenden Risikoanalysen zu prüfen.

Leider ist die geltende Vorschrift zur Bestellung behördlicher Datenschutzbeauftragter im Hamburgischen Datenschutzgesetz (§ 10a Absatz 1 Satz 1) nur eine Kann-Vorschrift mit der Folge, dass von den Senatsämtern und Fachbehörden bisher lediglich das Personalamt und die Behörde für Stadtentwicklung und Umwelt einen behördlichen Datenschutzbeauftragten bestellt haben.

Zur Stärkung der datenschutzrechtlichen Eigenverantwortlichkeit der Behörden sollte die Bestellung von behördlichen Datenschutzbeauftragten auch in Hamburg verpflichtend sein. Eine solche Verpflichtung zur Bestellung behördlicher Datenschutzbeauftragter besteht bereits für alle Bundesbehörden und die Behörden der Länder Bayern, Berlin, Brandenburg, Bremen, Hessen, Mecklenburg-Vorpommern, Niedersachsen, Nordrhein-Westfalen, Rheinland-Pfalz, Sachsen-Anhalt und Thüringen. Nur Baden-Württemberg,

Saarland, Sachen und Schleswig-Holstein haben wie Hamburg lediglich eine Kann-Vorschrift.

Ferner haben der Bund und alle Länder bis auf Hamburg, Brandenburg, Niedersachsen und Sachen-Anhalt in ihren Datenschutzgesetzen vorgeschrieben, dass die behördlichen Datenschutzbeauftragten zur effektiven Wahrnehmung ihrer Aufgaben unmittelbar der Leitung ihrer Behörde zu unterstellen sind. Dies sollte zur Stärkung der Position der behördlichen Datenschutzbeauftragten auch in Hamburg gelten.

Da in den Beratungen des Unterausschusses Datenschutz des Rechtsausschusses der Bürgerschaft deutlich wurde, dass von Seiten des Senats keine Neigung besteht, darauf hinzuwirken, dass weitere behördliche Datenschutzbeauftragte bestellt werden, hat sich der Hamburgische Datenschutzbeauftragte mit Schreiben vom 27. Februar 2007 direkt an die Bürgerschaft gewandt mit der Empfehlung, zur Verbesserung des Datenschutzes in den hamburgischen Behörden das Hamburgische Datenschutzgesetz dahingehend zu ändern, dass alle Behörden und sonstigen öffentlichen Stellen einen behördlichen Datenschutzbeauftragten zu bestellen haben.

§ 10a des Hamburgischen Datenschutzgesetzes sollte wie folgt novelliert werden:

1. § 10a Absatz 1 Satz 1 erhält folgende Fassung:

   „Die in § 2 Absatz 1 Satz 1 genannten Stellen haben eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten zu bestellen."

2. § 10a Absatz 4 Satz 1 erhält folgende Fassung:

   „Die behördlichen Datenschutzbeauftragten sind bei der Erfüllung ihrer Aufgaben unmittelbar der Leitung der Daten verarbeitenden Stelle zu unterstellen."

Leider ist weder vom Senat noch aus der Mitte der Bürgerschaft eine entsprechende Gesetzesvorlage eingebracht worden. Wir hoffen, dass in der nächsten Wahlperiode die erforderliche Gesetzesänderung erfolgt.

4. Personaldaten

4.1 Schutz der Personalakten und Personaldaten beim UKE

Grundlegende datenschutzrechtliche Vorgaben sind nicht eingehalten worden.

Durch verschiedene Hinweise wurden wir auf Defizite bei der Sicherung des Zuganges zu Personalakten aufmerksam. Daraufhin prüften wir bei der Personalabteilung des UKE die Aufbewahrung der Personalakten, die räumliche Unterbringung sowie die Zugangsberechtigungen der Mitarbeiter. Zusätzlich

erfolgte eine Prüfung der Zugriffsberechtigungen des beim UKE eingesetzten Systems SAP R/3 HR und der Vorgaben zur Auftragsdatenverarbeitung. Aufgrund weiterer Beschwerden erweiterten wir die Kontrolle um die Einhaltung der Passwortkonventionen.

Die Prüfung offenbarte Mängel bei der Einhaltung der anzuwendenden Datenschutzgesetze. Dies betraf sowohl das UKE als öffentliche Stelle, das dem Hamburgischen Datenschutzgesetz unterliegt, als auch die dem Bundesdatenschutzgesetz unterliegenden rechtlich selbständigen Töchter des UKE (vgl. 14.2). Weder war zum Zeitpunkt der Prüfung eine Risikoanalyse nach § 8 Abs. 4 HmbDSG noch eine Verfahrensbeschreibung nach § 9 Abs. 1 HmbDSG für das Verfahren der Lohn- und Gehaltsabrechnung mit SAP R/3 HR erstellt. Die von den jeweiligen verantwortlichen Stellen nach § 4g Abs. 2 BDSG der betrieblichen Datenschutzbeauftragten zur Verfügung zu stellenden Übersichten der Verfahren automatisierter Verarbeitungen lagen ebenfalls nicht vor, obwohl die Datenschutzbeauftragte des UKE und der selbständigen Töchter wiederholt auf das Fehlen dieser Unterlagen aufmerksam machte.

Die nach mehr als einem Jahr vorgelegten Verfahrensbeschreibungen und -übersichten entsprachen nicht den datenschutzrechtlichen Anforderungen. Die Datenschutzbeauftragte des UKE und der selbständigen Töchter hat ausführlich die Defizite aufgezeigt, denen wir uns angeschlossen haben.

Die Prüfung ist noch nicht abgeschlossen. Wir werden weiter berichten.

4.2 CLIX – Zentrale Fortbildung

Bei der Seminarverwaltung mit CLIX sind noch nicht alle datenschutzrechtlichen Probleme abschließend geklärt.

Für die Nutzung der Software CLIX zur Seminarverwaltung (vgl. 20. TB 3.3) wurde zwischenzeitlich mit den Spitzenorganisationen der Gewerkschaften eine Vereinbarung nach § 94 HmbPersVG geschlossen. Sie enthält Regelungen zum Datenimport aus dem Hamburg Service Informationssystem (HaSi). Danach ist vorgesehen, die notwendigen Daten regelmäßig zu importieren. Offen ist allerdings, was unter regelmäßig zu verstehen ist. Grundsätzlich dürfen personenbezogene Daten nur verarbeitet werden, soweit sie für die Erfüllung der Aufgabe erforderlich sind. Dies bedeutet, dass die Daten erst zum Zeitpunkt der Fortbildungsanmeldung des betroffenen Beschäftigten importiert werden dürfen. Eine vollständige Übernahme und regelmäßige Aktualisierung aller in HaSi gespeicherten Daten in CLIX ohne konkrete Anmeldung für eine Fortbildungsveranstaltung wäre nicht zulässig.

Die Erörterungen mit dem Personalamt werden fortgesetzt.

5. Statistik

5.1 Schulstatistik

Ein bundesweit einheitliches Schulstatistik-Verfahren setzt voraus, dass datenschutz- und statistikrechtliche Anforderungen erfüllt werden.

Zur vorgesehenen Umstellung der Schulstatistik auf Individualdaten mit bundeseinheitlichem Kerndatensatz (KDS) haben wir erhebliche datenschutzrechtliche Bedenken angemeldet, weil für die Erhebung und Einspeisung der Schüler- und Lehrerdaten aus allen 16 Bundesländern in einer gemeinsamen Statistik-Datenbank erst die landesrechtlichen Rechtsgrundlagen zu schaffen sind (vgl. 20. TB, 4.1).

Dies ist für Hamburg inzwischen im Rahmen der Hamburger Schulrechtsreform geschehen.

So dürfen die staatlichen Schulen und die zuständige Behörde nach § 89 des Hamburgischen Schulgesetzes (HmbSG), geändert durch Gesetz vom 17. Mai 2006 (HmbGVBl. S. 243) i.V.m. § 6 der Schul-Datenschutzverordnung (SchulDSVO) vom 20. Juni 2006 (HmbGVBl. S. 349) alle in §§ 1 und 5 SchulDSVO genannten Daten für Schulstatistiken verarbeiten. Dabei darf ein eindeutiges personenbezogenes Kennzeichen (Schüler-ID) verwendet werden, das eine Verfolgung der schulischen Laufbahn der Schülerinnen und der Schüler unter Einbeziehung ihrer vorschulischen Bildung erlaubt, ohne die Identität zu offenbaren (Pseudonymisierung). Dem Statistischen Amt für Hamburg und Schleswig-Holstein dürfen nur pseudonymisierte Daten zu statistischen Zwecke übermittelt werden.

Damit sind zwar die landesrechtlichen Voraussetzungen für die Erhebung und Übermittlung von Daten zum Zwecke von Schulstatistiken in Hamburg gegeben, hinsichtlich der Einführung des von der Kultusministerkonferenz (KMK) angestrebten bundesweit einheitlichen Schulstatistiksystems besteht jedoch noch datenschutz- und statistikrechtlicher Klärungs- und Regelungsbedarf.

Dazu hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 26./27. Oktober 2006 in ihrer Entschließung „Keine Schülerstatistik ohne Datenschutz“ auf folgende verfassungsrechtliche Vorgaben einer künftigen Schülerstatistik hingewiesen:

- Der Umfang des Erhebungsprogramms ist auf den für die Statistikzwecke dienlichen Umfang zu beschränken.
- Bei allen Festlegungen sind die Grundsätze der Erforderlichkeit und der Verhältnismäßigkeit zu beachten.
- Bei der Datenverarbeitung ist das Gebot der personellen, organisatorischen, räumlichen und verfahrensmäßigen Trennung von Verwaltungsvollzug und Statistik einzuhalten und das Statistikgeheimnis zu gewährleisten.

Anfang Mai 2007 wurde von der Kommission für Statistik der KMK ein „Konzept für die länderübergreifende Weiterverarbeitung und Nutzung der Individualdaten“ erarbeitet. Der Arbeitskreis Statistik der Datenschutzbeauftragten des Bundes und der Länder hat dazu Position bezogen und darauf hingewiesen, dass bei einer amtlichen Statistik insbesondere folgende (einheitliche) Regelungen im Gesetz zu treffen sind:

- Festlegung der Hilfs- und Erhebungsmerkmale,
- Regelungen der Auskunftspflicht,
- Festlegung der technischen und organisatorischen Maßnahmen zur frühestmöglichen Pseudonymisierung/Anonymisierung.

Die Kommission für Statistik der KMK hat dann im Juni 2007 ein modifiziertes „Konzept für die Nutzung von Individualdaten“ erarbeitet, zu dem das Einvernehmen mit der Konferenz der Datenschutzbeauftragten des Bundes und der Länder hergestellt werden sollte.

Dazu hat im August 2007 ein Gespräch zwischen der „Arbeitsgruppe Kerndatensatz/Datengewinnung“ der Kommission für Statistik der KMK und Vertretern der Konferenz der Datenschutzbeauftragten des Bundes und der Ländern stattgefunden. Seitens der KMK wird nun eine gemeinsame Datenhaltung und eine Schüler-ID nicht mehr vorgesehen. Aus Sicht der Datenschutzbeauftragten besteht jedoch weiterhin erheblicher Klärungsbedarf, insbesondere zu folgenden Fragestellungen:

- Endgültige Konzeptvorstellungen,
- Einzelheiten zu temporären Zusammenfassungen der Daten für länderübergreifende Auswertungen,
- Darstellung von Bildungsverläufen im Rahmen von Länderregelungen,
- Präzisierung des Verschlüsselungskonzepts,
- Frage, wer die Daten insoweit auswertet,
- Bewertung der im KDS enthaltenen Daten hinsichtlich ihrer Erforderlichkeit für den Verwaltungsvollzug,
- Festlegung der Erhebungs- und Hilfsmerkmale (dargestellt am Beispiel des Merkmals „Migrationshintergrund“).

Da ein abschließendes Ergebnis noch nicht erzielt werden konnte, sind weitere Gespräche zu führen.

Neben den länderübergreifenden Klärungen besteht bei der Umsetzung in Hamburg noch erheblicher Handlungsbedarf. So haben wir die Behörde für Bildung und Sport u. a. darauf hingewiesen, dass die für Statistik verantwortliche Stelle konkret zu benennen und diese Stelle vom Verwaltungsvollzug abzuschotten ist, ferner ist der Schlüssel für die Pseudonymisierung der Schüler-ID festzulegen.

5.2 Registergestützte Volkszählung (Zensus 2011)

Auch eine registergestützte Volkszählung kann nur unter strikter Einhaltung der datenschutz- und statistikrechtlichen Grundsätze erfolgen.

Die Bundesregierung hat im August 2006 die Grundsatzentscheidung gefällt, dass sich Deutschland an dem für 2011 vorgesehenen EU-weiten Zensus (Volkszählung) mit einem registergestützten Verfahren beteilt. Mit dem Zensus 2011 sollen nicht nur die Daten zur Bevölkerung und deren Erwerbssituation erhoben werden, sondern auch zur Wohnsituation der Menschen. Daher wird auch eine Gebäude- und Wohnungszählung durchgeführt.

Vor dem Hintergrund der Erfahrungen mit der Volkszählung in den 80er Jahren, bei der es einen massiven Widerstand der Bürgerinnen und Bürger gegen die Erfassung ihrer persönlichen Daten durch den Staat gab und der zur Feststellung des Grundrechts auf informationelle Selbstbestimmung durch das Bundesverfassungsgericht im sog. Volkszählungsurteil von 1983 führte, wagt es der Staat heute nicht mehr, Volkszählungsdaten im Wege einer traditionellen Volkszählung durch direkte Befragung aller Einwohner zu erheben. Die benötigten Daten sollen daher durch die Auswertung der Melderegister und anderer Verwaltungsregister gewonnen werden. Lediglich die Daten über Gebäude und Wohnungen werden bei deren Eigentümern postalisch erfragt, weil es darüber keine flächendeckenden Verwaltungsregister gibt. Ergänzende Stichproben sollen mittels Fragebogen erfolgen.

Für die Durchführung des registergestützten Zensus 2011 sind umfangreiche organisatorische Vorbereitungen erforderlich. Grundlage für die vollständige Erfassung der Bevölkerung ist die Ermittlung aller existierenden Gebäude mit Wohnraum einschließlich aller bewohnten Unterkünfte. Dazu müssen zunächst die Adressen der Gebäude- und Wohnungseigentümer festgestellt werden. Dies soll im Rahmen eines neuen Anschriften- und Gebäuderegisters erfolgen.

Zum Aufbau und zur Pflege dieses Registers sollen die Dateien der Landesvermessungsbehörden, der Meldebehörden und der Bundesagentur für Arbeit genutzt werden, weil sie die hierfür erforderlichen Angaben flächendeckend in der benötigten Qualität und Aktualität enthalten und über die Zusammenfassung der unterschiedlichen Dateien insbesondere die Vollzähligkeit der Erhebungseinheiten sichergestellt werden soll.

Der Aufbau des Anschriften- und Gebäuderegisters bedarf jedoch einer gesetzlichen Grundlage. Der Bund hat daher den Ländern Anfang Dezember 2006 einen Referentenentwurf eines Gesetzes zur Vorbereitung eines registergestützten Zensus einschließlich einer Gebäude- und Wohnungszählung 2010/2011 (Zensusvorbereitungsgesetz) zugeleitet, zu dem wir Anfang 2007 eine kritische Stellungnahme abgegeben haben:

- Nach § 2 Abs. 1 war vorgesehen, dass das Anschriften- und Gebäuderegister zwar vom Statistischen Bundesamt erstellt und betrieben wird, von den Statistischen Ämtern des Bundes und der Länder aber gemeinsam aufgebaut, gepflegt und genutzt werden soll.

Damit wurde nicht normenklar geregelt, welche Stelle dabei die datenschutzrechtliche Verantwortung für die gemeinsame Datei trägt, welche Verarbeitungsbefugnisse für die einzelnen Stellen bestehen und welche Stelle die technischen und organisatorischen Schutzmaßnahmen zu treffen hat.

- Mit der in § 3 Nr. 13 geplanten Speicherung der georeferenzierten Gebäudeadresse wird eine gebäudescharfe Abgrenzung geschaffen, mit der eine kleinräumige Auswertung von Erhebungsmerkmalen ermöglicht werden soll. Diese punktgenauen Koordinatenwerte lassen jedoch Auswertungsmöglichkeiten zu, die unterhalb der bisher als tiefste Aggregationsstufe definierten Blockseite liegen und nunmehr personenbeziehbar sind. Zwar sollen die Koordinatenwerte auch der Entwicklung von Konzepten zur Unterbindung einer Deanonymisierung dienen, eine geeignete Anonymisierungsmethode ist dem Gesetzentwurf jedoch nicht zu entnehmen.

- Nach § 7 Abs. 2 sollen die Statistischen Ämter der Länder die Ergebnisse der zusammengeführten Daten der Meldebehörden, Vermessungsbehörden und der Bundesagentur für Arbeit überprüfen, nicht zusammenführbare Anschriften feststellen und den Meldebehörden die Adressbereiche mitteilen, für die Anhaltspunkte auf unvollständige und fehlerhafte Datenmitteilungen vorliegen. Die Meldebehörden haben dann zu „klären“, ob sie vollständig und fehlerfrei übermittelt haben, und übermitteln für die betreffenden Adressbereiche nochmals vorhandenen Daten, sofern dies erforderlich ist. Das Ergebnis der Überprüfung wird von den Statistischen Ämtern in das Anschriften- und Gebäuderegister eingebracht. Der dabei verwendete Begriff „Adressbereiche“ ist jedoch zu unbestimmt und bedarf daher einer entsprechenden Definition.

Diese Regelung halten wir auch deshalb für problematisch, da sie dem verfassungsrechtlichen Gebot der strikten Trennung von Statistik und Verwaltungsvollzug nicht gerecht wird.

Die überarbeitete Fassung des Zensusvorbereitungsgesetzes vom 20. März 2007 enthält nunmehr klarere Regelungen zum Anschriften- und Gebäuderegister. Danach wird das Register vom Statistischen Bundesamt erstellt und geführt, wobei die Statistischen Landesämter am Aufbau und der Pflege mitwirken. Die technische Infrastruktur für die Zusammenarbeit der Statistischen Ämter wird zentral vom Statistischen Bundesamt bereitgestellt. Damit wurde unserer Forderung nach einer klareren Regelung der Verantwortlichkeiten und Verarbeitungsbefugnisse entsprochen.

Hinsichtlich der Gefahr einer Deanonymisierung bei kleinräumigen Auswertungen bleibt abzuwarten, welche Anonymisierungsmethoden dafür entwickelt werden.

Unsere Bedenken, dass die Meldebehörden die Daten der Rückmeldung über nicht zusammenführbare Adressenbereiche zu eigenen Zwecken nutzen könnten, sind insoweit ausgeräumt, als die Meldebehörden nur „anhand der vorhandenen Daten“ klären sollen, ob die ursprüngliche Übermittlung richtig war, Einzelprüfungen vor Ort aber nicht mehr vorgesehen sind.

Wir werden im weiteren Gesetzgebungsverfahren darauf achten, dass der Datenschutz und die Vorgaben des Volkszählungsurteils von 1983 auch für den Zensus 2011 eingehalten werden.

6. Finanzen und Steuern

6.1 Rechtsverordnung über die Einrichtung einer zentralen Immobiliendatenbank

Für Online-Zugriffe auf personenbezogene Daten der zentralen Immobiliendatenbank ist eine Rechtsgrundlage erforderlich.

Seit 2005 wurde das von der Finanzbehörde – Liegenschaftsverwaltung – eingesetzte modulare „elektronische Liegenschafts-Verwaltungs-Informationssystem (eLVIS)“ im Rahmen des Behörden und Ämter übergreifenden Projekts ImmoAktiv zu einer zentralen städtischen Immobiliendatenbank ausgebaut.

Dadurch sollen die Geschäftsprozesse der Stadt- und Landschaftsplanung, der Wirtschaftsförderung und der Liegenschaftsverwaltung im Rahmen des städtischen Immobilenmanagements, der Flächenentwicklung und der Wirtschaftsförderung transparenter gestaltet und optimiert werden.

Mit Abschluss des Projekts ImmoAktiv im Herbst 2006 wurden insgesamt ca. 50.000 Flurstücke im Eigentum der Freien und Hansestadt Hamburg sowie der öffentlichen Unternehmen mit unmittelbarer städtischer Beteiligung in der Immobiliendatenbank bestandsmäßig erfasst. Hierzu gehören auch die personenbezogenen Daten von Grundstückseigentümern (z.B. bei An- bzw. Verkauf), Vertragspartnern (z.B. bei Vermietung, Verpachtung), Immobilien-Interessenten, Notaren sowie privaten und gewerblichen Kontakten.

Aufgrund der fachlichen Zuständigkeiten sind bei vielen Geschäftsprozessen (z.B. bei der Vergabe von Gewerbegrundstücken) verschiedene Behörden und Ämter und im Bereich der Grundstücksbereitstellung auch private Vermarktungsunternehmen zu beteiligen und auf die Daten der Immobiliendatenbank angewiesen. Daher sollten diese Stellen jeweils einen automatisierten lesen-

den bzw. schreibenden Zugriff auf die zu ihrer Aufgabenerfüllung erforderlichen Immobiliendaten erhalten.

Wir mussten die Finanzbehörde – Liegenschaftsverwaltung – darauf hinweisen, dass die Einrichtung und die gemeinsame Nutzung einer Datenbank, in oder aus der mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten wollen, nur zulässig ist, wenn dafür eine Rechtsverordnung nach Maßgabe von § 11a des Hamburgischen Datenschutzgesetzes (HmbDSG) besteht. Dabei ist zu berücksichtigen, dass Stellen außerhalb des öffentlichen Bereichs nach § 11 Abs. 4 HmbDSG keinen automatisierten Zugriff auf Datenbanken der öffentlichen Verwaltung mit personenbezogenem Inhalt erhalten dürfen. Ein mit der „Vermarktung“ beauftragtes privates Unternehmen ist daher von einem automatisierten Zugriff auszuschließen.

Die Verordnung hat insbesondere die Art der zu verarbeitenden Daten, die Stellen, die in der gemeinsamen Datenbank Daten verarbeiten dürfen, sowie den Umfang ihrer Verarbeitungsbefugnisse anzugeben. Weiterhin bedarf es einer Festlegung, welche Stelle die datenschutzrechtliche Verantwortung gegenüber dem Betroffenen trägt und die technischen und organisatorischen Maßnahmen trifft. Damit nachträglich festgestellt werden kann, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat, sind alle Zugriffe auf die Immobiliendatenbank automatisch zu protokollieren (Revisionsfähigkeit). Die Protokolle sind sechs Monate aufzubewahren.

Die Finanzbehörde – Liegenschaftsverwaltung – ist unseren Hinweisen gefolgt. Der Senat hat am 6. Februar 2007 die Verordnung über die Einrichtung einer zentralen Immobiliendatenbank der Freien und Hansestadt Hamburg (Immobiliendatenbankverordnung) beschlossen (HmbGVBl. S. 33).

6.2 Kontenabrufverfahren

Die verfassungsgerichtliche Überprüfung des Kontenabrufverfahrens hat die Kritik der Datenschutzbeauftragten bestätigt.

Mit dem „Gesetz zur Förderung der Steuerehrlichkeit“ von Ende 2003 (BGBl. I S. 2931) erhielten ab 2005 die Finanzämter in Besteuerungsverfahren sowie eine unbestimmte Zahl von Behörden in sozialrechtlichen Angelegenheiten über das Bundeszentralamt für Steuern einen Zugriff auf sog. Kontenstammdaten (z.B. Name, Geburtsdatum, Anzahl und Nummern der Konten, Verfügungsberechtigte), die von den Kreditinstituten nach § 24c des Kreditwesengesetzes vorgehalten werden müssen.

Voraussetzung für die Berechtigung zu einer automatisierten Kontenabfrage war bislang, dass die abfragende Behörde in sozialrechtlichen Angelegenheiten ein Gesetz anzuwenden hatte, das „an Begriffe des Einkommensteuergesetzes anknüpft“ (z.B. Einkommen, Einkünfte), und eigene Ermittlungen nicht zum Ziele führten oder keinen Erfolg versprachen. Welche Behörden dies

im Einzelnen sein sollten, ging aus dem Gesetz nicht eindeutig hervor. Dies ist nach dem verfassungsrechtlichen Bestimmtheitsgebot jedoch unverzichtbar.

Hierauf hatten die Datenschutzbeauftragten des Bundes und der Länder bereits während des Gesetzgebungsverfahrens im Herbst 2003 aufmerksam gemacht und klare, für den Bürger verständliche Regelungen gefordert. Weiterhin hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Jahre 2004 in der Entschließung „Staatliche Kontoabfrage auf den Prüfstand“ den Bundesgesetzgeber aufgefordert, die Kontenabfrage insbesondere im Hinblick auf den Kreis der abfrageberechtigten Behörden kritisch zu überprüfen. Darüber hinaus wurde bemängelt, dass die Betroffenen über eine Kontendatenabfrage nicht informiert wurden. Dies widerspricht dem verfassungsrechtlichen Transparenzgebot.

Die Verfassungsmäßigkeit des automatisierten Kontenabrufverfahrens wurde auch von mehreren Betroffenen bezweifelt. Auf Grund entsprechender Verfassungsbeschwerden hat das Bundesverfassungsgericht hat am 12. Juli 2007 entschieden, dass die Abfrage der Kontenstammdaten durch die Finanzämter grundsätzlich mit der Verfassung vereinbar ist. Das Gericht stellte aber fest, dass die Vorschrift über die Kontenabfrage durch andere Behörden nicht der Normenklarheit und -bestimmtheit entspricht, und legte eine Frist zur gesetzlichen Neuregelung der Kontenabfrage bis zum 31. Mai 2008 fest.

Der Gesetzgeber hat daraus die notwendigen Konsequenzen gezogen und die Regelungen zum Kontenabrufverfahren mit dem Unternehmensteuerreformgesetz 2008 geändert.

Danach dürfen nunmehr nur diejenigen Behörden das Bundeszentralamt für Steuern um Kontendaten zu nichtsteuerlichen Zwecken ersuchen, die für die Verwaltung

1. der Grundsicherung für Arbeitssuchende nach dem Zweiten Buch Sozialgesetzbuch,
2. der Sozialhilfe nach dem Zwölften Buch Sozialgesetzbuch,
3. der Ausbildungsförderung nach dem Bundesausbildungsförderungsgesetz,
4. der Aufstiegsfortbildungsförderung nach dem Aufstiegsfortbildungsförderungsgesetz und
5. des Wohngeldes nach dem Wohngeldgesetz

zuständig sind.

Darüber hinaus ist neu aufgenommen worden, dass der Betroffene auf die Möglichkeit eines Kontenabrufs hinzuweisen bzw. nach erfolgtem Kontenabruf über die Durchführung zu benachrichtigen ist. Außerdem ist das Abrufersuchen von der abrufenden Behörde zu dokumentieren.

Damit sind wesentliche Forderungen der Datenschutzbeauftragten des Bundes und der Länder erfüllt worden.

7. Arbeitslosengeld II (MISTRAL-Verfahren)

Wir haben bei der Einführung des MISTRAL- Verfahrens zur Vermittlung von Ein-Euro-Jobs die Sicherung datenschutzrechtlicher Standards durchgesetzt.

Zum 1. Januar 2007 sollte in Hamburg ein neues Verfahren zur Vermittlung von Arbeitsgelegenheiten nach § 16 Abs. 3 SGB II eingeführt werden. Die Arge sollte zu diesem Zweck diese Aufgabe auf die Behörde für Wirtschaft und Arbeit (BWA) übertragen. Diese wiederum sollte dann die öffentliche Beschäftigungsgesellschaft Hamburger Arbeit (HAB) mit der alleinigen Erfüllung dieser Aufgaben beauftragen. Die HAB sollte dann der alleinige Ansprechpartner der einzelnen Beschäftigungsträger sein, die die Ein-Euro-Jobs konkret vermitteln. Das Ziel der Maßnahme war es, die Vermittlung von Arbeitsgelegenheiten effektiver zu gestalten. Hierzu sollte die IT-gestützte Lösung „MISTRAL“ geschaffen werden. Dazu sollte eine Datenbank genutzt werden, auf die sowohl die HAB als auch die einzelnen Träger Zugriff erhielten. In dieser Datenbank sollten zu den zu vermittelnden Personen u.a. Informationen über den Lebenslauf, vorliegende Behinderungen, Schulden und Erfolg der Maßnahme gespeichert werden. Auf diese Weise sollten den jeweiligen Beschäftigungsträgern die personenbezogenen Daten direkt zur Verfügung gestellt werden. Angedacht war, das Verhältnis von BWA zur HAB als Auftragsdatenverarbeitung auszugestalten.

Wir haben das Projekt sowohl in rechtlicher als auch in technischer Hinsicht begleitet. Von Beginn an haben wir daraufhin gewiesen, dass auch die Ausgestaltung der Vereinbarung zwischen der HAB und den einzelnen Beschäftigungsträgern als Auftragsdatenverarbeitung über sogenannte Unteraufträge zu erfolgen habe. Diese Grundsatzfrage ist dann auch akzeptiert worden. Probleme gab es dann jedoch bei der Frage, welche datenschutzrechtlichen Standards bei der Ausgestaltung der Unteraufträge von den einzelnen Trägern zu verlangen seien. Wir haben darauf bestanden, dass auch bei den privatrechtlich organisierten Unterauftragnehmern die im öffentlichen Bereich herrschenden datenschutzrechtlichen Standards erhalten bleiben und die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen nach dem Stand der Technik gewährleistet werden. Hierzu gehört insbesondere die Aktivierung einer laufend aktualisierten Firewall und von Antivirenprogrammen. Der Zugriff zum MISTRAL-System musste mit trägerbezogenen Clientzertifikaten und mit komplexen Passworten abgesichert werden. Diese Forderungen hat die HAB letztendlich akzeptiert.

Die Realisierung der festgelegten Maßnahmen werden wir in 2008 überprüfen.

8. Polizei

8.1 Novellierung des Polizeirechts

Die Rechtsprechung des Bundesverfassungsgerichts zur präventiven Telekommunikationsüberwachung, zum Schutz des Kernbereichs privater Lebensgestaltung und zur Rasterfahndung erfordert Änderungen des Gesetzes über die Datenverarbeitung der Polizei (PolDVG).

Im vorangegangenen Tätigkeitsbericht (20.TB, 7.2) hatten wir ausgeführt, dass es der Prüfung bedarf, ob die Regelungen zur präventiven Telekommunikationsüberwachung (§ 10a PolDVG) angesichts des Urteils des Bundesverfassungsgerichts zur präventiven Telekommunikationsüberwachung nachgebessert werden müssen. So muss die gesetzliche Eingriffsgrundlage einen umfassenden Schutz des Kernbereichs privater Lebensgestaltung sichern, nicht zuletzt durch eine Untersagung der Aufzeichnung intimer Gespräche zwischen engen Vertrauten. Ähnlich ist die Rechtslage bei der akustischen und optischen Wohnraumüberwachung nach § 10 Abs. 2 PolDVG zu sehen. Unter Bezugnahme auf die Rechtsprechung des Bundesverfassungsgerichts zum Kernbereichsschutz hat beispielsweise der Verfassungsgerichtshof Rheinland-Pfalz am 29. Januar 2007 die Datenerhebung durch den verdeckten Einsatz technischer Mittel in oder aus Wohnungen nach rheinland-pfälzischem Landesrecht nur deshalb für rechtmäßig befunden, weil dort bereits die Aufzeichnung kernbereichsrelevanter Gespräche untersagt ist.

Der Senat hatte zunächst einen Referentenentwurf zu allen aus seiner Sicht änderungsbedürftigen Vorschriften des PolDVG nach der Sommerpause 2006 in Aussicht gestellt (Bürgerschaftsdrucksache 18/3931). Im August 2006 teilte der Senat mit, es seien noch keine endgültigen Festlegungen über Inhalt und Umfang etwaiger Änderungsnotwendigkeiten erfolgt. Mehrfach haben wir nachgefragt und angeboten, mit uns vorab die Änderungsbedarfe zu erörtern. Diese Angebote wurden bislang nicht wahrgenommen. Bis Ende 2007 lag kein Referentenentwurf vor.

Zwischenzeitlich sind weitere Änderungsbedarfe entstanden. Am 4.4.2006 hat das Bundesverfassungsgericht beschlossen, dass eine Rasterfahndung im Vorfeld einer Gefahrenabwehr unzulässig ist. Eine allgemeine Bedrohung durch mögliche terroristische Anschläge, wie sie sich seit dem 11. September 2001 durchgehend dargestellt hat, rechtfertigt den mit einer Rasterfahndung verbundenen schwerwiegenden Eingriff nicht. Voraussetzung ist vielmehr eine konkrete Gefahr für hochrangige Rechtsgüter wie den Bestand oder die Sicherheit des Bundes oder eines Landes oder für Leib, Leben oder Freiheit einer Person. Die nordrhein-westfälische Eingriffsgrundlage für eine Rasterfahndung, über die das Bundesverfassungsgericht zu entscheiden hatte, knüpft zwar dem Wortlaut nach an das Vorliegen einer konkreten Gefahr an, wurde jedoch

von Polizei und Gerichten dahingehend weit ausgelegt, dass auch eine Dauergefahr, wie sie seit dem 11. September 2007 vorliege, ausreiche. Im Sinne dieser für verfassungswidrig befundenen Auslegung setzt § 23 Abs. 1 PolDVG schon tatbestandlich keine konkrete Gefahr voraus, sondern lässt einen automatisierten Datenabgleich zu, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dies zur Verhütung von Straftaten erheblicher Bedeutung erforderlich ist. § 23 Abs. 2 PolDVG dürfte mangels Anknüpfung an eine konkrete Gefahr ebenfalls verfassungsrechtlichen Anforderungen nicht genügen, soweit darin das Übermittlungsersuchen „auf im Einzelfall festzulegende Merkmale zu beschränken“ ist. Denn der Verwendungszweck der Daten ist auf die Erhebung und den Abgleich solcher Datenbestände beschränkt, die zur Abwehr einer konkreten Gefahr für bedrohte hochrangige Verfassungsgüter erforderlich sind; dies muss in der Norm klar zum Ausdruck kommen.

Die Datenschutzbeauftragten des Bundes und der Länder hatten auf ihrer 73. Konferenz im März 2007 in einer Entschließung an Bundesregierung, Landesregierungen und Parlamente appelliert, auf Befugnisnormen für Online-Durchsuchungen zu verzichten. Im September 2007 hat der Polizeipräsident in einer Presseerklärung mitgeteilt, er wolle Polizei und Verfassungsschutz Online-Durchsuchungen ermöglichen. Allerdings werde zunächst das Urteil des Bundesverfassungsgerichts zur Online-Durchsuchung nach dem nordrhein-westfälischen Verfassungsschutzgesetz abgewartet.

Wir werden die weitere Entwicklung kritisch begleiten.

Im Hinblick auf Zuverlässigkeitsüberprüfungen zwecks Akkreditierungen (vgl. 8.4 und 20. TB, 7.3) hat die Behörde für Inneres anlässlich der Maßnahmen beim G7- und G8-Gipfel und zur EU-Ratspräsidentschaft immerhin im März 2007 geäußert, dass eine für Bund und Länder einheitliche gesetzliche Bundesregelung durchaus wünschenswert wäre.

8.2 Polizeiliche Videoüberwachung Reeperbahn und Hansaplatz

Die Polizei hat uns die Bewertung und Prüfung der Videoüberwachung erheblich erschwert, indem sie es kategorisch abgelehnt hat, die dafür nach §§ 8 und 9 des Hamburgischen Datenschutzgesetzes (HmbDSG) vorgeschriebene Risikoanalyse und Verfahrensbeschreibung zu erstellen.

Im Juni 2005 wurde in das Gesetz über die Datenverarbeitung der Polizei mit § 8 Abs. 3 eine Regelung aufgenommen, wonach die Polizei an öffentlich zugänglichen Orten, die sog. Kriminalitätsbrennpunkte darstellen, eine offene Videobeobachtung nebst Bildaufzeichnung durchführen darf (vgl. 20. TB, 7.1). Seit März 2006 liefern zwölf dreh- und schwenkbare sowie zoomfähige Videokameras, auf Masten montiert, ständig Bilder aus dem Bereich der Reeperbahn in die Polizeieinsatzzentrale (PEZ), die dort auf einer großen Monitorwand

überwacht werden. Zusätzlich kann das Polizeikommissariat PK 15 (Davidwache) auf einem Monitor die Bilder einer Kamera überwachen.

Seit Januar 2006 sind wir mit der Polizei über die konkrete Ausgestaltung der Videoüberwachung der Reeperbahn im Gespräch. Dabei haben wir vor allem darauf bestanden, dass keine längere Erfassung von Eingangsbereichen erfolgt, die Kontakt- und Bewegungsprofile der Bewohner und Besucher ermöglichen würde. Es gelang, die privaten Bereiche (sog. private zones), die nicht überwacht werden dürfen, einvernehmlich mit der Polizei festzulegen, die Überwachung des Straßenraumes auf die Längsrichtung zu konzentrieren sowie Vorkehrungen durchzusetzen, die ein lang andauerndes Beobachten von Eingangsbereichen verhindern. Die Aufnahmen, die auf den Monitoren erscheinen, müssen mit den gespeicherten Bildern identisch sein. Sobald auch nur die Ränder privater Bereiche bei Dreh-, Schwenk- oder Zoombewegungen von einer Videokamera erfasst werden, werden durch die Aufzeichnungssoftware die Monitore in der Polizeieinsatzzentrale (PEZ) komplett schwarz geschaltet und eine Aufzeichnung findet nicht statt (sog. private masking). Die Polizei behielt sich allerdings zunächst vor, die Schwarzschaltungen privater Bereiche bei bestimmten Gefahrenlagen (genannt wurden z. B. Wohnungsbrand, Geiselnahme in einer Wohnung oder Suizidversuch) aufzuheben. Seit einer Entscheidung des Verwaltungsgerichts dazu darf eine Aufhebung der Schwarzschaltung aber nicht mehr erfolgen.

Für die gesamte Videoüberwachungsanlage haben wir wegen der besonderen Gefahren für die betroffenen Bürgerinnen und Bürger und der zahlreichen rechtlichen und technisch-organisatorischen Ausgestaltungsfragen die Vorlage einer durchgeführten Vorabkontrolle (sog. Risikoanalyse) und einer Verfahrensbeschreibung gefordert. Diese Unterlagen hätten vor der Einführung des automatisierten Verfahrens, mit dem personenbezogene Daten verarbeitet werden sollen, d.h. vor Inbetriebnahme der Videoüberwachungsanlage erstellt werden müssen (§ 8 Abs. 4, § 9 Abs. 1 HmbDSG). Die Polizei hält dies nicht für erforderlich, verwies im Wesentlichen auf ihre interne Dienstanweisung und nahm den Echtbetrieb ohne Risikoanalyse und vor Klärung zahlreicher datenschutzrelevanter Fragen auf. Uns fehlte damit ein systematisches Gesamtkonzept, das die Risiken der Videoüberwachung Reeperbahn und deren technisch-organisatorische Minimierung darstellt. So waren wir gezwungen , uns erst durch zähes Nachfragen einen Überblick darüber zu verschaffen, welche einzelnen Geräte die Polizei einsetzt, wo sich die Geräte, insbesondere Rechner, befinden, wie sie gegen unbefugtes Eindringen von außen gesichert werden, welche Software eingesetzt wird, welche Zugriffsberechtigungen innerhalb der Polizei bestehen, wie ihre Einhaltung abgesichert ist und welche Zugriffsmöglichkeiten der Auftragsdatenverarbeiter besitzt. Wir haben von Dezember 2006 bis Januar 2007 gemäß § 23 Abs. 5 HmbDSG eine Prüfung der Videoüberwachung vorgenommen, die zahlreiche Mängel offenbarte:

- Unsere Prüfung ergab unter anderem, dass die Schwarzschaltung einzelner Kameras vorübergehend deaktiviert worden war, um verdächtige Personen verfolgen zu können, ohne sie durch Schwarzschaltungen aufgrund von kurzzeitigen Erfassungen von private zones aus den Augen zu verlieren. Durch die von einer Anwohnerin der Reeperbahn erwirkten gerichtlichen Vorgaben wird es zurzeit technisch ausgeschlossen, dass die Polizei Schwarzschaltungen aufhebt.
- Mit dem Lieferanten der Hard- und Software, der die Anlage auch ständig pflegt, wurde kein Vertrag nach § 3 HmbDSG abgeschlossen worden.
- Die verbindliche interne „Dienstanweisung für die polizeiliche Videoüberwachung Reeperbahn“ wich in wesentlichen Punkten von der praktizierten Überwachung ab.
- Eine automatisierte Zwangsprotokollierung aller Zugriffe auf das System lief noch immer nicht.
- Die Freigaberichtlinie vom 04.04.2005 wurde nicht beachtet.
- Bildsequenzen, die für Strafverfolgungszwecke auf externe Datenträger gebrannt wurden, verblieben auf unbestimmte Zeit auf der Festplatte des zentralen Bedienplatzes.

Im Prüfbericht haben wir noch einmal auf die datenschutzrechtliche Verpflichtung hingewiesen, eine Risikoanalyse und Verfahrensbeschreibung vorzulegen. Im Hinblick auf die zahlreichen Mängel hatten wir empfohlen, zumindest die Aufzeichnung der Bilder bis zur Mängelbeseitigung auszusetzen. Die Polizei hat dies abgelehnt, allerdings bis Ende 2007 technisch-organisatorische Verbesserungen des Überwachungskonzepts vorgenommen. Inzwischen wurde eine automatische Zwangsprotokollierung (sog. Logbuch) eingerichtet. Die Verpflichtung der Auftrag nehmenden Firma auf den Datenschutz nach § 3 HmbDSG wurde zugesagt, steht allerdings noch aus. Schwarzschaltungen können bis auf weiteres nicht mehr aufgehoben werden. Die Dienstanweisung wurde im Juni 2007 überarbeitet, die Endfassung, die uns erst im November 2007 zur Verfügung gestellt wurde, berücksichtigt immer noch nicht alle Änderungswünsche. Die unnötige Speicherung kopierter Videosequenzen auf der Festplatte des zentralen Bedienplatzes entfällt. Fehlende technisch-organisatorische Beschreibungen wurden zwar zugesagt, die Erstellung einer Risikoanalyse und einer Verfahrensbeschreibung jedoch weiterhin abgelehnt – ein Umstand, der anlässlich einer Selbstbefassung des Unterausschusses Datenschutz der Hamburgischen Bürgerschaft mit dem Thema der polizeilichen Videoüberwachung auch bei den Abgeordneten wegen des klaren Wortlauts des Hamburgischen Datenschutzgesetzes auf Unverständnis stieß.

Am 3. Juli 2007 wurde mit fünf Kameras die Videoüberwachung des Hansaplatzes aufgenommen. Eine von uns als Vorbedingung geforderte unabhängige Evaluierung der Videoüberwachung Reeperbahn wurde abgelehnt. Auch

für dieses automatisierte Verfahren erhielten wir weder eine Risikoanalyse noch eine Verfahrensbeschreibung. Die technisch-organisatorischen Fragen, die noch nicht abschließend beantwortet sind, gleichen allerdings denen, die sich bereits bei der Videoüberwachung der Reeperbahn gestellt hatten. Allerdings ist hier eine Anlaufstelle für drogenabhängige und sich prostituierende Frauen vor der Videoüberwachung besonders zu schützen. Die Nutzung dieser Hilfseinrichtung muss völlig unbeobachtet möglich sein, sodass sich der von Kameras nicht erfassbare Bereich nicht nur auf den Eingang der Einrichtung, sondern auf ein ausreichend bemessenes Umfeld der Einrichtung erstrecken muss. Die Polizei hat unsere Anregung, dies in der internen Dienstanweisung für die Videoüberwachung des Hansaplatzes zu konkretisieren, aber noch nicht umgesetzt. Inwieweit sich seit November 2007 durch das Abholzen von Bäumen auf dem Hansaplatz, den Abriss der dortigen halbhohen Mauer und ein neues Nutzungskonzept für den Platz Änderungen des Videoüberwachungskonzepts ergeben müssen, werden wir überprüfen.

8.3 Projekt Korruptionsbriefkasten

Im Oktober 2006 startete die Polizei das Projekt „Korruptionsbriefkasten“: Damit soll die Möglichkeit geschaffen werden, über eine Webanwendung dem „Dezernat Interne Ermittlungen (D.I.E.)“ der Behörde für Inneres anonyme Hinweise zu Korruption in Behörden oder Unternehmen zu geben.

Im Dezember 2006 bat uns die Behörde für Inneres um eine erste Einschätzung zu diesem Vorhaben. Während sich Bürger, die über die seit dem 3. Januar 2006 eingerichtete „Onlinewache“ Mitteilungen an die Polizei richten möchten, registrieren lassen müssen, sollen in Korruptionsangelegenheiten Hinweisgeber, die anonym bleiben möchten, über das eGovernment-Portal HamburgGateway Mitteilungen an die D.I.E. machen können, ohne Spuren zu hinterlassen: Die Hinweisgeber sollen sich nicht registrieren lassen müssen und ihre IP-Adresse soll nicht gespeichert werden. Dem Hinweisgeber wird zu seiner Mitteilung ein Aktenzeichen angezeigt und er kann freiwillig ein eigenes geheimes Kennwort hinzugeben; mit Aktenzeichen und Kennwort hat er die Möglichkeit, später im HamburgGateway zu prüfen, ob die Polizei Nachfragen zu seinem Hinweis ins Netz gestellt hat.

Die Polizei will zur Akzeptanz des Korruptionsbriefkastens dem Hinweisgeber uneingeschränkte Anonymität garantieren. Dies bedarf jedoch besonderer technischer Vorkehrungen. So speichert Dataport als Betreiber des HamburgGateway automatisch sämtliche IP-Adressen aller Nutzer für mehrere Tage. Wir haben die Polizei darauf aufmerksam gemacht, dass, wenn auch mit einigem Aufwand, damit eine Identifizierung des Hinweisgebers möglich ist. Die Polizei hat zugesagt, mit Dataport ein Verfahren zu vereinbaren, in dem die Speicherung der IP-Adressen unterbleibt. Auch hinsichtlich der Möglichkeit, im Korruptionsbriefkasten mittels Kennwort und Aktenzeichen Rückfragen der Ermitt-

lungsbehörde zu beantworten, sind wir noch mit der Polizei in der Diskussion. Wenn dem Bürger Anonymität zugesichert wird, muss es auch technisch völlig ausgeschlossen sein, den Bürger über einen „Postkasten“, den er mittels Kennwortvergabe einrichtet, ausfindig zu machen.

Wie bei der Onlinewache besteht auch hier die Möglichkeit, dass ein Hinweisgeber personenbezogene Daten über Dritte (Beschuldigte, Zeugen, Opfer, Kontaktpersonen) über die Webanwendung an die Polizei sendet. Deshalb muss der Hinweisgeber darauf vertrauen können, dass diese Angaben Unbefugten unzugänglich sind. Die Polizei muss deshalb auch für den Korruptionsbriefkasten mit Dataport ein Verfahren vereinbaren, das gegen unbefugte Kenntnisnahme ausreichend geschützt ist. Darüber hinaus drängen wir darauf, dass im Falle von Nachfragen, die die Ermittler der DIE an das Postfach des Hinweisgebers senden, jedenfalls keine personenbezogenen Daten über Dritte offenbart werden, die nicht schon der Hinweisgeber mitgeteilt hatte.

8.4 Sicherheitsüberprüfungen und Akkreditierungsverfahren

Für eine auf Einwilligung gegründete Zuverlässigkeitsüberprüfung bei Großveranstaltungen soll im Verfassungsschutzgesetz eine Übermittlungsbefugnis geschaffen und eine Angemessenheitsprüfung vorgesehen werden.

Im letzten Tätigkeitsbericht (20.TB, 7.3) hatten wir das Akkreditierungsverfahren zur Fußballweltmeisterschaft und unsere Bedenken gegen eine im Gesetz nicht vorgesehene, lediglich auf eine Einwilligung des Betroffenen gestützte Sicherheitsüberprüfung durch das Landeskriminalamt (LKA) und das Landesamt für Verfassungsschutz (LfV) dargestellt.

Seitdem ist die bundesweite Diskussion über die Zulässigkeit und Rechtmäßigkeit derartiger Überprüfungen auf Einwilligungsgrundlage nicht zur Ruhe gekommen. Dies lag insbesondere daran, dass das als Ausnahme bezeichnete WM-Akkreditierungsverfahren zunächst auch auf den G7-Gipfel, auf den G8-Gipfel in Heiligendamm, dann auf Veranstaltungen zur deutschen EU-Ratspräsidentschaft und schließlich auf alle ähnlichen Großereignisse übertragen wurde bzw. wird.

In der bundesweiten Datenschutzdiskussion und auch gegenüber der Behörde für Inneres vertraten wir die Rechtsauffassung, dass die Einholung einer Einwilligung allein eine Überprüfung durch die Sicherheitsbehörden nicht rechtfertigen könne. Wir setzten uns ein für eine klare bereichsspezifische Regelung für Sicherheitsüberprüfungen, sofern derartige Überprüfungen tatsächlich im Allgemeininteresse unabweisbar wären.

Bereits 2005 war in das Hamburgische Polizeirecht eine Rechtsgrundlage für Datenübermittlungen an nicht öffentliche Stellen für Zwecke einer Zuverlässigkeitsüberprüfung mit Einwilligung des Betroffenen eingefügt worden (vg. 20. TB, 7.1 und 7.3). Die Überprüfung selbst wurde jedoch nicht geregelt. Auch

fehlt es an einer Befugnis zur Datenübermittlung zwischen den verschiedenen Sicherheitsbehörden. Dennoch beteiligten sich 2007 das LKA und das LfV an den Akkreditierungsverfahren des BKA zu Veranstaltungen des G8-Gipfels und der deutschen EU-Ratspräsidentschaft.

Mit dem Änderungsgesetzes zum Hamburgischen Verfassungsschutzgesetz (unten 9.1) ist die Regelung im Polizeirecht nun auch für den Verfassungsschutz übernommen worden. Es wurde eine Befugnisnorm für Übermittlungen an Dritte im nicht öffentlichen Bereich „für Zwecke einer Zuverlässigkeitsüberprüfung mit Einwilligung der Betroffenen“ geschaffen. Auf unsere Anregung wurde die Übermittlung auf „eine Bewertung“ (Sicherheitsbedenken: ja / nein) beschränkt und damit die Weitergabe der Erkenntnisse selbst ausgeschlossen. Neben der Einwilligung hat das LfV die Angemessenheit der Übermittlung zu prüfen. In diese Prüfung gehen der Anlass der Überprüfung („Zugang zu einer besonders gefährdeten Veranstaltung“), ein berechtigtes Interesse des Veranstalters sowie Art und Umfang der Erkenntnisse zu dem Betroffenen ein. Besonderen Wert legten wir darauf, dass das LfV dem Betroffenen die Gründe für eine negative Bewertung mitzuteilen hat, damit dieser sich ggf. dagegen wehren kann.

An unserer Rechtsauffassung, dass für die Zuverlässigkeitsüberprüfung selbst eine Einwilligung nicht ausreicht, sondern eine gesetzliche Grundlage erforderlich ist, halten wir fest. Es ist nicht mit dem Grundrecht auf informationelle Selbstbestimmung vereinbar, dass Veranstalter oder Sicherheitsbehörden den Umfang der erforderlichen Datenabgleiche und -übermittlungen frei bestimmen. Die verfassungsrechtlichen Prinzipien des Vorbehalts und Vorrangs des Gesetzes erfordern für diese einschneidenden Grundrechtseingriffe vielmehr eine Entscheidung des Gesetzgebers. Für bundesweite Datenabgleiche reichen dabei landesrechtliche Regelungen nicht aus. Die Polizei hält bundeseinheitliche Regelungen immerhin für wünschenswert (vgl. oben 8.1).

Keine Akkreditierungsverfahren zu Einzelereignissen, aber langfristig wirkende Sicherheitsüberprüfungen ebenfalls nur auf Einwilligungsbasis wünschen zunehmend auch Arbeitgeber. Dabei geht es seit längerem um die Praxis z.B. der Deutschen Bundesbank, Mitarbeiter von Fremdfirmen vor Erteilung einer Zutrittsberechtigung durch LKA und LfV überprüfen zu lassen. Anders als die Praxis in anderen Bundesländern lehnte das LKA Hamburg unserer Rechtsauffassung entsprechend eine derartige Zusammenarbeit mit der Deutschen Bundesbank ab. Gegenüber anderen Bundesländern verwiesen wir nicht nur auf den rechtsstaatlichen Vorbehalt und Vorrang des Gesetzes, sondern auch auf die fehlende Freiwilligkeit einer Einwilligung zur Sicherheitsüberprüfung und auf die Regelungen des Bundeszentralregistergesetzes. Zur Befriedigung der Sicherheitsbedürfnisse von Arbeitgebern schuf der Gesetzgeber das Institut des Führungszeugnisses und (für Behörden) die Registerauskunft; die Rechtsprechung entwickelte das (beschränkte) Fragerecht des

Arbeitgebers. Beides würde durch eine erzwungene und sehr viel weitergehende Sicherheitsüberprüfung auf Basis einer Einwilligung radikal entwertet. Erscheint eine erweiterte Sicherheits- oder Zuverlässigkeitsprüfung in Zeiten der Terrorabwehr unverzichtbar, hat darüber der Gesetzgeber zu entscheiden, der dann zugleich auch die Maßnahmen zum Schutz der informationellen Selbstbestimmung der Betroffenen zu treffen hat.

8.5 Löschungsantrag beim LKA

Anlässlich zweier Eingaben sind wir auf einen problematischen Umgang der Polizei mit Löschungen aus dem Vorgangsverwaltungssystem „ComVor-Index (CVI)“ gestoßen.

Die Petenten hatten an das Landeskriminalamt 132 (LKA 132) Anträge auf Auskunft über alle bei der Polizei Hamburg über sie gespeicherten personenbezogenen Daten gerichtet. Nach Erhalt der Selbstauskunft stellten sie Löschungsanträge zu den Daten, die sie als Beschuldigte in Strafverfahren auswiesen, da diese Strafverfahren eingestellt worden waren. Sie begründeten die Anträge damit, dass kein Restverdacht mehr hinsichtlich des eingetragenen Tatvorwurfs bestehe. Neben der Löschung aus Vorgangsdateien, einschließlich der beim Bundeskriminalamt (BKA) geführten Verbunddateien, wollten die Petenten auch die Löschung ihrer Daten aus dem CVI erreichen.

Das CVI dient als Vorgangsverwaltungsdatei im Wesentlichen dem Auffinden polizeilicher Vorgänge, nicht aber der Sachbearbeitung. Im CVI sind den Personen, über die Vorgänge angelegt werden, „Rollen“ zugeordnet, z. B. „Beschuldigter“, „Betroffener“, „angehaltene Person“, „sonstige Person“ oder „Fehlerfassung“. Selbst dann, wenn in einer Sache kein Ermittlungsverfahren eingeleitet oder ein Ermittlungs- oder Strafverfahren eingestellt wurde, hält es die Polizei regelmäßig noch für einen gewissen Zeitraum für erforderlich, über CVI etwas über den Verfahrensstand oder den Verbleib der Sachakten zu erfahren.

Die im CVI gespeicherten Daten unterliegen Speicherfristen, die mit dem Hamburgischen Datenschutzbeauftragten einvernehmlich festgelegt wurden. Der Lauf dieser Speicherfristen wird an ein Ereignis (z. B. bei Anhaltemeldungen) oder an das Datum einer Erledigung (z. B. Einstellung des Verfahrens) geknüpft; nach Ablauf der Fristen, die rollenabhängig gestaffelt sind (z. B. bei Beschuldigten: fünf Jahre, bei sonstigen Personen: ein Jahr), werden die Daten automatisch aus dem CVI gelöscht.

Die ausführlich begründeten Löschanträge der Petenten wurden von der Polizei per Bescheid abgelehnt mit der Begründung, durch die Festlegung der Speicherfristen gebe es für eine Löschung der Daten aus dem CVI „keinen Ermessensspielraum“. In einem Fall führte unsere Intervention allerdings zu einer sofortigen Löschung aus dem CVI, was später von der Polizei mit einem Versehen erklärt wurde.

Wir haben der Polizei verdeutlicht, dass wir die Begründung des ablehnenden Bescheids für rechtsfehlerhaft halten, und gebeten, diese Praxis mit uns und mit LKA 132 zu klären. Wir halten die Festsetzung von Speicherfristen nach dem Gesetz über die Datenverarbeitung der Polizei (PolDVG) zwar für rechtmäßig. Dadurch wird gesichert, dass Daten, zu denen keine weitere Sachbearbeitung im Einzelfall erfolgt, überhaupt nach angemessener Zeit gelöscht werden. Wenn die Voraussetzungen des § 24 Abs. 2 PolDVG vorliegen, müssen die Daten allerdings gelöscht werden. Das ist u. a. der Fall, wenn aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass ihre Kenntnis für die speichernde Stelle zur Erfüllung der in ihrem Zuständigkeitsbereich liegenden Aufgaben nicht mehr erforderlich ist. Hier besteht kein Ermessen, wohl aber ein Beurteilungsspielraum der Polizei. Sie muss bei einer Einzelfallbearbeitung prüfen, ob sie die Daten im CVI zum Auffinden der Sachvorgänge noch benötigt. Ein nachvollziehbar begründeter, ausdrücklich auf CVI bezogener Löschungsantrag muss eine Einzelfallbearbeitung auslösen. Die Polizei kann dabei zu dem Schluss gelangen, dass Informationen über den Verfahrensstand oder Verbleib von Vorgängen nicht mehr erforderlich sind. Das könnte beispielsweise dann der Fall sein, wenn sich erwiesen hat, dass ein anderer als der ursprünglich Beschuldigte die Straftat begangen hat.

Wir haben zugleich angemahnt, dass die Polizei im Beispielsfall auch ohne Antrag des Betroffenen sicherstellen muss, dass dieser nicht mehr unter der Rolle „Beschuldigter“ im CVI geführt wird, wenn für die Polizei zweifelsfrei feststeht, dass er die Tat nicht begangen hat. Es ist nicht zu rechtfertigen, dass fünf Jahre lang Einträge im CVI über erwiesenermaßen unschuldige Bürger bestehen bleiben, die sie als Beschuldigte mit einem bestimmten Deliktsvorwurf ausweisen. Diese Daten sind unrichtig und deshalb nach § 24 Abs. 1 PolDVG zu berichtigen, soweit sie nicht gelöscht werden müssen. Die Personenrolle müsste ggf. in „sonstige Person“ (Speicherfrist ein Jahr) oder in „Fehlerfassung“ (Speicherdauer ein Monat) umgewandelt werden.

Wir werden weiterhin auf eine schnellstmögliche Löschung zweifelsfrei unrichtiger Einträge im CVI drängen.

8.6 Verkehrsunfall-Auskunftsdienst im HH-Gateway

Die Polizei will Rechtsanwälten und Versicherungen die Möglichkeit bieten, online über das HamburgGateway Informationen über Verkehrsunfälle zu erhalten, um ihren Arbeitsaufwand sowie die Wartezeit der Auskunftsberechtigten zu verringern.

Im Februar 2006 hatten Verkehrsdirektion und IuK-Bereich der Polizei Hamburg zu dem geplanten Fachverfahren „Verkehrsunfall-Auskunftsdienst“ ein Projekt gestartet, zu dem uns im September 2006 erste Unterlagen zugesandt wurden. Rechtsanwälte und Kfz-Versicherer sollten in einem gesonderten Verfahren als „Firmenkunden“ legitimiert und in einer Registrierungsdatei gespei-

chert werden, um dann im Auskunftsverfahren nach §§ 474 ff. der Strafprozessordnung eine „Aktenkurzinformation“ über Verkehrsunfälle, die in der elektronischen Vorgangsbearbeitung der Polizei ComVor gespeichert sind, online abrufen zu können. Außerdem sollte die Übersendung der Verkehrsunfallakte zur Akteneinsicht online beantragt werden können. Das Verfahren wurde uns demonstriert.

Wir mussten die Polizei jedoch darauf hinweisen, dass das vorgesehene automatisierte Abrufverfahren unzulässig ist. Die Aktenkurzauskunft fällt nicht unter die ausnahmsweise erlaubten automatisierten Datenübermittlungen nach § 488 der Strafprozessordnung. Deshalb schlugen wir vor, das Verfahren in ein Anfrage- und ein Antwortverfahren aufzuspalten, sodass die auf Anfrage automatisiert erstellte Aktenkurzinformation nach Prüfung von der Polizei online übermittelt werden kann. Allerdings mussten wir darauf bestehen, das Verfahren erst dann freizugeben, wenn im HamburgGateway die dritte Sicherheitsstufe (Signaturverfahren) implementiert ist, mit der auch die Übermittlung von Daten mit hohem Schutzbedarf hinreichend sicher möglich ist. Bis dahin haben wir die Übersendung des automatisiert erstellten Aktenauszugs per Briefpost vorgeschlagen, da über Unfallverursacher, Unfallgegner, Opfer und Zeugen regelhaft besonders schutzbedürftige Daten mitgeteilt werden, z. B. über Alkoholisierung eines Fahrzeugführers, Verkehrsunfallflucht oder gesundheitliche Unfallfolgen.

Darüber hinaus haben wir zahlreiche Verbesserungsvorschläge eingebracht. Zur Registrierungsdatei haben wir eine ausreichende Information und die Einwilligung der Firmenkunden in die Speicherung ihrer personenbezogenen Daten gefordert. Dies betrifft zum Beispiel die Speicherung von Angaben über Gebührenzahlungsverhalten oder über den Entzug der Zulassung als Firmenkunde in der Registrierungsdatei oder die Protokollierung und Speicherung von Nutzungsdaten. Firmenkunden müssen bei jeder Anfrage ausdrücklich bestätigen, dass sie im konkreten Einzelfall aufgrund einer anwaltlichen Vertretung oder aufgrund eines bestehenden Versicherungsverhältnisses auskunftsberechtigt sind. Die Notwendigkeit einiger vorgesehener Angaben in der standardisierten Aktenkurzinformation haben wir kritisch hinterfragt.

Von November 2006 bis März 2007 wurde das Projekt zur Klärung der rechtlichen Fragen zurückgestellt. Im Juli 2007 wurden uns eine geänderte Verfahrensbeschreibung und Risikoanalyse zum Verfahren „Polizeiliche Aktenkurzinformation Verkehrsunfall (PAV)“ überlassen, die allerdings neue Fragen aufwarfen. Es wurde nicht deutlich, ob dieses Verfahren mit neuem Namen beide bisher geplanten Verfahren, nämlich das Registrierungs- und das Auskunftsverfahren, umfassen soll. Nachdem uns im September 2007 bekannt wurde, dass mit der inzwischen erfolgten Signaturkarteneinführung im HamburgGateway die dritte Schutzstufe eingerichtet wurde, haben wir gegenüber der Polizei alle noch nachbesserungsbedürftigen Punkte verdeutlicht. Wir werden die

Polizei weiterhin bei der Verwirklichung eines effizienten, datenschutzgerechten Verfahrens unterstützen.

9. Verfassungsschutz

9.1 Antiterrorgesetze und Novellierung des Verfassungsschutzgesetzes

Die Novellierung des Hamburgischen Verfassungsschutzgesetzes zum Jahresende 2007 begegnet grundsätzlichen datenschutzrechtlichen Einwänden sowie Bedenken im Detail, die nur teilweise ausgeräumt wurden.

Das Terrorismusbekämpfungsgesetz von 2002 hatte den Verfassungsschutzbehörden eine Reihe neuer Eingriffsbefugnisse – etwa Auskunftsrechte gegenüber Banken, Postdienstleistern, Telekommunikationsanbietern und Luftfahrtunternehmen sowie die Handy-Ortung – eingeräumt, diese aber zugleich auf Ende 2007 befristet und eine Evaluierung vorgesehen. Das „Terrorismusbekämpfungsergänzungsgesetz“ vom 5. Januar 2007 hob die Befristung unter Heranziehung eines – von den Datenschutzbeauftragten als unzureichend kritisierten – Evaluationsberichts wieder auf und führte zunächst zu einer Novellierung des Bundesverfassungsschutzgesetzes. Die Landesgesetzgeber folgten dem.

Die Behörde für Inneres gab einen entsprechenden Gesetzentwurf, der die Befugnisse des Verfassungsschutzes ein weiteres Mal erweitern sollte, Anfang Juli 2007 in die Behördenabstimmung. Im Zuge dieser Beratungen konnten einige Datenschutzprobleme entschärft werden: So wurde eine neue Befugnis zur Übermittlung von Erkenntnissen an private Unternehmen ebenso zurückgenommen wie eine Einschränkung des sogenannten Kernbereichsschutzes privater Lebensgestaltung im Bereich der akustischen Wohnraumüberwachung.

Dennoch verblieben vor allem zwei gravierende Beeinträchtigungen des informationellen Selbstbestimmungsrechts, denen auch der Senat nicht abhalf. Da der Senat in die entsprechende Mitteilung an die Bürgerschaft keinen Hinweis auf unsere Bedenken aufnahm, haben wir uns nach § 23 Abs.3 HmbDSG direkt an die Bürgerschaft gewandt und die Einwände im Innenausschuss vorgetragen:

Zum einen geht es um die Umsetzung des Bundesverfassungsgerichtsurteils vom 3. März 2004. Das Gericht stellte fest: „Zur Unantastbarkeit der Menschenwürde gem. Art.1 Abs.1 GG gehört die Anerkennung eines absolut geschützten Kernbereichs privater Lebensgestaltung“. In diesen Kernbereich darf der Staat prinzipiell nicht eingreifen. Der vorgelegte Gesetzentwurf berücksichtigt dies zwar im Bereich der akustischen Wohnraumüberwachung; der Schutz der Menschenwürde ist aber unteilbar und muss bei allen verdeck-

ten Informationserhebungen des Staates gleichermaßen eingehalten werden. Wir haben deswegen eine allgemeine Vorbehalts- bzw. Begrenzungsvorschrift für alle geheimen Ermittlungsmaßnahmen („nachrichtendienstliche Mittel“) gefordert, die in § 8 Abs. 1 HmbVerfSchG hätte aufgenommen werden müssen.

Zum anderen geht es um die Erweiterung der Auskunfts- und Datenerhebungsrechte des Verfassungsschutzes in dessen allgemeinen Aufgabenbereich der Bekämpfung von Bestrebungen gegen die freiheitliche demokratische Grundordnung (§ 4 Abs. 1 Nr. 1 HmbVerfSchG). Der Versuch, diese neue Befugnis tatbestandlich auf Bestrebungen, die Gewalt fördern oder anwenden, zu begrenzen, führt zu einer Normstruktur, die weder überschaubar noch praktisch umsetzbar ist. Sie verstößt eklatant gegen die vom Bundesverfassungsgericht gerade im Bereich der informationellen Selbstbestimmung geforderten Normenklarheit und -bestimmtheit. Wir haben Senat und Bürgerschaft dies anhand eines Beispielsfalls verdeutlicht: Verlangt das Landesamt für Verfassungsschutz z.B. von einem Telekommunikationsanbieter Auskunft über eine bestimmte Person, dann hat es unter anderen folgende Tatbestandsmerkmale zu prüfen bzw. kann sich auf diese stützen:

Die Auskunft ist erforderlich zur Aufklärung einer Bestrebung, die – ausweislich tatsächlicher Anhaltspunkte – die freiheitliche demokratische Grundordnung durch ihre Eignung zur Gewaltvorbereitung schwerwiegend gefährdet, indem sie (die Bestrebung) Vereinigungen unterstützt, welche Anschläge gegen Sachen befürwortet, und sich gegen eine Person richtet, von der aufgrund bestimmter Tatsachen anzunehmen ist, dass sie die Leistung (z.B. einen Teledienst) für eine dritte Person nutzt, zu der wiederum tatsächliche Anhaltspunkte dafür vorliegen, dass sie die schwerwiegende Gefahr (s.o.) nachdrücklich fördert.

Diese Häufung und Kombination von unbestimmten Rechtsbegriffen und Verweisen macht die Norm und ihre Anwendung sowohl für die betroffenen Personen als auch für Mitarbeiter des Verfassungsschutzes, die über die Einholung der Auskunft entscheiden sollen, unberechenbar. Niemand kann hier sinnvoll prüfen, ob das Auskunftsverlangen des Verfassungsschutzes im Einzelfall gesetzlich zulässig ist oder nicht. Damit verstößt die Norm – wie auch die entsprechende Norm des Bundesverfassungsschutzgesetzes – gegen das Grundrecht auf informationelle Selbstbestimmung und gegen das Rechtsstaatsgebot.

9.2 Leicht erfasst, schwer gelöscht

Erkenntnisse des Verfassungsschutzes, die für die Betroffenen gravierende Auswirkungen haben können, beruhen oft auf unbeweisbaren, aber auch nicht zu widerlegenden „Anhaltspunkten“ und Bewertungen.

Immer wieder wandten sich vor allem Ausländer an uns, die wegen eines belastenden Hinweises des Landesamtes für Verfassungsschutz (LfV) z.B. kein

Visum für eine Einreise erhielten, nicht eingebürgert wurden oder während der Fußballweltmeisterschaft ihrem Beruf in einer Cateringfirma nicht ausüben durften. Das von den Betroffenen in Anspruch genommene Auskunftsrecht gegenüber dem LfV ist aus Sicherheitsgründen eingeschränkt. Der Hamburgische Datenschutzbeauftragte ist jedoch befugt, in jedem Einzelfall Einsicht in die die Erkenntnisse des LfV zu nehmen und der betroffenen Person mitzuteilen, ob diese plausibel und nachvollziehbar sind. Nicht immer war dies der Fall.

So bestanden folgenreiche Erkenntnisse z.B. darin, dass im Einreisefall zwar nicht der Betroffene selbst, aber die einladende Person in Hamburg als Unterstützerin des Islamischen Zentrums Hamburg an der Außenalster gilt, das das LfV als Arm der „Islamistischen Revolution" bewertet. Auch wer regelmäßig die Quds-Moschee – nach Beurteilung des LfV ein Treffpunkt von islamistischen, auch gewaltbereiten Djihadisten – besucht und dort Kontakte zu Gläubigen pflegt, gibt bereits Anhaltspunkte für eine verfassungsfeindliche Bestrebung. Andere Erkenntnisse wie etwa eine Mitgliedschaft im „Volkshaus e.V." – Anlaufstelle gewaltbereiter Kurden in Hamburg – wurden von den Betroffenen plausibel und mit Dokumenten bestritten. Nicht selten beruhen die Erkenntnisse des LfV auf Berichten von V-Leuten, die (gesellschaftliche) Kontakte der betroffenen Person mit Islamisten, „Gefährdern" oder „Extremisten" selbst beobachteten oder auch nur von einem solchen Umgang hörten.

Der Verfassungsschutz hat die gesetzliche Aufgabe, Bestrebungen gegen die freiheitliche demokratische Grundordnung oder die Sicherheit der Bundesrepublik möglichst frühzeitig zu erkennen, dafür Informationen zu sammeln und entsprechende Erkenntnisse auszuwerten.

Dabei ist das LfV nicht auf Beweise oder Indizien beschränkt, sondern darf in einer Gesamtschau verschiedene „tatsächliche Anhaltspunkte", die je für sich nicht stichhaltig sein müssen, kombinieren und zur Überzeugung verdichten, dass eine Person Extremist, Islamist oder Gefährder ist. Das datenschutzrechtliche Problem dabei ist, dass das LfV aufgrund dieser personenbezogenen Daten über die bloße Informationsgewinnung hinaus folgenschwere Hinweise an andere Behörden und Stellen übermittelt.

In Gesprächen mit dem LfV haben wir in Einzelfällen eine Rücknahme des negativen Hinweises erreicht, die Einseitigkeit bestimmter Erkenntnisse bzw. ihrer Bewertung verdeutlichen können und insgesamt gefordert, dass vor einer Weitergabe von verfassungsschutzrechtlichen Bedenken an Dritte die betroffene Person möglichst weitgehend Gelegenheit zu einer Stellungnahme erhält. Auch sollten negative Hinweise an Dritte nicht ausschließlich auf den bloßen Kontakt zu anderen verdächtigen Personen gegründet, sondern erst dann abgegeben werden, wenn sich die Bedenken auch aus eigenen Äußerungen und / oder gefährdendem Verhalten der betroffenen Person ergeben. Angesichts der Folgenschwere mancher Hinweise des LfV wären dies Maß-

nahmen, die die Verhältnismäßigkeit und Angemessenheit des Verwaltungshandelns deutlich erhöhten.

Bei der Bewertung der verfassungsschutzrechtlichen Erkenntnisse darf sich der Datenschutzbeauftragte sicher nicht an die Stelle des LfV setzen. Er hat aber die Aufgabe, Nachvollziehbarkeit und Plausibilität der Beurteilungen auch vor dem Hintergrund der Argumente und Erläuterungen des Betroffenen zu prüfen. Dies gilt umso mehr, als eine (vorzeitige) Löschung von belastenden, aber nicht beweiskräftigen Einzelinformationen nach den Verfassungsschutzgesetzen kaum erreichbar ist, wenn sie – aus Sicht des LfV – zusammen mit anderen Beobachtungen und Erkenntnissen zu einem negativen Gesamtbild führen. Die Frage, was wir der betroffenen Person von unseren Prüfungserkenntnissen mitteilen dürfen, hat das LfV bisher eher großzügig beantwortet. Im Übrigen ist die Beschränkung bei der Weitergabe von uns hinzunehmen, die seltene Anregung, einen Rechtsanwalt einzuschalten, aber möglich.

10. Justiz

10.1 Strafermittlungen mit Hilfe eines privaten Vereins für Urheberrechtsschutz

Die datenschutzrechtliche Kritik an einer zu weitgehenden Beteiligung Privater in strafrechtliche Ermittlungen führte zu einer erhöhten Sensibilisierung und zurückhaltenderen Praxis bei den Strafverfolgungsbehörden.

Durch Beschwerden aus anderen Bundesländern sind wir auf eine problematische Praxis der Strafverfolgungsbehörden im ganzen Bundesgebiet aufmerksam geworden: Bei Ermittlungen wegen Verstoßes gegen das Urheberrecht schalten Staatsanwaltschaft und Polizei häufig einen Verein ein, der sich auf die zivilrechtliche Verfolgung von Urheberrechtsverletzungen spezialisiert hat. Mitarbeiter dieses Vereins wurden zum Teil sogar zu Beschlagnahmen vor Ort hinzugebeten, ihnen wurden Datenträger wie Videos, DVD, CD und Festplatten, aber zuweilen auch ganze Rechner übergeben sowie Name und Adresse beschuldigter Personen mitgeteilt. Der Verein vertritt seine Mitglieder aus der Film- und Computerspiel-Branche und hat die Aufgabe und das Know-how, Verstöße gegen das Urheberrecht festzustellen und für die Verletzten Strafantrag zu stellen. Da der Verein seine Dienste kostenlos anbietet, greifen Strafverfolgungsbehörden gerne auf seine Sachkenntnis zurück.

Datenschutzrechtlich problematisch ist diese Praxis dann, wenn der Verein

- bereits vor der Feststellung einer Rechtsverletzung die Identität des Beschuldigten erfährt,
- durch die Anwesenheit bei Durchsuchungen und Beschlagnahmen darüber hinaus die Wohn- bzw. Geschäftssituation des Beschuldigten kennenlernt,

- so umfassendes Material zur Prüfung erhält, dass dadurch auch nicht strafverfolgungs-relevante Informationen aus dem persönlichen Bereich des Beschuldigten offenbart werden (Festplatten),

- vor einer förmlichen Beendigung der Ermittlungen durch die Staatsanwaltschaft den Rechteinhabern die Identität der Rechtsverletzer mitteilt.

Die Hamburger Staatsanwaltschaft berichtete uns auf Anfrage, dass auch sie den Verein im Rahmen ihrer „Ermittlung jeder Art“ (§ 161 Abs.1, 163 Abs.1 der Strafprozessordnung) als „andere Stelle“ hinzuziehe. Dazu würden den Vereinsvertretern aber nur die mutmaßlichen Raubkopien selbst, also die gesonderten Datenträger, übergeben, nicht aber PCs oder Festplatten. Offen blieb, ob dem Verein auch die Personalien der Beschuldigten mitgeteilt werden. Staatsanwaltschaften anderer Bundesländer werteten die Dienste des Vereins teils als Sachverständigen-Äußerungen, teils als Zeugenaussagen und räumten ihm als Vertreter der Verletzten ein Akteneinsichtsrecht (§ 406 e StPO) ein.

Auf unsere Initiative behandelten die Datenschutzbeauftragten des Bundes und der Länder das Thema in ihrem Arbeitskreis Justiz. Es ergab sich weitgehende Übereinstimmung in der rechtlichen Bewertung, dass eine Einbeziehung des Vereins auf das notwendige Maß zu beschränken ist. Je nach Fragestellung und notwendiger Spezialkenntnis mag für den Verein im Einzelfall eine Sachverständigenfunktion (z.B. bei der notwendigen Überwindung von technischen Sicherungen), eine Zeugenaussage (Wer ist Rechtsinhaber? Wann ist das Werk erschienen?) oder auch nur eine Funktion als bloßer „Augenscheinsgehilfe“ (DVD-Etikett als Anzeichen für eine Raubkopie) in Betracht kommen. Eine Übergabe von Rechnern und Festplatten mit „überschießenden“ Informationen ist aber weder erforderlich noch zulässig. Akteneinsicht während der Ermittlungen ist nur einem Rechtsanwalt mit ausdrücklicher Vollmacht des Verletzten zu gewähren. Für die Feststellung oder den Ausschluss einer Rechtsverletzung muss der Verein auch die Identität des Beschuldigten nicht kennen. Die Anwesenheit von Vereinsvertretern bei polizeilichen Durchsuchungen und Beschlagnahmen ist grundsätzlich zu vermeiden. Insgesamt muss die Strafverfolgungsbehörde stets „Herr des Verfahrens“ bleiben.

Diese Rechtsauffassung vertrat auch ein Vertreter der Münchener Staatsanwaltschaft in einem ausführlichen Vortag vor dem Arbeitskreis der Datenschutzbeauftragten. Er bestätigte, dass seit der datenschutzrechtlichen Kritik und aufgrund entsprechender Rechtsprechung eine vorsichtigere und datenschutzfreundlichere Haltung bei Strafverfolgungsbehörden zu beobachten sei. Dennoch ist eine flächendeckende Verbreitung der datenschutzgerechten Verfahrensweise in allen Bundesländern noch nicht gesichert.

10.2 Einsicht in Strafermittlungsakte durch den Vermieter des Beschuldigten

Die Staatsanwaltschaft gewährte dem Vermieter eines Beschuldigten rechtswidrig Einsicht in die Ermittlungsakte, was zur fristlosen Kündigung führte.

Die Staatsanwaltschaft ermittelte 2006 gegen einen Beschuldigten wegen des Verdachts des Betäubungsmittelmissbrauchs. In der Ermittlungsakte befanden sich Zeugenaussagen, die Anordnung der Wohnungsdurchsuchung, die Auswertung der Handy-Telefonverzeichnisse und eine psychiatrische Stellungnahme des Universitätsklinikums Hamburg-Eppendorf. Auf Antrag der Vermieterin des Beschuldigten, einer Wohnungsgesellschaft, gewährte ihr die Staatsanwaltschaft Einsicht in die gesamte Ermittlungsakte. Die Vermieterin kündigte dem Beschuldigten daraufhin fristlos.

Die Akteneinsicht durch Private und sonstige Stellen ist in § 475 Strafprozessordnung geregelt. Sie darf nur gewährt werden, wenn der Antragsteller ein berechtigtes Interesse darlegt und der hiervon Betroffene kein „schutzwürdiges Interesse an der Versagung“ hat. Zumindest hinsichtlich der psychiatrischen Stellungnahme des UKE hatte der Beschuldigte ein erhebliches Interesse an ihrer Geheimhaltung. In der Abwägung mit dem Interesse der Vermieterin wurde dies nicht hinreichend berücksichtigt.

Die von uns erbetene Stellungnahme des Leitenden Oberstaatsanwaltes sah dies ebenso. Mit Beschluss vom 26. Oktober 2006 wies – in anderer Sache – auch das Bundesverfassungsgericht darauf hin, dass es einer Abwägung der Interessen und ggf. einer angemessenen Beschränkung des Zugangs zu den Beschuldigten-Daten bedarf: „Wird durch die Gewährung der Akteneinsicht in Grundrechte Betroffener eingegriffen, sind diese in der Regel anzuhören.“

Dies teilten wir dem Anwalt des Beschuldigten auf seine Anfrage mit. Im Juni 2007 erwirkte der Anwalt einen Feststellungsbeschluss des Landgerichts, der unsere Auffassung bestätigte.

10.3 Hamburgisches Maßregelvollzugsgesetz

Der Hamburgische Datenschutzbeauftragte hat bei der Novellierung des Hamburgischen Maßregelvollzugsgesetzes einige datenschutzrechtliche Verbesserungen erreicht, sich mit seiner Forderung, eine Videoüberwachung von Wohn- und Schlafräumen der untergebrachten Personen zu unterlassen, aber nicht durchsetzen können.

Die Hamburgische Bürgerschaft hat am 30. August 2007 die Novellierung des Hamburgischen Maßregelvollzugsgesetzes beschlossen. Der Hamburgische Datenschutzbeauftragte war mit dem Gesetzesvorhaben seit November 2004 befasst.

Von Beginn an hatten wir verfassungsrechtliche Bedenken gegen die vorgesehene Beleihung eines Privaten mit den Aufgaben des Maßregelvollzugs. Diese Bedenken sind allerdings keine datenschutzrechtlichen, sondern allgemein verfassungsrechtliche Bedenken. Der datenschutzrechtliche Aspekt liegt aber darin, dass wie gefordert haben, im Falle des Festhaltens an einer Beleihung eines Privaten zumindest sicherzustellen, dass der Private datenschutzrechtlich wie eine öffentliche Stelle behandelt wird mit der Folge, dass für ihn die entsprechende Anwendung des Hamburgischen Datenschutzgesetzes festgelegt wird. Dieser Forderung ist die Bürgerschaft mit der Schaffung des § 4 Abs. 6 nachgekommen.

Wir haben darüber hinaus im Rahmen der mehrfachen Abstimmung des Gesetzentwurfes datenschutzrechtliche Verbesserungen für eine Vielzahl von Normen vorgeschlagen und auch erreicht. So haben wir in § 9 vorgeschlagen, dass der nach jeweils fünf Jahren einzuschaltende Gutachter nicht nur extern, sondern auch ansonsten mangels Vorbefassung mit der untergebrachten Person völlig unvoreingenommen sein soll. Außerdem haben wir eine Reduzierung der Löschungsfrist in § 47 von dreißig auf zwanzig Jahre vorgeschlagen, die zwar immer noch sehr lang ist, aber im Hinblick auf § 184 Strafvollzugsgesetz vertretbar.

Nicht durchsetzen konnten wir uns mit unseren Vorschlägen zur Ausgestaltung der Videoüberwachung. So ist zwar zu begrüßen, dass eine Rechtsgrundlage für die Videoüberwachung im Maßregelvollzug ausdrücklich in das Gesetz aufgenommen wurde. Diese erweist sich aber als nicht datenschutzgerecht und verfassungsgemäß. So ist die Aufzeichnung der Videoüberwachung von Besuchern unverhältnismäßig, hier würde die Videobeobachtung des Besuchs ausreichen. Völlig unvertretbar ist § 40 a, der den Einsatz von optisch-elektronischen Einrichtungen zur Überwachung in Wohn- und Schlafräumen von untergebrachten Personen zulässt. Eine Videoüberwachung von Wohn- und Schlafräumen ist ein massiver Eingriff in das Persönlichkeitsrecht der untergebrachten Personen, der durch nichts zu rechtfertigen ist. Sollten ausnahmsweise akute Gefahren für Leib und Leben eine Videobeobachtung einer untergebrachten Person zwingend erfordern, so wäre dies ausschließlich in einem besonderen Beobachtungsraum zulässig.

10.4 Hamburgisches Strafvollzugsgesetz

Beim Erlass des neuen Strafvollzugsgesetzes konnten bei den vorgesehenen Regelungen zur Videoüberwachung zwar leichte Verbesserungen erreicht werden, mit der in § 120 Absatz 3 beschlossenen Videoüberwachung von Hafträumen verstößt das Gesetz aber gegen das allgemeine Persönlichkeitsrecht der Gefangenen in seiner Ausprägung als Recht auf informationelle Selbstbestimmung.

Die Ergebnisse der Föderalismusreform haben zu einer Übertragung der Gesetzgebungszuständigkeit im Strafvollzug auf die Länder geführt. Von dieser neuen Zuständigkeit hat auch Hamburg Gebrauch gemacht. Wir haben das Gesetzgebungsverfahren von Anfang an begleitet.

Da der Senat von einer Videoüberwachung im Strafvollzug nicht absehen wollte, begrüßen wir, dass ausdrückliche Regelungen für die Videoüberwachung in das Strafvollzugsgesetz aufgenommen wurden. Die Regelung der Videoüberwachung von Hafträumen geht jedoch mit ihrem unverhältnismäßigen Eingriff in die Privatsphäre der Gefangenen und in ihr Recht auf informationelle Selbstbestimmung weit über das verfassungsrechtlich Zulässige hinaus.

Die Videoüberwachung muss ausschließlich an die Erforderlichkeit zur Aufrechterhaltung der Sicherheit und Ordnung der Anstalt geknüpft werden. Wegen des Schutzes der Privatsphäre und des Schutzes des Kernbereichs privater Lebensgestaltung ist eine Videoüberwachung von Hafträumen unzulässig und auszuschließen. Denkbar erscheint, bestimmte Räume offen mit Videoüberwachung auszustatten, in die Gefangene im Einzelfall im Rahmen besonderer Sicherungsmaßnahmen zeitlich begrenzt verlegt werden können. Nicht hinzunehmen ist ferner unter den Bedingungen der gesicherten Anstalt eine nicht offene, d.h. versteckt bzw. geheim durchgeführte Videoüberwachung, wie sie in § 120 Absatz 3 Satz 3 vorgesehen wurde.

10.5 Zahnarztkartei für Strafgefangene

In den Hamburger Justizvollzugsanstalten wurden auf den bei Zahnbehandlungen von Gefangenen genutzten Karteikarten überflüssige Daten erfasst.

Aufgrund der Eingabe eines Strafgefangenen erhielten wir Kenntnis von den in den Hamburger Justizvollzugsanstalten bei Zahnbehandlungen von Gefangenen genutzten Karteikarten. Diese enthielten neben den medizinischen Angaben auch Felder über Vorstrafen, Delikte oder das Strafmaß der jeweiligen Gefangenen. Auf Nachfrage erklärte die Justizbehörde, dass der Karteivordruck in der Praxis nicht vollständig ausgefüllt werde. Es würden nur die Haftdaten erhoben, da diese für die Planung der Behandlung von Bedeutung seien. Diese Vorgehensweise vermochte uns im Hinblick auf den Grundsatz des sparsamen Umgangs gerade mit personenbezogenen Daten nicht zu überzeugen. Wir forderten daher die Justizbehörde auf, den Vordruck so zu überarbeiten, dass nur noch behandlungsbezogene Daten erhoben werden. Dieser Aufforderung kam die Justizbehörde nach. Der Vordruck wurde überarbeitet. Für die Übergangszeit wurden alle Justizvollzugsanstalten Hamburgs angewiesen, die nicht erforderlichen Daten nicht zu erheben.

Dieser Vorgang zeigt, dass wir in vielen Fällen zur Durchsetzung eines datenschutzkonformen Verhaltens der Behörden auf Eingaben der Betroffenen angewiesen sind.

11. Bauen und Wohnen

11.1 Datenschutzprobleme beim Verkauf von Erbbaugrundstücken an die Erbbauberechtigten

Zur Vorbereitung des Verkaufs von Erbbaugrundstücken übermittelte die Liegenschaftsverwaltung die Personalien der Erbbauberechtigten ohne deren Kenntnis an ein Maklerunternehmen.

Aufgrund zweier Beschwerden von Erbbauberechtigten im Jahre 2006 wurden wir auf das „Aktionsmodell" der Liegenschaftsverwaltung zum Verkauf von Erbbaugrundstücken aufmerksam. Nach entsprechenden Beschlüssen der Bürgerschaft hatte die Finanzbehörde 2004 Dienstleistungen ausgeschrieben, die den Verkauf von ca. 5000 Einfamilienhausgrundstücken an die Erbbauberechtigten vorbereiten sollten: Ermittlung der Kaufpreise, Erstellung von Angeboten, Durchführung der Kaufverhandlungen, Wahrnehmung der Notartermine und anderes. Unter „Arbeitsmaterial und Arbeitsorganisation" hieß es in den Ausschreibungsunterlagen: „Für das Portfolio wird die FHH dem Auftragnehmer die Grundstücke sowie die Erbbaurechtsnehmer benennen". Nach Erteilung des Zuschlags erhielt der Auftragnehmer die Daten der Erbbauberechtigten. Erst danach teilte die Finanzbehörde den Berechtigten mit, dass die Liegenschaft die Firma X „als kompetenten Partner gewinnen" konnte und dieser „in den nächsten Tagen mit Ihnen Kontakt aufnehmen" werde.

Der Auftragnehmer hatte Aufgaben der Liegenschaftsverwaltung übernommen, die langjährige Erfahrung und spezifische Sachkenntnis erforderten und eine nicht geringe Gestaltungs- und Entscheidungsfreiheit umfassten. Deswegen war nicht davon auszugehen, dass der Auftragnehmer nur „verlängerter Arm" der Liegenschaftsverwaltung und streng ihrer Weisung und Kontrolle unterworfen war. Damit kam datenschutzrechtlich eine Auftragsdatenverarbeitung, bei der die Verantwortung allein beim Auftraggeber blieb, nicht in Betracht. Vielmehr handelte es sich bei der Weitergabe der Personalien datenschutzrechtlich um eine Übermittlung an einen privaten Dritten, die in das informationelle Selbstbestimmungsrecht der Betroffenen eingriff und daher einer Einwilligung oder einer gesetzlichen Ermächtigung bedurfte.

Eine Einwilligung war nicht eingeholt worden. Über das Vorliegen einer gesetzlichen Ermächtigung zur Datenübermittlung konnten wir uns mit der Finanzbehörde nicht einigen. Nach unserer Rechtsauffassung fehlte es an einer Übermittlungsberechtigung: Dafür wäre mangels spezialgesetzlicher Eingriffsermächtigungen nur die Generalklausel des § 16 Hamburgisches Daten-

schutzgesetz in Betracht gekommen. Nach § 16 Abs.1 Nr.1 HmbDSG darf eine öffentliche Stellen personenbezogene Daten an Private nur übermitteln, wenn dies für die Erfüllung der Aufgaben der übermittelnden Stelle erforderlich ist und die Daten zu demselben Zweck übermittelt werden, für den sie erhoben wurden. Fordert man, dass gerade die Übermittlung „ohne Einwilligung" erforderlich sein muss – dies würde dem Grundrecht auf informationelle Selbstbestimmung am ehesten entsprechen -, dann ist von der Unzulässigkeit der Übermittlung auszugehen. Angesichts des Umfangs der gesamten Aktion wäre die vorherige Bitte an die 5000 Erbbauberechtigte um ihre Einwilligung keineswegs unzumutbar gewesen.

Nicht teilen konnten wir auch die Auffassung der Finanzbehörde, die Übermittlung der Berechtigtendaten hätte dem gleichen Zweck gedient wie die Erhebung dieser Daten. Dies wäre nur dann möglich gewesen, wenn man den ursprünglichen Erhebungszweck, nämlich die Eingehung und Durchführung des Erbbaurechtsverhältnisses, stark überdehnen und auch auf die Auflösung des Verhältnisses durch Verhandlungen mit einer unbekannten privaten Maklerfirma erstrecken könnte. Dies wäre realitätsfremd und nicht datenschutzgerecht. Wie ein Mieter geht auch der Erbbauberechtigte grundsätzlich davon aus, dass er nur mit seinem Vertragspartner – hier der Liegenschaft – über Vertragsänderungen kommuniziert und nicht über einen unbekannten Dritten. Ein solch weitreichender Auftrag, wie ihn die Finanzbehörde in ihrem „Aktionsmodell" erteilte, war nicht im Bewusstsein der Erbbauberechtigten bei Abschluss des Erbbauvertrages mit der Liegenschaft. Damit stellt die Übermittlung der persönlichen Berechtigtendaten durch die Finanzbehörde an einen privaten Dritten eine Zweckänderung dar, die nach § 13 HmbDSG nur unter bestimmten Voraussetzungen zulässig gewesen wäre, die hier aber nicht vorliegen.

Nahe gelegen hätte eine Inanspruchnahme des § 16 Abs.1 Nr.4 HmbDSG: Danach darf ohne Einwilligung übermittelt werden, wenn dies im öffentlichen Interesses liegt und die Betroffenen nicht widersprochen haben. Könnte man angesichts der Komplexität und des Umfangs der Aktion das öffentliche Interesse an der Beauftragung eines erfahrenen Unternehmens bejahen, hat es die Finanzbehörde jedoch versäumt, die Betroffenen vorher „über die beabsichtigte Übermittlung, die Art der zu übermittelnden Daten und den Verwendungszweck in geeigneter Weise zu unterrichten", § 16 Abs.1 Satz 2.

11.2 Übermittlung von Grundbuchauszügen zu Nachbar-Grundstücken

Die Praxis der Grundbuchämter, Grundbuchauszüge auch zu den Miteigentumsanteilen von Nachbarn zu erteilen, wurde aufgrund unserer Initiative aufgegeben.

Ausgangspunkt war folgender Sachverhalt: Ein Eigentümer eines Reihenhauses beantragte beim Grundbuchamt einen Grundbuchauszug. Die Abschriften vom Registergericht bezogen sich jedoch nicht nur auf das eigene Reihen-

haus, sondern auch auf die Grundstücke der Nachbarn. Die Auszüge offenbarten neben Größe, Lage und Eigentumsverhältnissen auch die eingetragenen Hypotheken einschließlich des Rangs und der zugrunde liegenden Forderderungen.

Grund für diese Übermittlung fremder Daten war, dass der Antragsteller zugleich Miteigentümer eines zum Reihenhausgrundstück gehörenden Garagenhofes war und für dieses Hofgrundstück ein eigenes Grundbuchblatt mit allen Miteigentümern besteht. Belastungen wie Hypotheken wurden als Gesamtrecht jeweils für beide Grundstücke eingetragen (Reihenhaus und Hof-Miteigentum). Dies war früher insbesondere Praxis bei Verkäufen von Liegenschaftsgrundstücken der Hansestadt. Wünscht nun der Eigentümer eines Reihenhauses einen Grundbuchauszug ohne nähere Angaben, erhielt er bislang tatsächlich beide Grundbuchauszüge und erfuhr so, für welche Schulden seine Nachbarn ihr Grundstück (Reihenhaus und Hof-Anteil) belasteten.

Wir haben diese Praxis kritisiert und angeregt, einem anfragenden Eigentümer zunächst ausschließlich den Grundbuchauszug zu seinem Hausgrundstück zu übermitteln – verbunden mit dem Hinweis, dass ihm auch noch ein Miteigentumsanteil an einer Gemeinschaftsfläche zustehe und dazu ein eigenes Grundbuchblatt – allerdings mit den Daten aller anderen Miteigentümer – existiere. Im Übrigen sollte – wie es heute auch überwiegend geschieht – die Möglichkeit der Grundbuchordnung genutzt werden, den Miteigentumsanteil am Hof zusammen mit dem Eigentum am Reihenhaus auf einem gemeinsamen Grundbuchblatt einzutragen.

Das betroffene Amtsgericht nahm unseren Vorschlag auf und beschränkt erbetene Grundbuchauszüge zur Klärung von Sicherheiten nun grundsätzlich auf das Hausgrundstück. Da es sich hier um ein prinzipielles Problem handelt, hat das Gericht auf unsere Bitte auch die Geschäftsleitungen der anderen Hamburger Amts- und Stadtteilgerichte unterrichtet.

11.3 Veröffentlichung von Geo- und Grundstücksdaten

Der Aufbau einer technischen Geodateninfrastruktur und ihre Verbindung zu Fachverwaltungen werfen schwierige datenschutzrechtliche Fragen auf, deren Beantwortung erst am Anfang steht.

Die neuen technischen Möglichkeiten der digitalen Erfassung, Darstellung und Verknüpfung von geografischen Daten mit anderen Informationen bedeuten für die Definition und den Schutz „personenbezogener Daten“ eine neue Bewährungsprobe. Einerseits hat die Wirtschaft hat großes Interesse an möglichst differenzierten georeferenzierten Informationen und die Öffentlichkeit ein durch Art. 5 des Grundgesetzes und die Informationsfreiheitsgesetze geschütztes Recht auf Information aus allgemein zugänglichen Quellen – etwa über die Standorte von Mobilfunksendemasten, über soziale und wirtschaft-

liche Stadt(teil)-Strukturen, über Umweltschäden in der Umgebung. Andererseits kann die Veröffentlichung räumlicher Merkmale im Einzelfall für Grundstückseigentümer große Bedeutung erlangen. Von der „Luftaufklärung“ nicht genehmigter Bauten, über wertbeeinflussende Daten zur Bodenbeschaffenheit und die Einbeziehung des Wohnstandorts in Scoring-Verfahren bis zur Erstellung von Bewegungsprofilen: die Aufbereitung und Veröffentlichung von Geodaten im Internet beinhalten auch Risiken für den Persönlichkeitsschutz.

Die Datenschutzbeauftragten des Bundes und der Länder versuchen derzeit, handhabbare Kriterien für eine datenschutzgerechte Nutzung von Geodaten zu erarbeiten. Die rechtliche Situation ist in den einzelnen Bundesländern verschieden. Gesetzliche Regelungen sind zum Teil sehr allgemein, zum Teil sehr speziell; einheitliche Standards fehlen. Ein Ausschluss des Personenbezugs bzw. der Schutzbedürftigkeit ist abhängig von der Art und Aufbereitung der Datenerfassung. Soweit Daten aus der Luft gewonnen werden – z.B. mit Bildaufnahmen durch Satelliten oder von Flugzeugen aus, ist sehr fraglich, ob sie noch „aus allgemein zugänglichen Quellen“ stammen und zur allgemeinen Nutzung freigestellt werden. Inzwischen ist die Bildauflösung meist so gewählt, dass einzelne Grundstücke identifiziert werden können. In diesen Fällen ist nicht mehr von einer Anonymisierung auszugehen.

Aufgrund einer europäischen Rahmenrichtlinie (INSPIRE) wird auf Bundesebene derzeit ein „Geodatenzugangsgesetz“ vorbereitet, das hinsichtlich des Datenschutzes auf das Umweltinformationsgesetz von 2004 verweist. Dort wird vor der Bekanntgabe personenbezogener Umweltinformationen eine Abwägung vorgeschrieben: Würde die Bekanntgabe die Interessen der Betroffenen erheblich beeinträchtigen, ist sie nur mit deren Einwilligung oder bei Überwiegen des öffentlichen Interesses zulässig.

In Hamburg bereitet der Landesbetrieb Geoinformation und Vermessung derzeit die technische und organisatorische Umsetzung der europäischen Rahmenrichtlinie vor. Eine standardisierte Geodateninfrastruktur soll es Nutzern ermöglichen, mit Fachdatenbanken zu kommunizieren sowie Geodaten zu selektieren, auszuwerten und mittels Internet-Technologie zur Verfügung gestellt zu bekommen. Als ein Instrument dafür wird das Geoportal der Metropolregion Hamburg entwickelt.

Da der Personenbezug von Geodaten und ihr Schutz in den Überlegungen des Landesbetriebes bisher nur eine geringe Rolle spielte, haben wir uns in einem Gespräch mit den Verantwortlichen ein Bild über den derzeitigen Planungsstand verschafft und durch Beispiele die Anliegen des Datenschutzes veranschaulicht. Derzeit sind in Hamburg (noch) keine datenschutzrechtlich problematischen Anwendungen der Geodateninfrastruktur erkennbar, die Kommunikation mit dem Landesbetrieb werden wir jedoch fortsetzen.

12. Soziales

12.1 Kindeswohlgefährdung

Datenschutz verhindert grundsätzlich keine Maßnahmen zur Erkennung und Verhinderung von Kindeswohlgefährdung.

Im Jahr 2005 hatte der Senat ein Bündel von Maßnahmen verabschiedet, um Jugendämter und andere Stellen besser in die Lage zu versetzen, im Falle einer Kindeswohlgefährdung schnell und wirksam zu handeln. Wir haben darüber berichtet (20. TB, 11.3). Zahlreiche Maßnahmen sind inzwischen umgesetzt worden, ohne dass dabei durchgreifende datenschutzrechtliche Probleme aufgetreten sind. Es handelt sich insbesondere um folgende Punkte:

- Einführung des Schulzwangs,
- Aufbau eines Zentralen Schülerregisters (vgl. 13.1),
- Datenaustausch mit Familienkassen,
- Spezielle Beziehungsgewaltsachbearbeiter an den Polizeikommissariaten, die sich um Fälle von Kindeswohlgefährdung kümmern,
- Konkretisierung des Schutzauftrags der Jugendhilfe bei Kindeswohlgefährdung,
- Verlängerung der Aufbewahrungsfristen für Akten in den Jugendämtern,
- Einrichtung einer Zentralen Kinderschutzhotline,
- Verbesserung der Zusammenarbeit zwischen der Polizei und der Staatsanwaltschaft mit dem Jugendamt,
- Bundesratsinitiative Hamburgs zur verbindlichen Ausgestaltung von Früherkennungsuntersuchungen bei Kindern,
- Entwicklung eines Leitfadens zur Erkennung von Kindeswohlgefährdungen in Kindertagesstätten,
- Erarbeitung einer Richtlinie zur Zusammenarbeit von Schulen und den Regionalen Beratungs- und Unterstützungsstellen mit den Jugendämtern,
- Festlegung schriftlicher Meldeverfahren bei fördern & wohnen, der ARGE SGB II und den Dienststellen der Fachämter für Grundsicherung und Soziales an die Jugendämter.

Diese Aufzählung zeigt, dass viele Informationsbeziehungen und Informationsgrundlagen verbessert werden konnten, die zu einer Stärkung der Handlungsmöglichkeiten zahlreicher Stellen geführt haben, ohne dass datenschutzrechtliche Gründe dem entgegenstanden. Nicht zuletzt durch unsere Beratung konnten die Projekte realisiert werden.

Ein vorgesehenes Projekt war jedoch datenschutzrechtlich unzulässig.

Im Bezirk Altona sollte modellhaft erprobt werden, ob regelmäßige Mitteilungen des Einwohneramtes an das Jugendamt über Geburten und Zuzüge von Kindern einen zusätzlichen Nutzen für das frühzeitige Erkennen von Kindeswohlgefährdung erbringen. Für eine solche Datenerhebung durch das Jugendamt war jedoch keine Rechtsgrundlage vorhanden: Gemäß § 62 Abs. 1 SGB VIII darf das Jugendamt Sozialdaten nur erheben, soweit ihre Kenntnis zur Erfüllung der jeweiligen Aufgabe erforderlich ist. Mit dem Begriff „jeweilige Aufgabe“ wird klargestellt, dass eine Datenerhebung stets einzelfallbezogen sein muss. Es soll sichergestellt werden, dass das Jugendamt keine Datenvorräte anlegt.

Der Modellversuch sah vor, die Meldedaten regelmäßig mit den Jugendamtsdaten abzugleichen. Ein derartiger genereller Datenabgleich ist jedoch nicht einzelfallbezogen. In den abschließenden Regelungen der §§ 11 bis 60 SGB VIII findet sich daher auch keine Aufgabe, die generelle Ermittlungen des Jugendamtes ohne Anhaltspunkte im Einzelfall erforderte. Der geplante Datenabgleich musste von uns daher als eine Datensammlung auf Vorrat moniert werden, eher einer Rasterfahndung vergleichbar, für die eine spezielle Rechtsgrundlage erforderlich wäre. Eine solche Rechtsgrundlage, wie etwa in § 52 SGB II, kennt das SGB VIII nicht.

Geprüft wurde auch, ob die dem Jugendamt gem. § 16 SGB VIII zugewiesene Aufgabe, Angebote zur Förderung der Familie bereitzustellen, weiterführt. Um derartige Angebote den in Betracht kommenden Familien in Form eines persönlich adressierten Anschreibens zu unterbreiten, benötigt das Jugendamt möglicherweise Adressdaten. Wir haben jedoch angezweifelt, ob ein solches Anschreiben zu den Aufgaben des Jugendamtes gehört. Um Familien nach der Geburt eines Kindes oder dem Zuzug mit einem Kind ein Formschreiben mit einem Angebot zur Förderung der Familie zuzusenden, genügt es, das Einwohneramt mit der Versendung des Schreibens zu beauftragen. Das wäre im Übrigen auch das Vorgehen, das das informationelle Selbstbestimmungsrecht der Betroffenen am wenigsten beeinträchtigte und somit dem hier ebenfalls zu beachtenden Grundsatz der Verhältnismäßigkeit entspräche.

Als Alternative wurde im Bezirk Altona ein Projekt entwickelt, mit dem in sozial benachteiligten Stadtteilen und Quartieren Netzwerke geschaffen bzw. bereits vorhandene Netzwerke so ausgebaut werden, dass die Hilfen auch Familien mit erhöhtem Unterstützungsbedarf erreichen. Für den Fall, dass ein Eingreifen erforderlich ist, ermöglichen verbindliche Kontrakte zwischen den Fachkräften des Netzwerkes eine frühe und abgestufte Intervention, um einer das Kindeswohl bedrohenden Gefahr rechtzeitig zu begegnen. Ein wesentliches Merkmal des auf zwei Jahre angelegten Projektes ist die Zusammenarbeit zwischen Gesundheitshilfe und Familienförderung bzw. Jugendhilfe. Der Zugang erfolgt in der Regel durch die Mütterberatungsstellen, aber auch über

Geburtskliniken, Schwangerenberatungsstellen und Hebammen. Dieses Projekt lässt sich datenschutzrechtlich unbedenklich durchführen.

12.2 Pflegedokumentation in Heimen

Einsicht in die Pflegedokumentation ist nur in engen datenschutzrechtlichen Grenzen zulässig.

Stationäre Pflegeeinrichtungen sind nach § 11 Abs. 1 Nr. 7 in Verbindung mit § 13 Abs. 1 Heimgesetz (HeimG) verpflichtet, über die Pflegebehandlung eine Pflegedokumentation zu führen. Es sind die Stammdaten der Bewohnerinnen und Bewohner zu erheben (§ 13 Abs. 1 Nr. 4 HeimG), die Verabreichung von Arzneimitteln aufzuzeichnen (§ 13 Abs. 1 Nr. 5 HeimG), die Pflegeplanungen und die Pflegeverläufe für pflegebedürftige Bewohner festzuhalten (§ 13 Abs. 1 Nr. 6 HeimG) und alle freiheitsbeschränkenden und freiheitsentziehenden Maßnahmen sowie die Angabe des für die Anordnung der Maßnahme Verantwortlichen (§ 13 Abs.1 Nr. 9 HeimG) zu dokumentieren. Aus der Pflegedokumentation muss somit jederzeit der lückenlose Verlauf und der Stand des Pflegeprozesses ablesbar sein. Eine so umfassende Pflegedokumentation enthält in aller Regel äußerst sensible Daten, die besonders schutzwürdig sind. Im Berichtszeitraum wurden wir insbesondere zu folgenden Punkten eingeschaltet:

1. Einwilligung in die Einsichtnahme durch Pflegekassen

Pflegekassen verlangen immer wieder, dass Pflegebedürftige darin einwilligen, der Kasse Einsicht in die Pflegedokumentation zu gewähren. So wurde uns beispielsweise folgendes Formular vorgelegt:

> Schweigepflichtentbindungserklärung und Herausgabegenehmigung
>
> Hiermit entbinde ich (Name und Geburtdatum) das Altenpflegeheim (Name und Anschrift) und alle Mitarbeiter(innen) des Heimes sowie alle Krankenhäuser und Ärzte, die mich im Zusammenhang mit meinem Aufenthalt im oben genannten Pflegeheim und/oder anlässlich meines Unfalls vom (Datum) gepflegt oder behandelt haben und/oder weiterhin pflegen oder behandeln, von der gesetzlichen Schweigepflicht gegenüber dem Medizinischen Dienst der Krankenversicherung (MDK) und erkläre gleichzeitig die Genehmigung zur Herausgabe der kompletten Pflegedokumentation und der ärztlichen Unterlagen an die Pflegekasse und an den MDK.
>
> Einer damit verbundenen Übermittlung meiner Patientendaten der Pflegekasse an den MDK, des Heimes sowie der behandelnden Ärzte an die Pflegekasse und den MDK sowie des MDK an die Pflegekasse stimme ich hiermit zu.

Eine Übermittlung der Pflegedokumentation an den Medizinischen Dienst der Krankenversicherung (MDK) ist ohne eine solche Erklärung zulässig. Der MDK darf personenbezogene Daten für Zwecke der Pflegeversicherung erheben, verarbeiten und nutzen, soweit dies für Prüfungen, Beratungen und gutachtliche Stellungnahmen – wie z.B. die Feststellung der Pflegebedürftigkeit oder die Notwendigkeit der Versorgung mit Pflegehilfsmitteln und technischen Hilfen – erforderlich ist. Ein Einsichtsrecht der Pflegekassen in die Pflegedokumentation ist dagegen gesetzlich nicht vorgesehen. Die Pflegekasse hatte offensichtlich deshalb das vorstehende Formular entwickelt, um auf diese Weise dennoch die Daten aus der Pflegedokumentation zu erhalten.

Das von der Pflegekasse mit dem Formular angestrebte Verfahren ist unzulässig. Im Zusammenhang mit der Anforderung von Krankenhausentlassungsberichten durch Krankenkassen hatten wir in der Vergangenheit bereits auf die Unzulässigkeit, hier Einwilligungserklärungen zu verlangen, hingewiesen (vgl. 19. TB, 6.1). Unsere Auffassung entspricht der Rechtsprechung des Bundessozialgerichts (zuletzt Urteil vom 28. Februar 2007, B 3 KR 12/06 R). Für eine Einwilligung durch den Pflegebedürftigen ist in diesem Zusammenhang – wie bei der gesetzlichen Krankenversicherung – kein Raum.

2. Qualitätsprüfung und Abrechnungsprüfung

Im Bereich der Pflegeversicherung gilt, dass die Pflegedokumentation unbedingt von den Abrechnungsunterlagen zu trennen ist. Da die Pflegedokumentation unter anderem Anamnese- und Diagnosedaten, also außerordentlich sensible Daten enthält, dürfen diese Daten nicht unnötig weiter verarbeitet werden. Auch eine Einsichtnahme der Pflegekasse in die Pflegedokumentation zur Überwachung der Wirtschaftlichkeit und Qualität der Leistungserbringung scheidet daher aus. Die Verfahren für diese Überprüfungen sind gesetzlich geregelt (§§ 79, 80 ff., 112 bis 115, 117 und 118 SGB XI). Danach ist es lediglich dem MDK bzw. den bestellten unabhängigen Sachverständigen gestattet, im Rahmen ihrer Aufgaben und Prüfungen Einsicht in Unterlagen mit medizinischen Daten zu nehmen. Ein Recht der Pflegekassen, im Rahmen der Wirtschaftlichkeits- und Qualitätsprüfung in Unterlagen mit sensiblen Daten der Pflegedürftigen einzusehen, sehen diese Regelungen gerade nicht vor. Die Pflegekasse ist damit nicht befugt, Daten aus der Pflegedokumentation zu erheben. Als Abrechnungsunterlage für die Pflegekasse kommen vielmehr nur solche Dokumente in Betracht, in denen Leistungen des Pflegedienstes nach Art, Preis und Menge sowie die Abgabe von Hilfsmitteln nachgewiesen werden.

Gegen die Einsichtnahme eines gemäß § 114 Abs. 6 Satz 1 SGB XI beteiligten Vertreters der betroffenen Pflegekasse in die Pflegedokumentation bestehen allerdings keine Bedenken, sofern der Vertreter der Pflegekasse im Rahmen einer örtlichen Prüfung nach § 114 Abs. 1 bis 3 SGB XI (Einzelprüfung, Stichproben- und vergleichende Prüfung) hinzugezogen wird, um – wie dies in der Begründung zu dieser Vorschrift ausdrücklich genannt ist – eine wirksame Prü-

fung der Abrechnung zu gewährleisten. Das ändert nichts daran, dass darüber hinaus weder eine Berechtigung noch eine Verpflichtung der Pflegeeinrichtung besteht, die Pflegedokumentation den Pflegekassen zu offenbaren. Die Pflegedokumentation stellt keine Abrechnungsgrundlage im Sinne des § 105 SGB XI dar. Der Inhalt der Abrechnungsunterlagen ist in § 105 Abs. 1 SGB XI abschließend geregelt. Insoweit besteht für eine Weitergabe der Pflegedokumentation an die Pflegekassen selbst weder eine rechtliche Grundlage noch ein Bedarf.

3. Einsichtnahme durch den Pflegebedürftigen und durch Angehörige

Der Auskunftsanspruch des Betroffenen gegenüber Heimen in privatrechtlicher Trägerschaft richtet sich nach § 34 Bundesdatenschutzgesetz (BDSG), da das BDSG Rechtsgrundlage für die Datenverarbeitung nicht-öffentlicher Stellen ist (vgl. §§ 27 ff. BDSG). Daneben besteht im Einzelfall ein Auskunftsanspruch aufgrund vertraglicher Bestimmungen und (Neben-) Pflichten. Im Regelfall wird somit der Pflegebedürftige gemäß § 34 BDSG bzw. auf Grund eines vertraglichen Anspruches ein Einsichtsrecht in die ihn betreffende Pflegedokumentation haben. Gleiches gilt für vom Pflegebedürftigen bevollmächtigte Angehörige und sonstige Personen sowie für gesetzlich bestellte Betreuer, soweit ihr Aufgabenkreis dies umfasst. Das Recht auf Einsichtnahme gilt auch über den Tod des Pflegebedürftigen hinaus, sofern er eine entsprechend wirksame Vollmacht erteilt hat.

Schwierig ist es, wenn Pflegebedürftige vorübergehend oder dauernd außerstande sind, einen Angehörigen rechtsgültig zu bevollmächtigen. In derartigen Fällen ist als Rechtfertigungsgrund für eine Offenbarung von Daten aus der Pflegedokumentation in erster Linie der mutmaßliche Wille des Betroffenen von Bedeutung. Es kommt in diesem Zusammenhang ganz wesentlich darauf an, dass die Offenbarung im Interesse des Pflegebedürftigen geboten ist. Dabei ist ein enger Maßstab anzulegen. Die Offenbarung muss beispielsweise dazu dienen, den Angehörigen zu ermöglichen, sich ein Bild darüber zu verschaffen, ob die vertraglich zugesagten Leistungen auch tatsächlich erbracht worden sind.

13. Bildung

13.1 Zentrales Schülerregister

Das zentrale Schülerregister ist datenschutzrechtlich noch nicht ausgereift.

Die Hamburgische Bürgerschaft hat mit dem Schulreformgesetz im Mai 2006 die Einrichtung eines Zentralen Schülerregisters (ZSR) beschlossen und hierfür im Schulgesetz in Verbindung mit der Schul-Datenschutzverordnung die Rechtsgrundlage gelegt. Das ZSR wurde erstmals für den im Frühjahr 2007

vorzustellenden Jahrgang der viereinhalbjährigen Kinder und für den zur ersten Klasse im Schuljahr 2007/2008 anzumeldenden Jahrgang eingesetzt. Das ZSR soll die Schulen und die Behörde für Bildung und Sport (BBS) darin unterstützen, Kinder, zu deren Familien auch nach mehrfachen Versuchen von den Schulen kein Kontakt hergestellt werden konnte, herauszufinden oder aber bei Feststellung des Wegzugs der Familie das Melderegister berichtigen zu lassen.

Das ZSR soll aber auch Aufgaben unterstützen, die nicht nur die BBS, sondern auch andere Behörden insbesondere zur Verbesserung des Kinderschutzes in Hamburg zu erfüllen haben. Um Jugendämter und andere staatliche Stellen in die Lage zu versetzen, im Falle einer Kindeswohlgefährdung schnell und wirksam zu handeln, hat der Senat zahlreiche Maßnahmen getroffen, um die Informationsgrundlagen der Jugendämter zu verbessern (vgl. 12.1). Dazu gehören auch die in der Schul-Datenschutzverordnung festgelegten Befugnisse zur Übermittlung von Daten aus dem ZSR an andere Behörden oder sonstige öffentliche Stellen sowie zum automatisierten Abruf von ZSR-Daten durch die Polizeivollzugsdienststellen, die Jugendämter und die Gesundheitsämter.

Nachdem die rechtlichen Grundlagen für das ZSR geschaffen worden waren, haben wir die BBS auch bei der praktischen Umsetzung dieser Regelungen begleitet. Grundlage war die von der BBS zu erstellende Verfahrensbeschreibung nach § 9 HmbDSG und die Risikoanalyse nach § 8 Abs. 4 HmbDSG. Wir stießen bei der Erörterung dieser Unterlagen immer wieder auf Punkte, die entweder datenschutzrechtlich unzulässig waren oder aber so unklar, dass sie sich einer Beurteilung entzogen. Einige unserer Kritikpunkte konnten zwar ausgeräumt werden, andere Punkte sind aber aus datenschutzrechtlicher Sicht nach wie vor offen.

Gemäß § 8 Abs. 2 Satz 2 Schul-Datenschutzverordnung ist die Datenverarbeitung der Schulen auf die Daten der Personen begrenzt, die ihre Schule besuchen, besucht haben, besuchen wollen oder sollen. Dies ist bei der Konzeption des ZSR und insbesondere bei der Gestaltung der Zugriffsmöglichkeiten bzw. des Berechtigungskonzeptes zu berücksichtigen. Eine schulübergreifende Zugriffsmöglichkeit der Schulen auf das ZSR ist durch die Schul-Datenschutzverordnung rechtlich nicht gedeckt. In der Praxis führte dies zu Problemen bei der Klärung der Frage, ob ein Kind an einer anderen als der regional zuständigen Schule (Bezirksgrundschule) vorgestellt oder angemeldet worden ist. Datenschutzrechtlich konnte dies dadurch gelöst werden, dass die Daten eines Schülers, der in der Zeit zwischen Schuljahresbeginn und dem 15. September nicht von der Bezirksgrundschule, sondern von einer anderen Schule aufgenommen wurde, noch bis zum 15. September von der Bezirksgrundschule aufgerufen werden können. Die Aufnahme des Schülers an einer Schule ist erst abgeschlossen, wenn er dort tatsächlich erscheint. Erst dann nimmt die aufnehmende Schule die entsprechende Eintragung im ZSR vor. Und erst dann

handelt es sich bei der Bezirksgrundschule nicht mehr um die Schule, die er besuchen soll, sondern die er besuchen sollte. Damit endet für die Bezirksgrundschule auch die Verpflichtung, die Schulpflicht der noch nicht aufgenommenen Schülerinnen und Schüler zu überwachen, d.h. sie benötigt keinen Zugriff mehr auf die entsprechenden Datensätze.

Unzureichend sind bisher noch die technischen und organisatorischen Maßnahmen, die für den Betrieb des ZSR getroffen worden sind:

- Es mangelt an einem schlüssigen Berechtigungskonzept. So ist nicht hinreichend klar dokumentiert, welche Mitarbeiter der BBS unter welchen Voraussetzungen für welche Aufgaben welche Zugriffsrechte auf welche personenbezogenen Daten haben. Damit ist es bislang auch nicht möglich, die jeweilige Erforderlichkeit der Zugriffsmöglichkeiten nachvollziehen zu können.
- Während der technische Support der ESARI Schulrechner auf Dataport übertragen wurde, soll der fachliche Support weiterhin durch Mitarbeiter der BBS erfolgen. Da jedoch die für ESARI Rechner bestehende Möglichkeit eines Online-Supports (Aufschalten auf den betroffenen Rechner zur Analyse der konkreten Fehlersituation nach vorheriger Zustimmung durch den Nutzer) für die BBS nicht besteht, ist es dabei zur Zeit möglich, dass sich der BBS-Support zur Fehleranalyse als Administrator durch die Eingabe der Schulnummer als jede beliebige Schule anmelden kann, ohne dass es hierzu einer Zustimmung des Mitarbeiters der Schule bedarf. Um die Verantwortungen auch hier klar abzugrenzen und Konflikte mit der Administration durch Dataport zu vermeiden, haben wir die BBS aufgefordert, schnellstmöglich mit Dataport zu einer datenschutzrechtlich tragfähigen Lösung zu kommen.
- Die Art und Weise sowie der Umfang der Protokollierung von Zugriffen sind nicht abschließend festgelegt.
- Zahlreiche von der BBS vorgesehene Auswertungsmöglichkeiten der im ZSR gespeicherten Daten müssen vor dem Einsatz von Auswertungstools noch konkretisiert und mit uns abgestimmt werden.

Diese und andere Punkte haben die BBS veranlasst, die bisher vorgelegten Konzepte und Unterlagen insgesamt grundlegend zu überarbeiten. Sie sollen uns im ersten Quartal des Jahres 2008 vorgelegt werden. Es bleibt abzuwarten, ob wir dann sagen können, dass es mit dem ZSR keine Datenschutzprobleme mehr gibt.

13.2 Datenbank UDIS der Behörde für Bildung und Sport

Es entwickelt sich eine neue Philosophie der Datenverarbeitung, deren datenschutzrechtliche Zulässigkeit noch nicht abschließend beurteilt werden kann.

Im Rahmen unserer Beteiligung an verschiedenen IT-Vorhaben der Behörde für Bildung und Sport (BBS) sind wir im Berichtszeitraum immer wieder auf Verbindungen zu dem Unternehmensdateninformationssystem (UDIS) gestoßen. Hierbei handelt sich um eine zentrale Datenbank der BBS, über deren Architektur und Wirkungsweise wir aber leider bislang nicht ausreichend unterrichtet sind.

Bereits 2002 wurden wir durch eine Bürgerschaftsdrucksache auf das Projekt Unternehmensdatenmanagement (PUMA) der BBS aufmerksam. Da uns dazu keine datenschutzrechtlichen Unterlagen (Verfahrensbeschreibung, Risikoanalyse) vorlagen, forderten wir unter Hinweis auf die Beteiligungsrichtlinie von der BBS aussagekräftige Unterlagen an. In der Antwort der BBS hieß es, dass im Rahmen von PUMA weder personenbezogene Daten im Sinne des § 1 HmbDSG erhoben würden noch die Verarbeitung personenbezogener Daten Gegenstand des Projekts sei. Vielmehr ginge es lediglich darum, bereits vorhandene Daten besser für Steuerungsentscheidungen der Behörde nutzbar zu machen. Durch Datenhaltung in einheitlichen, zentralen Datenbanken sollten redundante und widersprüchliche Datenbestände vermieden und der Arbeitsaufwand für die Erfassung und Datenpflege auf ein Mindestmaß reduziert werden. Die BBS sagte zu, wieder an uns heranzutreten, sobald bei der weiteren Projektarbeit eine Beteiligung des Hamburgischen Datenschutzbeauftragten zumindest ratsam sein würde (z.B. im Hinblick auf die Etablierung von Schnittstellen). Dies ist jedoch nur im Zusammenhang mit der Einrichtung eines Schulinformationssystems und der hiermit verbundenen Aufnahme personenbezogener Daten von Ansprechpartnern erfolgt.

Wir haben erst durch unsere Befassung mit anderen IT-Vorhaben der BBS festgestellt, dass in UDIS, dem Nachfolger des Projektes PUMA, nicht nur anonymisierte oder aggregierte Daten, sondern durchaus eine Vielzahl personenbezogener Daten verarbeitet werden. UDIS dient zwar derzeit lediglich einigen wenigen Fachanwendungen der BBS als relationales Datenbankmanagementsystem. Es sollen aber recht zügig weitere Fachanwendungen an UDIS angebunden werden. Bereits jetzt gibt es beispielsweise Schnittstellen zu den Verwaltungsverfahren der allgemeinbildenden und der berufsbildenden Schulen, zu einem Personalverfahren der Schulen sowie zum Zentralen Schülerregister (vgl. 13.1). Auch ein Verfahren „Statistische Anwendungen“ ist in UDIS bereits realisiert.

Die BBS vertritt bislang den Standpunkt, für UDIS sei weder eine Verfahrensbeschreibung noch eine Risikoanalyse erforderlich, weil es sich bei UDIS um kein eigenständiges Verfahren handele. Vielmehr komme es entscheidend darauf an, in den Verfahrensbeschreibungen und Risikoanalysen der an UDIS „angedockten“ Fachverfahren die datenschutzrechtlich erforderlichen Aussagen zu treffen. Dies ist auch erforderlich, weil aus den bisherigen Unterlagen zu den Fachverfahren ein Bezug zu UDIS ebenso wie Informationen über eine

Datenhaltung in UDIS nicht ersichtlich ist. Deshalb arbeitet die BBS mit Hochdruck daran, die bisher erstellten Unterlagen zu den Fachverfahren, die sich der Datenbank UDIS bedienen, den neuen Gegebenheiten anzupassen.

Unsere vorläufige Einschätzung von UDIS geht dahin, dass es sich um einen Anwendungsfall des § 11a Abs. 2 HmbDSG handelt. Denn viel spricht dafür, dass personenbezogene Daten aus unterschiedlichen Aufgabengebieten in einer gemeinsamen automatisierten Datei oder zumindest in verbundenen automatisierten Dateien verarbeitet werden. Damit bedarf die Einrichtung von UDIS der Zulassung durch die Leitung der Daten verarbeitenden Stelle, weil sich die Gefährdungslage bezüglich der informationellen Selbstbestimmung und damit der Regelungsbedarf in solchen Fällen verdichtet. Gemeinsame oder verbundene automatisierte Dateien sind regelmäßig dadurch gekennzeichnet, dass der Datenbestand ohne zentrale Kontrolle durch eine bestimmte Daten verarbeitende Stelle von allen angeschlossenen Stellen unmittelbar bedient werden kann und dass die eingebende Stelle keine Kontrolle darüber hat, wer eine von ihr eingegebene Information abruft. Da die BBS bislang eine Zulassung von UDIS nach § 11a Abs. 2 HmbDSG nicht erteilt hat, haben wir die Behörde aufgefordert, dies nachzuholen.

Wir werden weiterhin darauf drängen, dass alle datenschutzrechtlichen Details im Zusammenhang mit UDIS geklärt werden. Die BBS hat bisher nur zu einzelnen Punkten in der Konzeption von UDIS reagiert und Gegenmaßnahmen ergriffen: Das Datenmanagement in der BBS wird restrukturiert, die Geschäftsprozesse für die Datenerfassung, die Datenanalyse und die Datenausgabe werden analysiert, um sie anschließend den fachlichen Erfordernissen anzupassen. Dieses Restrukturierungsprogramm umfasst auch die Vorbereitung eines Projektes zur Einführung eines Data Warehouses, um das zukünftige Datenmanagement auf ein sicheres und nachhaltiges Fundament zu stellen. Ziel des Projektes ist es, jederzeit den Überblick über die Daten zu haben, Datenströme reibungslos durch verschiedene Applikationen zu leiten sowie Zugriffe, Nutzung und Verarbeitung der Daten – sei es durch Anwender oder durch Applikation – sicher und integer zu kontrollieren und zu dokumentieren. Wir werden die Entwicklung dieser Angelegenheit weiter kritisch beobachten.

13.3 Studien-Infonetz (STiNE) der Universität Hamburg

Der Start des neuen Campus-Netzes wurde von Sicherheitsmängeln begleitet.

Die Einführung der neuen Studiengänge im Bachelor-Master-System an der Universität Hamburg mit modularisiertem Studiensystem und studienbegleitenden Prüfungen machte eine IT-Unterstützung notwendig. Die Universität Hamburg hat deshalb unter dem Namen STiNE das System CampusNet der Firma Datenlotsen eingeführt, das zum Wintersemester 2006/07 in Betrieb genommen wurde. STiNE ist ein integriertes System für Studierende, Lehrende und Verwaltungspersonal zur Organisation aller Verwaltungsprozesse im Be-

reich von Studium und Lehre. Die Funktionalitäten im Vollbetrieb umfassen Studierendenverwaltung einschl. Bewerbung und Zulassungsverfahren, Prüfungsverwaltung, Unterstützung in der Lehre, Lehrveranstaltungsmanagement, Raummanagement und Qualitätsmanagement. Zum Wintersemester 2006/07 wurden zunächst die Bereiche Lehrveranstaltungsmanagement und Prüfungsverwaltung freigeschaltet, im Sommersemester 2007 wurden das Bewerbungsverfahren und die Studierendenverwaltung auf STiNE umgestellt, weitere Funktionen werden zum Wintersemester 2008/09 folgen.

Durch die zentrale Datenhaltung in einer Datenbank soll STiNE eine effiziente Datenhaltung und hohe Transparenz schaffen. Für die Studierenden ermöglicht STiNE, sich unabhängig von Öffnungszeiten und Sprechstunden von jedem beliebigen Computer mit Netzanschluss zu Veranstaltungen anzumelden, notwendige Bescheinigungen z.B. für Zwecke der Ausbildungsförderung oder der Krankenversicherung selbst auszudrucken und einen ständigen Überblick über Studienverlauf und Prüfungsleistungen zu erhalten. Verwaltungsvorgänge sollen vereinfacht und die Mitarbeiterinnen und Mitarbeiter vom Massengeschäft entlastet werden. Die Universität Hamburg ist eine der ersten großen Hochschulen in Deutschland, die ein solches integriertes IT-System eingeführt haben.

Der Start von StiNE verlief recht turbulent, zum Beginn des Wintersemesters 2006/07 herrschten teilweise chaotische Zustände. Es krankte zunächst an einem Software-Fehler und zu geringem Speicherplatz. Auch lückenhafte Dateneingaben einzelner Fachbereiche behinderten in der Anlaufphase die Leistung von StiNE. Das hatte zur Folge, dass es vielen Studierenden im Laufe der ordentlichen Anmeldefrist nicht möglich war, sich für alle Seminare anzumelden. Sie hatten versucht, sich einzuloggen und wurden vom System automatisch gesperrt. Studierende bekamen die Meldung, ihr Passwort sei falsch, oder es fehlten Lehrveranstaltungen an ihrem individuellen Portal.

Neben diesen Problemen gab es aber auch Sicherheitsmängel im System, die zwar aus datenschutzrechtlicher Sicht nicht verheerend waren. Es waren aber Mängel, die man bei sorgfältiger Testung des Systems hätte vermeiden können. So war es beispielsweise Informatikstudenten möglich, in sensible Datenbereiche vorzustoßen, weil sie über erweiterte Zugriffsmöglichkeiten verfügten. Ein Zugriff auf Daten von Kommilitonen konnte zumindest nicht ausgeschlossen werden.

Im Rahmen unserer Beteiligung bei der Einführung von StiNE haben wir frühzeitig darauf gedrungen, das Verfahren datenschutzgerecht und sicher zu administrieren. So konnten wir erreichen, dass die Verarbeitung der Daten verschlüsselt erfolgt, damit Unbefugte nicht an Prüfungsdaten gelangen können.

Inzwischen ist der Betrieb von StiNE in Routine übergegangen, das Netz läuft nach unseren Informationen jetzt reibungslos. Auch die Sicherheitslücken sind geschlossen worden.

13.4 Videoüberwachung in Schulen

Solange es keine spezialgesetzliche Regelung gibt, dürfen keine weiteren Videoüberwachungsanlagen in Schulen installiert werden.

Seit unserer letzten Berichterstattung über Videoüberwachung in Schulen (20. TB, 12.2) haben weitere Schulen Videokameras installiert oder deren Einsatz geplant. Die Schulen sehen in Anlagen zur Videoüberwachung ein im Einzelfall notwendiges Mittel zur Verhinderung von strafbaren Handlungen, insbesondere Diebstählen und Sachbeschädigungen in ihren Räumen und auf ihrem Grundstück. Sofern wir Gelegenheit haben, die Schulen vor der Installation einer Videoüberwachungsanlage beraten zu können, weisen wir auf die Rechtslage hin, die sich mit der Entscheidung des Bundesverfassungsgerichts vom 23. Februar 2007 zur Videoüberwachung im öffentlichen Bereich grundlegend geändert hat.

Die Videoüberwachung öffentlicher Gebäude und Räume – dazu gehören auch Schulen – stellt grundsätzlich einen Eingriff in das allgemeine Persönlichkeitsrecht in seiner Ausprägung als Recht der informationellen Selbstbestimmung dar. Das durch die Videoüberwachung gewonnene Bildmaterial kann und soll in aller Regel dazu genutzt werden, belastende hoheitliche Maßnahmen gegen Personen vorzubereiten, die in dem von der Überwachung erfassten Bereich beispielsweise Straftaten begehen. Die offene Videoüberwachung eines öffentlichen Ortes kann und soll zugleich abschreckend wirken und insofern das Verhalten der Betroffenen beeinflussen. Sofern es sich um eine Videoüberwachung mit Aufzeichnung handelt – was in Schulen ganz überwiegend der Fall ist – wird das Gewicht dieser Maßnahme dadurch erhöht, dass infolge der Aufzeichnung das gewonnene Bildmaterial in vielfältiger Weise ausgewertet, bearbeitet und mit anderen Informationen verknüpft werden kann. Von den Personen, die Schulräume betreten, dürfte aber nur eine Minderheit gegen Recht und Gesetz verstoßen. Mit der Videoüberwachung werden daher überwiegend Personen erfasst, gegen die sich die Maßnahme überhaupt nicht richtet.

Das Hamburgische Datenschutzgesetz (HmbDSG) enthält keine spezielle Regelung zur Videoüberwachung öffentlicher Gebäude und Räume. Deshalb wurde bislang eine solche Maßnahme auf die allgemeinen Regelungen zur Datenerhebung in § 12 HmbDSG gestützt unter Heranziehung der weiteren in § 6b BDSG festgelegten Voraussetzungen für eine Videoüberwachung. Videoüberwachungen wurden danach als zulässig angesehen, wenn insbesondere die Datenerhebung mit Kenntnis der Betroffenen erfolgte, d.h. wenn auf solche Überwachungen z.B. durch deutlich sichtbare Hinweisschilder auf-

merksam gemacht wurde. Hinzu kamen weitere Voraussetzungen, die jeweils im Einzelfall vorliegen mussten. Diese Vorgehensweise ist nach der obigen Entscheidung des Bundesverfassungsgerichts nicht mehr möglich.

Das Gericht musste sich mit einer geplanten Videoüberwachungsmaßnahme in Bayern befassen und kam zu dem Ergebnis, dass ein solcher Eingriff in das allgemeine Persönlichkeitsrecht nicht auf die allgemeinen Regelungen zur Datenerhebung im Datenschutzrecht gestützt werden könne. Diese Normen enthielten keine hinreichenden Vorgaben für Anlass und Grenzen der Maßnahmen, um als Ermächtigungsgrundlage für den Grundrechtseingriff in Betracht zu kommen. Sie begrenzten die Datenerhebung lediglich durch das Gebot der Erforderlichkeit. Dies allein könne die behördliche Praxis aber nicht hinreichend anleiten oder Kontrollmaßstäbe bereitstellen.

Das Gericht hat allerdings nicht ausgeschlossen, dass eine Videoüberwachung öffentlicher Einrichtungen mit Aufzeichnung des gewonnenen Bildmaterials auf der Grundlage einer hinreichend bestimmten und normenklaren Ermächtigungsgrundlage materiell verfassungsgemäß sein kann.

Nach dieser Entscheidung kann die bisher in Hamburg vertretene Auffassung, man könne die Videoüberwachung auf § 12 HmbDSG stützen, nicht mehr aufrechterhalten werden. Vielmehr ist es erforderlich, die Videoüberwachung öffentlicher Gebäude den Anforderungen des Bundesverfassungsgerichts entsprechend gesetzlich zu regeln. Die Hamburgische Bürgerschaft hat dies nach einem Hinweis des Hamburgischen Datenschutzbeauftragten erkannt und den Senat ersucht, eine hinreichend klare Rechtsgrundlage für die Videoüberwachung öffentlicher Orte – insbesondere von Schulräumen – zu schaffen. Wir gehen davon aus, dass es noch im Jahr 2008 zu einem entsprechenden Gesetzgebungsverfahren kommen wird und wir daran beteiligt werden.

Bis die Spezialnorm für die Videoüberwachung in Kraft tritt, besteht nach alledem kein Raum mehr für die Einrichtung weiterer Videoüberwachungsanlagen in Schulen.

14. Gesundheitswesen

14.1 Novellierung des Hamburgischen Krankenhausgesetzes

Eine auch vom Hamburgischen Datenschutzbeauftragten initiierte Novellierung des Krankenhausgesetzes regelt unter anderem erstmals in der Bundesrepublik die Errichtung von Biobanken.

Im Oktober 2006 beschloss die Bürgerschaft eine umfangreiche Novellierung des Hamburgischen Krankenhausgesetzes. Diese war bereits im Jahr zuvor mit betroffenen Institutionen erörtert worden, wurde noch in den Ausschussbe-

ratungen modifiziert und bis zur Verabschiedung eng mit uns abgestimmt. Datenschutzrechtliche Bedeutung haben insbesondere folgende Änderungen:

Zur Intensivierung der externen Aufsicht werden die Krankenhausverwaltungen nun verpflichtet, die Ärztekammer und die Approbationsbehörde zu informieren, wenn ein Mitarbeiter oder eine Mitarbeiterin des Krankenhauses im begründeten Verdacht steht, gegen Berufspflichten verstoßen zu haben. Dabei darf das Krankenhaus auf Verlangen auch notwendige Patientenunterlagen herausgeben. Diese Stärkung der externen Krankenhauskontrolle hielten wir zum Schutz der Patientinnen und Patienten für nachvollziehbar und vertretbar.

Neu geregelt wurde auch die Beratung und Betreuung durch den Sozialdienst. Dabei erfuhr der krankenhauseigene Sozialdienst eine datenschutzrechtliche Privilegierung: Für die interne Sozialberatung darf das Krankenhaus nun auch Patientendaten ohne eine gesondert einzuholende Einwilligung der Betroffenen erheben und speichern. Der krankenhausinterne Sozialdienst hat Zugang zu und ein Nutzungsrecht an den notwendigen Patientendaten im Krankenhaus, um seine Beratung und Betreuung vorzubereiten, die dann allerdings nur „in Absprache“ mit der betroffenen Person erfolgen darf. Eine Übermittlung von Patientendaten an externe Sozialdienste oder Reha-Einrichtungen, Pflegedienste oder ähnliche Stellen lässt das Gesetz dagegen weiterhin nur in den seltenen Ausnahmefällen zu, in denen eine Einwilligung nicht eingeholt werden kann und der mutmaßliche Wille des Patienten oder der Patientin nicht entgegensteht.

Neu eingeführt wurde ein verbindliches Beschwerdemanagement für Patientinnen und Patienten. An der technischen Umsetzung dieser Vorschrift im UKE waren wir beteiligt. Dabei ging es um die häufig auftauchende Frage, ob der Beschwerdegegner (z.B. ein Arzt) „automatisch“ den vollen Wortlaut der Beschwerde erhält und ob umgekehrt der Beschwerdeführer den vollen Wortlaut der Stellungnahme des Beschwerdegegners erfährt. Die Beschwerde im Volltext wird nur weitergeleitet, wenn dies für die Stellungnahme erforderlich ist. Der Beschwerdeführer erhält statt eines Zugriffs auf die vollständige Stellungnahme eine zusammenfassende Schlussmitteilung.

Die Regelungen zur Forschung mit Patientendaten wurden ebenfalls neu strukturiert. Die Bürgerschaft übernahm dazu unseren Textvorschlag, der die verschiedenen Verarbeitungsalternativen (anonym, mit Einwilligung, pseudonym) in eine klare Prioritätsfolge einordnet und auf eine Wiederholung der allgemeinen datenschutzrechtlichen Anforderungen z.B. an Einwilligungen verzichtet. Privilegiert bleibt der Forscher, der die Patienten, deren Daten er nutzt, selbst behandelt (hat). Andere Mitarbeiter des Krankenhauses, zum Beispiel Doktoranden, die an der Behandlung der betroffenen Patienten nicht beteiligt sind oder waren, werden wie externe Dritte, als Empfänger von Datenübermittlungen, behandelt. Neu ist auch die gesetzliche Forderung nach einer Abschottung des Behandlungsbereichs, in dem Daten namensbezogen verarbeitet

werden, vom Forschungsbereich, in dem Patientendaten ausschließlich anonym oder pseudonymisiert verarbeitet werden dürfen.

Als erstes Gesetz in der Bundesrepublik enthält das Hamburgische Krankenhausgesetz schließlich auf unseren Vorschlag hin eine Vorschrift für die Sammlung von Proben und Daten zu allgemeinen Forschungszwecken. Die Regelung beseitigt die bisherige rechtliche Grauzone und ermöglicht ausdrücklich die Errichtung von sogenannten Biobanken. Sie bindet diese aber an eine vorherige Anonymisierung der Proben und Daten oder an eine vorherige Einwilligung der betroffenen Patienten bzw. Probanden. In diesem Falle sind Proben und Daten vor Aufnahme in die Biobank zu pseudonymisieren – ggf. durch einen externen Datentreuhänder. Um einen Überblick zu bekommen über diese datenschutzrechtlich besonders sensiblen, weil langfristigen und zweckoffenen Vorratsdatenhaltungen, sind neue Biobanken in Hamburger Krankenhäusern beim Hamburgischen Datenschutzbeauftragten anzuzeigen (siehe auch unten 14.2).

14.2 Datenschutzprobleme im Universitäts-Klinikum Eppendorf

Neben einzelnen Datenschutzdefiziten in der täglichen Routine bestehen im UKE grundsätzliche Probleme des Patientendatenschutzes durch tiefgreifende organisatorische Umstrukturierungen und eine ehrgeizige technische Modernisierung.

Organisationsstruktur

Früher bildete das UKE eine einheitliche Organisationsstruktur als öffentlich-rechtliches Krankenhaus. Heute setzt sich die „UKE-Gruppe“ zusammen aus den Kern-Kliniken und Zentren, klinischen Töchtern wie dem Universitären Herzzentrum und dem Altonaer Kinderkrankenhaus, Privatkliniken (Martiniklinik), dem Ambulanzzentrum und verschiedenen Service- GmbH. Datenschutzrechtlich sind diese Einrichtungen je nach Status (stationär / ambulant; öffentlich-rechtlich / GmbH; Patientenbehandlung / Service) nach unterschiedlichen Rechtsgrundlagen zu beurteilen: So gilt das Hamburgische Krankenhausgesetz nur für die Kliniken der Allgemeinversorgung, also nicht für die Martiniklinik und das Ambulanzzentrum; das Bundesdatenschutzgesetz gilt für alle GmbH, egal ob Service oder Ambulanz- GmbH; das Hamburgische Datenschutzgesetz gilt, soweit die Forschung und die Personalverwaltung in den UKE-Kliniken betroffen ist.

Während die Behandlung der Patienten früher in einer datenschutzrechtlichen Stelle (UKE) erfolgte, ist sie nun auf verschiedene rechtlich selbständige Einheiten verteilt. Dies hat zur Folge, dass sich die Datenweitergabe von einer Einheit an eine andere (z.B. von der Strahlenklinik zum Ambulanzzentrum im selben Gebäude) rechtlich als Datenübermittlung darstellt, für die es ggf. einer ausdrücklichen Einwilligung des Patienten bedarf. Bei der Inanspruchnahme

der Service- GmbH (Krankentransport, Archiv, Essensversorgung) handelt es sich rechtlich um eine Auftragsdatenverarbeitung – ggf. mit einem Unterauftrag an den UKE- Geschäftsbereich Informationstechnik zur Nutzung des Klinikinformationssystems.

Die datenschutzgerechte Umsetzung dieser Strukturveränderungen erforderte intensive Diskussionen mit den Verantwortlichen des UKE. Erörtert und schließlich weitgehend geklärt wurden vor allem Zugriffsregeln für das übergreifende elektronische System sowie angemessene Aufklärungs- und Einwilligungstexte. Ein Ergebnis war der „Leitfaden zum Patientendatenschutz bei der einrichtungsübergreifenden Behandlung von Patienten im UKE aus Sicht der Informationsverarbeitung“. Es bleibt abzuwarten, ob die Leitung des UKE dieses Dokument als verbindliche Vorgabe beschließt.

Technische Modernisierung

Die technische Modernisierung äußert sich in vielen neuen Kommunikationsformen und EDV-Projekten wie W-LAN-(Funk-)Verbindungen, Internet-Telefonie, IXServ / Epnet (vgl. 20.TB 13.3); Service-Software SyncroTess, einer neuen Intensivstations-Überwachung ICM und einem Business-Warehouse-System. Zur Zeit läuft die Ausschreibung für ein Klinisches Arbeitsplatz System (KAS), dessen datenschutzrechtliche Anforderungen auch uns beschäftigten.

Über zwei Jahre haben wir mit dem UKE intensiv um ein Business Warehouse mit Patientendaten gerungen. Das Problem lag vor allem darin, dass mit demselben System sowohl operative Routine-Aufgaben mit personenbezogenen Daten erfüllt als auch statistische Auswertungen ohne Personenbezug durchgeführt werden sollten. Es ging um Zeitpunkt und Grad der Pseudonymisierung und Anonymisierung der Patientendaten und um das Zugriffskonzept. Einen ersten Entwurf mussten wir ablehnen, weil auch dann auf personenbeziehbare Patientendaten zugegriffen werden sollte, wenn dies für die Aufgabenerfüllung gar nicht erforderlich war. Ein neues Konzept mit einer geänderten Datenverarbeitungsstruktur kommt unseren Anforderungen wesentlich näher und ist derzeit in der Endabstimmung.

Zu dem neu eingeführten ICM-System der Intensivmedizin erreichte uns aus dem UKE selbst eine dringende Beschwerde über ernste Systemausfälle und Serviceprobleme. Danach standen Datensicherheit und -Verfügbarkeit in Frage – mit zum Teil lebensbedrohlichen Risiken. Auf unsere umgehende Nachfrage im UKE wurde uns mitgeteilt, dass inzwischen Abhilfe geschaffen sei, und dargestellt, wie in Zukunft die Stabilisierung des Systems und die jederzeitige Erreichbarkeit der technischen Kompetenz gewährleistet werden soll. Wir werden die weitere Entwicklung beobachten.

Unnötiger Zugriff auf frühere Behandlungsorte

Auch im täglichen Routinebetrieb traten Datenschutz-Defizite und -Probleme auf, die wir in enger Kooperation mit der Datenschutzbeauftragten des UKE zu bearbeiten hatten:

So beschwerte sich eine Patientin darüber, dass der behandelnde Arzt in der Medizinischen Notaufnahme ohne ihre Einwilligung aus dem elektronischen Informationssystem erfuhr, dass sie vor Jahren Patientin im Suizid-Gefährdeten-Zentrums des UKE war. In der Tat: Wollte ein Arzt im System ORDIS – nach der Behandlung – einen Arztbrief schreiben, zeigte ihm das System beim Aufruf des Patientennamens automatisch Datum und Einrichtung früherer Patientenaufenthalte im UKE an. Dies war nicht erforderlich und widersprach der informationellen Selbstbestimmung der Patienten. Auf unser Einschreiten hin wurde diese automatische Anzeige in ORDIS geändert und dieses nun ebenso konfiguriert wie die anderen Großsysteme SAP und IXServ.

Verschwinden von Teilen der Behandlungsdokumentation

Nicht zu beheben war das Verschwinden von Behandlungsdokumentationen im UKE. Soweit es dabei nur um Papierunterlagen geht, ist dies eher ein arztrechtliches Problem der Einhaltung der Berufsordnung (10-jährige Dokumentationspflicht) als eines des Datenschutzrechts. Für elektronische Daten gilt aber § 9 Bundesdatenschutzgesetz, der technische und organisatorische Maßnahmen z.B. zur Gewährleistung der Zugriffs- und Verfügbarkeitskontrolle fordert. In einem Falle musste das UKE derselben Patientin zu zwei voneinander unabhängigen Krankenhausaufenthalten mitteilen, dass Teile der gewünschten Behandlungsunterlagen nicht mehr aufzufinden sind. Strittig ist, ob die Dokumente (auch) auf elektronischen Datenträgern gespeichert waren. Da dies nicht die einzige Beschwerde über verloren gegangene Behandlungsunterlagen war, muss das UKE die Organisation und Umsetzung der Dokumentationspflicht – gerade vor dem Hintergrund zunehmender Digitalisierung – auf ihre langfristige Zuverlässigkeit überprüfen.

Anzeige von Biobanken

Seit der Änderung des Hamburgischen Krankenhausgesetzes im Oktober 2006 muss das UKE die Errichtung von Proben- und Datensammlungen (die sog. „Biobanken“) beim Hamburgischen Datenschutzbeauftragten anzeigen, § 12 a HmbKHG. Diese Sammlungen sind wegen ihrer eingeschränkten Zweckbindung, der langen Speicherdauer und der Nutzung für fremde Forschungsprojekte von besonderer datenschutzrechtlicher Sensibilität. Unser Versuch, das Forschungsdekanat im UKE zu motivieren, diese Meldungen von Biobanken schon im eigenen Interesse zu überwachen, zu systematisieren und zu koordinieren, blieb weitgehend erfolglos. Anfang November 2007 lagen uns erst fünf Anzeigen von einzelnen Klinik(teil)en vor – zum Teil unvollständig, zum Teil handelte es sich gar nicht um eine Biobank. Wir halten es nach wie vor

für sinnvoll, dass sich das Forschungsdekanat der Umsetzung des § 12 a HmbKHG annimmt – und sei es, um einer Fortsetzung der Einzelprüfungen vor Ort durch den Datenschutzbeauftragten vorzubeugen.

Austausch von Prüfungsdaten Studierender

Als herauskam, dass im UKE jahrelang eine Angestellte als Ärztin praktizierte, die keine der Staatsprüfungen erfolgreich abgelegt hatte, suchte die Klinikumsleitung nach technischen Lösungen, um einem derartigen Fall in Zukunft vorzubeugen. Gewünscht wurde ein weitgehender Datenaustausch zwischen dem Landesprüfungsamt in der Behörde für Soziales und Gesundheit einerseits und der medizinischen Fakultät der Universität andererseits. Besonders die Noten aller Prüfungsfächer und das Nichtbestehen einer Prüfung sollten der Universität und damit dem UKE mitgeteilt werden. Wir haben dem UKE deutlich gemacht, dass die bundesweite Approbationsordnung den Datenaustausch zwischen Landesprüfungsämtern und Universitäten auf die personenbezogene Mitteilung beschränkt, dass der/die Studierende den ersten Teil der Medizinischen Prüfung (früher: „Physikum“) bestanden hat. Selbst das endgültige Nichtbestehen der Medizinischen Prüfung ist nur den anderen Landesprüfungsämtern, nicht der Universität bzw. dem Universitätsklinikum mitzuteilen. Offensichtlich ging der Verordnungsgeber davon aus, dass die/der Studierende für die Fortsetzung des Studiums (klinische Semester) bzw. für die Anstellung im Universitätskrankenhaus selbst die entsprechenden Urkunden vorlegen muss – zumal es bei Bewerbern aus anderen Bundesländern einen Austausch zwischen dem Prüfungsamt und dem UKE nicht gibt.

Datenschutzrechtlich unproblematisch wäre eine bundesweite Vereinheitlichung dieser Urkunden zur besseren Kontrolle. Zugestimmt haben wir einer Einwilligungslösung: Bei der Anmeldung zur Prüfung kann der/die Studierende sich nach Aufklärung über die Regelungen der Approbationsordnung freiwillig damit einverstanden erklären, dass das Prüfungsamt die Noten nach bestandener Prüfung an den medizinischen Fachbereich der Universität weitergibt.

Meldungen zum Krebsregister

Auf einem anderen Gebiet konnten wir dem UKE schließlich zu einer „Verfahrensverschlankung“ verhelfen: Für die patientenbezogenen Meldungen zum Krebsregister hatte das UKE erst 2005 einen datenschutzfreundlichen Ablauf beschlossen. In der Praxis wurde die mündliche und schriftliche Einholung der Einwilligung des Patienten durch den behandelnden Arzt jedoch als zu kompliziert empfunden. Die zunächst angestrebte Aufnahme einer vorsorglichen Einwilligung zur Datenweitergabe an das Krebsregister in den Behandlungsvertrag für jeden UKE- Patienten konnten wir nicht akzeptieren. Dies wäre vielfach eine überraschende Klausel und entbehrte im Zeitpunkt der Krankenhausaufnahme häufig jeglicher Grundlage. Einigen konnten wir uns dagegen auf

Folgendes: Erkennt der „Case-Manager“ bei der Aufnahme eines Patienten aus den Überweisungsunterlagen, dass dieser Patient wegen einer Krebserkrankung oder eines Krebsverdachts aufzunehmen ist und dem Patienten dies bewusst ist, dann kann er den Patienten über das Krebsregister aufklären und die notwendige Einwilligung in eine mögliche Meldung bereits jetzt einholen. Der Patient wird in diesen Fällen nicht überrascht und hat sich mit der (Verdachts-)Diagnose schon auseinander gesetzt. Aufklärung und Einwilligungsbitte treffen auf ein vorbereitetes Patientenbewusstsein. Wir haben auch zugestimmt, dass die Dokumentation der Einwilligung durch einen elektronischen Eintrag im Patientendatensatz erfolgt. Sollte sich im Nachhinein ein Krebsverdacht nicht bestätigen und eine Meldung nicht Betracht kommen, ist der Einwilligungseintrag zu löschen.

Fazit

Insgesamt erfordert die datenschutzrechtliche Aufsicht und Beratung des UKE – zu der die Stellungnahmen zu einzelnen Forschungsprojekten noch hinzukommen – eine intensive und oft auch geduldige bis hartnäckige Betreuung. Die konstruktive Kooperation mit der betrieblichen Datenschutzbeauftragten ist dabei sehr förderlich. Als Aufsichtsbehörde über den Datenschutz sehen wir allerdings mit Sorge, dass die dargestellten Entwicklungen im UKE die Kapazität einer einzelnen betrieblichen Datenschutzbeauftragten vor Ort tendenziell überfordern, zumal dann, wenn sie gedrängt wird, diese Funktion auch noch für alle Tochter-Unternehmen der UKE-Gruppe zu übernehmen.

14.3 Neue Entwicklungen beim Hamburgischen Krebsregister

Eine neu eingeführte Meldepflicht von Pathologen zum Krebsregister konnte datenschutzgerecht gestaltet werden; der geplante Abgleich von Mammographie-Screeningdaten mit dem Krebsregister entbehrt derzeit einer rechtlichen Grundlage.

In aller Regel werden Krebsdiagnosen von Pathologen gestellt, die ihrerseits aber keinen Kontakt zu den betroffenen Patientinnen und Patienten haben und daher auch keine Meldung an das Krebsregister abgeben können, weil eine Meldung in Hamburg die Einwilligung des Patienten voraussetzt. Wenn auch die behandelnden Ärzte die Diagnosedaten dem Krebsregister nicht melden – wozu sie in Hamburg nicht verpflichtet sind -, dann gehen der epidemiologischen Forschung wichtige Daten verloren. In anderen Bundesländern gibt es bereits eine Meldepflicht. Auch der Datenaustausch zwischen den Krebsregistern, der wegen unterschiedlicher Behandlungs- und Wohnorte der Patienten erforderlich ist, beruht inzwischen auf einem einheitlichen Standard.

Im April 2007 beschloss die Bürgerschaft deswegen eine Ergänzung des Hamburgischen Krebsregisters, die vorab intensiv mit uns abgestimmt wurde. Um das legitime Interesse des Krebsregisters an einer Vervollständigung seiner

Datenbasis mit datenschutzrechtlichen Erfordernissen in Einklang zu bringen, wird nun auch für die Meldungen seitens der Pathologen ein sogenanntes Einweg-Verschlüsselungsverfahren aus Teilen des Namens und des Geburtsdatums angewandt, das alle Krebsregister zum Austausch der Meldungen nutzen, für die sie örtlich nicht zuständig sind. Diese Pseudonymisierung kann angesichts eines komplizierten Codes zur Standardisierung der Namensbestandteile nicht rückgängig gemacht werden (daher „Einweg-Verschlüsselung").

In Vorgesprächen mit den pathologischen Praxen und Krankenhausabteilungen konnte das Krebsregister unsere Forderung umsetzen, dass die Pathologen selbst die vom Register zur Verfügung gestellte Software zur Bildung dieser Pseudonyme (Kontrollnummern) verwenden, bevor sie sie dem Krebsregister melden. Da das Krebsregister auch für alle „normalen", d.h. auf Einwilligung oder Ausnahmeregelungen basierenden, namensbezogenen Meldungen eine Kontrollnummer im dargestellten Verfahren bildet, kann es die Daten früherer Meldungen mit denen der Pathologen abgleichen und bei einem „Treffer" die Daten zusammenfügen. Dasselbe gilt für später eingehende Arztmeldungen zu demselben von einem Pathologen gemeldeten Fall, der dem Krebsregister bisher nur in nicht identifizierbarer Form vorliegt. Bleibt eine namensbezogene Meldung durch den behandelnden Arzt ganz aus, so kann das Krebsregister aus den verschlüsselten Daten dennoch einen begrenzten epidemiologischen Erkenntnisgewinn ziehen, ohne das informationelle Selbstbestimmungsrecht der Betroffenen zu verletzen.

Schwieriger gestaltet sich die Kooperation zwischen dem inzwischen bundesweit eingeführten Mammographie-Screening und den Krebsregistern der Länder. (Nur für die Hamburger Frauen ist das Verfahren, das über das Bremer Gesundheitsamt als einladende „zentrale Stelle" abgewickelt werden soll, derzeit noch nicht angelaufen.) Die Regelungen der Krebsfrüherkennungs-Richtlinien sehen zwar einen Datenabgleich zwischen den zuständigen Stellen des Screening-Programms und den epidemiologischen Krebsregistern vor, legen aber nicht im Einzelnen die dafür erforderlichen Daten fest.

Seit Mai 2007 fordert die „Kooperationsgemeinschaft Mammographie" – ein Fachgremium der Kassenärztlichen Bundesvereinigung und der Spitzenverbände der Krankenkassen -, dass die Zentrale Stelle dem Krebsregister Postleitzahl, Wohnort, Geburtsmonat und -jahr jeder Patientin mitteilt. Ferner soll das Krebsregister Diagnosedatum und Daten der Gewebsanalysen an die Zentrale Stelle zurückmelden, damit sogenannte Intervallkarzinome festgestellt werden können. (Als Intervallkarzinome bezeichnet man Krebsdiagnosen, die zwischen zwei regelmäßigen Screening-Terminen gestellt werden, bei denen also die Möglichkeit besteht, dass sie bei der letzten Mammographie übersehen wurden („falsch-negatives" Untersuchungsergebnis)).

Wir haben diese Wünsche sowohl mit den Kolleginnen und Kollegen aus den anderen Bundesländern als auch mit dem Leiter des Hamburgischen Krebsregisters ausführlich erörtert. Außer Frage stehen die große Bedeutung der Qualitätssicherung und der Mortalitätsevaluation beim Mammographie-Screening – der Datenaustausch muss sich nach der fachlichen Erforderlichkeit richten und dann rechtlich einwandfrei geregelt werden. Schon die Rechtsqualität der Früherkennungsrichtlinien entspricht kaum dem Gesetzesvorbehalt für Eingriffe in das Grundrecht auf informationelle Selbstbestimmung. Die Rechtslandschaft in den Bundesländern ist überdies so heterogen – besonders hinsichtlich der Krebsregistergesetze –, dass allein eine Verfahrensabrede und selbst eine Ergänzung der Früherkennungsrichtlinien auf Bundesebene wenig hilft.

Hamburg hat mit der namensbezogenen Speicherung der Patientendaten auf Einwilligungsbasis zwar eine transparente Datengrundlage – diese enthält auch die genannten Zusatzdaten der Patientinnen. Das Hamburgische Krebsregistergesetz stellt an die Übermittlung von personenbeziehbaren Daten aus dem Register aber gerade deswegen klare Anforderungen. Auch erleichtert der gewünschte Datentransfer in ein anderes Bundesland (Bremen) die rechtliche Beurteilung nicht. Stattdessen sollte geklärt werden, ob in Hamburg nicht ein (personenbezogener) Datenaustausch zwischen dem behandelnden Frauenarzt, der örtlichen Screening-Einheit in Hamburg und dem Hamburgischen Krebsregister für die individuelle Qualitätssicherung ausreicht und dies dann auch rechtlich umgesetzt wird. Die zentrale Stelle und das im Screening-Programm vorgesehene Referenzzentrum sollten dagegen mit anonymen oder für sie nicht entschlüsselbar pseudonymisierten Daten auskommen.

Wir werden die bundesweite Diskussion in Kooperation mit dem Hamburgischen Krebsregister weiter verfolgen und mitgestalten.

14.4 Klinische Arzneimittelprüfungen und die Pseudonymisierung der Probandendaten

In vielen Arzneimittelstudien werden trotz eines gesetzlichen Pseudonymisierungsgebotes auch Initialen und Geburtsdaten der Probanden an den Sponsor der Studie (Arzneimittelhersteller) weitergegeben.

Das Arzneimittelgesetz verlangt bei Arzneimittelstudien, dass die Probanden einwilligen in eine „pseudonymisierte“ Datenübermittlung an den Sponsor, die Zulassungsbehörde und – im Falle unerwünschter Ereignisse – an das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM). In der Praxis vertraut der Sponsor jedoch selten allein auf das Pseudonym „Teilnehmer-/Probandennummer“. Weil bei Zahlendrehern oder anderen Fehlern in der Ziffer eine Zuordnung zu weiteren Daten desselben Probanden unmöglich ist, wird die Nummer häufig um die Initialen und das Geburtsdatum des Probanden ergänzt. So

kann „im Notfall“ z.B. doch noch die richtige Studienakte im Prüfzentrum gefunden werden.

Hiergegen hatten wir schon bei früheren Prüfungen von Studienzentren Einwände geltend gemacht und auch die Ethikkommission der Hamburger Ärztekammer überzeugen können: Wenn das Gesetz ausdrücklich eine Pseudonymisierung verlangt, so ist dies datenschutzrechtlich zu verstehen: Der Datenempfänger darf das Pseudonym nicht entschlüsseln können.

Anfang 2007 fand zu diesem Thema unter unserer Leitung eine Diskussion mit dem BfArM und Datenschutzvertretern aus anderen Bundesländern statt. Einigkeit bestand darin, dass Initialen und Geburtsdatum kein sicheres Pseudonym darstellen: Dem Übermittlungsempfänger ist es in vielen Fällen ohne großen Aufwand möglich, daraus die Identität der betroffenen Person zu ermitteln.

Unabhängig von den Arzneimittelstudien führt das BfArM eine Datenbank für unerwünschte Arzneimittelwirkungen (UAW), zu der Krankenhäuser, Ärzte, Arzneimittelhersteller und Patienten Meldungen abgeben. Das Arzneimittelgesetz verpflichtet den Inhaber einer Arzneimittelzulassung ausdrücklich zur „Anzeige“ von unerwünschten Ereignissen, schreibt aber keine Pseudonymisierung vor. Das BfArM verbreitet dazu ein Meldeformular, das das volle Geburtsdatum, die Initialen und das Geschlecht des betroffenen Patienten abfragt. Wichtig ist ihm, Doppelmeldungen zu demselben Patienten und zum selben Ereignis zu erkennen und die Schwelle für eine Meldung möglichst niedrig zu halten.

In Einzelfällen will das BfArM aber auch feststellen können, ob es sich bei der Meldung eines unerwünschten Ereignisses im Rahmen einer Arzneimittelstudie um denselben Patienten handelt, zu dem auch außerhalb der Studie eine Meldung über die Nebenwirkung eines Vergleichspräparats eingegangen ist. Dazu benötige es Angaben zur Identität des Betroffenen, die beiden Meldungen gemeinsam sind. Dafür eigneten sich Geburtsdatum und Initialen. Das BfArM leitet Meldungen zu unerwünschten Ereignissen auch an die betroffenen Arzneimittelhersteller /Sponsoren weiter, die sie den früher übermittelten Probandendaten während der Arzneimittelprüfung zuordnen wollen. In beiden Fällen würde die Ergänzung des Pseudonyms jedoch die potentielle Entschlüsselung bedeuten.

Zur Strukturierung und Auflösung dieser komplexen Rechtslage haben wir mit dem Landesdatenschutzbeauftragten von Hessen eine Arbeitsleitlinie entwickelt. Sie schließt die Verwendung von Initialen gänzlich aus, lässt aber bei Meldungen über unerwünschte Ereignisse außerhalb von Arzneimittelstudien die Angabe des Geburtsdatums zu. Erfordert die Praxis, dass der Sponsor / Hersteller Probandendaten aus der Arzneimittelstudie mit späteren Meldungen über Nebenwirkungen personenbezogen zusammenführt, so muss der Gesetzgeber dafür ein datenschutzgerechtes Pseudonymisierungsverfahren

schaffen oder die Übermittlung des Geburtsdatums in Arzneimittelstudien ausdrücklich zulassen. Bis dahin wollen die Datenschutzbeauftragten die Verwendung des Geburtsdatums (und nur dieses) vorerst dulden, um die Arzneimittelsicherheit nicht zu gefährden. Das BfArM wurde vom Bundesbeauftragten für den Datenschutz aufgefordert, das Meldeformular zumindest bezüglich der Initialen zu ändern.

14.5 Patientendatenverwaltung in ärztlichen Kooperationspraxen

In der Frage, wie sich das Recht der Patienten auf freie Arztwahl auf die Organisation der Datenverarbeitung in Gemeinschaftspraxen auswirkt, fanden die Datenschutzaufsichtsbehörden der Länder in Hamburg eine gemeinsame Antwort. Eine Veröffentlichung im Ärzteblatt verbreitete sie bei der Zielgruppe.

Seit längerem waren wir mit Anfragen von Patienten und Ärzten zur elektronischen Patientendatenverwaltung in Gemeinschaftspraxen befasst. Patienten wollten nicht, dass ihnen unbekannte Kollegen des behandelnden Arztes freien Zugriff auf ihre Behandlungsdaten haben. Patienten sahen sich mit Werbepost der Praxis konfrontiert, obwohl der behandelnde Arzt die Gemeinschaftspraxis lange verlassen hatte. Ärzte, die aus Gemeinschaftspraxen ausschieden, wollen die Daten „ihrer" Patienten mitnehmen und sie damit den ehemaligen Kollegen in der Praxis vorenthalten.

Zu diesem Thema führten wir Gespräche mit der Kassenärztlichen Vereinigung und der Ärztekammer Hamburg. Wir vertraten die Auffassung, dass die gemeinsame Patientendatei in einer Gemeinschaftspraxis so angelegt werden muss, dass Patienten nicht behandelnde Arztkollegen vom Datenzugriff ausschließen und dass Ärzte bei Auflösung einer Gemeinschaftspraxis nur die Daten der von ihnen behandelten Patienten weiter nutzen können. Die Ärztekammer hielt dem entgegen, dass immer die gesamte Gemeinschaftspraxis Vertragspartner der Patienten werde und bestimme, welcher Arztkollege die Behandlung durch- oder fortführt. Dies habe notwendig die unbeschränkte gemeinsame Datenverarbeitung zur Folge.

Dieses arztrechtliche wie datenschutzrechtliche Problem machten wir zum Tagesordnungspunkt des sogenannten Düsseldorfer Kreises, des Zusammenschlusses der Obersten Aufsichtsbehörden über den Datenschutz im nicht öffentlichen Bereich, der 2007 in Hamburg tagte und von uns geleitet wurde. Die Datenschutzkolleginnen und -kollegen einigten sich in den wesentlichen Aussagen auf unsere Rechtsauffassung: Das in den ärztlichen Berufsordnungen herausgestellte Recht der Patienten auf freie Arztwahl gilt ausdrücklich auch für alle Formen der ärztlichen Kooperation, also auch im Gemeinschaftspraxen – und zwar unabhängig von der Frage, wer Vertragspartner des Patienten ist. Macht der Patient seinen Willen deutlich, dass er nur von einem bestimmten Arzt der Kooperationspraxis – und ggf. noch von dessen Vertreter – behandelt werden möchte, muss dieser Arzt die ärztliche Schweigepflicht

auch gegenüber seinen Kolleginnen und Kollegen in der Praxis wahren. Dies bedeutet, dass auch die EDV-Datei für die Patientendaten für diese Fälle jedenfalls die Möglichkeit eines Zugriffsausschlusses für die anderen Ärztinnen und Ärzte der Praxis vorsehen muss („mandantenfähiges System“).

In den Fällen, in denen der Patient seine Arztwahl nicht ausdrücklich ausübt, ist es eine Frage der Umstände, ob ein konkludentes Einverständnis des Patienten mit einer Vertretung und Zugriffsberechtigung aller Praxisärzte anzunehmen ist. Dies wird bei einer kleinen Gemeinschaftspraxis unter Eheleuten oder einer Notfallambulanz am Wochenende möglicherweise anders zu beurteilen sein, als bei einer psychiatrischen oder einer besonders großen und Fachrichtungs-übergreifenden Gemeinschaftspraxis. In jedem Falle ist allen Kooperationspraxen dringend zu raten, die Frage der Arztwahl und der möglichen Vertretung und Zugriffsberechtigung am Beginn einer Behandlung mit der Patientin oder dem Patienten klar zu regeln und auch in der elektronischen Patientendatei abzubilden.

Letzteres ist auch für die Kolleginnen und Kollegen der Kooperationspraxis selbst wichtig: Es erleichtert, ja ermöglicht überhaupt erst die gebotene Trennung der Patientendatensätze, wenn die Praxis aufgelöst wird, neue Ärzte hinzukommen oder Kollegen die Praxis verlassen. Hier geht es nicht nur um datenschutzrechtliche, sondern auch um wettbewerbsrechtliche und damit ökonomische Fragen. Es ist damit von großer Bedeutung, bereits bei der Auswahl des elektronischen Patientenverwaltungssystems auf diese technischen Möglichkeiten zu achten.

Unter dem Titel „Patientendaten in ärztlichen Kooperationen sicher verwalten“ haben wir die Sach- und Rechtslage und die im Düsseldorfer Kreis abgestimmte Auffassung im Deutschen Ärzteblatt vom 7. September 2007 publiziert und so den direkt Betroffenen zugänglich gemacht.

14.6 Prüfung der Asklepiosklinik Barmbek

Die datenschutzrechtliche Prüfung des neuen Krankenhauses offenbarte eine Reihe von Mängeln und gab Anlass zu weiteren Kontrollen insbesondere zentral administrierter Systeme.

Anfang des Jahres 2007 führten wir vor Ort in der neu erbauten Asklepiosklinik Barmbek (AKB) eine technische und datenschutzrechtliche Prüfung durch, die wir durch Gespräche in der Zentrale der Asklepios Kliniken LBK Hamburg GmbH vertieften. Über folgende Probleme und Defizite setzten wir uns mit der Datenschutzbeauftragten der Asklepioskliniken und den zuständigen technischen Verantwortlichen auseinander:

Im AKB dürfen die Arbeitsplatzrechner nach einer Dienstvereinbarung auch zum privaten Surfen im Internet und zum privaten E-Mail-Austausch genutzt werden. Unsere Forderung, die dadurch entstehenden Sicherheitsrisiken

durch eine Terminalserver-Lösung auszuschließen, wurde mit dem Argument, dies wäre wenig anwenderfreundlich, verworfen. Verwiesen wurde auf verschiedene Sicherheitselemente und einen Penetrationstest im Mai 2007 mit positivem Ergebnis. Da dieser jedoch wesentliche Sicherheitslücken unberücksichtigt ließ, haben wir die Durchführung eines weiteren Tests gefordert, um insbesondere die Zugriffsmöglichkeiten von „Innentätern“ im AKB prüfen. Der E-Mail-Dienst wird bis zur Einführung eines Digital Rights Management und eines speziellen Authentifizierungssystems Anfang 2008 derzeit nicht für den Versand vertraulicher personenbezogener Daten genutzt.

Besonderes Augenmerk richteten wir auf die Patientenaufnahme. Wird ein Patient stationär aufgenommen, wird bei der Erfassung der Daten durch Eingabe des Patientennamens zunächst der Name der Asklepiosklinik angezeigt, in der der Patient früher einmal behandelt wurde. Bei einem früheren Aufenthalt in der Klinik Barmbek selbst kann die aufnehmende „Team Partnerin Administration“ (Aufnahmekraft mit weiteren Aufgaben) auch alle medizinischen Falldaten, einschließlich der Diagnosen und Operationsdaten seit 1996 lesen. Dies gilt selbst dann, wenn der Patient eine Heranziehung früherer Unterlagen ausdrücklich ablehnt – z.B. weil diese von Behandlungen in ganz anderen, nicht betroffenen AKB-Abteilungen stammen oder um eine unvoreingenommene fachliche Zweitmeinung zu erhalten. Diese weitreichende Zugriffsmöglichkeit des Aufnahmepersonals verstößt gegen das Hamburgische Krankenhausgesetz. Wir haben im Rahmen der anstehenden Umstrukturierungen Abhilfe gefordert. Da SAP eine entsprechende technische Lösung nicht zulässt, muss zumindest organisatorisch ein Verbot des Falldatenaufrufs durchgesetzt werden, wenn der Patient dazu nicht zuvor seine Einwilligung gibt. Ein bloßer Passus im Behandlungsvertrag, dass frühere Behandlungsunterlagen – auch von anderen Abteilungen – herangezogen werden können, widerspricht dem informationellen Selbstbestimmungsrecht des Patienten. Es kann im Einzelfall aus Sicht des Patienten gute Gründe dafür geben, dass diese Unterlagen vom aktuell behandelnden Arzt nicht eingesehen werden sollen. Es bedarf daher einer Modifikation des Behandlungsvertrages.

Bei einzelnen Aufnahmedaten haben wir die Freiwilligkeit der Angabe verdeutlicht, bei Freitextfeldern, die nur für bestimmte Mitteilungen bzw. in der Praxis gar nicht benutzt werden, haben wir uns für eine inhaltliche Festlegung dieser Felder eingesetzt bzw. ihre Streichung erreicht. Die Dienstanweisung Datenschutz und die Formular-Einwilligung in die Datenübermittlung an den Hausarzt werden bei der anstehenden Überarbeitung unsere Korrekturen berücksichtigen.

Im Nachgang zur Prüfung wurde in weiteren Gesprächen deutlich, dass zentrale, für alle Asklepios-Krankenhäuser in Hamburg implementierte Systeme wie das SAP Berechtigungssystem und ein Business Warehouse System noch einer vertieften Nachschau bedürfen. Diese wird zusammen mit dem zum Jah-

reswechsel 2007 / 2008 neu bestellten betrieblichen Datenschutzbeauftragten erfolgen. Mit der scheidenden Datenschutzbeauftragen der Hamburger Asklepios-Kliniken pflegten wir eine vertrauensvolle Zusammenarbeit.

14.7 Einwilligung in medizinische Forschungsprojekte

Die Einwilligung in die Nutzung von Proben und Behandlungsdaten zu Forschungszwecken stößt an Grenzen der Fähigkeit und Bereitschaft der betroffenen Patienten, komplizierte, aber datenschutzrechtlich gebotene Aufklärungen zu erfassen.

Schon im letzten Tätigkeitsbericht (20. TB, 14.4) hatten wir ausführlich auf eine Reihe von Problemen hingewiesen, die angesichts der Veränderungen in der Forschungslandschaft mit der Einholung von Patienteneinwilligungen in Forschungsprojekte verbunden sind. Für einen Teil dieser Fragen konnten im Berichtszeitraum Antworten gefunden werden, z.B. durch die Neufassung der Forschungsklausel und die Einführung einer Vorschrift für Biobanken im Hamburgischen Krankenhausgesetz (oben 14.1).

Zu anderen Themen wurde die Diskussion bundesweit fortgesetzt. So wurde der stellvertretende Dienststellenleiter als unabhängiger Sachverständiger zu einer Expertenanhörung des Bundestags-Gesundheitsausschusses eingeladen, um zum Entwurf eines Gendiagnostikgesetzes Stellung zu nehmen. Die Aufklärung und Einwilligung in die genetische Forschung spielte dabei eine wesentliche Rolle.

Darüber hinaus hat sich dieser Mitarbeiter an der bundesweiten Debatte auch mit einem wissenschaftlichen Beitrag in der Fachzeitschrift Medizinrecht beteiligt. Unter dem Titel „Datenschutzrechtliche Einwilligungen in medizinische Forschung – Selbstbestimmung oder Überforderung der Patienten?“ hat er versucht, einen Mittelweg zu finden zwischen den tendenziell rigiden datenschutzrechtlichen Anforderungen an wirksame Einwilligungen einerseits und der tatsächlichen Befindlichkeit der Patienten andererseits. Gerade in Universitätskliniken kann auf den einzelnen Patienten eine Fülle von Einwilligungen zukommen – zusätzlich zu den rein medizinischen. Das Interesse des Patienten konzentriert sich jedoch auf seine Behandlung und Heilung, nicht auf komplexe Forschungsfragen und -infrastrukturen. Es geht daher darum, dem Patienten die Entscheidungsgewalt in Bezug auf die grundsätzliche Teilnahmebereitschaft zu erhalten und ihn zugleich von Details zu entlasten.

In diesem Sinne haben wir mit dem Universitätsklinikum Hamburg-Eppendorf für verschiedene Fallkonstellationen Musterformulare entwickelt, die möglichst kurz und übersichtlich den Gegenstand umschreiben, auf den sich die jeweilige Einwilligung bezieht. Kaum reduzieren konnten wir die Vielzahl der nötigen

Einwilligungen, die nicht zuletzt der starken Aufsplitterung der UKE-Gruppe in rechtlich selbstständige Einheiten geschuldet ist (vgl. oben 14.2).

Ein besonders heikles Thema ist die Forschung an nicht einwilligungsfähigen Personen (z.B. Kindern, dementen Erwachsenen). Hierzu beteiligten wir uns an einer bundesweiten Erhebung und einem Workshop der Telematikplattform für Medizinische Forschungsnetze e.V. Es ging um die Frage, wie diese Personen durch Vertretungspersonen und / oder institutionelle Sicherungen im Forschungsprojekt (unabhängige Zweitbeurteilung) auch in ihrer informationellen Selbstbestimmung ausreichend geschützt werden können. In diesem Zusammenhang erreichte uns auch eine Anfrage des Deutschen Kinderkrebsregisters in Mainz: Welche Konsequenzen soll es haben, wenn die Kinder, deren Eltern in die Datenverarbeitung im Kinderkrebsregister eingewilligt hatten, volljährig bzw. selbst einwilligungsfähig werden? Wir vertraten dazu die Auffassung, dass die jungen Erwachsenen jedenfalls darüber aufgeklärt werden müssen, dass ihre Daten im Register geführt und zu Forschungszwecken genutzt werden. Anderenfalls könnten sie ihr Recht auf jederzeitigen Widerruf der in Ihrem Namen erteilten Einwilligung nicht geltend machen. Eine Art „Ewigkeitsgarantie“ wollten wir der elterlichen Entscheidung nicht einräumen, eine Widerspruchslösung hielten wir allerdings für ausreichend – auch und gerade vor dem Hintergrund der wissenschaftlichen Bedeutung dieser Datensammlung.

15. Gebühreneinzugszentrale GEZ

Ein besseres Datenschutzniveau im Umgang der GEZ mit personenbezogenen Daten zu erreichen, ist ein mühsames Geschäft.

Im 20. TB, 15.1, hatten wir über zwei Regelungen des Rundfunkgebührenstaatsvertrags (RGebStV) im 8. Rundfunkänderungsstaatsvertrag (8. RÄndStV) berichtet, die datenschutzrechtlich kritisch zu bewerten waren:

- Zur Beantragung der Rundfunkgebührenbefreiung sind der GEZ vollständige Leistungsbescheide vorzulegen.
- Die GEZ darf sich zur Feststellung, ob ein Rundfunkteilnehmerverhältnis vorliegt, des Adresshandels bedienen.

Die Landesdatenschutzbeauftragten hatten daher gefordert, im 9. RÄndStV zu regeln, dass bei einem Antrag auf Rundfunkgebührenbefreiung der GEZ nicht mehr der vollständige Leistungsbescheid vorzulegen ist, sondern eine spezielle Kurzbescheinigung, die nur die für die Entscheidung der GEZ über die Befreiung notwendigen Daten enthält. Dieser Vorschlag wurde aufgegriffen. Er konnte aber leider aus zeitlichen Gründen in den 9. RÄndStV, der am 1. März 2007 in Kraft trat, nicht mehr eingefügt werden; die Regelung wird aber Eingang in den 10. RÄndStV finden, der voraussichtlich zum 1. September 2008

in Kraft treten wird. Allerdings wird diese Neuregelung des § 6 Abs. 2 RGebStV bereits seit Monaten im Vorgriff praktiziert. Wie in den anderen Bundesländern haben sich auch in Hamburg die zuständigen Sozialdienststellen mit der GEZ auf Formulare „Bescheinigung zur Vorlage bei der GEZ“ geeinigt, die in PROSA erstellt werden.

Die Forderung der Landesdatenschutzbeauftragten, den Adressdatenabgleich durch die GEZ zu beschränken und ohne generelle Verweisung auf § 28 des Bundesdatenschutzgesetzes vollständig in § 8 Abs. 4 RGebStV zu regeln, wird voraussichtlich ebenfalls im 10. RÄndStV umgesetzt.

16. Ausländerangelegenheiten

16.1 Lesender Zugriff von Polizei und Verfassungsschutz auf die Ausländerdatei

Die erforderlichen Rechtsänderungen für den Zugriff auf die Ausländerdatei PaulaGo wurden geschaffen. Die Anzahl der angeschlossenen Arbeitsplätze hat sich nach der Erforderlichkeit für die Aufgabenwahrnehmung zu richten.

Über das Begehren von Polizei und Verfassungsschutz, zur Bekämpfung des islamistischen Terrorismus und zur Bekämpfung bestimmter Straftaten lesenden Zugriff auf das Ausländerfachverfahren PaulaGo zu nehmen, hatten wir bereits ausführlich berichtet (vgl. 20.TB, 16.2). Die rechtliche Grundlage für diesen Zugriff wurde mit der Zweiten Verordnung zur Änderung der Ausländerdatenverarbeitungsverordnung vom 24. Juli 2007 beschlossen.

Unsere Empfehlungen hatten sich seinerzeit hinsichtlich der gestaffelten Zugriffsvoraussetzungen für die Polizei unter anderem an der Systematik des Ausländerzentralregistergesetzes (AZRG) orientiert. Das AZRG ist inzwischen jedoch novelliert worden und differenziert nicht mehr nach der Art der zu übermittelnden Daten. Sämtliche Daten können nun auf Ersuchen und im Wege des automatisierten Abrufs übermittelt werden.

Wir haben daher einer entsprechenden Vereinfachung auch im angestrebten Verfahren zugestimmt.

Diskussionsbedarf ergab sich zu der Frage, wie viele Arbeitsplätze des Landesamtes für Verfassungsschutz mit einem Zugang zum System auszustatten wären. Während die Polizei die Erforderlichkeit für nur fünf Arbeitsplätze sah, wollte das LfV zunächst, dass dort alle Arbeitsplätze angeschlossen werden, da es keine gesonderte Einrichtung von Arbeitsplätzen zur Bekämpfung des islamistischen Terrorismus gebe.

Maßstab hierfür ist die Frage, an welchen Plätzen ein so schneller Zugriff erforderlich ist, dass er im Wege des automatisierten Abrufs erfolgen muss.

Für die Arbeitsplätze, an denen Einbürgerungsangelegenheiten bearbeitet werden, wurde dies verneint. Hier reicht es aus, wenn Einsicht in die Ausländerakte genommen wird.

Für beide Behörden wurde ein Stichprobenverfahren vorgeschrieben, durch das die Zulässigkeit der Abrufe anlassunabhängig zu prüfen ist. Zurzeit erwarten wir prüffähige Unterlagen für dessen technische Umsetzung.

16.2 Einrichtung des Hamburg Welcome Centers

Sollen Mitarbeiter für verschiedene sensible Fachaufgaben gleichzeitig zuständig sein, müssen gesetzlich vorgeschriebene Übermittlungsgrenzen durch zusätzliche organisatorische Maßnahmen sichergestellt werden.

Seit Anfang April 2007 steht das Hamburg Welcome Center (HWC), eine Dienststelle des Bezirksamts Mitte, allen Neubürgern als erste Anlaufstelle für Beratung und Informationen in den Räumlichkeiten der Handelskammer Hamburg zur Verfügung. Neben dieser Aufgabenstellung ist das HWC aber auch zuständige Stelle für qualifizierte Ausländer und ihre Familienangehörigen in allen ausländer- und melderechtlichen Angelegenheiten. Mit dieser Aufgabenkonzentration sollen dieser Zielgruppe in angenehmer Atmosphäre nach dem Grundsatz one face to the customer Zeit und Wege erspart werden.

Datenschutzrechtlich von Bedeutung ist, dass hier ein Sachbearbeiter für zwei besonders sensible Bereiche (Melde- und Ausländerwesen) gleichzeitig zuständig sein soll. Nach dem datenschutzrechtlichen Grundsatz der informationellen Gewaltenteilung, der die personelle Trennung verschiedener sensibler Fachaufgaben erfordert und eine gegenseitige Nutzung der Daten nur in eng begrenztem, gesetzlich geregeltem Unfang zulässt, sind die Bereiche Meldewesen und Ausländerangelegenheiten grundsätzlich getrennt zu bearbeiten.

Andererseits steht dem Senat die Organisationshoheit über die Verwaltungsstruktur zu.

Um hier zu einem datenschutzgerechten Ausgleich zu gelangen, haben wir empfohlen, die Mitarbeiter per Dienstanweisung zu verpflichten, ohne besondere Einwilligung der Betroffenen nur diejenigen Daten des jeweils anderen Verfahrens zu nutzen, die gesetzlich gegenseitig übermittelt werden dürfen. Daneben haben wir einige Vorschläge zur Ausgestaltung der Dienststelle gemacht.

Bei einem Besuch im Oktober 2007 konnten wir uns von der datenschutzgerechten Ausgestaltung der Dienststelle überzeugen. Auf unsere Nachfrage erfuhren wir, dass es bisher auch faktisch keine Probleme mit der Doppelzuständigkeit gegeben habe, da bei den Vorsprachen zunächst nur melderechtliche und erst später ausländerrechtliche Fragen betroffen seien.

17. Verkehr

17.1 Schwerpunkte in länderübergreifenden Verfahren und im Zulassungsbereich

Sowohl für Hamburg als auch länderübergreifend ist der Bereich Kfz-Zulassung Gegenstand mehrerer Projekte, die erhebliche datenschutzrechtliche Fragestellungen aufwerfen.

Im Bereich Verkehr geht die Tendenz zu länderübergreifenden Verfahren. Im Berichtszeitraum lag der Schwerpunkt im Bereich des Zulassungswesens. Die dort initiierten Verfahren beinhalten vielfältige Anstrengungen, das Massengeschäft der An-, Um- und Abmeldung von Kfz sowohl für den Bürger komfortabler als auch für die Verwaltung effizienter zu gestalten.

Das Projekt Lebenslage Umzug in der Metropolregion Hamburg (Kfz-Bereich) soll den Bürgern zur Vermeidung langer Behördenwege ermöglichen, länderübergreifend Ummeldungen auch bei einer anderen als der hierfür zuständigen Stelle vorzunehmen (siehe 17.2).

Das E-Government-Projekt Kfz-Ummeldung des Landesbetriebs Verkehr (LBV) soll die Sachbearbeitung vorbereiten und so das Anmeldeverfahren beschleunigen und Wartezeiten verkürzen (siehe 17.3).

Das von Hamburg federführend betriebene Projekt Deutschland Online Kfz hat darüber hinaus zum Ziel, die nach Lebenslagen beteiligten Personen und Stellen online und ohne Medienbruch in die Sachbearbeitung einzubeziehen. Gedacht ist an die betroffenen Bürger, Kfz-Händler, Versicherungen, TÜV u.a. Dies wird eine Reihe von Rechtsänderungen erfordern, die auf ihre datenschutzrechtliche Zulässigkeit kritisch geprüft werden müssen. Das Projekt befindet sich jedoch noch in der Phase der Erstellung eines Fachkonzepts. Prüffähige Unterlagen liegen bisher nicht vor.

17.2 Metropolregion Kfz

Die technische Unterstützung der Kfz-Ummeldungen in der Metropolregion bedarf einer gesetzlicher Ermächtigung. Es muss langfristig nachvollzogen werden können, wer wann welche Daten im Datensatz aufgenommen und geändert hat.

Das Projekt Metropolregion sieht vor, dass Bürger bei Umzügen innerhalb der Region ihre melderechtlichen und verkehrsrechtlichen Ummeldungen auch bei anderen Behörden vornehmen können und dürfen.

Das bedeutet für die Kfz-Ummeldung, dass diese nicht mehr bei einem bestimmten Verkehrsamt vorgenommen werden muss, sondern bei jedem beteiligten Verkehrsamt – und später auch bei den Meldeämtern – erledigt werden kann.

Hierzu stehen wir mit dem Projekt seit Sommer 2006 in intensivem Austausch.

Das ursprüngliche Konzept sah vor, dass hierfür die den jeweiligen Antrag bearbeitende Zulassungsbehörde auf den im Kfz-Register der Wegzugsgemeinde gespeicherten Datensatz zugreifen, ihn selbständig bearbeiten und ihn anschließend in das Kfz-Register der Zuzugsgemeinde einspeisen können sollte.

Wir haben darauf hingewiesen, dass der gegenseitige Zugriff der Zulassungsbehörden auf ihre örtlichen Register im Straßenverkehrsrecht bisher nicht vorgesehen ist und nach hamburgischem Landesrecht (§§ 11, 11 a Hamburgisches Datenschutzgesetz) einer Rechtsvorschrift bedarf. Da dies landesrechtlich bei länderübergreifenden Verfahren im Ergebnis den Abschluss eines Staatsvertrages mit den Nachbarländern erfordern würde, haben wir empfohlen, den Änderungsbedarf an den Bundesgesetzgeber heranzutragen.

Dies soll im Zusammenhang mit dem Projekt Deutschland Online Kfz weiterverfolgt werden.

Das Projekt hat jedoch zugesagt, die anstehende Pilotierung technisch so zu gestalten, dass sie auf der Grundlage des geltenden Rechts erfolgen kann.

Dies bedeutet, dass die bisher gespeicherten Daten aus dem Zentralen Fahrzeugregister beim Kraftfahrtbundesamt (KBA) abgerufen ,von der unzuständigen Zulassungsbehörde bearbeitet und an die Zulassungsbehörde der Zuzugsgemeinde übersandt werden, wo sie von zuständigen Mitarbeitern ins Fachverfahren bzw. ins örtliche Register eingepflegt werden.

Auch dabei muss sichergestellt sein, dass die Datensätze der teilnehmenden Behörden sicher gegeneinander abgeschottet sind, dass eine sichere Authentifizierung der zugreifenden Behörden gewährleistet ist (z.B. über qualifizierte elektronische Signaturen oder über das geschlossene TESTA-Netz), dass die Schutzmaßnahmen für den hohen Schutzbedarf der Datensätze ausreichen, dass Zugriffe und Veränderungen langfristig protokolliert werden und dass Emails verschlüsselt versandt werden. Nach dem Grundsatz der Datensparsamkeit muss für die Betroffenen eine Barzahlung der anfallenden Gebühren, Steuern und Rückstände möglich sein.

Bis Redaktionsschluss lagen die zugesagten Überarbeitungen des Technikkonzepts und der Kooperationsvereinbarung noch nicht vor.

17.3 Online-Angebote des Landesbetriebs Verkehr

Das Angebot an Online-Verfahren wurde weiter ausgebaut. Für eine medienbruchfreie Nutzung der Online-Verfahren fehlen mögliche technische Sicherheitsmaßnahmen.

Schon im letzten Bericht haben wir über Online-Angebote des Landesbetriebs Verkehr (LBV) berichtet (vgl. 20. TB, 17). Von den verschiedenen geplanten Verfahren haben wir zwei Verfahren bis zur Produktivsetzung begleitet:

- Führerschein-Erstantrag

  Fahrschulen sollen zur Beschleunigung des Verfahrens die Anträge für ihre Fahrschüler online stellen können. Bisher müssen alle erforderlichen Unterlagen in Papierform nachgereicht werden.

  Das Verfahren kann nach wie vor nicht medienbruchfrei angeboten werden, da die erforderlichen Unterlagen nur mit qualifizierter elektronischer Signatur rechtswirksam elektronisch übersandt werden können und für die Übermittlung medizinischer Daten weitere technische Sicherheitsmaßnahmen erforderlich sind. Die Finanzbehörde hat angekündigt, diese Voraussetzungen zu schaffen.

  Darüber hinaus darf von Ausländern nicht mehr die Nummer des Ausweispapiers und der Aufenthaltsstatus abgefragt und gespeichert werden. Hierfür besteht keine Rechtsgrundlage. Weiterhin haben wir verschiedene Anregungen zur Ausgestaltung der Antragsformulare und Masken gegeben, die vom LBV übernommen wurden.

  Das Verfahren wurde seit August 2007 von drei Fahrschulen getestet. Eine Öffnung für alle Fahrschulen erfolgte im Dezember 2007.

- Kfz-Ummeldung

  Mit diesem Online-Angebot soll erreicht werden, dass Diejenigen, die in Hamburg ein Kfz an- oder umzumelden haben, ihre Daten für eine Ummeldung vor ihrem Besuch beim LBV selbst elektronisch eingeben können. Soweit gewünscht, können bei Zuzug von außerhalb Hamburgs Angaben aus dem Verfahren Wunschkennzeichen (vgl. 20. TB, 17) berücksichtigt werden. Dadurch sollen sich die Warte- und Bearbeitungszeiten verkürzen.

  Im Verfahren hat der Antragsteller bestimmte Kfz-Daten einzugeben und erhält nach einem Kurzabgleich mit dem Fahrzeugregister die Rückmeldung, ob das Fahrzeug bekannt ist oder nicht. Zusätzlich hat er die geänderten Adressdaten einzugeben und kann als Zugezogener die Einzugsermächtigung für die Steuerverwaltung vorbereiten. Das Verfahren speichert die Angaben in einem Zwischenspeicher. Bei Vorsprache prüft der Sachbearbeiter die Angaben und gibt sie in das Fachverfahren ein. Anschließend können die neuen Papiere ausgedruckt werden.

  Verfolgt der Antragsteller die Umschreibung nicht weiter, werden seine Angaben nach Ablauf von einem Monat automatisch gelöscht.

  Es war sicherzustellen, dass das Verfahren nicht als „Auskunftssystem“ genutzt werden kann und die Bescheinigung nicht mehr Angaben über das Kfz enthält, als vom Antragsteller eingegeben wurden. So werden auch keine Versicherungsdaten angezeigt.

  Das Verfahren stand bei Redaktionsschluss unmittelbar vor der Einführung.

18. Wirtschaftsverwaltung

18.1 Zeitschrift für Hamburgs Auszubildende „azubinews“

Die Kammern dürfen die Privatanschrift von Auszubildenden nur dann für die Versendung einer Zeitschrift für Auszubildende nutzen, wenn die Zeitschrift von den Kammern selbst herausgegeben wird.

Wir erfuhren, dass den Hamburger Auszubildenden eine Zeitschrift, die sie als Auszubildende ansprach, von einem privaten Verlag an ihre Privatadresse geschickt wurde. Neben alters- und zielgruppengerechten Lifestyle-Themen bot die Zeitschrift auch eine Vielzahl von online- Gewinnspielen an und lud zu einer regelmäßigen Club-Veranstaltung ein, bei der den Auszubildenden gegen Vorlage des Adressaufklebers freier Eintritt gewährt wurde. Auf dem Titel des Blattes stand: „In Zusammenarbeit mit der Handwerkskammer und der Handelskammer“. Laut Impressum war es „das offizielle Magazin für Hamburgs Auszubildende“. Im Inhaltsverzeichnis befand sich ein Hinweis darauf, wie das Magazin abbestellt werden könne.

Es stellte sich heraus, dass die Kammern mit dem Verlag einen Vertrag geschlossen hatten, in dem sie sich verpflichteten, dem Verlag für die Versendung seiner Zeitschrift „azubinews“ regelmäßig die aktuellen Adressen aus den Auszubildendenverzeichnissen unentgeltlich zu überlassen. Im Gegenzug wurde der Verlag lediglich verpflichtet, im Impressum neben den üblichen Angaben einen Hinweis auf die Kammern nebst Anschriften aufzunehmen. Ein Gestaltungsrecht bzw. die Hoheit über die inhaltliche Ausgestaltung stand den Kammern nicht zu. Ihre Textvorschläge waren auf eine Seite pro Ausgabe begrenzt. Es fehlte auch eine Regelung, die die weitere Nutzung der Adressdaten zu kommerziellen Zwecken ausschloss.

Hiergegen bestanden datenschutzrechtliche Bedenken. Die Adressdaten der Auszubildenden stehen den Kammern nur im Rahmen ihrer gesetzlichen Aufgaben nach der Handwerksordnung bzw. dem Gesetz zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern sowie dem Berufsbildungsgesetz zur Verfügung.

Die Übermittlung der Daten an ein privates Anzeigenblatt zur privatrechtlichen Nutzung gehört nicht zu den gesetzlichen Aufgaben der Kammern. Zulässig ist lediglich die Versendung eigener oder in ihrem Auftrag erstellter Informationsblätter an die Auszubildenden. Darüber hinaus können Adressdaten nur genutzt werden, wenn die Betroffenen vorab ausdrücklich eingewilligt haben.

Unter den Gesichtspunkten von Datensparsamkeit und Erforderlichkeit stellte sich zudem die Frage, ob das Blatt die Auszubildenden nicht auch über eine Verteilung in den Schulen oder Ausbildungsbetriebe erreichen könnte.

Hierzu hatten die Kammern ausgeführt, dass die Zeitschrift die Empfänger mittels Verteilung nicht hinreichend sicher erreichen würde, und auf Konflikte mit Ausbildungsbetrieben verwiesen. Über die Auslage einer Zeitschrift würden bekanntermaßen weniger Personen erreicht als durch persönliche Adressierung.

Da den Kammern sehr an einer jugendgerechten Ansprache gelegen war, für die sie aber auf fachliche Unterstützung nicht verzichten könnten, haben wir mit den Beteiligten einen Vertrag entwickelt, der die Anforderungen an eine zulässige Auftragsdatenverarbeitung erfüllt: Der Verlag wurde mit der inhaltlichen Gestaltung der Zeitschrift und ihrer Zusatzangebote beauftragt, die presserechtliche Verantwortlichkeit und das Letztentscheidungsrecht über die Inhalte verblieb aber bei den Kammern. Wir haben sichergestellt, dass bei Gewinnspielen die erlangten Email-Adressen ausschließlich für die Gewinnermittlung genutzt werden durften und anschließend zu vernichten waren. Der Clubausrichter durfte keine Adressaufkleber, die als Eintrittskarten dienen, einbehalten.

Daneben wurden eindeutige Regelungen aufgenommen, wie der Verlag und ein von ihm beauftragter Frankierdienst mit den überlassenen Adressdaten umzugehen hätten.

Bei dieser Ausgestaltung haben wir es für vertretbar gehalten, wenn die Auszubildenden auch weiterhin ohne vorherige Einwilligung beliefert werden, sofern der Hinweis auf die Möglichkeit des Abbestellens regelmäßig und deutlich sichtbar erhalten bliebe.

Wie wir zu Redaktionsschluss von der Handelskammer erfuhren, ist es zu keinem Neuabschluss des Vertrages zwischen den Beteiligten gekommen; die Kammern zeigten aber weiterhin ein großes Interesse an einem solchen Projekt.

18.2 Multifunktionales Standort-Informationssystem IHK-MUSIS

Die Verknüpfung von Geobasisdaten mit personenbezogenen Daten von Mitgliedern der Handelskammer und ihre anschließende Vermarktung ist nur aufgrund einer speziellen Rechtsvorschrift oder mit Einwilligung der Betroffenen zulässig.

Mit dem Verfahren IHK-MUSIS hat die Handelskammer Hamburg mit neun weiteren Handelskammern aus Schleswig-Holstein, Niedersachsen und Mecklenburg-Vorpommern ein gemeinsames Standort-Informationssystem aufgebaut, das die kammereigenen Stammdaten von ca. 300.000 Mitgliedern für diese Kammern per automatisiertem Abruf zur Aufgabenwahrnehmung nutzbar macht. Diese Daten können mit verschiedenen digitalen Karten der Landesvermessungsämter im Maßstab zwischen 1:500 und 1:200 000 georeferenziert werden. So kann eine schnelle Orientierung zu einzelnen Grundstücken, Quartieren, Straßen oder Regionen erfolgen.

Es war vorgesehen, bestimmte Firmendaten, die nach § 9 Absatz 4 des Gesetzes zur vorläufigen Regelung des Rechts der Industrie- und Handelskammern (IHKG) zur Förderung von Geschäftsabschlüssen und zu anderen dem Wirtschaftsverkehr dienenden Zwecken an nicht-öffentliche Stellen übermittelt werden dürfen, georeferenziert im Internet für jedermann zum Abruf anzubieten. In den Standortbildern sollte die räumliche Verteilung der Unternehmen, differenziert nach Branchen und Beschäftigtengrößenklassen, enthalten sein. Die restlichen Daten, nämlich ursprünglich nur Firmenname, Name des Verantwortlichen, Anschrift und Telekommunikationsdaten, sollten als Listen zugefügt werden.

Werden zum Beispiel als Grundlage Liegenschaftskarten verwendet, sind darin neben dem Grundriss des Grundstücks selbst zusätzlich auch Angaben zu Flurstücksgrenzen, Nutzungsart und Art und Umfang der Bebauung enthalten.

Das Verfahren war datenschutzrechtlich von Belang, da nicht nur Firmendaten, sondern auch Daten von Kleingewerbetreibenden und Einzelpersonengesellschaften betroffen sind. Für diese Personengruppen gelten neben dem IHKG auch die Schutzvorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG).

Unsere hauptsächlichen Bedenken richteten sich gegen die namensbezogenen Übermittlungen an private Dritte. Das sind in diesem Zusammenhang auch andere Mitglieder derselben Kammer. Daneben wurden Verfahrensfragen behandelt, die mit der gemeinsamen Datenverarbeitung verbunden waren.

Wir haben darauf hingewiesen, dass die Verknüpfung der Mitgliedsdaten mit an sich zunächst anonymen Geodaten deren Anonymität aufhebt und diese gezielt hergestellten personenbezogenen Geodaten nicht ohne Einwilligung der Betroffenen oder aufgrund spezieller Rechtsvorschriften an Dritte übermittelt werden dürften.

Auch das Vermessungsgesetz selbst fordert eine Einwilligung der Betroffenen, wenn neben dem Kartenmaterial die dort genannten personenbezogenen Daten von den ursprünglichen Abnehmern an Dritte weitergegeben werden sollen.

Einen Rückgriff auf die allgemeinen Übermittlungsvorschriften des HmbDSG, auf den die Kammer sich berief, hielten wir angesichts des Wortlauts des § 9 Abs. 4 IHKG nicht für zulässig. Er zählt die an nicht-öffentliche Stellen übermittelbaren Daten abschließend auf und sieht – im Gegensatz zur Übermittlung an öffentliche Stellen in Abs. 6 – einen Rückgriff auf das HmbDSG nicht vor.

Daneben ergab sich Regelungsbedarf hinsichtlich des gemeinsam betriebenen Verfahrens und der angestrebten Abrufe durch Dritte.

Die Handelskammer Hamburg hat deshalb eine Satzung erlassen, in der die erforderlichen Regelungen getroffen wurden. Auch in Satzungen können da-

tenschutzrechtliche Befugnisse geregelt werden. Die Behörde für Wirtschaft und Arbeit als Aufsichtsbehörde über die Handelskammer hat die Regelungen als von der Satzungsbefugnis der Kammern gedeckt angesehen.

18.3 Automationsvorhaben Starter Center der Handwerkskammer Hamburg

Auch Angebote zur freiwilligen Datenverarbeitung sind so datenschutzfreundlich wie möglich zu gestalten. Die dafür notwendige Einwilligung darf insbesondere nicht zu einer beliebig definierbaren Datenverarbeitung auf Vorrat genutzt werden.

Im Herbst 2006 stellte uns die Handwerkskammer Hamburg das Vorhaben Starter Center für Existenzgründer vor. Das von einer privaten Firma entwickelte Verfahren wird in ähnlicher Form zum Teil seit längerer Zeit von anderen Kammern angeboten.

Auf der Grundlage einer Einwilligungserklärung unterstützt das Verfahren Existenzgründer dadurch, dass es alle Angaben, die für die konkrete Existenzgründung im Einzelfall von Handwerkskammer, Verbraucherschutzamt, Agentur für Arbeit, Rentenversicherungsträger, Berufsgenossenschaft, Innung und Finanzamt abgefragt werden, zusammenfasst. Alle Einzelangaben sind nur einmal in ein Metaformular einzugeben und werden daraus automatisiert in die verschiedenen Formularvordrucke der vorgenannten Stellen übertragen.

Auf diese Weise wird allerdings eine Vielzahl von personenbezogenen Daten bei der Kammer zusammengeführt, die weit über diejenigen Daten hinausgeht, die der Handwerkskammer bei der Anmeldung gesetzlich zu offenbaren wären.

Im Gegensatz zu den Angeboten anderer Kammern wurde der Datenkatalog von ca. 300 auf ca. 1000 mögliche Angaben erweitert, was nach unseren Feststellungen aus einer erheblich erweiterten Datenerhebung im Steuerbereich folgte. Diese weiteren Daten werden bisher lediglich bilateral zwischen Finanzamt und Betroffenen unter dem Schutz des Steuergeheimnisses ausgetauscht. Betroffen sind dabei eine Reihe besonders sensibler Daten wie Religionszugehörigkeit, Personalausweisnummer, Art und Höhe sonstiger Einnahmen, auch von Ehegatten und Kindern.

Das hier vorgestellte freiwillige Verfahren sollte einen ersten Schritt in Richtung einer medienbruchfreien Gewerbeanmeldung aus einer Hand darstellen. Da jedoch noch keine qualifizierte elektronische Signatur als Unterschriftersatz zur Verfügung steht, erfolgt zunächst keine automatisierte Weiterleitung der ausgefüllten Formulare an die jeweiligen Stellen. Der Betroffene hat daher die Anträge noch auszudrucken, zu unterschreiben und selbst an die jeweiligen Stellen zu übersenden. Lediglich eine Übernahme der Daten zur Handwerksrolle sollte automatisiert unterstützt werden.

Es war dennoch geplant, dass alle eingegebenen Daten von der Kammer mehrere Jahre gespeichert werden und für Beratungen und gezielte Mitgliederansprache sowie statistische Auswertungen genutzt werden sollten.

Unsere Bedenken bezogen sich im Wesentlichen auf folgende Bereiche:

Die Kammer als Teil der öffentlichen Verwaltung darf ihre Aufgaben nicht selbst frei definieren. Selbst bei dem sehr allgemein formulierten gesetzlichen Auftrag der Interessenvertretung des Handwerks ist die Einwilligung kein taugliches Mittel, den Auftrag zu überdehnen und eine derart umfangreiche Speicherung und Nutzung von Existenzgründungsdaten bei der Kammer zu rechtfertigen. Auch bei zusätzlichen Angeboten auf der Grundlage einer Einwilligung müssen neben der Freiwilligkeit auch die allgemeinen Datenschutzgrundsätze wie Zweckbindung, Erforderlichkeit, Datensparsamkeit sowie Eingriffstiefe bei der Gestaltung des Angebots beachtet werden. Auf eine eingehende Aufklärung ist besonderer Wert zu legen. Eine Einwilligung darf auch in diesem Fall nicht zu einer Datenverarbeitung auf Vorrat führen, nur um die bloße Möglichkeit einer eventuellen weiteren Verwendung der Daten etwa für Beratungszwecke zu erhalten.

Nach diesen Maßstäben wäre die Datenverarbeitung bei der Kammer schon deshalb nicht erforderlich, weil die Betroffenen das Angebot, mit Hilfe eines Metaformulars alle notwendigen Formulare zeitsparend auszufüllen, datenschutzgerechter nutzen könnten, wenn ihnen angeboten würde, die Anwendung auf ihren eigenen PC herunterzuladen und dort die Daten eingeben, speichern und in Formularen ausdrucken zu können.

Da die Kammer auf die Speicherung der Daten bei sich gleichwohl nicht verzichten wollte, wurde schließlich ein Verfahren vereinbart, das die Befugnisse der Nutzer stärkt und gleichzeitig ihre Daten dem Zugriff der Kammer weitgehend entzieht:

- Die Übermittlung der Daten vom Nutzer zur Kammer erfolgt in verschlüsselter Form.
- Die Speicherung erfolgt auf einem gesonderten Server in der Handwerkskammer in verschlüsselter Form.
- Der Nutzer kann seine Daten jederzeit selbst löschen.
- Spätestens drei Monate nach dem letzten Aufruf durch den Nutzer werden sie automatisch physikalisch gelöscht.
- Passwörter dürfen von der Kammer nicht eingesehen werden.
- Im Beratungsfall haben ausschließlich die Betroffenen selbst die Möglichkeit, die Daten heranzuziehen.
- Notwendige Zugriffe der Administration dürfen nur nach dem Vier-Augen-Prinzip vorgenommen werden und sind zu protokollieren.

Bei späteren Ausbaustufen, wie zum Beispiel der Weitergabe der Daten an die Handwerksrolle, ist u.a. sicherzustellen, dass die weitere Verarbeitung jeweils gesondert von den Nutzern anzustoßen ist (sog. Push-Prinzip).

Daneben haben wir besonderen Wert auf die Ausgestaltung der informierten Einwilligung gelegt:

Die Einwilligung hat neben den Anforderungen des Telemediengesetzes auch denen des Hamburgischen Datenschutzgesetzes zu entsprechen. Zusätzlich ist der Nutzer in einem deutlich sichtbaren, unmittelbar vor der Einwilligungserklärung platzierten Datenschutzhinweis verständlich, zutreffend und umfassend auch über das Verfahren, seine Möglichkeiten und Grenzen zu informieren. Ein Verweis auf eine weitere Internetseite reicht hierfür nicht aus.

Die Anmeldung zum Verfahren darf erst dann möglich sein, wenn die Einwilligung durch eine bewusste Handlung (Anklicken) erteilt wurde.

Sobald alternative Verarbeitungsvarianten angeboten werden, muss sich dies in der Anzahl der zur Auswahl stehenden Einwilligungsvarianten widerspiegeln. Hierzu hatten wir der Kammer im Lauf der Diskussion mehrere Entwürfe übermittelt.

Neben einer Reduzierung des Datenkatalogs haben wir zusätzlich erreicht, dass die Nutzer auf die Freiwilligkeit bestimmter Anträge hingewiesen werden und dass keine Angaben mit Erklärungswillen automatisiert ausgefüllt werden, wie z.B. die Teilnahme am Handwerk-Test.

Die Kammer hat zunächst auf eine Übertragung der Daten zur Handwerksrolle verzichtet. Seit Sommer 2007 ist das Verfahren in Betrieb. Im Herbst 2007 wurde die Übernahme der von uns entworfenen Einwilligungserklärung und die Einhaltung der technischen Anforderungen zugesagt; bis Redaktionsschluss stand die Umsetzung jedoch noch aus.

DATENSCHUTZ IM NICHT-ÖFFENTLICHEN BEREICH

19. Videoüberwachung

19.1 Videoüberwachung in Bahnen und Bussen

Der Einsatz der Videoüberwachungstechnik im öffentlichen Nahverkehr hat weiter zugenommen. Neben den U-Bahnen werden in Hamburg nun auch ein großer Teil der Busse sowie die S-Bahnen videoüberwacht.

Bis auf zehn Fahrzeuge älteren Typs sind in Hamburg mittlerweile alle U-Bahnen sowie sämtliche Haltestellen mit digitaler Videoaufzeichnungstechnik aus-

gerüstet. Hierüber hatten wir im 19. TB, 23.2 und 20. TB, 25.1 berichtet. Das Überwachungsverfahren wurde mit dem Hamburgischen Datenschutzbeauftragten abgesprochen.

Ende 2006 hat die Hamburger Hochbahn AG (HHA) mit der serienmäßigen Kamera-Ausrüstung der Hochbahn-Busse begonnen und 450 Busse bis Ende 2007 ausgerüstet. Die HHA hat die Erforderlichkeit der Videoaufzeichnung ausführlich begründet und die technische Ausstattung und den konkreten Umgang mit den Aufzeichnungen im Falle von Straftaten in einem Konzept zur Ausrüstung der Busse dargestellt (siehe 20.TB, 25.1). Wie in den U-Bahnen werden die Videoaufzeichnungen in den Bussen verschlüsselt auf einem digitalen Ringspeicher aufgezeichnet und automatisch nach Ablauf von 24 Fahrzeugbetriebstunden (48 Zeitstunden) überschrieben, sofern die Festplatte nicht wegen eines zu überprüfenden Vorfalls entnommen wird. Der Hamburgische Datenschutzbeauftragte hatte mit der HHA zunächst abgesprochen, dass Fahrzeuge mit Video-Aufzeichnung insbesondere in den Abend- und Nachstunden ab ca. 21 Uhr eingesetzt werden sollten.

Aus dem von der HHA Ende 2007 vorgelegten Bericht über Anlass und Umfang der zur Auswertung entnommenen Aufzeichnungen ergibt sich, dass Körperverletzungen den größten Anteil an den Vorfällen hatten, die im Busbereich zu einer Sicherung der Festplatten führten. Außerdem kam es zu zahlreichen Diebstählen und Sachbeschädigungen. Im ersten Halbjahr 2006 war in insgesamt 43 Fällen eine Entnahme der Festplatte erforderlich.

Die HHA hat nun mitgeteilt, dass künftig auch die übrigen Busse sowie die der Tochterunternehmen Jasper und Süderelbe Bus mit Videotechnik ausgerüstet werden sollen, da Öffentlichkeit und Fahrgäste in allen Verkehrsmitteln in Hamburg denselben Sicherheitsstandard erwarten würden. Eine Beschränkung der Videoüberwachung auf den Abend- und Nachtverkehr sei nicht ausreichend, da der größere Teil der Vandalismus-Schäden am Tag verursacht würde. Im Tagesverkehr bestehe eine ähnliche Häufigkeit von Vorfällen wie im Nachtverkehr. Die ersten Erfahrungen mit der Videoaufzeichnung in den Bussen hinsichtlich der Reduzierung von Kriminalität und Sachbeschädigungen seien positiv.

Die S-Bahn Hamburg GmbH setzt Videoüberwachungstechnik bei der Zugabfertigung und bei sicherheitsrelevanten Einrichtungen wie Fahrkartenautomaten, Rolltreppen, Aufzügen und Notrufsäulen ein. Neben der Videoüberwachung durch die Möglichkeit der Echtzeitbetrachtung findet eine Aufzeichnung der Aufnahmen statt. Darüber hinaus wird die S-Bahn Hamburg GmbH die bisher erst in einigen S-Bahn-Zügen installierte Videoüberwachungstechnik künftig auf alle Wagen der S-Bahn erweitern. Die Aufzeichnung erfolgt auf einem digitalen Ringspeicher in jedem Wagen, der nach 72 Stunden überspielt wird, es sei denn, die Festplatte muss wegen eines besonderen Vorkommnisses gesichert werden. Der Grund für die Aufbewahrungsfrist von 72 Stunden

ist der gegenüber den U-Bahnen längere Fahrzeugumlauf der S-Bahnen. Bei den S-Bahnen ist aufgrund der personellen Ausstattung und baulicher Gegebenheiten in einigen Bahnhöfen kein täglicher Abschlussdienst möglich, so dass eventuelle Sachbeschädigungen erst 1-2 Tage später entdeckt werden können. Das Verfahren ist mit dem Hamburgischen Datenschutzbeauftragten abgesprochen worden. Die S-Bahn Hamburg GmbH ist von uns aufgefordert worden, zum Nachweis der Erforderlichkeit der Videoüberwachung regelmäßig einen Bericht über Anlass und Umfang der zur Auswertung entnommenen Videoaufzeichnungen vorzulegen.

Die HADAG plant die Einführung von Videoüberwachung auf allen Fährschiffen, da diese im Einmannbetrieb eingesetzt werden. Überwacht werden soll neben der Technik im Maschinenraum zur Sicherheit der Fahrgäste die Rampe bei der Schiffsabfertigung sowie der Fahrgastraum der Schiffe, da es immer wieder zu Sachbeschädigungen sowie Belästigungen von und Angriffen auf Fahrgäste kommt. Einzelheiten des Verfahrens werden noch mit uns erörtert.

Der Hamburgische Datenschutzbeauftragte steht der zunehmenden Videoüberwachung öffentlicher Einrichtungen sehr kritisch gegenüber. Die ständige Präsenz von Kameras kann einen Überwachungsdruck erzeugen, der die Betroffenen in ihren Persönlichkeitsrechten verletzt und ein angepasstes Verhalten erzwingt. Trotz dieser kritischen Haltung ist die Ablehnung einer Videoüberwachung in öffentlichen Verkehrsmitteln nach den datenschutzrechtlichen Vorschriften dann nicht möglich, wenn die Voraussetzungen des § 6 b BDSG durch den Betreiber der Videoüberwachungsanlage erfüllt werden, d.h. insbesondere muss die Videoüberwachung erforderlich sein und die schutzwürdigen Interessen der betroffenen Fahrgäste müssen durch entsprechende technische und organisatorische Maßnahmen ausreichend geschützt werden.

Nach § 6 b BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Als Inhaber des Hausrechts sind die Betreiber von Verkehrsmitteln grundsätzlich befugt, die zum Schutz ihrer Einrichtungen erforderlichen Maßnahmen zu treffen. Die Erhöhung der Sicherheit sowie die Verhinderung von gegen Personen und Sachen gerichteten Straftaten sind als berechtigte Interessen anerkannt.

Zur Wahrnehmung der konkret zu benennenden Interessen muss die Videoüberwachung erforderlich sein. Dies setzt voraus, dass die Videotechnik zu einem verbesserten Schutz dieser Interessen führt, der auf andere Weise nicht ebenso gut erreicht werden könnte. Nach den mehrjährigen Erfahrungen mit Videoüberwachung in den U-Bahnen kann anhand der von der HHA vorgelegten Zahlen nicht bezweifelt werden, dass der Umfang der Vandalismusschäden und der anderen Straftaten durch die Videoüberwachung reduziert worden

ist. Eine Verhinderung von Straftaten und deren nachträgliche Aufklärung sowie die Stärkung des Sicherheitsempfindens der Fahrgäste könnten wahrscheinlich auch durch mehr Sicherheitspersonal in den öffentlichen Verkehrsmitteln erreicht werden. Dazu würde es jedoch nicht ausreichen, wenn nur ab und zu Sicherheitskräfte in Bussen und Bahnen mitfahren würden. Eine ständige Präsenz von Sicherheitspersonal wäre erforderlich, um die genannten Interessen effektiv zu schützen. Die Betreiber der öffentlichen Verkehrsmittel haben mitgeteilt, dass wegen der Größe des Verkehrsnetzes, der vielen Haltestellen und der Anzahl der Verkehrsmittel eine ständige Verfügbarkeit von Sicherheitskräften „vor Ort" trotz Aufstockung des Personals nicht möglich sei. Diese Argumentation ist nachvollziehbar, so dass der erstrebte Zweck der Videoüberwachung auf diese Weise nicht ebenso gut erreicht werden kann. Schließlich führt auch die Abwägung der wirtschaftlichen und rechtlichen Interessen der Betreiber der Verkehrsmittel mit den allgemeinen Persönlichkeitsrechten der Fahrgäste nicht zur Unzulässigkeit der Video-Aufzeichnungen. Dabei ist zu berücksichtigen, dass die Datenaufzeichnungen auf digitalen Ringspeichern, sogenannten „Black Box" erfolgen, die ständig überschrieben werden, falls die Aufnahmen nicht wegen eines besonderen Vorkommnisses sichergestellt werden müssen. Diese nur punktuelle und gelegentliche Überwachung der Fahrgäste durch Auswertung der Aufzeichnungen greift weniger stark in die Betroffenenrechte ein als eine ständige Beobachtung mittels Videogeräten. Maßnahmen zur Verhinderung eines Missbrauchs der Videoaufzeichnungen sind von den Betreibern der Verkehrsmittel mit dem Hamburgischen Datenschutzbeauftragten abgesprochen und getroffen worden. Der Hamburgische Datenschutzbeauftragte hält daher Video-Aufzeichnungen in öffentlichen Verkehrsmitteln in Hamburg für vertretbar.

19.2 Videoüberwachung in Wohnanlagen

Mit der immer preiswerter werdenden Videotechnik nimmt der Einsatz von Videoüberwachung auch im Bereich von Wohnanlagen zu. Dabei wird in den seltensten Fällen vorab überprüft, ob dies nach den datenschutzrechtlichen Vorschriften zulässig sein kann.

In der Praxis der Datenschutzaufsichtsbehörden häufen sich die Beschwerden über Eigentümer, die Eigentums- und zunehmend auch Mietwohnungsanlagen mit Videoüberwachungsanlagen ausstatten. Dabei werden die Zulässigkeitsgrenzen häufig weit überschritten. Nach § 6b des Bundesdatenschutzgesetzes ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nur unter sehr engen Voraussetzungen möglich (vgl. 19. TB, 23.1).

Insbesondere ist zu prüfen, ob die Maßnahme zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

In einem von der Datenschutzaufsichtsbehörde kontrollierten Fall waren diese Voraussetzungen hinsichtlich verschiedener Kameras nicht gegeben. Es handelte sich um eine große Wohnanlage mit Waschmaschinen-Raum für die Bewohner und einem kleinen integrierten Einkaufszentrum. Neben den Kameras, die von einigen Unternehmen im Einkaufszentrum angebracht waren, hatte auch die Betreiberin der Wohnanlage insgesamt 20 Kameras an verschiedenen Standorten installiert. Dabei wurden nicht nur der öffentlich zugängliche Raum im Einkaufszentrum, sondern auch öffentliche Wege sowie das Waschhaus und Parkplätze auf der Straße komplett überwacht. Zur Begründung wurde angeführt, dass es wiederholt zu Vandalismus, Unfällen mit Beschädigungen, Fahrerflucht sowie Falschparken gekommen sei. Darüber hinaus gab es auch Hinweise darauf, dass in den für Interessenten frei zugänglichen Geschäftsräumen eine Kamera angebracht war, die zusätzlich Tonaufnahmen erstellte. Letzteres ist absolut unzulässig und strafbar. In keinem Fall war eine Abwägung mit den berechtigten Interessen der Bewohner, die zu ihren Eingängen an den Kameras vorbei gehen mussten, und der sonstigen Besucher der Anlage, die für jeden frei zugänglich ist, vorgenommen worden.

Gemeinsam mit der Betreiberin der Anlage wurde die Abwägung hinsichtlich der Zulässigkeit jeder einzelnen Kamera nachgeholt. Dabei zeigte sich, dass für die Überwachung durch einzelne Kameras schon das berechtigte Interesse fehlte, weil keine vorangegangenen Vorfälle zu verzeichnen waren. In anderen Fällen – wie z.B. bei der Waschküche – konnte die Überwachungszeit auf die Nachtstunden reduziert werden, so dass einerseits Einbrüche aufgeklärt werden können, die Nutzer jedoch in ihren Persönlichkeitsrechten nicht beeinträchtigt werden. Zum Schutz der Mitarbeiter der Betreiberin waren die Kameras in deren Geschäftsräumen so zu verändern, dass durch Einschaltung der Kamera im Bedarfsfall „renitente“ Besucher erfasst werden können, aber keine permanente Überwachung (auch der Mitarbeiter selbst) stattfindet. Alle Kameras, die öffentlichen Grund erfassten, waren abzuschalten.

Der Umstand der Beobachtung und die verantwortliche Stelle sind nach § 6b Abs. 2 BDSG durch geeignete Maßnahmen erkennbar zu machen. Die Erkennbarkeit der Videoüberwachung war hier schon dadurch stark eingeschränkt, dass die Hinweisschilder nur wenige Zentimeter groß waren. Auch die Schilder waren also auszuwechseln.

Das Beispiel zeigt, dass Videokameras nicht ohne sorgfältige Prüfung eingesetzt werden dürfen. Immer wieder erreichen uns Hinweise auf neue Anlagen. Nicht in jedem Einzelfall ist es jedoch möglich, seitens der Datenschutzaufsichtsbehörde tätig zu werden. Vielfach beschränken Eigentümer den Einsatz der Anlagen auf Räumlichkeiten, die nicht öffentlich zugänglich sind, wie dies beispielsweise bei verschlossenen Tiefgaragen oder Hausfluren von reinen Wohnanlagen der Fall ist. Dann unterliegt die Anlage nicht der Kontrolle der Aufsichtsbehörde. Wir kön-

nen die Betroffenen dann nur auf den Zivilrechtsweg verweisen, um eine mögliche Einschränkung ihrer Persönlichkeitsrechte abzuwehren.

19.3 Videoüberwachung in Umkleidekabinen

Wie in anderen Bereichen auch nehmen Video-Überwachungsanlagen selbst in Umkleidekabinen zu.

Immer wieder erreichen uns Beschwerden darüber, dass in sog. Wellnessoasen, Fitnesscentern, Sportstudios etc. selbst die mit Duschen versehenen Umkleidebereiche durch Videokameras überwacht werden (vgl. Einzelheiten zu diesem Thema schon im 20.TB, 25.2). Wir fordern dann die Betreiber und deren betriebliche Datenschutzbeauftragte auf, diese unzulässigen Anlagen sofort zu beseitigen oder die Anlage zumindest so auszurichten, dass ausreichend überwachungsfreie und als solche deutlich gekennzeichnete Umkleidemöglichkeiten verbleiben. Dabei stellt sich häufig heraus, dass die Befürchtung der Besucher, durch die eingesetzte Technik beobachtet zu werden, nicht der Realität entspricht, da keine direkte Video-Beobachtung erfolgt, sondern die Aufnahmen nur aufgezeichnet werden. Diese Aufzeichnungen müssen unter Verschluss gehalten und dürfen nicht etwa vom Betreiber selbst eingesehen werden. Eine Auswertung der Aufzeichnungen darf nur in begründeten Einzelfällen bei dem Verdacht von Straftaten durch einen eingegrenzten Personenkreis erfolgen. In allen anderen Fällen sind die Aufzeichnungen zeitnah zu löschen bzw. zu überschreiben. Wesentlich ist jedoch, in den Einrichtungen Transparenz bezüglich des Einsatzes von Videoüberwachung zu erreichen, damit sich niemand heimlich überwacht fühlt und ausreichend Ausweichmöglichkeiten angeboten werden.

19.4 Videoüberwachung am Arbeitsplatz

Die Anfragen von Mitarbeitern und Betriebsräten nehmen zu. Dabei ist zu beobachten, dass Arbeitgeber die Videotechnik oft ohne Prüfung der Zulässigkeitsvoraussetzungen einsetzen.

Videotechnik wird vermehrt in der Arbeitswelt eingesetzt. Im Vordergrund steht oftmals nicht die direkte Arbeitnehmerüberwachung, sondern beispielsweise die Prozesssteuerung in der Produktion, die Materialkontrolle oder die Gebäudesicherung. Je nach Art und Einsatzzeit der verwendeten Videotechnik sowie dem Beobachtungsraum können dabei aber die Interessen der Beschäftigten betroffen sein. Sollen z.B. Kunden eines Ladengeschäfts beobachtet werden, kann sich der Fokus der Kamera auch auf die Verkäufer richten. In einem solchen Fall würden die Arbeitnehmer ununterbrochen an ihrem Arbeitsplatz überwacht werden.

Auffällig ist, dass aufgrund der mittlerweile relativ billigen Videotechnik viele Arbeitgeber auf die Idee kommen, ihre Arbeitnehmer am Arbeitsplatz bzw. während ihrer Tätigkeit mit oder ohne Aufzeichnung der Videobilder zu über-

wachen, beispielsweise in Bäckereien, Pflegeeinrichtungen, Kneipen, Einzelhandelsgeschäften.

Eine Videoüberwachung am Arbeitsplatz in nicht öffentlich zugänglichen Räumen ohne Aufzeichnung fällt nicht in den Anwendungsbereich des Bundesdatenschutzgesetzes.

Eine andere Qualität erhält die Videoüberwachung, wenn Aufnahmen angefertigt und auf Datenträgern gespeichert werden. Bei diesen Videobildern handelt es sich um personenbezogene Daten, da sich insbesondere bei Mitarbeitern leicht ein Bezug zu einer bestimmten Person herstellen lässt.

§ 28 Abs. 1 Nr. 1 BDSG (Vertragserfüllung) kommt als Zulässigkeitstatbestand nicht in Betracht. Ein weiterer Erlaubnistatbestand kann § 28 Abs. 1 Nr. 2 BDSG sein. Danach ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt (Abwägung). Basierend auf der Rechtsprechung des Bundesarbeitsgerichtes zur Videoüberwachung von Mitarbeitern ist in der Regel ein schutzwürdiges Interesses des Betroffenen anzunehmen (u.a. Beschluss vom 14.12.2004, 1 ABR 34/03 – www.bundesarbeitsgericht.de).

Videoüberwachung stellt einen erheblichen Eingriff in das allgemeine Persönlichkeitsrecht der betroffenen Arbeitnehmer dar. Das zulässige Maß einer Beschränkung des allgemeinen Persönlichkeitsrechts bestimmt sich nach dem Grundsatz der Verhältnismäßigkeit. Die Intensität einer Beeinträchtigung des allgemeinen Persönlichkeitsrechts hängt maßgeblich von der Dauer und der Art der Überwachungsmaßnahme ab. Gerade bei einer ständigen Überwachung kann sich der Arbeitnehmer nicht dieser Maßnahme entziehen, da er in der Regel nicht den überwachten Bereich verlassen kann. Die Intensität des Eingriffs in die Persönlichkeitsrechte der Arbeitnehmer ist deshalb als besonders hoch einzuschätzen, wenn eine Videoanlage ohne Zeitbeschränkung in Betrieb genommen würde.

Der Einsatz von Videotechnik kann im Einzelfall erforderlich sein, wenn kein anderes, gleich wirksames und das Persönlichkeitsrecht weniger einschränkendes Mittel zur Verfügung steht. In einem solchen Fall sind aus datenschutzrechtlicher Sicht präzise Regelungen zu treffen, wobei die Mitbestimmungsrechte des Betriebsrates nach § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG) zu beachten sind:

- Einsatzzwecke und Auswertungen festlegen,
- Systemdokumentation erstellen (Standorte Kameras, Aufzeichnungsgeräte, Monitore; Ausrichtung und Zoomfunktion Kameras; Systembeschreibung),

- Aufzeichnungszeiträume- und dauer bestimmen (Löschungsroutinen),
- Zugriffsberechtigungen festlegen,
- Zugriffe protokollieren,
- Speichermedien zugangssicher unterbringen,
- Information der betroffenen Beschäftigten (§ 4 Abs. 3 BDSG).

Bei Einsatz von Videotechnik am Arbeitsplatz ist nach § 4 d Abs. 5 Ziffer 2 BDSG eine Vorabkontrolle durchzuführen, da durch diese Maßnahme die Persönlichkeit des betroffenen Arbeitnehmers einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens bewertet werden kann. Die verantwortliche Stelle hat in diesen Fällen unabhängig von der Anzahl der mit der automatisierten Verarbeitung beschäftigten Personen einen betrieblichen Datenschutzbeauftragten zu bestellen (§ 4 f Abs. 1 BDSG).

20. Internationaler Datenverkehr

20.1 Übermittlung von Flugpassagierdaten in die USA

Obwohl die Klage gegen die Übermittlung von Flugpassagierdaten Erfolg hatte, hat sich die datenschutzrechtliche Situation verschärft.

Die Klage des Europäischen Parlaments vor dem Europäischen Gerichtshof gegen ein bilaterales Abkommen, das die rechtliche Grundlage für die Übermittlung von Flugpassagierdaten in die USA bieten sollte (vgl. 20. TB, 18.2) hatte Erfolg. Am 30. Mai 2006 hat der Europäische Gerichtshof das Abkommen zwischen der Europäischen Gemeinschaft und den USA ebenso für nichtig erklärt, wie die Entscheidung der Europäischen Kommission über die Angemessenheit des Schutzes der personenbezogenen Daten.

Dies führte jedoch nicht zur Einstellung der entsprechenden Datenübermittlungen, denn das Gericht hatte sich nicht mit den inhaltlichen Aspekten auseinandergesetzt. Vielmehr beruhte die Entscheidung allein darauf, dass die Anwendbarkeit der EU-Datenschutzrichtlinie verneint wurde. Bis zum 30. September 2006 wurde eine Übergangsfrist eingeräumt.

Das anschließende Zwischenabkommen zwischen der Europäischen Union und den USA galt bis Ende Juli 2007. Aus Sicht des Datenschutzes verschlechterte sich die Situation erneut. Die Fluggastdaten durften nicht mehr nur im Einzelfall, sondern sogar routinemäßig an weitere US-Sicherheitsbehörden weitergegeben werden.

Im August 2007 trat dann eine neue Vereinbarung in Kraft. Vereinbart wurde z.B., dass die Übermittlung künftig im Wege des sog. Push- Verfahrens erfolgen soll, währen die US-Sicherheitsbehörden in der Vergangenheit selbst Zugriff auf die Daten genommen hatten. Vordergründig wurde als weiterer da-

tenschutzrechtlicher Erfolg angesehen, dass nicht mehr 34, sondern nur noch 19 Daten zu übermitteln sind. Allerdings sind dabei mehrere der ursprünglichen Daten lediglich in Kategorien zusammengefasst. Die Weiterübermittlungsbefugnis von der Zoll- und Grenzschutzbehörde an weitere US-Sicherheitsbehörden blieb bestehen. Insgesamt dürfen die Daten bei den US-Behörden 15 Jahre aufbewahrt werden.

Die Verhandlungen mit den USA haben offenbar auch bei den EU-Innenministern Begehrlichkeiten geweckt. Mittlerweile wird auch für Europa neben einem elektronischen Register für biometrische Daten von Nicht-EU-Bürgern, die in die Europäische Union ein- oder ausreisen, eine Vernetzung nationaler Datenbanken gefordert.

20.2 Auftragsdatenverarbeitung in Drittländern außerhalb der EU

Die fortschreitende Globalisierung führt dazu, dass immer mehr Unternehmen dazu übergehen, ihre Datenverarbeitungen auch an Anbieter außerhalb des Geltungsbereichs der EU-Datenschutzrichtlinie auszulagern. Die damit verbundenen datenschutzrechtlichen Probleme sind gravierend.

Im Gegensatz zur Verarbeitung personenbezogener Daten im Auftrag innerhalb des Geltungsbereichs der EU-Datenschutzrichtlinie ist die Auftragsdatenverarbeitung in Drittländern vom Gesetzgeber nicht privilegiert. Konkret heißt dies, dass jeweils die Einhaltung der Übermittlungsvorschriften des Bundesdatenschutzgesetzes vor einer Weitergabe der personenbezogenen Daten in das Drittland geprüft werden muss (vgl. zu dem Themenkomplex 19. TB, 18.2). Darüber hinaus ist zu gewährleisten, dass entweder das Drittland generell ein angemessenes Datenschutzniveau aufweist oder zumindest das empfangende Unternehmen selbst ausreichende Datenschutzgarantien bietet. Die Konstellationen, die sich hieraus ergeben können, sind außerordentlich vielfältig. Je nachdem, ob eine Übermittlung an ein den Safe-Harbor-Regelungen unterliegendes Unternehmen stattfindet, EU-Standardverträge genutzt werden, Unternehmensrichtlinien vorliegen oder sogar die Voraussetzungen einer Ausnahme gegeben sind, sind unterschiedliche Rechtsfolgen zu beachten. Weitere Konstellationen ergeben sich z.B. aus der Einschaltung zusätzlicher Subunternehmer in EU- oder auch weiteren Drittländern. Aus dieser – nicht abschließenden – Aufzählung der möglichen Fälle wird deutlich, dass die Unternehmen, die die Daten im Ausland verarbeiten lassen wollen, die Rechtslage zur Beachtung des Datenschutzrechts jedes Mal sehr genau prüfen müssen.

Den Datenschutzaufsichtsbehörden werden immer wieder Einzelfälle zur Beurteilung vorgelegt, die zum Teil auch bundesweit im Rahmen der AG Internationaler Datenverkehr des Düsseldorfer Kreises diskutiert werden. Einige besonders komplizierte Fallgestaltungen führten dazu, dass Gespräche mit Vertretern der Wirtschaft stattgefunden haben. Als Ergebnis wurde ein Positionspapier erarbeitet, das den Unternehmen die Rechtslage erläutet.

Darüber hinaus beschloss der Düsseldorfer Kreis eine Handreichung zur rechtlichen Bewertung von Fallgruppen zur internationalen Auftragsdatenverarbeitung. Sie beinhaltet die häufigsten Fallkonstellationen und soll den Unternehmen die rechtliche Bewertung erleichtern. Im Einzelfall kann eine abweichende Bewertung erforderlich sein. Deshalb verbieten sich schematische Lösungen.

Im Internet ist der vollständige Text der Handreichung unter der folgenden Adresse abrufbar: http://fhh.hamburg.de/stadt/Aktuell/weitere-einrichtungen/datenschutzbeauftragter/informationsmaterial/wirtschaft/internationale-auftrags-dv.html

20.3 SWIFT

Aufgrund des massiven Drucks durch die europäischen Datenschutzaufsichtsbehörden konnte erreicht werden, dass Zahlungsverkehrsdaten aus Überweisungen, die den europäischen Wirtschaftraum betreffen, künftig nicht mehr in den USA gespeichert werden.

Im Juni 2006 wurde durch eine Veröffentlichung in der New York Times bekannt, dass das US-amerikanische Finanzministerium aufgrund von Beschlagnahmeanordnungen zum Zwecke der Bekämpfung des internationalen Terrorismus auf eine Vielzahl von Zahlungsverkehrsdaten im US-Rechenzentrum von SWIFT zugegriffen und diese für die Zwecke der Terrorismusbekämpfung ausgewertet hatte. Die Society for Worldwide Interbank Financial Telecommunication (SWIFT) mit Sitz in Belgien ist ein weltweit tätiger Banken-Dienstleister und betreibt ein Telekommunikationsnetzwerk zum automatisierten Austausch von standardisierten Zahlungsverkehrsnachrichten zwischen Kreditinstituten im internationalen Zahlungsverkehr. Bei sämtlichen Überweisungen ins Ausland und bei gesondert beauftragten Eilüberweisungen werden die in der Überweisung enthaltenen Daten über SWIFT an das Kreditinstitut der Begünstigten weitergeleitet. Aus Gründen der Datensicherheit werden die Transaktionsdaten durch SWIFT doppelt gespeichert, d.h. sowohl in seinem Rechenzentrum in den Niederlanden als auch in seinem Rechenzentrum in den USA. Daher war es den US-amerikanischen Sicherheitsbehörden möglich, auf die Transaktionsdaten von sämtlichen grenzüberschreitenden Zahlungsaufträgen, auch soweit sie nur innerhalb der EU erfolgten, zuzugreifen.

Die europäischen und die deutschen Datenschutzaufsichtsbehörden haben diese Spiegelung von Zahlungsverkehrsdaten von EU-Bürgern in dem SWIFT-Rechenzentrum in den USA kritisiert. Der Düsseldorfer Kreis hat im November 2006 beschlossen, dass die Spiegelung von Datensätzen im SWIFT-Rechenzentrum in den USA wegen fehlender Rechtsgrundlage sowohl nach deutschem Recht als auch nach EG-Datenschutzrecht unzulässig ist, da die USA über kein angemessenes Datenschutzniveau im Sinne des Art. 25 Abs. 1 und Abs. 2 der EG-Datenschutzrichtlinie verfügen. Die deutschen Banken wurden aufgefordert, unverzüglich Maßnahmen zu ergreifen, durch die im SWIFT- Ver-

fahren entweder eine Übermittlung von Daten in die USA unterbunden werden oder aber zumindest die übermittelten Datensätze hinreichend gesichert werden können. Unabhängig von diesen Maßnahmen wurden die Banken aufgefordert, ihre Kunden gemäß § 4 Abs. 3 BDSG darüber zu informieren, dass im Falle der Weiterleitung von grenzüberschreitenden Zahlungsaufträgen die Datensätze auch an ein in den USA ansässiges Rechenzentrum übermittelt werden. Der Beschluss des Düsseldorfer Kreises und weitere Informationen sind auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de veröffentlicht.

Die Bedenken und der Druck, den die deutschen und europäischen Datenschutzaufsichtsbehörden auf SWIFT ausgeübt haben, haben dazu geführt, dass das Unternehmen sich dazu entschlossen hat, die Nachrichtenarchitektur, d.h. das System der Speicherung der Überweisungsdaten, neu zu strukturieren. Zunächst sollen zwei Nachrichten-Verarbeitungszonen geschaffen werden (Europa und Transatlantik), für die es drei Rechenzentren geben wird. Neben dem Rechenzentrum in den Niederlanden und in den USA soll bis Ende 2009 in der Schweiz ein neues Datenverarbeitungszentrum entstehen. Das Rechenzentrum in der Schweiz wird neben dem Rechenzentrum in den Niederlanden die Nachrichten verarbeiten und speichern, die für die europäische Verarbeitungszone bestimmt sind. Damit soll sichergestellt werden, dass Nachrichten, die die Staaten des Europäischen Wirtschaftsraums und die Schweiz betreffen, in Europa verbleiben. Das Rechenzentrum in der Schweiz wird darüber hinaus mit dem Rechenzentrum in den USA den Nachrichtenverkehr für die Transatlantik- Verarbeitungszone verarbeiten und speichern. Zur Transatlantik- Zone werden die USA gehören. In allen übrigen Staaten können die nationalen Mitglieder von SWIFT wählen, zu welcher Zone sie gehören wollen. Zu gegebener Zeit wird SWIFT darüber informieren, welche Staaten sich für die Transatlantik- Zone entschieden haben. Für die Übergangszeit bis zum Abschluss der Neustrukturierung Ende 2009 hat SWIFT sich dem Safe Harbor-Abkommen unterworfen.

21. Telekommunikation Tele- und Mediendienste

21.1 Neuregelung des Telemedienrechts

Am 1. März 2007 ist das neue Telemediengesetz (TMG) in Kraft getreten.

Die früheren Vorschriften des Teledienstegesetzes, des Teledienstedatenschutzgesetzes und des Mediendienstestaatsvertrages wurden durch das TMG ersetzt (vgl. 20.TB, 19.1). Es gilt für alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht Telekommunikationsdienste oder Rundfunk sind.

Die Erwartung einer grundlegenden Klarstellung seit langem unbeantworteter Fragen hat sich damit jedoch nicht erfüllt. Weder werden die Abgrenzungen zum Bundesdatenschutzgesetz oder zum Telekommunikationsgesetz zweifelsfrei geregelt, noch kommt es wenigstens zu einer terminologischen Anpassung. Den Datenschutzaufsichtsbehörden verbleibt also weiterhin die Aufgabe, zu sachgerechten Auslegungen im Einzelfall zu kommen.

21.2 Vorratsspeicherung von Verkehrsdaten

Der Bundestag hat am 9. November 2007 die Neuregelung der Telekommunikationsüberwachung beschlossen, mit der die Vorratsdatenspeicherung eingeführt wird.

Diese Umsetzung der Europäischen Richtlinie zur Vorratsdatenspeicherung erfolgt ungeachtet der bereits im Vorfeld laut gewordenen massiven Bedenken gegen die Einführung einer sechsmonatigen Aufbewahrungspflicht für alle Verbindungsdaten der Telekommunikation. Schon in ihrer Entschließung im Rahmen der 73. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 8. bis 9. März 2007 haben diese betont, dass die Vorratsdatenspeicherung deutschem Verfassungsrecht widerspricht. Nach der Rechtsprechung des Bundesverfassungsgerichts ist die Speicherung von Daten auf Vorrat zu nicht hinreichend bestimmbaren Zwecken verfassungswidrig. Zudem würde die für eine freiheitliche Gesellschaft konstitutive unbefangene Kommunikation erheblich beeinträchtigt. Die Konferenz hat die Bundesregierung – aus heutiger Sicht vergeblich – aufgefordert, die Umsetzung der Europäischen Richtlinie solange zurückzustellen, bis der bereits angerufene Europäische Gerichtshof über deren Rechtmäßigkeit entschieden hat.

Der vollständige Text der ausführlichen Entschließung kann nachgelesen werden unter http://www.thueringen.de/datenschutz/datenschutz/entschliessungen_datenschutzkonferenz/73/vorratsdatenspeicherung/.

22. Versicherungswirtschaft

22.1 Schweigepflicht-Entbindungserklärung

Die von den Datenschutzaufsichtsbehörden bereits sein langem bemängelte Schweigepflicht-Entbindungserklärung in der Krankenversicherung wird von der Versicherungswirtschaft überarbeitet.

Nachdem in den Jahren 2004/2005 trotz intensiver Erörterungen in der Arbeitsgruppe Versicherungswirtschaft keine Einigung auf ein geändertes Verfahren bei der Einholung der Schweigepflicht-Entbindungserklärung bei Leistungsanträgen in der privaten Krankenversicherung erzielt werden konnte, wurden die Verhandlungen zwischen den Datenschutzaufsichtsbehörden und der Versi-

cherungswirtschaft abgebrochen (vgl. 19. TB, 19.1, 20. TB, 20.2). Die Datenschutzaufsichtsbehörden hatten gefordert, dass Versicherungsunternehmen sich bei jeder Leistungsprüfung eine konkrete auf den Einzelfall bezogene Schweigepflicht-Entbindungserklärung erteilen lassen. Wegen des Dissenses zwischen Versicherungswirtschaft und Datenschutzaufsichtsbehörden regte der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit im Jahr 2006 beim Bundesministerium der Justiz an, in den Entwurf eines Gesetzes zur Reform des Versicherungsvertragsrechts eine Regelung für die Abgabe der Schweigepflicht-Entbindungserklärung gegenüber Versicherungen aufzunehmen. Dieses Anliegen wurde gestärkt durch den Beschluss des Bundesverfassungsgerichts vom 23. Oktober 2006 (1 BvR 2027/02). Das Gericht stellte darin fest, dass eine formularmäßige und sehr allgemein umschriebene Schweigepflicht-Entbindungserklärung in der Berufsunfähigkeitsversicherung dem Interesse der Betroffenen an informationeller Selbstbestimmung entgegensteht. Statt dem Abverlangen einer umfassenden pauschalen Schweigepflichtentbindung müsse ein Weg angeboten werden, der die durch die Schweigepflichtentbindung ermöglichten Auskünfte im Einzelfall und konkret beschreibe.

Durch das Gesetz zur Reform des Versicherungsvertragsgesetzes vom 23. November 2007 ist in § 213 VVG nun eine Regelung zur Erhebung von Gesundheitsdaten bei Dritten aufgenommen worden.

§ 213 Erhebung von personenbezogenen Gesundheitsdaten bei Dritten

(1) Die Erhebung personenbezogener Gesundheitsdaten durch den Versicherer darf nur bei Ärzten, Krankenhäusern und sonstigen Krankenanstalten, Pflegeheimen und Pflegepersonen, anderen Personenversicherern und gesetzlichen Krankenkassen sowie Berufsgenossenschaften und Behörden erfolgen; sie ist nur zulässig, soweit die Kenntnis der Daten für die Beurteilung des zu versichernden Risikos oder der Leistungspflicht erforderlich ist und die betroffene Person eine Einwilligung erteilt hat.

(2) Die nach Absatz 1 erforderliche Einwilligung kann vor Abgabe der Vertragserklärung erteilt werden. Die betroffene Person ist vor einer Erhebung nach Absatz 1 zu unterrichten; sie kann der Erhebung widersprechen.

(3) Die betroffene Person kann jederzeit verlangen, dass eine Erhebung von Daten nur erfolgt, wenn jeweils in die einzelne Erhebung eingewilligt worden ist.

(4) Die betroffene Person ist auf diese Rechte hinzuweisen, auf das Widerspruchsrecht nach Absatz 2 bei der Unterrichtung.

Die Datenschutzaufsichtsbehörden begrüßen die Neuregelung, die die Datenschutzrechte der Versicherten stärkt. Nach Wechsel des Vorsitzes in der Arbeitsgruppe Versicherungswirtschaft auf das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein wurden 2006 die Verhandlungen zwischen den Datenschutzaufsichtsbehörden und der Versicherungswirtschaft über die Formulierung einer Schweigepflicht-Entbindungserklärung für die Risikoprüfung bei Vertragsschluss und für den Leistungsfall wieder aufgenommen. Mittlerweile liegt als Diskussionsgrundlage ein Entwurf vor, der den Betroffenen bei der Prüfung der Leistungspflicht die Möglichkeit einräumt, die Schweigepflicht-Entbindungserklärung entweder bereits bei Abschluss des Vertrags oder in jedem Leistungsfall abzugeben. In jedem Fall muss der Betroffene vor der Datenerhebung unterrichtet und auf sein Widerspruchsrecht hingewiesen werden.

Über den Fortgang der Angelegenheit werden wir berichten.

22.2 Einwilligungsklausel in Antragsformularen

Trotz der intensiven, sich bereits über mehrere Jahre hinziehenden Erörterungen konnten sich die Datenschutzaufsichtsbehörden und die Versicherungswirtschaft noch nicht auf eine neue allgemeine Einwilligungsklausel für die Datenverarbeitung durch Versicherungen einigen.

Unter dem Vorsitz des Unabhängigen Landeszentrums für Datenschutz wurden die Erörterungen in der Arbeitsgruppe Versicherungswirtschaft über die Neufassung der Einwilligungsklausel in die Datenverarbeitung, die als Bestandteil jedes Versicherungsvertrages von dem Antragsteller vor Vertragsabschluss zu unterzeichnen ist, fortgeführt. Die Kritik der Datenschutzaufsichtsbehörden an der vorliegenden Klausel und dem Merkblatt zur Datenverarbeitung haben wir ausführlich im 20. TB, Ziffer 20.1 dargestellt. Der Gesamtverband der Deutschen Versicherungswirtschaft (GDV) hat mittlerweile den im September 2005 zunächst vorgelegten Entwurf für eine allgemeine Einwilligungsklausel überarbeitet und zusätzlich begonnen, Verhaltensregeln nach § 38 a BDSG zu formulieren, die einzelne Datenverarbeitungsprozesse in der Versicherungswirtschaft präzisieren sollen. Unterstützt wird der GDV bei der Erarbeitung der Vorschläge durch den ehemaligen Datenschutzbeauftragten des Landes Berlin.

Im Jahr 2007 wurde ein Lenkungsausschuss gebildet, dem das Unabhängige Landeszentrum für Datenschutz als Vertreter der Arbeitsgruppe Versicherungswirtschaft und Vertreter des Gesamtverbands der Versicherungswirtschaft (GDV) und des Verbraucherzentrale Bundesverband e.V. (vzbv) angehören. Aufgabe des Ausschusses ist es, die vom GDV vorgelegten Klauselentwürfe zu diskutieren sowie die Erstellung der Verhaltensregeln zu begleiten. Neben dem Entwurf einer Schweigepflicht-Entbindungserklärung (siehe 22.1) wurden in dem Ausschuss bisher der Entwurf für eine daten-

schutzrechtliche Einwilligungserklärung zur Verarbeitung von Gesundheitsdaten sowie eine Einwilligungserklärung für die Verarbeitung von Daten zu Werbezwecken diskutiert. Die Werbeklausel ist grundsätzlich von den Mitgliedern der Arbeitsgruppe Versicherungswirtschaft gebilligt worden. Der im Lenkungsausschuss erörterte Entwurf für die allgemeine Einwilligungserklärung in die Verarbeitung von Gesundheitsdaten von Versicherungen war dagegen in der Arbeitsgruppe Versicherungswirtschaft nicht konsensfähig und wird vom GDV erneut überarbeitet werden.

Über den Fortgang der Angelegenheit werden wir berichten.

22.3 Warn- und Hinweissysteme

Nach der massiven Kritik der Datenschutzaufsichtsbehörden an dem Datenaustausch im Rahmen der zentralen Warn- und Hinweissysteme hat die Versicherungswirtschaft sich bereit erklärt, das Verfahren zu ändern.

Die Versicherungswirtschaft hat ein neues Konzept für die Warn- und Hinweissysteme vorgelegt. Das Konzept sieht vor, dass die Warn- und Hinweissysteme künftig durch den Gesamtverband der Versicherungswirtschaft (GDV) als Auskunftei im Sinne des § 29 BDSG betrieben werden sollen. Der Datenbestand soll in getrennten Datenpools für Anfragen bei Versicherungsanträgen und für Anfragen im Leistungsbereich gespeichert werden. Die Versicherungswirtschaft kommt mit der Neustrukturierung der Forderung der Datenschutzaufsichtsbehörden nach, das Verfahren datenschutzgerechter zu gestalten. Das derzeitige Verfahren war wegen fehlender Transparenz und der Vielzahl der an alle Versicherungsunternehmen einer Branche übermittelten Daten heftig kritisiert worden (vgl. 20. TB, Ziffer 20.3). Eine ausführliche Beschreibung des derzeitigen Verfahrens kann im Internet unter www.datenschutzzentrum.de/wirtschaft sowie unter www.gdv.de abgerufen werden.

Die beabsichtigte Umstrukturierung wird im Rahmen der Arbeitsgruppe Versicherungswirtschaft intensiv erörtert werden.

22.4 EU-weite Prüfung der Datenverarbeitung durch Krankenversicherungen

Nachdem die Ergebnisse der EU-weit durchgeführten Prüfung vorliegen, werden von der Artikel 29 Gruppe Empfehlungen zur Verbesserung des Datenschutzes bei Krankenversicherungen erarbeitet.

Im Berichtszeitraum wurden die Ergebnisse der Fragebogenaktion (vgl. 20.TB, 20.5) in nationalen Berichten der einzelnen Mitgliedsländer zusammengefasst. Da es sich um die erste abgestimmte Maßnahme zur Durchsetzung des Datenschutzes in den EU-Mitgliedstaaten handelte, wurden die nationalen Ergebnisse in der Art. 29 Gruppe intensiv erörtert. Ferner wurde ein Abschlussbericht durch die für den Datenschutz zuständige Abteilung bei der Europä-

ischen Kommission erstellt. In diesem Bericht wird eine positive Bilanz der Aktion sowohl im Hinblick auf die Prüfmethode als auch auf die Zusammenarbeit mit den Versicherungen und das Ergebnis der Prüfung gezogen. Derzeit werden Empfehlungen der Art. 29 Gruppe zur Verbesserung des Datenschutzes in dem geprüften Sektor erarbeitet. Auch wenn Datenschutz und Datensicherheit bei Krankenversicherungen bereits einen hohen Stellenwert haben, wird es insbesondere zur Information der Betroffenen über die Datenverarbeitung und zum Umfang der erhobenen Daten einige Verbesserungsvorschläge geben.

22.5 Ausgliederung von Datenverarbeitungen

Die datenschutzrechtlichen Vorschriften müssen sowohl bei der vollständigen Ausgliederung des operativen Geschäfts auf andere Versicherungsunternehmen als auch bei der Übertragung von Teilgeschäften eingehalten werden.

In der Sitzung der Arbeitsgruppe Versicherungswirtschaft wurden mehrfach datenschutzrechtliche Probleme erörtert, die sich aus der Übertragung von einzelnen Geschäftsbereichen auf andere Versicherungsunternehmen und der damit zusammenhängenden Datenverarbeitung ergeben. Zunehmend beschränkt sich die Übertragung allerdings nicht auf einzelne Geschäftsbereiche. In vielen Fällen kommt es zu einer vollständigen Funktionsübertragung in der Versicherungsbranche, das heißt, es werden der Vertrieb, die Bestandsverwaltung, die Leistungsbearbeitung, das Rechnungswesen, die Vermögensanlage oder die Vermögensverwaltung ganz oder zu einem wesentlichen Teil auf ein anderes Unternehmen übertragen. Versicherungsunternehmen werden nur noch als juristisch selbständige Hüllen mit wenigen Mitarbeitern betrieben. Das tatsächliche Geschäft einschließlich der Verarbeitung der personsonbezogenen Daten der Versicherungsnehmer wird von anderen Unternehmen, die dem gleichen Konzern angehören, übernommen. Während bei der Ausgliederung von Teilbereichen der Verarbeitung häufig eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG vorliegt, ist die Datenverarbeitung bei einer vollständigen Ausgliederung des Geschäfts nach § 28 BDSG zu beurteilen. Die Datenschutzaufsichtsbehörden sind sich einig, dass die Datenübermittlung bei einer vollständigen Funktionsausgliederung an ein anderes Unternehmen nur zulässig sein kann, wenn gemäß § 28 Abs. 1 Nr. 2 BDSG die schutzwürdigen Interessen der Betroffenen ausreichend berücksichtigt werden. Hierfür ist neben der Transparenz des Verfahrens die Einräumung einer Widerspruchsmöglichkeit gegen die Übertragung der Datenverarbeitung erforderlich.

Da Funktionsausgliederungen nach § 5 Abs. 3 Ziffer 4 Versicherungsaufsichtsgesetz durch die Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) genehmigt werden, ist die Arbeitsgruppe Versicherungswirtschaft an die BaFin mit der Bitte herangetreten, die Datenschutzaufsichtsbehörden am Genehmigungsverfahren zu beteiligen oder die Unternehmen zumindest darauf hin-

zuweisen, dass eine datenschutzrechtliche Prüfung und Bewertung der Funktionsausgliederung den Datenschutzaufsichtsbehörden vorbehalten bleibt.

23. Schufa

23.1 Neue Klausel

Die Schufa hat den Datenschutzaufsichtsbehörden mitgeteilt, dass sie eine im Wortlaut geänderte Schufa-Klausel zu Kontoeröffnungsanträgen einsetzen wird.

Bereits im Dezember 2005 hat die Schufa der zuständigen Datenschutzaufsichtbehörde in Hessen eine neue Klausel vorgelegt, die die Kreditinstitute ihren Kunden z.B. bei Eröffnung eines Girokontos vorlegen sollen. Da die Änderung dieser wichtigen Klausel Auswirkungen auf die Datenverarbeitung der angeschlossenen Kreditinstitute hat, sind auch alle Datenschutzaufsichtsbehörden zumindest mittelbar betroffen. Angesichts der Fülle von datenschutzrechtlichen Fragen, die mit dem neuen Text aufgeworfen wurden, haben in den Jahren 2006 und 2007 intensive Verhandlungen und Gespräche seitens der Arbeitsgruppe Schufa des Düsseldorfer Kreises mit Vertretern der Schufa auch unter Einbeziehung des Zentralen Kreditausschusses (ZKA) stattgefunden.

Hauptkritikpunkt an der zunächst vorgelegten Klausel war die Aufnahme des Begriffs „wirtschaftliches Risiko“, der später durch „Ausfall- oder Aufwandsrisiko“ ersetzt wurde. Dies erfolgte in einem Zusammenhang, der es nahelegte, dass eine uneingeschränkte Abfrage bei der Schufa schon dann zulässig sein kann, wenn lediglich normale Vertragsrisiken bestehen, die nicht mir einer Vorleistung oder einem finanziellen Ausfallrisiko des anfragenden Unternehmens verbunden sind. Hinzu kam, dass die gerade in diesen Fällen unerlässliche Abwägung mit den schutzwürdigen Interessen der Betroffenen unerwähnt blieb.

Nachdem etliche weitere offene Punkte der Klausel geklärt werden konnten, legte die Schufa im Vorfeld einer Sondersitzung zwischen Vertretern der AG Schufa/Auskunfteien, der Schufa und des ZKA im Juni 2007 eine geänderte Klausel vor. Darin wird auf die Aufnahme des Berechtigungstatbestandes „Aufwandsrisiken“ verzichtet, auch die Abwägung mit den Betroffeneninteressen wird erwähnt. Eine nochmalige Erörterung der Klausel konnte daher zunächst unterbleiben.

Gleichzeitig unterrichtete die Schufa in dieser Sitzung über Neuerungen, die auch in der Klausel ihren Niederschlag finden sollen. Hierüber bleiben die Aufsichtsbehörden weiter mit der Schufa im Gespräch.

Zwischen den Datenschutzaufsichtsbehörden und den Auskunfteien, einschließlich der Schufa, haben sich zu einzelnen Punkten Differenzen entwickelt, die unter Einbeziehung der jeweils betroffenen Branchen geklärt werden

sollen. Begonnen wurde mit dem Nachmeldeverfahren insbesondere der Schufa an den Versandhandel im Dezember 2007.

23.2 Altersverifikationssysteme

Die zunehmende Nutzung des Internet in Bereichen, die eine eindeutige Berechtigung der Nutzer voraussetzen, erfordert auch eine Weiterentwicklung der Altersverifikationssysteme.

Der bereits im 20. Tätigkeitsbericht unter 21.3 geschilderte Fall, in dem ein Zigarettenhersteller im Internet als Werbemaßnahme verschiedene Telespiele anbietet, konnte im Berichtszeitraum geklärt werden. Da eine gesetzliche Verpflichtung zur eindeutigen Altersverifikation in dem zu beurteilenden Fall nicht bestand, reichte es aus, die Seiten zusätzlich zur autorisierten Abfrage bei der Schufa mit umfassenden Datenschutzinformationen zu versehen und die Internet-Registrierung durch eine postalische Registrierungsinformation in einem geschlossenen, neutralen Umschlag zu bestätigen. Auf diese Weise erfahren diejenigen (erwachsenen) Personen, unter deren Namen die Registrierung erfolgt, von der Eintragung. Sollte es sich um eine missbräuchliche Verwendung ihrer Daten handeln, haben sie die Möglichkeit, dem entgegenzuwirken.

Die Kommission für Jugendmedienschutz (KJM), zu der eine Arbeitsgruppe des Düsseldorfer Kreises Kontakt aufgenommen hat, hat die von ihr bisher positiv bewerteten Konzepte zur Sicherstellung einer geschlossenen Benutzergruppe in ihrem Internetangebot veröffentlicht. Diese Systeme gewährleisten die in einigen Fällen erforderliche Altersüberprüfung bei der Nutzung bestimmter Internetangebote. Näheres hierzu ist unter http://www.kjm-online.de/public/kjm/index.php?show_1 = 85,56 nachzulesen.

24. Andere Auskunfteien

24.1 Erhebung von Positivdaten durch Auskunfteien

Die Erhebung und Verarbeitung von Positivdaten durch eine Auskunftei erfordert in der Regel eine Einwilligung des Betroffenen.

Handels- und Wirtschaftsauskunfteien erheben, speichern und übermitteln in zunehmendem Maße sogenannte Positivdaten. Diese Praxis ist in die Kritik der Datenschutzaufsichtsbehörden geraten, weil dafür in den meisten Fällen eine einschlägige Rechtsgrundlage fehlt. Die Datenerhebung, -verarbeitung und -nutzung ist nur zulässig, wenn ein Gesetz dies erlaubt oder der Betroffene eingewilligt hat. Im Rahmen der gesetzlich erforderlichen Abwägung wird man im Ergebnis davon ausgehen können, dass es zulässig ist, aus öffentlichen Verzeichnissen erlangte Identifikationsdaten des Betroffenen wie Name, Adresse und Geburtsdatum zu speichern. Auch im Falle von Negativdaten, die bei-

spielsweise auf der Grundlage von Schuldnerverzeichnisdaten oder gegen den Betroffenen erwirkten Titeln beruhen, gibt es in der Regel keine datenschutzrechtlichen Probleme.

Allerdings enthalten die Auskünfte von Handels- und Wirtschaftsauskunfteien vielfach auch personenbezogene Daten, die weder reine Identifikationsdaten sind, noch als Negativmerkmale qualifiziert werden können. Hierzu gehören Kategorien wie etwa Familienstand, Zahl der Kinder, Immobilienbesitz (manchmal nur geschätzt), berufliche Angaben oder auch positiv abgewickelte Geschäftsverbindungen. Sofern es sich dabei um Angaben zu Privatpersonen handelt, die nicht gewerblich tätig sind, ist deren Interesse, selbst über die Verwendung ihrer Daten zu bestimmen als schutzwürdig einzustufen. Darüber hinaus besteht eine erhöhte Gefahr der Unrichtigkeit der Angaben. Daher kommt in diesen Fällen als datenschutzrechtliche Rechtsgrundlage nur die Einwilligung des Betroffenen in die Aufnahme der entsprechenden Merkmale in Betracht. Beachtet werden müssen dabei die gesetzlichen Voraussetzungen nach § 4a BDSG, wonach die Einwilligung in der Regel schriftlich zu erteilen ist, auf der freien Entscheidung des Betroffenen beruhen und frei widerruflich sein muss.

Der Düsseldorfer Kreis hat sich in seiner Sitzung in Hamburg im April 2007 eingehend mit dieser Fragestellung befasst und einstimmig den folgenden Beschluss gefasst:

Erhebung von Positivdaten zu Privatpersonen bei Auskunfteien

Nicht nur sog. Verbraucherauskunfteien wie beispielsweise die SCHUFA, sondern auch Handels- und Wirtschaftsauskunfteien erheben und verarbeiten zunehmend Bonitätsdaten zu Privatpersonen, die nicht gewerblich tätig sind. Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich weisen in diesem Zusammenhang darauf hin, dass die Handels- und Wirtschaftsauskunfteien insoweit die selben datenschutzrechtlichen Vorgaben zu beachten haben wie die „Verbraucherauskunfteien".

Handels- und Wirtschaftsauskunfteien können daher sog. Positivdaten zu Privatpersonen grundsätzlich nicht auf Grundlage des § 29 Abs. 1 BDSG erheben. Denn bei Positivdaten – das sind Informationen, die keine negativen Zahlungserfahrungen oder sonstiges nicht vertragsgemäßes Verhalten zum Inhalt haben – überwiegt das schutzwürdige Interesse der betroffenen Personen, selbst über die Verwendung ihrer Daten zu bestimmen. Werden die Daten übermittelt, ist insoweit bereits die Übermittlung nach § 28 BDSG regelmäßig unzulässig.

Will eine Auskunftei Positivdaten zu Privatpersonen erheben, bedarf es dafür einer wirksamen Einwilligung der Betroffenen im Sinne des § 4a BDSG. Sofern die Auskunftei oder ihre Vertragspartner zu diesem Zweck eine für eine Vielzahl von Fällen vorformulierte Einwilligungsklausel verwenden, die als Allgemeine Geschäftsbedingung im Sinne des § 305 BGB zu werten ist, muss eine entsprechende Einwilligung darüber hinaus den Anforderungen des § 307 BGB genügen.

24.2 Nutzung von Inkassodaten

Die Übermittlung von negativen personenbezogenen Daten aus dem Inkassobereich an Auskunfteien ist grundsätzlich nicht zulässig. Ausnahmen sind nur unter Beachtung bestimmter Anforderungen möglich.

Schon im 19. Tätigkeitsbericht wurde ausführlich über die unzulässige Praxis von Inkassounternehmen berichtet, negative Auskünfte ohne weitere Überprüfung an Auskunfteien zu übermitteln (19. TB, 21.1). Die damals von der Datenschutzaufsichtsbehörde Hamburg aufgestellten Kriterien zur Zulässigkeit der Übermittlung gelten nach wie vor.

Im Jahre 2006 griff der Verband der Handelsauskunfteien gegenüber der Arbeitsgruppe Auskunfteien des Düsseldorfer Kreises das Thema erneut auf. Die Problematik wurde vor dem Hintergrund, dass zwar in der Arbeitsgruppe Auskunfteien Einigkeit hinsichtlich bestimmter Grundsätze bestanden hatte, aber kein Beschluss des Düsseldorfer Kreises erwirkt worden war, noch einmal intensiv diskutiert. Im November 2006 wurde dann mehrheitlich ein Beschluss des Düsseldorfer Kreises gefasst, in dem folgendes festgestellt wurde:

Eine generelle Übermittlung von weichen Negativdaten aus dem Inkassobereich für die Auskunftserteilung ist auf Grund entgegenstehender überwiegender schutzwürdiger Interessen des Betroffenen nicht zulässig.

Kann jedoch nach sorgfältiger Einzelfallabwägung die Zahlungsunfähigkeit oder Zahlungsunwilligkeit zweifelsfrei festgestellt werden, d.h. besteht kein Grund zu der Annahme, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, wird eine Übermittlung unter folgenden Voraussetzungen als zulässig angesehen:

1. Es muss sich um eine unbestrittene Forderung handeln.

2. Sowohl Gläubiger als auch Inkassounternehmen haben die der Einmeldung zugrunde liegende Forderung gegenüber dem Schuldner nachweisbar jeweils mindestens zweimal vergeblich schriftlich gemahnt.
3. Der Schuldner wird (z.B. in den Mahnschreiben) darüber informiert, dass eine Einmeldung bei einer Auskunftei erfolgt, soweit die Forderung unbestritten ist und keine Zahlung innerhalb der gesetzten Frist erfolgt.
4. Die Einmeldung erfolgt frühestens dann, wenn vier Arbeitstage seit Ablauf der im letzten Mahnschreiben des Inkassounternehmens genannten Zahlungs- bzw. Rückantwortfrist von zehn Tagen verstrichen sind.

Gegen diesen Beschluss hat sich der Verband der Handelsauskunfteien erneut gewandt. In der Praxis der Datenschutzaufsichtsbehörde Hamburg konnten Zweifelsfälle hinsichtlich der Zulässigkeit der Meldung von sog. weichen Negativmerkmalen an Auskunfteien in der Vergangenheit zufriedenstellend gelöst werden. Eklatante Verstöße wurden bisher nicht festgestellt, würden jedoch unter Berücksichtigung der aufgestellten Grundsätze geahndet werden.

24.3 Auskünfte an die Wohnungswirtschaft

Vermieter und Auskunfteien tauschen nach wie vor Informationen über Mietinteressenten aus. Dies ist aber nur unter eingeschränkten Voraussetzungen und in Bezug auf bestimmte Merkmale zulässig.

Neben der Schufa (vgl. 19.TB, 20.3) übermitteln auch andere Auskunfteien personenbezogene Daten an Vermieter. Schon im November 2004 hat der Düsseldorfer Kreis in einem einstimmigen Beschluss Grundlagen für den Umgang mit diesem Thema geschaffen. Die darin aufgestellten Voraussetzungen wurden von der Aufsichtsbehörde Hamburg für die Aufsichtstätigkeit konkretisiert und sowohl mit betroffenen Auskunfteien als auch mit der Vermieterseite erörtert. Sie werden im Folgenden näher erläutert:

- Aus Sicht des Datenschutzes sind auf branchenspezifische Daten beschränkte Auskunftssysteme vorzuziehen, bei denen die Daten gesicherte Rückschlüsse auf Mietausfallrisiken zulassen.
- Eine uneingeschränkte Auskunft über bei branchenübergreifenden Auskunfteien gespeicherte Daten an potentielle Vermieter ist dagegen unzulässig.

Diese Übereinkunft unter den Datenschutzaufsichtsbehörden bedeutet, dass jegliche Erhebung personenbezogener Daten durch Vermieter bei Auskunf-

teien unzulässig ist, sofern nicht nachstehende Einschränkungen berücksichtigt werden:

- Bei der Prüfung, in welchem Umfang nach § 29 BDSG an potentielle Vermieter personenbezogene Daten übermittelt werden dürfen, sind die schutzwürdigen Belange der Mietinteressenten im Hinblick auf die Bedeutung der Wohnung für die Lebensgestaltung in besonderer Weise zu berücksichtigen. Auskünfte über Eintragungen im Schuldnerverzeichnis sind stets zulässig.

Die Abwägung im Rahmen von Mietverhältnissen erfolgt unter anderen Kriterien als bei sonstigen Vorleistungsfällen. Der Vermieter leistet durch die Überlassung des Mietobjekts vor und ist im Zusammenhang mit Leistungsstörungen auf die rechtlichen Möglichkeiten der Kündigung angewiesen. Dabei kann es zu Problemen im Zusammenhang mit dem Kündigungsschutz und etwaigen Räumungen kommen. Allerdings ist ein Mietverhältnis in der Regel durch Vorauszahlung der Miete gekennzeichnet. Darüber hinaus erhält der Vermieter eine gewisse Zahlungssicherheit durch die Kaution. Von Vermietern wird aber immer wieder auf Mietnomaden hingewiesen, die Wohnungen schon in dem Bewusstsein anmieten, die Miete nicht zu zahlen.

Demgegenüber sind die Interessen der Mieter zu beachten. Bei den meisten Mietern hat die Zahlung der Miete Priorität. Das aus den Auskünften von Auskunfteien ersichtliche Zahlungsverhalten lässt nicht ohne weiteres den Rückschluss auf Mietzahlungen zu. Auch lassen sich Vermieter die Zahlungsfähigkeit ihrer Mieter durch Einkommens- und sonstige Nachweise belegen.

Die Abwägung der Interessenlage führt dazu, dass die Datenschutzaufsichtsbehörde folgende Auskünfte durch Auskunfteien an Vermieter zulässt:

- Daten aus öffentlichen Schuldnerverzeichnissen (Eidesstattliche Versicherungen und Haftbefehle),
- harte Negativdaten (Vollstreckungsbescheide, fruchtlose Pfändungen, rechtskräftige Urteile etc.).

(Meldungen von Vermietern an Auskunfteien nur bei harten Daten. keine Nachmeldungen. Unzulässig sind Auskünfte über weiche Negativdaten (Mahnbescheide, mehrfache Mahnungen etc.).

Es bestehen auch Zweifel an der Zulässigkeit einer Beauskunftung auf Grund einer abverlangten Einwilligung des Mieters. Entsprechendes gilt für das Verlangen der Vorlage einer Selbstauskunft des Mietinteressenten.

Nach Auffassung der Datenschutzaufsichtsbehörde ist die Einforderung einer Einwilligung beim Mieter unzulässig, weil dieser die Einwilligung nicht – wie vom Bundesdatenschutzgesetz vorgesehen – auf freiwilliger Basis erteilt, sondern unter dem Druck steht, den Mietvertrag abschließen zu wollen.

Nachdem diese Grundsätze sowohl den Auskunfteien als auch Vermietern bekannt gemacht wurden, wird die Datenschutzaufsichtsbehörde gegen Verstöße entsprechend vorgehen.

25. Kreditwirtschaft

25.1 Kreditscoring

Der Forderung der Datenschutzaufsichtsbehörden nach mehr Transparenz für die Betroffenen beim Einsatz von Scoring-Verfahren wird durch die Kreditwirtschaft nur unzureichend nachgekommen.

Der Einsatz von Scoring-Verfahren zur Feststellung der Kreditwürdigkeit von Antragstellern und zur Bonitätsbewertung während der Laufzeit eines Kredits ist ein in der Kreditwirtschaft übliches Verfahren der Risikoklassifizierung zur Erfüllung von Basel II, der Eigenkapitalübereinkunft der im Baseler Ausschuss für Bankenaufsicht vertretenen europäischen Finanzaufsichtsbehörden und Zentralbanken. Wir haben über Kreditscoring bereits ausführlich im 20. TB, 21.1 berichtet. Neben der Frage, welche personenbezogenen Daten für die Berechnung des Score-Wertes genutzt werden dürfen, ist aus datenschutzrechtlicher Sicht insbesondere die mangelnde Transparenz der Bewertungen für die Betroffenen ein Problem. Der Düsseldorfer Kreis hatte dazu in der Sitzung vom 10./11. November 2006 beschlossen, dass den Betroffenen auf Antrag die in die Score-Berechnung einfließenden personenbezogenen Merkmale, die dafür genutzten Daten der Kredit suchenden Person und die vier maßgeblichen Merkmale, die im Einzelfall den konkreten Score-Wert der betroffenen Person negativ beeinflusst haben, mitzuteilen sind. Nach Auffassung der Datenschutzaufsichtsbehörden ergibt sich dieses Informationserfordernis aus der Abwägung der berechtigten Interessen der Kreditinstitute mit den schutzwürdigen Belangen der Betroffenen gemäß § 28 Abs. 1 Nr. 2 BDSG. Nur bei einer umfassenden Information der Betroffenen kann davon ausgegangen werden, dass ihre schutzwürdigen Interessen die Interessen der Kreditwirtschaft an der Datenverarbeitung und -nutzung für das Kreditscoring nicht überwiegen. Der Gesetzentwurf der Bundesregierung vom 10. September 2007 sieht in § 34 BDSG eine Erweiterung der Auskunftsrechte der Betroffenen gegenüber Scoringbetreibern vor.

Die Forderung nach mehr Transparenz des Bewertungsverfahrens ist von der Kreditwirtschaft bisher nicht ausreichend umgesetzt worden. Das von den Verbänden des Zentralen Kreditausschusses (ZKA) zum Kreditscoring erarbeitete Informationsmaterial enthält nur allgemeine Erläuterungen zum Kreditscoring und dessen Vorteilen. Der Kunde wird auf die Möglichkeit verwiesen, sich die Gründe für die Ablehnung eines Kreditantrages oder für eine Kreditentscheidung von seiner Bank erläutern zu lassen. Die Kreditwirtschaft beabsichtigt derzeit nicht, den Betroffenen auf Nachfrage einzelne Merkmale,

die den Score im Einzelfall beeinflusst haben, mitzuteilen. Als Grund wird angeführt, dass ein Score-Wert nicht allein an einzelnen Merkmalen festgemacht werden könne. Außerdem könne das Verfahren wegen des Geschäftsgeheimnisses und der Vermeidung von Missbräuchen durch Kunden und Kundenbetreuer nicht völlig offen gelegt werden. Diese Auffassung überzeugt die Datenschutzaufsichtsbehörden nicht. Sie haben in der Sitzung des Düsseldorfer Kreises in Hamburg am 19./20. April 2007 einen weiteren Beschluss zur Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten beim Einsatz von Scoring-Verfahren im Bereich der Kreditwirtschaft gefasst, der auf der Internetseite des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit unter www.bfdi.bund.de veröffentlicht ist. Die Datenschutzaufsichtsbehörden beabsichtigen, ihre bereits auf die derzeitige Gesetzeslage gestützten Forderungen unmittelbar gegenüber den Kreditinstituten durchzusetzen.

25.2 Verkauf von Darlehensforderungen

Bei der Veräußerung von Darlehensforderungen müssen auch die Datenschutzrechte der Forderungsschuldner berücksichtigt werden.

Aufgrund von Beschwerden vieler Bürger, die sich gegen den Verkauf von Darlehensforderungen und die damit verbundene Weitergabe ihrer personenbezogenen Daten an Unternehmen in den USA richteten, haben sich die Datenschutzaufsichtsbehörden mit der Frage beschäftigt, ob und in welchem Umfang die datenschutzrechtlichen Vorschriften beim Forderungsverkauf zu berücksichtigen sind. Nach Auffassung der Datenschutzaufsichtsbehörden sind Übermittlungen von personenbezogenen Daten im Zusammenhang mit Darlehensverkäufen oder Forderungsabtretungen ins Ausland nach § 28 Abs. 1 Nr. 2 BDSG ohne Einwilligung der Forderungsschuldner nur zulässig, wenn es sich um eine notleidende Forderung handelt. Soll die Forderung an eine Stelle außerhalb der EU oder des EWR übertragen werden, ist die damit verbundene Datenübermittlung darüber hinaus nur zulässig, wenn in dem betreffenden Land ein angemessenes Datenschutzniveau besteht oder Vorkehrungen gemäß § 4c Abs. 2 BDSG getroffen worden sind.

Der Zentrale Kreditausschuss (ZKA) hat demgegenüber auf die Grundsatzentscheidung des Bundesgerichtshofs vom 27. Februar 2007 hingewiesen, wonach sich weder aus den zivilrechtlichen Vorschriften des BGB noch aus dem Datenschutzrecht oder den Regelungen des Bankgeheimnisses ein Abtretungsverbot in Bezug auf die Darlehensforderung herleiten lasse. Nach Angabe des ZKA ist der Verkauf von Darlehensforderungen ein Instrument zur Diversifizierung von Kreditrisiken und daher für die einzelnen Kreditinstitute nicht nur in Deutschland, sondern in den meisten EU-Mitgliedstaaten von großer Bedeutung.

Hier ist der Bundesgesetzgeber gefordert, derartigen Fallkonstellationen einen Riegel vorzuschieben, zumindest aber für Transparenz für die Schuldner bei solchen Verkäufen zu sorgen.

26. Handel

26.1 Übermittlung von Kundendaten durch Versandhandelsunternehmen an Auskunfteien

Der Versandhandel lässt bei der Erschließung neuer Geschäftsmodelle den Datenschutz außer Acht.

Bei der Prüfung einer in Hamburg ansässigen Auskunftei wurde bekannt, dass ein Hamburger Versandhandelsunternehmen zu jedem seiner Kunden, mit dem es in laufender Geschäftsbeziehung stand, aus dessen persönlichem Zahlungs- und Geschäftsabwicklungsverhalten einen Bonitätswert/Scorewert errechnete und diesen Kunden-Scorewert, verbunden mit den Kundenadressdaten und weiteren zur eindeutigen Identifikation der Kunden erforderlichen Kundendaten, der Auskunftei für deren Geschäftszwecke zur Verfü-gung stellte. Von Kunden, über die dem Versandhandelsunternehmen „harte“ negative Bonitätsdaten vorlagen und mit denen daher keine laufenden Geschäftsbeziehungen mehr bestanden, wurden keine Bonitätswerte an die Auskunftei weitergegeben. Aus der Bewertungsskala von 0,1 (sehr gute Bewertung) bis 6 (sehr schlechte Bewertung) wurden daher nur Bonitätswerte von Kunden weitergegeben, die zwischen 0,1 und 2,9 (befriedigende Bewertung) lagen.

Diese Kunden-Scorewerte wurden vom Versandhandelsunternehmen insgesamt an die Auskunftei übermittelt und dort auf deren Server getrennt von den Auskunfteidaten gespeichert. Nach einer Vereinbarung zwischen dem Versandhandelsunternehmen und der Auskunftei konnte die Auskunftei im Einzelfall auf den Kunden-Bonitätswert zugreifen, wenn sie selbst über keine bonitätsrelevanten Daten über die angefragte Person verfügte.

Die AGB des Versandhandelsunternehmens enthielten unter dem Stichwort Datenschutz eine Beschreibung der Datenweitergabe an die Auskunftei, die wie folgt lautet: „… Bonitätsdaten auf Basis mathematisch-statistischer Verfahren werden mit Adressdaten zudem an …Name und Anschrift der Auskunftei… weitergegeben, die bei Nachweis eines berechtigen Interesses Auskunft an Dritte erteilt.“

Der Hamburgische Datenschutzbeauftragte untersagte dem Versandhandelsunternehmen die Übermittlung der Kunden-Scorewerte an die Auskunftei wegen fehlender Rechtsgrundlage.

Das Versandhandelsunternehmen wandte dagegen ein, es läge mit dem Datenschutzhinweis in seinen AGB eine Einwilligung der Kunden in die Datenübermittlung vor. Andere Versandhandelsunternehmen würden ebenfalls Kunden-Bonitätsdaten an Auskunfteien übermitteln. Auch ohne das Vorliegen einer Einwilligung der Kunden entspräche die Übermittlung von Scorewerten in vollem Umfang den datenschutzrechtlichen Bestimmungen nach §§ 28, 29 BDSG.

Nach Auffassung des Hamburgischen Datenschutzbeauftragten war die Weitergabe von umfangreichen Kundendaten durch das Versandhandelsunternehmen

an die Auskunftei nicht nach § 28 Abs. 1 Nr. 1 BDSG zulässig, da sie nicht der Zweckbestimmung des Vertragsverhältnisses mit dem Kunden diente. Die Datenweitergabe konnte auch nicht auf § 28 Abs. 1 Nr. 2 BDSG gestützt werden. Zwar hatte das Versandhandelsunternehmen ein berechtigtes wirtschaftliches Interesse an der Vermarktung der bei ihm vorhandenen Bonitätsdaten seiner Kunden. Allerdings überwogen die schutzwürdigen Interessen der betroffenen Versandhauskunden an dem Ausschluss der Nutzung oder Übermittlung ihrer Daten. Die Kunden waren nicht ausreichend darüber informiert, dass ihr Zahlungsverhalten bzw. Kundenverhalten gegenüber dem Versandhandelsunternehmen von diesem mit einem Scorewert bewertet und eine Auskunftei weitergegeben wurde. Die Information in den AGB war unter datenschutzrechtlichen Gesichtspunkten unzureichend. Sie war überraschend und drucktechnisch in den Katalogen kaum lesbar.

Ein Kunde, der im Versandhandel bestellt, muss nicht damit rechnen, dass sein bisheriges, gegebenenfalls langjähriges Kundenverhalten gegenüber dem Versandhandelsunternehmen künftig entscheidend dafür sein kann, ob er Lieferungen von anderen Unternehmen erhält, die bei einer Auskunftei Auskünfte über seine Bonität erfragen. Sein Kundenverhalten im Versandhandel würde zum Maßstab für seine Bonität auch gegenüber künftigen Vertragspartnern werden. Die Argumentation des Versandhandelsunternehmens, die Übermittlung von positiven Scorewerten der Kunden an die Auskunftei läge im grundsätzlichen Interesse der Betroffenen selbst, „weil es diesen ermöglichen würde, erstmals Bestellungen bei anderen Händlern aufzugeben, die dann unverzüglich und ohne zusätzliche Bonitätsabfragen – außer der bei der Auskunftei über ihr Kaufverhalten beim Versandhandelsunternehmen – ausgeführt würden“, war verfehlt. Bei dieser Argumentation wurde verkannt, dass die Betroffenen grundsätzlich selbst über die Verwendung ihrer personenbezogenen Daten bestimmen. Sie dürfen nicht zum Objekt wirtschaftlichen Handels dadurch gemacht werden, dass der Handel selbst definiert, was für den Kunden bzw. seine Daten gut ist. Es bestanden daher schutzwürdige Interessen der Versandhandelskunden an dem Ausschluss der Übermittlung ihrer Kundendaten an eine Auskunftei.

Als Rechtsgrundlage für die Datenweitergabe durch das Versandhandelsunternehmen kam auch § 28 Abs. 3 Nr. 1 BDSG nicht in Betracht. Zwar hatte die Auskunftei ein berechtigtes wirtschaftliches Interesse an der Nutzung von Bonitätsdaten vieler Personen einschließlich der Scorewerte, um diese Daten für eigene Zwecke zur Auskunftserteilung zu nutzen. Jedoch bestand Grund zu der Annahme, dass die betroffenen Versandhauskunden ein überwiegendes schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung ihrer Daten haben (siehe oben).

Die Datenweitergabe war auch nicht nach § 28 Abs. 3 Nr. 3 BDSG zulässig, da die an die Auskunftei übermittelten Daten weit über die in § 28 Abs. 3 Nr. 3 BDSG genannten Daten hinausgingen. Zudem erfolgte die Datenweitergabe an die Auskunftei nicht zum Zwecke der Werbung oder der Markt- und Meinungsforschung.

Nach Auffassung des Hamburgischen Datenschutzbeauftragten wäre die Weitergabe von Bonitätsdaten der Versandhauskunden an Auskunfteien nach den Vorschriften des BDSG nur mit einer Einwilligung der Kunden zulässig gewesen. Eine solche Einwilligung der Versandhauskunden lag jedoch nicht vor. Nach § 4 a BDSG ist eine Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung der Daten hinzuweisen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Datenschutzhinweis in den AGB des Versandhandelsunternehmens entsprach weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligungserklärung. Eine so weitgehende Datenweitergabe, wie sie von dem Versandhandelsunternehmen durchgeführt wurde bzw. weiterhin beabsichtigt ist, konnte nicht durch eine Klausel in Allgemeinen Geschäftsbedingungen gerechtfertigt werden. Vielmehr ist eine Einwilligung des Betroffenen erforderlich, der ausdrücklich darauf hingewiesen werden müsste, welche Daten zu welchem Zweck an wen weitergegeben wurden. Es ist zweifelhaft, ob im Versandhandel, soweit dieser auf telefonischen Bestellungen basiert, eine schriftliche Einwilligung eingeholt werden kann, die den Anforderungen des § 4 a BDSG entspricht.

Die Verbraucherzentrale Hamburg, die von der Aufsichtsbehörde auf die Datenübermittlungsklausel in den AGB das Versandhandelsunternehmen hingewiesen wurde, hat das Unternehmen aufgefordert, die Klausel künftig zu unterlassen.

Die Datenschutzaufsichtsbehörden haben die Problematik in der Sitzung des Düsseldorfer Kreises in Hamburg am 19./20. April 2007 erörtert und einstimmig den folgenden Beschluss gefasst:

> Weitergabe von Kundendaten durch Versandhandelsunternehmen an Auskunfteien
>
> Die Übermittlung von personenb#ezogenen Daten über das vertragsgemäße Zahlungs- und Geschäftsabwicklungsverhalten ihrer Kunden sowie die Übermittlung von Scorewerten, die auf der Grundlage dieses Verhaltens berechnet wurden, durch Versandhandelsunternehmen an Auskunfteien zur Nutzung für deren eigene Geschäftszwecke ist unzulässig, es sei denn, die Kunden haben ausdrücklich in die Weitergabe dieser Daten eingewilligt.
>
> Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Das Hamburger Versandhandelsunternehmen und seine Tochterunternehmen haben den Beschluss des Düsseldorfer Kreises mittlerweile umgesetzt. Eine Weitergabe der oben beschriebenen Kundendaten an die Auskunftei findet nicht mehr statt. Die Datenschutzklauseln der Online-Shops sind geändert worden. Die Drucklegung in den Katalogen wird zum Beginn des Jahres 2008 umgesetzt werden.

26.2 Übermittlung von Umzugsdaten an Adresshändler

Datenübermittlungen des Versandhandels ersetzen Melderegisterauskünfte und Informationen über Nachsendeanträge.

Der Düsseldorfer Kreis hat in der Sitzung in Hamburg am 19./20. April 2007 die Frage der datenschutzrechtlichen Zulässigkeit der Übermittlung von Umzugsdaten durch Versandhandelsunternehmen an Adresshändler erörtert und dazu den folgenden Beschluss gefasst:

> Weitergabe von umzugsbedingten Adressänderungen durch Versandhandelsunternehmen
>
> Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest: Übermittelt ein Unternehmen Umzugsadressen seiner Kunden an andere Unternehmen zur weiteren Übermittlung dieser Adressänderungen an angeschlossene Unternehmen zum Zwecke des Adressabgleichs, so ist dies nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß § 4a BDSG zulässig.
>
> Ein Datenschutzhinweis in den Allgemeinen Geschäftsbedingungen eines Versandhandelsunternehmens entspricht weder der Form noch dem Inhalt nach den Anforderungen an eine wirksame Einwilligung im Sinne von § 4a BDSG. Eine Einwilligung der Kunden setzt voraus, dass diese ausdrücklich darauf hingewiesen werden, welche Daten zu welchem Zweck an wen weitergegeben werden sollen.

Hintergrund des Beschlusses war die Weitergabe von Umzugsinformationen durch ein deutsches Versandhandelsunternehmen an einen großen Adresshändler. Neben der alten Adresse wurde auch die neue Adresse an den Adresshändler übermittelt. Nach Auffassung des Versandhandelsunternehmens war die Weitergabe der Umzugsinformationen nach § 28 Abs. 1 Nr. 2 und Abs. 3 Nr. 1 BDSG zulässig, da keine entgegenstehenden Interessen der Versandhauskunden gegen das Verfahren erkennbar seien. Die Kunden würden in den AGB über die Datenweitergabe informiert. Außerdem würde der Adresshändler die neuen Adressen nur zur Aktualisierung bestehender Datenbestände verwenden, d.h. wenn die Person mit der alten

Adresse bereits im Datenbestand des Dritten enthalten sei. Auch andere Versandhandelsunternehmen wollten dieses lukrative Geschäftsmodell übernehmen.

Bei der Erörterung im Düsseldorfer Kreis bestand Einvernehmen, dass die bei der Zulässigkeitsprüfung im Rahmen der Abwägung zu berücksichtigenden schutzwürdigen Interessen der Versandhauskunden höher zu bewerten sind als die wirtschaftlichen Interessen der Versandhandelsunternehmen und der Adresshändler. Es sollte grundsätzlich jedem selbst überlassen bleiben, ob und wem er mitteilt, dass er umgezogen ist. Hinzu kommt, dass die Betroffenen nicht damit rechnen müssen, dass eine Bestellung im Versandhandel eine Adress-Berichtigungswelle im gesamten Bundesgebiet auslösen kann. Während die Betroffenen bei den bei der Post AG gestellten Nachsendeaufträgen selbst entscheiden können, ob sie eine Mitteilung ihrer neuen Adressen wünschen, erfolgte die Weitergabe der umzugsbedingten Adressänderung durch Versandhandelsunternehmen ohne eine entsprechende Einwilligung der Kunden. Im Düsseldorfer Kreis bestand Einigkeit, dass die Übermittlung von Umzugsadressen der Versandhauskunden an Adresshändler zur weiteren Übermittlung an angeschlossene Unternehmen nur mit einer ausdrücklichen Einwilligung der Betroffenen gemäß § 4a BDSG zulässig ist.

Die Einräumung einer Widerspruchsmöglichkeit für die Kunden ist nicht ausreichend. Ein Versandhandelsunternehmen hatte vorgeschlagen, seine Kunden in einem Anschreiben über eine beabsichtigte Übermittlung von umzugsbedingten Adressänderungen an Adresshändler zu unterrichten. Den Kunden sollte die Möglichkeit eingeräumt werden, innerhalb einer Frist von vier Wochen zu widersprechen. Nach Meinung der Datenschutzaufsichtsbehörden berücksichtigte auch dieses Verfahren die Interessen der betroffenen Kunden nicht im erforderlichen Umfang, da die Kunden selbst aktiv werden müssen, wenn sie die Übermittlung nicht wünschen. Im Übrigen kann nicht sichergestellt werden, dass die Betroffenen derartige Schreiben tatsächlich lesen, da nicht auszuschließen ist, dass als Werbepost angesehene Schreiben von Versandhandelsunternehmen durch Kunden weggeworfen werden.

26.3 Member Cards – Service ohne Datenschutz?

Bei der Datenverarbeitung im Zusammenhang mit der Herausgabe und Nutzung von so genannten Member Cards, die einem ausgewählten Personenkreis als Werbemittel für die kostenfreie Nutzung von Einrichtungen eines Einkaufszentrums zugesandt werden, sind die Vorschriften des Bundesdatenschutzgesetzes zu beachten.

Durch eine Beschwerde wurden wir darauf aufmerksam, dass von einem großen Einkaufszentrum an einen ausgewählten Personenkreis als Werbemaßnahme

Member-Cards übersandt wurden. Diese ermöglichen eine kostenfreie Nutzung einer Members Lounge und das kostenlose Parken im Einkaufszentrum. Die mit einem Chip versehenen Members Cards wurden mit einem persönlichen Anschreiben, in dem die Vorzüge der Karte geschildert wurden, an ausgewählte Personen, unter anderem Politiker, übersandt. Das Anschreiben enthielt allerdings keine Informationen darüber, ob und welche Daten auf dem Chip gespeichert werden und ob über Lesegeräte ausgewertet werden kann, wann und wie lange sich die Karteninhaber in der Members Lounge oder im Parkhaus aufhalten.

Auf Anfrage hat das die Karten herausgebende Unternehmen mitgeteilt, dass auf den Member-Cards ein Code gespeichert ist. Anhand des Codes erkenne das Zugangssystem, ob die Karte zugelassen und damit der Inhaber zum Zugang berechtigt sei. Vorübergehend werde gespeichert, wann welche Karten an welchem Lesegerät eingesetzt würden. Anderenfalls könne nicht festgestellt werden, ob der Inhaber der Karte auch berechtigt sei, den jeweiligen Bereich, wie z.B. das Parkhaus, wieder zu verlassen. Die Daten würden jedoch kurzfristig nach deren Einsatz gelöscht. Nach der Löschung sei nur noch eine statistische Erfassung, wie viele Besucher beispielsweise die Lounge oder das Parkhaus während einer bestimmten Zeit besucht hätten, möglich. Die Daten würden nicht an Dritte weitergegeben.

Nach den Vorschriften des Bundesdatenschutzgesetzes war die Vorgehensweise des Unternehmens zu beanstanden. Grundsätzlich ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nach der Rechtsvorschrift des § 28 Abs. 1 Satz 1 Nr. 2 BDSG, auf die sich das Unternehmen berufen hat, zulässig, soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt. Der mit der Herausgabe der Karte verbundene Werbeeffekt und die so mögliche Kundenbindung können als berechtigtes Interesse des Unternehmens zur Nutzung und Speicherung von personenbezogenen Daten anerkannt werden. Allerdings besteht nach der dargestellten Sachlage Grund zu der Annahme, dass überwiegende schutzwürdige Interessen der Betroffenen der Datenverarbeitung im Zusammenhang mit dem Einsatz der Karte entgegenstehen und diese nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG unzulässig ist. Die Betroffenen erhalten die Karte, ohne einen entsprechenden Antrag gestellt zu haben. Ihre Daten werden ohne ihr Zutun für die Herausgabe der Karte erhoben und gespeichert, ohne dass sie sich gegen die Datenverarbeitung wenden können. Sie werden nicht über den Umfang der Datenverarbeitung bei Einsatz der Karte unterrichtet und haben daher keine Vorstellung, wann welche Daten zu welchem Zweck wie lange gespeichert werden. Wegen des Fehlens einer solchen Information kann man auch nicht davon ausgehen, dass die Betroffenen durch die Nutzung der Karte in die entsprechende Erhebung und Verarbeitung von Daten beim Einlass in die Lounge oder das Parkhaus konkludent einwilligen, so dass die Datenverarbeitung auch nicht nach § 4 Abs. 1 BDSG zulässig ist.

Es ist daher unbedingt erforderlich, den Umfang der Datenverarbeitung in den Hinweisen zur Member-Card zu beschreiben. Da nach § 35 Abs.2 Nr. 2 BDSG personenbezogene Daten zu löschen sind, wenn ihre Speicherung unzulässig ist, muss das Unternehmen außerdem dafür Sorge tragen, dass die Daten für die Member-Card gelöscht werden, wenn die Betroffenen die Karte nicht nutzen oder ausdrücklich eine Löschung ihrer Daten wünschen. Das Unternehmen hat zugesagt, diese Forderungen umsetzen.

27. Werbung

27.1 Fehlende Hinweise auf das Widerspruchsrecht nach § 28 Abs. 4 BDSG

Viele werbende Unternehmen ignorieren ihre Informationspflichten nach dem Bundesdatenschutzgesetz.

Mehr als sechs Jahre gelten mittlerweile die erweiterten Regelungen des Bundesdatenschutzgesetzes im Bereich der Werbung sowie der Markt- und Meinungsforschung. Sie verpflichten die werbende Stelle und das Markt- und Meinungsforschungsunternehmen, diejenige Person, der Werbung oder ein Fragebogen zur Marktforschung zugeschickt werden soll, „bei der Ansprache" zum Zweck der Werbung oder der Markt- und Meinungsforschung, d.h. im Anschreiben über die verantwortliche Stelle sowie über das Widerspruchsrecht zu informieren (§ 28 Abs. 4 Satz 2 BDSG). Folgende Formulierungen seien hier beispielhaft genannt:

„Wenn Sie künftig unsere Angebote nicht mehr erhalten möchten, teilen Sie uns dies bitte schriftlich, unter Beifügung des Original-Werbeanschreibens, das Ihre Adresse enthält, mit."

„Sollten Sie zukünftig keine weiteren Informationen von uns oder anderen Unternehmen erhalten wollen, teilen Sie uns das bitte kurz schriftlich oder telefonisch mit."

Nicht erforderlich ist die Nennung der Vorschrift des § 28 Abs. 4 Satz 2 BDSG oder eine wörtliche Wiedergabe dessen Inhalts. Dem Betroffenen muss aber aus der verwendeten Formulierung unmissverständlich klar werden, dass er weitere Werbeanschreiben oder Aufforderungen zur Teilnahme an Meinungsumfragen durch die Einlegung eines Widerspruchs verhindern kann. Sofern das Werbeschreiben die dafür verantwortliche Stelle nebst Anschrift deutlich erkennen lässt, ist ein weiterer Hinweistext nicht erforderlich.

1. Gestaltung der Belehrung:

   Damit der Hinweis wahrgenommen werden kann, sollte der Text hervorgehoben sein. Dazu gibt es verschiedene gestalterische Möglichkeiten, z.B. Kursiv-Satz abgesetzt vom Werbetext am Ende des Werbebriefes, einge-

rahmter Kasten unten oder rechts oben neben dem Adressfeld. Kleine oder fast farblose Schrift ist nicht geeignet. Der Hinweis darf auch nicht in den Werbeschreiben versteckt werden.

2. Ort der Belehrung:

   In der Regel muss der Hinweis auf das Widerspruchsrecht auf dem Anschreiben selbst erfolgen. In Einzelfällen kann eine ausdrückliche Information in den beigefügten AGB, auf dem Kuvert oder im Katalog ausreichend sein. Dies könnte insbesondere dann gelten, wenn nur der Katalog ohne gesondertes Anschreiben übersandt wird.

3. Wiederholung der Belehrung:

   Die Frage, ob das Tatbestandsmerkmal „bei der Ansprache" dahingehend ausgelegt werden kann, dass die Unterrichtungspflicht nur für das jeweils erste Werbeanschreiben bestehe, so dass in nachfolgenden Werbeschreiben auf den Hinweis verzichtet werden könnte, ist zu verneinen. Zum einen bedeutet „Ansprache" in diesem Zusammenhang lediglich, dass es sich um persönlich adressierte Werbung handelt im Gegensatz zu nicht personalisierten Wurfsendungen oder Zeitungsbeilagen. Zum anderen wird im Einzelfall nicht nachweisbar sein, dass das vorangegangene Anschreiben geöffnet bzw. gelesen und damit der Hinweis wahrgenommen wurde.

4. Beauftragung eines Dienstleisters:

   Wird ein Dienstleister (Adresshändler, Lettershop usw.) mit der Herstellung und dem Versand von Werbesendungen beauftragt, hat sich der Auftraggeber davon zu überzeugen, dass in der Webesendung die erforderlichen Informationen enthalten sind.

Seit Mai 2001 musste die Aufsichtsbehörde ca. 40 Unternehmen, oftmals wiederholt, auf die Hinweispflicht aufmerksam machen und ihre Einhaltung einfordern. Vielen Unternehmen ist nicht bewusst, dass ein Verstoß gegen die Hinweispflicht eine Ordnungswidrigkeit nach § 43 Abs. 1 Nr. 3 BDSG darstellt.

27.2 Präzise Auskunft über Herkunft der Daten und Werbewiderspruch

Alle Versender von Werbepost sind verpflichtet, präzise Auskunft über die Herkunft der personenbezogenen Daten zu geben und Werbewidersprüche zu beachten.

Viele Bürger, die an sie adressierte Werbung in ihrem Briefkasten vorfinden, gehen davon aus, dass ihre Adressdaten nur mit ihrer Einwilligung für Werbezwecke genutzt und an Dritte übermittelt werden dürfen. Das ist jedoch falsch. Das Bundesdatenschutzgesetz privilegiert die Werbewirtschaft und sieht dementsprechend vor, dass die Adressdaten auch ohne Einverständnis des Betroffenen für Werbung sowie für Markt- und Meinungsforschungszwecke genutzt und übermittelt werden dürfen, solange der Betroffene der Zusendung von Werbung nicht widersprochen hat oder das werbende Unternehmen keine schutzwürdigen Interessen des Betroffenen, von der Werbung verschont zu werden, anneh-

men muss. Viele Bürger empfinden die Zusendung von Werbung als Belästigung und wollen keine Werbung mehr erhalten und sind daran interessiert zu erfahren, woher das werbende Unternehmen ihre Daten erhalten hat, und machen daher von ihrem Auskunftsrecht nach § 34 Abs.1 BDSG Gebrauch. Von den werbenden Unternehmen erhalten die Betroffenen aber oft keine oder nur eine unvollständige Auskunft. Vielfach wird geantwortet:

- Die Quelle könne aus Datenschutzgründen nicht genannt werden,
- die Daten stammten von Partnerunternehmen oder Kooperationspartnern, ohne dass deren Namen und Anschriften genannt würden,
- es bestünde keinerlei Zugriff auf den Datenbestand des Kooperationspartners,
- man hätte als staatliches Lotterieunternehmen Einblick in sämtliche Datenbanken; eine konkrete Datenbank wird jedoch nicht genannt,
- die Daten würden dem „zentralen Register für Werbemedien in Berlin" – das es gar nicht gibt – entnommen,
- zufriedene Kunden hätten dem werbenden Unternehmen Interessentendaten zur Verfügung gestellt.

Teilweise wird dem Betroffenen als Antwort mitgeteilt, seine Daten seien gelöscht worden, über die Herkunft der Daten wird er allerdings nicht informiert. Dem gegenüber gilt:

Nach § 34 Abs. 1 BDSG kann der Betroffene Auskunft verlangen über

1. die zu seiner Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. Empfänger oder Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Die verantwortliche Stelle, das ist das werbende Unternehmen, ist verpflichtet, dem Betroffenen Auskunft zu erteilen. Dabei reicht es beispielsweise nicht, pauschal mitzuteilen, Adressen würden von einem Partnerunternehmen stammen. Anzugeben sind dann Firmenname und eine zustellungsfähige Anschrift, damit der Betroffene dort seine Datenschutzrechte wahrnehmen kann. Soweit das werbende Unternehmen personenbezogene Daten des Betroffenen nutzt, die bei einer ihm nicht bekannten Stelle gespeichert sind, hat es auch sicherzustellen, dass der Betroffene Kenntnis über die Herkunft der Daten erhalten kann (§ 28 Abs. 4 Satz 2 BDSG).

Widerspricht der Betroffene der Nutzung oder Übermittlung seiner Daten für Zwecke der Werbung oder der Markt- oder Meinungsforschung, ist eine Nutzung oder Übermittlung für diese Zwecke unzulässig (§ 28 Abs. 4 Satz 1 BDSG). Der Hinweis des werbenden Unternehmens, der Betroffene könne sich auf die Robinsonliste setzen lassen, reicht nicht. Vielmehr muss das werbende

Unternehmen selbst, z.B. durch eine interne Sperrliste, dafür sorgen, dass der Betroffene von diesem Unternehmen keine Werbesendung mehr erhält.

Viele Betroffene verlangen eine Löschung ihrer Daten. Sie haben jedoch nur einen Anspruch auf Sperrung ihrer Daten. Dies macht auch Sinn. Viele Unternehmen mieten Adressen an, ohne sie selbst zu speichern, sie können daher auch dort nicht gelöscht werden. Da aber der Werbende dafür verantwortlich ist, eine Sperrung des Betroffenen zu berücksichtigen, ist der beste Weg für das Unternehmen, selbst eine Sperrliste zu führen. Wenn das Unternehmen den Adresshändler bittet, den Datensatz zu sperren, hilft dies nicht viel. Denn bei der nächsten Aktion kann sich das Unternehmen eines anderen Adresshändlers bedienen und dieser ist nicht über die Sperrung informiert. So käme es erneut zu einer Aussendung an Betroffene, die widersprochen haben und sich – zu Recht – dann darüber beschweren. Eine Löschung bei den Adresshändlern hätte das gleiche Ergebnis. Die Adresshändler füllen ihre Datenbestände mit neuen und aktualisierten Daten auf. Auf dieses Art und Weise kämen dann wieder Betroffene in die Adressdateien, obwohl sie eigentlich widersprochen haben. Im Ergebnis ist das Sperren die beste Lösung, um einen Widerspruch zu berücksichtigen.

28. Sonstiges

28.1 Mahnung durch Computeranruf

Es ist nicht zulässig, säumige Schuldner über einen computergesteuerten Telefonanruf zu mahnen.

Große Unternehmen, aber auch Inkassobüros, gehen teilweise dazu über, offene Rechnungen per Computeranruf telefonisch anzumahnen. Die Gründe dafür liegen auf der Hand: Einerseits sind Telefonate deutlich kostengünstiger als schriftliche Mahnungen, andererseits finden sich derart Angesprochene möglicherweise schneller bereit, die ausstehenden Forderungen zu begleichen. Dies umso mehr, als eine Wiederholung eines solchen Anrufs nicht ausgeschlossen werden kann. Damit ist aber in vielen Fällen die Gefahr verbunden, dass dritte Personen von den Schulden des Betroffenen erfahren.

Genau das sind auch die datenschutzrechtlichen Risiken, die die Mahnung durch Computeranruf unzulässig macht. Nach § 9 Satz 1 BDSG ist die innerbetriebliche Organisation bei automatisierter Verarbeitung oder Nutzung personenbezogener Daten so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Dabei ist zu gewährleisten, dass Unbefugte keinen Zugriff auf personenbezogene Daten erhalten. Gerade in diesem sensiblen Bereich kann es nicht zulässig sein, es dem Zufall zu überlassen, wer den Anruf entgegen nimmt.

Der Düsseldorfer Kreis hat daher in seiner Sitzung im April 2007 in Hamburg einstimmig folgenden Beschluss gefasst:

Mahnung durch Computeranruf

Die obersten Aufsichtsbehörden für den Datenschutz im nicht-öffentlichen Bereich stellen dazu fest:

Eine telefonische Mahnung durch Computeranruf ist wegen der hohen Gefahr, dass ein anderer als der vorgesehene Empfänger die Nachricht erhält und so personenbezogene Daten einem Dritten unbefugt offenbart werden, unzulässig.

28.2 Telefonwerbung durch Parteien

Telefonwerbung ohne eine ausdrückliche vorherige Einwilligung ist unzulässig. Dies gilt auch für Telefonanrufe, die dem Zweck der Wahlwerbung dienen sollen.

Vor der Bürgerschaftswahl 2008 hat der Hamburgische Datenschutzbeauftragte darauf hingewiesen, dass Telefonwerbung ohne eine ausdrückliche vorherige Einwilligung derjenigen, die angerufen werden sollen, unzulässig ist. Dies gilt nicht nur für kommerzielle Telefonwerbung, die nach dem Gesetz gegen den unlauteren Wettbewerb verboten ist, sondern in gleicher Weise für Telefonanrufe, die dem Zweck der Wahlwerbung dienen sollen. Auch bereits der bloße Anruf bei Bürgern mit der Aufforderung, zur Wahl zu gehen, ist, soweit der Anruf im Zusammenhang mit der Nennung einer Partei steht, unzulässig. Erst recht unzulässig ist ein Anruf von Seiten einer Partei, mit dem eine bestimmte Stimmabgabe erreicht werden soll. Unerbetene Telefonanrufe verletzen das Persönlichkeitsrecht und die Privatsphäre der Angerufenen auch dann, wenn sie von einer politischen Partei zu Wahlzwecken vorgenommen werden. Die angerufenen Bürger haben einen Anspruch auf Unterlassung solcher Anrufe. Die Parteien können sich auch nicht auf das Parteienprivileg berufen. Das Bestreben einer politischen Partei, möglichst viele Stimmberechtigte für ihre Ziele zu gewinnen, hat hinter dem Recht des Einzelnen auf Respektierung seines häuslichen Lebensbereichs zurückzutreten.

Hintergrund des Hinweises waren Telefonkampagnen mehrerer politischer Parteien im Zusammenhang mit der Bürgerschaftswahl 2004. Damals beschwerten sich zahlreiche Bürger über die telefonische Wahlwerbung der Parteien. Der Hamburgische Datenschutzbeauftragte hat die Parteien daher aufgefordert, auf telefonische Werbung für die Bürgerschaftswahl zu verzichten.

29. Bußgeldfälle

Im Berichtszeitraum mussten erneut Bußgelder festgesetzt werden.

Für die Aufsichtsbehörde steht bei der Kontrolle der Durchführung des Datenschutzes in den Unternehmen nicht im Vordergrund, Bußgelder zu verhängen.

Die Unternehmen zeigen in der Regel Einsicht und Verständnis für die Forderungen, Ratschläge und Hinweise der Aufsichtsbehörde. Dennoch sind Bußgeldverfahren unvermeidlich.

Drei Verfahren betrafen zwei verantwortliche Stellen, die jeweils durch denselben Geschäftsführer/Inhaber vertreten wurden. Trotz mehrfacher Aufforderung zur Auskunftserteilung gegenüber der Aufsichtsbehörde wurde nicht reagiert bzw. die Auskunft nicht vollständig erteilt (§ 43 Abs. 1 Nr. 10 BDSG). Das gegen beide verantwortliche Stellen verhängte Bußgeld in Höhe von insgesamt € 1.800 wurde im Einspruchsverfahren vom Amtsgericht wegen wirtschaftlich schlechter Verhältnisse des Beschuldigten auf € 500 herabgesetzt.

Strafanträge wurden nicht gestellt.

30. Meldepflicht und Prüftätigkeit

30.1 Meldepflicht und Register nach § 4d BDSG

Die Zahl der Meldungen ist leicht gestiegen.

Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die nach § 4d BDSG der Meldepflicht unterliegen. Bisher haben 42 Unternehmen ihre Angaben zur Meldepflicht entsprechend den Vorgaben des § 4e BDSG angepasst oder sich zum ersten Mal zum Register gemeldet (vgl. 18. TB, 29.1, 19. TB, 27.1, 20. TB 30.1). Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich folgendes Bild:

- Speicherung zum Zwecke der Übermittlung
  - Auskunfteien/Warndienste 10
  - Informationsdienste 4
  - Adresshändler 5
- Speicherung zum Zwecke der anonymisierten Übermittlung
  - Markt- und Meinungsforschung 23

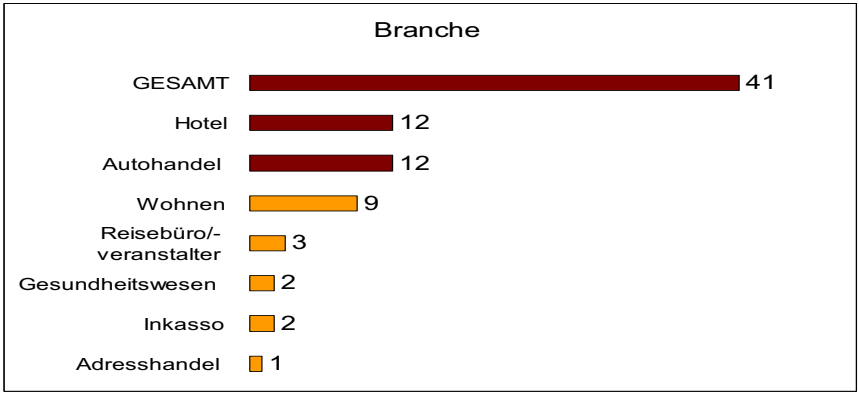
30.2 Prüfungen

Bei unseren anlassfreien Unternehmensprüfungen wurden teilweise gravierende Datenschutzmängel festgestellt.

Im Berichtszeitraum haben wir in insgesamt 41 Unternehmen die Einhaltung der datenschutzrechtlichen Bestimmungen geprüft. Nach unseren Erfahrungen aus den vergangenen Jahren haben wir verstärkt den Schutz der per-

sonenbezogenen Daten in den konkreten Datenverarbeitungsprozessen kontrolliert. Dabei wurde vor allem Wert auf die Prüfung der Rechtmäßigkeit der Erhebung und Verarbeitung – insbesondere Übermittlung – personenbezogener Daten gelegt. Unser Ziel ist es, mehr Transparenz zu erzeugen, sowohl für die betroffenen Kunden / Mitglieder etc. aber auch für die Unternehmensleitungen. Dabei verweisen wir auf das überarbeitete Muster eines Verfahrensverzeichnisses (nach § 4g i.V.m. § 4e BDSG), das Interessierten auch als Download auf unserer Internet-Seite www.datenschutz.hamburg.de zur Verfügung steht.

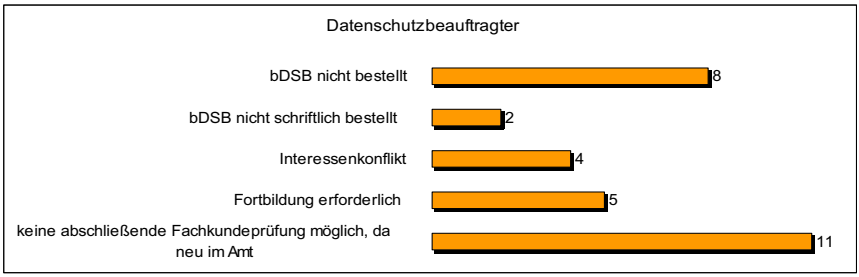
Unsere Kontrollen haben wir in folgenden Bereichen vorgenommen:

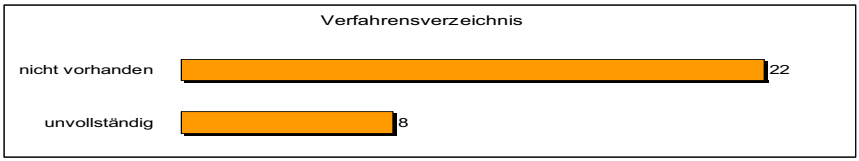


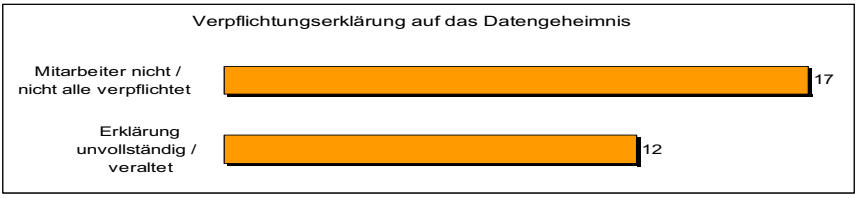
Gegenstand der Prüfungen war vor allem:

- Die Verpflichtung zur Bestellung eines Datenschutzbeauftragten nach § 4f BDSG und die Fachkunde des Datenschutzbeauftragten nach § 4g Abs. 1 BDSG,
- das Verfahrensverzeichnis nach § 4g Abs. 2 BDSG,
- die Verpflichtung der Mitarbeiter, die personenbezogene Daten verarbeiten, auf das Datengeheimnis nach § 5 BDSG,
- die erforderlichen technischen und organisatorischen Maßnahmen nach § 9 BDSG,
- die Anforderungen bei einer Auftragsdatenverarbeitung nach § 11 BDSG,
- die Meldepflicht nach § 4d BDSG.

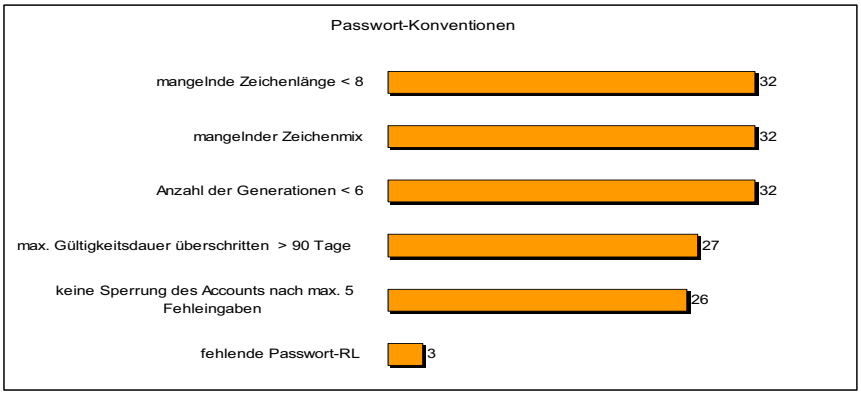
Keine Prüfung konnte ohne die Feststellung von Mängeln abgeschlossen werden. Die folgenden Angaben basieren auf 35 Prüfungen, da 6 Prüfungen zum Stichtag (31.12.2007) noch nicht abgeschlossen waren. Es war zu beanstanden:



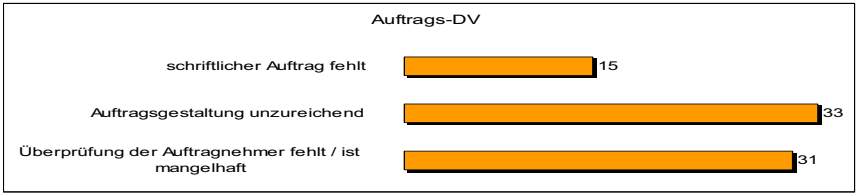




Auch im Bereich der IT-Sicherheit stellten wir zahlreiche Mängel fest:



Zahlreiche Datenverarbeitungen waren unzureichend gegen unberechtigte Zugriffe gesichert. Die Empfehlungen zum IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik – BSI – wurden nicht oder nur teilweise berücksichtigt.



Trotz gesetzlicher Verpflichtung fehlte bei rund 60 % der geprüften Unternehmen ein Verfahrensverzeichnis, etwa 23 % der kontrollierten Firmen hatten keinen betrieblichen Datenschutzbeauftragten bestellt. In Fällen einer Auftragsdatenverarbeitung fehlte es ganz überwiegend an der erforderlichen Kontrolle der Auftragsdatenverarbeiter. Obwohl das Datenschutzrecht in erster Linie eine Selbstkontrolle der Wirtschaft vorsieht, belegen die bei unseren Prüfungen festgestellten Mängel, dass einer Kontrolle durch die Aufsichtsbehörde notwendig ist. Trotz knapper personeller Ressourcen werden wir daher weiterhin anlassfreie Unternehmensprüfungen durchführen.

BÜRGERSERVICE UND DIENSTSTELLE

31. Eingaben

Jede Person kann sich an den Hamburgischen Datenschutzbeauftragten wenden, wenn sie der Ansicht ist, bei der Verarbeitung ihrer persönlichen Daten durch eine hamburgische Behörde oder durch ein Unternehmen mit Sitz in Hamburg in ihren Rechten verletzt worden zu sein. Die vielen Eingaben, die an uns herangetragen werden, zeigen, dass datenschutzrechtliche Bestimmungen sowohl von den öffentlichen als auch von den nicht öffentlichen Stellen nicht immer ausreichend beachtet werden. Unsere Einschaltung führt in der Regel aber zu befriedigenden Ergebnissen.

Die Zahl der Eingaben steigt weiter an. Von Januar 2006 bis Dezember 2007 gingen 1.333 schriftliche Eingaben ein. Sie betrafen – getrennt für die Jahre 2006 und 2007 – folgende Datenschutzbereiche:

	2006	2007
Versicherungswirtschaft	19	19
Kreditwirtschaft	15	33
Priv. Wohnungswirtschaft	6	16
Versandhandel	9	15
sonst. Handel	22	33
Werbung, Direktmarketing	94	107
Schufa, Auskunfteien	35	53
Markt- und Meinungsforschung	1	7
Vereine	21	9
Freie Berufe	12	22
Soziales u. Gesundheitsw., nicht-öff.	13	4
Personaldatenschutz, nicht-öff.	24	22
Verkehrswesen, nicht-öff.	2	3
Sonstiges, nicht-öff.	55	48
Justiz	10	10
Strafvollzug	13	8
Sicherheitsüberprüfungen	2	1
Verfassungsschutz	9	7
Polizei	27	29
Staatsanwaltschaft	7	12
Meldewesen	12	13
Wahlen	-	1
MDK, Kranken- und Pflegedienste	6	2
ALG II	23	47
andere Sozialbereiche	34	24
Gesundheitswesen, öff.	7	9
Personaldatenschutz, öff.	21	17
Verkehrswesen, öff.	7	4
Ausländerwesen	4	2
Finanz- und Steuerwesen	12	5
Bildungswesen	27	20
Wirtschaftsverwaltung	5	3
Telekommunikation	24	10
Tele- und Mediendienste	39	51
Medien	2	7
Technik	7	6
Personenstandswesen	4	-
Statistik	1	1
Bau- und Vermessungswesen	4	1
Hochschulen	2	4
Scientology	5	9
Umweltschutz	1	2
Sonstiges, öff.	18	21
Abgaben	59	54
Insgesamt Eingaben:	643	690

32. Beratungen und Informationsangebote

Beratungen und Prüfungen nehmen den größten Teil der Kapazität der Dienststelle in Anspruch. Unsere Informationsmaterialien werden von den Bürgerinnen und Bürgern überwiegend per Internet abgerufen.

Im Berichtszeitraum haben wir insgesamt 2.600 Bürgerinnen und Bürger, die sich persönlich, telefonisch oder schriftlich mit ihren Fragen und Problemen zum Datenschutz an uns gewandt haben, beraten (2006 ca. 1.280 Fälle, 2007 ca. 1.320 Fälle).

Wir prüften im Jahr 2006 in über 370 Fällen und im Jahr 2007 in über 440 Fällen öffentliche und nicht öffentliche Stellen. In rund 115 Fällen im Jahr 2006 und in rund 80 Fällen im Jahr 2007 gaben wir Stellungnahmen zu Datenschutzfragen in Rechts- oder Verwaltungsvorschriften ab.

Unsere Informationsmaterialien werden gut nachgefragt. Die Handreichungen und Materialien werden überwiegend über unser Internet-Angebot abgerufen (www.datenschutz.hamburg.de).

Dienststelle (Stand: 1. Februar 2008)

Der Hamburgische Datenschutzbeauftragte Tel: 040/42854-4040
Klosterwall 6, 20095 Hamburg Fax: 040/42841-4000
E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.datenschutz.hamburg.de

		Durchwahl
Dienststellenleiter:	Hartmut Lubomierski	– 4041 –
Stellvertreter:	Dr. Hans-Joachim Menzel	– 4049 –
Vorzimmer:	Heidi Niemann	– 4040 –
Geschäfts- und Verwaltungsangelegenheiten der Dienststelle	Rolf Nentwig	– 4043 –
Informationsmaterial	Irene Heinsohn	– 4042 –
	Heidi Niemann	– 4040 –
IuK-Leitung und IuK-Planung, Internetangebot der Dienststelle	Martin Schemm	– 4044 –
Grundsatzfragen des Datenschutzrechts einschließlich EU-Recht, Datenschutzgesetze, Parlamentsangelegenheiten	Dr. Renate Thomsen	– 4062 –
Gesundheitswesen, Bauen und Wohnen / Vermessungswesen, Umwelt, Justiz / Staatsanwaltschaft, Verfassungsschutz, Sicherheitsüberprüfungen, Archivwesen, Kultur	Dr. Hans-Joachim Menzel	– 4049 –
Ausländerangelegenheiten, Wirtschaftsverwaltung, Gewerberecht, Verkehrswesen, Wahlen und Volksabstimmungen	Eva-Verena Scheffler	– 4064 –
Polizei, Feuerwehr, Rundfunk / Medien	Heike Wolters	– 4052 –
Strafvollzug, SGB II (Arbeitslosengeld 2), Kinderbetreuung, Forschung	Dr. Manfred Jäger	– 4045 –

Soziales (außer SGB II), Bildungswesen,
Allgemeine Bezirksangelegenheiten, Kirchen
Detlef Malessa – 4050 –

Statistik, Personenstandswesen, Meldewesen, Finanz-,
Steuer- und Rechnungswesen
Gunnar Hansen – 4046 –

Auskunfteien/SCHUFA, Internationaler Datenverkehr,
Gewerbliche Dienstleistungen, Tele- und Mediendienste,
Freie Berufe, Bauen und Wohnen
Helga Naujok – 4058 –

Versicherungswirtschaft, Kreditwirtschaft, Handel, Industrie, Vereine
Elisabeth Duhr – 4059 –

Arbeitnehmerdatenschutz/Personalwesen, Adresshandel/ Werbung,
Markt- und Meinungsforschung
Evelyn Seiffert – 4060 –

E-Government, Chipkarten, SAP, technisch-organisatorische Beratung
und Prüfung
Dr. Sebastian Wirth – 4053 –

Betriebssysteme, Netzwerke, Verschlüsselungstechniken, Signatur,
Biometrie, technisch-organisatorische Beratung und Prüfung
Ulrich Kühn – 4054 –

Dokumentenmanagement/Archivierung, Videoüberwachungstechnik,
technisch-organisatorische Beratung und Prüfung
Jutta Nadler – 4055 –

Betriebssysteme, Netzwerke, Standardsoftware,
technisch-organisatorische Beratung und Prüfung,
anlassfreie Unternehmensprüfung
Bernd Uderstadt – 4061 –

Elektronischer Rechtsverkehr, technisch-organisatorische Beratung
und Prüfung
Thomas Morische – 4048 –

Stichwortverzeichnis