19. Tätigkeitsbericht
des
Hamburgischen Datenschutzbeauftragten
zugleich
Tätigkeitsbericht der Aufsichtsbehörde
für den nicht öffentlichen Bereich
2002/2003

vorgelegt im Februar 2004

(Redaktionsschluß: 3. Dezember 2003)
Dr. Hans-Hermann Schrader

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

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 20459 Hamburg · Tel. 4 28 41 20 47 · Fax 4 28 41 23 72
mailbox@datenschutz.hamburg.de

Vertrauliche Informationen sollten uns elektronisch nur verschlüsselt übermittelt werden; wir geben dazu nähere Hinweise.

Auflage: 2.000 Exemplare

Druck: Lütcke & Wulff, 22525 Hamburg

INHALTSVERZEICHNIS

Datenschutz im öffentlichen Bereich

Datenschutz im nicht öffentlichen Bereich

Bürgerservice und die Dienststelle

Vorbemerkung

Nach dem Zwischenbericht über wichtige Themen aus dem Jahr 2002 wird nun wiederum ein ausführlicher Zweijahresbericht – über die Berichtsjahre 2002 und 2003 – vorgelegt.

Wegen der besonderen Bedeutung des E-Government werden diesmal Datenschutzbeiträge zu diesem Themenfeld vorangestellt. Damit wird an unsere Darstellung im 18. Tätigkeitsbericht (18. TB, 3.1) angeknüpft und zugleich auf die Mitteilung des Senats an die Bürgerschaft vom 24. Juni 2003 (Drs. 17/3032) zu „E-Government – Moderne Stadt im Netz“ mit dem 2. E-Government-Aktionsfahrplan eingegangen.

Unser eigener Service für die Bürgerinnen und Bürger mit deren Beratung und der Betreuung der vielfältigen Eingaben, eine Übersicht über die Datenschutzveranstaltungen und unsere Öffentlichkeitsarbeit sowie die Entwicklung der Dienststelle sind am Ende dieses Tätigkeitsberichtes wiedergegeben.

Datenschutzrecht und -technik

1. E-Government

1.1 Allgemeines

Datenschutzanforderungen müssen umfassend berücksichtigt werden, um für E-Government-Angebote die Akzeptanz der Bürgerinnen und Bürger zu gewinnen. Das allgemein festgeschriebene Ziel eines umfassenden Datenschutzes muss dazu in den einzelnen E-Government Verfahren konsequent konkretisiert werden.

1.1.1. Erwartungen und Bedenken

Die Verwaltung will ihre Dienstleistungen für die Bürgerinnen und Bürger sowie für Unternehmen verstärkt über das Internet anbieten. Während bisher die Bereitstellung allgemeiner Informationen im Vordergrund stand, rücken zunehmend die einzelfallbezogene Kommunikation und die Transaktionen in den Mittelpunkt der E-Government-Aktivitäten. Bei der Transaktion werden Verwaltungsaktivitäten unter Einschluss der abschließenden Entscheidung und deren Bekanntgabe für beide Seiten verbindlich und vollständig auf elektronischem Weg abgewickelt. Dazu gehören auch die ggf. erforderlichen Bezahlvorgänge. Der Senat hat die große Bedeutung des E-Government für eine wirtschaftliche und kundenorientierte Verwaltung und die Gestaltung der Stadt betont. (s. insbesondere Mitteilung des Senats an die Bürgerschaft, E-Government - Moderne Stadt im Netz, Bürgerschaftsdrucksache 17/3032).

Die Nutzung des Internets bei der Informationsbeschaffung hat in den letzten Jahren stark zugenommen. Viele Bürgerinnen und Bürger stehen jedoch Online-Transaktionen sehr reserviert gegenüber, insbesondere wenn Bezahlvorgänge eingebunden sind. Dies zeigt die repräsentative Hamburger Bürgerbefragung 2003. Auch international angelegte Studien kommen zu dem Ergebnis, dass gerade in Deutschland große Bedenken gegen die Übertragung personenbezogener Daten im Internet vorherrschen. Gleichzeitig belegen diese Studien jedoch auch, dass die Bürgerinnen und Bürger große Erwartungen an die Ausweitung des E-Government-Angebotes haben. Ein umfassender Datenschutz und Sicherheitsmaßnahmen sind daher wesentliche Erfolgsfaktoren für E-Government-Anwendungen, um den Bedenken der Bürgerinnen und Bürger gegenüber diesen Online-Dienstleistungen der Verwaltung entgegenzuwirken.

1.1.2 Handlungsempfehlungen

Der Hamburgische Datenschutzbeauftragte hat gemeinsam mit den Datenschutzbeauftragten des Bundes und der Länder Handlungsempfehlungen für ein „Datenschutzgerechtes eGovernment“ erarbeitet. Die Broschüre richtet sich einerseits an Entscheidungsträger in der Verwaltung und andererseits an Bürgerinnen und Bürger sowie Wirtschaftsunternehmen, die die neuen Angebote des E-Government nutzen. In der Broschüre werden die spezifischen Anforderungen und Risiken, die mit dem E-Government verbunden sind, ausführlich beschrieben.

Dazu gehört die Zunahme von personenbeziehbaren Daten, die bei der Nutzung von Online-Diensten anfallen oder auch die Möglichkeit, zentrale und bereichsübergreifende Datenbestände anzulegen. Auch die Risiken, die bei der Daten verarbeitenden Stelle und während des Transports der Daten über das Internet bestehen, werden betrachtet. Außerdem kann der Computer des E-Government-Nutzers ein Angriffsziel sein und so zu einer Gefährdung der Vertraulichkeit der personenbezogenen Daten führen.

Einen großen Raum nehmen in der Broschüre konkrete Handlungsempfehlungen und die Beschreibung von technischen und organisatorischen Schutzmaßnahmen ein. Die Grundsätze der Erforderlichkeit sowie der Datenvermeidung und der Datensparsamkeit sind bereits bei der Konzeptions- und Planungsphase von E-Government-Angeboten zu berücksichtigen. In Risikoanalyen sind die spezifischen Gegebenheiten zu betrachten und technische und organisatorische Maßnahmen abzuleiten. IT-Verantwortliche können die aufgelisteten Handlungsempfehlungen als Checkliste nutzen, um Maßnahmen und Vorkehrungen für datenschutzgerechte und sichere E-Government-Anwendungen festzulegen. Für die Nutzerinnen und Nutzer sind insbesondere die vorgestellten Instrumente des Selbstdatenschutzes von großer Bedeutung.

Die Broschüre enthält abschließend viele datenschutzfreundliche Praxislösungen. Diese Beispiele sind auch als Beleg zu sehen, dass datenschutz-

freundliche Lösungen möglich und wirtschaftlich vertretbar sind. Eine von den dort beschriebenen Anwendungen ist das vom Bezirksamt Hamburg-Mitte realisierte Verfahren „Fundinfo“, das die Suche nach verloren gegangenen Gegenständen über das Internet ermöglicht. Da zum Teil sensible Daten bei der Suche in die Bildschirmmasken eingegeben werden können, werden auch bei den Suchanfragen die Daten über eine verschlüsselte SSL-Verbindung übertragen.

Die Handlungsempfehlungen stießen auf unserem Stand bei der 1. Hamburger E-Government-Messe auf großes Interesse. Die Empfehlungen nutzen wir auch für die Begleitung der hamburgischen E-Government-Projekte, von denen einige in den folgenden Abschnitten näher erläutert werden.

Der Hamburgische Datenschutzbeauftragte hat erreicht, dass die datenschutzrechtlichen Anforderungen in der Mitteilung des Senats an die Bürgerschaft „E-Government – Chancen für Hamburg nutzen“ (Bürgerschaftsdrucksache 17/1091) verstärkt berücksichtigt wurden. So wurde darin ausdrücklich aufgeführt, dass bei den E-Government-Anwendungen so wenig Daten wie möglich zu verarbeiten sind. Reine Informationsangebote sind daher grundsätzlich anonym nutzbar zu machen, wie dies bei der Suche in „Fundinfo“ realisiert wurde.

Es ist durch geeignete Maßnahmen dafür Sorge zu tragen, dass Datenbestände aus unterschiedlichen Quellen nicht zweckwidrig zusammengeführt werden können. Ferner konnten wir erreichen, dass der Senat festgeschrieben hat, für E-Government-Anwendungen mit besonders schutzwürdigen Daten weitere Schutzmaßnahmen zu prüfen und ggf. umzusetzen. Diese ergänzenden Maßnahmen dienen ebenfalls dem erklärten Ziel, das E-Government in Hamburg so sicher wie möglich zu machen und dafür zu sorgen, dass das Vertrauen von Bürgern und Wirtschaft gewonnen werden kann.

1.1.3 Vorhaben „Metropolregion Hamburg“

Im Rahmen des Gesamtvorhabens „Metropolregion Hamburg“ wird von Hamburg, Niedersachsen, Schleswig-Holstein und den beteiligten Städten, Kreisen und Gemeinden das Ziel verfolgt, auch die Zusammenarbeit im Bereich E-Government zu verstärken. Mittelfristig soll erreicht werden, dass sich die Verwaltungskunden mit ihren Anliegen an jede Verwaltung in der Metropolregion wenden können. In einer ersten vorgelegten Machbarkeitsstudie wurden dazu Ansätze und Möglichkeiten aufgezeigt. Gleichzeitig werden jedoch auch zahlreiche offene rechtliche und technische Fragestellungen benannt, die für die weiteren Vorhaben zu klären sind.

Die sich aus solchen Vorhaben ergebenden datenschutzrechtliche Risiken müssen in Risikoanalysen noch bewertet werden. Dazu gehört auch das in der Studie benannte Fernziel, gemeinsam genutzte Datenbestände aufbauen zu

wollen. Als Leitlinien sind die datenschutzrechtlichen Anforderungen aus der Broschüre „Datenschutzgerechtes eGovernment“ in die Machbarkeitsstudie übernommen worden. Im Rahmen der weiteren Konzeptionierung gilt es, die rechtliche Zulässigkeit und die Anforderungen an den Datenschutz zu konkretisieren; daraus sind dann technische und organisatorische Schutzmaßnahmen abzuleiten. Für den weiteren Projektverlauf wurde mit der Finanzbehörde vereinbart, dass der Hamburgische Datenschutzbeauftragte frühzeitig in die Planungen eingebunden wird.

1.2 HamburgGateway mit Zugang zur Online-Melderegisterauskunft

Die Anforderungen des Datenschutzes sind bei der Online-Melderegisterauskunft über das Gateway berücksichtigt worden. Bei zukünftigen Anwendungen, in denen besonders sensible Daten verarbeitet werden sollen, sind zusätzliche technische Maßnahmen im Gateway erforderlich.

1.2.1 Einheitlicher Zugang

Das HamburgGateway schafft einen einheitlichen Zugang zu allen E-Government-Angeboten der hamburgischen Verwaltung. Die verfahrensübergreifende Infrastruktur steht den Bürgern bis auf Wartungsfenster rund um die Uhr zur Verfügung und soll künftig für alle Online-Dienstleistungen, bei denen Transaktionen stattfinden, von den unterschiedlichen behördenspezifischen Fachverfahren genutzt werden. Für das HamburgGateway wurden eine Risikoanalyse durchgeführt und umfangreiche Sicherheitsmaßnahmen realisiert.

Im HamburgGateway werden zentrale Dienste wie die Registrierung und Authentisierung der Kunden und die Online-Zahlungsanbindung gewährleistet. Die Kommunikation zwischen Bürger und Gateway erfolgt mit einer SSL-Verschlüsselung. Wenn die Antworten zu einer Anfrage nicht unmittelbar bereit gestellt werden können, wird der Kunde nach der Bereitstellung der Antwort mit einer E-Mail informiert, dass das Ergebnis der Anfrage vorliegt. Die Antwort selber wird jedoch nicht per E-Mail versandt, sondern diese kann sich der Kunde über eine verschlüsselte Verbindung aus dem Gateway abholen.

Das HamburgGateway stellt derzeit zwei unterschiedliche Sicherheitsstufen bereit. Bei der ersten Sicherheitsstufe reicht eine Online-Registratur. Diese Sicherheitsstufe ist erforderlich, um die Antworten kundenspezifisch und sicher zustellen zu können. Bei der zweiten Sicherheitsstufe werden die Kundendaten in einem Kundenzentrum anhand eines vorgelegten Ausweisdokumentes überprüft. Nach der Freischaltung können auch Fachanwendungen mit erhöhten Sicherheitsanforderungen sowie kostenpflichtige Dienstleistungen genutzt werden. Der Nutzer authentisiert sich im Gateway durch die Eingabe der Benutzerkennung und eines mindestens 8-stelligen komplexen Passworts. In

einer nächsten Ausbaustufe des Gateway soll auch die qualifizierte elektronische Signatur im HamburgGateway eingebunden werden können.

Neben Bürgerinnen und Bürgern können sich auch Firmenkunden im Gateway registrieren und freischalten lassen. Auch diese Kunden melden sich mit Benutzerkennung und Passwort an. Die alleinige Passwortprüfung wird den Datenschutzanforderungen in den Fällen jedoch nicht gerecht, in denen Unternehmen auf E-Government-Verfahren zugreifen wollen, bei denen sensible personenbezogene Daten wie z. B. Gesundheitsdaten verarbeitet werden. Es sind zusätzliche technische Maßnahmen – z.B. SSL-Client-Zertifikate – erforderlich, die sicherstellen, dass der Zugriff auch wirklich aus dem jeweiligen Unternehmen heraus erfolgt. Nur in diesem Fall greifen die unternehmensspezifischen Sicherheitsmaßnahmen. Da es häufig vorkommt, dass Beschäftigte Passworte in unzulässiger Weise weiter geben, könnten in diesen Fällen die sensiblen Daten sonst von beliebiger Stelle aus dem Internet abgerufen werden. Für eine datenschutzgerechte Lösung muss hier nachgebessert werden.

Bei den Online-Bezahlverfahren kann per Lastschriftverfahren oder mit einer Kreditkarte bezahlt werden. Anonyme Bezahlverfahren etwa mit einer Prepaid-Karte oder datensparsame Bezahlverfahren über das Handy sind noch nicht mit eingebunden. Zwar wurde unsere Anforderung nach Einbindung solcher datenschutzfreundlichen Lösungen bei der Ausschreibung mit aufgenommen. Der ausgewählte Dienstleister stellt ein solches Bezahlverfahren jedoch nicht zur Verfügung. Hier gilt es die weitere Entwicklung aufmerksam zu beobachten und bei einer stärkeren Verbreitung solcher Bezahlverfahren diese auch im HamburgGateway zur Verfügung zu stellen. Dies kann dazu beitragen, die Bedenken der Bürger gegenüber E-Government-Anwendungen abzubauen.

1.2.2 Online-Melderegisterauskunft

Mit der Online-Melderegisterauskunft steht ein erstes Fachverfahren zur Verfügung, das über das HamburgGateway erreichbar ist. Nach einer einmaligen Registrierung und Freischaltung durch ein Kundenzentrum können einfache Melderegisterauskünfte vollständig über das Internet eingeholt werden. Die rechtlichen Voraussetzungen wurden durch die Novellierung des Hamburgischen Meldegesetzes und der Meldedatenübermittlungsverordnung (MDÜV) geschaffen (vgl. 4.1).

Melderegisterauskünfte werden über das Internet nur erteilt, wenn die Kunden neben dem Vor- und Familiennamen der Einwohner zwei der drei folgenden Angaben zur Identifizierung machen: Geburtsdatum, Geschlecht, eine frühere Anschrift. Die betroffenen Personen können der Melderegisterauskunft an Private über das Internet ohne Angaben von Gründen und kostenfrei widersprechen. Kann wegen des Widerspruchs die beantragte Auskunft über das Inter-

net nicht erteilt werden, so wird der Antrag zur weiteren Bearbeitung im herkömmlichen Verfahren an die Meldebehörde weitergeleitet und die auskunftsersuchende Person elektronisch benachrichtigt.

1.3 HamburgService

Bei der Einführung eines Call-Centers für die hamburgische Verwaltung sind datenschutzrechtliche Vorgaben zu beachten.

Im Laufe des Jahres 2004 soll der HamburgService starten. Hinter diesem Namen verbirgt sich die telefonische Erreichbarkeit der hamburgischen Verwaltung unter einer einzigen zentralen Rufnummer. Der HamburgService ist Teil des vom Senat beschlossenen E-Government-Fahrplans und soll zu einer bürger- und wirtschaftsfreundlichen sowie effizienteren öffentlichen Verwaltung Hamburgs beitragen.

Das Konzept für den HamburgService sieht in seiner ersten Ausbaustufe zunächst vor, alle Aufgaben der bisher sieben bezirklichen Telefonzentralen in einem neuen Call-Center im Bezirksamt Wandsbek zu bündeln. Dabei handelt es sich um

- die Telefonvermittlung von Ansprechpartnern innerhalb der Hamburger Verwaltung,
- die Auskünfte bei allgemeinen Anliegen (z. B. Aufgaben und Zuständigkeiten von Dienststellen, Öffnungszeiten, Telefon- und Faxnummern, Raumnummern oder Verkehrsverbindungen) und über typische „Lebenslagen“ (Umzug, Heirat etc.),
- die Aufnahme und Weiterleitung von Anliegen an die entsprechenden Dienststellen, falls nicht direkt telefonisch mit den zuständigen Sachbearbeitern verbunden werden kann,
- das Zusammenstellen und den Versand von Formularen, Broschüren und Vordrucken,
- die Aufnahme von Beschwerden und ihre Weiterleitung an die für die Bearbeitung zuständigen Stellen,
- bei Bedarf das Verweisen auf das Internetangebot der hamburgischen Verwaltung und den Download von Broschüren und Formularen.

Für die Umsetzung dieses Vorhabens ist ein umfangreiches Informationssystem erforderlich, das den Mitarbeiterinnen und Mitarbeitern im neuen Call-Center die für die Aufgabenerfüllung notwendigen Daten bereitstellt. Dieser künftige gemeinsame Bestand an Organisations- und Kommunikationsdaten soll die Basis nicht nur für den HamburgService, sondern auch für andere Anwendungen der Verwaltung – Verbesserung der Datenpflege für den Bürger-

und Firmenservice (DIBIS), Telefonlisten und Organigramme der Behörden und Ämter (FHHadressBuch) sowie das Hamburg Handbuch – sein. Eine Integration in die an allen Büroarbeitsplätzen verfügbare Struktur des FHHinfoNET ist vorgesehen.

Die weiteren Ausbaustufen sehen eine Ausdehnung auf weitere Behörden und Ämter vor. Die Serviceleistungen sollen erweitert werden, z. B. um Auskünfte zum konkreten Bearbeitungsstand von Verwaltungsverfahren.

Aus unserer Sicht werden hier an zentraler Stelle insbesondere für die Aufnahme und Weiterleitung von persönlichen Anliegen und Beschwerden der Bürgerinnen und Bürger zum Teil sehr sensible personenbezogene Daten erhoben und in einem automatisierten Verfahren gespeichert und weiterverarbeitet. Hierfür ist vor der Entscheidung über die Einführung eine Risikoanalyse gemäß § 8 Abs. 4 Hamburgisches Datenschutzgesetz (HmbDSG) erforderlich, die die konkret zu treffenden technischen und organisatorischen Sicherheitsmaßnahmen enthält.

Die Entgegennahme von Anrufen und die Bearbeitung der Anfragen im zentralen Call-Center für andere Behörden und Ämter ist Datenverarbeitung im Auftrag. Die Bestimmungen des § 3 Abs. 1 und 2 HmbDSG sind einzuhalten. Für den Online-Zugriff auf andere Verwaltungsverfahren wäre zudem eine Rechtsverordnung des Senats gemäß § 11 HmbDSG erforderlich.

Das Sollkonzept mit den konkreten Vorschlägen und Handlungsschritten liegt uns inzwischen vor. Erste grundsätzliche Gespräche zu den datenschutzrelevanten Aspekten des Projekts haben bereits stattgefunden. Wir werden das Vorhaben weiter begleiten.

1.4 DV-Verfahren Integrierte Erfassung und Bearbeitung von Zuwendungen (INEZ)

Die Anforderungen an eine pseudonyme Bearbeitung sind bisher nicht erfüllt. Zum Schutz der besonders sensiblen Daten sind daher zusätzliche technische Maßnahmen zur sicheren Authentifizierung erforderlich.

Das automatisierte Verfahren INEZ wird bereits seit Anfang 2000 in der Behörde für Soziales und Familie (BSF) genutzt, um die Zuwendungsbearbeitung zu unterstützen (vgl. 18.TB, 3.1.4). Die Zuwendungsempfänger – das sind meistens privatrechtlich organisierte Freie Träger – haben die für das Zuwendungs-Controlling erforderlichen Informationen regelmäßig zu aktualisieren. Um Medienbrüche und Doppelarbeit bei der Aktualisierung zu vermeiden, wird einer geschlossenen Benutzergruppe ein lesender und schreibender Zugriff auf INEZ-Daten über das Internet ermöglicht. Diese Anwendung heißt „Web-INEZ“ und läuft in der Pilotierung seit dem Sommer 2001 für einen eingeschränkten Nutzerkreis.

Für die einzelnen Zuwendungsvorhaben werden eine Vielzahl von Daten über Personen verarbeitet, die von dem jeweiligen Zuwendungsempfänger betreut werden, darunter auch Sozial- und Gesundheitsdaten. Bereits im September 2001 haben wir uns mit der BSF darauf verständigt, dass zum Schutz der übertragenen Daten neben einer starken Verschlüsselung auch eine sichere Authentifizierung der externen Nutzerinnen und Nutzer erfolgen muss. Es war Konsens, dass die alleinige Angabe eines Passwortes nicht ausreicht. Die Ankündigung eines sicheren Verfahrens hat die BSF jedoch weder umgesetzt noch in die Planung eingebracht, die für die Einbindung von INEZ in das HamburgGateway (vgl. 1.2) erforderlich wurde.

In der Überarbeitung der Risikoanalyse hat die BSF die im Internet übertragenen Daten trotz gegenteiliger Ankündigung erneut als anonymisierte Einzeldatensätze eingestuft. Zwar konnten wir erreichen, dass die Felder Name und Anschrift nicht mehr über das Internet übertragen werden. Eine anonyme oder pseudonyme Nutzung der Daten geht damit jedoch nicht einher. Zum einen wird eine eindeutige Personennummer verwendet, die einer Person zugeordnet werden kann. Zur Bildung und Nutzung dieser Nummer gibt es auch keine einheitlichen Vorgaben durch die Behörde, die sicherstellen, dass die Zuordnung zwischen Personennummer und Person nur den jeweiligen Sachbearbeitern des Zuwendungsempfängers bekannt ist.

Wie wir bei einzelnen Zuwendungsempfängern vor Ort feststellen konnten, wird diese Nummer zum Teil auch auf Listen und Schreiben von Zuwendungsempfängern genutzt, die dem betreuten Personenkreis zugänglich sind. Die Daten sind damit ohne großen Aufwand einer bestimmten oder bestimmbaren Person zuzurechnen. Zum anderen ermöglicht auch die von der BSF geforderte Übertragung des vollständigen Geburtsdatums bei Projekten, die im Rahmen des Europäischen Sozialfonds gefördert werden, eine einfache Zuordnung zu einer bestimmbaren Person. Die Anforderungen des § 4 Abs. 9 bzw. 10 Hamburgisches Datenschutzgesetz sind daher bisher nicht erfüllt. Die BSF hat angekündigt, einheitliche Vorgaben für die Gestaltung und Nutzung der Personennummer bei den Zuwendungsempfängern zu machen und zu prüfen, ob die Übertragung des Geburtsdatums in Web-INEZ entfallen kann.

Wir werden uns weiter dafür einsetzen, dass die Verarbeitung von Daten in INEZ nach Möglichkeit pseudonym erfolgt oder andernfalls ein sicheres Authentifizierungsverfahren realisiert wird.

2. Neues Datenschutzrecht

2.1 Europa- und Bundesrecht

2.1.1 Europäische Verfassung

Das Grundrecht auf Datenschutz ist aus der Grundrechte-Charta der Europäischen Union fast wortgleich in den Entwurf einer Europäischen Verfassung übernommen worden.

In Art. 8 der Grundrechte-Charta der Europäischen Union, die der Europäische Rat am 7. Dezember 2000 proklamiert hatte (18. TB, 2.1.1), war das Grundrecht auf Datenschutz bereits erfreulich deutlich gefasst worden. Der Konvent, der den Entwurf der Europäischen Verfassung vorbereitete, hat diesen Text fast wörtlich übernommen. Zur Betonung der Grundrechte als Menschenrechte hatte er dabei die Worte „Jede Person hat das Recht ...“ durch die Worte „Jeder Mensch hat das Recht ...“ ersetzt. Der volle Wortlaut dieses Art. II-8 ist auf der Rückseite des Tätigkeitsberichtes wiedergegeben.

Für die Stellung der Datenschutzbeauftragten ist es wichtig, dass dabei auch Art. 8 Abs. 3 der Grundrechte-Charta unverändert übernommen wurde. Danach wird die Einhaltung der Grundrechtsbestimmungen „von einer unabhängigen Stelle überwacht.“ Wenn die Europäische Verfassung nach der Beratung durch die Regierungskonferenz in dieser Form beschlossen wird, werden die Datenschutzbeauftragten gemeinschaftsrechtlich zu Verfassungsorganen. Dies wird im Sinne einer gemeinschaftsrechtskonformen Auslegung und Anwendung des Landesrechts zu berücksichtigen sein.

2.1.2 Bundesdatenschutzgesetz

Die Tätigkeit im nicht öffentlichen Bereich war dadurch geprägt, für eine wirksame Umsetzung des Bundesdatenschutzgesetzes zu sorgen.

Nach der Anpassung des Bundesdatenschutzgesetzes gemäß der EG-Datenschutzrichtlinie (18. TB, 2.1.2) ging es vor allem um die Umsetzung des an vielen Stellen novellierten Gesetzes in den Unternehmen. Dazu haben die Mitarbeiterinnen der Aufsichtsbehörde mit ausführlichen Erläuterungen des Ersten Abschnitts des Bundesdatenschutzgesetzes in der sog. Hamburger Kommentierung zum BDSG (DuD 2002, Heft 1) sowie mit den Erläuterungen für die weiteren Abschnitte des BDSG zum Datenschutz im nicht öffentlichen Bereich (DuD 2003, Heft 1) beigetragen.

2.2 Hamburgische Datenschutzvorschriften

2.2.1 Hamburgisches Datenschutzgesetz

Die Regelung zur Schriftform für digitale Dokumente in § 4 a des Gesetzes ist entfallen.

Mit dem Gesetz zur Anpassung verwaltungsrechtlicher Vorschriften an den elektronischen Rechtsverkehr vom 18. November 2003 wurde ein neuer § 3 a (Elektronische Kommunikation) in das Hamburgische Verwaltungsverfahrensgesetz (HmbVwVfG) eingefügt. Dadurch wurde die besondere Vorschrift für den Bereich des Datenschutzes in § 4 a Hamburgisches Datenschutzgesetz entbehrlich, ohne dass mit der Aufhebung dieser Vorschrift eine materielle Änderung verbunden ist.

Aus unserer Sicht ist es allerdings wichtig, dass nunmehr möglichst bald die in § 3 a Abs. 4 HmbVwVfG vorgesehene Rechtsverordnung nach Abstimmung mit uns erlassen wird. Erst durch diese Verordnung wird festgelegt werden, durch welche „andere als mit einer qualifizierten elektronischen Signatur versehene elektronische Dokumente“ das nach hamburgischem Recht bestehende Schriftformerfordernis gewahrt werden kann. Außerdem sollen in der Verordnung die notwendigen technischen Einzelheiten geregelt werden. Ob und inwieweit diese Änderung in der Praxis in größerem Umfang für den elektronischen Rechtsverkehr genutzt werden wird, ist offen.

2.2.2 Bereichsspezifische Datenschutzvorschriften

Bei den neuen Rechtsvorschriften sind unsere Vorschläge vielfach aufgegriffen worden.

Das Hamburgische Verfassungsschutzgesetz (HmbVerfSchG), das Hamburgische Sicherheitsüberprüfungsgesetz (HmbSÜG) und das Gesetz zur Ausführung des Artikel 10-Gesetzes sind am 4./17. Dezember 2002 in erheblichem Umfang novelliert worden. Kernpunkte sind insbesondere die Regelung von Auskunftsbefugnissen des Verfassungsschutzes entsprechend dem Terrorismusbekämpfungsgesetz des Bundes (vgl. 18. TB, 17.1) sowie der verdeckte Einsatz besonderer technischer Mittel in Wohnungen. Nach lebhafter öffentlicher Diskussion konnte erreicht werden, dass die Schwelle für heimliche wohnungstechnische Eingriffe des Verfassungsschutzes gegenüber nicht verdächtigen Personen deutlich angehoben und der besondere Schutz von Berufsgeheimnisträgern mit Zeugnisverweigerungsrecht gesetzlich abgesichert wurde.

Durch Änderungen des Melderechts wurde die Befugnis zu automatisierten Abrufen von Daten aus dem Melderegister erheblich erweitert (vgl. 1.2 und 4.).

Das Hamburgische Schulgesetz vom 16. April 1997 wurde am 27. Juni 2003 geändert und ist zum Schuljahresbeginn 2003/2004 in Kraft getreten. Wir haben eindeutige Formulierungen und mehr Normenklarheit bei den Informationsrechten von früheren Erziehungsberechtigten volljähriger Schülerinnen und Schüler, bei den Vorschriften zur Besetzung von Schulleitungsstellen und bei der Datenverarbeitung zu Zwecken der Evaluation erreichen können. Der Schwerpunkt unserer Bemühungen richtete sich darauf, den volljährigen Schülerinnen und Schülern ein Widerspruchsrecht einzuräumen, bevor deren Eltern von der Schule über verhängte Ordnungsmaßnahmen unterrichtet werden. Die Betroffenen müssen nun vor einer Unterrichtung der Eltern durch die Schule in geeigneter Form auf das Widerspruchsrecht hingewiesen werden.

In das Hamburgische Pressegesetz (Änderungsgesetz vom 28. Januar 2003) wurde mit § 11 a eine Regelung zum Redaktionsdatenschutz aufgenommen (vgl. unten 3.12).

Der Entwurf für ein neues übergreifendes „Kammergesetz für Heilberufe“, das sieben Hamburger Gesetze ersetzen soll, enthält nun das Gebot, Patientendaten vor einer Weitergabe an die Aufsichtsbehörde grundsätzlich zu anonymisieren.

Der Entwurf zur Änderung des Krebsregistergesetzes vom 27. Juni 1984, der die Kommunikation mit anderen Krebsregistern und mit dem Melderegister erleichtern soll, wurde von Beginn an mit uns abgestimmt.

Bei der am 7. Oktober 2003 beschlossenen „Verordnung über die Einrichtung eines automatisierten Verfahrens zum Abruf personenbezogener Daten über Ausländerinnen und Ausländer mit nicht nachgewiesenen Altersangaben“ konnten wir nur durchsetzen, dass nicht auch das Institut für Rechtsmedizin Zugriff auf die zentrale Datenbank erhält. Bei den Zugriffsregelungen im übrigen blieb unsere Kritik erfolglos (vgl. unten 12.1).

3. Informations- und Kommunikationstechnik/Medien

3.1 Verschlüsselungsmöglichkeiten unter Windows 2000

Auch drei Jahre nach der Aufnahme des Produktivbetriebs unter Windows 2000 wird die Komponente zur Verschlüsselung des internen Verwaltungsnetzes nicht genutzt. Wir konnten jedoch erreichen, dass eine nähere Untersuchung von technischen Maßnahmen zur Sicherstellung der Vertraulichkeit im Netz durchgeführt werden soll.

Die IuK-Infrastruktur der hamburgischen Verwaltung wird flächendeckend auf das Betriebssystem Windows 2000 bzw. Windows 2003 umgestellt. Insbesondere mit dem zentralen Verzeichnisdienst Active Directory sind auch zusätzliche

Sicherheitsrisiken verbunden (vgl. 18. TB, 3.2.2). Es werden mittlerweile über 11.000 aktive Benutzerkonten der Behörden im Active Directory verwaltet.

Das Landesamt für Informationstechnik (LIT) hat für die Nutzung des Active Directory ein Sicherheitskonzept erstellt. Konzeptionelle Festlegungen wurden u.a. detailliert im Betriebskonzept, dem Berechtigungskonzept für die Administratoren und in der Securityüberwachung beschrieben. Danach werden die Aktivitäten der Organisations-Administratoren im LIT differenziert protokolliert. Das LIT plant, ein Audit-System für alle Windows 2000 Server im LIT einzuführen, mit dem die Überwachung der Server unter sicherheitsrelevanten Gesichtspunkten verbessert werden soll. Auch die Protokollierung bei der Berechtigungsvergabe soll umgesetzt werden. Aufgetretene Schwierigkeiten bei der Überwachung der Server belegen, dass eine technikunterstützte Auswertung dringend erforderlich ist. Wir werden uns dafür einsetzen, dass die Realisierung wie geplant im Jahr 2004 erfolgt und sich nicht weiter verzögert.

Wir haben bereits in der Broschüre „Datenschutz bei Windows 2000“ u. a. darauf hingewiesen, dass mit diesem Betriebssystem die Netzwerksicherheitsarchitektur „IPSec“ zur Verfügung steht, mit der die Vertraulichkeit, Authentizität und Integrität bei der Datenübertragung sichergestellt werden kann. Der Einsatz von IPSec gewährleistet den Schutz sowohl vor externen als auch vor internen Angriffen auf das Verwaltungsnetz. Es besteht bei unverschlüsselter Datenübertragung die Gefahr, dass unberechtigte Personen Sicherheitslücken ausnutzen und den Datenverkehr durch den Einsatz sogenannter Sniffer abhören. Dabei haben nicht zuletzt die Sicherheitsvorfälle im Berichtszeitraum aufgezeigt, dass auch das verwaltungsinterne Netz nicht sicher vor Angriffen ist.

Auch Behörden sehen sehr wohl die Erforderlichkeit, besonders sensible Daten wie z. B. Gesundheitsdaten bei der Übertragung im internen Netz zu verschlüsseln. Erste Ansätze zur Nutzung von IPSec haben jedoch gezeigt, dass für eine praxisgerechte Konfiguration Domänen-Administrationsrechte erforderlich sind, so dass eine systematische Untersuchung der Einsatzbedingungen nur in Zusammenarbeit mit dem LIT vorgenommen werden kann. Die vom LIT geplante systematische Untersuchung der Einsatzmöglichkeiten von IPSec für die hamburgische Verwaltung wurde jedoch im Berichtszeitraum entgegen einer Ankündigung nicht vorgenommen.

Ohne eine vertiefte Prüfung hat das LIT statt dessen entschieden, von einer Ausweitung des IPSec-Einsatzes abzusehen. Bei dieser Entscheidung wurde auf Erfahrungen verwiesen, die beim Einsatz von IPSec bei der Steuerverwaltung gemacht wurden. Im Bereich der Steuerverwaltung wird jedoch IPSec nur für die Router-zu-Router-Verschlüsselung genutzt. Die von uns vorgeschlagene Ende-zu-Ende-Verschlüsselung, die IPSec auch ermöglicht, ohne dass zusätzliche Investitionen für IPSec-fähige Router erforderlich sind, wurde damit gerade nicht näher betrachtet.

Auf unseren Vorschlag hat der Rechtsausschuss am 27. November 2003 einstimmig der Bürgerschaft empfohlen, folgendes Ersuchen zu beschließen:

> Die Bürgerschaft ersucht den Senat, über die nähere Untersuchung – einschließlich der Kosten-Nutzen-Relation – technischer Maßnahmen zum Schutz der Vertraulichkeit bei der Datenübertragung innerhalb des verwaltungsinternen Netzes, wie z. B. IPSec, zu berichten und ggf. gemäß dem Ergebnis der Untersuchung geeignete technische Maßnahmen für Anwendungen mit hohem Schutzbedarf bereitzustellen.

3.2 Sichere Passworte

Die Passwortrichtlinie wurde aktualisiert. Weitere IT-Richtlinien müssen dringend den aktuellen Datenschutzanforderungen angepasst werden, damit sie den IT-Verantwortlichen und behördlichen DV-Revisoren als Grundlage dienen können.

Die Abfrage eines Passwortes ist eine sehr weit verbreitete Methode, um einen Zugangsschutz zu IT-Systemen zu gewährleisten. Ein Rechnersystem kann jedoch mittels eines Passworts vor unbefugtem Zugriff nur dann ausreichend geschützt werden, wenn es einem Angreifer nicht gelingt, die Zeichenkombination mit Rechnerhilfe bereits in kurzer Zeit zu ermitteln. Da sich die Leistungsfähigkeit handelsüblicher Computer ständig erhöht, müssen die Mindestanforderungen an Passworte dem technischen Stand angepasst werden.

Der Hamburgische Datenschutzbeauftragte hat bereits im Jahr 2000 in einer Untersuchung gezeigt, dass ein ausreichender Schutz nur mit komplexen Passworten aus mindestens 8 Zeichen zu erzielen ist. Sichere Passworte müssen darüber hinaus Sonderzeichen, Ziffern sowie Groß- und Kleinbuchstaben enthalten. Dabei sollte auf eine gute Mischung des Zeichenvorrates geachtet werden. Wenn Passworte bekannte Worte enthalten, an die z. B. nur eine Ziffer oder ein Sonderzeichen angehängt ist, können diese auch innerhalb von sehr kurzer Zeit ermittelt werden.

Die Finanzbehörde hat die Ergebnisse jetzt aufgegriffen und die Passwortrichtlinie zum 1. Oktober 2003 angepasst. Damit gelten diese Mindestanforderungen einheitlich für die hamburgische Verwaltung. Auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat unsere Untersuchung zum Anlass genommen, den entsprechenden Abschnitt im IT-Grundschutzhandbuch zu überarbeiten. Eine Veröffentlichung soll in Kürze erfolgen.

Hinsichtlich weiterer IT-Richtlinien, die die Finanzbehörde zur Gewährleistung datenschutzrechtlicher Anforderungen erlassen hat, besteht dringender Handlungsbedarf. Diese Richtlinien stammen überwiegend aus der ersten Hälfte

der neunziger Jahre und spiegeln den damaligen Stand wider. Der technische Fortschritt gerade im IT-Bereich ist so groß, dass seit dieser Zeit mehrere Technikgenerationen vergangen sind. Damit sind neue Gefährdungen und technische Ansätze zur Beherrschung dieser Gefahren hinzugekommen. Dies hat zu Folge, dass durch die Einhaltung der gültigen IT-Richtlinien zum Teil auch Grundschutzanforderungen nicht mehr erfüllt werden. Dazu gehören die folgenden Beispiele:

- PC-Richtlinie

  In die PC-Richtlinie sollte die Umgehensweise mit mobilen Rechnern wie Laptop und Handhelds zusätzlich aufgenommen werden, da diese Geräte auch zunehmend in der hamburgischen Verwaltung genutzt werden. Wir haben zum Einsatz solcher Geräte eine Handreichung in unserem Internetangebot veröffentlicht.

- Freigaberichtlinie

  Die derzeitige Freigaberichtlinie stellt stark auf Verfahren ab, die auf getrennten Rechnern ablaufen. Die Richtlinie sollte das Zusammenspiel unterschiedlicher Rechnerebenen und die zum Teil enge Verbindung von Betriebssystemen mit Modulen, bei denen in großem Umfang spezifische Einstellungen für den Einsatz in der hamburgischen Verwaltung vorgenommen werden, berücksichtigen.

Die Finanzbehörde hat angekündigt, eine Aktualisierung der IT-Richtlinien vorzunehmen, und dazu eine Prioritätenliste mit Zeitplanung erstellt. Die fortgeschriebenen Richtlinien mit höchster Priorität sollen danach in der ersten Jahreshälfte 2004 veröffentlicht werden.

Wir werden bei der Aktualisierung und bei unseren datenschutzrechtlichen Prüfungen die angegebenen Kriterien zu Grunde legen, um die technischen und organisatorischen Maßnahmen zu beurteilen.

3.3 Dokumentenverwaltung

Zur Gewährleistung des Schutzes personenbezogener Daten sollte die Ausgestaltung der elektronischen Dokumentenverwaltung hamburgweit nach verbindlichen, einheitlichen Vorgaben erfolgen.

Die im Landesamt für Informationstechnik aufgebaute Infrastruktur zur digitalen Aktenführung wird in zunehmendem Maße von den Behörden und Ämtern genutzt. Die Einrichtung und Ausgestaltung der elektronischen Dokumentenverwaltung und Aktenplanverwaltung erfolgt hierbei nach den jeweiligen rechtlichen und organisatorischen Vorgaben der anwendenden Stellen. Ein einheitliches und verbindliches Verfahren, welches die datenschutzrechtlichen Grundsätze berücksichtigt, wurde den Behörden bisher nicht vorgegeben. Dieser Sachstand ist angesichts des fortschreitenden Einsatzes der elektronischen Dokumentenverwaltung datenschutzrechtlich unbefriedigend.

Im 18. TB (3.4) hatten wir bereits verschiedene Problemfelder in Bezug auf die heute in Papierakten und künftig in elektronischen Akten enthaltenen personenbezogenen Daten aufgezeigt. Um die Erfüllung der datenschutzrechtlichen Anforderungen bei der Einrichtung und Ausgestaltung des Verfahrens und auch im täglichen Umgang mit der Automation zu gewährleisten, halten wir die Erstellung verbindlicher, einheitlicher Vorgaben für die Behörden und Ämter für dringend erforderlich.

Im Unterausschuss Datenschutz der Bürgerschaft vom 23. Oktober 2003 kündigte die Finanzbehörde die Erarbeitung entsprechender Regelungen im Rahmen eines behördenübergreifenden Projektes – unter Beteiligung des Hamburgischen Datenschutzbeauftragten – an. Angesichts des dargestellten Ziels, bis September 2005 in allen Behörden ein funktionsfähiges, einheitliches Aktenführungssystem einzusetzen, ist der zeitliche Rahmen vorgegeben. Wir werden uns weiter für eine datenschutzgerechte Gestaltung des Verfahrens einsetzen.

3.4 FHHinfoNET

Obwohl seit Ende Oktober 2002 die „Erweiterte Sicherheit" für die Postfächer im FHHinfoNET zur Verfügung steht, ist mit der flächendeckenden Einrichtung an den PC-Arbeitsplätzen der Verwaltung noch immer nicht begonnen worden.

Das vom Landesamt für Informationstechnik (LIT) betriebene Mailing-System der hamburgischen Verwaltung (FHHinfoNET), insbesondere die Verschlüsselung elektronisch versandter Nachrichten mit sensiblen personenbezogenen Inhalten, ist in den letzten Jahren immer Thema in unseren Tätigkeitsberichten gewesen (siehe 18. TB, 3.2.1). Obwohl wir uns mit der Finanzbehörde und dem LIT bereits darauf verständigt hatten, dass der flächendeckende Einsatz der sogenannten „Erweiterten Sicherheit" ab April 2002 beginnen sollte, ist dies bis heute immer wieder hinausgezögert worden.

Das LIT betreibt seit Ende Oktober 2002 erfolgreich eine funktionierende Infrastruktur zur Verschlüsselung und Signatur von Nachrichten im FHHinfoNET. Trotzdem ist die Nutzung dieser Technik bislang nur für einen sehr geringen Anteil der PC-Arbeitsplätze in den Behörden und Ämtern eingerichtet worden. Vor allem in den Bereichen, die sensible personenbezogene Daten verarbeiten, besteht kaum die Möglichkeit, diese im Rahmen der jeweiligen Aufgabenerfüllung verschlüsselt per E-Mail übermitteln zu können.

Auf unseren Vorschlag hat der Rechtsausschuss am 27. November 2003 nunmehr einstimmig der Bürgerschaft empfohlen, folgendes Ersuchen zu beschließen :

> Die Bürgerschaft ersucht den Senat, zur Gewährleistung der Vertraulichkeit der personenbezogenen Daten, die per E-Mail innerhalb der hamburgischen Verwaltung übertragen werden, die im FHHinfoNET bereits verfügbare „Erweiterte Sicherheit" umgehend an allen Bildschirmarbeitsplätzen einzuführen, insbesondere in Bereichen, in denen Personal-, Sozial- und Gesundheitsdaten verarbeitet werden.

Wir erhoffen uns hiervon eine deutliche Unterstützung für die bereits mehrfach angekündigte Verbreitung der Verschlüsselung und Signatur elektronischer Nachrichten in der Verwaltung.

3.5 Einsatz von Personal Digital Assistants (PDA)

Die zunehmende Verbreitung und Nutzung von PDA auch in der hamburgischen Verwaltung haben wir zum Anlass genommen, auf die damit verbundenen Risiken für gespeicherte personenbezogene Daten aufmerksam zu machen.

Im Berichtszeitraum erhielten wir zahlreiche Anfragen zu den Risiken der Nutzung mobiler Datenverarbeitungsgeräte, insbesondere zum Abgleich von elektronischen Terminkalendern und E-Mail zwischen privaten PDA und dienstlichen PC am Arbeitsplatz. Wir haben die datenschutzrechtlichen Aspekte hierzu aufbereitet und Empfehlungen gegeben, die auch weiterhin über unser Internetangebot allgemeine Verbreitung finden.

Hinsichtlich der Zulässigkeit des Einsatzes von PDA in den Behörden und Ämtern sind darüber hinaus die hierzu einschlägigen Richtlinien zu beachten. Nach der seit Ende November 2003 geltenden Fassung der Richtlinie zur Gestaltung der IuK-Architektur in der hamburgischen Verwaltung (IUK-A-RL) sind PDA wie lokale Büroarbeitsplätze zu behandeln. Der Betrieb unterliegt den für PC geltenden Vorschriften.

Hierzu zählt insbesondere Abschnitt 4 Abs. 3 der Richtlinie über die Sicherheit der Datenverarbeitung auf Arbeitsplatzrechnern in der hamburgischen Verwaltung (PC-RL). Danach ist die Verarbeitung dienstlicher Daten auf privat beschafften PC grundsätzlich unzulässig. Dieses Gebot gilt aber nicht, soweit für die Erledigung dienstlicher Aufgaben keine besonders schutzwürdigen Daten mit Software zur Textverarbeitung, Tabellenkalkulation oder Geschäftsgrafik verarbeitet werden.

Diese Ausnahme ist von der Finanzbehörde jetzt über die IUK-A-RL erweitert worden um „Outlook-Daten“. Gemeint sind alle mit der Standardsoftware Microsoft Outlook verarbeiteten Informationen wie Postein- bzw. -ausgänge, Kalendereintragungen und Adressen. Sensible Daten dürfen darüber hinaus nur verschlüsselt auf einem passwortgesicherten PDA gespeichert werden.

Jeder Nutzer eines PDA ist selbst verantwortlich für die Einhaltung des Datenschutzes und ist verpflichtet, seine IuK-Stelle über die Inbetriebnahme des Gerätes zu unterrichten. Eine schriftliche Genehmigung gemäß Abschnitt 4 Abs. 4 PC-RL ist damit leider nicht mehr erforderlich.

Die Finanzbehörde geht davon aus, dass eine sensible E-Mail entsprechend den geltenden Vorschriften nur verschlüsselt übersandt wird und auf dem PDA nach Synchronisation mit dem PC deshalb nicht gelesen werden kann. Wie unter 3.4 beschrieben, verfügt bislang aber kaum ein Büroarbeitsplatz im

FHHinfoNET über die Möglichkeit, Nachrichten verschlüsselt zu übermitteln. Auch eine von außen über das Internet in den Postfächern der Verwaltung eingehende E-Mail wird von den Absendern nur selten verschlüsselt.

Dies führt zwangsläufig dazu, dass sensible personenbezogene Daten auf PDA unverschlüsselt gespeichert werden. Denn ob Nachrichten oder Terminplanungen lesbare sensible personenbezogene Daten beinhalten oder nicht, stellt der Benutzer des PDA in der Regel erst nach der Synchronisation mit dem PC fest. Wir halten es daher weiterhin für erforderlich, auf allen für die oben genannten Zwecke in der hamburgischen Verwaltung genutzten PDA grundsätzlich eine Verschlüsselungskomponente zu installieren. Diese steht für aus dem Rahmenvertrag beschaffte Geräte auch zur Verfügung.

Ein zusätzliches Problem besteht in der Kombination von PDA und Mobilfunktechnologie in einem einzigen Gerät. Die damit einhergehende Möglichkeit des Zugriffs auf Informationsdienste im Internet erhöht beim Anschluss an stationäre Endgeräte die Risiken für die hierauf gespeicherten personenbezogenen Daten erheblich. Denn auch PDA können ladbare Programme ausführen und sind deshalb wie alle Computer anfällig gegen Schadensoftware, insbesondere trojanische Pferde.

Aus unserer Sicht ist die Verbindung eines solchen mobilen Rechners mit einem PC in den Behörden und Ämtern nicht zulässig. In der Rahmenvereinbarung mit dem Landesamt für Informationstechnik (LIT) über die Bereitstellung von Infrastrukturanschlüssen (§ 3, Ziffer 3.2.1) haben sich alle Dienststellen schriftlich verpflichtet sicher zu stellen, dass an den Endgeräten keine zusätzlichen Netzöffnungen vorgenommen werden. Die Gesamtsicherheit des Netzes der hamburgischen Verwaltung würde dadurch in Frage gestellt. Die bislang vor allem vom LIT zentral getroffenen aufwändigen Schutzvorkehrungen greifen dann nicht mehr. Hier müssen im Rahmen der Fortschreibung der PC-RL, die nach den Ankündigungen der Finanzbehörde im April 2004 abgeschlossen sein soll, zusätzliche verbindliche Vorgaben erfolgen.

Da PDA wie PC zu behandeln sind, ist im übrigen die Installation eines Virenschutzprogramms auch auf diesen Geräten nach der geltenden PC-RL zwingend vorgeschrieben.

3.6 Internet am Arbeitsplatz

Durch eine zentrale Bereitstellung von Terminal-Server-Diensten können wirksame Maßnahmen zum Schutz von Arbeitsplätzen der hamburgischen Verwaltung vor Gefahren aus dem Internet getroffen werden.

Im 18. TB, 3.3.1 hatten wir darüber berichtet, dass durch die Verlagerung der Internet-Nutzung auf besondere Rechner im Rahmen von Terminal-Server-Diensten ein wirksamer Schutz vor möglichen Risiken für die PC-Arbeitsplätze

der Verwaltung realisiert werden kann. Auf unseren Vorschlag hat die Bürgerschaft am 9./10. April 2003 folgendes Ersuchen beschlossen:

> Die Bürgerschaft ersucht den Senat, für Anwendungen der Verwaltung mit hohem Schutzbedarf – insbesondere der Verarbeitung von personenbezogenen Daten, die einem Berufs- oder Amtsgeheimnis unterliegen – bei der Nutzung des Internet zusätzliche Sicherheitsvorkehrungen zu treffen und die – auch finanziellen – Möglichkeiten einer zentralen Bereitstellung von Terminal-Server-Diensten durch das Landesamt für Informationstechnik für die Arbeitsplätze der Behörden zu klären.

Eine Antwort des Senats wurde inzwischen zusammen mit der Stellungnahme zu diesem Tätigkeitsbericht zugesagt. Das Landesamt für Informationstechnik hat die erforderliche Infrastruktur bereits erfolgreich im Betrieb und mit mehreren hundert Anwendern getestet. Aus technischer Sicht besteht für alle Behörden und Ämter die Möglichkeit, dieses Dienstleistungsangebot zu nutzen.

3.7 Dataport

Die Behörden und Ämter der hamburgischen Verwaltung erhalten ab Januar 2004 einen neuen Dienstleistungspartner. Zukünftig werden wichtige Bereiche wie der Betrieb des zentralen Rechenzentrums und des stadtweiten Daten- und Telekommunikationsnetzes von einer neuen Einrichtung übernommen: Dataport.

Das Landesamt für Informationstechnik (LIT), die Zentralstelle Informations- und Kommunikationswesen der Bezirksverwaltung im Senatsamt für Bezirksangelegenheiten (SfB-IuK) und die Datenzentrale Schleswig-Holstein (DZ-SH) werden ab 1. Januar 2004 zu einer rechtsfähigen Anstalt öffentlichen Rechts mit Sitz in Altenholz bei Kiel fusionieren. Die neue Einrichtung wird unter dem Namen Dataport gemeinsames Dienstleistungsunternehmen für die Verwaltungen beider Länder. Sie soll ihren Kunden eine bürger- und wirtschaftsfreundliche sowie effiziente elektronische Aufgabenerledigung durch Informations- und Kommunikationstechniken (IuK) ermöglichen.

Der Staatsvertrag zwischen dem Land Schleswig-Holstein und der Freien und Hansestadt Hamburg über die Errichtung von Dataport wurde am 27. August 2003 unterzeichnet. Nach bereits erfolgter Beratung im Haushaltsausschuss stehen noch die Zustimmung der Bürgerschaft in Gesetzesform und die anschließende Ratifizierung aus. Daneben ist noch eine Satzung zur Regelung der inneren Angelegenheiten erforderlich.

Schon im Juli 1999 hatten Hamburg und Schleswig-Holstein in einem Verwaltungsabkommen eine enge Kooperation zwischen LIT und DZ-SH beschlos-

sen. Auf dieser Basis werden zur Zeit die Großrechneranwendungen beider Länder nur noch in Hamburg betrieben, Druckausgaben einschließlich Papiernachbearbeitung und Versand erfolgen ausschließlich in der DZ-SH. Die Datenschutzbeauftragten von Hamburg und Schleswig-Holstein haben deshalb im Oktober 1999 selbst eine Vereinbarung getroffen, durch die gewährleistet wird, dass auch die Datenschutzkontrolle im Rahmen der länderübergreifenden Zusammenarbeit des LIT und der DZ-SH weiterhin effektiv ausgeübt wird (17. TB, 3.5).

Die jetzt anstehende Fusion geht weit über die bisherige Kooperation der beiden Rechenzentren hinaus. Die DZ-SH stellt den Behörden des Landes Schleswig-Holstein und den schleswig-holsteinischen Kommunen bislang schon ein umfassendes Angebot von Hard- und Software sowie von Dienstleistungen auf dem Gebiet der IuK zur Verfügung. Das LIT ist Dienstleistungspartner für alle Verwaltungsbereiche der Freien und Hansestadt Hamburg und unterhält die Geschäftsfelder Rechenzentrumsbetrieb, Netzbetrieb, Telekommunikation, Projekte, PC Service-Center, Schulungszentrum, Betrieb Hamburgweiter Dienste, Beratung und Entwicklung. SfB-IuK ist Auftragnehmerin für Entwicklung und Betreuung der bezirklichen IuK-Verfahren, für Benutzerservice sowie Schulung.

Die den derzeit drei Einrichtungen von den jeweiligen Landesverwaltungen zugewiesenen Aufgaben auf dem Gebiet der IuK werden in vollem Umfang mit dem Ziel der Bündelung der IuK-Dienstleistungen auf Dataport übertragen und niederlassungsübergreifend organisiert. Zusammen wird das neue gemeinsame Unternehmen 1.180 Mitarbeiterinnen und Mitarbeiter beschäftigen.

Für Dataport gilt grundsätzlich das Recht des Sitzlandes Schleswig-Holstein. Dies gilt so auch für die Anwendung des Datenschutzrechts. In § 15 des Staatsvertrags wurden aber unter Beteiligung des Landesbeauftragten für den Datenschutz Schleswig-Holstein und uns abweichende Regelungen getroffen.

Staatsvertrag über die Errichtung von Dataport

§ 15

Datenschutz, Sicherheitsüberprüfungen

(1) Für die Verarbeitung personenbezogener Daten durch Dataport und ihre Niederlassungen gelten die Vorschriften des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG) mit Ausnahme des § 3 Absatz 2. Die Anstalt bestellt eine behördliche Datenschutzbeauftragte oder einen behördlichen Datenschutzbeauftragten nach § 10 LDSG.

(2) Verarbeitet die Anstalt oder eine ihrer Niederlassungen personenbezogene Daten für hamburgische öffentliche Stellen oder in deren Auftrag, gelten dafür das Hamburgische Datenschutzgesetz (HmbDSG) mit Ausnahme seines § 2 Absatz 2 und die sonstigen für hamburgische öffentliche Stellen geltenden Vorschriften über den Datenschutz. Die oder der Hamburgische Datenschutzbeauftragte überwacht die Einhaltung dieser Vorschriften, berät die Anstalt und ihre Niederlassungen insoweit in Fragen des Datenschutzes und nimmt insoweit das Anhörungsrecht gegenüber der oder dem Datenschutzbeauftragten der Anstalt wahr. Weitere Beanstandungen nach § 25 Absatz 1 Satz 2 HmbDSG richtet die oder der Hamburgische Datenschutzbeauftragte an die für behördenübergreifende IuK-Angelegenheiten zuständige Behörde der Freien und Hansestadt Hamburg.

(3) Für die Verarbeitung personenbezogener Daten von Bewerberinnen und Bewerbern, gegenwärtigen oder früheren Beschäftigten der Anstalt und ihrer Niederlassungen gilt ergänzend zu § 23 Absatz 1 LDSG § 28 Absatz 1 und 2 sowie Absatz 4 bis 7 HmbDSG.

(4) Für die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen gelten das Hamburgische Sicherheitsüberprüfungsgesetz (HmbSÜG) und die nach § 34 dieses Gesetzes erlassene Rechtsverordnung.

(5) Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein und die oder der Hamburgische Datenschutzbeauftragte können sich einvernehmlich gegenseitig mit der Durchführung der Überwachung beauftragen.

Danach gilt hamburgisches Landesrecht, wenn die Anstalt

- für hamburgische öffentliche Stellen, gleichgültig auf welcher Rechtsgrundlage, Dienstleistungen insbesondere in den Bereichen Telekommunikation, elektronischer Rechtsverkehr (§ 3 a Hamburgisches Verwaltungsverfahrensgesetz) und Systemadministration erbringt,
- im Auftrag hamburgischer öffentlicher Stellen personenbezogene Daten verarbeitet,
- Tätigkeiten verrichtet, die nach § 3 Abs. 4 Hamburgisches Datenschutzgesetz (HmbDSG) der Datenverarbeitung im Auftrag gleichgestellt sind.

Die Landesdatenschutzgesetze finden auch insoweit ohne Einschränkungen Anwendung, als Dataport unternehmerisch am Wettbewerb teilnimmt; die entgegenstehenden Vorschriften des § 3 Abs. 2 des Schleswig-Holsteinischen Gesetzes zum Schutz personenbezogener Informationen (LDSG) und des § 2 Abs. 2 HmbDSG gelten für die Anstalt nicht.

Gemäß § 15 Abs. 3 des Staatsvertrags gelten für den Arbeitnehmerdatenschutz in der Anstalt die entsprechenden Vorschriften des HmbDSG. Dabei wird durch die Verweisung auf § 28 Abs. 7 HmbDSG klargestellt, dass z. B. personenbezogene statistische Erhebungen, die keiner Verhaltens- oder Leistungskontrolle dienen, hinsichtlich Zugriffen der Mitarbeiterinnen und Mitarbeiter bei automatisierter Datenverarbeitung unzulässig sind.

Auch für Sicherheitsüberprüfungen gelten die Vorschriften nach hamburgischem Recht. Hierdurch kann unter bestimmten Voraussetzungen für Beschäftigte in sicherheitsempfindlichen Bereichen der Anstalt eine Überprüfung ohne Mitwirkung des Landesamtes für Verfassungsschutz und ohne Einbeziehung von Ehegatten, Lebenspartnerinnen bzw. Lebenspartnern oder Lebensgefährtinnen bzw. Lebensgefährten durchgeführt werden.

Die Datenschutzbeauftragten von Schleswig-Holstein und Hamburg können sich mit Wirkung gegenüber Dataport wechselseitig mit der Durchführung der Überwachung beauftragen. Das bei der Kontrolle jeweils anzuwendende Recht bestimmt sich auch im Falle eines solchen Auftrags nach § 15 Abs. 1 bis 4 des Staatsvertrags. In Anlehnung an die bereits bestehende Kooperationsvereinbarung vom Oktober 1999 wollen wir in Kürze eine neue Vereinbarung abschließen. Sie wird die dann andere rechtliche und tatsächliche Situation bei einer Fusion der Datenzentralen berücksichtigen.

3.8 Prüfung von WLAN-Funknetzen

Die Überprüfung von Funknetzen in hamburgischen Krankenhäusern hat Mängel beim Betrieb dieser Technik offenbart. Ohne Zusatzmaßnahmen sind solche Netze nicht dazu geeignet, schützenswerte personenbezogene Daten zu übermitteln.

Unterstützt durch einen Praktikanten der Fachhochschule Ulm war der Hamburgische Datenschutzbeauftragte im vergangenen Jahr in der Lage, Funknetze nach dem WLAN-Standard hinsichtlich ihrer Datensicherheit nach § 8 HmbDSG bzw. § 9 BDSG zu überprüfen. Das erforderliche Equipment – ein handelsüblicher Laptop mit WLAN-Karte und Richtantenne – wurde mit geeigneter, frei erhältlicher Software ausgestattet, die es ermöglicht, Funknetze aufzuspüren und zu orten. Dabei wurden folgende wesentliche Betriebsparameter analysiert:

– Wem ist das Netz räumlich und sachlich zuzurechnen?

– Werden Daten offen übertragen? Werden personenbezogene Daten übertragen?

– Welche Adressen werden benutzt? Wie umfangreich ist das Netz?

– Reicht der Empfang auf öffentlichen oder frei zugänglichen Grund?

Zudem wurden unter Laborbedingungen Erfahrungswerte für die aus der Literatur (z. B. http://www.bsi.de/literat/doc/drahtloskom/drahtloskom.pdf) bekannten Schwachstellen des WLAN-Standards gewonnen.

Vor dem Hintergrund einschlägiger Szenarien über den Einsatz von Funknetzen im Gesundheitsbereich sowie der Tatsache, dass dort regelmäßig sensible Daten verarbeitet werden, fand die Überprüfung in hamburgischen Krankenhäusern statt. Geprüft wurden sowohl öffentliche als auch private Kliniken, teilweise unter Mitwirkung der Datenschutzbeauftragten der Einrichtungen. Dabei bestätigte sich unsere Vermutung, dass auch in diesem Bereich WLAN zum Einsatz kommen, wenn auch keineswegs flächendeckend.

Die gefundenen und geprüften Netze waren mehrheitlich nicht ausreichend gesichert. Infolge dessen wären unberechtigte Dritte mit gewissem, aber begrenztem Aufwand in der Lage gewesen, übertragene Daten zur Kenntnis zu nehmen. Zudem hätte die Möglichkeit bestanden, die Funknetze sowie ggf. daran angeschlossene Krankenhausnetze zu manipulieren. Lediglich eines der WLAN war auf eine Weise gesichert, die ein solches Szenario weitgehend ausschließt.

Die beanstandeten Funknetze sind mittlerweile abgeschaltet und durch verkabelte Netze ersetzt worden. Bei einem WLAN wurden zunächst eine Reihe von Sofortmaßnahmen getroffen, die das Angriffsrisiko verringern. Diese Maßnahmen sind jedoch weder aus Sicht des Datenschutzes noch aus Sicht des Betreibers als Dauerlösung geeignet. Die Implementierung einer sicheren Verschlüsselung innerhalb des WLAN auf Basis von IPSEC wurde für kurz nach Redaktionsschluss dieses Berichts mit dem Betreiber verbindlich vereinbart.

Aus datenschutzrechtlicher Sicht ergeben sich insgesamt folgende Anforderungen an den Betrieb von WLAN:

1. Die verwendete Funknetzwerktechnologie ist grundsätzlich nicht geeignet, um sensible personenbezogene Daten zu übertragen. Die Maßnahmen, die bei WLAN-Netzen nach dem gebräuchlichsten Standard „IEEE 802.11b“ getroffen werden können, genügen nicht, um die in den Datenschutzgesetzen geforderten Schutzziele (insbes. die Vertraulichkeit) zu gewährleisten.

   Auf die Übertragung entsprechender Daten ist daher entweder zu verzichten oder das erforderliche Schutzniveau ist durch geeignete zusätzliche Maßnahmen (insbes. Verschlüsselung auf höheren Protokollschichten, Stichwort: VPN-Tunnel, IPSEC) so herzustellen, dass die Sicherheitsschwächen der WLAN-Technik nicht ausschlaggebend für die Gesamtsicherheit des Systems sind. Beim Einsatz von kryptografischen Tunneln ist zu beachten, dass auch die Endpunkte der Tunnel – z. B. durch den Einsatz von Personal Firewalls – ausreichend abgesichert werden müssen.

2. Der Betrieb des WLAN ist durch folgende Maßnahmen abzusichern:

– WEP ist mit einem Schlüssel von 104/128 Bit Länge zu nutzen. Dabei ist darauf zu achten, dass diese Schlüssellänge tatsächlich erreicht wird; dies geschieht am besten durch die direkte Eingabe eines entsprechenden Hexadezimalwerts.

– Wird stattdessen ein Kennwort verwendet, um den WEP-Schlüssel zu erzeugen, ist darauf zu achten, dass dieses Kennwort oder der wesentliche Teil davon nicht leicht zu erraten ist (kein Wörterbuch-Wort).

– Der WEP-Schlüssel ist regelmäßig (Orientierung: Verfallszeiten für Passwörter) zu wechseln.

– Im Access Point ist die MAC-Filterung zu nutzen, so dass nur Geräte mit festgelegten Adressen am WLAN teilnehmen können. Dies schützt in gewissem Maße vor Verbindungsversuchen fremder Funknetzwerkkarten.

– Die SSID des Netzes sollte auf einen nichtsprechenden oder allgemeinen Namen ("Funknetz") eingestellt sowie versteckt werden, um eine Identifikation des Betreibers zu erschweren.

– Der Administrationszugang für den Access Point sollte an bestimmte IP-Adressen bzw. an den kabelgebundenen Zugang gebunden werden, so dass eine Administration per Funk nicht möglich ist.

– Es sollte geprüft werden, ob die Abstrahlung des Funknetzwerks auf öffentlichen Grund oder benachbarte Gebäude reicht, und die Sendeleistung des Access Points ggf. reduziert werden. Die unerwünschte Abstrahlung kann bei manchen Geräten auch durch die Verwendung geeigneter externer Antennen reduziert werden.

– Der Access Point sollte so untergebracht werden, dass er nur für autorisiertes Personal erreichbar ist (z. B. in bestimmten Räumen oder in Zwischendecken), so dass eine Manipulation (z. B. ein Reset) durch Unbefugte nicht möglich ist.

– Das Funknetzwerk sollte außerhalb der normalen Nutzungszeiten abgeschaltet werden. Dies kann beispielsweise über eine Schaltuhr in den Nachtstunden und am Wochenende geschehen.

3. Sofern es gelingt, den WEP-Schlüssel zu brechen und eine gültige Adresse einzustellen, kann ein Angreifer den WLAN-Verkehr nicht nur mithören, sondern auch mit den anderen Geräten des Funknetzes kommunizieren und dabei ggf. Sicherheitsschwächen ausnutzen. Daher sind die Endgeräte mit geeigneten Schutzmaßnahmen (Personal Firewall, Virenscanner) auszustatten und regelmäßig auf Schwachstellen zu überprüfen.

4. Damit Angriffe auf das WLAN nicht eine unmittelbare Bedrohung für die gesamte DV-Infrastruktur bedeuten, ist das Funknetz physikalisch in einem separaten Subnetz zu betreiben. Die Verbindung zum Kabelnetzwerk ist mit geeigneter Technik (Firewall) so abzusichern, dass Verbindungen nur im jeweils erforderlichen Maße möglich sind.

5. Da einer Funktionsstörung durch Fremdstrahlung schwer entgegengewirkt werden kann, sind Vorkehrungen zu treffen, die für diesen Fall einen Betrieb im notwendigen Umfang gleichwohl gewährleisten. Ebenfalls ist eine Notfallplanung zu entwickeln, wie auf eine Attacke auf das WLAN reagiert werden soll.

6. Bei der Beschaffung von WLAN-Hardware und WLAN-fähigen Geräten ist darauf zu achten, dass diese die erforderlichen Sicherheitsmaßnahmen auch unterstützen. Das Sicherheitsniveau darf nicht von den Geräten (z. B. PDA) bestimmt werden, die in dieser Hinsicht die geringsten Möglichkeiten bieten.

7. Organisatorisch sollte sichergestellt werden, dass Funknetze nur mit Kenntnis und Zustimmung der IT-Abteilung oder vergleichbarer Einheiten aufgebaut und betrieben werden.

Vor dem Hintergrund der beschriebenen WLAN-Prüfungen in Hamburg hatten wir im zuständigen Bund-Länder-Arbeitskreis der Datenschutzbeauftragten auch rechtliche Fragen aufgeworfen und Einvernehmen mit den anderen Landesbeauftragten erzielt: Nach § 38 Abs. 4 Satz 3 in Verbindung mit § 24 Abs. 2 Satz 1 Nr.1, Abs. 6 BDSG kann das Fernmeldegeheimnis einer Kontrolle durch die Aufsichtsbehörde nicht entgegengehalten werden. Konsens bestand deswegen darin, dass die Aufsichtsbehörden der Länder bzw. – bei öffentlichen Stellen – die Landesdatenschutzbeauftragten befugt sind, zur Erfüllung ihrer Aufgaben auch ohne vorherige Ankündigung zu prüfen, ob überhaupt WLANs im Einsatz sind, ob der WLAN-Verkehr verschlüsselt oder offen erfolgt, ob personenbezogene Daten ausgetauscht werden und ob technisch-organisatorische Sicherheitsmaßnahmen ausreichen.

Der Bundesbeauftragte für den Datenschutz ist nach § 91 Abs. 4 Telekommunikationsgesetz (TKG) erst dann zuständig, wenn sich bei der Prüfung ergibt, dass die Stelle, die ein WLAN betreibt, selbst geschäftsmäßig Telekommunikationsdienste anbietet. Dazu gehört z. B., wenn diese Stelle es Kunden, Patienten oder Gästen ermöglicht, sich über den WLAN-Accesspoint in das Internet einzuloggen, um zu "surfen" oder E-Mails auszutauschen.

§ 86 Satz 1 TKG verbietet allen Personen, empfangene WLAN-Nachrichten und die Tatsache ihres Empfangs anderen mitzuteilen. Ein privates Unternehmen, das Sicherheitsmodule für den Betrieb von WLANs anbietet und selbst unsichere Netze aufspürt, hatte uns gefragt, ob dieses Verbot auch für den Hinweis auf unsichere WLANs an die Datenschutzaufsichtsbehörde gilt. Nach Rück-

sprache mit dem Bundeswirtschaftsministerium verneinte der Arbeitskreis der Datenschutzbeauftragten dies, weil die Vorschrift dem Schutz des Fernmeldegeheimnisses diene und das Aufdecken von Sicherheitsmängeln nicht verhindern solle.

3.9 Speicherung von IP-Nummern durch Provider

Die Praxis von Internet-Providern, IP-Nummern sämtlicher Nutzer zu speichern, ist in vielen Fällen mit den geltenden datenschutzrechtlichen Bestimmungen nicht zu vereinbaren.

Im Jahr 2002 entwickelte sich unter den Datenschutzaufsichtsbehörden eine Diskussion über die Frage, ob, unter welchen Bedingungen und in welchem Umfang Provider Daten über die Nutzung von Telediensten speichern dürfen. Zu diesen Nutzungsdaten – Merkmale über die Identifikation des Nutzers, über Beginn, Ende und Umfang der Nutzung – zählen auch die IP-Nummern.

Anbieter von Zugangsdiensten (Access-Provider) und anderen Telediensten (Content-Provider) sind an die Bestimmungen des Teledienstedatenschutzgesetzes (TDDSG) gebunden, in dem der zulässige Umgang mit Nutzungsdaten festgeschrieben ist. Die Regelungen des §6 TDDSG sind dabei als abschließend zu beurteilen; ein Rückgriff auf allgemeine Erlaubnistatbestände des BDSG ist ausgeschlossen. Für Content-Provider, die Mediendienste anbieten, gelten gleichlautende Bestimmungen des Mediendienste-Staatsvertrags (MDStV). Diese Regelungen sehen eine Speicherung von Nutzungsdaten über den Zeitpunkt der Inanspruchnahme des Dienstes hinaus nur insoweit vor, als diese zu Abrechnungszwecken erforderlich sind.

Die IP-Nummer als personenbezogenes Datum

Mit Hilfe seiner IP-Nummer bzw. IP-Adresse ist ein Nutzer zu einem bestimmten Zeitpunkt eindeutig im Internet identifizierbar. Während sog. statische IP-Nummern einem Nutzer fest zugeordnet sind und ihn daher dauerhaft identifizieren, verfügen die meisten Nutzer über eine dynamische Adresse, die ihnen für einen aktuellen Nutzungszeitraum zugewiesen wird. Zu einer anderen Zeit ist die Adresse an andere Nutzer vergeben oder bleibt ungenutzt.

Die dynamische Vergabe von IP-Adressen erfolgt durch Access-Provider. Für diese ist daher ein direkter Personenbezug der vergebenen Adressen gegeben. Für Content-Provider ist zwar ein Personenbezug dynamischer IP-Adressen unmittelbar nicht in jedem Fall herstellbar, kann durch Zusatzwissen jedoch hergestellt werden. Dabei sind die umfänglichen Möglichkeiten der Zusammenführung von Daten im Internet zu berücksichtigen. Auf IP-Adressen sind daher die datenschutzrechtlichen Vorschriften für Nutzungsdaten anzuwenden.

Ausgangspunkt der Diskussion war die Entscheidung des Regierungspräsidiums Darmstadt, die im Fall eines namhaften Providers eine Zulässigkeit der Speicherung von IP-Adressen auch in solchen Fällen festgestellt hat, in denen aufgrund der vertraglichen Vereinbarung (Flatrate-Tarif) eine Nutzung für Abrechnungszwecke gerade nicht gegeben ist. Zur Begründung wurde darauf verwiesen, dass die IP-Nummern gleichwohl zum Nachweis der Korrektheit der Abrechungen sowie zur Aufklärung von Missbrauchsfällen erforderlich seien.

Wie sich zeigte, waren die Auffassungen der Datenschutz-Aufsichtsbehörden zu diesem Thema derart divergent, dass eine gemeinsame Positionierung nur in Teilaspekten möglich war. Einzelne Aufsichtsbehörden (darunter der Hamburgische Datenschutzbeauftragte) äußerten sich auch in der Öffentlichkeit kritisch zu der Auffassung aus Darmstadt und kündigten für ihren Zuständigkeitsbereich ein anderes Vorgehen an. Einverständnis konnte jedoch darüber erzielt werden, dass die Speicherung über den Nutzungszeitraum hinaus zulässig ist, soweit dies im Einzelfall zur Gewährleistung der Datensicherheit erforderlich ist.

Mit einer solchen Einzelfall-Betrachtung ist eine pauschale Speicherung sämtlicher IP-Nummern jedenfalls nicht vereinbar. Auch soweit eine solche Speicherung auf die Gewährleistung der betrieblichen Sicherheit des Anbieters gestützt wird, halten wir dies für nicht vereinbar mit den rechtlichen Bestimmungen.

Wir haben bereits im Jahre 2002 damit begonnen, die Access-Provider in unserem Zuständigkeitsbereich hinsichtlich des Umgangs mit Nutzungsdaten zu überprüfen. Wir hatten aufgrund der geschilderten Diskussion eine endgültige Festlegung in einigen Fällen jedoch zunächst verschoben. Mittlerweile haben wir diese Überprüfung wieder aufgenommen und die Provider zu einer Löschung der IP-Adressen aufgefordert, die für Abrechnungszwecke nicht erforderlich sind.

3.10 Internet-Nutzung in der Staats- und Universitätsbibliothek (SUB)

Für Benutzer des Internet-Zugangs der SUB haben wir einen Verzicht auf die Protokollierung der Zugriffe durchgesetzt.

Ausgelöst durch ein polizeiliches Auskunftsbegehren wurde seitens der SUB die Frage an uns herangetragen, ob dort vorliegende Protokolldaten an Ermittlungsbehörden herausgegeben werden dürfen. Wir erfuhren in diesem Zusammenhang erstmals von dem seit fünf Jahren bestehenden Angebot, als Bibliotheks-Benutzer Internet-Arbeitsplätze in den Räumen der SUB für Recherchen nutzen zu können. Das Angebot ist kostenfrei, jedoch für jeden Nutzer zeitlich limitiert.

Bei einer Prüfung der technischen Realisierung dieses Angebots stellte sich heraus, dass umfangreiche Log-Daten über die Zugriffe der Nutzer geführt werden. Diese Daten umfassten auch die URL der abgerufenen Seiten, die über die IP-Adressen der Arbeitsplätze den Nutzern zugeordnet werden kann. Der SUB wäre es daher möglich gewesen, das Surf-Verhalten eines Nutzers über einen längeren Zeitraum auch rückwirkend auszuwerten.

Die SUB tritt hier gegenüber den Nutzern als Access-Provider und damit als Anbieter eines Teledienstes auf. Wie in 3.9 ausgeführt, ist der Umgang mit Nutzungsdaten für Access-Provider durch die Bestimmungen des Teledienstedatenschutzgesetzes festgelegt. Bei den protokollierten URL handelt es sich um Nutzungsdaten von besonderer Aussagekraft, die bereits die Inhaltsebene berühren.

Wir haben die Protokollierung der SUB daher als unzulässig kritisiert und einen Verzicht oder eine Anonymisierung der Protokolle gefordert. Dem ist die SUB gefolgt und hat angekündigt, einerseits die Speicherung der An- und Abmeldungen der Nutzer auf die für den Zweck der Benutzerbetreuung angemessene Dauer von 24 Stunden zu beschränken. Zum anderen sollen die aufgerufenen URL nurmehr anonymisiert protokolliert werden. Diese Protokolle dienen der Optimierung des Angebots sowie als Grundlage für mögliche Sperrungen von bestimmten Seiten, die mit den geltenden Benutzungsregeln nicht vereinbar sind.

3.11 Entwicklungen beim Tele-Medienrecht (EMDSG und TKG)

Die durch Zusammenfassung bestehender rechtlicher Bestimmungen geplante neue Medienordnung ist ins Stocken geraten. Der Entwurf eines neuen Telekommunikationsgesetzes führt zu Verschlechterungen des Datenschutzes.

Die datenschutzrechtlichen Bestimmungen bei den elektronischen Medien sind auf verschiedene Regelwerke auf Bundes- und Länderebene verteilt. Die weitgehende Übereinstimmung der Datenschutzbestimmungen im Teledienstedatenschutzgesetz (TDDSG) und im Mediendienste-Staatsvertrag (MDStV) legen eine Zusammenfassung zu einem für Anbieter und Nutzer von Tele- und Mediendiensten besser handhabbaren Gesamtwerk und eine Harmonisierung mit den Datenschutzbestimmungen im Telekommunikationsrecht nahe.

Das Bundesministerium für Wirtschaft und Arbeit (BMWA) hat bereits im Jahr 2002 Strukturüberlegungen für ein „Gesetz über den Datenschutz bei der Nutzung elektronischer Medien – EMDSG“ vorgelegt, in dem das bisherige TDDSG und die Datenschutzbestimmungen des MDStV zusammengeführt werden. Die Zusammenführung der Parallelregelungen und die vorgeschlagenen materiell-rechtlichen Bestimmungen wurde von den Datenschutzbeauftragten begrüßt.

Dagegen stieß die vom BMWA vorgeschlagene Umgestaltung der datenschutzrechtlichen Aufsicht durch Schaffung neuer Instrumente der freiwilligen Selbstkontrolle – vergleichbar mit der Praxis im Jugendschutz – auf weitgehende Ablehnung der Datenschutzbeauftragten. Kritisiert wurde dabei vor allem, dass bei Umsetzung der Vorschläge die Befugnisse der Datenschutzaufsichtsbehörden in diesem Bereich wesentlich zurückgedrängt würden, ohne dass ein Ersatz geschaffen würde, der die Einhaltung und Überwachung eines ausreichenden Datenschutzniveaus garantieren könnte. Diese Kritik zeigte offenbar Wirkung, denn in einem Entwurf zum EMDSG vom Mai 2003 wurde die Umgestaltung der Aufsichtsstruktur zurückgenommen.

Ob das BMWA bei dieser Position bleibt, muss abgewartet werden, denn mittlerweile ist das Gesetzesvorhaben offenbar ins Stocken geraten. Nach aktuellen Informationen sollen zunächst das in § 9 a BDSG angelegte Gesetz zum Datenschutzaudit und möglicherweise weitere Novellierungen im Datenschutzrecht auf den Weg gebracht werden, bevor die nächsten Schritte im Bereich der elektronischen Medien unternommen werden.

Parallel zur Neuordnung des Multimediarechts hat die Bundesregierung die Novellierung des Telekommunikationsgesetzes (TKG) auf den Weg gebracht (BR-Drs. 755/03 v. 17. Oktober 2003). Die vorgesehenen Änderungen der Datenschutzbestimmungen setzen zum einen die EG-Richtlinie über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Richtlinie 2002/58/EG) in deutsches Recht um. Der Entwurf enthält darüber hinaus jedoch auch Verschlechterungen für den Datenschutz der Nutzer von Telekommunikationsdiensten und würde so zu einer weiteren Auseinanderentwicklung des Multimediarechts und des Telekommunikationsrechts beitragen. Zu diesen Änderungen hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 21. November 2003 eine Entschließung verabschiedet, die aus dem Web-Angebot des Bundesbeauftragten für den Datenschutz abgerufen werden kann (http://www.bfd.bund.de/information/DS-Konferenzen/66_67_ent1.html).

Kritisch ist insbesondere, dass die Anbieter in Zukunft das Recht bekommen sollen, alle entstehenden Verkehrsdaten (also auch die Zielrufnummern) unverkürzt bis zu sechs Monate nach Versendung der Rechnung zu speichern. Damit würde ohne überzeugende Begründung die bewährte Regelung aufgegeben, regelmäßig bloß eine verkürzte Speicherung zuzulassen, sofern die Kundinnen und Kunden sich nicht für die vollständige Speicherung oder komplette Löschung entscheiden. Das Wahlrecht des Kunden soll zwar erhalten bleiben, wird in der Praxis jedoch kaum wahrgenommen.

Die außerdem vorgesehene Verpflichtung der Anbieter, die Identität der Käufer von Prepaid-Handys festzustellen, auch wenn diese Daten für die Abwicklung des Dienstes nicht erforderlich sind, stellt einen nicht gerechtfertigten Eingriff in das Recht auf informationelle Selbstbestimmung der Nutzer dar. Die Käufer

geben solche Handys häufig an andere weiter und sind daher nicht identisch mit den späteren Nutzerinnen und Nutzern. Die Daten über die Identität der Käufer lassen deswegen keinen nennenswerten Informationsgewinn für Sicherheitsbehörden erwarten.

Schließlich soll den Strafverfolgungsbehörden, der Polizei und den Nachrichtendiensten der Zugriff auf Passwörter und PINs voraussetzungslos, also ohne Bindung an einen Straftatenkatalog und ohne Richtervorbehalt, erlaubt werden. Auch dies wäre ein unverhältnismäßiger Eingriff in das Fernmeldegeheimnis nach Art. 10 GG.

Es ist zu hoffen, dass der Gesetzgeber den Entwurf im weiteren Gesetzgebungsverfahren an den genannten sensiblen Punkten korrigiert und damit den gebotenen Schutz des Telekommunikationsgeheimnisses sicherstellt. Zu begrüßen wäre ferner eine spätere Zusammenführung der Datenschutzbestimmungen im Telekommunikations- und Multimediarecht.

3.12 Redaktionsdatenschutz

Durch eine Ergänzung des Hamburgischen Pressegesetzes werden Presseunternehmen – auch solche, die sich nicht dem Pressekodex des Deutschen Presserates unterwerfen – auf den Redaktionsdatenschutz verpflichtet.

Im 18.Tätigkeitsbericht berichteten wir vom neuen Redaktionsdatenschutz in § 41 BDSG (vgl. 18.TB, 2.2.3) und von der Notwendigkeit, dazu im Landesrecht Regelungen zu treffen. Mit dem zweiten Gesetz zur Änderung des Hamburgischen Pressegesetzes vom 28. Januar 2003 ist dies geschehen. Der neue § 11a HmbPresseG betrifft die Erhebung, Verarbeitung und Nutzung personenbezogener Daten „zu eigenen journalistisch-redaktionellen oder literarischen Zwecken“. Hierfür verweist er auf die Regelungen im BDSG zum Datengeheimnis, zu notwendigen Datensicherungsmaßnahmen und entsprechenden Richtlinien sowie zur Schadensersatzpflicht.

Darüber hinaus konnten wir erstmals in der Bundesrepublik erreichen, dass § 11 a HmbPresseG auch eine Regelung für diejenigen Presseunternehmen trifft, die sich dem Pressekodex und der Beschwerdeordnung des Deutschen Presserats (als verbandlichen Richtlinien) nicht unterwerfen: Für sie gilt § 41 Abs. 3 BDSG entsprechend. Er gibt Personen, die von der Presseberichterstattung in ihrem Persönlichkeitsrecht beeinträchtigt werden, ein eingeschränktes Recht auf Auskunft und Berichtigung unrichtiger Daten.

Dass es sich bei dieser Regelung nicht nur um datenschutzrechtliche Vorsorge handelt, zeigt ein Bericht des Deutsche Presserats in seinem Jahrbuch 2003: Danach hatte der Deutsche Presserat im November 2001 ca. 700 Unternehmen des Bundesverbandes Deutscher Zeitungsverleger und des Verbandes Deutscher Zeitschriftenverleger um die Abgabe einer Selbstverpflichtung auf den Pressecodex und die Grundsätze zum Redaktionsdatenschutz gebeten.

Bis Anfang 2003 unterzeichneten 583 von ihnen. Von den ebenfalls ca. 700 nicht verbandsgebundenen, meist kleineren Presseunternehmen gaben nur 107 die Verpflichtungserklärung ab.

Im übrigen führt das Jahrbuch 2003 des Deutschen Presserats ausführlich in den Redaktionsdatenschutz ein und veröffentlicht erste Erfahrungen des neuen Beschwerdeausschusses. Dabei zeigt sich, dass eine eindeutige Zuordnung der Beschwerden zum allgemeinen Beschwerdeausschuss einerseits und zum Beschwerdeausschuss Redaktionsdatenschutz andererseits kaum möglich ist. Denn das Recht auf informationelle Selbstbestimmungs der betroffenen Personen ist auch bei vielen Verpflichtungen des Pressekodex berührt, die nicht als Spezialregelungen zum Redaktionsdatenschutz neu eingeführt wurden. Die weitere Praxis wird hier handhabbare Zuordnungskriterien zu entwickeln haben.

Datenschutz im öffentlichen Bereich

4. Meldewesen

Novellierung des Melderechts

Bürgerschaft und Senat haben die Weichen für ein modernes, effizientes Meldewesen mit hohem Datenschutzstandard gestellt.

Durch die Änderung des Hamburgischen Meldegesetzes (HmbMG) vom 2. Juli 2003 sowie die Änderungen der Meldedatenübermittlungsverordnung (MDÜV) vom 22. Juli und 30. September 2003 sind die Regelungen über automatisierte Abrufe von Daten aus dem Melderegister deutlich erweitert und einer neuen Systematik zugeführt worden. Das Meldewesen stellt die erste Fachanwendung für das HamburgGateway – das „digitale Tor zu Hamburgs Verwaltung“ – dar und bildet damit einen wesentlichen Faktor bei der Optimierung von Geschäftsprozessen im Rahmen des E-Government (vgl. 1.2). Die rechtlichen und technischen Rahmenbedingungen für diese Entwicklung sind mit uns intensiv abgestimmt worden.

Die automatisierten Abrufe von Meldedaten durch hamburgische Behörden oder sonstige öffentliche Stellen sind auf Grund der Gesetzesnovelle nach drei Berechtigungsstufen (Grunddaten, erweiterte Grunddaten und Spezialdaten) differenziert. Grunddaten (Familienname, Vorname, Doktorgrad, gegenwärtige Anschrift, Tag des Ein- und Auszugs und Angabe über den Verbleib, Tag und Ort der Geburt, Sterbetag und Sterbeort) dürfen allen hamburgischen Behörden oder sonstigen öffentlichen Stellen ohne Angabe des Abrufzwecks durch automatisierten Abruf aus dem Melderegister übermittelt werden. Erweiterte Grunddaten (frühere Namen, frühere Anschriften) dürfen von den hamburgischen Dienststellen, die in einem abschließenden Katalog der MDÜV aufge-

führt sind, ohne Angabe des Abrufzwecks automatisiert abgerufen werden. Der Abruf von Spezialdaten (z. B. gesetzlicher Vertreter, Staatsangehörigkeiten, Familienstand) bleibt den in der MDÜV einzeln genannten hamburgischen Dienststellen für die dort näher bestimmten Zwecke vorbehalten.

Der Datenschutzstandard für automatisierte Abrufe von Meldedaten durch hamburgische Dienststellen ist in der MDÜV detailliert festgelegt. So enthält die MDÜV Regelungen über die Protokollierung von Abrufen, die Aufbewahrung und Verwendung der Protokolldaten, die Überprüfung von Abrufen im Wege der Dienst- und Fachaufsicht sowie die Unterrichtung der Betroffenen von Amts wegen in schwer wiegenden Fällen eines unzulässigen Abrufs.

In Anpassung an das Melderechtsrahmengesetz (MRRG) des Bundes hat Hamburg ferner die Rechtsgrundlagen für eine Online-Melderegisterauskunft an Private geschaffen. Die Erteilung einer einfachen Melderegisterauskunft über Vor- und Familienname, Doktorgrad und gegenwärtige Anschrift im Wege des automatisierten Abrufs über das Internet setzt voraus, dass der Anfragende als Kunde bei der zentralen Informations- und Kommunikationsdienststelle für die Freie und Hansestadt Hamburg (HamburgGateway) registriert ist, sich durch Vorlage eines Ausweispapiers authentifiziert hat und freigeschaltet wurde. Die Auskunft wird nur erteilt, wenn der Anfragende die betroffene Person mit Vor- und Familiennamen und mindestens zwei der nachfolgenden Daten: Geburtsdatum, Geschlecht, eine frühere oder gegenwärtige hamburgische Anschrift, konkret bezeichnet hat.

Treffen die Anfragedaten auf mehrere im Melderegister gespeicherte Personen zu, so wird – wie schon bisher bei schriftlichen Anträgen – eine Auskunft zur Vermeidung von Personenverwechslungen abgelehnt. Melderechtliche Auskunftssperren zur Vorbeugung von Gefahren für Leben, Gesundheit und persönliche Freiheit schließen nicht nur eine schriftliche, sondern auch eine elektronische Auskunft an Private generell aus. Die Sicherheit der Datenverarbeitung wird nach der MDÜV insbesondere durch eine Verschlüsselung bei der Datenübermittlung gewährleistet.

Unabhängig davon kann jeder Einwohner der Internet-Melderegisterauskunft an Private durch Erklärung gegenüber dem Einwohneramt (Bezirks- oder Ortsamt) ohne Angabe von Gründen und gebührenfrei widersprechen. Die Behörde für Inneres (BfI) hat in Abstimmung mit uns ein Informationsblatt zum Widerspruchsrecht herausgegeben, das auch über unser Internet-Angebot abrufbar ist.

Wir erörtern mit den beteiligten Fachbehörden die Voraussetzungen und das Verfahren für automatisierte Abrufe von Meldedaten durch außerhamburgische Behörden. Wir gehen davon aus, dass solche Abrufe nur soweit und solange zulässig sind, wie sich aus der Vielzahl oder besonderen Eilbedürftigkeit der Datenübermittlungen ein begründeter Bedarf ergibt. Entfällt der Bedarf

oder werden unberechtigte Abrufe festgestellt, so ist die Freischaltung für den automatisierten Abruf unverzüglich aufzuheben. Auch sollte die MDÜV sicherstellen, dass die für die abrufende außerhamburgische Behörde jeweils zuständigen Datenschutzbeauftragten des Bundes und der Länder möglichst umfassend beteiligt werden. Für den automatisierten Abruf durch außerhamburgische Behörden ist zudem eine Evaluierung gesetzlich vorgeschrieben. Sie soll zuverlässige Aussagen darüber ermöglichen, von welchen Stellen, für welche Zwecke und in welchem Umfang die Möglichkeiten des automatisierten Abrufs tatsächlich genutzt werden. Dies setzt voraus, dass der zuständigen Behörde in Hamburg die Anzahl der Abrufe in regelmäßigen Abständen mitgeteilt wird.

5. Umwelt

Kataster zu Standorten von UMTS-Mobilfunksendeanlagen

Für die Erstellung und Veröffentlichung von Mobilfunkkatastern fehlen zum Teil die erforderlichen Rechtsgrundlagen.

Die Regulierungsbehörde für Telekommunikation und Post (RegTP) hat den Landes- und Kommunalbehörden den Zugriff auf eine Datenbank mit Informationen über Sendefunkanlagen ermöglicht. Sie will damit vor allem einen konstruktiven Beitrag zur Versachlichung der kontrovers geführten Diskussion um den Mobilfunk leisten. Die Standortdatenbank ist nur einem festgelegten Nutzerkreis (Landes- und Kommunalbehörden) über ein passwortgeschütztes Zugangsberechtigungssystem zugänglich und soll zur Erfüllung ihrer Aufgaben nach dem Bauplan- und Bauordnungsrecht und der Gesundheitsfürsorge dienen.

Im Zuge der Planung zahlreicher neuer Standorte von Empfangs- und Sendeanlagen zum Aufbau des UMTS-Mobilfunknetzes wächst in der Bevölkerung die Sorge vor Gesundheitsgefährdungen durch elektromagnetische Strahlung. Die Speicherung und Veröffentlichung (z. B. im Internet) der Standortdaten von Mobilfunkantennen durch die Kommunen oder andere öffentliche Stellen stehen daher in verstärktem Maße in der öffentlichen Diskussion.

Die Frage, unter welchen Voraussetzungen eine Weitergabe der Standortdaten von Mobilfunkantennen an Dritte zulässig ist, wurde auf der Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 24./25. Oktober 2002 erörtert. Hierzu wurde eine Entschließung verabschiedet, mit der der Bundesgesetzgeber aufgefordert wird, im Rahmen einer immissionsschutzrechtlichen Regelung über die Erstellung und Veröffentlichung von Mobilfunkkatastern zu entscheiden.

Unabhängig davon stellte sich für die in Hamburg zuständige Behörde für Umwelt und Gesundheit (BUG) die Frage, ob und inwieweit der Bürger einen Anspruch auf Nutzung der Standortdatenbank bei der RegTP hat. Wir haben die BUG gebeten, nach geltender Rechtslage zu verfahren, die sich wie folgt darstellt:

Die Mobilfunkbetreiber sind nach § 7 Abs. 1 der 26. Bundesimmissionsschutzverordnung (BImSchVO) verpflichtet, den Standort von Hochfrequenzanlagen sowie bestimmte Niederfrequenzanlagen der BUG anzuzeigen. Somit handelt sich bei den Mobilfunkstandorten um umweltrelevante Daten im Sinne des Umweltinformationsgesetzes (UIG), deren Erhebung und Speicherung bei der BUG als zulässig anzusehen ist. Zu diesen Daten hat grundsätzlich jedermann freien Zugang (§ 4 Abs. 1 UIG), soweit dieser Anspruch nicht nach § 7 oder § 8 UIG zu beschränken oder zu versagen ist.

Da die Standortdaten auch Angaben zur Lage (z. B. Straße und Hausnummer) enthalten, können die jeweiligen Grundstückseigentümer bestimmbar gemacht werden (z. B. über das Grundbuchamt). Soweit es sich dabei um natürliche Personen handelt, liegen personenbezogene Daten im Sinne des § 4 Abs. 1 Hamburgisches Datenschutzgesetz (HmbDSG) vor. Die Verarbeitung (z. B. Übermittlung) dieser Daten ist nur zulässig, wenn eine Rechtsvorschrift sie erlaubt oder die Betroffenen eingewilligt haben (§ 5 Abs. 1 HmbDSG).

Sind Mobilfunkantennen von öffentlichen Wegen erkennbar, handelt es sich bei diesen Standortdaten (z. B. Straße und Hausnummer) um offenkundige Daten, die gegenüber Dritten ohne Einschränkung offenbart werden können. Bei verdeckten Mobilfunkantennen ist hingegen eine Abwägung zwischen dem Recht auf informationelle Selbstbestimmung des betroffenen natürlichen Grundeigentümers und dem Interesse der Allgemeinheit an einem freien Zugang zu Umweltinformationen vorzunehmen. Dazu müssen die Betroffenen gem. § 8 Abs. 2 UIG gehört werden. Erst nach erfolgter Anhörung und deren Einbeziehung in den Abwägungsprozess ist im Einzelfall über die Offenbarung zu entscheiden.

Nach unserem Kenntnisstand ist die „Offenkundigkeit von Standortdaten“ der zuständigen Behörde in der Regel überhaupt nicht bekannt und wird weder in entsprechenden behördlichen Akten noch in Datenbanken (z. B. Standortdatenbank der RegTP) als Merkmal erfasst. Daher wäre vor diesem Hintergrund eine allgemeine Offenbarung der Standortdaten als bedenklich anzusehen. Somit können auch insoweit grundsätzlich nur Einzelfallprüfungen in Betracht kommen.

6. Soziales

6.1 Anforderung ärztlicher Unterlagen durch Krankenkassen bei Krankenhäusern

Ein jahrelanger Streit ist beendet: Die Krankenkassen haben nicht das Recht, selbst die Behandlungsunterlagen der Krankenhäuser einzusehen.

Mit der Zulässigkeit der Anforderung von Krankenhaus-Entlassungsberichten haben wir uns in den letzten Jahren wiederholt beschäftigt (vgl. 18. TB, 10.1). Unsere hierzu vertretene Rechtsauffassung hat das Bundessozialgericht durch Urteil vom 23. Juli 2002 (Az. B 3 KR 64/01 R) bestätigt. Nach diesem Ergebnis haben wir näher untersucht, ob auch das vor Jahren mit uns abgestimmte Einwilligungsverfahren datenschutzrechtlich noch vertretbar ist (vgl. 13. TB, 21.8.2). Wir sind dabei zu folgendem Ergebnis gekommen:

In dem Urteil legt das Gericht dar, dass Krankenkassen nicht aus eigenem Recht Einsicht in Behandlungsunterlagen verlangen können, sondern insoweit auf ein Tätigwerden des Medizinischen Dienstes der Krankenversicherung (MDK) angewiesen sind. In § 301 SGB V sei aus datenschutzrechtlichen Gründen abschließend aufgezählt, welche Angaben den Krankenkassen bei der Krankenhausbehandlung ihrer Versicherten zu übermitteln sind. Behandlungsdaten der Versicherten gehörten nicht hierzu. Für die Krankenkassen sei es zur Erfüllung ihrer Aufgaben auch nicht erforderlich, in die Behandlungsunterlagen der Versicherten Einsicht zu nehmen. Bei Zweifeln an der sachlich-rechnerischen Richtigkeit einer Krankenhausabrechnung habe die Krankenkasse nach § 275 Abs. 1 Satz 1 SGB V eine gutachterliche Stellungnahme des MDK einzuholen. Der MDK sei im Falle einer Abrechnungsprüfung ermächtigt, die erforderlichen Sozialdaten bei den Krankenhäusern anzufordern. Gleichzeitig sei der MDK verpflichtet, der Krankenkasse das Ergebnis der Begutachtung sowie die erforderlichen Angaben über den Befund mitzuteilen.

Damit stellt das Bundessozialgericht klar, dass es allein Aufgabe des MDK ist, medizinische Unterlagen für die sachlich-rechnerische Prüfung der Abrechnung eines Krankenhauses zu beurteilen. Die Verfahrensweise, eine Einwilligung des Versicherten zur Übermittlung von Behandlungsunterlagen einzuholen, stellt folglich eine Umgehung der abschließenden Regelung des § 301 SGB V sowie der gesetzlichen Regelung dar, dass allein der MDK für die Prüfung medizinischer Sachverhalte zuständig ist.

In Hamburg hatten wir bislang diese Einwilligungslösung in begründeten Einzelfällen hingenommen, sofern der Versicherte zuvor hinreichend über das Verfahren aufgeklärt wurde. In Anbetracht der Fortentwicklung der Rechtsprechung hat sich unsere Rechtsauffassung hierzu gewandelt. Wir meinen, dass nunmehr Forderungen der Krankenkassen an Krankenhäuser und Ärzte, bei Vorliegen einer Einwilligungserklärung des Versicherten die Behandlungsun-

terlagen an die Krankenkasse zu übermitteln, rechtlich nicht mehr gedeckt und damit unzulässig sind.

Bei Beratungen und Kontrollen von Krankenkassen werden wir auf diese Rechtsauffassung verweisen. Außerdem haben wir die unserer Kontrolle unterliegenden Krankenkassen gebeten, ihre Praxis entsprechend anzupassen und verfahrensmäßig sicher zu stellen, dass in die Behandlungsunterlagen ausnahmslos der MDK einsehen kann. Weder für die Abrechnung mit den Leistungserbringern (§ 284 Abs. 1 Satz 1 Nr. 8 SGB V) noch für die Beteiligung des MDK (§ 284 Abs. 1 Nr. 7 SGB V) muss die Krankenkasse selbst Einsicht in die Behandlungsunterlagen nehmen können. Es ist danach auch nicht vertretbar, dass die Krankenkasse die Behandlungsunterlagen dahingehend überprüft, ob der MDK überhaupt nach § 275 Abs. 1 Satz 1 SGB V zur Abgabe einer gutachtlichen Stellungnahme beauftragt werden soll.

Die Behörde für Umwelt und Gesundheit (BUG), die in Hamburg für die Fachaufsicht in der gesetzlichen Krankenversicherung zuständig ist, teilt grundsätzlich unsere Rechtsauffassung. Wir gehen deshalb davon aus, dass die BUG die datenschutzrechtlichen Gesichtspunkte im Rahmen ihrer Aufsichtstätigkeit angemessen berücksichtigen wird. Auch der Hamburgischen Krankenhausgesellschaft haben wir anheim gestellt, die ihr angeschlossenen Einrichtungen über die neue Situation zu unterrichten.

6.2 Überprüfung der Arbeitsunfähigkeit von Versicherten

Die Betriebskrankenkasse (BKK) Hamburg hat bei der Überprüfung von „Blaumachern" gegen den Datenschutz verstoßen.

Die BKK Hamburg hat im Berichtszeitraum zahlreichen Arbeitgebern eine Reihe von Ärzten namentlich genannt, die bei der Krankenkasse unter dem Verdacht stehen, übermäßig viele Arbeitsunfähigkeitsbescheinigungen auszustellen. Damit hat die BKK Hamburg die Vorschriften des Sozialgesetzbuches zur Überprüfung der Arbeitsunfähigkeit von Versicherten missachtet.

Das Sozialgesetzbuch enthält spezielle Regelungen, wie bei Zweifeln an der Arbeitsunfähigkeit von Versicherten zu verfahren ist. Danach ist die Krankenkasse in solchen Fällen gesetzlich verpflichtet, den Medizinischen Dienst der Krankenversicherung (MDK) einzuschalten. Allein der MDK hat zu prüfen, ob die Zweifel der Krankenkasse an der Arbeitsunfähigkeit zu Recht bestehen. Das Ergebnis dieser Überprüfung erfährt die Krankenkasse dann vom MDK, damit sie möglicherweise weitere Maßnahmen treffen kann, die ihr nach den Bestimmungen des Sozialgesetzbuches zustehen, z. B. Kürzung des Krankengeldes.

Nach dem Gesetz ist es der Krankenkasse nur gestattet, auf die ihr bereits vorliegenden Informationen aus dem Krankengeld-Management zurückzugreifen, bevor sie den MDK einschaltet. Sie darf nicht zusätzlich noch weitere Er-

mittlungen anstellen, um zu klären, ob der MDK überhaupt eingeschaltet werden soll. Immer dann, wenn die Krankenkasse die Arbeitsunfähigkeit eines Versicherten bezweifelt, hat sie den MDK mit einer gutachterlichen Stellungnahme zu beauftragen.

Durch das Rundschreiben an die Arbeitgeber hat die BKK Hamburg versucht, weitere Daten zu erheben, um – wie sie es genannt hat – „Blaumacher zu entlarven". Eine Rechtfertigung für diese Vorgehensweise ergibt sich aus dem Gesetz nicht.

Auch ist es gesetzlich nicht zugelassen, den Arbeitgebern die Ärzte namentlich zu benennen, die bei der Krankenkasse in den Verdacht geraten sind, übermäßig viele Arbeitsunfähigkeitsbescheinigungen auszustellen. Es handelt sich um personenbezogene Daten, die an Dritte nur weitergegeben werden dürfen, wenn ein Gesetz dies zulässt oder der Betroffene eingewilligt hat. Da beides nicht vorlag, hat die BKK Hamburg gegen das Datenschutzrecht verstoßen.

Im Rahmen unserer Aufsichtstätigkeit konnten wir zunächst erreichen, dass die BKK Hamburg zukünftig im Zusammenhang mit der Überprüfung der Arbeitsunfähigkeit von Versicherten keine Briefe mehr an Arbeitgeber mit einer Ärzteliste versendet. Damit war zwar der gerügte Mangel für die Zukunft behoben. Die eingetretene Datenschutzverletzung konnte dadurch aber nicht geheilt werden, weil bei den angeschriebenen Arbeitgebern die Daten weiterhin vorhanden sind. Deshalb haben wir die BKK Hamburg aufgefordert, die Arbeitgeber ein weiteres Mal anzuschreiben und darum zu bitten, die Arztdaten zu löschen.

Die BKK Hamburg weigerte sich nachhaltig, dieser Aufforderung nachzukommen. Erst nachdem wir diese Haltung nach § 25 Hamburgisches Datenschutzgesetz (HmbDSG) gegenüber dem Senator der Behörde für Umwelt und Gesundheit beanstandet haben, hat die Krankenkasse reagiert und ist in unserem Sinne tätig geworden. Damit ist der Datenschutzverstoß schließlich doch noch geheilt worden.

6.3 Projekt SAM der Allgemeinen Ortskrankenkassen

Die Pilotierung der ersten Module hat begonnen. Allerdings bereitet die hohe Integration der Altsysteme noch Schwierigkeiten.

Die Allgemeinen Ortskrankenkassen (AOK) betreiben mit dem AOK-Bundesverband, der AOK Systems GmbH und der SAP AG gemeinsam die Entwicklung einer neuen Software, die den künftigen Anforderungen der gesetzlichen Krankenversicherung entsprechen soll. Zu diesem Zweck ist das Projekt SAM (SAP-AOK-Master) installiert worden, das nach den bisherigen Planungen in ca. sechs Jahren abgeschlossen sein soll. Dann erst wird die bislang von der AOK eingesetzte Software IDVS II vollständig abgelöst werden. Die ersten

SAM-Module sind im Mai 2003 bei der AOK Mecklenburg-Vorpommern in die Pilotierung gegangen.

Die Datenschutzbeauftragten des Bundes und der Länder sind von der AOK-Organisation von Beginn an in die Planungen eingebunden worden und haben eigens für die datenschutzrechtliche Projektbegleitung eine Unterarbeitsgruppe ihres Arbeitskreises Gesundheit und Soziales eingesetzt. Die Federführung für diese Unterarbeitsgruppe haben wir übernommen.

Das Hauptaugenmerk unserer Projektbegleitung ist darauf gerichtet, dass die im derzeitigen IDVS II-Verfahren von den Datenschutzbeauftragten als problematisch angesehenen Punkte zufriedenstellend gelöst werden. Hierbei handelt es sich beispielsweise um den geschäftsstellenübergreifenden Zugriff auf Versichertendaten, die Trennung von Kranken- und Pflegeakten, die Einrichtung eindeutiger Zugriffs- und Berechtigungsverfahren sowie die ordnungsgemäße Archivierung, Sperrung und Löschung von Daten.

Im Berichtszeitraum ist die Unterarbeitsgruppe der Datenschutzbeauftragten auf Einladung des AOK-Bundesverbandes in mehreren Zusammenkünften über den Entwicklungsstand unterrichtet worden. Im Mai 2003 sind die Module Business-Partner (BP) und Customer Relationship Management (CRM) bei der AOK Mecklenburg-Vorpommern in die Pilotierung gegangen. Für die Anwender funktioniert die Software reibungslos. Die hohe Integration der Altsysteme des IDVS II bereitet allerdings noch technische Probleme. Deswegen wird sich der Einsatz der ersten Module bei der AOK Hamburg in das Jahr 2004 verschieben. Der Leistungsbereich, in dem die entscheidenden und sensiblen Versichertendaten verarbeitet werden, beginnt mit der Pilotierung voraussichtlich erst im Jahr 2005.

Unsere datenschutzrechtlichen Anforderungen an die Einführung des SAM-Programms haben wir sehr zeitig in einem Forderungskatalog zusammengefasst, der 21 Punkte beinhaltet. Beispielsweise geht es uns dabei um Folgendes:

- Es muss klar sein, inwieweit die einzelnen Krankenkassen von der Masterversion des Programms abweichen können. Die hierfür veränderbaren Verarbeitungsparameter müssen festgelegt werden.

- Die in dem Verfahren erfassbaren Personengruppen sind eindeutig zu definieren und die Rechtsgrundlagen für die Erfassung und weitere Verarbeitung der Daten sind zu benennen.

- Für alle Personengruppen und Datenkategorien sind Löschungsfristen bzw. Löschungskriterien festzulegen. Das Gleiche gilt für die Sperrung von Daten.

- Es ist vorzusehen, dass alle tatsächlich gespeicherten Daten (also auch die Historie) zu einer bestimmten Person zusammengefasst und beauskunftet werden können.
- Die Nutzung der Software ohne eine Vergabe von Berechtigungsprofilen ist zu unterbinden.
- Die Benutzerkonten und die in ihnen festgelegten Zugriffs- und Veränderungsrechte sind einschließlich der Historie so zu protokollieren, dass Veränderungen auch von der Administration nicht unbemerkt vorgenommen werden können.
- Jegliche Auswertung der Datenbestände, die Statistik- oder Kontrollzwecken dienen soll, darf nur mit anonymisierten bzw. pseudonymisierten Daten erfolgen.

Die AOK-Organisation arbeitet daran, die Umsetzung unserer Forderungen zu realisieren. Sofern der hierfür zu Grunde gelegte Zeitplan eingehalten werden kann, werden wir in der Lage sein, eine grundlegende datenschutzrechtliche Bewertung der ersten Module des SAM-Programms im Jahr 2004 vornehmen zu können. In unserem nächsten Tätigkeitsbericht werden wir darauf zurückkommen.

6.4 Prüfung der Landesunfallkasse

Die Verwaltungsabläufe und die automatisierte Verarbeitung entsprechen grundsätzlich den datenschutzrechtlichen Anforderungen. Ein Löschkonzept für die verarbeiteten Daten steht jedoch noch aus.

6.4.1 Allgemeines

Die Landesunfallkasse Hamburg (LUK) ist gesetzlicher Unfallversicherungsträger der Freien und Hansestadt Hamburg. Bei ihr sind mehr als 600.000 Menschen im Bundesland Hamburg versichert bei Arbeitsunfällen, Wegeunfällen und Berufskrankheiten. Sie ist eine Körperschaft des öffentlichen Rechts mit Selbstverwaltung. Die Aufgaben der LUK bestehen primär darin, Arbeitsunfällen, Berufskrankheiten und arbeitsbedingten Gesundheitsgefahren vorzubeugen, die Gesundheit nach einem Arbeitsunfall oder einer Berufskrankheit mit allen geeigneten Mitteln wiederherzustellen sowie die Versicherten oder ihre Hinterbliebenen durch Geldleistungen zu entschädigen.

Die Prüfung diente zum einen dazu, zwischenzeitlich im Verfahren eingetretene Veränderungen – insbesondere nach dem Inkrafttreten des Siebten Teil Sozialgesetzbuch (SGB VII) – zu berücksichtigen, die sich seit einer Prüfung aus dem Jahre 1995 (vgl. 14. TB, 5.1) ergeben haben. Zum anderen war diesmal der Fokus der Prüfung darauf gerichtet, ob die automatisierte Verarbeitung

von Sozialdaten bei der LUK den Anforderungen des § 78 a Zehnter Teil Sozialgesetzbuch (SGB X) entspricht.

6.4.2 Verwaltungsabläufe

Die Prüfung hat ergeben, dass die Verwaltungsabläufe und die von der LUK genutzten Formulare grundsätzlich den datenschutzrechtlichen Anforderungen entsprechen. Dies gilt auch für die Zusammenarbeit mit den anderen Leistungsträgern und für die neue Arbeitsweise bei Bagatellfällen, bei denen die LUK keine Einzelakten anlegt, sondern diese in Ordnern sammelt. Aufgrund unserer Anregung soll der in § 199 Abs. 3 SGB VII festgeschriebene Ersterhebungsgrundsatz in der Datenschutz-Dienstanweisung der LUK zusätzlich erläutert werden. Danach werden Auskünfte über Erkrankungen und frühere Erkrankungen von anderen Stellen oder Personen erst eingeholt, wenn hinreichende Anhaltspunkte für einen ursächlichen Zusammenhang zwischen der versicherten Tätigkeit und dem schädigenden Ereignis oder der schädigenden Einwirkung vorliegen.

In der Prüfung wurde auch die Regelung des § 200 Abs. 3 SGB VII angesprochen, wonach der Unfallversicherungsträger dem Versicherten vor Erteilung eines Gutachtenauftrages mehrere Gutachter zur Auswahl benennen soll. Der Betroffene ist außerdem auf sein Widerspruchsrecht nach § 76 Abs. 2 SGB X hinzuweisen und über den Zweck des Gutachtens zu informieren. Diese gesetzliche Verpflichtung wird nach den Worten der LUK durch eine entsprechende Vordruckgestaltung umgesetzt. Generell würden dem Versicherten drei Gutachter zur Auswahl benannt werden. Der Versicherte könne aber auch selbst einen Vorschlag unterbreiten. In jedem Fall sei der Wunsch des Versicherten maßgeblich. In den Fällen, in denen der Versicherte sich nicht meldet, würde die LUK den ersten der in der Liste aufgeführten Gutachter mit dem Gutachtenauftrag betrauen.

Die LUK akzeptiert zwar grundsätzlich das Vorschlagsrecht des Versicherten, lässt es aber weitgehend leer laufen, in dem sie mangels ausdrücklicher Regelung in § 200 Abs. 2 SGB VII nicht auf diese Berechtigung hinweist. Bereits auf Grund der allgemeinen Vorschrift des § 14 SGB I hat jedoch jeder Anspruch auf Beratung über seine Rechte und Pflichten nach dem Sozialgesetzbuch. Deshalb haben wir angeregt, das Anschreiben an den Versicherten dahingehend zu ergänzen, dass er berechtigt ist, selbst einen oder auch mehrere Gutachter vorzuschlagen.

Dem Gutachterauswahlrecht nach § 200 Abs. 2 SGB VII entspricht es im Übrigen nicht, wenn der Versicherte aus dem Einladungsschreiben oder erst bei seinem Erscheinen am Untersuchungstag erfährt, dass nunmehr ein anderer als der vom Versicherten ausgewählte Gutachter die Begutachtung vornehmen wird, weil der übereinstimmend ausgewählte Gutachter dazu – aus wel-

chen Gründen auch immer – nicht in der Lage ist. Bei Ausfall des ausgewählten Gutachters ist dem Versicherten erneut Gelegenheit für eigene Vorschläge zu geben.

Wegen der Bedeutung der Gutachterauswahl und der Vielzahl der damit zusammenhängenden datenschutzrechtlichen Fragen werden wir diese Problematik – losgelöst von der Prüfung – weiter mit der LUK erörtern.

6.4.3 Automatisierte Datenverarbeitung

Für die automatisierte Datenverarbeitung wird von der LUK seit dem 1. Januar 2000 das Verfahren GUSO (Gemeinsame UnfallversicherungsSOftware) eingesetzt, das im Auftrag des Bundesverbandes der Unfallversicherungsträger der öffentlichen Hand entwickelt wurde. Auch die Pflege und Wartung von GUSO erfolgt im Auftrag der Arbeitsgemeinschaft. Eine Verfahrensbeschreibung liegt vor. Die Anwendung wird in einer IuK-Infrastruktur betrieben, die dem Stand der Technik entspricht. Zu einzelnen Aspekten sind ergänzende technische und organisatorische Maßnahmen erforderlich, deren Umsetzung die LUK zum Teil auch bereits angekündigt hat.

- Ein Löschkonzept für die gespeicherten Sozialdaten besteht nicht. Da die Stammdaten auch aus dem Vorläuferverfahren übernommen wurden, sind in GUSO personenbezogene Daten seit 1990 gespeichert. Ein Löschkonzept soll bis zum Ende 2003 erstellt werden. Dieses gilt es zeitnah umzusetzen.

- Das bisherige Testkonzept bei der LUK entspricht nicht den datenschutzrechtlichen Anforderungen. Für die Tests steht zwar eine gesonderte Testumgebung zur Verfügung, die für die Überprüfung neuer Versionsstände genutzt wird. Die Testsachbearbeitung wird von ausgewählten Sachbearbeitern der LUK auf der Basis von Produktionsdaten durchgeführt. In der Testumgebung arbeiten die Sachbearbeiter bisher jedoch nicht mit ihrem jeweiligen Berechtigungsprofil aus der Produktionsumgebung, sondern sie haben einen Vollzugriff auf die Fälle. Die LUK hat angekündigt, zukünftig die Berechtigungen der Produktionsumgebung auf die Testumgebung zu übertragen.

- Der Zugangsschutz zu den Arbeitsplatzrechnern erfolgt durch Passworte. Die Mindestanforderungen an Passworte (vgl. 3.2) werden hinsichtlich der erforderlichen Komplexität und Gültigkeitsdauer nicht erfüllt. Die LUK wird die Anforderungen mit dem anstehenden Betriebssystemwechsel erfüllen.

- An einzelnen Arbeitsplätzen, die auch Zugang zu GUSO haben, steht zusätzlich ein Internetzugang zur Verfügung. An solchen Arbeitsplätzen, an

denen auch sensible personenbezogene Daten verarbeitet werden, sind zusätzliche Schutzmaßnahmen gegen Missbrauchsrisiken zu treffen, die bei Integration des Internet- und E-Mail-Zugangs an diesen Arbeitsplätzen bestehen (vgl. 3.6). Zur Reduzierung dieser Risiken besteht bei der LUK noch Handlungsbedarf.

6.5 Datenabgleich der Ämter für Ausbildungsförderung mit dem Bundesamt für Finanzen

Ohne eine entsprechende Rechtsgrundlage ist das Abgleichverfahren rechtswidrig, auch wenn damit der Missbrauch von Sozialleistungen aufgedeckt werden soll.

Die Ämter für Ausbildungsförderung – so auch das Studentenwerk Hamburg – sind bundesweit fast ausnahmslos dazu übergegangen, einen Datenabgleich mit dem Bundesamt für Finanzen (BfF) durchzuführen, um die von den Antragstellern und Leistungsbeziehern gemachten Angaben über Einkünfte und anrechenbares Vermögen zu überprüfen. Hierzu übermittelt das Studentenwerk die Namen und andere identifizierende Daten derjenigen Personen an das BfF, die Leistungen nach dem Bundesausbildungsförderungsgesetz (BAföG) beantragen bzw. erhalten. Das BfF gleicht die Angaben mit den bei ihm vorhandenen Daten über die Höhe der gemäß Freistellungsauftrag tatsächlich in Anspruch genommenen Freistellungen von der Zinsabschlagsteuer ab und unterrichtet in den Treffer-Fällen das Studentenwerk über den Betrag.

Die vom Studentenwerk übermittelten Angaben unterliegen als Sozialdaten nach den §§ 11 und 18 SGB I den Regelungen der Sozialgesetzbücher und unterfallen damit dem in § 35 Abs. 1 SGB I normierten Sozialgeheimnis. Die Erhebung, Verarbeitung und Nutzung dieser Sozialdaten ist nach § 35 Abs. 2 SGB I nur unter den Voraussetzungen des 2. Kapitels des SGB X zulässig. Dort bestimmt § 67 d Abs. 1, dass eine Übermittlung von Sozialdaten nur in Betracht kommt, soweit eine gesetzliche Übermittlungsbefugnis nach den §§ 68 bis 77 SGB X oder nach einer anderen Rechtsvorschrift in diesem Gesetzbuch vorliegt.

Für die im ersten Schritt erforderliche Übermittlung der Daten von den Ämtern für Ausbildungsförderung an das BfF fehlt es an einer solchen Norm. Insbesondere kann § 45 d Einkommensteuergesetz (EStG) die fehlende Befugnisnorm im Bereich des SGB X nicht ersetzen. In § 45d Abs. 3 EStG ist zwar geregelt, dass das BfF den Sozialleistungsträgern bestimmte Daten mitteilen darf, soweit dies zur Überprüfung des bei der Sozialleistung zu berücksichtigenden Einkommens oder Vermögens erforderlich ist. Diese Vorschrift legitimiert je-

doch nicht die Ämter für Ausbildungsförderung, die Sozialdaten an das BfF zu übermitteln. Der Gesetzgeber ist deshalb gefordert, eine geeignete Befugnisnorm zu schaffen.

Wie eine solche Befugnisnorm aussehen könnte, lässt sich für den Bereich der Sozialhilfe den Regelungen des § 117 Bundessozialhilfegesetz (BSHG) entnehmen. Nach § 117 Abs. 1 Satz 1 Nr. 3 BSHG sind die Träger der Sozialhilfe befugt, Personen, die Leistungen nach diesem Gesetz beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin zu überprüfen, ob und welche Daten nach § 45 d Abs. 1 EStG dem BfF übermittelt worden sind. Ferner sind die Träger der Sozialhilfe nach § 117 Abs. 2 Satz 1 BSHG befugt, Personen, die Leistungen nach diesem Gesetz beziehen, auch regelmäßig im Wege des automatisierten Datenabgleichs daraufhin zu überprüfen, ob und in welcher Höhe und für welche Zeiträume von ihnen Leistungen nach diesem Gesetz durch andere Träger der Sozialhilfe bezogen werden oder wurden. Nach § 117 Abs. 1 Satz 2 BSHG dürfen hierzu die erforderlichen Daten anderen Sozialhilfeträgern oder einer zentralen Vermittlungsstelle – das ist das BfF – übermittelt werden.

Nach alledem entspricht das Abgleichverfahren der Ämter für Ausbildungsförderung mit dem BfF nicht den datenschutzrechtlichen Anforderungen. Zwar gehen auch wir davon aus, dass dieser Datenabgleich angesichts des offenbar festgestellten erheblichen Missbrauchs wünschenswert sein kann. Dies ändert jedoch nichts daran, dass die erforderliche Rechtsgrundlage für einen derartigen Datenabgleich zur Zeit nicht gegeben ist. Solange dies nicht erfolgt ist, ist der Datenabgleich in dieser Form nicht rechtmäßig.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat sich im September 2003 mit dieser Angelegenheit befasst und unsere Rechtsposition bestätigt. Klargestellt wurde auch, dass die fehlende Regelung vorzugsweise im BAföG erfolgen sollte. Darüber hinaus hat es die Konferenz zur Vermeidung von Missverständnissen und zur Vorbeugung von fehlerhaften Erklärungen für erforderlich gehalten, die BAföG-Antragsteller bereits im Antragsformular deutlich auf den Datenabgleich hinzuweisen. Der Bundesbeauftragte für den Datenschutz hat diese Rechtsposition den beteiligten Bundesministerien übermittelt.

Die Behörde für Wissenschaft und Forschung (BWF) wurde von uns frühzeitig auf die geschilderte Rechtsproblematik hingewiesen. Wir konnten erreichen, dass sich die BWF für eine Änderung des BAföG in unserem Sinne einsetzen will. Das Datenabgleichverfahren wurde jedoch in Hamburg nicht eingestellt. Von einer datenschutzrechtlichen Beanstandung dieser Praxis haben wir nur deshalb abgesehen, weil nach Auskunft der BWF das Problem im Rahmen der für 2004 anstehenden BAföG-Novellierung gelöst werden soll.

7. Personaldaten

7.1 Outsourcing für Beihilfe und Versorgungsleistungen

Die datenschutzrechtlichen Probleme beim Outsourcing der Bearbeitung von Beihilfe, freier Heilfürsorge und Versorgungsleistungen sind noch nicht abschließend geklärt.

Der Senat prüft, ob bestimmte Aufgaben an private Stellen ausgelagert werden können. Aus datenschutzrechtlicher Sicht sind die Überlegungen zur Auslagerung der Bearbeitung von Beihilfe, freier Heilfürsorge und Versorgungsleistungen von besonderer Bedeutung.

Personenbezogene Daten von Beschäftigten können im Wege der Auftragsdatenverarbeitung nach § 3 HmbDSG durch andere Stellen verarbeitet werden. Dabei sind folgende Kriterien wichtig:

- Es erfolgt nur eine technische Unterstützung.
- Für die Einhaltung datenschutzrechtlicher Vorschriften ist der Auftraggeber allein verantwortlich.
- Adressat der Rechte der Betroffenen bleibt die Daten verarbeitende Stelle.
- Die Daten verarbeitenden Stellen haben den auftragnehmenden Stellen die entsprechenden Weisungen zu erteilen.

Wenn die Leistungsbeschreibung eines Vertrages auch sachbearbeitende Tätigkeiten beinhaltet, wird nicht nur die Datenverarbeitung als Hilfstätigkeit übertragen. Dies ist insbesondere dann der Fall, wenn folgende Leistungen erbracht werden sollen, die sich nicht auf die technische Hilfeleistung beschränken:

- Berechnung der Beihilfeleistungen, Leistungen der freien Heilfürsorge oder des Ruhegeldes
- Übernahme des Schriftwechsels für notwendige amts- oder vertrauensärztliche Begutachtungen

Hier ist eine selbständige Erledigung durch den Auftragnehmer vorgesehen. In solchen Fällen liegt eine Aufgabenübertragung vor. Für die Beurteilung, ob es sich um Auftragsdatenverarbeitung handelt, ist nicht ausschlaggebend, dass der Beihilfebescheid namens und im Auftrag des Auftraggebers erstellt wird und die Auszahlung von ihm selbst veranlasst wird. Maßgebend ist allein die absolute Weisungsgebundenheit des Auftragnehmers, die bei einer solchen Vertragsgestaltung nicht vorliegt.

Als Rechtsgrundlage für die Übermittlung von Personaldaten kommt andererseits § 28 Abs. 1 HmbDSG in Betracht. Danach können personenbezogene Daten von Beschäftigten verarbeitet werden, soweit dies eine Rechtsvorschrift, ein Tarifvertrag, eine allgemeine Regelung der obersten Dienstbehörde, die mit

den Spitzenorganisationen der zuständigen Gewerkschaften und Berufsverbände beziehungsweise mit den Berufsverbänden der Richterinnen und Richter verbindlich vereinbart worden ist, oder eine Dienstvereinbarung vorsieht. Wenn z. B. vorrangige Rechtsvorschriften zur Verarbeitung personenbezogener Daten vorliegen, wäre demgemäß die Übermittlung von Personaldaten zulässig.

> § 28 Abs. 4 HmbDSG:
>
> Eine Übermittlung der Daten von Beschäftigten an Stellen außerhalb des öffentlichen Bereichs ist nur zulässig, soweit
>
> 1. die Stelle, der die Daten übermittelt werden sollen, ein überwiegendes rechtliches Interesse darlegt,
> 2. Art und Zielsetzung der Aufgaben, die der oder dem Beschäftigten übertragen sind, die Übermittlung erfordert oder
> 3. offensichtlich ist, dass die Übermittlung im Interesse der betroffenen Person liegt, und keine Anhaltspunkte vorliegen, dass diese in Kenntnis des Übermittlungszweckes ihre Einwilligung nicht erteilen würde.

Wenn eine Übermittlung der Daten von Beschäftigten an nicht öffentliche Stellen erfolgen soll, ist sie nur nach den vorstehenden Kriterien des § 28 Abs. 4 HmbDSG zulässig. Diese Zulässigkeitstatbestände liegen bei der Auslagerung der Bearbeitung von Beihilfe, freier Heilfürsorge und Versorgungsleistungen nicht vor.

Zulässig wäre eine Übermittlung, wenn jeder Mitarbeiter einwilligen würde. Dies dürfte jedoch aus praktischen Erwägungen nicht möglich sein. Die weitere Klärung, auf welcher Rechtsgrundlage derartige Auslagerungen praktiziert werden sollen, bleibt unter Beteiligung insbesondere des Personalamtes abzuwarten.

7.2 Telearbeit

Aus datenschutzrechtlicher Sicht gibt es auch weiterhin keine grundsätzlichen Bedenken gegen den Zugriff von häuslichen Bildschirmarbeitsplätzen auf besonders sensible personenbezogene Daten in Fachanwendungen der hamburgischen Verwaltung.

Im Berichtszeitraum erhielten wir erneut zahlreiche Anfragen von Mitarbeitern und Vorgesetzten in der hamburgischen Verwaltung zur Zulässigkeit von Telearbeit in Bereichen mit sensiblen personenbezogenen Daten. Wir haben dabei auf unsere ausführliche Darstellung des Themas im 18. TB, 3.9 verwiesen. Wenn alle verbindlichen Rahmenbedingungen eingehalten werden, bestehen aus unserer Sicht grundsätzlich keine Bedenken gegen häusliche Telearbeits-

plätze mit direktem Zugriff auf IuK-Anwendungen der Verwaltung. Solange bereichsspezifische Rechtsvorschriften es nicht konkret ausschließen, können auch besonders sensible personenbezogene Daten im Rahmen von Telearbeit verarbeitet werden.

Zur Zeit gibt es bereits über 100 Telearbeitsplätze in der hamburgischen Verwaltung. Anfang September 2003 startete z. B. ein Modellversuch zur Einbeziehung von Publikumsdienststellen. Mehrere Mitarbeiterinnen und Mitarbeiter des Sozialamtes Eimsbüttel können ihre Aufgaben an zwei Tagen in der Woche auch von ihrem häuslichen Arbeitsplatz wahrnehmen.

Die vom Landesamt für Informationstechnik gewährleisteten Sicherheitsanforderungen für die technische Anbindung der Telearbeitsplätze an das Netz der hamburgischen Verwaltung werden ständig überwacht und weiterentwickelt. Daran werden wir umfassend beteiligt.

8. Statistik

Fusion der Statistischen Landesämter Hamburg und Schleswig-Holstein

Im Staatsvertrag über die Zusammenführung der Statistischen Landesämter zu einer gemeinsamen Anstalt ist auch das Datenschutzrecht angemessen geregelt worden.

Die Länder Hamburg und Schleswig-Holstein haben vereinbart, aus Gründen der Wirtschaftlichkeit, Effizienz und Effektivität ihre bestehende Zusammenarbeit auf dem Gebiet der amtlichen Statistik zu vertiefen. Aus diesem Grund sollen die Statistischen Landesämter Hamburg und Schleswig-Holstein mit Wirkung vom 1. Januar 2004 zu einer gemeinsamen Einrichtung in der Rechtsform einer Anstalt des öffentlichen Rechts zusammengeführt werden. Die Bürgerschaft hat das Gesetz zum Staatsvertrag über die Zusammenführung der beiden Landesämter am 26. November 2003 beschlossen.

In dem Staatsvertrag ist u.a. vorgesehen, dass die gemeinsame Anstalt mit dem Namen „Statistisches Amt für Hamburg und Schleswig-Holstein – Anstalt des öffentlichen Rechts“ ihren Sitz in Hamburg hat und Standorte in Kiel und Hamburg unterhält. Für die Einrichtung und den Betrieb der Anstalt gilt hamburgisches Landesrecht, soweit in diesem Staatsvertrag nichts anderes bestimmt ist. Damit wird gleichzeitig zum Ausdruck gebracht, dass für die Verarbeitung personenbezogener Daten bei der Anstalt grundsätzlich das Hamburgische Datenschutzgesetz anzuwenden ist.

Da von dieser Regelung auch das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein betroffen ist, haben wir im Vorwege der Behördenabstimmung mit unseren Kollegen in Schleswig-Holstein und den für die statistischen Landesämtern zuständigen Innenressorts abgestimmt, welche Regelung zum Datenschutz in den Staatsvertrag aufgenommen werden soll. Die datenschutzrechtliche Bestimmung lautet dementsprechend:

§ 14 Datenschutz

(1) Für die Verarbeitung personenbezogener Daten durch die Anstalt gelten die Vorschriften des Hamburgischen Datenschutzgesetzes (HmbDSG) mit Ausnahme des § 2 Absatz 2. Die Anstalt bestellt eine behördliche Datenschutzbeauftragte oder einen Datenschutzbeauftragten nach § 10 a HmbDSG.

(2) Die oder der Hamburgische Datenschutzbeauftragte und das Unabhängige Landeszentrum für Datenschutz können sich einvernehmlich gegenseitig mit der Durchführung der Überwachung beauftragen.

Mit der Regelung des Absatz 1 wird u.a. bestimmt, dass das HmbDSG auch dann anzuwenden ist, wenn die Anstalt Daten für öffentliche Stellen in Schleswig-Holstein verarbeitet. Es findet auch Anwendung, soweit die Anstalt als Unternehmen am Wettbewerb teilnimmt; die gegenteilige Vorschrift des § 2 Abs. 2 HmbDSG gilt deshalb nicht. Nach Absatz 2 können sich die oder der Hamburgische Datenschutzbeauftragte und das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein z. B. bei Prüfungen in Schleswig-Holstein auch mit Wirkung gegenüber der Anstalt mit der Durchführung der Überwachung beauftragen.

9. Finanzen und Steuern

9.1 Ressourcensteuerung mit SAP R/3

Mit einer Verordnung nach § 11 a Hamburgisches Datenschutzgesetz (HmbDSG) ist die Führung von Einheitspersonenkonten im SAP/R3-Verfahren zur integrierten Ressourcensteuerung auf eine datenschutzrechtliche Grundlage gestellt worden.

Das zentrale IuK-Verfahren für die integrierte Ressourcensteuerung „sap für hamburg“ (18. TB, 3.2.3) stellt die bislang auf unterschiedlichen Betriebssystemen und Softwareprodukten laufenden Haushalts- und Kassenanwendungen auf eine Hamburgweit einheitliche Basis. Namen, Anschriften und Bankverbindungen der in Zahlungsvorgängen auftretenden Firmen und Einzelpersonen – hierzu gehören auch die Mitarbeiterinnen und Mitarbeiter der Verwaltung, soweit sie z. B. die Kosten für Dienstreisen erstattet bekommen – werden dabei nur noch einmal in einer einzigen Datei gespeichert. Darauf erhalten alle mittelbewirtschaftenden Stellen der hamburgischen Verwaltung unabhängig von ihrem jeweiligen Aufgabenbereich einen lesenden Zugriff.

Damit wird aus Sicht der Finanzbehörde die Kassenführung erheblich erleichtert. Die Anwenderinnen und Anwender von „sap für hamburg“ (z. Z. insgesamt etwa 3.300 berechtigte SAP-User, davon ein sehr großer Anteil mit den Befugnissen zur Mittelbewirtschaftung) können sich so vor der Neuanlage eines

Debitoren- oder Kreditorenstammdatensatzes davon überzeugen, dass ein solcher Stammdatensatz nicht bereits im System vorhanden ist. Ein behördenübergreifender lesender Zugriff auf Einzelheiten des jeweiligen Zahlungsvorgangs über die aufgabenbezogenen behörden- und ämterspezifischen Buchungskreise hinaus wird zwar durch eine restriktive Berechtigungsvergabe verhindert. Es besteht aber jederzeit die Möglichkeit, unabhängig von der jeweiligen Zuständigkeit auf die Anschriften und Bankverbindungen aller Zahlungsempfänger und Schuldner der gesamten Verwaltung zuzugreifen.

Gemäß § 11 a HmbDSG bedarf die Einrichtung gemeinsamer oder verbundener automatisierter Dateien, in oder aus denen mehrere Daten verarbeitende Stellen personenbezogene Daten verarbeiten sollen, der ausdrücklichen Zulassung durch eine Rechtsvorschrift. Für die bereits in allen Behörden und Ämtern betriebene Einrichtung und Nutzung der Einheitspersonenkonten ist nunmehr am 7. Oktober 2003 die „Verordnung über die gemeinsame Personenkontendatei des ressourcensteuernden Verfahrens“ (HmbGVBl. S. 492) vom Senat erlassen worden. In ihr werden die zu verarbeitenden Daten und alle beteiligten Stellen mit dem Umfang ihrer Verarbeitungsbefugnis angegeben sowie die datenschutzrechtliche Verantwortung festgelegt.

9.2 Pfändung von Kraftfahrzeugen mit einer Parkkralle

Die Ausweitung des Verfahrens auf andere rückständige Steuern ist datenschutzrechtlich vertretbar.

Die Finanzbehörde hat den Einsatz von Wegfahrsperren (sog. Parkkrallen) zwecks Beitreibung rückständiger Kraftfahrzeugsteuern im Rahmen eines 6-monatigen Pilotversuchs beim Finanzamt für Verkehrssteuern und Grundbesitz getestet. Dieser Pilotversuch wurde mit uns abgestimmt und ist nach Auffassung der Finanzbehörde erfolgreich verlaufen. Aus diesem Grund soll die Parkkralle nicht nur zur Beitreibung von rückständigen Kraftfahrzeugsteuern, sondern auch von anderen Steuerarten dauerhaft zum Einsatz kommen.

Solch ein Verfahren hat datenschutzrechtliche Relevanz, weil durch die Anbringung des Pfandsiegels und der Parkkralle eines auf öffentlichen Straßen oder Plätzen geparkten Kraftfahrzeugs in der Öffentlichkeit bekannt wird, dass hier eine Pfändungsmaßnahme des zuständigen Finanzamtes gegen einen Vollstreckungsschuldner durchgeführt wird.

Rechtsgrundlage für die Vollstreckung von Kraftfahrzeugen säumiger Steuerzahler und das Anbringen der Parkkralle ist § 286 Abgabenordnung (AO). Nach Absatz 1 dieser Vorschrift hat der Vollziehungsbeamte bewegliche Sachen, die sich im Gewahrsam des Vollstreckungsschuldners befinden, dadurch zu pfänden, dass er sie in seinen Besitz nimmt (Wegnahme). Absatz 2 bestimmt, dass andere Sachen als Geld, Kostbarkeiten und Wertpapiere im Gewahrsam des Vollstreckungsschuldners zu

lassen sind, wenn die Befriedigung hierdurch nicht gefährdet wird. Bleiben die Sachen im Gewahrsam des Vollstreckungsschuldners, so ist die Pfändung nur wirksam, wenn sie durch Anlegung eines Pfandsiegels oder in sonstiger Weise ersichtlich gemacht ist.

Bei der Pfändung von Kraftfahrzeugen, die mit Einverständnis der Vollstreckungsstelle (zuständiges Finanzamt) im Gewahrsam des Vollstreckungsschuldners verbleiben, wird in der Regel davon ausgegangen, dass die Befriedigung des Vollstreckungsgläubigers gefährdet ist, weil Fahrzeuge verhältnismäßig leicht fortgeschafft werden können. Ist das Kraftfahrzeug, wie allgemein üblich, auf der Straße abgestellt, kann der Vollziehungsbeamte das Entfernen des Fahrzeugs durch das Anbringen einer Parkkralle verhindern.

Voraussetzung hierfür ist, dass zunächst überhaupt eine wirksame Pfändung des Fahrzeugs vorliegt, die durch Anlegung von Pfandsiegeln oder in sonstiger Weise (z. B. Anbringung einer Pfandanzeige) ersichtlich gemacht ist. Denn für eine isolierte Verwendung der Parkkralle (ohne Pfändung und Pfandsiegel) gibt es keine rechtliche Legitimation.

Die Pfändung eines Kraftfahrzeugs darf gemäß § 254 Abs. 1 AO jedoch erst erfolgen, wenn die Leistung fällig ist und der Vollstreckungsschuldner zur Leistung aufgefordert worden ist (Leistungsgebot) und seit der Aufforderung mindestens eine Woche verstrichen ist. Außerdem muss sie verhältnismäßig, d.h. geeignet, erforderlich und angemessen sein, insbesondere hinsichtlich der Verwendung der Parkkralle wegen der dabei möglichen Prangerwirkung.

Weiterhin ist vor dem Anbringen des Pfandzeichens und der Parkkralle durch den Vollziehungsbeamten stets zu prüfen, ob das Kraftfahrzeug nicht ein „zur Fortsetzung der Erwerbstätigkeit erforderlicher Gegenstand“ des Vollstreckungsschuldners ist, der gemäß § 811 Nr. 5 Zivilprozessordnung (ZPO) unpfändbar ist. Bei dieser Gelegenheit kann der Vollziehungsbeamte den Vollstreckungsschuldner auch darauf hinweisen, dass sein Fahrzeug zwecks Betreibung der ausstehenden Steuerschuld ggf. durch Wegnahme gepfändet wird, es sei denn, dass sich für den Vollziehungsbeamten Erkenntnisse ergeben, dass der Schuldner innerhalb von 3 Tagen die Steuerschuld begleichen kann. Zur Gewährleistung, dass das Fahrzeug zwischenzeitlich nicht entfernt wird, kann eine Festsetzung des Fahrzeugs mittels Parkkralle sinnvoll sein. Erfolgt innerhalb dieses Zeitraumes keine Befriedigung, ist das Fahrzeug aus dem Verkehr zu nehmen.

Werden diese Voraussetzungen erfüllt, so sind auch die Pfändung mit einer Parkkralle und die zwangsläufig damit verbundene Datenübermittlung an solche Personen datenschutzrechtlich zulässig, die den Eigentümer des mit dem Pfandsiegel und der Parkkralle versehenen Fahrzeugs kennen (z. B. Nachbarn).

Der Finanzbehörde haben wir mitgeteilt, dass wir eine Ausweitung des Verfahrens für datenschutzrechtlich vertretbar halten, soweit dieses – wie beim Pilotprojekt – durch gesetzliche Vorschriften gedeckt ist und dabei der Grundsatz der Verhältnismäßigkeit gewahrt wird. Aus diesem Grund müssen in jedem Fall die gesetzlichen Voraussetzungen für die Vollstreckung (z. B. Leistungsbescheid, Fälligkeit der Leistung) und die Pfändung des Kraftfahrzeugs (z. B. Anbringen des Pfandsiegels) vorliegen. Weiterhin darf es sich bei den ausstehenden Steuerschulden nicht um geringfügige Beträge handeln und andere Vollstreckungsversuche (z. B. Lohnpfändungen) müssen trotz intensiver und langandauernder Bemühungen erfolglos geblieben sein. Außerdem sollte der Einsatz der Parkkralle wie beim Pilotprojekt auf 3 Tage beschränkt bleiben.

10. Schule und Universität

10.1 Regionale Beratungs- und Unterstützungsstellen (REBUS)

Die neue Konzeption der Beratung, Unterstützung und Förderung bei schulischen Problemlagen ist verwirklicht worden, ohne uns systematisch an der Projektentwicklung zu beteiligen.

Seit dem 1. Oktober 2000 werden in 15 Regionalen Beratungs- und Unterstützungsstellen (REBUS) die Aufgaben und Dienstleistungen gebündelt und wahrgenommen, die vorher von der Schülerhilfe, den Schulen für Verhaltensgestörte, den Schulstellen der schulischen Erziehungshilfe, den Psychologinnen und Psychologen der Gesamtschulen und einem Teil der Mitarbeiterinnen und Mitarbeiter des Haus- und Krankenhausunterrichts bearbeitet wurden. REBUS sind Organisationseinheiten einer Dienststelle des Amtes für Bildung der Behörde für Bildung und Sport (BBS), sie sind keine Schulen. Sie haben jeweils eine eigene Leitung und eine Leitungsvertretung. Alle REBUS unterstehen einer eigenen Fach- und Dienstaufsicht und sie haben eine zentrale Verwaltungseinheit. Bei REBUS sind regelmäßig Schulpsychologen, Lehrkräfte/Sonderpädagogen und Sozialpädagogen sowie eine Verwaltungskraft tätig. Grundsätzlich sollen die drei Berufsgruppen der Fachkräfte mit jeweils zwei Mitgliedern vertreten sein.

Neben den verschiedenen Möglichkeiten, die REBUS zur Überwindung von schulischen Problemlagen durch Beratung und Unterstützung anbieten kann, sind die REBUS auch für die Verfolgung von Schulpflichtverletzungen zuständig. In besonders schwierigen Fällen können dazu schulersetzende Maßnahmen als Hilfe zur Reintegration und die Einbeziehung von problemlösenden Beiträgen der Jugendhilfe gehören. Wird innerhalb einer bestimmten Frist keine deutliche Verbesserung des Schulbesuchs erzielt, hat REBUS den Einsatz von geeigneten rechtlichen Maßnahmen (Mittel des Verwaltungszwangs, Bußgeld, Strafverfahren) vorzubereiten.

Im Hinblick auf das breitgefächerte Aufgabenspektrum arbeiten die REBUS mit einer Vielzahl von Stellen zusammen. Dazu gehören Kindergärten und Tagesheime, Ärzte, Therapeuten, Kureinrichtungen und Kliniken, eine Vielfalt von Beratungsstellen, verschiedene Ämter, Träger und Einrichtungen offener Jugendarbeit, Wohngruppen und Heime sowie die Polizei. Hauptpartner in der Zusammenarbeit sind die Allgemeinen Sozialen Dienste (ASD), Jugendämter, Gesundheitsämter, der Jugendpsychiatrische Dienst (JPD), Kinder- und Familienzentren und andere regionale Hilfezentren.

Im Rahmen ihrer Beratungstätigkeit sind die REBUS ihren Klienten gegenüber zur persönlichen Verschwiegenheit verpflichtet. In diesem Zusammenhang muss die Einwilligung des Betroffenen oder seiner Erziehungsberechtigten eingeholt werden, wenn es um die Erhebung und Übermittlung von Daten geht.

Was die Dokumentation der Fallarbeit von REBUS angeht, sind wir wegen einzelner Fragestellungen zur Vordruckgestaltung um Stellungnahme gebeten worden. Regelhaft sind wir jedoch nicht an der Projektentwicklung beteiligt worden. Deshalb haben wir in der zweiten Hälfte des Berichtszeitraumes die Tätigkeit der REBUS einer datenschutzrechtlichen Querschnittsüberprüfung unterzogen. Bis zum Redaktionsschluss war diese Prüfung zwar noch nicht beendet, aber es zeigt sich, dass einige Belange des Datenschutzes bei der Projektentwicklung nicht bedacht worden sind.

So ist die gleichzeitige Aufgabenwahrnehmung von Beraten und Bestrafen problematisch, weil die Beratung auf der Basis freiwillig preisgegebener Daten beruht und diese Informationen nicht ohne Einwilligung für Erziehungs- und Ordnungsmaßnahmen nach § 49 Hamburgisches Schulgesetz (HmbSG) oder für die Verfolgung von Ordnungswidrigkeiten und Straftaten (§§ 113, 114 HmbSG) genutzt werden dürfen. Es gibt auch keine einheitliche Praxis in den REBUS zur Reichweite der Schweigepflicht nach § 203 Strafgesetzbuch (StGB) gegenüber Kollegen, Dienstvorgesetzten, der Fachaufsicht und der Innenrevision. Kritisch ist ebenfalls, dass die REBUS für ihren jeweiligen Zuständigkeitsbereich eigene EDV-Systeme für die Fallbearbeitung und Falldokumentation entwickelt haben, ohne vorher die damit verbundenen Gefährdungen für die Persönlichkeitsrechte der Betroffenen nachvollziehbar und abschließend geklärt zu haben. Um diesen „Wildwuchs“ zu beseitigen, entwickelt eine eigens hierfür von der BBS eingesetzte Projektgruppe ein für alle REBUS verbindliches einheitliches Programmsystem zur Unterstützung der Fallbearbeitung, statistischer Auswertungen und der Anfragenerfassung. An dieser Entwicklung sind wir jetzt beteiligt.

Auf das Ergebnis der REBUS-Querschnittsprüfung werden wir im nächsten Tätigkeitsbericht näher eingehen.

10.2 Technikunterstützung im Verwaltungsbereich der allgemeinbildenden Schulen (TUVAS)

Die datenschutzrechtlichen Risiken müssen bei Verfahrensänderungen auf der Grundlage der aktuell eingesetzten Technik neu bewertet werden.

Im Rahmen des Projektes TUVAS sollen die Schulbüros der staatlichen allgemeinbildenden Schulen mit einheitlicher Hard- und Software ausgestattet werden, um die Leistungsfähigkeit dieser Schulen bei den vielfältigen Planungs- und Steuerungsaufgaben in der Schulverwaltung zu unterstützen und zu fördern. Wir haben das Verfahren in den vergangenen Jahren datenschutzrechtlich begleitet (vgl. 17. TB, 9.1 und 18. TB, 14.1). Das Projekt ist nunmehr so weit vorangeschritten, dass die Schulen mit der erforderlichen Hardware ausgestattet und das Schulverwaltungsprogramm „Lehrer- und Schülerdatenbank“ (LUSD) für die überwiegende Anzahl der Arbeitsplätze in der Schulverwaltung ausgeliefert werden konnte.

Das mit uns abgestimmte Schutzkonzept für den dezentralen Einsatz der LUSD auf den Verwaltungsrechnern der Schulen beinhaltete

- eine dezentrale Datenhaltung in den Schulen,
- die physikalische Trennung des Verwaltungsnetzes vom pädagogischen Netz,
- den Verzicht auf Internetanbindung und E-Mail ohne zusätzliche Sicherheitsvorkehrungen sowie
- die Verschlüsselung bei einem Datenaustausch personenbezogener Daten.

Trotz unserer langjährigen datenschutzrechtlichen Begleitung des Projektes haben wir kurz vor Ende des Berichtszeitraumes lediglich zufällig erfahren, dass bereits 26 Schulen über ein virtuelles Netzwerk mit der IT-Infrastruktur der hamburgischen Verwaltung (FHHinfoNet) verbunden wurden. 16 dieser Schulen erproben den Zugriff über einen Windows Terminal Server (WTS) im Landesamt für Informationstechnik (LIT), ohne dass wir an dieser elementaren Verfahrensänderung – nämlich der Abkehr von einer dezentralen Datenhaltung – beteiligt oder die mit der aktuellen Technik verbundenen Risiken von den Projektverantwortlichen neu bewertet wurden. Auch die Verfahrensbeschreibung wurde nicht entsprechend angepasst.

Wir haben daher Gespräche mit dem Projekt geführt und angemahnt, die maßgeblichen Bestimmungen des § 8 Abs. 4 und § 9 Hamburgisches Datenschutzgesetz künftig zu beachten. Dies wurde uns von den Verantwortlichen zugesichert und sowohl eine entsprechende Überarbeitung der Risikoanalyse als auch der Verfahrensbeschreibung angekündigt. Bis zum Redaktionsschluss lagen uns beide Unterlagen noch nicht vor.

Auf der Grundlage der bisherigen Gesprächsergebnisse zeichnet sich jedoch ab, dass die angestrebte zentrale Datenhaltung weniger datenschutzrechtliche Risiken beinhalten würde.

Wir haben darauf hingewiesen, dass die Schulen personenbezogene Daten per E-Mail im FHHInfoNet wegen ihrer Sensibilität nur versenden dürfen, wenn die hierfür zur Verfügung stehenden Verschlüsselungstechniken („Erweiterte Sicherheit“) genutzt werden. Der Zugriff auf das Internet darf nur über den WTS im LIT erfolgen.

Die Projektverantwortlichen haben auf unsere Hinweise insgesamt konstruktiv reagiert, so dass wir davon ausgehen, dass unsere weitere Beteiligung an der Verfahrensentwicklung so verläuft, wie es die Richtlinien vorsehen.

10.3 Projekt Hoch7 der Universität Hamburg

Entgegen der gesetzlichen Anforderungen ist eine Produktionsaufnahme vor der Erstellung einer Risikoanalyse erfolgt.

Die sechs Hamburger Hochschulen und die Staats- und Universitätsbibliothek Carl von Ossietzky haben sich im November 2000 zum Hamburger Hochschul-Kooperationsmodell (HHKM) zusammengeschlossen. Ein gemeinsames Ziel war die Einführung des kaufmännischen Rechnungswesens auf der Basis der Standardsoftware SAP R/3. Zur Planung und Realisierung dieses IuK-Vorhabens wurde das Projekt Hoch7 eingesetzt. Neben der Entwicklung eines Referenzmandanten und eines Berechtigungskonzeptes für alle beteiligten Institutionen beinhaltete das Projekt weitere grundlegende Veränderungen wie den Aufbau eines zentralen SAP-Rechenzentrums, den Aufbau und Betrieb eines VPN-Verwaltungsnetzes sowie die Entwicklung eines Hoch7-Standard PC für die Arbeitsplätze in den Verwaltungsbereichen der Kooperationspartner.

Unsere nach § 23 Abs. 4 Satz 2 Hamburgisches Datenschutzgesetz (HmbDSG) erforderliche Beteiligung erfolgte leider erst zu einem bereits fortgeschrittenen Planungsstand und blieb auf Einzelaspekte des Verfahrens wie Fragen zur Netzarchitektur und zum Berechtigungskonzept beschränkt. Die angekündigte Vorlage eines umfassenden Hoch7-Sicherheitskonzeptes ist bisher ebenso unterblieben wie die Vorlage einer Risikoanalyse gemäß § 8 Abs. 4 HmbDSG und einer Verfahrensbeschreibung nach § 9 HmbDSG, obwohl wir die Projektverantwortlichen wiederholt an die Vorlage der Unterlagen erinnert haben.

Zum Jahresbeginn 2003 haben die Kooperationspartner den SAP-Produktiv-Betrieb aufgenommen. Damit wurde gegen die Bestimmungen des § 8 Abs. 4 HmbDSG verstoßen, welche die Daten verarbeitenden Stellen verpflichtet, bereits vor der Entscheidung über die Einführung eines neuen DV-Verfahrens eine Risikoanalyse durchzuführen.

Die Aufgabe der Erstellung der gesetzlich erforderlichen Unterlagen wurde nunmehr auf das SAP-Rechenzentrum des Regionalen Rechenzentrums der Universität übertragen.

Von dort wurden die Unterlagen zügig erstellt und kurz vor Redaktionsschluss zugeleitet.

Das ändert jedoch nichts daran, dass die Projektverantwortlichen durch die bisherige Behandlung der Angelegenheit den Rechtsgedanken des vorgezogenen Datenschutzes missachtet haben. Sinn und Zweck der Regelung des § 8 Abs. 4 HmbDSG ist es gerade, sich schon vor dem Einsatz oder der Änderung eines automatisierten Verfahrens bewusst zu machen, welche Risiken für den Datenschutz mit einem bestimmten Verfahren verbunden sind und wie diese beherrscht werden können.

11. Bauen und Wohnen

11.1 Prüfung des Hamburger Mietenspiegels

Bei einer Datenverarbeitung im Auftrage ist die Einhaltung der datenschutzrechtlichen Bestimmungen durch den Auftraggeber sicherzustellen.

Hamburg gibt zur Orientierung von Mietern und Vermietern regelmäßig einen qualifizierten Mietenspiegel für die nicht preisgebundenen Mietwohnungen heraus. Für die Erstellung der Mietenspiegel 2003 und 2005 hat der Senat die Mietenspiegelbefragungsverordnung vom 25. Februar 2003 (HmbGVBl. S. 19) erlassen. Die Befragung ist freiwillig.

Mit der Durchführung der Mieter- und Vermieterbefragung sowie mit der Auswertung der Erhebungsdaten hatte die für den Mietenspiegel zuständige Behörde für Bau und Verkehr – Amt für Wohnen, Stadterneuerung und Bodenordnung – (BBV) ein privates Unternehmen beauftragt.

Das beauftragte Unternehmen wird gemäß § 3 Hamburgisches Datenschutzgesetz (HmbDSG) im Auftrag tätig und hatte sich der Kontrolle durch den Hamburgischen Datenschutzbeauftragten zu unterwerfen. Bei der Verarbeitung personenbezogener Daten im Auftrag öffentlicher Stellen tragen die Auftraggeber letztlich die alleinige Verantwortung für die Einhaltung datenschutzrechtlicher Bestimmungen. Aus diesem Grund ist das auftragnehmende Unternehmen unter besonderer Berücksichtigung der Eignung der von ihr getroffenen technischen und organisatorischen Maßnahmen sorgfältig auszuwählen. Weiterhin darf dieses Unternehmen die Daten nur im Rahmen der Weisungen des Auftraggebers (BBV) verarbeiten.

Die wesentlichen Weisungen zum Datenschutz bei der Mietenspiegelerhebung 2003 ergeben sich aus dem zwischen der BBV und dem auftragnehmenden Unternehmen geschlossenen Vertrag (z. B. § 3 Datenschutz), der Anlage 1 (Hamburger Mietenspiegel 2003 – Datenschutz- und Datensicherungskon-

zept) und aus der Anlage 3 (Hamburger Mietenspiegel 2003 – Merkblatt zum Datenschutz), das sämtlichen Betroffenen zugesandt worden ist.

Die Mietenspiegelbefragung erfolgte mittels Fragebogen durch Interviewer. Jeder Fragebogen besteht aus einem sog. Deckblatt, das u.a. die für die Durchführung der Befragung erforderlichen Hilfsmerkmale (Name, Vorname, Anschrift und ggf. Telefonnummer des Betroffenen) sowie eine laufende Nummer enthält und dem 6-seitigen Fragebogen mit den Angaben des Betroffenen (Erhebungsmerkmale), der auf Seite 1 nochmals die gleiche laufende Nummer wie auf dem Deckblatt aufweist. Über diese Kontrollnummer besteht die Möglichkeit, bis zum Abschluss der Plausibilitätsprüfung eine Verbindung der Hilfsmerkmale mit den Erhebungsmerkmalen herzustellen (z. B. für Rückfragen bei dem Betroffenen). Die Erhebungsdaten dürfen nur anonym ausgewertet werden.

Im Rahmen unserer Kontrolltätigkeit haben wir bei dem auftragnehmenden Unternehmen das Verfahren bei der Mietenspielerhebung 2003 geprüft. Dabei haben wir folgende schwerwiegende Datenschutzmängel festgestellt:

- Nach der Mietenspiegelbefragung sind die für die Durchführung der Befragung erforderlichen Hilfsmerkmale (Name, Vorname, Anschrift und ggf. Telefonnummer des Betroffenen) nicht von dem 6-seitigen Fragebogen mit den Angaben des Betroffenen (Erhebungsmerkmale) getrennt worden. Auch nach Erfassung der Daten im DV-System wurde solch eine Trennung nicht vorgenommen.

  Dies steht im Widerspruch zu der vertraglichen Vereinbarung im gemeinsam abgestimmten „Datenschutz- und Datensicherungskonzept Mietenspiegel 2003“, wonach die zur Durchführung der Mietenspiegelbefragung erforderlichen Hilfsmerkmale (Namen, Anschriften, Telefonnummern der Betroffenen) durch die Feldleitung von den Erhebungsmerkmalen (von den Fragebögen) nach erfolgter Prüfung auf Vollständigkeit und Plausibilität zu trennen (z. B. durch Abtrennen der Deckblätter) und an anderer gesicherter Stelle aufzubewahren sind. Weiterhin hat die EDV-Erfassung der Erhebungsmerkmale ohne die Hilfsmerkmale zu erfolgen, so dass keine Rückschlüsse auf einzelne Personen möglich sind.

  Durch diese Trennungsregelung und faktische Anonymisierung der Erhebungsdaten soll die gegenüber den Betroffenen im „Merkblatt Hamburger Mietenspiegel 2003“ zugesicherte anonyme statistische Auswertbarkeit der Daten gewährleistet werden. Daher besteht nach dem Grundsatz der Erforderlichkeit eine Verpflichtung, die Deckblätter mit den Hilfsmerkmalen zum frühest möglichen Zeitpunkt von den ausgefüllten Fragebögen zu trennen und zu vernichten.

- Das auftragnehmende Unternehmen hat für die Datenerfassung der Erhebungsdaten ein weiteres Unternehmen als sog. Unterauftragnehmer einge-

schaltet, ohne hierfür die erforderliche Einwilligung der BBV eingeholt zu haben.

Damit hat das auftragnehmende Unternehmen gegen die vertragliche Regelung des § 3 verstoßen, wonach die Einschaltung eines Unterauftragnehmers von der vorherigen schriftlichen Einwilligung der BBV abhängig gemacht worden ist. Somit ist die Datenverarbeitung bei dem Unterauftragnehmer nach unserer Auffassung in nicht legitimierter Weise erfolgt.

- Mit der Mietenspiegelerhebung wurden beim Auftragnehmer zwei Mitarbeiter betraut, die der BBV gegenüber nicht als mit der Aufgabenerledigung betraute Personen benannt wurden. Diese Benennung wurde aber in § 17 gefordert. Damit wurden unbefugten Personen personenbezogene Daten zugänglich gemacht.
- Sämtlich Hilfsmerkmale sowie Erhebungs- und Auswertungsdaten wurden in dem DV-System des auftragnehmenden Unternehmens in einem gemeinsamen Verzeichnis gespeichert.

  Trotz anders lautender Vertragsvereinbarungen ist auch im DV-System keine Trennung von Hilfs- und Erhebungsmerkmalen vorgenommen worden. Dieses wurde aber speziell im „Datenschutz- und Datensicherungskonzept Mietenspiegel 2003“ festgelegt. Weiterhin ist vereinbart worden, dass die Auswertung der Erhebungsmerkmale in einem von den Hilfsmerkmalen befreiten Datensatz zu erfolgen hat und die Auswertungsdateien in einem gesonderten Bereich abzulegen sind. Außerdem steht diese Verfahrensweise im Widerspruch zu den Aussagen im „Merkblatt Hamburger Mietenspiegel 2003“, wonach den von der Mietenspiegelerhebung 2003 Betroffenen zugesichert worden ist, dass die Adressen der Betroffenen und die Erhebungsdaten auf verschiedenen Rechnern verwaltet und diese Daten nur anonymisiert ausgewertet und verschlüsselt werden.

  Die Feststellungen haben nach unserer Auffassung gezeigt, dass das auftragnehmende Unternehmen bei der Durchführung der Mietenspiegelerhebung 2003 gegen eine Vielzahl der vertraglich festgelegten Datenschutzregelungen in erheblicher Weise verstoßen hat. Aus diesem Grund haben wir das Unternehmen aufgefordert, dafür Sorge zu tragen, dass die vertraglichen Vereinbarungen zum Datenschutz umgehend erfüllt werden. Die zuständige BBV als verantwortliche Stelle haben wir entsprechend unterrichtet.

Die aufgeführten Mängel sind zwar nachträglich behoben worden. Es ist aber durch die verantwortliche Stelle sicherzustellen, dass derartige Vorkommnisse bei künftigen Mietenspiegelerhebungen ausgeschlossen werden können.

Insbesondere bei freiwilligen Befragungen sind die öffentlichen Stellen auf das Wohlwollen und das Einverständnis der Betroffenen angewiesen. Aus diesem

Grund müssen zugesicherte Datenschutzmaßnahmen unbedingt eingehalten werden. Geschieht dies nicht, so ist nach unseren Erfahrungen nur mit einer sehr geringen Akzeptanz bei den Betroffenen zu rechnen. Ob sich unter derartigen Voraussetzungen dann noch repräsentative Mietenspiegelbefragungen durchführen lassen, muss bezweifelt werden.

Öffentliche Stellen wie die BBV haben die Ausführung des Hamburgischen Datenschutzgesetzes sowie anderer Vorschriften über den Datenschutz für ihren Geschäftsbereich sicherzustellen. Da sie als Auftraggeber die alleinige Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen tragen, bleibt es ihnen vorbehalten, geeignete Maßnahmen zu ergreifen, um die Einhaltung von vertraglichen Vereinbarungen zu gewährleisten. Dieses könnte beispielsweise durch verstärkte Kontrollen bei der auftragnehmenden Stelle oder durch schriftliche Festlegung der einzelnen Forderungen mit schriftlicher Bestätigung, dass diese erfüllt worden sind, erreicht werden.

Wir werden daher die BBV um entsprechende Stellungnahme bitten. Über das Ergebnis werden wir weiter berichten.

11.2 Prüfung des Verfahrens vordringlich Wohnungssuchender beim Bezirksamt Hamburg-Nord

Die Prüfung ergab datenschutzrechtliche Defizite und führte zu Änderungen organisatorischer und technischer Datenschutzmaßnahmen.

Im Berichtszeitraum haben wir im Bezirksamt Hamburg-Nord – Einwohneramt – die Verarbeitung personenbezogener Daten bei der „Versorgung von vordringlich Wohnungssuchenden mit Wohnraum“ geprüft. Hierbei handelt es sich – im Gegensatz zu anderen hamburgischen Bezirksämtern – weitgehend um ein nicht-automatisiertes Verfahren. Während die Führung der Wohnraumdatei dv-mäßig unterstützt wird, erfolgt die Antragsbearbeitung (inkl. Einkommensberechnung, Erteilung von Berechtigungsbescheiden usw.) sowie die Wohnungsvermittlung überwiegend noch manuell.

Im Rahmen der Erfassung der öffentlich geförderten Wohnungen sowie der Anerkennung von vordringlich Wohnungssuchenden und der Vermittlung von Sozialwohnungen stützt sich das Verfahren im Wesentlichen auf das Zweite Wohnungsbaugesetz (II. WoBauG), das Wohnraumförderungsgesetz (WoFG) sowie auf die vom Senat herausgegebene „Globalrichtlinie über die Versorgung von vordringlich Wohnungssuchenden mit Wohnraum“.

Die Prüfung führte zu folgenden Feststellungen und Forderungen:

- Da sich die Diensträume des geprüften Bereiches im Erdgeschoss befinden, haben sich die technischen und organisatorischen Maßnahmen zur Verhinderung eines unbefugten Zugriffs auf personenbezogene Daten auf die Türen und auch auf die ungesicherten Fenster zu erstrecken. Wir haben

daher um geeignete Maßnahmen gebeten, um einen Zugriff auf die sensiblen personenbezogenen Daten durch Unbefugte zu verhindern (z. B. durch abschließbare Fenstergriffe).

- In den zu führenden Wohnungsakten wurden nicht nur die „Dringlichkeitsscheine“ des aktuellen Mieters, sondern auch die sämtlicher Vormieter über den gesamten Bindungszeitraum aufbewahrt.

  Gemäß § 32 Abs. 2 WoFG hat die zuständige Stelle insbesondere über die Wohnungen, ihre Nutzung, die jeweiligen Mieter und Vermieter sowie über die Belegungsrechte Daten zu erheben und zu verarbeiten, soweit dies zur Sicherung der Zweckbestimmung der Wohnungen erforderlich ist. Damit ist eindeutig festgelegt, dass es sich dabei nur um die aktuellen Mieter handeln kann. Für die Aufbewahrung der Berechtigungsscheine ehemaliger Mieter besteht daher keine Notwendigkeit. Wir haben eine entsprechende Bereinigung der Wohnungsakten verlangt.

- Im Archivraum des Einwohneramtes wurden nicht nur Akten des Abschnitts Wohnungsvergabe gelagert, sondern auch Akten des Jugendamtes. Diese enthalten sensible personenbezogenen Daten, die unter die besonderen Vorschriften des Sozialgesetzbuches (SGB) fallen.

  Zur Gewährleistung der Schutzvorschriften des SGB haben wir eine vollständige Trennung der Akten durch entsprechende technische Maßnahmen gefordert, so dass der Zugriff auf die Akten des jeweils anderen Fachamtes nicht mehr möglich ist.

- Eine Mitarbeiterin des Bereiches konnte über einen Online-Zugriff auf MEWES (Automation Meldewesen) selbsttätig Melderegisterdaten von Antragstellern abrufen.

  Für diese automatisierte Abrufmöglichkeit war eine Rechtsgrundlage nicht zu ermitteln. Gemäß § 2 Abs. 1 der Meldedatenübermittlungsverordnung (MDÜV) übermitteln die Meldebehörden den für die Führung der Wohnraumdatei zuständigen Stellen bei Bedarf zwar die zur Aufgabenerfüllung erforderlichen Daten. Damit ist aber keinesfalls die Möglichkeit eines selbstständigen Abrufes der Daten im Wege eines Online-Zugriff verbunden. Ein automatisierter Abruf personenbezogener Daten darf nach § 11 HmbDSG nur eingerichtet werden, wenn eine Rechtsvorschrift dies ausdrücklich zulässt. Für die erforderliche Rechtsgrundlage sind daher die entsprechenden Maßnahmen einzuleiten.

Das Bezirksamt Hamburg-Nord hat unsere Forderungen zur Verbesserung des Datenschutz umgesetzt, so dass die Verfahrensweise des geprüften Bereiches nunmehr den datenschutzrechtlichen Vorschriften entspricht.

11.3 Videoüberwachung von Baustellen durch die Behörde für Bau und Verkehr

Für eine unbedenkliche Videoüberwachung sind umfangreiche Festlegungen erforderlich.

Die Behörde für Bau und Verkehr – Tiefbauamt – (BBV) ist an uns herangetreten, weil die Bauüberwachung der Baustelle „Alsterbrücke Trillup“ teilweise mittels Videokamera durchgeführt werden sollte. Dabei war vorgesehen, dass bei der Baustelle eine Videokamera installiert wird, deren Bilder über ein Passwort per Internet vom zuständigen Bauüberwachungspersonal abgerufen werden können. Auf diese Weise könnten viele der sonst notwendigen Dienstfahrten entfallen und wieder mehr technische Aufgaben erfüllt werden.

Gegen das vorgestellte Konzept, die Baustellenüberwachung von Brücken- und Ingenieurbauwerken mittels Videokamera zu überwachen hatten wir keine grundsätzlichen datenschutzrechtlichen Bedenken. Es muss aber sichergestellt werden, dass ausschließlich Übersichtsaufnahmen (sog. Panorama-Aufnahmen) erstellt werden, die weder eine direkte noch eine indirekte (z. B. über das Kfz.-Kennzeichen) Identifizierung von Personen zulassen. Denn nur dann können Beeinträchtigungen der Persönlichkeitsrechte von Betroffenen (z. B. Bauarbeiter, Zulieferer) ausgeschlossen werden. Sofern durch die Videokamera auch benachbarte Grundstücke bzw. Gebäude oder öffentliche Wege erfasst werden, dürfen auch in diesen Bereichen keine direkten oder indirekten Identifizierungen von Personen möglich sein.

Im Einzelnen wurden mit der BBV folgende Vereinbarungen getroffen:

- Durch das Kamerasystem werden in stündlichen Abständen jeweils 6 Standbilder erstellt und auf einem passwortgeschützten Internetserver gespeichert.
- Zugangsberechtigt ist nur ein namentlich festgelegter Personenkreis.
- Die Bildaufnahme erfolgt nur für die Dauer der Baumaßnahme. Nach Bauabschluss ist die Kamera abzubauen.
- Änderungen der Kameraeinstellungen durch das Bauüberwachungspersonal müssen ausgeschlossen werden.
- Auf beiden Brückenseiten wird auf den Umstand der Videoüberwachung hingewiesen.
- Vor Aufnahme des Echtbetriebes kann sich der Hamburgische Datenschutzbeauftragte davon überzeugen, dass keine Personen bestimmbar gemacht werden können.
- Die gespeicherten Bilder sind spätestens nach der Schlussrechnung zu löschen.

- Über den Umgang mit der Videoüberwachungsanlage ist eine Dokumentation zu erstellen.

Da die Baumaßnahme zwischenzeitlich abgeschlossen worden ist, konnte auch die Kamera abgebaut und die Daten gelöscht werden.

12. Ausländerangelegenheiten

12.1 Zentraldatei zur Altersfeststellung minderjähriger Ausländer

Unsere Kritik an undifferenzierten Lesezugriffen der vielen angeschlossenen Dienststellen auf alle Daten der zentralen Datei wurde vom Senat nicht geteilt.

Seit längerem bemühte sich die Behörde für Inneres um eine effizientere Praxis der Altersfeststellungen bei minderjährigen Ausländerinnen und Ausländern. Hintergrund ist die Erfahrung der Ausländerbehörde, dass viele junge Flüchtlinge falsche Geburtsdaten angeben; sie wollen z. B. als unter 16-Jährige nicht in andere Bundesländer weiterverteilt, sondern in betreute Erstaufnahmeeinrichtungen der Jugendhilfe in Hamburg aufgenommen werden. Hat die Ausländerbehörde den Eindruck, dass die Jugendlichen älter sind als angegeben, gibt sie ihnen ein fiktives Geburtsdatum und zeigt sie meist wegen versuchter mittelbarer Falschbeurkundung bei der Kriminalpolizei an. Die Altersschätzung kann der Jugendliche auf eigene Kosten im Institut für Rechtsmedizin überprüfen lassen. Auch im Rahmen von Strafverfahren werden solche medizinischen Altersfeststellungen durchgeführt.

Damit alle Stellen, die mit den Jugendlichen zu tun haben, immer über deren Identität, insbesondere über ihr „gültiges“ Alter informiert sind, bereitete die Ausländerbehörde eine zentrale Datenbank vor. Sie umfasst die Personalien, die Daten der Altersschätzungen und -feststellungen sowie Verfahrens- und Vorgangsdaten. In mehreren Gesprächen mit der Ausländerbehörde erörterten wir die datenschutzrechtlichen Probleme und konnten im Einzelnen auch Konsens erzielen.

Keine Einigkeit erreichten wir jedoch darüber, ob alle ca. 700 Endanwender der verschiedenen Ausländer-, Sozial-, Jugend-, Polizei- und staatsanwaltschaftlichen Dienststellen und des Instituts für Rechtsmedizin jeweils auf alle erfassten Daten zugreifen sollten. Wir forderten, den Zugriffsumfang nach der Erforderlichkeit der Daten für die Aufgabenerfüllung der jeweiligen Dienststelle zu differenzieren, und lehnten einen Zugriff des Instituts für Rechtsmedizin überhaupt ab. Die Ausländerbehörde wollte einer Zugriffsbeschränkung schon deswegen nicht folgen, weil sie für die Datenbank die Software BASIS vorgesehen hatte, die solche Differenzierungen nicht zulässt. Ein Wechsel oder eine Modifikation des Systems sei unverhältnismäßig teuer. Das Institut für Rechtsmedizin wurde allerdings aus dem Kreis der Zugriffsberechtigten ganz herausgenommen.

In der Senatsvorlage für die nach § 11 HmbDSG erforderliche Verordnung erläuterten wir noch einmal unsere differenzierende Position. Dessen ungeachtet erließ der Senat am 7. Oktober 2003 die „Verordnung über die Einrichtung eines automatisierten Verfahrens zum Abruf personenbezogener Daten über Ausländerinnen und Ausländer mit nicht nachgewiesenen Altersangaben“ ohne die von uns gewünschten Unterscheidungen.

12.2 Stichprobenprüfung bei Zugriffen auf die Ausländerdatei

Bei Zugriffen nicht aktenführender Stellen auf Ausländerdaten schreibt die Verordnung eine Stichprobenprüfung vor. Das entsprechende Verfahren wurde auf unsere Initiative effektiver gestaltet.

Die Ausländerdatenverarbeitungsverordnung fordert, dass Zugriffe von nicht aktenführenden Stellen auf das Ausländerdatensystem PAULA (z. B. der zentralen Ausländerbehörde anstelle der zuständigen bezirklichen Ausländerabteilung) durch ein Stichprobenverfahren kontrolliert werden. Damit soll nachträglich festgestellt werden, ob die rechtlichen Zulässigkeitsvoraussetzungen für einzelne Datenabrufe vorlagen oder nicht.

Die Ausländerdienststellen erarbeiteten im Jahre 2000 ein entsprechendes Verfahren, das wir akzeptierten. Danach mussten nicht aktenführende Sachbearbeiterinnen und Sachbearbeiter bei jedem Zugriff im System einen Zugriffsgrund (von 10 zur Auswahl gestellten Zugriffsgründen) anklicken – z. B. „Prüfung der Zuständigkeit“ oder „Vorsprache Ausländer“. Ferner wurde festgelegt, wer in welcher Form aus den flächendeckend protokollierten Datenzugriffen eine Stichprobe auswählt und kontrolliert.

Bei einer datenschutzrechtlichen Prüfung im Mai 2002 mussten wir feststellen, dass dieses Verfahren nur sehr unvollständig in die Praxis umgesetzt worden war. Von diesem Mangel waren wir zuvor nicht unterrichtet worden. Wir ließen uns aber davon überzeugen, dass diese Form der Kontrolle aufwändig, aber wenig effektiv war. Insbesondere ist es schwierig, im Nachhinein zu prüfen, ob der angeklickte Zugriffsgrund tatsächlich vorlag.

Nach vielen Verzögerungen auf Seiten der Ausländerbehörde einigten wir uns mit ihr auf ein anderes Verfahren: Statt einer Stichprobe aus der flächendeckenden Protokollierung der Zugriffsbegründung für jeden Zugriff soll nun bereits die Zugriffsbegründung auf Stichproben beschränkt, aber verbindlicher und aussagekräftiger werden. Die Kontrolle erfolgt dabei durch eine beim n.-ten Datenzugriff unvermutet sich öffnende Eingabemaske.

Dort wird über die Kontrollmaßnahme aufgeklärt und eine Freitext-Begründung bzw. die Mitteilung des Anlasses für den Zugriff sowie die Angabe der getroffenen Maßnahme gefordert. Die Maske kann von der zugreifenden Person nicht ohne Eintrag gelöscht oder entfernt werden und löst eine Kontrollmitteilung beim Vorgesetzten aus. Der Vorgesetzte hat die Überprüfung der Zugriffsbe-

gründung innerhalb von 2 Tagen durchzuführen und seine Entscheidung revisionssicher zu dokumentieren. Zur Gewährleistung einer Mindest-Kontrolldichte sollen systemseitig die sog. Zugriffszähler so eingestellt werden, dass jede Sachbearbeiterin und jeder Sachbearbeiter durchschnittlich ca. einmal im Monat kontrolliert wird.

Nach der grundsätzlichen Einigkeit über diese Verfahrensweise kommt es nun auf die technische Umsetzung und die verbindliche Einführung bei allen zentralen und bezirklichen Ausländerdienststellen an. Da die rechtliche Pflicht zur Stichprobenkontrolle bereits seit mehr als 3 Jahren – unerfüllt – besteht, sind weitere Verzögerungen nicht vertretbar.

12.3 Anweisung zu Sicherheitsprüfungen von Ausländern

Die Umsetzung des Terrorismusbekämpfungsgesetzes im Ausländerrecht schränkt den Datenschutz von Ausländern erheblich ein. Die von der Innenbehörde dazu vorbereitete Weisung für Sicherheitsbefragungen und -abfragen bedarf datenschutzrechtlicher Ergänzungen.

Das Terrorismusbekämpfungsgesetz von 2002 hat in das Ausländergesetz drei Regelungen eingeführt, die der Gefahr terroristischer Aktivitäten vorbeugen sollen: § 47 Abs.2 Nr.5 AuslG fordert, Ausländer „in der Regel“ auszuweisen, wenn sie in einer Sicherheits-Befragung falsche Angaben über frühere Aufenthalte oder über Verbindungen zu verdächtigen Personen bzw. Organisationen machen. § 8 Abs.1 Nr.5 AuslG schließt eine Aufenthaltsgenehmigung für Ausländer aus, die die freiheitliche demokratische Grundordnung oder die Sicherheit des Landes gefährden, gewaltbereit erscheinen oder Terror-Vereinigungen unterstützen. § 64 a AuslG erweitert hierzu die Anfrage- und Datenübermittlungsmöglichkeiten zwischen Ausländer- und Sicherheitsbehörden.

Um das Terrorismus-Risiko möglichst klein zu halten, dürfen danach ausländerrechtliche Abwehrmaßnahmen auch ohne eine Klärung von Vorwürfen, Verdachtsmomenten oder Gefahr-Indizien getroffen werden. Auch die Anforderungen an die Bestimmtheit der Tatbestände und die Annahme einer Gefährdung sind deutlich herabgesetzt. Damit wird das informationelle Selbstbestimmungsrecht aller hier lebenden Ausländerinnen und Ausländer aus bestimmten Staaten stark eingeschränkt: Die Gefahr, dass aufgrund ungeprüfter unzutreffender Informationen, „harmloser“ Kontakte oder missverständlicher Äußerungen auch völlig unbeteiligte und „unschuldige“ Menschen – auch umworbene „qualifizierte Zuwanderer“ – ausgewiesen werden, hat sich erheblich erhöht.

Als eines der ersten Bundesländer will Hamburg die neuen gesetzlichen Möglichkeiten in einer verbindlichen Weisung zur tatsächlichen Praxis machen: Staatsangehörige bestimmter Staaten sollen vor Erteilung einer Aufenthaltsgenehmigung regelmäßig anhand eines Fragebogens nach Aufenthalten,

Kontakten und Fehlverhalten befragt werden. Zudem werden Landeskriminalamt und Landesamt für Verfassungsschutz um Auskunft darüber gebeten, ob Erkenntnisse entsprechend § 47 Abs. 2 Nr. 5 oder § 8 Abs. 1 Nr. 5 AuslG vorliegen.

Angesichts der gesetzlichen Regelung im Ausländergesetz können sich datenschutzrechtliche Erwägungen nur noch gegen das Wie, nicht gegen das Ob der vorgesehenen Weisung richten, die sich eng an die gesetzlichen Vorgaben hält. So haben wir gefordert, dass die Kommunikation zwischen Ausländer- und Sicherheitsbehörden nur über verschlossene Briefpost, verschlüsselte E-Mails oder über vorprogrammierte und eindeutig zugeordnete Telefaxanschlüsse erfolgen darf. Ferner sollte sich eine Aktenanforderung der Sicherheitsbehörden auf die für ihre Prüfung notwendigen Aktenteile beschränken. Angeregt haben wir auch, für die Mitteilungen von Erkenntnissen an die Ausländerbehörde eine Frist einzuführen, um den zu Gerüchten und Falschinformationen verleitenden Schwebezustand für die betroffene Person zu begrenzen.

13. Polizei

13.1 Rasterfahndung

Bis auf knapp 40 polizeilich relevante Datensätze wurden sämtliche im Zusammenhang mit der Rasterfahndung gespeicherten Daten im Dezember 2002 und Januar 2003 gelöscht.

Im Gefolge der Rasterfahndungen nach dem 11. September 2001 (vgl. 18. TB, 19.2) hat es im Berichtszeitraum eine Fülle von Aktivitäten gegeben.

Damit die Mängel bei der polizeilichen Durchführung der letzten Rasterungen künftig vermieden werden, hat die Polizei auf unsere Initiative und in enger Abstimmung mit uns eine Verfügung erarbeitet. Darin enthalten sind die für Rasterfahndungen sowohl gemäß § 98 a Strafprozessordnung (StPO) als auch gemäß § 23 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) zu beachtenden Verfahrensschritte.

Im Berichtszeitraum haben wir die Datenübermittlungen durch Einwohnermelde- und Ausländerdienststellen sowie Hochschulen an die Polizei überprüft, die anlässlich der Rasterfahndungen im Herbst 2001 erfolgt waren. Wir haben dabei eine Reihe von Mängeln festgestellt. So ist die Erstellung und Lieferung der Datenträger teilweise nicht dokumentiert worden. Die durch die Anordnung unpräzise festgelegten Auswahlkriterien – wie z. B. Altersgrenzen – wurden unterschiedlich ausgelegt, so dass verschiedene Dienststellen die Daten von Personen aus unterschiedlichen Altersgruppen geliefert haben. Ferner haben die verpflichteten Stellen zusätzliche Daten geliefert, die weder in der Anordnung genannt noch von der Polizei angefordert worden sind.

Diese Mängel beruhten durchweg auf der mangelnden Vertrautheit der Daten liefernden Stellen mit den bei einer Rasterfahndung gemäß § 23 PolDVG zu beachtenden Voraussetzungen und Verfahrensschritten. Mängel ergaben sich auch durch den extremen Zeitdruck, unter dem die Rasterfahndungen nach den Ereignissen vom 11. September 2001 durchgeführt worden sind. Wir haben deshalb eine Arbeitshilfe erarbeitet und den Dienststellen in den von den Rasterfahndungen betroffenen Bereichen zur Verfügung gestellt. Wir haben der Polizei empfohlen, bei künftigen Rasterfahndungen in anderen Verwaltungsbereichen diese Arbeitshilfe sofort den jeweiligen Dienststellen als Handreichung zur Verfügung zu stellen.

Die Polizei hat nach den Rasterungen und unserer raschen Kontrolle der Datenverarbeitung die von anderen Dienststellen gelieferten Datenbestände vollständig unverzüglich vernichtet. Seitdem kann niemand mehr feststellen, wer – ohne alle Rasterungskriterien zu erfüllen und damit Trefferfall zu sein – in die Rasterungen einbezogen worden ist. Für Personen, über die Daten (z. B. von Hochschulen) geliefert worden waren, die aber nicht als Trefferfälle herausgerastert wurden, waren damit die Grundrechtseingriffe im Zusammenhang mit der Rasterfahndung zu diesem Zeitpunkt beendet.

Das Landeskriminalamt (LKA) hatte die Trefferfälle – also die dreistellige Zahl der Personen, die im Rahmen der polizeilichen Rasterungen herausgefiltert worden sind – mit den üblichen Ermittlungsmethoden (z. B. Befragung von Betroffenen, Umfelderkundungen) abgearbeitet. Während dieser Zeit sind die Datensätze aller Trefferfälle rund ein Jahr lang gespeichert geblieben.

In diesem Zusammenhang hat das LKA seine Trefferfälle auch in die beim Bundeskriminalamt (BKA) geführte „Schläfer-Datei“ eingestellt. Das BKA hat im Rahmen von Abgleichen gemäß § 28 BKA-Gesetz die vom LKA in die „Schläfer-Datei“ eingestellten Personendatensätze auf Übereinstimmungen mit anderen, dem BKA vorliegenden Datenbeständen (z. B. über Fluglizenzinhaber) überprüft und die um die dortigen Erkenntnisse angereicherten Datensätze an das LKA zurück übermittelt.

Für alle Trefferfälle haben die Grundrechtsbeeinträchtigungen zumindest bis in den Spätherbst 2002 angedauert. Im Dezember 2002 und Januar 2003 wurden bei rund 95 Prozent der Trefferfälle die Personen über die bisherige Speicherung vom LKA unterrichtet und die Datensätze gelöscht. Lediglich die Daten von knapp 40 Personen mit polizeilich relevanten Erkenntnissen blieben gespeichert.

Im Hinblick auf § 23 Abs. 3 und 5 PolDVG erscheint es nicht unproblematisch, dass die Polizei erst Ende 2002/ Anfang 2003 im wesentlichen gleichzeitig die meisten Betroffenen benachrichtigt und ihre Datensätze gelöscht hat. Die Voraussetzungen des Anspruchs auf unverzügliche Benachrichtigung und Datenlöschung sind bei jeder Person gesondert zu prüfen und führen kraft Gesetzes

zu unterschiedlichen Zeitpunkten, zu denen Benachrichtigung und Löschung geboten sind. Bei Personen, bei denen seit längerem fest steht, dass bei ihnen (einschließlich ihrer möglichen Verbindungen zu anderen Personen) relevante Erkenntnisse weder angefallen sind noch anfallen werden, wäre nach unserer Auffassung eine frühzeitigere Benachrichtigung und Löschung angezeigt gewesen. Unsere Bedenken konnten wir jedoch zurückstellen, da für diese große Personengruppe mit den Benachrichtigungen und Löschungen die bislang andauernden Grundrechtseingriffe insgesamt beendet waren.

Auf Grund von Erfahrungen mit der Rasterfahndung zur Gefahrenabwehr (in Hamburg gemäß § 23 PolDVG) seit dem Herbst 2001 begegnet die Verfahrensweise – anders als die Rasterfahndung zur Strafverfolgung nach § 98 a StPO – insgesamt prinzipiellen Bedenken. Die Eignung der Rasterfahndung zur Bekämpfung der Gefahren, die vom internationalen Terrorismus ausgehen, erfordert eine bundeseinheitliche Handhabung. Die Rasterfahndung zur Gefahrenabwehr ist aber als Element des Polizeirechts landesrechtlich geregelt. Von Land zu Land gelten bei ihr u.a. unterschiedliche Anordnungszuständigkeiten, Eingriffsvoraussetzungen und Zugriffsmöglichkeiten auf Datenbestände.

Diese föderalistische Vielfalt hat etwa dazu geführt, dass nach einer rechtskräftigen Gerichtsentscheidung im Frühjahr 2002 die in Hessen bei der Rasterfahndung erhobenen Daten unverwertet vernichtet werden mussten; nach einer darauf folgenden Änderung des Landesrechts und anschließenden widerstreitenden Gerichtsentscheidungen ist dort der Weg zur Durchführung der Rasterfahndung erst im Februar 2003 frei geworden. Wenn als Antwort auf die am 11. September 2001 begründete bundesweite Gefahrenlage eine flächendeckende Rasterfahndung teilweise auch mehr als ein Jahr danach noch nicht durchgeführt werden kann, lässt schon dieser Zeitablauf es sehr fraglich erscheinen, ob dies ein geeignetes Mittel zur Abwehr akuter Bedrohungen ist.

Es verwundert daher nicht, wenn Teilerfolge im Kampf gegen den internationalen Terrorismus nach dem 11. September 2001 nur geringfügig durch die Rasterfahndung erreicht wurden. Dann aber vermag dieses Instrument der Gefahrenabwehr die Eingriffe in Grundrechte einer Vielzahl völlig Unbeteiligter schwerlich zu rechtfertigen.

13.2 Waffenbesitzverwaltung

Die Zentralisierung der Waffenbesitzverwaltung bei der Polizei wurde datenschutzkonform ausgestaltet.

Vor dem Hintergrund der Ereignisse in einer Erfurter Schule mit 17 Toten wurden vom Gesetzgeber verschiedene Änderungen im Waffengesetz (WaffG) beschlossen. Im Zusammenhang mit der Umsetzung dieser Novellierung wurde in Hamburg seitens des Senats eine Zentralisierung des Vollzugs des Waffenrechts vorgesehen. Die bisherige Praxis der Verwaltung von waffenerlaubnis-

rechtlichen Angelegenheiten bei den einzelnen Wirtschafts- und Ordnungsämtern soll zukünftig durch ein modernes computergestütztes Waffenregister an einer zentralen Stelle bei der Polizei ersetzt werden. Zum personellen Aufbau dieser neuen Dienststelle wurden 23 Beamte von den Bezirksämtern und der Landespolizeiverwaltung abgestellt.

Von der Polizei erfolgte gegenüber unserer Dienststelle eine frühestmögliche und seit Beginn der Planungs- und Realisierungsphase projektbegleitende Einbindung. Aufgrund der Zusammenführung verschiedenster datenverarbeitender Stellen und der notwendigen Datenübermittlungen und -abgleiche zwischen unterschiedlichen Behörden waren im Vorfeld mehrere datenschutzrechtliche Fragen zu bewerten.

Die Neuregelung räumt der Waffenbehörde in § 5 WaffG nicht die Befugnis zur Regelanfrage bei Gesundheitsämtern ein, ob Antragsteller dort bereits bekannt sind. Die Polizei kritisiert diese Regelung, weil sie z. B. auch psychisch auffälligen Antragstellern Erlaubnisse erteilen muss, wenn ihr diese Auffälligkeiten nicht bekannt sind. Deshalb fordert die Polizei die Möglichkeit der Regelanfrage auch bei Gesundheitsämtern. Wir halten die hierzu angestrebte Gesetzesänderung nur dann für vertretbar, wenn der Umfang der zu übermittelnden Daten streng begrenzt wird und die Daten alsbald zu löschen sind, falls die Erkenntnisse keinen Zweifel an der waffenrechtlichen Eignung des Antragstellers zu begründen vermögen.

Nach Maßgabe der neuen waffengesetzlichen Änderungen führt die Waffenbehörde Datenübermittlungen und -abgleiche mit der zuständigen Meldebehörde durch. Dabei ist vorgesehen, dass der Datenabgleich direkt von der Polizei auf die Datensätze des bezirklichen Meldeverfahrens MEWES im Hinblick auf Namensänderungen, Wegzug oder Tod eines Antragstellers sowie dessen bereits erteilte Waffenerlaubnisse erfolgen kann. Für diese fachlich zwingend gebotenen Abfragen fungiert das polizeiliche Einwohnermeldeverfahren EWO als Schnittstelle und gibt im täglichen Dienst den Sicherheitskräften Informationen über registrierte Waffenbesitzer.

Unter Berücksichtigung der hohen Einwohnerzahl Hamburgs war es bei diesem Datenabgleich fachlich erforderlich, individuelle Suchkriterien neben dem Namen und dem Geburtsdatum eines Antragsteller festzulegen. Es können nunmehr datenschutzfreundlich auch Mehrfachauskünfte über mehrere in Betracht kommende Antragsteller vermieden werden.

Im Rahmen der Zuverlässigkeitsüberprüfung als Voraussetzung für die Erteilung einer waffenrechtlichen Erlaubnis wurde ein Verfahren zur automatisierten Abfrage aus dem örtlichen polizeilichen Auskunftssystem POLAS abgestimmt. Beim Vorhandensein eines entsprechenden Positiv- bzw. Negativ-Datensatzes erfolgt seitens der Waffenbehörde eine schriftliche Anfrage beim Landeskriminalamt (LKA). Das LKA übermittelt nach fachlicher Prüfung bei

Einträgen, die Auswirkungen auf die Zuverlässigkeit eines Antragstellers indizieren, diese Informationen an die Waffenbehörde.

Neben der Möglichkeit, über die entsprechende personenbezogene EWO-Abfrage Kenntnisse über evtl. waffenrechtliche Erlaubnisse zu erlangen, wurde ferner eine Waffenrecherche mit dem ausschließlichen Suchkriterium der Waffennummer eingerichtet. Dadurch kann die Polizei Waffen einer Person zuordnen bzw. überprüfen und feststellen, ob mitgeführte bzw. aufgefundene Waffen legal geführt werden bzw. der Besitz legal ist.

Das Projekt Waffenbesitzverwaltung wird im Rahmen der Projektfortschreibung weiter von uns begleitet.

14. Justiz

14.1 Rechtsstaatliche Sicherungen bei der Telekommunikationsüberwachung

Der Gesetzgeber und die Strafverfolgungsbehörden müssen wirksame Vorkehrungen treffen, damit die Rechte Betroffener bei einer Überwachung der Telekommunikation in der Praxis besser geschützt werden.

Das Max-Planck-Institut für ausländisches und internationales Strafrecht hat im Mai 2003 ein Gutachten zur Rechtswirklichkeit und Effizienz der Überwachung der Telekommunikation und anderer verdeckter Ermittlungsmaßnahmen im Strafverfahren vorgelegt. Im Anschluss an dieses Gutachten, das im Auftrag des Bundesministeriums der Justiz erstellt wurde, hat die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 25./26. September 2003 in Leipzig eine Entschließung verabschiedet, die Forderungen an den Gesetzgeber und die Strafverfolgungsbehörden für ein höheres rechtsstaatliches Schutzniveau enthält. Die Bedeutung dieser Forderungen ergibt sich insbesondere daraus, dass die Zahl der Anordnungen zur Telekommunikationsüberwachung pro Jahr im Zeitraum von 1990 bis 2000 um das Sechsfache auf über 15.700 gestiegen ist.

Der Richtervorbehalt, der eine effiziente präventive Kontrolle von Grundrechtseingriffen gewährleisten soll, muss in der Praxis gestärkt werden. Insbesondere ist es erforderlich, dass Überwachungsanordnungen nicht nur formelhaft, sondern substanziell und im Hinblick auf den Einzelfall begründet werden. Die Bewertung der Ermittlungsergebnisse, die Grundlage der Anordnung sind, darf nicht allein der Kriminalpolizei und Staatsanwaltschaft vorbehalten bleiben, sondern muss vom Richter in eigener Verantwortung nachvollzogen und kritisch überprüft werden. Der Gesetzgeber sollte festlegen, dass personenbezogene Informationen aus Überwachungsmaßnahmen, die auf einer unzulänglich begründeten Anordnung beruhen, weder zu Beweiszwecken noch als Ansatz für weitere Ermittlungen verwendet werden dürfen.

Der Schutz persönlicher Vertrauensverhältnisse zu nahen Angehörigen und Berufsgeheimnisträgern (z. B. Ärzten, Rechtsanwälten, Journalisten), denen im Strafprozess ein Zeugnisverweigerungsrecht zusteht, sollte auch bei Überwachungen der Telekommunikation garantiert sein. Der Gesetzgeber sollte zu diesem Zweck Beweiserhebungsverbote, die bereits eine Datenerhebung in besonders geschützten Bereichen ausschließen, mindestens jedoch Beweisverwertungsverbote schaffen.

Personenbezogene Informationen aus Telekommunikationsüberwachungen und anderen heimlichen Ermittlungsmaßnahmen im Strafprozess unterliegen einer besonderen Zweckbindung. Sie dürfen nur unter engen, im Gesetz abschließend bestimmten Voraussetzungen für andere Strafverfahren oder außerhalb der Rechtspflege genutzt oder übermittelt werden. Damit diese Zweckbindung in der Praxis durchgesetzt wird, bedarf es einer speziellen Kennzeichnung der Daten, die ihre Herkunft aus einer Überwachungsmaßnahme deutlich macht.

Die Untersuchung durch das Max-Planck-Institut hat gezeigt, dass die gesetzlich vorgeschriebene Benachrichtigung der Beteiligten von der Überwachung in ca. 75 % der Fälle unterbleibt oder in den Akten zumindest nicht dokumentiert wird. Dadurch wird die Möglichkeit der Beteiligten, nachträglich die Rechtmäßigkeit der Maßnahme gerichtlich überprüfen zu lassen, erheblich beeinträchtigt. Diese Defizite beim Gesetzesvollzug müssen von den Strafverfolgungsbehörden behoben werden. Ferner sollte der Gesetzgeber nicht nur – wie bislang schon – bei Maßnahmen der akustischen Wohnraumüberwachung, sondern künftig auch für Telekommunikationsüberwachungen vorschreiben, dass die Benachrichtigung der Beteiligten nur mit richterlicher Zustimmung länger als sechs Monate nach Beendigung der Maßnahme zurückgestellt werden darf. Auch für diese richterliche Zustimmung bedarf es einer substanziellen, auf den Einzelfall abstellenden Begründung.

14.2 Behördlicher Aktentransport

Die Defizite bei der Versendung sensibler personenbezogener Unterlagen geben nach wie vor Anlass zu erheblicher Besorgnis.

Unsere Kontrollen beim Behörden-Transport-Service (BTS), die in den Vorjahren bereits gravierende Verletzungen des Datenschutzes ergeben hatten (vgl. 17. TB, 18; 18. TB, 5.2), setzten wir im Berichtszeitraum intensiv fort. Wegen deutlicher Mängel bei der Versendungspraxis einzelner Amtsgerichte sahen wir uns im März 2002 zu einer förmlichen Beanstandung gegenüber dem Präses der Justizbehörde veranlasst.

Auch danach stellten wir Datenschutzverstöße im Verantwortungsbereich der Justiz fest. Offen ohne Umschlag vorgefunden wurden z. B. ein beim Verwaltungsgericht Hamburg anhängiger Auskunftsantrag zur polizeilichen Raster-

fahndung (vgl. auch 13.1 und 18. TB, 19.2), ein Aufnahmeersuchen der Staatsanwaltschaft Hamburg zur Unterbringung des Betroffenen in einem psychiatrischen Krankenhaus, Beschlüsse in Betreuungssachen sowie neurologische, kardiologische, orthopädische und urologische Gutachten aus sozialgerichtlichen Verfahren. Ferner wurden wir durch den unverschlossenen Transport darauf aufmerksam, dass das Insolvenzgericht auf telefonisches Ersuchen Bescheinigungen über Spielbankbesuche des Betroffenen übermittelt hat.

Wir gingen zunächst davon aus, dass es sich bei diesen Verstößen um – gravierende – Einzelfälle handelte. Zu dieser Annahme gelangten wir auch deshalb, weil die Gerichte ab Mitte 2002 begonnen haben, den aufgedeckten Mängeln durch stichprobenartige interne Überprüfungen mit monatlicher Dokumentation und Berichtspflicht gegenüber dem Präsidenten des Amtsgerichts Hamburg Rechnung zu tragen.

Bei einer weiteren Kontrolle im Oktober 2003 beobachteten wir allerdings eine besorgniserregende Häufung von offenen Sendungen. So fanden wir in größerer Anzahl Beschlüsse über die vorläufige Entziehung der Fahrerlaubnis, Testamente und Erbscheine sowie Unterlagen aus Verfahren vor dem Hamburgischen Oberverwaltungsgericht in Ausländer- und Asylsachen unverschlossen vor. Daher haben wir der Justizbehörde eine weitere Beanstandung in Aussicht gestellt. Die Gerichte teilten uns darauf mit, dass den für die Defizite Verantwortlichen die erforderlichen Belehrungen erteilt und weitere 100 verschließbare Sammel-Transportkisten angeschafft worden seien. Wir werden die Entwicklung auch künftig aufmerksam verfolgen.

Im November 2003 fanden wir beim BTS einige Auskünfte aus dem Zentralregister und dem Erziehungsregister sowie in erheblicher Anzahl Hinweise auf Grund von Suchvermerken im Zentralregister offen vor. Die Registerauskünfte enthielten umfangreiche Eintragungen, z. B. über Verurteilungen wegen sexuellen Missbrauchs von Kindern sowie über die Unterbringung in einem psychiatrischen Krankenhaus oder in einer Entziehungsanstalt. Aus den Hinweisen der Registerbehörde (Generalbundesanwalt) konnten wir z. B. die Untersuchungs- oder Strafhaft ersehen, in einem Falle aus dem Aktenzeichen auf die Durchführung einer DNA-Analyse schließen.

Die Mitteilungen des Generalbundesanwalts waren sämtlich an die Staatsanwaltschaft Hamburg adressiert, dort zum Zeitpunkt unserer Prüfung aber offensichtlich noch nicht eingegangen. Wir haben veranlasst, dass die sensiblen Unterlagen beim BTS vor ihrer Weiterbeförderung verschlossen wurden, und die Staatsanwaltschaft Hamburg von unseren Feststellungen in Kenntnis gesetzt. Wir sind bemüht, die für den massiven Datenschutzverstoß Verantwortlichen kurzfristig zu ermitteln, und behalten uns je nach Ergebnis dieser Bemühungen eine förmliche Beanstandung vor.

15. Strafvollzug

Einheften des Vollstreckungsblattes in die Gesundheitsakte von Gefangenen

Die personenbezogenen Angaben in der Gesundheitsakte müssen auf den Umfang beschränkt bleiben, der für die Aufgabenwahrnehmung und den Schutz des medizinischen Personals erforderlich ist.

Gefangene im Strafvollzug haben Anspruch auf Gesundheitsfürsorge und ärztliche Versorgung. Deren Qualität hängt auch davon ab, dass dem Arzt die für eine Untersuchung oder Behandlung erforderlichen Informationen über den Patienten rechtzeitig vorliegen. Zu diesem Zweck werden Gesundheitsakten über die Gefangenen geführt. Sie sind immer dann vorzulegen, wenn der Gefangene in der Anstalt dem Arzt vorgestellt oder in das Krankenhaus innerhalb des Vollzuges eingewiesen wird. Dagegen bestehen aus Sicht des Datenschutzes im Grundsatz keine Bedenken. Die gegenwärtige Praxis, dass aus dem Vollstreckungsblatt in der Gesundheitsakte für Arzt und Krankenpfleger in sämtlichen Fällen auch die Straftat, die zum Haftaufenthalt geführt hat, und die Höhe der Freiheitsstrafe ersichtlich sind, bedarf jedoch dringend einer kritischen Überprüfung.

Diese Praxis stützt sich auf die bundeseinheitlich geltende Vollzugsgeschäftsordnung (VGO). Der Gesetzgeber hat den Inhalt der Gesundheitsakte nicht näher geregelt, so dass die Einzelheiten durch eine Allgemeine Verfügung der Justizbehörde festgelegt werden. Keines der Argumente, die von der Justizbehörde zur Rechtfertigung der Vollzugspraxis angeführt wurden, hat uns überzeugt. Richtig ist zwar, dass der Arzt im Einzelfall prüfen muss, ob es sinnvoll ist, unmittelbar vor einer Entlassung des Gefangenen noch eine Operation oder eine zahnprothetische Behandlung durchzuführen. Zu diesem Zweck muss der Arzt jedoch nur den voraussichtlichen Zeitpunkt der Entlassung kennen, nicht hingegen das Strafmaß oder die abgeurteilte Straftat.

Die Kenntnis von dem Delikt, das der Gefangene begangen hat, ist auch nicht deshalb erforderlich, damit der Arzt Simulanten erkennen kann, die mit falschen Angaben eine Behandlung oder ein Medikament erschleichen wollen. Der Arzt muss sich, wie bei den in Freiheit befindlichen Patienten auch, auf seine Fachkunde und Erfahrung verlassen, um den Wahrheitsgehalt der Schilderung des Patienten zu beurteilen. Im Übrigen kann auch bei einem wegen Betruges Vorbestraften nicht generell unterstellt werden, dass die von ihm beschriebenen Beschwerden oder Schmerzen nur vorgetäuscht sind.

Um den zusätzlichen Verwaltungsaufwand für die Vollzugsbediensteten bei der Führung von Gesundheitsakten in möglichst engen Grenzen zu halten, haben wir dem Strafvollzugsamt wiederholt angeboten, mit uns einen Katalog von Straftaten abzustimmen, für die ein nachvollziehbares Informationsinteresse bei Ärzten und Krankenpflegern besteht. Nur diese Straftaten sollten aus der Gesundheitsakte hervorgehen. Dabei muss neben medizinischen Kriterien

auch der Schutz von Leben, Gesundheit und Freiheit des Behandlungspersonals bedacht werden.

So haben wir keine Bedenken dagegen, dass Ärzte und Krankenpfleger durch einen knappen Hinweis in der Gesundheitsakte von einer vorsätzlichen Tötung, Körperverletzung, Geiselnahme, einem Sexual-, Betäubungsmittel- oder Waffendelikt erfahren, das der Gefangene begangen hat. Dagegen ist es weder medizinisch noch zur Sicherheit des Personals notwendig, dass aus der Gesundheitsakte eine Verurteilung z. B. wegen Subventions- oder Kapitalanlagebetruges, wegen Geldwäsche oder einer Insolvenzstraftat zu entnehmen ist. Die Höhe der Freiheitsstrafe sollte in keinem Falle aus der Gesundheitsakte ersichtlich sein.

Leider hat sich das Strafvollzugsamt, wie in zahlreichen anderen Fragen des Datenschutzes auch, unseren Vorschlägen gänzlich verschlossen. Deshalb haben wir im Juli 2003 unsere Überlegungen auch den Mitgliedern des Unterausschusses Datenschutz der Hamburgischen Bürgerschaft unterbreitet.

16. Gesundheit

16.1 Gesundheitsmodernisierungsgesetz (GMG)

„In letzter Minute" wurde ins GMG ein neues Abrechnungssystem für ambulante Behandlungen eingeführt, das den Krankenkassen umfassende Informationen über ihre Versicherten gibt. Datenschutzfreundlicher sind dagegen die Vorschriften zur elektronischen Gesundheitskarte.

Im Mai 2003 beteiligten wir uns mit einer eigenen Stellungnahme an der bundesweiten Diskussion der Datenschutzbeauftragten um die verschiedenen Entwürfe für das neue Gesundheitsmodernisierungsgesetz.

Das im September vom Bundestag verabschiedete Gesetz enthält eine ganze Reihe von Vorschriften mit datenschutzrechtlicher Relevanz. Besonders einschneidend ist ein neues Abrechnungssystem für ambulante Behandlungen, das erst unmittelbar vor den Lesungen im Bundestag in den Gesetzentwurf eingeführt wurde: Bisher übermittelten die Kassenärztlichen Vereinigungen den Krankenkassen Informationen über ambulante Leistungen nur fallbezogen, aber nicht versichertenbezogen. In Zukunft sollen die Kassenärztlichen Vereinigungen den Kassen auch mitteilen, welcher Arzt welche Leistungen aufgrund welcher Diagnose für welche Patienten erbracht hat.

Die damit beabsichtigte Erweiterung der Kontrollmöglichkeiten der Kassen hätte jedoch auch mit pseudonymisierten Übermittlungen erreicht werden können, die bei konkreten Auffälligkeiten die notwendige versichertenbezogene Aufklärung zugelassen, im übrigen aber einen offenen Personenbezug vermieden hätten. In einer Entschließung mahnte die Konferenz der Datenschutzbeauftragten des Bundes und der Länder am 26.September 2003 strenge

Zweckbindungsregeln an, um zu verhindern, dass die Krankenkassen die verschiedenen Patientendaten zu umfassenden Versichertenprofilen zusammen führen.

Der neue § 291 a Sozialgesetzbuch V führt die „elektronische Gesundheitskarte“ ein. Diese soll vor allem das elektronische Rezept ermöglichen, aber auch Optionen für elektronische Arztbriefe, Notfalldaten und Behandlungsdokumentationen enthalten. Die tatsächliche Umsetzung und Anwendung dieser Optionen wird ausdrücklich an das Einverständnis der Patienten gebunden. Die informationelle Selbstbestimmung der Patienten soll sich nicht auf das Ob der Nutzung der elektronischen Karte beschränken, sondern sich auch auf das Wie – z. B. hinsichtlich des Umfangs der zu speichernden Daten und der Lesebefugnisse – erstrecken. Datenschutzrechtlich wird es entscheidend auf die konkrete technische und organisatorische Ausgestaltung der gesetzlich vorgesehenen Chipkarte und ihres Einsatzes ankommen.

Weitere datenschutzrechtlich relevante Bestimmungen im GMG seien hier nur kurz aufgezählt:

- Die Krankenversicherungskarte erhält zur Verhinderung des Missbrauchs ein Lichtbild des Versicherten und das Merkmal „Zuzahlungsstatus“.
- Die gemeinsamen Prüfungs- und Beschwerdeausschüsse der Kassen und Kassenärztlichen Vereinigungen bekommen von den Kassen erstmals auch Abrechnungsdaten aus Krankenhäusern und Arzneimittelabrechnungen.
- Neu eingeführt wird eine zentrale „Arbeitsgemeinschaft für Aufgaben der Datentransparenz“. Die Kassen übermitteln Versichertendaten an eine Vertrauensstelle, die diese pseudonymisiert und zur zweckgebundenen Auswertung an eine Datenverarbeitungsstelle weitergibt.
- Die Löschungsfristen für Abrechnungsdaten werden von 2 auf 4 Jahre verdoppelt.
- Die bisher nicht umgesetzte Pflicht der Leistungserbringer, die Patienten über für sie erbrachte Leistungen und deren Kosten zu unterrichten, wird nun als „Patientenquittung“ „auf Verlangen“ und gegen Gebühr präzisiert.

Es ist wahrscheinlich, dass die Umsetzung der neuen Verfahren und Instrumente in der Praxis erhebliche datenschutzrechtliche Fragen aufwerfen wird.

16.2 Prüfung Neugeborenen-Screening

Die Prüfung des Neugeborenen-Screenings im Universitätsklinikum Eppendorf (UKE) deckte Mängel auf. Insbesondere die namensbezogene unbefristete Aufbewahrung der Blutproben und Speicherung der Befunddaten ist datenschutzrechtlich nicht zu vertreten.

Bundesweit hat der Datenschutz die Brisanz des Neugeborenen-Screenings als mögliche Ressource für die Genforschung entdeckt. Die Krankenhausträger sind zunehmend bemüht, ihre Gewebe-, Blut- und Datensammlungen interessierten Forschern und Arzneimittelherstellern zur entgeltlichen Nutzung anzubieten. Das UKE hat kürzlich eine entsprechende Vermarktungs-Gesellschaft gegründet und fördert derzeit bei den Ärztinnen und Ärzten das Bewusstsein für den Wert dieser Ressourcen, aber auch für die Anforderungen an deren Organisation (vgl. auch 17.1).

Vor diesem Hintergrund haben wir im September 2003 das Neugeborenen-Screening in der UKE-Kinderklinik geprüft. Das Screening-Verfahren läuft wie folgt ab: Vor der Geburt erhalten die Gebärenden ein Faltblatt, das über die Neugeborenen-Untersuchungen informiert. Nach der Geburt wird dem Kind Blut entnommen und auf einen Filzstreifen aufgetragen. Dieser Streifen ist Teil einer Karte, auf der die Personalien der Mutter und des Kindes sowie z. B. Geburtsgewicht, Mehrling, Gestationsalter und – freiwillig – die Nationalität eingetragen werden. Aus den Blutproben werden automatisiert kleine Plättchen herausgestanzt und ebenfalls automatisch analysiert. In einer Datenbank erfassen die Mitarbeiterinnen der Screening-Stelle die Personalien des Kindes zusammen mit den (seltenen) auffälligen Befunden oder (meist) mit dem Vermerk „unauffällig". Die Karten mit den Restblutproben und den Personalien werden chronologisch gebündelt aufbewahrt. Seit Einrichtung dieses Verfahrens 1992 wurden weder Karten vernichtet noch Daten gelöscht.

Die Prüfung ergab folgende Mängel und Sicherheits-Defizite:

- Das Informationsfaltblatt erreicht möglicherweise viele Gebärende gar nicht. Es enthält keine abschließende Aufzählung der Krankheiten, auf die untersucht wird, und keine Aufklärung über die weitere Datenverarbeitung, einschließlich der dauerhaften namensbezogenen Speicherung.
- Die beiden Laborräume der Screening-Stelle, in denen sich der PC befindet und wo ein Teil der Karten offen lagert, stehen meist offen und sind für Mitarbeiterinnen und Mitarbeiter anderer Labore auf demselben Etagenflur ohne weiteres zugänglich.
- Der PC, in dem die Screening-Ergebnisse namensbezogen gespeichert werden, hat keinerlei Zugriffsschutz, insbesondere keinen Passwortschutz.
- Weder für die Aufbewahrung der Karten noch für die Speicherung der Daten gibt es eine Befristung, also einen möglichen Zeitpunkt für eine Vernichtung bzw. Löschung.

Darüber hinaus erscheinen grundsätzliche Überlegungen dazu geboten, ob nach der Analyse und Befundmitteilung noch ein Bedarf für eine namensbezogene Aufbewahrung der Filzstreifen besteht. In anderen Bundesländern werden Proben nach wenigen Wochen oder Monaten vernichtet, anonymisiert

oder pseudonymisiert. Dazu ist zunächst zu klären, wie lange sich das Neugeborenenblut überhaupt für spätere Kontrollanalysen oder für Forschungszwecke eignet.

Sollten sich das Blut bzw. wichtige Bestandteile lange halten, erscheint jedenfalls für die Nutzung zu Forschungszwecken ein direkter Namensbezug auf das Kind nicht mehr erforderlich. Ob stattdessen eine vollständige Anonymisierung (z. B. durch Abtrennen des Filzstreifens von der Karte) oder eine Pseudonymisierung (Codierung mit Re-Identifizierungsmöglichkeit) geboten ist, hängt in erster Linie von den Zielsetzungen der jeweiligen Forschungsprojekte ab. Dabei ist jedoch auch zu berücksichtigen, dass der Behandlungsvertrag für die Entbindung sich nur auf die Blutanalyse zur Erkennung vorher festgelegter Krankheiten bezog, nicht aber auf eine personenbeziehbare (auch pseudonyme) Aufbewahrung zu noch unbestimmten Forschungszwecken.

Ob die theoretische Möglichkeit einer späteren Zweitanalyse in der Praxis auch tatsächlich genutzt wird – z. B. wenn eine durch den Screening-Befund ausgeschlossene Krankheit später doch auftritt -, ist mitentscheidend für die „Erforderlichkeit“ einer weiteren namensbezogenen oder zumindest personenbeziehbaren Aufbewahrung und Datenspeicherung. Allenfalls kommt bei längerer Aufbewahrung und Speicherung jedoch auch hier nur eine solche in pseudonymisierter Form in Betracht. Dabei ist auch an einen externen Datentreuhänder zu denken, der die Pseudonymisierung und De-Pseudonymisierung organisiert, ohne Kenntnis von den medizinischen Daten zu bekommen.

Insbesondere diese Pseudonymisierungfragen – bei geklärter Erforderlichkeit eines Personenbezuges – bedürfen einer vertieften Prüfung, die auch den Plänen des UKE zur Vermarktung von Ressourcenbanken insgesamt zugute kommen wird.

16.3 Brustzentrum Hamburg-Süd

Durch unsere Beratung konnte die Organisation und die Aufklärungs- und Einwilligungserklärung des Behandlungszentrums für Brustkrebspatientinnen in Hamburg-Harburg datenschutzgerecht gestaltet werden.

Seit November 2002 begleiteten wir die Gründung des „Brustzentrum Hamburg-Süd e.V.“. Ziel dieses Zentrums ist es, einerseits die verschiedenen an einer Behandlung beteiligten Ärzte und Stellen durch die Nutzung der gleichen Praxis-Software miteinander kompatibel zu machen und andererseits die Qualität der Behandlungsergebnisse zu sichern bzw. zu steigern. Uns wurden Verfahrensbeschreibung und Datensicherheitskonzept der in Aussicht genommenen Praxis-Software sowie das entsprechende Datenkonzept der „Mamma-

Akte“ zur Verfügung gestellt. In mehreren Gesprächen und Briefwechseln konnten folgende Punkte geklärt werden:

- Alle Mitglieder des Zentrums dokumentieren ihre Behandlungen – ggf. zusätzlich – mit einem in Nordrhein-Westfalen entwickelten speziell onkologischen Dokumentationssystem.
- Die Übermittlung der Behandlungsdaten an weiter behandelnde Zentrumsmitglieder erfolgt zwar patientinnenbezogen, aber verschlüsselt auf einer Diskette, die die Patientin selbst übergibt. Nur Zentrumsmitglieder (Labor und Pathologie), die von der Patientin nicht aufgesucht werden, erhalten die Diskette – mit Einwilligung der Patientin – per Post oder Boten. Die Mitglieder des Zentrums erfahren, unter welcher Fall-Nummer die anderen behandelnden Stellen die Patientin jeweils führen.
- Daneben werden die Behandlungsdaten in pseudonymisierter Form an eine zentrale Datenbank des Zentrums im Allgemeinen Krankenhaus Harburg versandt und dort gespeichert. Das Pseudonym enthält das Kennzeichen der behandelnden und übermittelnden Stelle sowie deren (nicht-sprechende) Fallnummer für die Patientin.
- Die Personen, die die Datenbank zu Qualitätssicherungszwecken auswerten, dürfen nicht identisch sein mit einzelnen Behandlern. Bei Auffälligkeiten wird dem betroffenen Behandler die Fallnummer einer betroffenen Patientin mitgeteilt, damit er sie de-pseudonymisiert und das Problem klären kann, ohne dem Datenbank-Personal die Identität der betroffenen Patientin offenbaren zu müssen.
- Soweit Daten aus der zentralen Datenbank an externe Forscher weitergegeben werden sollen, sind die Fallnummern noch einmal zu verschlüsseln oder vollständig zu anonymisieren.
- Jede Patientin erhält in der ersten behandelnden Stelle eine ausführliche Information über das Brustzentrum, seine Mitglieder und die Datenverarbeitungsverfahren und wird um eine schriftliche Einwilligung gebeten. Auch die Folgen eines möglichen Widerrufs der Einwilligungserklärung werden umschrieben.
- Festzulegen ist noch, wie lange die Daten in der zentralen Qualitätssicherungs-Datenbank gespeichert werden sollen.

In der weiteren beratenden Begleitung und ggf. Prüfung werden wir vor allem auf die Einhaltung der Trennung zwischen personenbezogener Behandlung und pseudonymisierter Qualitätssicherung achten. Möglicherweise muss zu diesem Zwecke noch eine weitere Verschlüsselung der Behandler-Fallnummern gefordert werden. Die Einführung einer on-line-Übermittlung von Behandlungsdaten (statt der Diskette) sowie von Fremdzugriffen durch Fernwartung bedarf der erneuten datenschutzrechtlichen Abstimmung.

Inzwischen hat das Brustzentrum als eingetragener Verein und speichernde Stelle der zentralen Datenbank einen betrieblichen Datenschutzbeauftragten bestellt.

Bezüglich der Gründung weiterer „Brustzentren“ – wie z. B. dem „Brustzentrum-Nord“ – werden wir uns bei Beratung und Kontrollen von den vorstehenden Eckpunkten leiten lassen.

16.4 Pseudonymisierung von Laboraufträgen

Die Datenschutzbeauftragten fordern bundesweit, bei Analyseaufträgen an Labore die Patientennamen grundsätzlich zu codieren. Dies trifft in der Praxis auf wenig überzeugende prinzipielle Widerstände.

Schon vor 10 Jahren hatten wir anlässlich der Routineanalysen von Blut- und Stuhlproben von Asylbewerbern mit dem Hygienischen Institut die Möglichkeiten einer pseudonymisierten Auftragsvergabe diskutiert und verschiedene Fallkonstellationen unterschieden (vgl. 12.TB, 21.8.1). Seitdem haben auch andere Datenschutzbeauftragte in ihrem Zuständigkeitsbereich die Initiative ergriffen und die Pseudonymisierung von Laboraufträgen gefordert. Der Bundesbeauftragte für den Datenschutz äußerte sich in gleichem Sinne in seinem Tätigkeitsbericht von 2001/2002. Dem widersprachen im Juli 2003 der Berufsverband Deutscher Laborärzte e.V. und die Deutsche Vereinte Gesellschaft für Klinische Chemie und Laboratoriumsmedizin e.V. in schriftlichen Stellungnahmen. In einem Bund-Länder-Arbeitskreis erörterten die Datenschutzbeauftragten die Argumente der Ärzteverbände, sahen sie aber nur in Ausnahmefällen als begründet an.

Das Thema betrifft sowohl den öffentlichen Gesundheitsdienst (Gesundheitsämter), das Universitätsklinikum Eppendorf und die Landesbetriebs-Krankenhäuser als Auftraggeber wie als Labor (Hygieneinstitut) als auch den nicht öffentlichen Bereich – private Krankenhäuser und niedergelassene Ärzte als Auftraggeber und z. B. private Spezial- und Großlabors als Auftragnehmer.

Die Forderung nach einer Pseudonymisierung von Laboraufträgen bezieht sich auf den Bereich der gesetzlich Versicherten, weil diese vom Labor keine eigene Rechnung erhalten. Ferner geht es nur um die Fälle, in denen es keinen persönlichen Kontakt zwischen dem Patienten und dem Laborarzt gibt und dieser auch nicht als beratender Konsiliararzt zur persönlichen Behandlung hinzugebeten wird. Betroffen sind damit die alltäglichen Routineanalysen, die häufig in Großlabors, z.T. über Laborgemeinschaften niedergelassener Ärzte ohne weitere Patientenkontakte durchgeführt werden.

In diesen Regelfällen ist eine Übermittlung des Patientennamens durch den Auftraggeber an das Labor nicht erforderlich. Ein Pseudonym reicht aus. Der Einwand, ohne den Patientennamen bestehe Verwechslungsgefahr, greift vor allem deswegen nicht durch, weil bei Namen – insbesondere ausländischen –

die konkrete Schreibweise oft unklar ist, während ein automatisiert generierter Zahlen- (Bar-)Code auf einem Etikett eindeutig ist. In beiden Fällen bedarf es einer zuverlässigen Organisation der Beauftragung (Beschriftung mit Namen bzw. Pseudonym und dessen Zuordnung) einerseits und eindeutigen Zuordnung des Analyseergebnisses zur Probe im Labor sowie zum Patienten beim Auftraggeber andererseits.

Auch das Argument, der Laborarzt müsse die Analyseergebnisse mit früheren Befunden vergleichen und dem Auftraggeber ggf. Hinweise zur weiteren Behandlung geben können, überzeugt nicht. Zum einen erscheint es eher zufällig, ob der – ggf. neue – behandelnde Arzt dasselbe Labor mit derselben bzw. einer vergleichsfähigen Analyse beauftragt. Zum anderen wäre ein solcher Vergleich auch mit relativ dauerhaften Pseudonymen wie der Krankenversicherungsnummer möglich (, wenn frühere Analysen nicht ausschließlich mit dem Patientennamen archiviert wurden).

Der weitere Einwand, auch Laborärzte müssten nach der Berufsordnung ihre Tätigkeit dokumentieren, übersieht, dass dies auch mit Pseudonymen erfolgen kann, wenn im seltenen Bedarfsfall über den Auftraggeber die Identität der Patienten zu ermitteln ist. Eine eigene patientennamens-bezogene Dokumentationssammlung beim Labor – in der Regel ohne Kenntnis der betroffenen Patienten – ist datenschutzrechtlich nicht nur nicht erforderlich, sondern angesichts zunehmender Begehrlichkeiten der Forschung auch missbrauchsgefährdet.

Nach dem Infektionsschutzgesetz (IfSG) sind auch Labore verpflichtet, bestimmte Infektionen namensbezogen an das Gesundheitsamt zu melden. Dies bezieht sich zunächst auf die dem Labor tatsächlich vorliegenden Daten; das IfSG normiert selbst keine gesetzliche Befugnis oder gar Verpflichtung der Auftraggeber, den Laboren die Namen der Patienten zu übermitteln. Der Auftraggeber (der behandelnde Arzt) kann die geforderte namentliche Meldung nach Zuordnung des Analyseergebnisses selbst abgeben. Damit die Infektionsschutzbehörden und das Robert-Koch-Institut aber bei Gefahr so schnell wie möglich reagieren können, erscheint es datenschutzrechtlich vertretbar, bei Laboraufträgen, die auf die Ermittlung von IfSG-Krankheiten gerichtet sind oder solche einschließen, einen Namensbezug zuzulassen.

Ist damit für die Regel- und Routinefälle eine Pseudonymisierung der Laboraufträge geboten – und bei vielen Aufträgen an das Hygieneinstitut, einzelne Großlabore und bei Laborgemeinschaften auch schon tägliche Praxis –, so gibt es eine Reihe von Konstellationen, die ausnahmsweise eine namensbezogene Beauftragung des Labors rechtfertigen. Dies liegt weitgehend in der Beurteilungskompetenz des auftraggebenden behandelnden Arztes: So kann ein Vergleich mit früheren, nur namensbezogen gespeicherten Analysen erbeten oder eine Beratung des Patienten durch das Labor selbst gewünscht werden. Bei Infektions-Untersuchungen von verschiedenen Familienmitgliedern

(z. B. Asylbewerbern) könnte die Zusammengehörigkeit durch Vornamen gekennzeichnet werden. In besonders eiligen und wichtigen Laboruntersuchungen in Krankenhäusern kann die Namensangabe zur umgehenden Ergebnis-Weitergabe und Patientenzuordnung auf der Station erforderlich sein.

Die nun bundesweit abgestimmte Position der Datenschutzbeauftragten zur Pseudonymisierung von Laboraufträgen werden wir vertreten und mit den betroffenen Stellen im Hinblick auf die jeweiligen konkreten Konstellationen erörtern.

17. Forschung

17.1 Probenbank des UKE-Zentrallabors

Unsere Beratung des Universitätsklinikums Eppendorf (UKE) bei der Einrichtung einer Probenbank des Zentrallabors verbesserte das Verfahren zur Anonymisierung von Proben und Daten.

Im August 2003 trat das Institut für klinische Chemie / Zentrallaboratorien des UKE mit einem Konzept für eine Probenbank an uns heran. Restproben aus Routine-Analysen zu Behandlungszwecken sollen durch klinische Daten ergänzt und interessierten Dritten (Forschern, Arzneimittelherstellern) zur Verfügung gestellt werden. Auf eine konkrete Einwilligung sollte aus Praktikabilitätsgründen verzichtet werden. Mit dieser Probenbank will das UKE seine Ressourcen auch kommerziell besser nutzen.

Zunächst sah das UKE vor, dass die Proben und Daten mit dem Namen und dem Geburtstag der Patienten gekennzeichnet werden und bleiben, bis sie an einen Interessenten weitergegeben werden. Eigene Forschungsanalysen während der Aufbewahrungszeit sind nicht vorgesehen. Falls notwendig sollten die Patienten bereits im Behandlungsvertrag über dieses Verfahren aufgeklärt und um eine pauschale Vorab-Einwilligung gebeten werden.

In unserer Beratung machten wir deutlich, dass Behandlungs- und Forschungszweck voneinander zu trennen sind, eine Erstreckung des Behandlungsvertrages auf Forschungsmaßnahmen deswegen nicht in Betracht kommt. Vielmehr bemühten wir uns in einem ausführlichen Gespräch um eine frühestmögliche, aber noch praxistaugliche Anonymisierung von Proben und Daten. Das Dilemma war, dass erst die Routine-Analyse und die klinischen (Behandlungs-)Daten über die Eignung der Probe für die Probenbank entscheiden, die Daten aber zum Teil erst später verfügbar sind und dem Patienten zugeordnet werden müssen. Eine vorsorgliche ausführliche Vorab-Aufklärung und -Einwilligung für den Fall, dass sich nachträglich die Eignung des Probenrestes ergeben sollte, erschien wenig sinnvoll und datenschutzrechtlich zweifelhaft.

Mit dem UKE haben wir schließlich folgende Lösung gefunden, die wir datenschutzrechtlich noch für vertretbar halten: Aufgrund der klinischen Daten, insbesondere der Diagnose, die bereits zur Routine-Analyse (zu Behandlungszwecken) übermittelt werden, trifft das Labor-Personal eine vorläufige Entscheidung über die Vernichtung oder Aufbewahrung des Probenrestes und fordert im letzteren Fall von der behandelnden Stelle umgehend ergänzende bzw. vertiefende klinische Informationen ab, die auf ein Minimum reduziert wurden.

Diese Datenerhebung hat jedoch innerhalb der Zeit zu geschehen, in der die Patientin oder der Patient noch im UKE aufgenommen ist und behandelt wird. Auch wenn der Probenrest und die ergänzenden Daten streng genommen bereits außerhalb des Behandlungszweckes – und damit außerhalb des Behandlungsvertrages – aufbewahrt bzw. übermittelt werden, besteht für den Patienten, das Labor und den behandelnden Arzt in dieser Zeit noch ein Zusammenhang mit der Behandlungssituation. Jederzeit kann das Labor oder das medizinische Personal zu Behandlungszwecken weitere Maßnahmen ergreifen oder Daten erheben. Die besonders sensible Hauptdiagnose ist dem Labor ohnehin bereits bekannt.

Die Forschungsklausel des Hamburgischen Krankenhausgesetzes ist hier zwar mangels eines konkreten, befristeten Forschungsprojekts nicht direkt anwendbar. Ihre Aussage, dass die behandelnden Ärzte desselben Krankenhauses auch mit den Behandlungsdaten ihrer Patienten forschen dürfen, legt jedoch auch eine rechtliche Legitimität des dargestellten Verfahrens zumindest nahe.

Spätestens mit der Entlassung des Patienten aus dem UKE – und nicht erst mit dem Ende der „Behandlung“, die bei Krebspatienten meist über Jahre andauert – ist die endgültige Entscheidung über die Aufnahme von Probe und Daten in die Probenbank zu treffen und die Anonymisierung durchzuführen. Dazu sind nicht nur der Name und das Geburtsdatum zu entfernen, sondern auch die Einzelbefunde so zu runden, dass auch über sie eine Re-Identifikation nicht mehr möglich ist. Dies gilt auch für externe Befunde früherer Analysen, die die behandelnde Einheit aus der Patientenakten entnommen und dem Labor zugesandt hatte. Ferner ist die organisatorische und räumliche Abschottung zwischen Routine-Analyse und Probenbank endgültig sicherzustellen.

Nach Beendigung des stationären Aufenthalts der betroffenen Patienten existiert damit nur noch eine anonymisierte Proben- und Datenbank, die sowohl von den Forschern des UKE als auch von externen Forschern genutzt werden kann.

17.2 „Lebensbilder“ aus der NS-Zeit

Auch heute noch muss Forschung über Lebensschicksale aus der NS-Zeit die Persönlichkeits- und Datenschutzrechte der Betroffenen und ihrer Angehörigen achten.

Die Akten des Amtes für Wiedergutmachung sind auch über 50 Jahre nach ihrer Entstehung Fundgruben für Familien- und Zeitgeschichte-Forscher. Im Rahmen einer Eingabe hatten wir zu beurteilen, ob und unter welchen Bedingungen ein Hamburger Bürger Wiedergutmachungsakten von 10 Personen einsehen und auswerten darf, die Angeklagte in einem Hochverratsprozess in der NS-Zeit waren. Einer dieser Angeklagten war der Vater des Antragstellers. Die Wiedergutmachungsakten enthalten zahlreiche Informationen über die Lebensumstände der Betroffenen, aber auch von deren Familien und Nachkommen.

Zunächst wiesen wir das Amt für Wiedergutmachung auf die Forderung des Hamburgischen Archivgesetzes hin, abgeschlossene Akten innerhalb von 30 Jahren dem Staatsarchiv anzubieten. Vom Archiv übernommene Akten unterliegen hinsichtlich personenbezogener Daten detaillierten Nutzungsregeln, die das Persönlichkeitsrecht der betroffenen Personen schützen sollen. Da die Wiedergutmachungsakten jedoch auch heute noch häufig gebraucht würden, gibt es nach Auskunft des Amtes eine Vereinbarung mit dem Staatsarchiv, ihm die Akten erst 2010 zu übergeben.

Wollte der Antragsteller zunächst private Familienforschung betreiben, will er nun anhand der 10 Familienschicksale der Frage nachgehen, wie Verfolgung im NS-Staat erlebt und erlitten wurde. Die Qualifikation für eine zeitgeschichtliche Forschung besitzt der Antragsteller. Das Forschungsergebnis möchte er in Form von „Lebensbildern“ im Sinne von Familiengeschichten veröffentlichen.

Nach §27 Abs.5 und 6 Hamburgisches Datenschutzgesetz dürfen Forscher „personenbezogene Daten ohne Einwilligung der Betroffenen nur veröffentlichen, wenn dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.“ Dies wurde in der Vergangenheit jedoch nur dann angenommen, wenn es sich um wichtige staatliche oder gesellschaftliche Funktionsträger (Richter, Polizeidirektoren u.a.) handelte, die in der Öffentlichkeit bekannt geworden sind. Dies traf bei den genannten 10 Angeklagten und deren Familien nicht zu.

Wir haben den Antragsteller deswegen dringend gebeten, sich mit den Angehörigen der betroffenen Personen zu verständigen, um eine einvernehmliche Form der Aktenauswertung und ggf. Veröffentlichung zu erreichen. Ohne eine entsprechende Einwilligung haben wir dem Antragsteller nur zugestehen können, die Akten zwar einzusehen, aber jegliche Dokumente, Exzerpte oder Vermerke auf Papier oder Datenträgern nur anonymisiert oder pseudonymisiert aus dem Amt für Wiedergutmachung mitzunehmen. Für eine Veröffentli-

chung kommt ohne eine Einwilligung nur eine anonyme Darstellung in Betracht. Dies schließt die Form von „Lebensbildern“ möglicherweise aus, die für Verwandte oder Bekannte auch ohne Namen ausreichend Anhaltpunkte für eine Re-Identifikation aufweisen werden.

Angesichts der überschaubaren Anzahl der betroffenen Personen bzw. Familien erscheint die Einholung einer Einwilligung auch vor dem Hintergrund der grundrechtlichen Forschungsfreiheit zumutbar. Die Vorstellung, dass die Familien der betroffenen NS-Verfolgten „Lebensbilder“ über sich lesen (müssen), ohne zuvor in irgendeiner Weise mit dem Autor gesprochen zu haben, zeigt die Beeinträchtigung ihres Persönlichkeitsrechts. Auch datenschutzrechtlich wäre dieses nicht vertretbar.

17.3 Forschungsprojekte

Bei einer Reihe von Forschungsprojekten konnte unsere Beratung eine Verbesserung des Datenschutzes erreichen.

Im Berichtszeitraum hatten wir wieder zu einigen Forschungsprojekten datenschutzrechtlich Stellung zu nehmen. Bei den nachstehenden Vorhaben benötigten die Forscher Daten aus dem Hamburger Krebsregister. Das Hamburgische Krebsregistergesetz sieht in diesen Fällen die Beteiligung des Hamburgischen Datenschutzbeauftragten vor.

- „Postmenopausale Hormonsubstitution und Brustkrebsrisiko“ der Arbeitsgruppe Epidemiologie der Behörde für Umwelt und Gesundheit und des UKE,
- „Akute und posttraumatische Belastungsreaktionen bei Brustkrebspatientinnen“ des Zentrums für Psychosoziale Medizin am UKE,
- „Effekte psychoonkologischer Betreuung auf die Überlebenszeit und Lebensqualität bei Patienten mit gastrointestinalen Tumoren“ des Klinikums der Christian-Albrechts-Universität zu Kiel.

Bei unserer Stellungnahme ging es um Fragen der Probanden-Rekrutierung, um die Erforderlichkeit der Krebsregisterdaten für das Vorhaben, um die Formulierung des Aufklärungs- und Einwilligungsblattes sowie um die Ausgestaltung der Anonymisierung bzw. Pseudonymisierung und der Datenlöschung. Ferner ist in diesen Fällen sicherzustellen, dass die Forscher nur Daten von solchen Krebspatienten erhalten, die seinerzeit in die Meldung an das Krebsregister eingewilligt hatten.

Die folgenden weiteren Forschungsprojekte wurden uns von Hamburger Institutionen vorgelegt:

- „Auswirkungen des Reisens auf den Gesundheitszustand der Reisenden“, Reisemedizinisches Zentrum des Bernhard-Nocht-Institutes,

- Genforschungsprojekt „Gesundes Altern“, Amalie Sieveking Krankenhaus,
- „Beziehungsbiographien im sozialen Wandel“, Klinik für Psychiatrie und Psychotherapie des UKE,
- „Kohortenstudie zur Krebsinzidenz bei den Beschäftigten des Wasserschlosses Winsen / Luhe“, Arbeitsgruppe Epidemiologie der Behörde für Umwelt und Gesundheit und des UKE,
- „Vergleichende Studie von in Hamburg lebenden Gewaltopfern“, Hamburger Initiative gegen Aggressivität und Gewalt e.V. und Institut für Rechtsmedizin am UKE,
- Telefonbefragung für das Senatsamt für die Gleichstellung,
- Befragung „Lebensqualität und Gesundheit im Alter“, Gesundheits- und Umweltamt Hamburg-Eimsbüttel,
- „Suizid und Suizidversuch. Untersuchung des Mortalitätsrisikos in einem 15-Jahres-Zeitraum“, Klinik für Psychiatrie und Psychotherapie des UKE,
- „Monitoring von Suizidversuchen im Rahmen der Multicentre Study des WHO-European Network for Suicide Research and Prevention“, Therapiezentrum für Suizidgefährdete, Klinik für Psychiatrie und Psychotherapie des UKE,
- „Survey zur Teilnahme an Schutzimpfungen im frühen Kindesalter in Hamburg“, Institut für Hygiene und Umwelt,
- „Körpermaß und Hodentumor“, Arbeitsgemeinschaft für Urologische Onkologie,
- „Services for Supporting Family Carers of Elderly People in Europe (EUROFAMCARE)“, Institut für Medizin-Soziologie des UKE,
- „Basisdokumentation forensische Psychiatrie“, Zentrum für Psychosoziale Medizin des UKE.

Eine Darstellung der datenschutzrechtlichen Probleme bei allen diesen Vorhaben würde den Berichtsrahmen sprengen. Beispielhaft sei anhand des Projekts „Monitoring von Suizidversuchen“ die immer wieder auftretende Frage nach der Personenbeziehbarkeit und Pseudonymisierung der verarbeiteten Daten skizziert:

Das Therapiezentrum für Suizidgefährdete des UKE (TZS) entwickelte für Krankenhäuser, Hausärzte und weitere psychotherapeutische / psychiatrische Einrichtungen einen „Monitoring-Bogen Suizidversuche“. Auf diesem sollen Ärzte und andere Therapeuten sensible medizinische und psychosoziale Informationen von solchen Patientinnen und Patienten dokumentieren, die sie nach einem Selbstmordversuch behandelten. Ohne Wissen der Patienten soll dieser Bogen monatlich an das Therapiezentrum im UKE geschickt werden.

Dieses bildet aus dem Geburtsdatum und anderen Daten ein Pseudonym, unter dem dann die weitere Datenverarbeitung erfolgt.

Wir hatten dem TSZ deutlich zu machen, dass der Monitoring-Bogen angesichts verschiedener Daten, insbesondere des vollen Geburtsdatums, als personenbeziehbar anzusehen war und deswegen bereits die Übermittlung von der behandelnden Institution an das TSZ der Einwilligung der Betroffenen bedurfte. Mit dem TSZ diskutierten wir auch die andere Möglichkeit, den Monitoring-Bogen so zu ändern, dass eine Personenbeziehbarkeit für das TSZ ausgeschlossen wurde, aber dennoch nachfolgende Informationen (z. B. nach einem weiteren Selbstmordversuch) der früheren Dokumentation zugeordnet werden können. Letzteres konnten wir durch die Bildung eines Ein-Weg-Schlüssels aus Buchstaben des Namens und einer Quersumme aus dem Geburtsdatum erreichen.

Die zunächst vereinbarte Reduktion des Geburtstages auf das Alter, Ersetzung der Staatsangehörigkeit durch die Alternative „deutsch / nicht deutsch“ und Verkürzung der Wohnort-Postleitzahl auf 4 Stellen reichten jedoch nicht aus, die Personenbeziehbarkeit aufzuheben: Die dringend gewünschte genaue Zeitangabe des Suizidversuchs und die Angabe der behandelnden Stelle ermöglicht es immer noch, die betroffene Person durch eine einfache telefonische Rückfrage (ggf. unter Vorspiegelung eines Arztstatus) zu ermitteln. Gerade vor dem Hintergrund der Unbefristetheit des Projekts und seiner Datenbankfunktion mussten wir dem Projektträger mitteilen, dass aus Datenschutzsicht leider nur die Alternative „informierte Einwilligung oder vollständige Aufhebung der Personenbeziehbarkeit“ verbleibt. Erstere wird häufig nicht zu bekommen sein, letztere würde den Verzicht auf wesentliche Erkenntnismöglichkeiten bedeuten. Möglicherweise ist dieses Projekt einer der ganz seltenen Fälle, in denen Datenschutzanforderungen die Durchführung des Vorhabens überhaupt verhindern.

Schließlich hatten wir uns mit mehreren Forschungsprojekten zu befassen, die überregional bzw. multi-zentrisch angelegt waren oder sind und bei denen wir uns auch mit den Datenschutzbeauftragten oder Aufsichtsbehörden der anderen Länder verständigen mussten. Dazu gehörten Vorhaben wie

- Evaluierung anthroposophischer Medizin eines Berliner Forschungsinstituts,
- „Arbeitsbelastung von Ingenieurstudenten“ der Fachhochschule Ingolstadt, woran sich auch die Hamburger Hochschule für angewandte Wissenschaft beteiligte,
- Epidemiologisches Multiple-Sklerose-Register der MS-Forschungs- und Projektentwicklungs gGmbH, Hannover,
- 3 Kompetenznetzwerke (maligne Lymphome, ambulant erworbene Pneumonie, Sepsis).

Datenschutz im nicht öffentlichen Bereich

18. Internationaler Datenverkehr

18.1 Allgemeines

Auch nach einiger Zeit der Erfahrung mit der Neuregelung des Internationalen Datenverkehrs treten noch weitere Fragen zur Umsetzung auf.

Schon mit Einführung der neuen Vorschriften über den Internationalen Datenverkehr im Bundesdatenschutzgesetz von 2001 wurde deutlich, dass das Gesetz insoweit nicht klar und eindeutig ist (vgl. auch 18.TB, 28). Zusätzlich ist die Europäische Datenschutzrichtlinie zu berücksichtigen und möglichst einheitlich auszulegen. Deshalb ist es notwendiger denn je geworden, die ausgesprochen diffizilen Themen und Probleme seitens aller Datenschutzaufsichtsbehörden aufzugreifen, zu diskutieren und unter Einbeziehung der zuständigen Bundesministerien, der Europäischen Institutionen und der Wirtschaft Lösungen zuzuführen.

Neben der zunehmenden internationalen Verflechtung von Unternehmen, von der auch kleinere Firmen nicht ausgeschlossen sind, hat auch die sich immer weiter verbreitende Nutzung des Internet dazu geführt, dass Übermittlungen personenbezogener Daten ins Ausland zur Normalität geworden sind. Ob es sich darum handelt, dass Personaldaten eines Konzerns weltweitem Zugriff unterliegen oder Werbemaßnahmen durch einen Mailserver in den USA durchgeführt werden sollen, immer sind komplizierte datenschutzrechtliche Überlegungen anzustellen.

Die Datenschutzaufsichtsbehörden sehen sich zunehmendem Beratungsbedarf von Unternehmen gegenüber, die personenbezogene Daten ins Ausland übermitteln möchten oder dies auch schon – in einigen Fällen unter Verletzung der Datenschutzrechte – tun. Die Gründe dafür sind vielfältig. Es geht um Personal-, Kunden- oder Werbedaten, um Übermittlungen ins europäische Ausland, aber auch darüber hinaus, um Daten, die im Ausland selbst benötigt werden oder dort nur für deutsche Auftraggeber verarbeitet werden sollen. Jeder einzelne Fall weist Besonderheiten auf, die vor einer Auskunft an anfragende Unternehmen zunächst recherchiert werden müssen. Einige große Konzerne ziehen solchen Einzelfallberatungen die Lösung über Unternehmensrichtlinien vor, in denen für alle Unternehmen eines Konzerns weltweit gleichermaßen ein – auch den europäischen Maßstäben entsprechender – Datenschutzstandard festgeschrieben wird.

In der AG Internationaler Datenschutz des Düsseldorfer Kreises unter Vorsitz Berlins, in der wir intensiv mitarbeiten, werden die Themen näher erörtert. Neben zahlreichen einzelnen datenschutzrechtlichen Fragen mit internationalem Bezug und der Aufrechterhaltung des Kontakts zur Europäischen Kommission werden insbesondere auch von Konzerunternehmen eingereichte Da-

tenschutz-Unternehmensrichtlinien im Einzelnen behandelt. Im Folgenden werden die Grundzüge des Internationalen Datenverkehrs dargestellt, die von den Unternehmen zu berücksichtigen sind.

18.2 Datenübermittlungen ins Ausland

Verantwortliche Stellen, die personenbezogene Daten ins Ausland übermitteln, müssen sich im Vorfeld folgende Fragen stellen:

- Ist es nach dem Bundesdatenschutzgesetz zulässig, alle dafür vorgesehenen personenbezogenen Daten an Dritte zu übermitteln ?

Die Antwort richtet sich nach den materiellen Vorschriften des Bundesdatenschutzgesetzes (§§ 4, 28, 29 BDSG). Es dürfen keine personenbezogenen Daten ins Ausland übermittelt werden, die nicht auch innerhalb Deutschlands verarbeitet werden dürften. Im Rahmen von Unternehmensanfragen wurde deutlich, dass diese einfache Prüfung vor dem Hintergrund komplizierter erscheinender Voraussetzungen für die Auslandsdatenübermittlung häufig vernachlässigt wurde.

- Handelt es sich bei dem Empfänger um jemanden, der seinen Sitz in einem Mitgliedstaat der EU hat ?

Angesichts des freien Datenverkehrs in der EU müssen unter diesen Umständen neben der materiellen Zulässigkeit keine weiteren Voraussetzungen erfüllt werden. Eine auch in Deutschland zulässige Datenübermittlung unterliegt auch innerhalb des EU-Auslands keinen Beschränkungen.

- Ist der Empfänger eine verantwortliche Stelle in einem Drittland ?

In diesen Fällen gibt es zahlreiche datenschutzrechtliche Fragen, die sehr unterschiedlich zu beantworten sind. z. B.:

- Liegt ein Ausnahmetatbestand vor? In wohl der Mehrzahl der Fälle gibt es die Möglichkeit der Datenübermittlung in ein sog. Drittland auch aus sonstigen Gründen. Beispielsweise kann der Betroffene selbst seine Einwilligung geben; eine Auslandsüberweisung durch den Betroffenen selbst ist ohne Einschränkungen möglich; ein Reisevertrag über eine Reise nach Kenia ist nur durchführbar bei einer zulässigen Übermittlung personenbezogener Daten an das afrikanische Hotel oder die Fluglinie.
- Gibt es in diesem Drittland ein angemessenes Datenschutzniveau? Dann ist keine weitere Zulässigkeitsprüfung erforderlich. Für Ungarn, die Schweiz, Argentinien und unter festgelegten Einschränkungen auch für die USA und Kanada hat die EU-Kommission die Angemessenheit des Datenschutzniveaus bereits festgestellt. In Kürze wird voraussichtlich auch Guernsey dazu gehören.

- Kann die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweisen ? Unter dieser Voraussetzung kann die zuständige Aufsichtsbehörde einzelne Übermittlungen oder bestimmte Arten von Übermittlungen personenbezogener Daten in Drittländer, die von den übrigen Ausnahmen nicht schon erfasst sind, genehmigen.

Daneben gibt es die Möglichkeit, die mit Entscheidung der EU-Kommission vom 15. Juli 2001 verabschiedeten Standardvertragsklauseln oder die mit Entscheidung der EU-Kommission vom 27. Dezember 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländern wortwörtlich zu verwenden. Die Klauseln sind im Internet unter www.europa.eu.int/comm/internal_market/en/dataprot/wpdocs/index.htm abrufbar. Insbesondere für Unternehmen, die ihre Daten durch Auftragsdatenverarbeiter in Drittländern verarbeiten lassen, ist dies ein einfacher Weg, unter Einhaltung der Datenschutzbestimmungen eine Auslagerung der Datenverarbeitung vorzunehmen.

Die Einzelheiten der aufgeführten Fragen wurden nicht nur mit den übrigen Aufsichtsbehörden der Länder eingehend diskutiert, sondern waren insbesondere Gegenstand etlicher Beratungsgespräche mit Unternehmen beim Hamburgischen Datenschutzbeauftragten.

19. Versicherungswirtschaft

19.1 Schweigepflicht-Entbindungserklärung

Die bei Abschluss eines Krankenversicherungsvertrags von dem Versicherungsnehmer abzugebende Schweigepflicht-Entbindungserklärung aus dem Jahr 1989 entspricht nicht den Anforderungen an eine wirksame Einwilligung gemäß § 4 a BDSG. Die von den Datenschutzaufsichtsbehörden geforderte Änderung der Klausel stößt auf großen Widerstand bei der Versicherungswirtschaft.

Wer sich privat gegen Krankheitsrisiken absichern will, muss bei Abschluss des Versicherungsvertrags eine Vielzahl von personenbezogenen Daten, insbesondere Gesundheitsdaten, über sich und seine Familiengehörigen angeben sowie das Versicherungsunternehmen ermächtigen, Auskünfte über seinen Gesundheitszustand von Dritten einzuholen. Nach § 28 Abs. 7 BDSG ist die Datenerhebung durch Krankenversicherer zur Gesundheitsvorsorge und Gesundheitsversorgung im erforderlichen Umfang zulässig.

Davon zu unterscheiden ist die Frage, ob Ärzte, Angehörige anderer Heilberufe und sonstige Stellen, die unter § 203 StGB fallen, eine Befugnis haben, die erfragten Daten an die Unternehmen weiterzugeben. Die strafrechtlich relevante Befugnis zur Offenbarung von Gesundheitsdaten ergibt sich für den genannten Personenkreis in der Regel aus der vom Betroffenen im Krankenversicherungsantrag zu unterzeichnenden Schweigepflicht-Entbindungserklärung. Da

die Weitergabe der Gesundheitsdaten auch in den Anwendungsbereich des BDSG fällt, ist die Datenübermittlung durch die Ärzte, Angehörige anderer Heilberufe und sonstige Stellen, die unter § 203 StGB fallen, nach § 4 Abs. 1 BDSG darüber hinaus nur zulässig, wenn die Erklärung die in § 4 a BDSG geregelten Voraussetzungen an eine wirksame Einwilligung enthält.

Eine Besonderheit im Zusammenhang mit der Erklärung ist, dass sie nicht gegenüber dem Arzt als Träger der Privatgeheimnisse abgegeben wird, sondern der Daten erhebenden Versicherung zur Verfügung gestellt wird. Die Ärzte und andere Auskunftsberechtigte werden in allgemeiner Form über den Text der unterzeichneten Erklärung informiert und können bei Zweifeln eine Kopie der Schweigepflicht-Entbindungserklärung anfordern. Der Text dieser Erklärung ist im Jahr 1989 unter Beteiligung der Datenschutzaufsichtsbehörden neu gefasst worden. Gegen die Verwendung der jetzt 15 Jahre alten Schweigepflicht-Entbindungserklärung bestehen nach Novellierung des BDSG im Jahr 2001 erhebliche datenschutzrechtliche Bedenken. Sie genügt nicht mehr den datenschutzrechtlichen Anforderungen des § 4 a BDSG an eine wirksame Einwilligungserklärung.

Nach § 4 a Abs. 1 und Abs. 3 BDSG muss aus einer Einwilligungserklärung für die Betroffenen klar erkennbar sein, welche Gesundheitsdaten von wem zu welchem Zweck erhoben, verarbeitet oder genutzt werden sollen. Die Einwilligung muss aus datenschutzrechtlicher Sicht auf die im Einzelfall erforderlichen Gesundheitsdaten beschränkt sein. Die Betroffenen müssen über die Reichweite der Erklärung informiert werden. Die pauschalen Zustimmungen, die der Text der Schweigepflicht-Entbindungserklärung aus dem Jahr 1989 vorsieht, erfüllen diese Voraussetzungen nicht.

Die Obersten Aufsichtsbehörden haben in der Arbeitsgruppe Versicherungswirtschaft, in der Hamburg den Vorsitz hat, die Gründe für eine Überarbeitung der Klausel mit den Vertretern der Versicherungswirtschaft erörtert. Eine Übereinstimmung mit der Versicherungswirtschaft über die Neufassung der Klausel konnte noch nicht erzielt werden. Die Versicherungswirtschaft ist bisher zu einer umfassenden Änderung der Klausel nicht bereit. Sie hat darauf verwiesen, dass die Klausel von der Rechtsprechung als zulässig beurteilt worden sein soll. Eine Überarbeitung ist aus Sicht der Versicherungswirtschaft nur sinnvoll, wenn mehr Transparenz für die Versicherungsnehmer erreicht werden kann. Die Verhandlungen mit der Versicherungswirtschaft sind sehr schwierig. Stellungnahmen von Seiten der Versicherungswirtschaft erfolgen in der Regel nur nach mehrmaligen Aufforderungen, so dass der Eindruck entsteht, die Versicherungswirtschaft möchte die Überarbeitung hinauszögern.

Der derzeitige Verhandlungsstand zu den einzelnen Absätzen des Mustertextes einer Schweigepflicht-Entbindungserklärung wird im Folgenden mit den Positionen der Obersten Aufsichtsbehörden und der Versicherungswirtschaft dargestellt:

1. Schweigepflicht-Entbindung zur Risikobeurteilung bei Vertragsschluss (Abs.1)

> Mir ist bekannt, dass der Versicherer – soweit hierzu ein Anlass besteht – Angaben über meinen Gesundheitszustand und bei anderen Krankenversicherern auch Angaben über frühere, bestehende oder beantragte Versicherungsverträge zur Beurteilung der Risiken eines von mir beantragten Vertragsabschlusses überprüft. Zu diesem Zweck befreie ich Ärzte, Zahnärzte, Angehörige anderer Heilberufe sowie Angehörige von Krankenanstalten und Gesundheitsämtern, die mich in den letzten zehn Jahren untersucht, beraten oder behandelt haben, von ihrer Schweigepflicht – und zwar auch über meinen Tod hinaus – und ermächtige sie, dem Versicherer die erforderlichen Auskünfte zu erteilen. Dies gilt auch für Angehöriger anderer Kranken-, Lebens- und Unfallversicherer, mit denen ich bisher in Vertragsbeziehungen stand oder stehe. Diese Ermächtigung endet fünf Jahre nach Antragstellung.

Absatz 1 der Schweigepflicht-Entbindungserklärung ist nach Auffassung der Obersten Aufsichtsbehörden als Einwilligung nach § 4 a BDSG datenschutzrechtlich zu unbestimmt und widerspricht dem Erforderlichkeitsgrundsatz. Die Betroffenen werden über die Reichweite der abzugebenden Erklärung im Unklaren gelassen, da aus der Klausel nicht eindeutig ersichtlich ist, bei welchem Anlass die Befugnis bestehen soll, von der Erklärung Gebrauch zu machen. Zweifel bestehen auch an der Notwendigkeit einer Datenerhebungsbefugnis, die sich auf einen Datenverarbeitungszeitraum von 10 Jahren bezieht und für 5 Jahre bestehen soll.

Die Vertreter der Versicherungswirtschaft sind der Auffassung, dass die Schweigepflicht-Entbindungserklärung nicht nach § 4 a BDSG zu beurteilen ist. Sie verweisen auf § 16 VVG als bereichsspezifische Vorschrift, nach der die Erhebung von Gesundheitsdaten im erforderlichen Umfang zulässig sein soll. Zweck der Erklärung und der darin enthaltenen Fristen ist nach ihren Angaben eine sichere Risikobeurteilung. Es gehe dabei nicht um neue Krankheiten, die nach Vertragsschluss entstanden sind, sondern um alte, verschwiegene Krankheiten. Innerhalb der Fristen soll die Möglichkeit einer Überprüfung bestehen, ob der Versicherungsnehmer seiner vorvertraglichen Anzeigepflicht nachgekommen ist. Die Frist von 5 Jahren ergäbe sich aus Erfahrungswerten bei kostenintensiven Behandlungen. Ein Auftreten bestimmter Erkrankungen nach einer Frist von 5 Jahren könne darauf hindeuten, dass die Erkrankungen bereits bei Antragstellung vorlagen und verschwiegen wurden.

Die Obersten Aufsichtsbehörden und die Vertreter der Versicherungswirtschaft haben eine vorläufige Einigung über einen neuen Text von Absatz 1 der Klausel erzielt. Dabei ist die Klausel durch Formulierungsänderungen konkretisiert

und damit für die Betroffenen transparenter geworden. Die Versicherungswirtschaft wird noch abschließend zu dem Text Stellung nehmen.

2. Schweigepflicht-Entbindung bei Leistungsanträgen (Abs.2)

> Mir ist ferner bekannt, dass der Versicherer zur Beurteilung seiner Leistungspflicht auch Angaben überprüft, die ich zur Begründung etwaiger Ansprüche mache oder die sich aus von mir eingereichten Unterlagen (z. B. Rechnungen, Verordnungen) sowie von mir veranlassten Mitteilungen eines Krankenhauses oder von Angehörigen eines Heilberufes ergeben. Auch zu diesem Zweck befreie ich die Angehörigen von Heilberufen oder Krankenanstalten, die in den vorgelegten Unterlagen genannt sind oder die an der Heilbehandlung beteiligt waren, von ihrer Schweigepflicht; dabei hat die Geltendmachung eines Leistungsanspruches die Bedeutung einer Schweigepflichtentbindung für den Einzelfall. Von der Schweigepflicht entbinde ich auch zur Prüfung von Leistungsansprüchen im Falle meines Todes. Diese Schweigepflichtentbindung für die Leistungsprüfung bezieht sich auch auf die Angehörigen von anderen Kranken- und Unfallversicherern, die nach dort bestehenden Versicherungen befragt werden dürfen.

Nach Auffassung der Obersten Aufsichtsbehörden erfordert die Rechtslage gemäß § 4 a BDSG für Gesundheitsdaten die Einholung einer Schweigepflicht-Entbindungserklärung bei der Leistungsprüfung, die sich auf den konkreten Einzelfall bezieht. Absatz 2 der Klausel in der vorliegenden Fassung enthält eine pauschale auf die Zukunft gerichtete Entbindung von der Schweigepflicht. Bei Abgabe der Erklärung ist den Betroffenen weder der Name des Arztes noch der Anlass für künftige ärztliche Behandlungen usw. bekannt. Die Erklärung kann sich daher nicht auf konkrete Gesundheitsdaten beziehen, was nach § 4 a Abs. 3 BDSG für eine wirksame Einwilligung erforderlich wäre. Die auf die Zukunft gerichtete Erklärung hat zudem den Nachteil, dass Versicherungsnehmer sich bei langfristigen Versicherungsverträgen zum Zeitpunkt der Verwendung nicht mehr an die Schweigpflicht-Entbindungserklärung bei Vertragsschluss erinnern können, wie Eingaben bei den Aufsichtsbehörden zeigen.

Die Obersten Datenschutzaufsichtsbehörden erwägen, die Ärztekammern darauf hinzuweisen, dass wegen der datenschutzrechtlich unzulässigen Klausel keine Gesundheitsdaten an die Versicherer weitergegeben werden dürfen. Bisher ist im Hinblick auf die laufenden Verhandlungen mit der Versicherungswirtschaft davon abgesehen worden.

Den datenschutzrechtlichen Bedenken gegen Absatz 2 der Erklärung hält die Versicherungswirtschaft entgegen, dass die Erklärung im Interesse der Versi-

cherungsnehmer liege. Da es im Zusammenhang mit der Erstattung von Leistungsansprüchen häufig zu Rückfragen käme, z. B. weil die Diagnose nicht mit den Einzelbeträgen in der Rechnung übereinstimme, sei die Einholung von Schweigepflicht-Entbindungserklärungen in Einzelfällen zeitaufwendig und führe für die Versicherungsnehmer zu Verzögerungen bei der Leistungserstattung. Für ca. 30.000 Leistungsanträge pro Jahr sei bei dem jeweiligen Versicherer eine Überprüfung der Angaben erforderlich. Die Forderung der Aufsichtsbehörden würde zur Einführung eines kostenintensiven Antragsverfahrens führen. Krankenversicherer, die derzeit bewusst auf Formulare für die Erstattungsanträge verzichten, müssten dann Leistungsanträge einführen. Die damit verbundenen höheren Kosten würden von den Verbraucherschutzorganisationen sehr kritisch gesehen. Die Versicherungswirtschaft gab auch zu bedenken, dass die Schweigepflicht-Entbindungserklärung bei Erstattungsanträgen eine andere Qualität habe als im Zusammenhang mit dem Vertragsschluss. Durch Einreichung der Rechnungen bei den Versicherern würden die Versicherungsnehmer bereits selbst den größten Teil ihrer Gesundheitsdaten mitteilen.

Als Kompromisslösung wurde in der Arbeitsgruppe Versicherungswirtschaft zunächst eine regelmäßige jährliche Information der Versicherungsnehmer über eine bei Vertragsschluss abgegebene Schweigepflicht-Entbindungserklärung für Leistungsanträge und das insoweit bestehende Widerrufsrecht durch die Versicherer vorgesehen. Dieser Kompromissvorschlag wurde jedoch vom Düsseldorfer Kreis als Formalismus angesehen, der nicht geeignet sei, Mängel einer früher erteilten pauschalen Einwilligungserklärung zu beseitigen. Im Düsseldorfer Kreis bestand Einigkeit, dass zur Überprüfung der Leistungspflicht der Versicherungen ärztliche Unterlagen nur auf Grund einer im jeweiligen Einzelfall abgegebenen Schweigepflicht-Entbindungserklärung des Versicherungsnehmers angefordert werden können. Die Verhandlungen sollen zunächst in der Arbeitsgruppe Versicherungswirtschaft fortgesetzt werden.

3. Schweigepflicht-Entbindungserklärung für mitzuversichernde Personen (Abs. 3)

> Diese Erklärung gebe ich auch für meine mitzuversichernden Kinder sowie die von mir gesetzlich vertretenen mitzuversichernden Personen ab, die die Bedeutung dieser Erklärung nicht selbst beurteilen können.

Hinsichtlich Absatz 3 der Schweigepflicht-Entbindungserklärung hatten die Obersten Aufsichtsbehörden eine Streichung angeregt. Die Erklärung, wonach die Einwilligung auch für die mitzuversichernden Kinder sowie gesetzlich vertretene mitzuversichernde Personen abgegeben werde, die die Bedeutung dieser Erklärung nicht selbst beurteilen können, stellt keine Einwilligung gemäß § 4 a BDSG dar, sondern lediglich eine Erläuterung. Es wäre daher aus-

reichend, an anderer geeigneter Stelle, z. B. im Merkblatt, darauf hinzuweisen, dass minderjährige Kinder, die die Bedeutung der Erklärung selbst beurteilen können, die Erklärung auch selbst unterzeichnen müssen. Die Erörterungen zu diesem Punkt werden fortgesetzt werden.

Klärungsbedürftig ist auch noch die Frage des äußeren Erscheinungsbildes der Schweigepflicht-Entbindungserklärung. Dabei wird es vor allem um die Frage gehen, in welcher Form die besondere Hervorhebung der Klausel nach § 4 a Abs. 1 Satz 4 BDSG zu erfolgen hat. Schweigepflicht-Entbindungserklärungen sind häufig Bestandteil der Allgemeinen Geschäftsbedingungen. In diesen Fällen werden die Versicherungsnehmer in den Antragsformularen vor Abgabe ihrer Unterschrift auf die Erklärungen hingewiesen.

Ob und inwieweit auch die in anderen Versicherungszweigen (u.a. Lebens-, Unfall-, Berufsunfähigkeitsversicherung) genutzten Schweigepflicht-Entbindungserklärungen datenschutzrechtlich zulässig sind, bleibt einer gesonderten Überprüfung vorbehalten.

19.2 Warn- und Hinweissysteme

In den Warn- und Hinweissystemen der verschiedenen Versicherungssparten werden Daten zwischen einzelnen Versicherungsunternehmen ausgetauscht und nicht in Form einer zentralen Datei beim Gesamtverband geführt.

Über den Austausch personenbezogener Daten im Rahmen der zentralen Warn- und Hinweissysteme der Versicherungswirtschaft wurde in vergangenen Tätigkeitsberichten schon häufig berichtet (zuletzt 9.TB 5.3.1, 10. TB 25.1-25.5, 11. TB 25.1-25.2, 12. TB 24.1 -24.2). Im Berichtszeitraum war das System wieder Gegenstand von Gesprächen mit der Versicherungswirtschaft. Anlass für die erneute Erörterung waren Eingaben und Fragen, die zeigen, dass bei vielen Versicherungsnehmern Unklarheiten über den Ablauf des Verfahrens bestehen. Dabei überwiegt der Irrtum, dass der Gesamtverband der Versicherungswirtschaft (GDV) eine zentrale Warndatei unterhält, aus der die einzelnen Versicherungen Daten abrufen können. Dies ist nicht zutreffend. Zur Erläuterung des bereits in den früheren Tätigkeitsberichten wiedergegebenen Verfahrens wird dieses noch einmal im Zusammenhang dargestellt:

Bei der Prüfung der Angaben zu einem Versicherungsantrag oder im Falle eines Schadens kann es zur Risikobeurteilung, zur weiteren Aufklärung des Sachverhalts oder zur Verhinderung von Versicherungsmissbrauch notwendig sein, bei anderen Versicherungen Auskünfte einzuholen oder Daten an andere Versicherer weiter zu geben. Zu diesem Zweck lassen sich die Versicherungsunternehmen bereits im Versicherungsantrag eine Einwilligung unterzeichnen, die den Austausch von Informationen ermöglicht. Die Versicherungen haben zur gegenseitigen Datenübermittlung ein System entwickelt, bei dem Informationen über Versicherungsnehmer ausgetauscht werden, ohne dass perso-

nenbezogene Daten an zentraler Stelle gespeichert werden (zu den Einzelheiten vgl. 9. TB, 5.3.1).

Das Verfahren läuft wie folgt ab: Liegen hinsichtlich einer Person bestimmte Voraussetzungen oder Auffälligkeiten vor, so meldet das Versicherungsunternehmen den Namen und die Adresse sowie das Aktenzeichen an den Gesamtverband der Versicherungswirtschaft. Die Voraussetzungen für die Meldung sind in den verschiedenen Versicherungssparten unterschiedlich festgelegt und in dem mit der Einwilligungserklärung zum Versicherungsvertrag ausgehändigten Merkblatt nachlesbar.

Der Verband codiert Namen und Adressangaben der betroffenen Personen mittels eines speziellen Verfahrens. Die codierten Daten sind durch den Verband nicht rückübersetzbar. Sie werden in Listenform per Datenfernübertragung oder über CD ROM an die einzelnen Versicherungsunternehmen übersandt. Eine Aktualisierung der Listen erfolgt in Abständen zwischen zwei und vier Wochen. Im Rahmen der Antrags- bzw. Schadenbearbeitung durch ein Versicherungsunternehmen kommt es zu einem Abgleich mit den gelieferten codierten Daten zur Risikoanalyse, zur Aufklärung des Sachverhalts bzw. zur Verhinderung von Versicherungsmissbrauch. Das abgleichende Versicherungsunternehmen codiert ebenfalls Namen und Adressangaben der zu überprüfenden Person und kann so feststellen, ob bereits eine Meldung in dem Hinweissystem erfolgt ist. Da es nicht immer sicher ist, dass die zu überprüfende Person mit derjenigen übereinstimmt, die bei dem Abgleich angezeigt wird, muss persönlich Kontakt mit dem meldenden Versicherungsunternehmen aufgenommen werden.

Eine automatische Löschung der codierten Daten in den Hinweissystemen erfolgt nach 5 Jahren. Im Hinweissystem der Berufsunfähigkeitsversicherer werden die Daten erst nach 10 Jahren gelöscht. Die Obersten Aufsichtsbehörden haben unter Hinweis auf § 35 Abs. 2 Satz 2 Nr. 4 BDSG grundsätzlich eine Löschung der codierten Daten nach 4 Jahren gefordert. Die Vertreter der Versicherungswirtschaft halten an der Löschungsfrist von 5 Jahren fest.

19.3 Einstellung von Versichertendaten von Holocaust-Opfern ins Internet

Für die Entschädigung von Holocaust-Opfern konnte ein datenschutzgerechtes Verfahren gefunden werden, eine Liste mit deren Versichertendaten ins Internet einzustellen.

Holocaust-Opfer und ihre Nachkommen haben die Möglichkeit, bei der ICHEIC (International Commission on Holocaust Era Insurance Claims) einen Antrag auf Entschädigung für nicht ausgezahlte Versicherungen aus europäischen Versicherungsverträgen zu stellen, die zwischen dem 1. Januar 1920 und dem 9. Mai 1945 abgeschlossen wurden.

Im 18. TB (22.2) hatten wir darüber berichtet, dass der betroffene Personenkreis auf der Grundlage sogenannter Holocaust-Versicherungsgesetze ab 1999 ermittelt wurde. Dazu wurden mehrere europäische Versicherungsgesellschaften von amerikanischen Behörden gegen Androhung des Lizenzentzuges aufgefordert, Listen sämtlicher Vorkriegspolicen der unterschiedlichen Versicherungssparten im Internet zu veröffentlichen. Gegen entsprechende Bescheide hatten deutsche Versicherungsunternehmen geklagt, da eine derartige Offenbarung datenschutzrechtlich problematisch und mit erheblichen Kosten verbunden ist.

Die Obersten Datenschutzaufsichtsbehörden hielten eine Veröffentlichung der Daten im Internet nach den Vorschriften des BDSG für unzulässig, da die Aufforderung in großem Umfang auch Versicherungsnehmer betraf, die nicht zum Kreis der Holocaust-Opfer gehörten. Ihre Kritik führte zu einer datenschutzgerechten Ausgestaltung des Verfahrens zur Erstellung einer Liste von deutschen Versicherungsnehmern, die Holocaust-Opfer waren.

Durch eine Vereinbarung aus dem Jahr 2002 zwischen der ICHEIC, der Bundesstiftung „Erinnerung, Verantwortung und Zukunft“ und dem Gesamtverband der Versicherungswirtschaft (GDV) wurden die Modalitäten eines Verfahrens zur Bearbeitung nicht ausgezahlter Versicherungspolicen, die an Opfer des NS-Regimes ausgestellt wurden, festgelegt und dabei die datenschutzrechtliche Kritik berücksichtigt. Um Berechtigte auf die Möglichkeit eines Entschädigungsanspruchs aufmerksam zu machen, wurde eine Liste von jüdischen Policeninhabern aus der relevanten Zeit zusammengestellt.

Das Verfahren zur Erarbeitung dieser Liste fand – wie von den Obersten Datenschutzaufsichtsbehörden gefordert – in Deutschland statt, so dass eine Übermittlung ins Ausland unterblieb. Dazu wurden zunächst vom Bundesaufsichtsamt für Finanzdienstleistungen (BAFin) bei deutschen Versicherungsunternehmen die Daten von Inhabern von Lebensversicherungspolicen erhoben, die ihre Police zwischen dem 1. Januar 1920 und dem 9. Mai 1945 abgeschlossen haben. Aus diesen Daten erstellte der Gesamtverband der Versicherungswirtschaft als Auftragnehmer nach § 11 BDSG eine Liste. Diese Liste wurde durch das BAFin mit einer von Bundesarchiv erstellten Liste der jüdischen Einwohner in Deutschland aus der Zeit von 1933 bis 1945 und einer von Yad Vashem zur Verfügung gestellten Liste der Holocaust-Opfer abgeglichen. Die entstandene Gesamtliste wurde auf der Website der ICHEIC (www.icheic.org) veröffentlicht. Sie soll Nachkommen von Holocaust-Opfern die Prüfung ermöglichen, ob ihnen eine Entschädigung zustehen könnte. In der Veröffentlichung wird darauf hingewiesen, dass ein Anspruch auf Löschung von personenbezogenen Daten für die Betroffenen besteht, die nicht wünschen, dass ihre Namen veröffentlicht werden. Durch diesen Hinweis wird das von den Obersten Datenschutzaufsichtsbehörden geforderte Widerspruchsrecht der Betroffenen umgesetzt.

19.4 GDV Unternehmensrichtlinie

Die Erörterung der Unternehmensrichtlinie des Gesamtverbandes der Versicherungswirtschaft (GDV) ist abgeschlossen.

Der Mustertext des GDV zu einer Unternehmensrichtlinie für die Datenweitergabe innerhalb international tätiger Versicherungsunternehmen wurde mit den Obersten Datenschutzaufsichtsbehörde eingehend erörtert. Gemäß den Ergebnissen in der Arbeitsgruppe Internationaler Datenverkehr hat der GDV den Text umfassend überarbeitet. Die datenschutzrechtlichen Anforderungen wurden dabei berücksichtigt. Der Düsseldorfer Kreis hat im November 2002 beschlossen, dass der Mustertext zu einer Unternehmensrichtlinie als Grundlage für eine Genehmigung nach § 4 c BDSG bzw. als Grundlage für ein angemessenes Datenschutzniveau nach § 4 b BDSG geeignet sein kann.

19.5 Rennlisten

Rennlisten sollen in der Versicherungswirtschaft nur nach vorheriger Einwilligung der Betroffenen oder ohne personenbezogene Daten genutzt werden.

Im Berichtszeitraum haben die Obersten Aufsichtsbehörden mit der Versicherungswirtschaft die Erörterung über die Zulässigkeit von sog. Rennlisten fortgeführt (vgl. 18.TB, 22.5). Dabei handelt es sich um vergleichende Übersichten von Handelsvertretern einer Geschäftsstelle oder Region. Aus den Übersichten gehen die vermittelten Versicherungsgeschäfte für einen bestimmten Zeitraum hervor, so dass zumindest teilweise das aus den vermittelten Geschäften erzielte Einkommen abgeleitet werden kann. Die Rennlisten werden von der Versicherungswirtschaft für notwendig gehalten, um den Mitarbeitern im Außendienst Leistungsvergleiche zu ermöglichen und ihnen Leistungsanreize zu geben und Leistungsziele aufzuzeigen. Die Zulässigkeit der personenbezogenen Leistungsübersichten ergibt sich nach Auffassung der Versicherungswirtschaft aus dem Bestehen des Vertretervertragsverhältnisses.

Die Obersten Datenschutzaufsichtsbehörden teilen diese rechtliche Einschätzung nicht. Sie halten das Verfahren ohne eine Einwilligung der Betroffenen nach § 4 a BDSG für datenschutzrechtlich bedenklich und forderten eine Änderung der bisherigen Praxis. Die Handelsvertreter müssten bei Vertragsschluss zumindest auf die in dem jeweiligen Versicherungsunternehmen bestehende Praxis und die Möglichkeit, jederzeit der Aufnahme in die Leistungsübersichten widersprechen zu können, hingewiesen werden. Im Ergebnis geben die Obersten Aufsichtsbehörden einer Leistungsübersicht den Vorzug, aus der sich in einer Rangfolge zahlenmäßig die Umsätze der Versicherungsvermittler ergeben, ohne jedoch deren Identität preiszugeben. Den Betroffenen könnte dann mitgeteilt werden, an welcher Stelle sie in der Leistungsübersicht stehen.

Die Versicherungswirtschaft hat sich grundsätzlich bereit erklärt, künftig entweder eine Einwilligung der Betroffenen für die Aufnahme in die Rennliste einzuholen oder die Listen nur mit Pseudonym zu führen. Der Gesamtverband der Versicherungswirtschaft (GDV) hat sich nun für eine Einwilligungsklausel in neuen Agenturverträgen ausgesprochen und die Mitgliedsunternehmen entsprechend unterrichtet. Bei bestehenden Verträgen werden die Mitarbeiter, die noch keine Einwilligungsklausel unterzeichnet haben, auf ihr Widerspruchsrecht hingewiesen.

19.6 Direktversicherung

Beim Abschluss von Direktversicherungen muss sichergestellt werden, dass der Arbeitgeber über das Antragsformular keine Kenntnis der Gesundheitsdaten des Arbeitnehmers erhält.

Im Zusammenhang mit dem Abschluss von Direktversicherungen zur betrieblichen Altersvorsorge haben wir uns mit der Frage beschäftigt, ob und welche Daten der Arbeitgeber dadurch über den Gesundheitszustand der Mitarbeiter erfährt. In der Regel ist der von dem Mitarbeiter auszufüllende Formularteil mit seinen Angaben zur Gesundheit Bestandteil des Antragsformulars. Dieses Antragsformular wird in einigen Fällen über den Arbeitgeber an das Versicherungsunternehmen weitergegeben, so dass der Arbeitgeber Kenntnis von den Gesundheitsdaten erlangen kann.

Nach Aufforderung durch die Obersten Datenschutzaufsichtbehörden hat die Versicherungswirtschaft zugesagt, die Angaben zur Gesundheit der Mitarbeiter auf einem getrennten Formularteil festzuhalten, der dann in einem verschlossenen Umschlag über den Versicherungsvermittler oder den Arbeitgeber an die Versicherung weitergegeben werden kann. Bisher noch ohne Ergebnis wurde die Frage erörtert, ob durch die Übersendung der Versicherungspolice an den Arbeitgeber Rückschlüsse, etwa durch einen Risikoaufschlag oder Leistungsausschlüsse, auf den Gesundheitszustand eines Mitarbeiters möglich sind und darin eine unzulässige Übermittlung von Gesundheitsdaten liegt.

Über den Fortgang der Angelegenheit werden wir berichten.

20. Schufa

20.1 Schufa jetzt in Wiesbaden

Die Schufa hat ihren Sitz jetzt in Wiesbaden. Dennoch werden in Hamburg weiter Beschwerden von betroffenen Bürgern bearbeitet.

Bisher bestand auch in Hamburg eine regionale Schufa-Gesellschaft als rechtlich selbständige GmbH. Zum 1. Januar 2002 wurden die verschiedenen regionalen Schufa-Gesellschaften zu einem einheitlichen Unternehmen mit Sitz

in Wiesbaden unter dem Namen der SCHUFA Holding AG zusammen geschlossen.

Angesichts der bundesweit sehr hohen Anzahl von Eingaben, die die Schufa betreffen, erscheint es aber nicht sinnvoll, jetzt das Regierungspräsidium Darmstadt allein mit der Beschwerdebearbeitung zu befassen. Dies gilt besonders deshalb, weil Fehler z. B. bei der Meldung personenbezogener Daten häufig auch durch Falschmeldungen seitens der Anschlusspartner der Schufa, die überall ihren Sitz haben können, auftreten. Zahlreich sind auch die Fälle, in denen den Betroffenen eine Information über die rechtlichen Grundlagen oder eine schnelle Klärung bei der örtlichen Zweigstelle zur Erledigung ihrer Anliegen ausreicht.

Daher wurde zwischen den Aufsichtsbehörden aller Bundesländer vereinbart, dass vor Abgabe der Beschwerden an das Regierungspräsidium Darmstadt jeweils vor Ort versucht werden soll, eine Aufklärung zu erreichen. Lediglich im Falle von Auffassungsunterschieden mit der Schufa oder bei Grundsatzangelegenheiten wird an die zuständige Aufsichtsbehörde in Darmstadt abgegeben. Darüber hinaus werden die die Schufa betreffenden Probleme auch weiterhin länderübergreifend in der Arbeitsgruppe Schufa des Düsseldorfer Kreises geklärt, in der auch Gespräche mit Vertretern der Schufa geführt werden. Wir beteiligen uns an der Arbeitsgruppe und den Gesprächen mit der Schufa.

20.2 Schufa-Score-Verfahren

Hinsichtlich der Ausgestaltung des Schufa-Score-Verfahrens konnten datenschutzrechtliche Fortschritte erzielt werden.

Nach wie vor gibt es zwischen den Obersten Aufsichtsbehörden der Länder und der Schufa kontroverse Gespräche über die Einzelheiten des Schufa-Score-Verfahrens (vgl. hierzu 16. TB, 20.1). Durch dieses Verfahren wird anhand statistisch-mathematischer Methoden aus Erfahrungen mit dem Zahlungsverhalten von Personengruppen in der Vergangenheit eine Prognose im Einzelfall ermittelt. Einige Fragen, wie z. B. die Informationen des Betroffenen über konkrete Score-Werte konnten in der jüngeren Vergangenheit bereits geklärt werden (vgl. z. B. 18. TB, 23.2).

Dieser tagesaktuelle Score-Wert entspricht in der Regel jedoch nicht demjenigen, den die Schufa zu einem anderen Zeitpunkt an ein anfragendes Unternehmen übermittelt hat. Genau an dieser Information hat der Betroffene aber häufig ein Interesse. Offen bleibt daher nach wie vor, wie Betroffene konkret den an ein Unternehmen durch die Schufa übermittelten Wert erfahren können. Fortschritte in dieser Frage zeichnen sich jetzt dahin gehend ab, dass die Schufa, die den an ein Unternehmen übermittelten Score-Wert bisher nicht selbst speichert, zugesichert hat, dies mit der in Kürze in Betrieb gehenden neuen Software-Generation zu gewährleisten. Damit verbunden wäre dann ein

Rechtsanspruch des Betroffenen auf Beauskunftung dieses Wertes durch die Schufa. Es bleibt abzuwarten, in welchem Zeitraum und mit welchen Inhalten diese Zusage umgesetzt wird.

Die Schufa hat auch mitgeteilt, dass eine Scorewert-Ermittlung für Kunden dann nicht vorgenommen wird, wenn der Betroffene – aus welchen Gründen auch immer – Widerspruch gegen die Übermittlung eines solchen Wertes eingelegt hat. Obwohl eine solche Widerspruchsmöglichkeit von den Datenschutzaufsichtsbehörden grundsätzlich positiv bewertet wird, ist in diesem Zusammenhang zu beachten, dass auch negative Auswirkungen entstehen können:

Der Scorewert wird ausschließlich dann ermittelt, wenn keine negativen Daten über den Betroffenen gespeichert sind (vgl. 16. TB, 20.1). In der Vergangenheit wurde dem Unternehmen, das diesen Wert von der Schufa anfordert, mitgeteilt, dass keine Scorewert-Ermittlung erfolgt, weil der Betroffene Widerspruch eingelegt hat. Der Eindruck, den das anfordernde Unternehmen dadurch von dem jeweils Betroffenen hat, war in solchen Fällen nicht absehbar und unter Umständen sogar nachteilig. Die Gespräche mit der Schufa über diese Frage haben zu der Zusage der Schufa geführt, künftig auf die Übermittlung des Filtertextes „Betroffener widerspricht Scoreermittlung“ an die Vertragspartner zu verzichten.

20.3 Schufa-Auskünfte an die Wohnungswirtschaft

Noch immer konnte kein datenschutzfreundlicher Weg für Schufa-Auskünfte an die Wohnungswirtschaft gefunden werden.

Das Thema Schufa-Auskünfte an die Wohnungswirtschaft wurde auch in diesem Berichtszeitraum wieder intensiv mit der Schufa erörtert (zuletzt 18. TB, 23.3). Auch wenn die Zuständigkeit für die Schufa jetzt in Hessen konzentriert ist (s.o. 20.1), sind die übrigen Obersten Aufsichtsbehörden mit den entsprechenden datenschutzrechtlichen Fragen intensiv befasst. Dies liegt im Bereich der Schufa-Auskünfte an die Wohnungswirtschaft daran, dass Anschlusspartner der Schufa Vermieter in allen Bundesländern sind bzw. werden sollen. Daher stellt sich auch in allen Bundesländern die Frage nach der Rechtmäßigkeit von Datenerhebungen und Datenübermittlungen.

Unserer Auffassung nach beabsichtigt die Schufa das Verfahren, das Grundlage des Hamburger Pilotverfahrens gewesen ist (vgl. 17. TB, 20.4), weit über die zu diesem Test festgelegten Rahmenbedingungen hinaus auszudehnen. Zu diesem Zweck wurde den Obersten Aufsichtsbehörden im Mai 2002 von der Schufa eine erneut überarbeitete Fassung der vorgesehenen Einwilligungsklausel zu Mietanträgen vorgelegt. Die Einwilligungsklausel verfolgt aber nicht mehr wie im Pilotverfahren (vgl. zuletzt 18. TB, 23.3) das Ziel, die frühere, ausführlichere Selbstauskunft des Mieters durch ein transparentes, in sich ge-

schlossenes Verfahren der Auskunft an einen Vermieter zu ersetzen. Die Schufa selbst hat mitgeteilt, sie habe zu keinem Zeitpunkt beabsichtigt, mit der Anpassung über die zu dem Test festgelegten Rahmenbedingungen hinaus zu gehen. Vielmehr bleibe das ursprüngliche Ziel, die sehr viel ausführlichere Selbstauskunft durch die B-Auskunft zu ersetzen.

In dem B-Auskunftsverfahren erhalten die Anfragenden nicht nur die für sie interessanten Negativdaten des jeweils Betroffenen. Sie sind vielmehr auch selbst verpflichtet, Leistungsstörungen im Verhältnis zu ihrem Vertragspartner an die Schufa zu melden. Verbunden damit ist die Absicht, die Daten, die Vermieter über ihre Mieter melden, in die übrige Auskunftspraxis der Schufa einfließen zu lassen. Sogar Mietrückstände sollen von den Vermietern unter bestimmten Umständen an die Schufa gemeldet werden, die damit in die Lage versetzt wird, diese Schulden auch an andere Anfrager wie Banken oder Telekommunikationsunternehmen weiter zu geben.

Zunächst war sogar vorgesehen (vgl. auch 18. TB, 23.3), den Vermietern Auskünfte über die zu dem Mieter gespeicherte Summe der monatlichen Belastungen zu erteilen. Derartige Daten könnten, abgesehen davon, dass eine Übermittlung nicht erforderlich ist, nur in den seltensten Fällen genau sein. Die Schufa hat nämlich so gut wie nie eine vollständige Aufstellung der monatlichen Belastung Betroffener. Auf Betreiben der Obersten Aufsichtsbehörden für den Datenschutz hat die Schufa jedoch zwischenzeitlich erklärt, dieses Merkmal zumindest derzeit nicht in das Verfahren aufzunehmen. Es bleibt abzuwarten, ob zu diesem speziellen Punkt zu anderer Zeit erneut die Diskussion aufgenommen werden muss.

Obwohl mehrere Erörterungen der Obersten Aufsichtsbehörden für den Datenschutz mit Vertretern der Schufa stattfanden, konnte nicht mit letzter Eindeutigkeit festgestellt werden, welche Zielsetzung die Schufa mit der verbliebenen Einwilligungsklausel verfolgt. Entweder ist diese Klausel viel zu weit gehend oder aber – nimmt man die Aussagen der Schufa, dass viele danach mögliche Übermittlungen nicht stattfinden sollen – in weiten Teilen überflüssig. Beide Möglichkeiten bieten jedoch nicht die gebotene Transparenz und Konkretisierung. Die Obersten Aufsichtbehörden haben nun Alternativen aufgezeigt, nach denen dem Anliegen der Vermieter sogar ohne Einwilligung weitgehend entsprochen werden kann. Bisher hat die Schufa dazu nicht Stellung genommen.

20.4 Weitere Anschlusspartner der Schufa

Mit der Eröffnung immer neuer Geschäftsfelder entwickelt sich die Schufa weg von ihrer Tradition als reines Bonitätsinformationssystem für die Kreditwirtschaft.

Das Thema Schufa-Auskünfte an die Wohnungswirtschaft zeigt bereits, dass die Schufa sich neben den traditionellen Anschlusspartnern aus der Kredit-

wirtschaft zunehmend solche aus anderen Branchen sucht. Nach den Einzelhandelsunternehmen einschließlich des Versandhandels, den Telekommunikationsanbietern und den Vermietern will die Schufa jetzt auch für Versicherungs- und Inkassounternehmen als Auskunftei tätig werden.

Eine eingehende Befassung mit der Problematik durch die Obersten Aufsichtsbehörden für den Datenschutz hat bisher noch nicht stattgefunden. Dies liegt insbesondere daran, dass die Frage, ob die Übermittlung nach den datenschutzrechtlichen Vorschriften oder durch eine Einwilligung des Betroffenen gerechtfertigt sein kann, nach den konkreten Umständen zu beurteilen ist. Die bisher vorgetragenen Fälle haben allerdings erhebliche Zweifel daran aufkommen lassen, dass sich alle Vorstellungen der Schufa in datenschutzgerechter Weise lösen lassen. Die Angelegenheit wird weiter mit der Schufa erörtert werden.

21. Andere Auskunfteien

21.1 Zulässige Übermittlung von Negativdaten an Auskunfteien

Nicht in allen Fällen dürfen negative Auskünfte über Personen an Auskunfteien weiter gegeben werden. Zulässig ist das erst nach Prüfung verschiedener Voraussetzungen und einer Einzelfallbeurteilung.

Auskunfteien sind darauf angewiesen, dass ihnen Informationen über das Zahlungsverhalten von Personen übermittelt werden. Zulässig ist das nach den Vorschriften des Bundesdatenschutzgesetzes (BDSG) nur dann, wenn das berechtigte Interesse eines Dritten an der Kenntnis der Daten besteht und insbesondere kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Erhebung, Verarbeitung oder Nutzung hat (vgl. §§ 28 Abs. 3 Nr. 1, 29 Abs. 1 Nr. 1 und Abs. 2 Nr. 1 a) BDSG).

Nach Auffassung der Obersten Aufsichtsbehörden für den Datenschutz sind schutzwürdige Betroffeneninteressen immer dann nicht beeinträchtigt, wenn sog. „harte“ Negativdaten wie Zwangsvollstreckung, Konkurs, Haftbefehl, Abgabe einer Eidesstattlichen Versicherung, Pfändung oder Inanspruchnahme einer Lohnabtretung gemeldet werden. Diese Daten sind jederzeit nachprüfbar und deuten darauf hin, dass der Betroffene zahlungsunfähig oder zahlungsunwillig ist. Daher muss er die Weitergabe der Informationen an diejenigen, die daran – etwa wegen eines Kredits oder einer sonstigen Vorleistung – ein berechtigtes Interesse haben, hinnehmen.

Auskunfteien, insbesondere solche, die im Verbund mit einem Inkassounternehmen arbeiten, gehen aber zunehmend dazu über, Auskünfte über Betroffene schon dann zu erheben und zu übermitteln, wenn die Stufe eines solchen „harten“ Negativdatums noch nicht erreicht ist. Begründet wird das mit dem Wortlaut des Gesetzes, der allein eine Abwägung zwischen den berechtigten

Interessen des Empfängers und den schutzwürdigen Interessen des Betroffenen an dem Ausschluss einer Übermittlung fordert. Insbesondere Inkassounternehmen, aber auch andere Datenlieferanten von Auskunfteien möchten solche Übermittlungen schon dann vornehmen, wenn mehrere Mahnungen erfolglos geblieben sind.

Die Datenschutzaufsichtsbehörden der Länder und der Verband der Handelsauskunfteien haben sich mit dieser Frage sehr intensiv auseinandergesetzt. Dabei hat sich herausgestellt, dass seitens einiger Datenschutzaufsichtsbehörden Zweifel daran bestehen, dass andere als die „harten" Negativdaten übermittelt werden dürfen. Ausgehend von einem Urteil des Saarländischen Oberlandesgerichts ist der Hamburgische Datenschutzbeauftragte der Auffassung, dass dies unter strengen Voraussetzungen zulässig ist. Danach müssen die folgenden Kriterien erfüllt sein, um eine Zulässigkeit der Übermittlung begründen zu können:

- Offensichtlich unstreitiger Forderungsrückstand,
- wiederholte vergebliche Zahlungsaufforderungen,
- Hinweise auf Zahlungsunfähigkeit oder -unwilligkeit und
- sorgfältige Einzelfallabwägung.

21.2 Recht auf Auskunft

Die Neufassung des Bundesdatenschutzgesetzes (BDSG) hat dazu geführt, dass die Betroffenen von Auskunfteien eher Auskunft über Herkunft und Empfänger ihrer personenbezogenen Daten erhalten.

Betroffene können nach § 34 Abs. 1 BDSG von der verantwortlichen Stelle Auskunft auch über Herkunft und Empfänger ihrer personenbezogenen Daten verlangen. Vor der Neufassung des Bundesdatenschutzgesetzes im Mai 2001 waren Auskunfteien insofern privilegiert, als sie diese Auskunft nur erteilen mussten, wenn der Betroffene begründete Zweifel an der Richtigkeit der Daten geltend machte. Diese Situation war jahrelang für die Betroffenen, die ein großes Interesse daran hatten zu erfahren, wer bei einer Auskunftei Informationen über sie eingeholt hatte, äußerst unbefriedigend und führte auch immer wieder zu Beschwerden bei den Datenschutzaufsichtsbehörden.

Das neue Gesetz gewährt diese Einschränkung des Auskunftsrechts nur dann, wenn nicht seitens der Auskunftei das Interesse an der Wahrung des Geschäftsgeheimnisses überwiegt. Mit der Neuregelung sollen die Auskunftsrechte der Betroffenen gestärkt werden. In der Umsetzung gab es zunächst erhebliche Differenzen zwischen den Auskunfteien und den Datenschutzaufsichtsbehörden. Die Auskunfteien vertraten die Auffassung, jede Geschäftsbeziehung zu einem ihrer Kunden stelle ein überwiegendes Interesse an der Wahrung des Geschäftsgeheimnisses dar.

Mit dieser Einstellung wurde der Sinn und Zweck der neuen Vorschrift vollständig unterlaufen. Das Gesetz geht nämlich von einer Abwägung im Einzelfall aus, die nur dann zu einer Verweigerung der Auskunft führen kann, wenn die Auskunftei Gründe für ein ausnahmsweise vorliegendes höheres Interesse an der Wahrung des Geschäftsgeheimnisses vorbringt. Betroffene haben auch kein Verständnis dafür, wenn ihnen beispielsweise der Name eines großen – berechtigterweise abfragenden -Unternehmens vorenthalten wird und sie statt dessen Spekulationen über etwaige unberechtigte Abfragen anstellen müssen. Ebenso wenig ist in der Regel davon auszugehen, dass vorleistende Unternehmen Probleme mit der Bekanntgabe der Anfrage haben.

Der Verband der Handelsauskunfteien hat jetzt vermittelnd angeboten, dass eine Auskunftserteilung seitens der Auskunfteien zumindest über die Empfänger der Daten immer dann erfolgt, wenn bestimmte Branchen (Kreditversicherungen/Versicherungen, Versandhandel, Telekommunikation, Banken, Leasing-/Factoringgesellschaften, Konzerngesellschaften) beteiligt sind. Darüber hinaus soll die Auskunft unbeschränkt erteilt werden, wenn begründete Zweifel an der Richtigkeit der Daten, Schadensersatzansprüche wegen Unrichtigkeit der Daten, Missbrauch durch den Datenempfänger oder Zweifel am berechtigten Interesse des Datenempfängers vorliegen.

Die Datenschutzaufsichtsbehörden sehen eine solche Lösung zwar als Fortschritt, nicht jedoch als abschließend an. Darüber hinaus kann es auch Einzelfälle anderer Art geben, in denen kein überwiegendes Interesse an der Wahrung des Geschäftsgeheimnisses vorliegt. Es bleibt abzuwarten, wie die Auskunftspraxis sich unter den getroffenen Vorgaben entwickelt. Darüber hinaus werden Gespräche auch über die Bekanntgabe der Herkunft der Daten geführt werden müssen.

21.3 Warndateien im Internet

Das Internet bietet zunehmend eine Plattform zur Anschwärzung von Personen. In fast allen Fällen ist das unzulässig und kann auch mit einem Bußgeld geahndet werden.

Uns erreichten mehrere Anfragen von Unternehmensgründern und von bereits bestehenden Unternehmen, die schlechte Erfahrungen mit der Zahlungsmoral ihrer Kunden gemacht hatten und daher beabsichtigten, Warndateien über das Zahlungsverhalten von Personen oder auch von Unternehmen im Internet zur Verfügung zu stellen. Im Bereich anderer Datenschutzaufsichtsbehörden stellen sich diese Probleme ebenfalls.

Die Anfragen zu Warndateien, auf die jedermann im Internet Zugriff nehmen könnte, waren schnell beantwortet, weil derartige Vorhaben unzulässig sind. Eine solche Veröffentlichung verletzt nämlich die schutzwürdigen Interessen jedes einzelnen Betroffenen, weil interessierte Internetbenutzer jederzeit Zu-

griff auf diese Daten nehmen können, ohne dass ihr berechtigtes Interesse im Einzelfall – als Voraussetzung einer zulässigen Datenübermittlung – geprüft werden könnte.

Diejenigen, die sich bei uns nach der Zulässigkeit einer nur für eine geschlossene Benutzergruppe zugänglichen Warndatei erkundigten, nahmen hiervon ohne intensivere Befassung mit den datenschutzgerechten Möglichkeiten Abstand. Auch diese Unternehmen müssen nämlich die strengen Voraussetzungen an das zulässige Betreiben einer Auskunftei erfüllen und sich zusätzlich um erhebliche technische Sicherheitsvoraussetzungen kümmern. Eine Umsetzung scheiterte in der Regel schon daran, dass die Interessenten nicht bereit waren, zu überprüfen, ob die Betroffenen ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung haben. Daneben wäre es unter anderem erforderlich, das berechtigte Interesse des Empfängers an der Auskunft aufzuzeichnen, den Betroffenen von der erstmaligen Übermittlung zu benachrichtigen, ihm Auskunft zu erteilen und die Berichtigung, Löschung und Sperrung der Daten erforderlichenfalls sicher zu stellen.

Nicht jedes Unternehmen mit entsprechenden Plänen erkundigt sich jedoch im Vorwege bei den Datenschutzaufsichtbehörden nach den Zulässigkeitsvoraussetzungen eines solchen Vorhabens. So wurden wir durch einen aufmerksamen Kunden auf die Veröffentlichung von sog. Schlechtzahlern durch einen Händler aufmerksam, der ohne Einschränkung Kunden, die nicht nach seinen Vorstellungen zahlten, für jeden zugänglich im Internet veröffentlichte. Dies widerspricht den Vorschriften des Bundesdatenschutzgesetzes, in solchen Fällen besteht außerdem ein sehr hohes Missbrauchsrisiko durch die Veröffentlichung falscher Angaben.

Es ist damit zu rechnen, dass auch künftig Unternehmensgründer das Internet nutzen, um neue Auskunfteien ins Leben zu rufen. Die Aufsichtsbehörden werden darauf zu achten haben, dass dabei die Datenschutzvorschriften nicht außer Acht gelassen werden.

21.4 Broschüre Handels- und Wirtschaftsauskunfteien

Der Hamburgische Datenschutzbeauftragte veröffentlichte eine neue Broschüre über Handels- und Wirtschaftsauskunfteien.

Nach Änderung des Bundesdatenschutzgesetzes im Jahre 2001 ergab sich die Notwendigkeit, die Broschüre Handels- und Wirtschaftsauskunfteien der neuen Gesetzeslage anzupassen. Im April 2002 kam diese Informationsschrift, die zusammen mit Bremen, Niedersachsen und Nordrhein-Westfalen entwickelt wurde, heraus. Sie richtet sich vor allen Dingen an interessierte Bürger, die erfahren möchten, wie Handels- und Wirtschaftsauskunfteien arbeiten und welche Rechte sie geltend machen können. Die Broschüre ist beim Hamburgischen Datenschutzbeauftragten erhältlich.

22. Kreditwirtschaft

22.1 Schufa-Klausel bei Guthabenkonto/Konto für Jedermann

Zur Überprüfung, ob ein Konto für Jedermann eröffnet werden kann, holen die Kreditinstitute eine Schufa-Anfrage ein.

Die Obersten Aufsichtsbehörden haben mit den Vertretern des Zentralen Kreditausschusses in der Arbeitsgruppe Kreditwirtschaft erörtert, ob auch bei Einrichtung eines Girokontos auf Guthabenbasis die Unterzeichnung der Schufa-Klausel verlangt werden kann. Denjenigen, die infolge wirtschaftlicher Schwierigkeiten eine negative Schufa-Auskunft haben, war in der Vergangenheit die Eröffnung eines Girokontos häufig mit Hinweis auf die schlechte Auskunft abgelehnt worden. Dies führte zu einer gesellschaftlichen und wirtschaftlichen Benachteiligung, da in der Regel die zum Lebensunterhalt notwendigen Zahlungen über ein Girokonto abgewickelt werden (Lohn und Gehalt, Miete usw.).

Die Obersten Aufsichtsbehörden hatten daher gefordert, dass den betroffenen Personen ein Girokonto auf Guthabenbasis ohne Unterzeichnung der Schufa-Klausel eingerichtet werden müsste. Zwischen den Obersten Aufsichtsbehörden und den Vertretern der Kreditwirtschaft bestand Einvernehmen, dass für die Führung eines Kontos auf Guthabenbasis eine Unterzeichnung der Schufa-Klausel nicht erforderlich ist, da ein kreditorisches Risiko in diesen Fällen nicht besteht.

Zur Abwendung einer gesetzlichen Regelung hat sich die Kreditwirtschaft im Jahr 1995 freiwillig bereit erklärt, für sozial und wirtschaftlich Schwache zumindest ein Girokonto „zur Entgegennahme von Gutschriften, zu Barein- und auszahlungen und zur Teilnahme am Überweisungsverkehr“ zur Verfügung zu stellen (ZKA-Empfehlung zum „Girokonto für Jedermann“). Die Vertreter der Kreditwirtschaft haben hierzu dargelegt, dass bei einem solchen Konto in der Regel durch technische Sperren sichergestellt wird, dass das Konto nur auf Guthabenbasis geführt wird. Bis auf diese Einschränkung unterscheidet sich das Konto nicht von einem gewöhnlichen Girokonto.

Um zu überprüfen, ob eine Person zu dem von der ZKA-Empfehlung „Girokonto für Jedermann“ begünstigten Personenkreis gehört, ist nach Darstellung der Kreditwirtschaft eine Schufa-Anfrage erforderlich. Ergibt sich daraus, dass die Person bislang kein Girokonto hat und ansonsten auch keine der in der ZKA-Empfehlung „Girokonto für Jedermann“ beschriebenen Unzumutbarkeitsgründe für das Kreditinstitut vorliegen, wird für die Person ein Girokonto eröffnet. Davon zu unterscheiden ist die Führung eines Kontos nur auf Guthabenbasis, was in der Regel nur für solvente Kunden aus verschiedenen Gründen eingerichtet wird. Aufgrund dieser neuen Informationen werden die Aufsichtsbehörden ihre bisherige datenschutzrechtliche Bewertung überprüfen.

Die Vertreter der Kreditwirtschaft wiesen darauf hin, dass es bei jedem im Zentralen Kreditausschuss organisierten Bankenverband eine bzw. mehrere Streitschlichtungsstelle(n) gibt. Jeder, der meint, entgegen der ZKA-Empfehlung „Girokonto für Jedermann“ sei ihm ein Konto verweigert worden, kann sich an die jeweils zuständige Stelle wenden.

22.2 EC-Karte mit Altersangaben

Kontogebundene EC-Karten werden künftig mit einem Legitimationsvermerk bei Karteninhabern, die das 18. Lebensjahr vollendet haben, versehen.

Wir hatten über die Absicht des Bundesgesundheitsministeriums und des Verbands der Automatenaufsteller berichtet (18. TB, 24.4), durch ein Altersmerkmal auf der kontogebundenen EC-Karte Jugendlichen unter 16 Jahren den Zugang zu Zigarettenautomaten zu verwehren bzw. zu erschweren. So sollte § 10 des Jugendschutzgesetzes Rechnung getragen werden. Nach dieser Vorschrift dürfen Tabakwaren nicht in Automaten angeboten werden, es sei denn, durch technische Vorrichtungen oder ständige Aufsicht ist sichergestellt, dass Kinder und Jugendliche unter 16 Jahren Tabakwaren nicht entnehmen können.

Aus Sicht der Aufsichtsbehörden bestanden gegen dieses Vorhaben datenschutzrechtliche Bedenken. Der Zentrale Kreditausschuss hat daher das Konzept überarbeitet und ein neues Verfahren vorgeschlagen. Danach wird die EC-Karte mit einem Legitimationsvermerk bei Karteninhabern, die das 18. Lebensjahr vollendet haben, versehen. Der Vermerk enthält bei volljährigen Karteninhabern kein Datum. Bei minderjährigen Karteninhabern enthält der Vermerk das verschlüsselte Datum, an dem der Karteninhaber volljährig wird. Von diesem Datum kann das Automaten-Lesegerät zurückrechnen und so überprüfen, ob der Inhaber der Karte beim Zigarettenkauf mittlerweile volljährig ist. Anderenfalls wird der Kauf verweigert. Die Einwilligung zur Aufbringung des Datums auf der Geldkarte wird bei minderjährigen Kunden bereits bei Kontoeröffnung mit dem Antragsformular eingeholt werden.

Die Obersten Aufsichtsbehörden haben gegen das geänderte Verfahren und das zur Umsetzung erforderliche technische Sicherheitskonzept keine datenschutzrechtlichen Bedenken.

23. Videoüberwachung

23.1 Allgemeines

Bei der Videoüberwachung öffentlich zugänglicher Räume werden häufig die gesetzlichen Anforderungen nicht ausreichend berücksichtigt.

Das Thema Videoüberwachung war im Berichtszeitraum Gegenstand mehrerer Eingaben bei der Aufsichtsbehörde. Dabei konnte festgestellt werden, dass immer mehr Videoüberwachungsanlagen installiert werden. Neben öffentlich

zugänglichen Plätzen, Kaufhäusern und Bürogebäuden werden u.a. auch Hotels, Bars, Restaurants und Sportstudios mit Videoüberwachungsanlagen ausgestattet. Auch im privaten Bereich bringen Bürger Videoüberwachungsanlagen an ihren Häusern an.

Als häufigster Grund für die Installation der Anlagen wird die Erhöhung der Sicherheit genannt, d.h. durch die Videoüberwachung sollen Straftaten verhindert oder aufgeklärt werden. Die Installation von Webcams und die Einstellung der Aufnahmen in das Internet dient dagegen meist Werbezwecken einzelner Unternehmen. Begünstigt wird die Zunahme der Videoüberwachung auch dadurch, dass es mittlerweile leicht anzubringende Überwachungskameras mit guter Aufnahmequalität preiswert im Supermarkt gibt.

Mit § 6 b BDSG hat der Gesetzgeber im Rahmen der Novellierung vom 23. Mai 2001 die Überwachung mit Videokameras an bestimmte gesetzliche Voraussetzungen gebunden.

§ 6 b Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen

(1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,

2. zur Wahrnehmung des Hausrechts oder

3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

(2) Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.

(3) Die Verarbeitung oder Nutzung von nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

(4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den §§ 19 a und 33 zu benachrichtigen.

(5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

Bei unseren Prüfungen stellten wir immer wieder fest, dass diese Vorschrift nicht bekannt ist und die dort geregelten Voraussetzungen auch nicht eingehalten werden. Erschwert wird die Arbeit der Aufsichtsbehörde durch das häufig fehlende Problembewusstsein, dass Persönlichkeitsrechte durch die Videoüberwachung beeinträchtigt werden. Videokameras werden von den Betroffenen hingenommen nach dem Motto „ich habe nichts zu verbergen".

Dabei wird die Gefahr einer immer engmaschigeren Überwachung nicht gesehen, die im Extremfall zu einer nahezu totalen Nachvollziehbarkeit aller Lebensbereiche des Einzelnen führen kann. § 6b BDSG berücksichtigt dieses Spannungsfeld durch die Beschränkung der Zulässigkeit auf eine tatsächlich erforderliche Beobachtung und das Erfordernis einer einzelfallbezogenen umfassenden Güter- und Interessenabwägung unter Beachtung der schutzwürdigen Interessen der Betroffenen.

23.2 Videoüberwachung in U-Bahnen

Die Hamburger Hochbahn AG (HHA) hat unter Beachtung datenschutzgerechter Auflagen mit der flächendeckenden Ausstattung ihrer U-Bahn-Fahrzeuge mit Video-Aufzeichnungstechnik begonnen.

Nach Beendigung des mehrjährigen Testbetriebs (vgl. 18.TB, 25.3.2) hat die HHA mit der flächendeckenden Ausstattung ihrer U-Bahn-Wagen mit Videokameras und digitalen Aufzeichnungsgeräten begonnen. Die Aufnahmen erfolgen durch zwei festeingestellte Kameras pro Wagen. Die Datenaufzeichnungen auf einen digitalen Ringspeicher, eine sogenannte „Black Box", werden nach 24 Stunden automatisch überschrieben, falls die Aufnahmen nicht wegen eines wichtigen Vorkommnisses sichergestellt und ausgewertet werden. Dies ist der Fall, wenn Fahrgäste eine entsprechende Meldung machen oder größere Schäden an einem Fahrzeug festgestellt werden. Die Herausnahme von Aufzeichnungen aus den Fahrzeugen darf nur erfolgen bei strafbaren Handlungen, Unfällen und besonderen Betriebs- und Schadensereignissen, die abschließend und vollständig benannt werden. Der Zugriff auf die Videodaten ist lediglich einem konkret angegebenen, sehr begrenzten Personenkreis möglich. Eine laufende Beobachtung der Videoaufnahmen, z. B. durch den Fahrer oder Mitarbeiter der Betriebszentrale, erfolgt nicht. An den überwachten Wagen ist ein Hinweisschild mit dem Text „Zu Ihrer Sicherheit erfolgt in diesem Wagen eine Videoaufzeichnung" angebracht.

Wir haben als Aufsichtsbehörde für den Datenschutz bereits den Testbetrieb begleitet und halten das jetzige Vorhaben bei Beachtung konkret definierter datenschutzrechtlicher Vorkehrungen für vertretbar. Die HHA hat zugesagt, diese Vorkehrungen zu treffen und beizubehalten.

Das Konzept beruht in seinen Grundzügen auf einem Richtlinienpapier zum „Einsatz der Videotechnik im öffentlichen Personennahverkehr (ÖPNV)", welches in den vergangenen Jahren gemeinsam von einer bundesweiten Arbeits-

gruppe der Landesdatenschutzbeauftragten und dem Verband Deutscher Verkehrsunternehmen (VDV) erarbeitet wurde. Die im Mai 2002 veröffentlichten – und mit den Aufsichtsbehörden der Länder abgestimmten – Empfehlungen des Verbandes sind von der HHA in ihrem Konzept entsprechend berücksichtigt worden.

Die datenschutzrechtliche Bewertung des Vorhabens richtet sich nach § 6 b Abs. 1 BDSG. Danach ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) nur zulässig, soweit sie gemäß Nr. 2 zur Wahrnehmung des Hausrechts bzw. nach Nr. 3 zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Zur Bewertung der Frage, inwieweit eine flächendeckende Ausstattung aller Fahrzeuge mit Video-Aufzeichnungstechnik aus datenschutzrechtlicher Sicht zulässig ist, waren das wirtschaftliche und rechtliche Interesse der HHA an der geplanten Ausweitung der Videoüberwachung sowie das allgemeine Persönlichkeitsrecht der davon betroffenen Fahrgäste zu berücksichtigen und gegeneinander abzuwägen. Dabei war insbesondere zu beachten, dass eine ständige Videoüberwachung eines öffentlich zugänglichen Raumes nach der Rechtsprechung des BGH einen weitreichenden Eingriff in das allgemeine Persönlichkeitsrecht darstellt und allenfalls dann zulässig sein kann, wenn keine anderen zumutbaren Mittel zur Verfügung stehen, um schwerwiegende Beeinträchtigungen der Rechte Dritter abzuwehren (vgl. BGH NJW 1995, 1955ff).

Eine ständige Videoüberwachung, der sich ein Betroffener nicht entziehen kann, greift stärker in das allgemeine Persönlichkeitsrecht ein als eine nur punktuelle und gelegentliche Überwachung anhand der Videoaufzeichnungen. Zu berücksichtigen war dabei , dass die HHA als öffentliches Unternehmen Grundrechte der Fahrgäste besonders zu beachten hat und dass es sich bei öffentlichen Verkehrsmitteln um eine Daseinsvorsorge handelt, auf die viele Menschen angewiesen sind.

Die HHA hat zudem die von der Aufsichtsbehörde geforderten Maßnahmen gemäß § 9 BDSG zur Verhinderung eines Missbrauchs der Videoaufzeichnungen getroffen. Dazu gehört insbesondere eine Verschlüsselung der Bilddaten und eine Dienstanweisung, die diese Vorgaben verbindlich regelt.

23.3 Videoüberwachung in einer Bar

Die zunehmende Videoüberwachung macht auch vor Gaststätten und Bars nicht halt.

Durch eine Beschwerde wurden wir darauf aufmerksam, dass in einer Bar Videoüberwachung und auch -aufzeichnung durchgeführt wird. Davon ist einer-

seits der Eingangsbereich der Bar, aber auch der daran vorbei gehende öffentliche Weg betroffen. Andererseits wird auch in der Bar selbst videoüberwacht und -aufgezeichnet.

Nach § 6 b BDSG ist die Videoüberwachung durch nicht öffentliche Stellen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte dafür bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Diesen Voraussetzungen entspricht die von dem Betreiber der Bar durchgeführte Videoüberwachung nicht vollständig.

Das Unternehmen hat vorgetragen, dass die Videoüberwachung zur Verhinderung von Straftaten vor und in der Bar und zur Wahrnehmung des Hausrechts erforderlich sei. An dieser Erforderlichkeit bestanden zunächst erhebliche Zweifel. Es ist zur Erreichung der vorgenannten Zwecke zweifellos nicht erforderlich, unbeteiligte Passanten auf dem öffentlichen Gehweg, die nicht zu den Gästen der Bar gehören, aufzunehmen. Die Videoüberwachung darf daher keine Bereiche des öffentlichen Gehwegs umfassen. Anders würde die Angelegenheit zu beurteilen sein, wenn unter Hinweis auf die Überwachung lediglich der unmittelbare Eingangsbereich der Bar betroffen wäre.

Der Aufsichtsbehörde wurde zunächst nicht ausreichend nachgewiesen, dass auch eine Videoüberwachung des Innenraums der Bar zur Erreichung der genannten Zwecke notwendig ist. Dabei ist zu bedenken, dass Gäste eines Lokals, zumal einer Bar, möglichst ungestört ihre Freizeit verbringen möchten. In der Regel wird der Erhalt der Privatsphäre und die Freiheit vor systematischer Beobachtung durch Dritte innerhalb der Räumlichkeiten einer Gaststätte selbstverständlich angenommen. Es wird nicht davon ausgegangen, dass jedes Gespräch mit anderen Gästen, jedes Verhalten und auch der Getränkekonsum aufgezeichnet wird und aufgezeichnet werden kann, selbst wenn die Kameras sichtbar angebracht sind und im Außenbereich deutlich darauf hingewiesen wird.

Zugunsten der Betroffenen ist in der Regel davon auszugehen, dass ihre schutzwürdigen Interessen gegenüber der nachträglichen Aufklärung von gelegentlichen Straftaten überwiegen. Zur Verhinderung von Straftaten reichen in der überwiegenden Zahl der Fälle zum einen eine Überwachung des Eingangs und zum anderen eine erhöhte Aufmerksamkeit des Personals aus. Anderenfalls wäre zu befürchten, dass eine flächendeckende Videoüberwachung und –aufzeichnung in Gaststätten sich durchsetzt, die dazu führt, dass ein beobachtungs- und aufzeichnungsfreier Bar-, Restaurant- oder Kneipenbesuch für niemanden mehr möglich ist. In dem konkreten Einzelfall hat der Inhaber der Bar jedoch letztlich nachvollziehbare Gründe darlegen können, die die Abwägung zu seinen Gunsten ausfallen ließen und nur eine Änderung der Videoüberwachung im Eingangsbereich erforderlich machten.

23.4 Videoüberwachung an einem Gebäude mit Übertragung ins Internet

Auch bei Panorama-Aufnahmen im Internet überwiegen regelmäßig die Persönlichkeitsrechte von Betroffenen.

Durch einen Betroffenen wurden wir auf die Videoüberwachung an einem Geschäftsgebäude aufmerksam gemacht, bei der u.a. die Videoaufnahmen des Gebäudeeingangsbereiches in das Internet gestellt worden sind.

Diese Videoüberwachungsanlage wurde von einem in diesem Gebäude ansässigen Unternehmen betrieben. Als Zweck wurde angegeben, dass die Anlage primär der Verhinderung und der Aufklärung von strafrechtlichen Vorgängen dienen soll, weil es in der Vergangenheit bei diesem Unternehmen nachweislich zu Diebstählen gekommen ist.

Bei dieser Anlage wurden insgesamt sechs Kameras eingesetzt. Mit fünf herkömmlichen Videokameras wurden die zwei Hauseingänge (Haupt- und Nebeneingang) und zwei Laderampen mit den Eingängen zu den firmeneigenen Lagerräumen überwacht. Als sechste Kamera wurde eine Webcam eingesetzt, mit der ausschließlich der Haupteingang und die daneben befindlichen Parkplätze überwacht wurden. Die überwachten Bereiche sind während der allgemeinen Geschäftszeiten öffentlich zugänglich.

Neben einer Aufzeichnung der Videoaufnahmen wurden die Videobilder der Webcam auch noch über die Internetpräsentation des Unternehmens der Öffentlichkeit zugänglich gemacht. Über die dabei angebotenen Optionen war es jedem Internet-User möglich, eine Steuerung der Webcam vorzunehmen und Vergrößerungen von Videobildern zu erstellen. Weiterhin wurde so jedem Internet-User weltweit die Möglichkeit eingeräumt, den Haupteingang des Gebäudes und die daneben liegenden Parkplätze zu überwachen und betroffene Personen (z. B. Mitarbeiter, Geschäftspartner, Kunden, Lieferanten von allen im Gebäude ansässigen Unternehmen) zu identifizieren. Außerdem wurde auf diese Weise die Verarbeitung und Nutzung dieser Aufnahmen völlig unkontrollierbar.

Gemäß § 6 b BDSG ist eine Videoüberwachung öffentlich zugänglicher Räume durch nichtöffentliche Stellen nur zulässig, soweit sie zur Wahrnehmung des Hausrechts oder berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Der für diese Videoüberwachungsanlage angegebene Zweck, die Verhinderung und Aufklärung von strafrechtlichen Vorfällen, konnte hinsichtlich der Webcam und zweier herkömmlicher Videokameras nicht nachvollzogen werden, weil mit diesen Kameras keine dem Unternehmen zugehörigen Räumlichkeiten überwacht wurden. Die Anlage war insoweit als unzulässig anzusehen. Außerdem wurde mit der Darstellung der Videoaufnahmen im Internet in

erheblichem Maße in die Persönlichkeitsrechte der Betroffenen eingegriffen, so dass die Anlage auch in dieser Hinsicht als unzulässig zu betrachten war.

Aus diesem Grund haben wir das Unternehmen aufgefordert, auf die Videoüberwachung des Haupteingangsbereiches mittels Webcam zu verzichten und sich bei der übrigen Videoüberwachung – entsprechende dem angegebene Zweck – auf die eigenen Unternehmensräumlichkeiten zu beschränken. Dabei sollte auch insgesamt auf die Überwachung der Hauseingänge verzichtet werden. Darüber hinaus haben wir das Unternehmen aufgefordert, die weiteren Zulässigkeitsvoraussetzungen des § 6b BDSG zu erfüllen (z. B. Hinweise auf die Videoüberwachung, schriftliche Festlegung des konkreten Zwecks).

Das Unternehmen hat daraufhin auf die Überwachung der Hauseingänge mit den herkömmlichen Videokameras verzichtet. Die Videoaufnahmen der Webcam hat sie dagegen weiterhin, nunmehr nur noch in verkleinerter Form, als sog. Panoramaaufnahme in das Internet gestellt, wobei auch die Steuerungsmöglichkeiten der Kamera nicht mehr angeboten wurden. Durch diese Maßnahmen sollte nach Ansicht des Unternehmens eine Identifizierung von Personen nicht mehr möglich sein, so dass auch keine Beeinträchtigungen von Persönlichkeitsrechten mehr stattfinden können.

Dieser Auffassung konnten wir nicht folgen, weil es trotz der zwischenzeitlich vorgenommenen Änderungen weiterhin möglich war, dass eine Person bestimmbar gemacht oder bestimmten Sachverhalten zugeordnet werden konnte. Denn über die Internetdarstellung war für einen Dritten (z. B. Vorgesetzten, Kollegen, Ehepartner) weiterhin erkennbar, zu welchen Zeitpunkten eine bereits bekannte Person das Gebäude betritt oder verlässt, insbesondere dann, wenn diese ein Kraftfahrzeug in einer auffälligen Farbe fährt (z. B. rot oder weiß) und den Wagen regelmäßig neben dem Hauseingang parkt.

Somit handelte es sich bei den Internetdarstellungen weiterhin um personenbezogene Daten im Sinne des Bundesdatenschutzgesetzes (BDSG), für deren Verarbeitung (z. B. Übermittlung in das Internet) entweder eine Rechtsgrundlage oder eine Einwilligung der Betroffenen erforderlich ist. Da beides nicht gegeben war, haben wir diese Videoüberwachung insoweit weiterhin als unzulässig angesehen und den Abbau der Kamera gefordert. Das Unternehmen hat daraufhin auf den weiteren Einsatz der Webcam und die Präsentation der Videoaufnahmen im Internet verzichtet.

24. Gesundheit

24.1 Prüfung einer Gewebeprobenbank

Die Prüfung einer gewerblichen Tumorgewebe-Probenbank führte zur Forderung, insbesondere für den zukünftigen Ausbauzustand ein sicheres und belastbares Pseudonymisierungsverfahren zu organisieren.

Im Februar 2003 prüften wir eine als GmbH geführte Gewebeprobenbank, die eng, aber rechtlich selbstständig, mit einem gemeinnützigen Krankenhaus zusammenarbeitet und dessen Proben und Behandlungsdaten zur genetischen Forschung nutzt. Aus der rechtlichen Selbstständigkeit folgte unsere – umgehend erfüllte – Forderung nach Bestellung eines eigenen betrieblichen Datenschutzbeauftragten. Als kritischer Punkt erwies sich die Organisation der Zuordnung von Proben, klinischen Daten und Nachsorgedaten:

Ausgangspunkt der Datenverarbeitung ist eine ausführliche Aufklärung mit Einwilligungserklärung, die die Patienten vor der Operation erhalten und unterzeichnen. Ihr Text musste korrigiert werden, um den Patienten transparent zu machen, wann und in welcher Form die Gewebeproben mit den klinischen Daten aus Krankenakte bzw. Fragebogen sowie mit späteren Nachsorge-Daten verbunden werden. Auch Hinweise auf die Freiwilligkeit und die Widerrufbarkeit der Einwilligung waren zu ergänzen.

Die Erfassungskräfte der GmbH legen für alle operierten Personen, die die Einwilligungserklärung unterschrieben, eine Schlüsselliste mit dem Patientennamen und einer sog. Case-Nummer an. Diese Liste wird im Krankenhaus verwahrt und ist für die Erfassungskräfte der GmbH zugänglich. Die OP-Proben und die unmittelbar danach auszufüllenden Erfassungsbögen mit den klinischen und sozialen Daten werden ausschließlich mit der Case-Nummer gekennzeichnet. Den so pseudonymisierten Erfassungsbögen werden Anästhesieprotokolle und Laborergebnisse beigefügt, von denen zuvor ebenfalls der Patientenname entfernt wurde.

Die Nachsorgedaten wurden bis zu unserer Prüfung in der Weise erhoben, dass die nachbehandelnden Ärzte einen Bogen des Krankenhauses mit Namen und Case-Nummer des Patienten ausfüllten und dem Krankenhaus zurückschickten. Die hierin liegende datenschutzwidrige und unnötige Entschlüsselung der Case-Nummer gegenüber den nachbehandelnden Ärzten wurde inzwischen auch rückwirkend korrigiert.

Alle diese Daten werden in eine Datenbank auf einem besonderen Server übertragen. Auf unseren Hinweis wurden inzwischen Benutzeranmeldung und Benutzerverwaltung dem gebotenen Datensicherheitsstandard angepasst, hochwertige Verschlüsselungsverfahren implementiert sowie der Einsatz von SSL-Client-Zertifikaten zugesagt. Die Patientendaten werden nur mit einer vom System generierten Codenummer und der Case-Nummer sowie einem Einwegschlüssel verbunden, der ebenfalls automatisch aus dem Namen, Geburtsnamen, Vornamen und Geburtsdatum gebildet wird. Die letztgenannten Identifikationsdaten werden nicht gespeichert.

Das datenschutzrechtliche Hauptproblem sahen wir in der fehlenden organisatorischen Trennung des Behandlungsbereichs (Krankenhaus, OP) vom Forschungsbereich (GmbH, Probenbank), zwischen denen die Erfassungskräfte

der GmbH hin- und herpendeln. Denn auch unabhängig von einer Einwilligung des Patienten muss die datenverarbeitende Stelle dafür sorgen, dass der Rückgriff der Forschung auf patientenbezogene Behandlungsdaten auf ein Minimum reduziert und mit einem Maximum an (angemessenem) Missbrauchsschutz versehen wird.

Insbesondere im Hinblick auf die geplante Ausweitung der Proben- und Datenbeschaffung auf andere Krankenhäuser, auf die stark anwachsende Zahl von Proben und Daten sowie auf den Zugriff der GmbH-Mitarbeiterinnen auf die gesamten Patientenakten haben wir von der Leitung der Gewebeprobenbank ein neues Konzept der Pseudonymisierung gefordert. Dabei sollen die Proben- und Datenhaltung einerseits und die Verwaltung der Pseudonyme und Identitätsdaten andererseits verschiedenen Stellen zugeordnet werden. Eine solche Einschaltung eines externen Datentreuhänders, der nur die Pseudonymisierung und bei Bedarf auch die De-Pseudonymisierung organisiert, ohne Zugriff auf Proben und Daten zu haben, ist eine Forderung, die die Datenschutzbeauftragten bereits 2001 in einem Gesetzesvorschlag für genetische Untersuchungen an den Gesetzgeber gerichtet hatten. Die GmbH hat hierfür die Beauftragung eines Rechtsanwalts in Aussicht gestellt. Für die Neukonzeption des Pseudonymisierungsverfahrens haben wir mit der GmbH eine Frist bis Ende 2003 vereinbart.

24.2 Datenschutzorganisation in privaten Krankenhäusern

Wir baten die privaten und gemeinnützigen Hamburger Krankenhäuser um Benennung ihrer betrieblichen Datenschutzbeauftragten. Dies verursachte mehrere Neubestellungen von Datenschutzbeauftragten und Nachfragen nach Aus- und Fortbildungsmöglichkeiten.

Im November 2001 baten wir alle gemeinnützigen, privaten und zum Teil auch kirchlichen Krankenhäuser in Hamburg, uns eine Kopie der schriftlichen Bestellung des oder der betrieblichen Datenschutzbeauftragten zur Verfügung zu stellen. Die Reaktion hierauf war sehr unterschiedlich: Während einzelne Häuser das gewünschte Dokument zusandten, erhielten wir aus anderen Kliniken Fragen nach der Zuständigkeit der Hamburger Aufsichtsbehörde für den Datenschutz, nach den Voraussetzungen für die Bestellung eines betrieblichen Datenschutzbeauftragten und nach Einrichtungen, die die notwendige Aus- und Fortbildung für diese Aufgabe anbieten.

Für kirchliche Krankenhäuser ist die Zuständigkeit der staatlichen Datenschutz-Aufsichtsbehörde in der Literatur umstritten; dies gilt zumindest für Klinik-Träger in privater Rechtsform wie Vereine oder GmbHs. Der Hamburgische Datenschutzbeauftragte erzielte Einvernehmen mit den Datenschutzbeauftragten der Kirchen darüber, dass Einrichtungen, die die Kirchen unabhängig von der Rechtsform in einer Liste als Teile der Kirche festlegten, der staatlichen Datenschutzaufsicht entzogen und nur dem kirchlichen Datenschutzbeauf-

tragten unterstellt sind.

Die Pflicht zur Bestellung einer oder eines betrieblichen Datenschutzbeauftragten ist abhängig von der Größe der Klinik. Es gibt in Hamburg kleine Häuser, die nach eigenen Angaben höchstens vier Mitarbeiterinnen oder Mitarbeiter mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beschäftigen und damit keinen Datenschutzbeauftragten bestellen müssen.

Weiter wandten sich einzelne Krankenhaus-Mitarbeiterinnen an uns, die als zukünftige betriebliche Datenschutzbeauftragte vorgesehen waren und sich die nach § 4 f Abs.2 BDSG notwendige Fachkunde verschaffen wollten. Wir vermittelten ihnen die Adressen einschlägiger Fortbildungseinrichtungen. Der offensichtliche Umstand, dass bisher kein betrieblicher Datenschutzbeauftragter bestellt war, verwirklichte den Tatbestand einer Ordnungswidrigkeit, wurde von uns aber angesichts des Bemühens um Nachbesserung nicht weiter verfolgt.

Mit zwei Verwaltungsleitern von Krankenhäusern klärten wir schließlich die Frage, ob auch in Kliniken ein externer Datenschutzbeauftragter nach § 4 Abs.2 Satz 2 BDSG bestellt werden darf. Hier knüpften wir an die schon im 16. Tätigkeitsbericht (18.1.3) vertretene Auffassung an, dass die ärztliche Schweigepflicht den Durchgriff eines externen Datenschutzbeauftragten auf Patientendaten verbietet.

Zulässig erscheint es hingegen, wenn der oder die externe Datenschutzbeauftragte sich auf Fragen der Organisation, Technik-Gestaltung und Fortbildung beschränkt und konkrete Patientenbeschwerden oder Kontrollaufgaben mit Personenbezug durch eine Kontaktperson im Krankenhaus bearbeiten lässt, die selbst der ärztlichen Schweigepflicht unterliegt. Letztlich unterliegt es dem Organisationsrecht des Krankenhausträgers, ob er einer oder einem internen Datenschutzbeauftragten bei Bedarf eine externe Fachkraft für Datenschutz und Datensicherheit an die Seite stellt oder ob er die externe Fachperson zu der oder dem betrieblichen Datenschutzbeauftragten bestellt und dieser oder diesem eine interne Hilfsperson zuordnet. Entscheidend ist, dass nur die in das Krankenhaus integrierte Person Zugriff auf die Patientendaten bekommen darf.

25. Sonstiges

25.1 Teilnehmererfassung bei Großveranstaltungen

Auch bei der Teilnehmererfassung für sportliche Großveranstaltungen sind die Vorschriften des BDSG zu beachten.

Großveranstaltungen wie die populären Marathonläufe erfreuen sich zunehmender Beliebtheit. Zur organisatorischen Abwicklung solcher Veranstaltun-

gen müssen personenbezogene Daten der Teilnehmer erhoben und verarbeitet werden.

Die Datenerhebung erfolgt in der Regel schriftlich, wobei Teilnahmeerklärungen für Sportveranstaltungen heute zunehmend auch über das Internet abgegeben werden können. Dabei ist zu beachten, dass der Veranstalter nach § 28 Bundesdatenschutzgesetz (BDSG) nur solche Daten erheben und verarbeiten darf, die im engen Zusammenhang mit dem Vertragszweck stehen und für die Durchführung des Vertrags erforderlich sind. Dies gilt zweifelsohne für den Namen, die Anschrift und das Alter der Teilnehmer.

Daten, die für die Erfüllung des Vertrags nicht erforderlich sind – z. B. Angaben zu Beruf oder Hobbys – dürfen nur mit ausdrücklicher Einwilligung des Teilnehmers erhoben werden. Der Teilnehmer muss in derartigen Fällen darüber aufgeklärt werden, zu welchem Zweck diese Daten erhoben werden sollen und dass die Angaben freiwillig erfolgen. Dem Teilnehmer dürfen keine Nachteile entstehen, wenn er die Angaben nicht macht. Bei einer Anmeldung über das Internet kommt in diesen Fällen die Besonderheit hinzu, dass die Abgabe der Einwilligung durch eine bewusste und eindeutige Handlung des Teilnehmers am Bildschirm erfolgen muss. Dies kann z. B. durch das Anklicken eines eindeutig beschrifteten Feldes erfolgen. Die Einwilligung ist nach § 4 Abs. 2 Teledienstedatenschutzgesetz (TDDSG) zu protokollieren.

Zur Datenerfassung während der Sportveranstaltung nutzen die Veranstalter zunehmend die Möglichkeit der Leistungserfassung mit sogen. Transpondern. Der Transponder, der z. B. an den Schuh des Sportlers geklebt werden kann, enthält einen Mikrochip mit einer Identifikationsnummer. Per Funk werden Angaben z. B. über Startzeitpunkt und Zieleinlauf der Sportler an ein Erfassungssystem übertragen und ausgewertet. Bei diesem System kann es sich um ein integriertes System handeln, dass neben der Leistungserfassung die gesamte Vertragsabwicklung möglich macht. Es werden auch Systeme eingesetzt, die sich auf die Leistungserfassung beschränken und die so ermittelten Daten an die Stelle, die für die Vertragsabwicklung und Ausstellung einer Urkunde zuständig ist, übermitteln. Die Erfassung und Verarbeitung der Leistungsdaten wird häufig durch spezialisierte Dienstleistungsfirmen als Auftragsdatenverarbeiter übernommen. In jedem Fall handelt es sich aufgrund der eindeutig personenbeziehbaren Identifikationsnummer bei der Leistungserfassung um die Verarbeitung personenbezogener Daten, so dass die Vorschriften des BDSG zu beachten sind.

Fotos und Filmaufnahmen, die von dem Ereignis gemacht werden, dürfen grundsätzlich für die anschließende Berichterstattung genutzt und veröffentlicht werden. Dies gilt auch dann, wenn einzelne Personen erkennbar sind. Das Recht der Teilnehmer am eigenen Bild nach dem Kunsturhebergesetz (KunstUrG) erfährt im Hinblick auf diese Berichterstattung eine Einschränkung. Weitere Nutzungen, z. B. zu Werbezwecken, sind dagegen nur zulässig, wenn der

Teilnehmer gegenüber dem Sportveranstalter eine entsprechende Einwilligung abgegeben hat. Hierbei ist darauf zu achten, dass die vorgesehenen Verwendungszwecke in der abzugebenden Erklärung genau beschrieben werden. Gezielt von einzelnen Teilnehmern während der Veranstaltung aufgenommene Fotos, z. B. zum Verkauf als persönliches Erinnerungsfoto, dürfen nur zu diesem Zweck genutzt werden.

25.2 Gesichtserkennung bei der Spielbank

Die Spielbank Hamburg beabsichtigt, ein biometrisches Gesichtserkennungsverfahren für Zugangskontrollen einzusetzen.

Bereits im 18. Tätigkeitsbericht wurde unter 1.3 ausführlich dargestellt, welche datenschutzrechtlichen Anforderungen wir an die Ausgestaltung und den Einsatz biometrischer Systeme stellen. Erstmals hatten wir jetzt konkret zu beurteilen, ob ein biometrisches Verfahren den datenschutzrechtlichen Anforderungen entspricht.

Im Januar 2003 erfuhren wir von der Absicht der Spielbank Hamburg, Zugangskontrollen über den Einsatz eines biometrischen Gesichtserkennungsverfahrens abzusichern.

Das Verfahren soll nach den Vorstellungen der Spielbank ausschließlich dem Zweck dienen, Spielsüchtige auszuschließen, die sich selbst haben sperren lassen. Bei Personen, die auf eigenen Wunsch und daher auf freiwilliger Basis von sich sog. Referenzdaten fertigen lassen, kann im Falle des Eintritts der zugehörigen Person in die Räume der Spielbank dann ein Abgleich vorgenommen und der Zugang verweigert werden.

Über die Frage, ob überhaupt eine Speicherung erfolgen soll und ggf. über die Speicherdauer ist gegenwärtig noch nicht entschieden worden.

Datenschutzrechtlich ist die vorgesehene biometrische Gesichtserkennung, die mit einer Videoüberwachung in Zusammenhang steht, nach unserer Auffassung als Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen nach § 6 b BDSG einzustufen. Insbesondere sind die aufgenommenen Daten im Gegensatz zu der von der Spielbank vertretenen Auffassung als personenbezogene Daten anzusehen. Biometrische Verfahren sind nämlich geradezu darauf ausgerichtet, auf eine Person zugeschnittene unverwechselbare Merkmale festzuhalten. Dies soll im Falle von Gesichtserkennung – sofern das Verfahren ordnungsgemäß funktioniert – sehr viel einfacher und eindeutiger möglich sein, als z. B. bei einer Kontonummer, Videoaufnahme oder einfachen Fotografie, deren Personenbezug nicht in Zweifel gezogen wird.

Der Einsatz des Verfahrens ist jedoch nur dann möglich, wenn es zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Soweit die Spielbank vorgetragen hat, das Verfahren zum Selbstschutz der Spielsüchtigen einzusetzen, kann wohl von der Wahr-

nehmung berechtigter Interessen ausgegangen werden, obwohl es sich offensichtlich um wenige Personen handelt.

Datenschutzrechtliche Zweifel ergeben sich aber schon bei der Erforderlichkeit des Einsatzes eines solch weit reichenden Verfahrens, weil andere Möglichkeiten der Zugangssicherung – wie etwa eine Kontrolle der Ausweise – denkbar sind. Die Spielbank hat zugesichert, sich zu diesem Punkt noch konkret zu äußern. Darüber hinaus dürfen keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. An dieser Stelle ist anzumerken, dass die weit überwiegende Anzahl der Spielbankbesucher keine Sperre hat und gleichwohl eine entsprechende Überprüfung hinnehmen müsste. Dies ist insbesondere deswegen als kritisch einzustufen, weil es sich bei der biometrischen Gesichtserkennung um die Erhebung unverwechselbarer Merkmale handelt, die bei jeder Person, wie auch z. B. der Fingerabdruck, individuell ausgeprägt sind. Gerade im Falle der noch nicht eindeutig nachgewiesenen Erforderlichkeit des Einsatzes des Verfahrens zu den vorgesehenen Zwecken muss von überwiegenden entgegen stehenden Interessen der Betroffenen ausgegangen werden.

Sollte die Erforderlichkeit seitens der Spielbank noch nachgewiesen werden, wird im Zusammenhang mit den schutzwürdigen Interessen der Betroffenen über die Frage zu diskutieren sein, ob neben der Erhebung der Daten zum Abgleich mit den Referenzdaten überhaupt eine darüber hinausgehende Speicherung notwendig ist.

Die kritische datenschutzrechtliche Einschätzung der biometrischen Gesichtserkennung wird durch eine neue praxisnahe Studie des Bundesamtes für Sicherheit und Informationstechnik (BSI) unterstützt. Das BSI hat verschiedene Gesichtserkennungssysteme getestet und dabei festgestellt, dass die Erkennungsleistung der Systeme unter 50% lag, in einigen Fällen sogar fast keine Testpersonen erkannt wurden. Unter diesen Umständen muss im konkreten Fall im Rahmen der Prüfung der Verhältnismäßigkeit noch untersucht werden, ob das in Aussicht genommene System überhaupt geeignet ist, die versprochene Leistung zu erbringen. Anderenfalls bestünde die Gefahr, dass neben der Nichterkennung der Referenzpersonen auch unzutreffende Meldungen bei nicht erfassten Personen entstünden, die ihren schutzwürdigen Interessen zuwiderliefen.

Da bei dem Einsatz biometrischer Zugangserkennungsverfahren datenschutzrechtliche Fragen von grundsätzlicher Bedeutung vorliegen, wurde die Angelegenheit mit den übrigen Obersten Aufsichtsbehörden der Länder im Düsseldorfer Kreis erörtert. Das Ergebnis wird Grundlage weiterer Gespräche mit der Spielbank sein.

26. Bußgeldfälle

Im Berichtszeitraum wurden insgesamt 9 Bußgeldverfahren eingeleitet.

Neben der Verhängung von Bußgeldern wegen Nichterteilung einer Auskunft auf Verlangen der Aufsichtsbehörde wurde in zwei Fällen ein Bußgeld wegen nicht ordnungsgemäßer Vernichtung von personenbezogenen Daten verhängt. Ein ehemaliger Gesellschafter hatte nach Auflösung einer Finanzberatungsgesellschaft Kreditunterlagen mit personenbezogenen Daten in unverschlossenen Müllsäcken an die Straße gestellt. Die darin befindlichen Unterlagen wurden auf den Bürgersteig und die umliegenden Vorgärten verteilt. Der Bußgeldbescheid ist rechtskräftig. Die Entsorgung von Versicherungsanträgen und dazugehörigen Unterlagen durch einen Versicherungsvermittler in einem frei zugänglichen Papiercontainer führte ebenfalls zum Erlass eines Bußgeldes.

Ein Bußgeld wurde gegen den Mitarbeiter einer Aus- und Fortbildungseinrichtung verhängt. Er hatte an eine Fernsehredaktion hoch sensible Informationen aus psychologischen Vorgesprächen mit einem Fortzubildenden weitergegeben. Dies begründete er damit, dass er sich gegen unzutreffende Behauptungen des Fortzubildenden zum Schutz der Aus- und Fortbildungseinrichtung wehren wollte. Er erschütterte aber gezielt die Glaubwürdigkeit des Fortzubildenden durch die Übermittlung von gesundheitlichen und sehr persönlichen Informationen, obwohl zuvor die Vertraulichkeit des Gesprächs zugesichert worden war. Der Bußgeldbescheid ist rechtskräftig.

27. Meldepflicht und Prüftätigkeit

27.1 Meldepflicht und Register nach § 4 d BDSG

Die Zahl der Meldungen ist deutlich gestiegen.

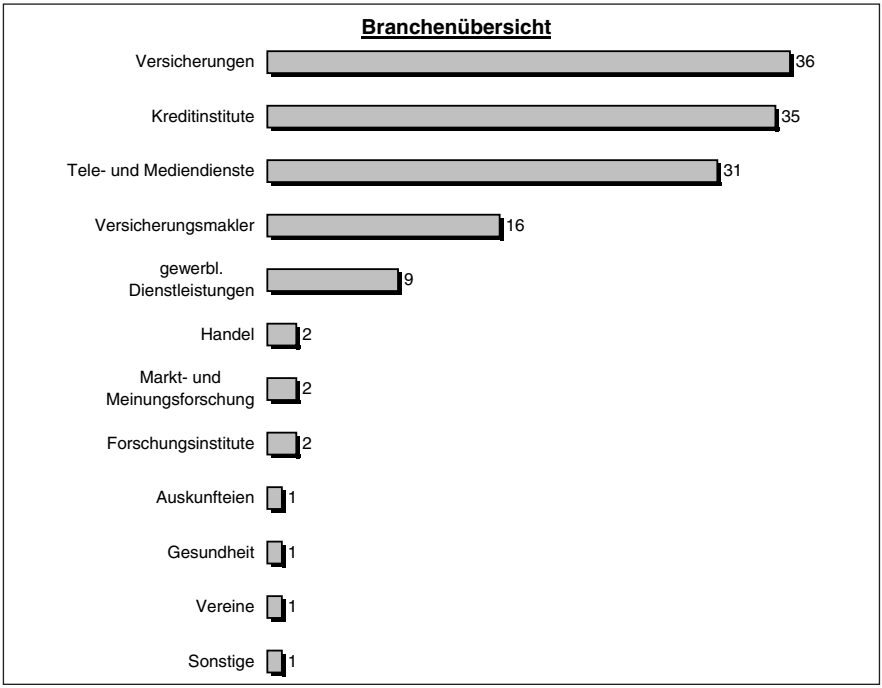
Die Aufsichtsbehörde führt nach § 38 Abs. 2 BDSG ein Register der Stellen, die nach § 4 d BDSG der Meldepflicht unterliegen. Bisher haben 30 Unternehmen ihre Angaben zur Meldepflicht entsprechend den Vorgaben des § 4 e BDSG angepasst oder sich zum ersten Mal zum Register gemeldet (vgl. 18. TB, 29.1). Unterteilt nach der Art der meldepflichtigen Verfahren ergibt sich folgendes Bild:

• Speicherung zum Zwecke der Übermittlung	
Auskunfteien/Warndienste	8
Informationsdienste	3
Adresshändler	1
• Speicherung zum Zwecke der anonymisierten Übermittlung	
Markt- und Meinungsforschung	18

27.2 Prüfungen

Die Prüfungen von nicht öffentlichen Stellen sind erheblich ausgeweitet worden.

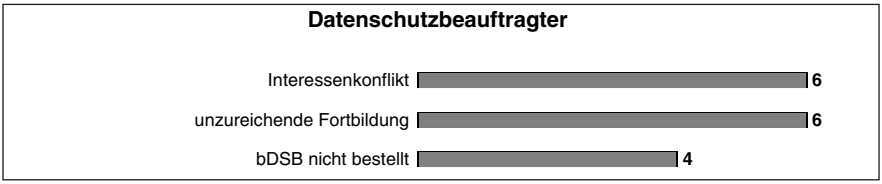
Die neue Regelung der anlassfreien datenschutzrechtlichen Kontrolle von nicht öffentlichen Stellen ermöglicht eine umfangreichere Datenschutzaufsicht als bisher. Schwerpunkte der Prüfungen im Berichtszeitraum bildeten die Kundendatenverarbeitung und die Einhaltung der Anforderungen bei Tele- und Mediendiensten. Insgesamt wurden 137 Unternehmen geprüft.

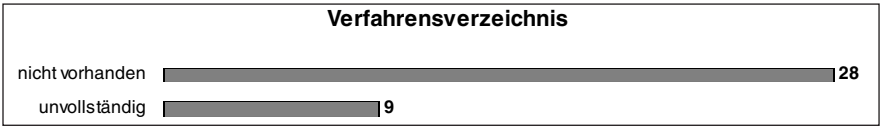


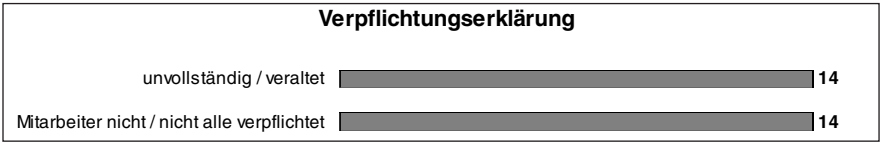
Gegenstand der Prüfungen war, außer bei Tele- und Mediendiensten:

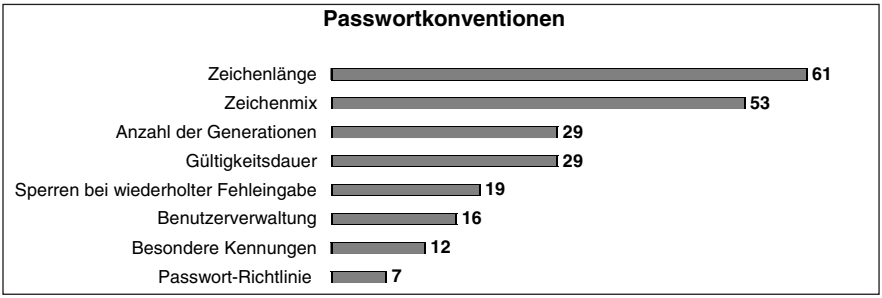
- die Verpflichtung zur Bestellung eines Datenschutzbeauftragten nach § 4 f BDSG und seine Fachkunde nach § 4 g Abs. 1 BDSG,
- das Verfahrensverzeichnis nach § 4 g Abs. 2 BDSG,
- die Verpflichtung auf das Datengeheimnis nach § 5 BDSG,
- die technischen und organisatorischen Maßnahmen nach § 9 BDSG,
- die Auftragsdatenverarbeitung nach § 11 BDSG,
- die Meldepflicht nach § 4 d BDSG.

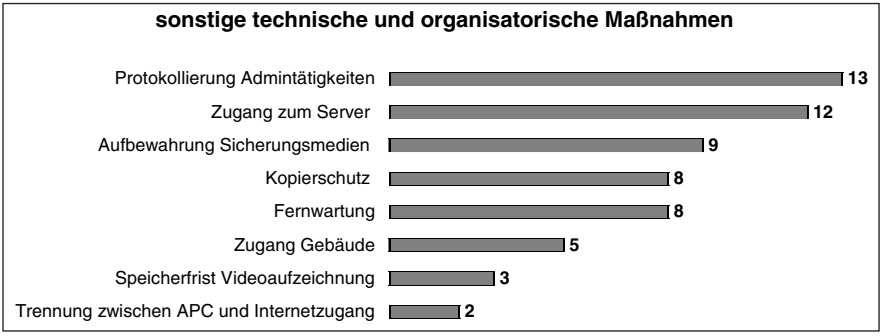
Nur bei 3 Firmen hat die Aufsichtsbehörde keine Forderungen erhoben. Im Folgenden sind die überprüften Themenbereiche mit ihren wesentlichsten Mängeln dargestellt.

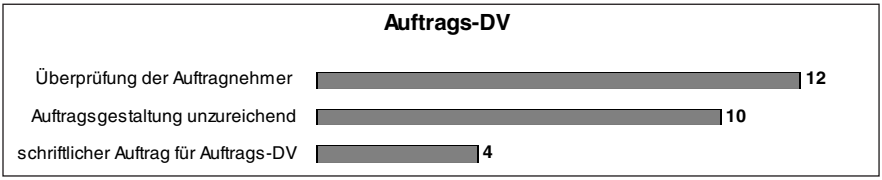

Datenschutzbeauftragter
Interessenkonflikt 6
unzureichende Fortbildung 6
bDSB nicht bestellt 4


Verfahrensverzeichnis
nicht vorhanden 28
unvollständig 9


Verpflichtungserklärung
unvollständig / veraltet 14
Mitarbeiter nicht / nicht alle verpflichtet 14


Passwortkonventionen
Zeichenlänge 61
Zeichenmix 53
Anzahl der Generationen 29
Gültigkeitsdauer 29
Sperren bei wiederholter Fehleingabe 19
Benutzerverwaltung 16
Besondere Kennungen 12
Passwort-Richtlinie 7


sonstige technische und organisatorische Maßnahmen
Protokollierung Admintätigkeiten 13
Zugang zum Server 12
Aufbewahrung Sicherungsmedien 9
Kopierschutz 8
Fernwartung 8
Zugang Gebäude 5
Speicherfrist Videoaufzeichnung 3
Trennung zwischen APC und Internetzugang 2


Auftrags-DV
Überprüfung der Auftragnehmer 12
Auftragsgestaltung unzureichend 10
schriftlicher Auftrag für Auftrags-DV 4

Prüfungen bei Anbietern von Tele- und Mediendiensten haben ergeben, dass in vielen Fällen Datenschutzvorschriften nicht eingehalten werden. Der Einsatz des Online-Prüftools OPTuM ermöglicht die automatisierte Analyse folgender Aspekte eines Internet-Angebots:

- Unterrichtung des Nutzers über den Datenschutz,
- Verwendung von Cookies,
- Automatische Weitervermittlungen zu Angeboten Dritter,
- Veröffentlichung personenbezogener Daten im Internet,
- Erhebung von Daten mittels Formularen.

Die dabei festgestellten Datenschutzmängel betrafen unter anderem schlecht auffindbare oder inhaltlich unzulängliche Datenschutzinformationen, die Verwendung von Cookies mit sehr langer Gültigkeitsdauer und die automatische Weitervermittlung mittels versteckter Elemente (sog. Web-Bugs).

Weitere Prüfungen haben ergeben, dass die Provider in der Mehrzahl der Fälle erheblich mehr personenbezogene Nutzungsdaten speichern, als es das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag erlauben.

Bürgerservice und die Dienststelle

28. Unterstützung der Bürgerinnen und Bürger

Die weiterhin hohe Zahl der Eingaben und der gute Besuch der Datenschutzveranstaltungen unterstreichen das Interesse am Schutz der personenbezogenen Daten. Unsere Informationsangebote wurden wieder intensiv in Anspruch genommen.

Im Jahr 2002 betrug die Zahl der schriftlichen Eingaben 562 und im Jahr 2003 insgesamt 542. Wie in den Vorjahren haben wir auch die Zahl der persönlichen, telefonischen und schriftlichen Beratungen der Bürgerinnen und Bürger festgehalten. Demnach haben wir die Bürger im Jahr 2002 in rund 1.800 Fällen beraten und im Jahr 2003 in über 1.400 Fällen.

Die Beratungen für öffentliche und nicht öffentliche Stellen, die letztlich wiederum den Bürgern zu Gute kommen, beliefen sich im Jahr 2002 auf über 1.700 Fälle und im Jahr 2003 auf rund 1.300 Fälle. Außerdem prüften wir im Jahr 2002 in über 210 Fällen und im Jahr 2003 in rund 420 Fällen öffentliche und nicht öffentliche Stellen. In rund 100 Fällen im Jahr 2002 und im Jahr 2003 gaben wir Stellungnahmen zu Datenschutzfragen hinsichtlich Rechts- oder Verwaltungsvorschriften ab.

28.1 Eingaben

Anhand der jahresweise erfassten Zahl der Eingaben zeigte sich der weiterhin hohe Stand der Fälle, in denen sich die Bürgerinnen und Bürger schriftlich an

uns wenden. Von Anfang Dezember 2001 bis Ende November 2003 gingen 1.104 Eingaben ein. Sie betrafen – getrennt für die Jahre 2002 und 2003 – folgende Datenschutzbereiche:

	2002	**2003**
Versicherungswirtschaft	22	21
Kreditwirtschaft	25	21
private Wohnungswirtschaft	9	15
Versandhandel	8	10
sonst. Handel	17	20
Werbung, Direktmarketing	103	80
Schufa, Auskunfteien	42	53
Markt- und Meinungsforschung	1	2
Vereine	9	11
freie Berufe	2	29
Soziales und Gesundheitswesen, nichtöffentlich	14	19
Personaldatenschutz, nichtöffentlich	28	21
Verkehrswesen, nichtöffentlich	14	2
Sonstiges, nichtöffentlich	24	25
Justiz	9	10
Strafvollzug	13	11
Sicherheitsüberprüfung	2	-
Verfassungsschutz	5	5
Polizei	21	24
Staatsanwaltschaft	10	13
Meldewesen	8	24
MDK, Kranken- und Pflegekassen	10	7
andere Sozialbereiche	19	24
Gesundheitswesen, öffentlich	16	6
Personaldatenschutz, öffentlich	18	9
Verkehrswesen, öffentlich	11	19
Ausländerwesen	4	4
Finanz-, Steuerwesen	9	8
Bildungswesen	14	7
Wirtschaftsverwaltung	-	2
Telekommunikation	11	11
Teledienste	87	43
Medien	3	6
Personenstandswesen	-	5
Statistik	1	1
Bau-, Vermessungswesen	2	4
Hochschulen	3	-
Umweltschutz	1	-
Sonstiges, öffentlich	14	10

28.2 Veranstaltungen

Die von mir mitgegründete Hamburger Datenschutzgesellschaft (HDG) hat jeweils wieder im Frühjahr 2002 und auch 2003 Veranstaltungen zusammen mit der Handelskammer Hamburg durchgeführt. Ende Mai 2002 fand ein Forum über „Elektronische Kontrollen in der Wirtschaft – Biometrie, Internet und Email“ statt; Ende Mai 2003 wurde das Thema „Wirtschaft als Datenspeicher für den Staat ? – Anforderungen der Sicherheitsbehörden und Pflichten der Unternehmen“ behandelt.

Auf den schon traditionellen Herbstveranstaltungen im Warburg-Haus war der Vortrag des Vizepräsidenten des Bundesverfassungsgerichtes, Prof. Hassemer, Ende Oktober 2002 über „Einige Thesen zur Selbstbestimmung im dritten Jahrtausend“ stark besucht. In dieser Reihe der Veranstaltungen sprach Ende Oktober 2003 der Berliner Beauftragte für Datenschutz und Informationsfreiheit, Prof. Dr. Garstka, über „Die Novellierung des Bundesdatenschutzgesetzes – Stand der Diskussion“ und damit über die Schwerpunkte der zweiten Stufe der Novellierung nach der Anpassung an die Europäische Datenschutzrichtlinie.

28.3 Öffentlichkeitsarbeit

Unsere Broschüren, Faltblätter usw. zu über 20 Themengebieten, die am Ende dieses Berichts wiedergegeben sind, wurden wieder in großem Umfang verbreitet. Dazu gehörten im Jahr 2002 die Schrift „Datenschutz bei Windows 2000“ – mit rund 31.000 Abrufen im Monat nach der Veröffentlichung in unserem Internetangebot – sowie die neuen Informationen zum Datenschutz in Vereinen und bei Handels- und Wirtschaftsauskunfteien (siehe auch 21.4). Spitzenreiter im gesamten hamburgischen Angebot im Internet war Anfang des Jahres 2002 unsere aktualisierte „Orientierungshilfe Tele- und Mediendienste“. Ebenfalls nur im Internet verbreiteten wir im September 2002 ein neues Merkblatt „Schulen ans Netz mit Sicherheit“ für Schulleitungen, Lehrerinnen und Lehrer, Schülerinnen und Schüler sowie deren Eltern.

Anfang 2003 folgte als Service-Angebot der Datenschutzbeauftragten des Bundes und der Länder eine gemeinsame Broschüre „Datenschutzgerechtes eGovernment“ mit Handlungsempfehlungen für die jeweils Verantwortlichen in der Verwaltung und auch für die Bürgerinnen und Bürger sowie interessierte Wirtschaftsunternehmen. Im März 2003 wurden die aktualisierten „Tipps und Informationen zu Adressenhandel und unerwünschter Werbung“ veröffentlicht; zu diesem Themenbereich gibt es immer noch die meisten Eingaben der Bürgerinnen und Bürger.

Zur Öffentlichkeitsarbeit gehören auch unsere Vorträge und Beiträge für Veröffentlichungen. Wir äußerten uns auf diesem Wege im Jahr 2002 rund 65 mal

und im Jahr 2003 rund 20 mal zu Datenschutzfragen. Besonders wichtig für die Verbreitung unserer Anliegen sind die Kontakte zu den Medien, also Interviews, Beantwortung der Fragen von Journalisten usw.. Auf diese Weise hatten wir im Jahr 2002 rund 180 Medienkontakte und im Jahre 2003 rund 120 Medienkontakte.

29. Entwicklung der Dienststelle

Die Dienststelle hat die Gesamtzahl von 20 Mitarbeiterinnen und Mitarbeitern erreicht.

Eine Finanzierung neuer Stellen aus dem Haushalt kam bei der schwierigen Gesamtlage nicht mehr in Betracht. Dennoch wurde es auf unterschiedliche Weise ermöglicht, dass die Gesamtzahl der Mitarbeiterinnen und Mitarbeiter auf 20 stieg, darunter viele Teilzeitbeschäftigte. Die Stellenzahl betrug insgesamt 16,63.

Der Senat beabsichtigt gemäß Beschluss vom Juni 2003, den Stellenbestand beim Hamburgischen Datenschutzbeauftragten zum Januar 2005 um rund 10 % zu reduzieren. Der Hamburgische Datenschutzbeauftragte hat daraufhin der Justizbehörde mitgeteilt, dass der gemäß § 22 Hamburgisches Datenschutzgesetz (HmbDSG) notwendige Personalbestand mit der jetzigen Stellenzahl durch die Beschlüsse des Senats über die Personalverstärkung im Haushaltsjahr 2001 nachgewiesen und eine Aufgabenreduzierung inzwischen auf keinen Fall eingetreten ist. Infolge dessen verbleibt allenfalls die Möglichkeit einer Umstrukturierung der Dienststelle mit teilweiser Absenkung der Besoldungsgruppen oder besser eine überwiegende Finanzierung der Stellen bei der Aufsichtsbehörde durch eine Umlage der Wirtschaft ähnlich wie in vergleichbaren Fällen beim Bund und in Hamburg.

Der langjährige Vertreter des Hamburgischen Datenschutzbeauftragten, Peter Schaar, ist am 14. November 2003 vom Bundestag zum Bundesdatenschutzbeauftragten gewählt worden. Damit ist nach Prof. Bull zum zweiten Mal ein Hamburger in dieses verantwortungsvolle Amt berufen worden.

Der bisherige Hamburgische Datenschutzbeauftragte Dr. Hans-Hermann Schrader, dessen zweite und letzte Amtszeit bei rechtzeitiger Bestellung seines Nachfolgers am 5. März 2003 beendet gewesen wäre, führte das Amt weiter. Bei Redaktionsschluss dieses Berichts am 3. Dezember 2003 und damit nach 9 Monaten war eine Nachfolgeentscheidung weiterhin nicht abzusehen. Da die Amtszeit gemäß § 21 Abs. 3 HmbDSG bis zur Bestellung eines Nachfolgers ohne weiteres kraft Gesetzes als verlängert gilt, ist das Amt – auch und gerade in dieser Situation – mit allen Rechten und Pflichten uneingeschränkt weiterzuführen.

Geschäftsverteilung (Stand: 1. Dezember 2003)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg
E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.hamburg.datenschutz.de

Tel: 040/42841 – 2044
Fax: 040/42841 – 2372

		Durchwahl
Dienststellenleiter:	Dr. Hans-Hermann Schrader	– 2044 –
Stellvertreter:	Dr. Hans-Joachim Menzel	– 2558 –
Vorzimmer:	Heidi Niemann	– 2045 –
Verwaltungsangelegenheiten der Dienststelle:	Rolf Nentwig	– 2563 –
Informationsmaterial:	Irene Heinsohn	– 2047 –
	Heidi Niemann	– 2045 –

Grundsatzfragen des Datenschutz- und Informationszugangsrechts, Datenschutzgesetze, Parlamentsangelegenheiten, Justiz, Strafvollzug, Verfassungsschutz, Sicherheitsüberprüfungen, Meldewesen, Wahlen und Volksabstimmungen, Ausweis- und Paßangelegenheiten, Archivwesen:
Dr. Harald Wollweber – 2046 –

Polizei, Feuerwehr, Staatsanwaltschaft, Straßenverkehrsverwaltung, Verkehrsordnungswidrigkeiten, Gewerbeaufsicht, Wirtschaftsverwaltung:
Herbert Janßen – 2581 –

Bauen, Wohnen, Vermessungswesen, Personenstandswesen, Umwelt, Statistik, Finanz-, Steuer- und Rechnungswesen:
Gunnar Hansen – 2223–

Gesundheitswesen, Forschung, Kultur, Telekommunikations-, Rundfunk- und Presserecht, Ausländerwesen:
Dr. Hans-Joachim Menzel – 2558–

Soziales, Bildungswesen, Allgemeine Bezirksangelegenheiten, Kirchen:

Detlef Malessa – 2089–

Betriebssysteme, Netzwerke, Verschlüsselungstechniken, Signatur, SAP, IuK-Beauftragter, technisch-organisatorische Beratung und Prüfung:

N.N. – 1760 –

Landesamt für Informationstechnik (LIT), Elektronischer Rechtsverkehr, IuK-Leitung, IuK-Planung, technisch-organisatorische Beratung und Prüfung:

Dietmar Nadler – 2236 –

DV-Verfahren der Dienststelle, Systemadministration, Internetangebot:

Martin Schemm – 2063 –

Betriebssysteme, Netzwerke, Chipkarten, E-Government, technisch-organisatorische Beratung und Prüfung:

Dr. Sebastian Wirth – 1769 –

Tele- und Mediendienste, Internet-Dienste, Biometrie, technisch-organisatorische Beratung und Prüfung:

Ulrich Kühn – 2564 –

Standard-Software und Dokumentenmanagement/Archivierung, Vertretung IuK-Leitung/Iuk-Planung, technisch-organisatorische Beratung und Prüfung:

Jutta Nadler – 1373 –

Internationaler Datenverkehr, Auskunfteien/SCHUFA, Freie Berufe, Gewerbliche Dienstleistungen:

Helga Naujok – 2556 –

Versicherungswirtschaft, Handel, Industrie, Vereine, Kreditwirtschaft:

Elisabeth Duhr – 2541 –

Werbung/Adresshandel, Markt- und Meinungsforschung, Personaldatenschutz:

Evelyn Seiffert – 2468 –

Transport und Verkehr, Prüfungen:

Bernd Uderstadt – 2276 –

Stichwortverzeichnis

Veröffentlichungen zum Datenschutz

Beim Hamburgischen Datenschutzbeauftragten können derzeit folgende Veröffentlichungen kostenlos abgeholt werden oder per Post gegen Einsendung von Briefmarken im Wert von 0,77 € angefordert werden:

Broschüren

Hamburgisches Datenschutzrecht 2001

Datenschutz in der Arztpraxis

Datenschutz bei Windows NT

Datencheckheft, 6. Auflage

Mehr Service – weniger Datenschutz

Vom Bürgerbüro zum Internet

Windows 2000

Datenschutzgerechtes eGovernment

Informationsblätter

Was tun wir für Sie ?

Tipps und Informationen zu Adressenhandel und unerwünschter Werbung

Datenschutz im privaten Bereich

Handels- und Wirtschaftsauskunfteien

Datenschutz und Verbraucherschutz rund ums Telefon

Virtuelles Datenschutzbüro

Surfen, Klicken und Bestellen, Datenschutz und Verbraucherschutz im Internet

Datenschutz im Verein

Internet

Informationen und Veröffentlichungen des Hamburgischen Datenschutzbeauftragten können auch im Internet unter – www.hamburg.datenschutz.de – abgerufen werden.

Verlagsveröffentlichungen

Schrader, Datenschutzrecht, in Hoffmann-Riem, Koch (Hrsg.) Hamburgisches Staats- und Verwaltungsrecht, Nomos Verlag, 1998

Bäumler, Breinlinger, Schrader (Hrsg.) Datenschutz von A - Z, Loseblattwerk, Luchterhand Verlag, 1999

Schaar, Kommentierungen zum TDDSG und MDStV, in Roßnagel (Hrsg.) Recht der Multimediadienste, 2000

Schaar, Die Möglichkeiten der Datenschutzaufsichtsbehörden, in Bäumler (Hrsg.) E-Privacy, Vieweg-Verlag, 2000

Schaar, Datenschutz im Internet, Beck-Verlag, 2002

Duhr, Datenschutz in Auskunfteien, in Roßnagel (Hrsg.) Handbuch Datenschutzrecht, Beck-Verlag, 2003

Naujok, Datenschutz bei Versicherungen, in Roßnagel (Hrsg.) Handbuch Datenschutzrecht, Beck-Verlag, 2003