**BÜRGERSCHAFT
DER FREIEN UND HANSESTADT HAMBURG**

Drucksache 17/2294

17. Wahlperiode

20. 02. 03

Der Hamburgische Datenschutzbeauftragte

**An die
Frau Präsidentin der Bürgerschaft**

Betr.: Bericht 2002 des Hamburgischen Datenschutzbeauftragten

Gemäß § 23 Absatz 3 Satz 3 Hamburgisches Datenschutzgesetz übersende ich der Bürgerschaft den Bericht 2002 mit kurzer Darstellung der wesentlichen Punkte des letzten Jahres.*

Dem Senat leite ich den Bericht 2002 gleichzeitig zu.

Dr. Schrader

* Verteilt nur an die Abgeordneten der Bürgerschaft.

Bürgerschaftsdrucksachen – außer Senatsvorlagen – sind – gedruckt auf chlorfrei gebleichtem Papier – zu beziehen bei:
Druckerei Wartenberg & Söhne GmbH, Theodorstraße 41 w, 22761 Hamburg, Telefon 89 97 90 - 0

Der Hamburgische Datenschutzbeauftragte

Bericht 2002

Bericht
2002

vorgelegt im Februar 2003
(Redaktionsschluss: 4. Dezember 2002)

Dr. Hans-Hermann Schrader

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

Herausgegeben vom Hamburgischen Datenschutzbeauftragten
Baumwall 7 · 20459 Hamburg · Tel.: 4 28 41 20 47 · Telefax: 4 28 41 23 72
Auflage: 1.700 Exemplare

Druck: Lütcke & Wulff, 22525 Hamburg

INHALTSVERZEICHNIS

Datenschutz im öffentlichen Bereich

Datenschutz im nichtöffentlichen Bereich

1. Vorbemerkung

Nach 12 Jahren als Hamburgischer Datenschutzbeauftragter endet meine zweite und letzte Amtszeit am 5. März 2003 mit der gesetzlichen Maßgabe, dass ich das Amt bis zur Bestellung einer Nachfolgerin oder eines Nachfolgers weiter zu führen habe. Demgemäß lege ich diesen „Bericht 2002“ als letzten Bericht während meiner Amtszeit vor. Der Bericht gibt wiederum – zwischen den ausführlicheren zweijährlichen Tätigkeitsberichten – die wesentlichen Punkte zu aktuellen Themen wieder.

Eine effektive Arbeit für die Bürgerinnen und Bürger wurde mir auch dadurch ermöglicht, dass sich die personelle Verstärkung der Dienststelle für die Daueraufsicht über die Wirtschaft inzwischen deutlich auswirkt. Mit der automatischen Prüfung von Internetangeboten durch ein entsprechendes Programm-Tool sind wir außerdem neue Wege bei einer bereits beträchtlichen Zahl von Prüfungen gegangen.

Den Mitarbeiterinnen und Mitarbeitern möchte ich bei dieser Gelegenheit für ihre kompetente und engagierte Tätigkeit danken. Wesentlich unterstützt wurde ich von meinem Stellvertreter, Herrn Schaar, der ab November 2002 (wie schon früher ein anderer Mitarbeiter) aus der Dienststelle in die freiberufliche Tätigkeit mit einer neu gegründeten Datenschutz GmbH gewechselt ist.

Im Sinne meines Vorwortes zu Beginn meiner zweiten Amtszeit (16. Tätigkeitsbericht 1997) liegt mir weiterhin daran, dass die Bürgerinnen und Bürger sich um ihr Grundrecht auf Datenschutz zunehmend auch selbst kümmern. Dazu haben wir vielfältig Hilfe zur Selbsthilfe geleistet gemäß dem Motto zuletzt auf der Rückseite des „Berichts 2000“: Selbst ist der Bürger – wir helfen ihm gern.

Dass es zur Selbstbestimmung der Menschen auf ihr Selbst-Bewusstsein ankommt, hat der Hamburger Dichter Paul Fleming schon vor fast 400 Jahren in den harten Zeiten des Dreißigjährigen Krieges in seinem Gedicht „An Sich“ beschrieben, das auf der Rückseite dieses Berichts wiedergegeben ist. In unserer Zeit des Terrorismus mit den vielfältigen Einschränkungen der Bürgerfreiheit ist dies ein bedenkenswerter Ansporn, an der Selbstbestimmung mit Energie und Ausdauer festzuhalten.

2. Aktuelle Situation

2.1 Datenschutzrechtliche Entwicklung

Das Terrorismusbekämpfungsgesetz von Anfang 2002 hat zu weitreichenden Einschränkungen der Freiheitsrechte geführt. Mit weiteren Rechtsänderungen wurde unseren Anliegen ganz oder teilweise entsprochen.

Die absehbaren Auswirkungen des Terrorismusbekämpfungsgesetzes vom 9. Januar 2002 sind bereits im 18. Tätigkeitsbericht (18. TB) nach den

grundsätzlichen Hinweisen in der dortigen Einleitung (S. 2f.) bei den jeweiligen Themen näher behandelt worden. Landesrechtlich war die Umsetzung des Terrorismusbekämpfungsgesetzes mit dem „Entwurf eines Gesetzes zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzes“ vom 10. September 2002 besonders umstritten. Im Vordergrund stand dabei das Vorhaben, erstmals dem Verfassungsschutz in Hamburg die verdeckte akustische und optische Überwachung in Wohnungen zu erlauben (Großer Lauschangriff). Die damit geplanten Eingriffe selbst in die Vertrauensverhältnisse zu Berufsgeheimnisträgern wie Ärzten, Rechtsanwälten und Journalisten konnten auf unsere Initiative schließlich weitgehend verhindert werden (siehe in diesem Bericht unter 7.).

Am 4. Juni 2002 wurde die früher fehlende ausdrückliche gesetzliche Verordnungsermächtigung für diejenigen Regelungen geschaffen, die in der Verordnung des Senats vom 11. September 2001 den Inhalt des Rechenschaftsberichts der Volksinitiatoren betreffen. Die Bürgerschaft folgte damit einstimmig unserer Anregung (vgl. 18. TB, 4.1.1).

Durch die Verordnung über den elektronischen Rechtsverkehr in gerichtlichen Verfahren vom 9. April 2002 hat der Senat die Erfordernisse für elektronische Dokumente, insbesondere hinsichtlich Signatur, Vertraulichkeit und Format, festgelegt.

Für Sicherheitsüberprüfungen ohne Mitwirkung des Landesamtes für Verfassungsschutz (LfV) fehlt nach wie vor die erforderliche Rechtsverordnung des Senats. Wesentliche Ursache der Verzögerung sind Auffassungsunterschiede zum Umfang dieser Sicherheitsüberprüfungen im Bereich der Informations- und Kommunikationstechnik. Die Forderung der Finanzbehörde, über die Systemadministration hinaus alle Arbeitsplätze und Funktionen im IuK-Bereich einzubeziehen, halten wir für unverhältnismäßig und mit der Intention des Hamburgischen Sicherheitsüberprüfungsgesetzes nicht vereinbar.

Im nicht öffentlichen Bereich war die Arbeit dadurch geprägt, für eine wirksame Umsetzung des novellierten Bundesdatenschutzgesetzes gemäß der EG-Datenschutzrichtlinie zu sorgen (vgl. 18. TB, 2.1.2). 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) beigetragen. Ihre Erläuterungen für die weiteren Abschnitte des BDSG zum Datenschutz im nicht öffentlichen Bereich werden in DuD 2003, Heft 1 veröffentlicht.

2.2 Zusammenarbeit mit den Behörden

Die Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten vom 12. November 1992 ist nach wie vor von den hamburgischen öffentlichen Stellen einzuhalten.

Der Senat hat in seiner Mitteilung an die Bürgerschaft vom 24./25. Juni 2002 (Drucksache 17/1091) bekräftigt, dass durch rechtliche Regelungen des Datenschutzes und der Datensicherheit „Rahmenbedingungen für die ... Datenverarbeitung in der öffentlichen Verwaltung gesetzt“ sind, die „strikt zu beachten“ sind. Die Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten besagt dazu, dass er bei sämtlichen „von einem Vorgang berührten Belangen des Datenschutzes im Zusammenhang mit der Verarbeitung personenbezogener Daten“ zu beteiligen ist (siehe 2.2 der Richtlinie).

Im zweiten Halbjahr 2002 haben sich aber die Fälle gehäuft, in denen diese Beteiligungspflicht der hamburgischen öffentlichen Stellen nicht eingehalten wurde. Beispiele sind dafür die fehlende Behördenabstimmung der Senatsdrucksachen

- Einführung des „Kita-Gutschein-Systems“ in Hamburg (Behörde für Bildung und Sport)
- „Geschlossene Unterbringung für Minderjährige bei Kindeswohlgefährdung anlässlich der Begehung schwerer Straftaten in gravierenden und/oder wiederholten Fällen und Maßnahmen der Jugendhilfe zur Stärkung der Erziehungsverantwortung der Eltern“ (Behörde für Soziales und Familie)
- „Umsetzung des Gesetzes über eine bedarfsorientierte Grundsicherung im Alter bei Erwerbsminderung, Grundsicherungsgesetz“ (Behörde für Soziales und Familie)
- „Konzept zur Bekämpfung der Korruption in Hamburg“ (Behörde für Inneres)
- Aktenvorlageersuchen der Bürgerschaft zu den Mehrkosten für die Justizvollzugsanstalt Billwerder (Justizbehörde).

In diesen Fällen handelt es sich eindeutig um Angelegenheiten mit Datenschutzrelevanz. Gerade die Behördenabstimmung von Senatsdrucksachen gehört zum Kernbereich der Fälle im Sinne der Richtlinie zur Beteiligung des Hamburgischen Datenschutzbeauftragten. Dort heißt es im ersten Spiegelstrich, dass der Datenschutzbeauftragte jeweils „am Abstimmungsverfahren über Senatsdrucksachen zu beteiligen (ist), soweit Belange des Datenschutzes berührt werden.“

In diesem Zusammenhang ist außerdem zu berücksichtigen, dass nach der Geschäftsordnung des Senats streitig gebliebene Punkte in die Senatsdrucksache aufzunehmen sind. Dies ist z. B. bei der Senatsdrucksache „Entwurf eines Gesetzes zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzes“ durch die Behörde für Inneres nicht geschehen. Die Senatsdrucksache enthält außer dem Satz, dass der Hamburgische Datenschutzbeauftragte beteiligt worden ist, keinerlei Hinweis auf die

verschiedenen ausdrücklichen Änderungsvorschläge in unserer Stellungnahme im Rahmen der Behördenabstimmung. Infolge dessen ist dem Senat auch die Meinungsverschiedenheit z.B. über die Berücksichtigung der Vertrauensverhältnisse zu Ärzten, Rechtsanwälten, Journalisten und anderen Berufsgeheimnisträgern nicht schon zur Senatsberatung, sondern erst durch unsere spätere Presseerklärung zur Mitteilung des Senats an die Bürgerschaft bekannt geworden (siehe in diesem Bericht unter 7.).

Schließlich ist daran zu erinnern, dass die Bürgerschaft am 1./2. Februar 1995 zum 12. Tätigkeitsbericht beschlossen hatte: „Die Bürgerschaft ersucht den Senat, er möge in allen künftigen Gesetzentwürfen in der Begründung Auskunft über eventuelle Einschränkungen des Datenschutzes geben." Der Senat hat sich hierzu in seiner Stellungnahme vom 25. April 1995 wie folgt geäußert: „Der Senat wird dem Ersuchen der Bürgerschaft Rechnung tragen und künftig in der Begründung zu Entwürfen zu Landesgesetzen auf etwaige Einschränkungen des Rechts auf informationelle Selbstbestimmung besonders hinweisen".

In der Stellungnahme des Senats vom 28. Mai 1996 zum 14. Tätigkeitsbericht heißt es insoweit ergänzend: „Die Antwort des Senats auf das bürgerschaftliche Ersuchen, in der Begründung künftiger Gesetzentwürfe Auskunft über eventuelle Einschränkungen des Datenschutzes zu geben, wurde den Senatsämtern und Fachbehörden durch Rundschreiben der Justizbehörde vom 28. Juni 1995 nochmals besonders bekannt gemacht und erläutert. Dabei ist auch darauf hingewiesen worden, dass es der Intention der Bürgerschaft am ehesten entspreche, in den allgemeinen Teil der Gesetzesbegründung einen gesonderten Abschnitt aufzunehmen, der auf etwaige Einschränkungen des Grundrechts hinweise, während die detaillierte Begründung bei den einzelnen Gesetzesvorschriften erfolgen könne."

In der Mitteilung des Senats an die Bürgerschaft vom 10. September 2002 zur Änderung von Verfassungsschutzvorschriften fehlt sowohl ein Abschnitt im allgemeinen Teil der Gesetzesbegründung als auch eine nähere Begründung bei den einzelnen Gesetzesvorschriften hinsichtlich der Einschränkungen des Datenschutzes. Vielmehr finden sich nur vereinzelte Hinweise auf den Datenschutz. Im Interesse des Selbstbestimmungsrechts der Bürgerinnen und Bürger ist es dringend geboten, dass die vorgeschriebene Verfahrensweise künftig wieder uneingeschränkt eingehalten wird.

2.3 Unterstützung der Bürger

Die Bürger haben sich wieder in großer Zahl an uns gewandt und viele Informationsangebote in Anspruch genommen.

Die von uns jahresweise erfasste Zahl der schriftlichen Eingaben der Bürger betrug – ähnlich wie bei dem hohen Stand im Jahr 2001 – bis Ende November 2002 über 560. Schwerpunkte waren wiederum die Bereiche Werbung und Adresshandel und ähnlich zahlreich wie schon 2001 der Bereich Teledienste. Außerdem haben wir die Bürger bis Ende November 2002 persönlich, telefonisch oder schriftlich in über 1.800 Fällen beraten. Die Zahl der Beratungen öffentlicher und nicht öffentlicher Stellen, die auch den Bürgern unmittelbar oder mittelbar zugute kommen, betrug bis Ende November 2002 über 1.700.

Großen Anklang fanden wieder unsere Broschüren, Faltblätter usw. zu über 20 Themengebieten, die am Ende dieses Berichts wiedergegeben sind. Im Internet veröffentlichten wir – als Spitzenreiter im gesamten hamburgischen Angebot – die aktualisierte „Orientierungshilfe Tele- und Mediendienste“ mit rund 11.600 Abrufen im Januar 2002 sowie die Schrift „Datenschutz bei Windows 2000“ mit rund 31.000 Abrufen im Februar 2002. Für unser Internetangebot sind ca. 24.000 Seitenabrufe pro Monat zu verzeichnen.

Die von mir mitgegründete Hamburger Datenschutzgesellschaft (HDG) hat Ende Mai 2002 wiederum zusammen mit der Handelskammer Hamburg ein Forum über „Elektronische Kontrollen in der Wirtschaft – Biometrie, Internet und Email –“ durchgeführt. Stark besucht war auch Ende Oktober 2002 im Warburg-Haus der Vortrag des Vizepräsidenten des Bundesverfassungsgerichts, Prof. Hassemer, über „Einige Thesen zur Selbstbestimmung im dritten Jahrtausend“.

2.4 Ausstattung der Dienststelle

Die Dienststelle hat nunmehr 20 Mitarbeiterinnen und Mitarbeiter.

Bei der schwierigen Haushaltslage wurde es dennoch ermöglicht, die erfreuliche Gesamtzahl von 20 Mitarbeiterinnen und Mitarbeitern zu erreichen. Bei dem großen Anteil von Teilzeitbeschäftigten beträgt die Stellenzahl insgesamt 16,33.

3. Informations- und Kommunikationstechnik

3.1 E-Government

Datenschutzanforderungen müssen umfassend berücksichtigt werden, um für E-Government-Angebote die Akzeptanz der Bürgerinnen und Bürger zu gewinnen.

Für die Verwaltungsmodernisierung spielt das E-Government eine wichtige Rolle (s. insbesondere Mitteilung des Senats an die Bürgerschaft vom 24./25. Juni 2002, E-Government-Chancen für Hamburg nutzen, Bürgerschafts-Drucksache 17/1091). Dabei ist einer der Erfolgsfaktoren für E-Government-Projekte, dass die Nutzerinnen und Nutzer die Gewissheit haben, dass bei der Verarbeitung ihrer Daten die Anforderungen des Datenschutzes umfassend

gewährleistet werden. Die Datenschutzbeauftragten der Länder und des Bundes haben diese Anforderungen und auch beispielhafte Lösungsansätze in der Broschüre „Datenschutzgerechtes E-Government“ dargestellt, die Ende 2002 veröffentlicht wird.

Der Hamburgische Datenschutzbeauftragte hat erreicht, dass die datenschutzrechtlichen Anforderungen in der o.a. Mitteilung des Senats an die Bürgerschaft „E-Government – Chancen für Hamburg nutzen“ verstärkt berücksichtigt wurden. Es sind bei den E-Government-Anwendungen so wenig Daten wie möglich zu verarbeiten. Reine Informationsangebote sind daher grundsätzlich anonym nutzbar zu machen. Wir haben uns aber auch dafür eingesetzt, dass die Option einer anonymen Bezahlfunktion offen gehalten und mittelfristig umgesetzt wird. Auch bei einem vergleichbaren Behördengang werden keine Kontendaten erfasst, wenn man dort eine Gebührenmarke zieht. Dies sollte auch auf E-Government-Anwendungen übertragen werden. Des weiteren soll auch durch geeignete technische Maßnahmen dafür Sorge getragen werden, dass Daten aus unterschiedlichen Datenbeständen nicht rechtswidrig zusammengeführt werden können.

Ein Beispiel für ein Informationsangebot ist die im Berichtszeitraum vom Bezirksamt Hamburg-Mitte realisierte Anwendung „Fundinfo“, die eine 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.

Neben den Informationsangeboten für die Bürgerinnen und Bürger sind zahlreiche Anwendungen im E-Government-Fahrplan enthalten, bei denen sich die Nutzerinnen und Nutzer gegenüber der Behörde authentifizieren müssen. Für diese Anwendungen soll ein einheitlicher Zugang entwickelt werden, der den Sicherheitsanforderungen entspricht. An diesem „Hamburg-Gateway“ wird die Authentizität überprüft. Dabei sollen folgende unterschiedliche Sicherheitslevel eingerichtet werden, die je nach Sensibilität der verarbeiteten Daten erfüllt sein müssen:

- Der Benutzer richtet sich online über das Internet einen Zugang ein, ohne dass eine weitere Überprüfung vorgenommen wird.
- Der Benutzer registriert sich einmalig persönlich bei einer Behörde und belegt seine Identität mit einem Personalausweis oder Reisepass.
- Der Benutzer registriert zusätzlich seine qualifizierte elektronische Signatur.
- Für Firmenkunden soll bei der Verarbeitung sensibler Daten eine gesicherte Authentifizierung eingerichtet werden.

In einem ersten Schritt sollen die beiden zuerst genannten Level zur Verfügung gestellt werden. Vorgänge, bei denen aufgrund gesetzlicher Anforderungen eine Unterschrift erforderlich ist, sind jedoch nur bei Nutzung der qualifizierten elektronischen Signatur möglich. Die elektronische Signatur sollte auch für hamburgische E-Government-Anwendungen möglichst schnell genutzt werden können. Wir setzen uns dafür ein, dass für die Firmenkunden eine sichere Authentifizierung ermöglicht wird. Die alleinige Eingabe eines Passwortes zur Überprüfung der Authentizität reicht bei der Verarbeitung sensibler Daten nicht aus. In diesem Fall kann nicht sichergestellt werden, dass der Aufruf über das Internet auch wirklich aus den Räumlichkeiten der Institution mit den dort vorhandenen technischen und organisatorischen Sicherungsmaßnahmen erfolgt. Daher sind zusätzliche Sicherheitsmaßnahmen wie z.B. SSL-Client-Zertifikate erforderlich.

Die Daten aus den E-Government-Anwendungen werden über eine verschlüsselte SSL-Verbindung an die Nutzer übermittelt. Die Vertraulichkeit wird somit gewährleistet. Eine Übermittlung in Form einer unverschlüsselten E-Mail ist nicht geplant. Wenn ein Ergebnis nicht innerhalb einer Online-Sitzung bereitgestellt werden kann, wird der Nutzer nur mit einer E-Mail unterrichtet, sobald er das Ergebnis abrufen kann. Er muss sich dann erneut authentifizieren und eine verschlüsselte Verbindung aufbauen, über die die Ergebnisdaten übertragen werden.

Für das Hamburg-Gateway und die Pilotanwendung Melderegisterauskunft wurde eine Risikoanalyse durchgeführt. Wir werden darauf achten, dass auch für die weiteren Entwicklungen die Datenschutzbelange frühzeitig und umfassend berücksichtigt werden, um so den Modernisierungsprozess der Verwaltung aktiv zu unterstützen.

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

Ein sicheres Authentifizierungsverfahren fehlt immer noch.

Das automatisierte Verfahren INEZ wird 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 haben die für das Zuwendungs-Controlling erforderlichen Informationen regelmäßig zu aktualisieren. Um Medienbrüche und Doppelarbeit bei der Aktualisierung zu vermeiden, soll einer geschlossenen Benutzergruppe ein lesender und schreibender Zugriff auf INEZ-Daten über das Internet ermöglicht werden. Diese Anwendung heißt „Web-INEZ“ und läuft in der Pilotierung seit dem Sommer 2001 für einen eng begrenzten 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. Die alleinige Überprüfung eines Passwortes reicht nicht aus, da mit einem erspähten Passwort der Zugriff auf die sensiblen Daten von jedem Rechner aus möglich wäre, der an das Internet angeschlossen ist. Die Schutzmaßnahmen sollten im Rahmen der Pilotierung realisiert werden, bevor der Nutzerkreis erweitert wird.

Trotz wiederholter Erinnerungen hat die BSF die Realisierung einer sicheren Authentifizierungslösung im Berichtszeitraum nicht vorangetrieben. Die BSF beabsichtigte zwischenzeitlich, die vereinbarten Schutzmaßnahmen gar nicht mehr umzusetzen. Damit besteht ein erhebliches Risiko, dass die Daten von nicht berechtigten Personen eingesehen und auch verändert werden können. Über diese gravierende Planungsänderung wurden wir nicht direkt informiert, sondern haben nur auf Umwegen davon erfahren. Parallel dazu hat die BSF den Kreis der Nutzer der Pilotierung und den Umfang der Daten, die während der Pilotierung verarbeitet werden, erweitert und damit das Risiko einer missbräuchlichen Nutzung der Daten deutlich vergrößert.

Vor einer produktiven Nutzung von Web-INEZ müssen die erforderlichen technischen Maßnahmen zur sicheren Authentifizierung getroffen werden, damit den Verpflichtungen, die sich aus §8 Abs. 2 Hamburgisches Datenschutzgesetz (HmbDSG) ergeben, entsprochen wird. Diese Maßnahmen sind umgehend zu treffen, um auch den Schutz der Daten zu erhöhen, die bereits in der Pilotierung mit Web-INEZ verarbeitet werden. Die BSF hat aufgrund unserer Intervention jetzt zugesagt, ein entsprechendes Schutzkonzept im 1.Quartal 2003 zu erstellen. Wenn dies nicht erfolgt, kommt eine förmliche Beanstandung nach §25 HmbDSG wegen der andauernden datenschutzrechtlichen Mängel in Betracht.

3.3 Einsatz von Windows 2000 in der hamburgischen Verwaltung

Ein Sicherheitskonzept für den Einsatz von Windows 2000 liegt vor. Möglichkeiten des Betriebssystems zur Umsetzung von Datenschutzanforderungen sind noch ungenutzt.

Die IuK-Infrastruktur der hamburgischen Verwaltung wird flächendeckend auf das Betriebssystem Windows 2000 umgestellt. Insbesondere mit dem zentralen Verzeichnisdienst Active Directory sind auch zusätzliche Sicherheitsrisiken verbunden (vgl. 18. TB, 3.2.2). Es werden mittlerweile über 4500 Benutzerkonten verschiedener Behörden im Active Directory verwaltet.

Für die Nutzung des Active Directory wurde vom Landesamt für die Informationstechnik (LIT) 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. Die Protokollierung der Administratoren-Konten in den Behörden und die Vorgehensweise für die Auswertung der Protokolle wird vom LIT noch konzeptionell aufgearbeitet. Aufgrund der Größe der regelmäßig entstehenden Protokolle sollte eine Auswertung technisch unterstützt werden.

Die Administratoren des LIT können im Active Directory auch in die administrativen Bereiche der Behörden eingreifen. Aufgrund unserer Anforderungen wurde eine organisatorische Regelung für einen solchen Eingriff getroffen. Ein sicherheitskritischer Eingriff darf danach nur aufgrund eines Auftrags (per Mail oder Fax) vorgenommen werden, der vom LIT revisionssicher dokumentiert wird.

Die Benutzer der Konten, die im Active Directory verwaltet werden, können sich grundsätzlich in der gesamten Domäne anmelden. Da nach dem Betriebskonzept alle Behörden in eine gemeinsame Domäne eingebunden sind, kann die Anmeldung auch außerhalb der Räumlichkeiten der jeweiligen Behörde erfolgen. Die Risiken, ein fremdes Benutzerkonto zum Ausspähen von Daten zu missbrauchen, steigen damit gegenüber der bisherigen Situation mit getrennten Domänen der einzelnen Behörden. Die Geheimhaltung der Benutzerpasswörte ist daher besonders wichtig. Es sind jedoch zahlreiche technische Angriffsmöglichkeiten und Vorgehen zum Ausspähen von Passworten bekannt. Daher sollten die Behördenadministratoren zusätzliche Schutzmaßnahmen treffen, um den Zugriff auf bestimmte Geräte zu beschränken und so die Risiken eines Passwort-Missbrauchs verringern. Das LIT hat dieses für die kritischen Administratorenkonten vorgenommen.

Wir haben 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. Die vom LIT geplante systematische Untersuchung der Einsatzmöglichkeiten von IPSec für die hamburgische Verwaltung wurde jedoch immer noch nicht begonnen, obwohl Windows 2000 schon seit mehr als zwei Jahren produktiv genutzt wird.

Ohne eine umfassende Prüfung wurde vom LIT 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.

Bereits im 14. Tätigkeitsbericht hatten wir darauf hingewiesen, dass immer wieder Vorbehalte seitens der Verfahrensverantwortlichen und des LIT gegen die Einführung einer verschlüsselten Datenkommunikation deutlich werden, ohne dass die jeweiligen technischen Möglichkeiten und der damit zusammenhängende Aufwand systematisch betrachtet wurden (vgl. 14.TB, 3.1.4). Wir werden uns auch weiterhin dafür einsetzen, dass die bereitgestellten technischen Möglichkeiten zur Umsetzung von Datenschutzanforderungen genutzt werden.

3.4 Ressourcensteuerung mit SAP R/3

Mit einer Verordnung nach § 11 a Hamburgisches Datenschutzgesetz (HmbDSG) wird für die Führung von Einheitspersonenkonten im SAP/R3-Verfahren zur integrierten Ressourcensteuerung die datenschutzrechtliche Grundlage geschaffen.

Über das zentrale IuK-Verfahren für die integrierte Ressourcensteuerung „sap für hamburg“ haben wir ausführlich im 18. TB (3.2.3) berichtet. Es soll die bislang auf unterschiedlichen Betriebssystemen und Softwareprodukten laufenden Haushalts- und Kassenanwendungen auf eine Hamburgweit einheitliche Basis stellen. Gegenüber dem bisherigen Mittelbewirtschaftungsverfahren wird es dabei eine datenschutzrechtlich besonders relevante Veränderung geben.

Bislang konnten alle Behörden und Ämter voneinander getrennte Dateien mit ihren Debitoren und Kreditoren anlegen, was für die Verwaltung insgesamt zu einer mehrfachen Speicherung kassenrelevanter personenbezogener Daten führte. Das neue Verfahren setzt dagegen die Schaffung von Einheitspersonenkonten zwingend voraus. Namen, Anschriften und Bankverbindungen werden nur noch einmal in einer einzigen Datei gespeichert, auf die alle mittelbewirtschaftenden Stellen der hamburgischen Verwaltung unabhängig von ihrem jeweiligen Aufgabenbereich einen lesenden Zugriff erhalten. Dies ist erforderlich, weil die Anwenderinnen und Anwender von „sap für hamburg“ sich vor der Neuanlage eines Debitoren- oder Kreditorenstammdatensatzes davon überzeugen müssen, dass ein solcher Stammdatensatz nicht bereits im System vorhanden ist.

Der behördenübergreifende lesende Zugriff bezieht sich allein auf die Namen, Anschriften und Bankverbindungen der in Zahlungsvorgängen auftretenden Firmen und Einzelpersonen. Hierzu gehören auch die Mitarbeiterinnen und Mitarbeiter der Verwaltung, soweit ihnen z.B. die Kosten für Dienstreisen erstattet werden. Ein Zugriff auf die Einzelheiten des jeweiligen Zahlungsvorgangs über die aufgabenbezogenen behörden- und ämterspezifischen Buchungskreise hinaus wird dagegen durch eine restriktive Berechtigungsvergabe verhindert.

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. Die bereits erfolgte Einrichtung und Nutzung der Einheitspersonenkonten soll nun nachträglich durch eine Rechtsverordnung des Senats zugelassen werden. In ihr werden die zu verarbeitenden Daten und alle beteiligten Stellen mit dem Umfang ihrer Verarbeitungsbefugnis angegeben sowie die Stelle festgelegt, die gegenüber den betroffenen Personen die datenschutzrechtliche Verantwortung trägt und Maßnahmen zur Datensicherung trifft. Ein erster Entwurf liegt uns vor. Er wird in Kürze in die Behördenabstimmung gegeben.

3.5 Sichere Nutzung des Internets am Arbeitsplatz

Die Maßnahmen zum Schutz von Arbeitsplätzen der hamburgischen Verwaltung vor Gefahren aus dem Internet sind weiterhin defizitär.

Seit geraumer Zeit besteht Einvernehmen mit der Finanzbehörde, darüber, dass für Anwendungen mit hohem Schutzbedarf bei der Nutzung des Internet zusätzliche Sicherheitsvorkehrungen zu treffen sind. Wir haben im 18. TB (3.3.1) darauf hingewiesen, dass wir – auch aus eigener täglicher Praxis – die Verwendung von Terminal-Servern für eine gut geeignete Ausprägung dieser Sicherheitsvorkehrungen halten.

Der Senat hat in seiner Stellungnahme zum 18. TB angegeben, dass für einen Einsatz dieser Technik mit großen Nutzerzahlen Erfahrungen im Rahmen des Projekts TUVAS gewonnen werden sollen. Dies ist bislang nicht erfolgt und aus Sicht des Projekts auch nicht geplant. Vielmehr werden dort zurzeit Alternativansätze verfolgt. Wir haben daher der Bürgerschaft mit Schreiben vom 25. November 2002 ein Ersuchen an den Senat vorgeschlagen, den Behörden bald Terminal-Server-Dienste durch das Landesamt für Informationstechnik (LIT) bereit zu stellen.

Damit bleibt den einzelnen Fachbehörden eine integrierte vollständige Nutzung des Internet in vielen Fällen weiterhin verwehrt, da sie auf andere, weniger sichere oder weniger komfortable Lösungen zurückgreifen müssen. Dabei handelt es sich zum einen um die eingeschränkte Internet-Nutzung mittels URL-Positiv-Listen und zum anderen um den Betrieb besonderer, ausschließlich für die Internet-Nutzung vorgesehener Arbeitsplätze.

Die vom LIT darüber hinaus mittlerweile realisierte generelle Sperrung einzelner URL (Negativ-Liste) hat in Hinblick auf die Datensicherheit insgesamt nur eine sehr geringe Wirkung.

3.6 FHHinfoNET

Nach nicht unerheblicher Verzögerung kann nun seit Ende Oktober 2002 mit der flächendeckenden Einrichtung der „Erweiterten Sicherheit“ an den PC-Arbeitsplätzen der Verwaltung begonnen werden.

Das vom Landesamt für Informationstechnik (LIT) betriebene Mailing-System der hamburgischen Verwaltung („FHHinfoNET“) wird bereits seit vier Jahren in unseren Tätigkeitsberichten ausführlich behandelt. Im Mittelpunkt steht dabei die Verschlüsselung elektronisch versandter Nachrichten mit sensiblen personenbezogenen Inhalten. Die Umstellung der Server im LIT auf Exchange 2000 ließ im Jahr 2001 die Ausweitung der bis dahin möglichen und bereits teilweise genutzten Signaturen auf alle PC-Arbeitsplätze nicht zu. Die weiteren Planungen sahen vor, in der hamburgischen Verwaltung eine die Anforderungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) erfüllende Public-Key-Infrastruktur einzurichten. Der flächendeckende Einsatz der „Erweiterten Sicherheit“ sollte dann ab April 2002 erfolgen (siehe 18. TB, 3.2.1).

Aufgrund technischer Probleme bei der Umsetzung der Vorgaben des BSI trat jedoch eine Verzögerung von mehreren Monaten ein. Dies führte zu einem unbefriedigenden Zustand. Zum einen standen zeitlich auslaufende, auf der alten Basis eingerichtete Zertifikate, die in wenigen sensiblen Bereichen wie der Personaldatenverarbeitung und der Steuerverwaltung bislang noch im Einsatz waren, nicht mehr wie gewohnt für die tägliche Arbeit zur Verfügung. Zum anderen mussten Anwender, die die Verschlüsselung für ihre Aufgaben nutzen wollten, auf unbestimmte Zeit weiter darauf verzichten.

Seit Ende Oktober 2002 hat das LIT nun jedoch eine funktionierende Infrastruktur zur Verschlüsselung und Signatur von Nachrichten im FHHinfoNET eingerichtet. Die organisatorischen und technischen Anforderungen an die flächendeckende Umsetzung sind in einem mit dem BSI abgestimmten Konzept festgelegt worden. Die Behörden und Ämter der hamburgischen Verwaltung sind nun aufgefordert, die „Erweiterte Sicherheit“ in ihren Bereichen zügig an allen PC-Arbeitsplätzen einzuführen.

3.7 Dokumentenverwaltung

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

Im 18. TB (3.4) hatten wir bereits verschiedene Problemfelder in Bezug auf die bisher 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 Ämtern für erforderlich.

Im Februar 2002 wurde im Landesamt für Informationstechnik (LIT) ein DOKUMENTA-Kundenbeirat gegründet. Zur Erarbeitung von Vorschlägen für die notwendigen, übergeordneten Vorgaben für den Umgang mit elektronischen Akten und Schriftstücken wurde die Unterarbeitsgruppe (UAG) Regelungen eingesetzt. Der Hamburgische Datenschutzbeauftragte ist an dieser beteiligt.

Im Juni 2002 wurde von der UAG „Regelungen über das Staatsarchiv“ eine Umfrage über die in den Behörden und Ämtern derzeit geltenden Bestimmungen zur Aufbewahrung, Vernichtung und Archivierung von Schriftstücken durchgeführt. Diese konnte bisher erst grob ausgewertet werden.

Hinsichtlich der datenschutzrechtlichen Behandlung verschiedener Aktenarten und der Verteilung von Aufgaben, Verantwortlichkeiten und Kompetenzen bei der Einführung des elektronischen Verfahrens sind für Anfang 2003 seitens der Finanzbehörde Gespräche mit dem Staatsarchiv vorgesehen. Auf dieser Grundlage sollen die notwendigen Regelungen unter Beteiligung der UAG erarbeitet werden.

3.8 Aktualisierung von IT-Richtlinien und DV-Revision

Die behördlichen DV-Revisionen müssen ihre Arbeit auf der Grundlage aktueller Datenschutzanforderungen wahrnehmen. Die meisten derzeitigen IT-Richtlinien genügen dafür nicht mehr.

Wenn personenbezogene Daten automatisiert verarbeitet werden, sind technische und organisatorische Maßnahmen zu treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität und die Revisionsfähigkeit gewährleisten können. Die Sicherungsziele sind im § 8 Abs. 2 des Hamburgischen Datenschutzgesetzes (HmbDSG) festgelegt.

Die Finanzbehörde hat hinsichtlich verschiedener Einzelthemen IT-Richtlinien erlassen, die gewährleisten sollen, dass diese datenschutzrechtlichen Anforderungen erfüllt werden. Im Gegensatz zu den abstrakt formulierten Anforderungen im HmbDSG sind darin ganz detaillierte Kriterien enthalten, die beim Einsatz von IT-Technik von den Behörden einzuhalten sind. Mit Ausnahme der Architekturrichtlinie, die im Berichtszeitraum aktualisiert wurde, stammen die IT-Richtlinien aber aus der erste Hälfte der neunziger Jahre und spiegeln den damaligen technischen 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 zur Folge, dass durch die Einhaltung der gültigen IT-Richtlinien zum Teil auch Grundschutzanforderungen nicht mehr erfüllt werden.

Wir setzen uns daher seit längerem dafür ein, dass die einschlägigen IT-Richtlinien dem aktuellen technischen Stand angepasst werden. Dabei sind insbesondere die nachfolgenden Richtlinien zu nennen:

- Passwortrichtlinie

  Aufgrund der Leistungsfähigkeit gängiger Rechner ist ein ausreichendes Schutzniveau mit einer Mindest-Passwortlänge von 6 Zeichen nicht erreichbar. Solche Passworte lassen sich je nach Komplexität mit frei verfügbaren Programmen zum Teil innerhalb weniger Minuten knacken.

- 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 dahingehend angepasst werden, dass 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, berücksichtigt werden.

Wir werden bei unseren datenschutzrechtlichen Prüfungen auch diese Kriterien zu Grunde legen, um die realisierten technischen und organisatorischen Maßnahmen zu beurteilen.

Die Stellen, die dem Hamburgischen Datenschutzgesetz unterliegen, haben dafür zu sorgen, dass die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen überwacht wird. Durch die DV-Revisionen soll sicher gestellt werden, dass die datenschutzrechtlichen Anforderungen von den Daten verarbeitenden Stellen eingehalten werden. Die behördlichen DV-Revisionen können diese Aufgabe nur dann effizient und effektiv wahrnehmen, wenn ihnen aktuelle IT-Richtlinien zur Verfügung stehen.

3.9 Online-Prüfungen

Prüfungen bei Anbietern von Internet-Diensten haben ergeben, dass in vielen Fällen Datenschutzvorschriften nicht eingehalten werden. Insbesondere werden erheblich mehr personenbezogene Nutzungsdaten gespeichert, als es das Gesetz erlaubt.

Im Berichtszeitraum wurde eine Reihe von Anbietern von Tele- und Mediendiensten geprüft. Dabei handelte es sich sowohl um Anbieter von Internet-Zugangsdiensten (Access Provider) als auch um Anbieter von Inhalten (Content Provider). Dabei kam auch das ursprünglich beim Hamburgischen Datenschutzbeauftragten entwickelte Prüftool OPTuM („Online-Prüfung von Tele- und Mediendiensten“) zum Einsatz (vgl. 18. TB, 3.5.4). In seiner mittlerweile fortgeschriebenen Form ermöglicht dieses Programm die automatisierte Analyse folgender Aspekte eines Internet-Angebots:

- Anbieterkennzeichnung
- 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 feststellbaren 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). Ein häufig anzutreffendes Problem stellen auch unzureichende Anbieterkennzeichnungen dar.

In der Mehrzahl der Fälle haben die Prüfungen zudem ergeben, dass die Provider erheblich mehr personenbezogene Nutzungsdaten speichern, als es das Teledienstedatenschutzgesetz und der Mediendienste-Staatsvertrag erlauben. Bei diesen Nutzungsdaten handelt es sich z.B. um die IP-Nummer des vom Nutzer verwendeten Systems, Kennungen und Passwörter des Nutzers oder die Adressen der aufgerufenen Seiten einschließlich inhaltlicher Bestandteile wie Suchbegriffe innerhalb von Anfragen bei einer Suchmaschine.

Wir haben durchgesetzt, dass die unzulässig gespeicherten Daten gelöscht werden und dass die Angebote auch im Übrigen an die gesetzlichen Vorgaben angepasst werden. Die beschriebene Prüfpraxis werden wir fortsetzen und dabei auch auf die Internet-Angebote öffentlicher Stellen ausdehnen.

Datenschutz im öffentlichen Bereich

4. Allgemeine Verwaltungsangelegenheiten

Behördlicher Aktentransport

Aus der förmlichen Beanstandung, die wir wegen zahlreicher Datenschutzverstöße aussprechen mussten, haben die Gerichte nachdrücklich Konsequenzen gezogen.

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. Bei Prüfungen im Januar und Februar 2002 fanden wir Anklageschriften, Strafurteile, Fragebögen zum Versorgungsausgleich, Testamente, Erbscheine und andere Sendungen der Amtsgerichte mit sensiblen personenbezogenen Daten in großer Anzahl offen ohne Umschlag vor.

Deshalb sprachen wir im März 2002 eine förmliche Beanstandung gegenüber dem Präses der Justizbehörde aus. Die Justizbehörde verwies in ihrer Stellungnahme auf die bereits unternommenen Anstrengungen zur Gewährleistung des Datenschutzes und unterstrich, dass es sich bei den festgestellten Verstößen nicht um strukturelle Vollzugsdefizite beim Post- und Aktenaustausch, sondern um Fehlverhalten im Einzelfall handele. Auch in den folgenden Monaten wurden wir beim BTS aber wiederholt auf unverschlossene Sendungen von Amtsgerichten in Familien-, Betreuungs-, Freiheitsentziehungs-, Straf- und Bußgeldsachen aufmerksam. Daher sahen wir Anlass, der Justizbehörde im Juni 2002 eine weitere Beanstandung an den Senat in Aussicht zu stellen.

Ab Mitte 2002 begannen die Gerichte, den aufgedeckten Mängeln beim Versand durch stichprobenartige interne Überprüfungen mit monatlicher Dokumentation und Berichtspflicht gegenüber dem Präsidenten des Amtsgerichts Hamburg Rechnung zu tragen. Sendungen mit personenbezogenen Daten, die offen in der Zentralverwaltung der Gemeinsamen Annahmestelle des Land- und Amtsgerichts Hamburg eingehen, werden von deren stellvertretendem Leiter mit angeheftetem Formblatt unter Hinweis auf den Datenschutzverstoß an die Absender zurückgeschickt. Ferner wird für jeden Monat eine Dokumentation der Defizite beim Datenschutz erstellt, und zwar differenziert nach einzelnen Gerichten und Dezernaten sowie für die Justizbehörde, die Justizkasse, die Untersuchungshaftanstalt und die Staatsanwaltschaft. Das Amtsgericht Hamburg hat zugesagt, uns über die wesentlichen Ergebnisse der Dokumentation einmal jährlich, bei auffälligen Fehlentwicklungen auch in kürzeren Zeitabständen zu berichten.

Als Folge dieser erfreulichen organisatorischen Vorkehrungen beobachteten wir bei Kontrollen des BTS im Oktober und November 2002 nur noch relativ wenige Verletzungen des Datenschutzes durch Gerichte. Offen versandt wurde ein Bewährungsheft mit einer unbeschränkten Auskunft aus dem Zentralregister und dem Erziehungsregister. Die Übermittlung der Registerauskunft an die Bewährungshilfe für Erwachsene halten wir nach den Vorschriften des Bundeszentralregistergesetzes (BZRG) für unzulässig. Deshalb sind wir im Rahmen unseres gesetzlichen Beratungsauftrags in Angelegenheiten der Rechtspflege mit den zuständigen Amtsgerichten in eine Erörterung dieser Frage eingetreten.

Auch außerhalb der Justiz stellten wir erhebliche Datenschutzverstöße beim Post- und Aktenaustausch fest. Verantwortlich hierfür waren insbesondere Bezirks- und Ortsämter. Deshalb haben wir dem Leiter des Senatsamtes für Bezirksangelegenheiten (SfB) dringend empfohlen, Abhilfemaßnahmen entsprechend den neuen Regelungen bei der Gemeinsamen Annahmestelle der Gerichte zu ergreifen. Beim BTS offen vorgefunden wurden z.B. Sozialhilfe- und Ausländerakten, ein Wohngeldbewilligungsbescheid, Korrespondenz wegen melderechtlicher Auskunftssperren, der auf Grund eines Suchvermerks im Bundeszentralregister ergangene Hinweis, die Anzeige eines Kreditinstituts wegen einer verdächtigen Finanztransaktion, Unterlagen über eine drohende Gewerbeuntersagung wegen rückständiger Steuern und Beiträge sowie Rechnungen von Krankenhäusern und anderen Einrichtungen, die detailliert Aufschluss über eine Multiple Sklerose, eine pädagogische Betreuung, eine vollstationäre Unterbringung in der Psychiatrie oder über eine Gruppentherapie wegen Glücksspielabhängigkeit vermittelten.

Als besonders gravierende Verletzung des Datenschutzes ist ferner hervorzuheben, dass die Bußgeld- und Strafsachenstelle eines Finanzamts dem zuständigen Arbeitsamt in einer Steuerstrafsache unverschlossen eine Mitteilung nach § 31 a der Abgabenordnung (AO) wegen vermuteten Leistungsmissbrauchs übersandt hat. Dem Schreiben des Finanzamts waren als Anlagen umfangreiche Kopien von Kontoauszügen des Beschuldigten beigefügt. Sie vermittelten, weit über den Zweck der Mitteilung hinaus, umfassend Einblick in die Zahlungsvorgänge. Schwärzungen bezüglich solcher Kontobewegungen, die für das Arbeitsamt offensichtlich irrelevant waren, wurden auf den Kopien nicht vorgenommen. So war es dem Arbeitsamt möglich, nicht nur das Freizeit- und Konsumverhalten des Kontoinhabers, sondern auch die Begleichung der Rechnungen von Ärzten und eines Optikers nachzuvollziehen.

5. Soziales

5.1 Projekt SAM bei den Allgemeinen Ortskrankenkassen

Die anstehende Modernisierung der Informationssysteme bei den Allgemeinen Ortskrankenkassen muss auch dazu genutzt werden, die datenschutzrechtlichen Defizite der alten Systeme zu beseitigen.

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 (**S**AP-**A**OK-**M**aster) installiert worden, das nach den bisherigen Planungen in sechs bis sieben Jahren abgeschlossen sein soll. Dann erst wird die bislang von der AOK eingesetzte Software IDVS II vollständig abgelöst werden. Die ersten SAM-Module sollen jedoch voraussichtlich bereits im Frühjahr 2003 zunächst bei der AOK Mecklenburg-Vorpommern in die Pilotierung gehen.

Die Datenschutzbeauftragten des Bundes und der Länder haben von diesen Planungen erfahren und eigens für die datenschutzrechtliche Projektbegleitung eine Unterarbeitsgruppe ihres Arbeitskreises Gesundheit und Soziales eingesetzt. Die Federführung für diese Unterarbeitsgruppe haben wir übernommen.

Das Hauptaugenmerk der Projektbegleitung wird darauf gerichtet sein, 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 und auf dem Laufenden gehalten worden. Soweit erkennbar, ist damit ein konstruktiver und für beide Seiten Gewinn bringender Dialog begonnen worden, der allerdings nur dann erfolgreich andauern kann, wenn der AOK-Bundesverband den Datenschutzbeauftragten die erforderlichen Informationen uneingeschränkt und zeitnah zur Verfügung stellt.

5.2 Anforderung ärztlicher Unterlagen durch Krankenkassen bei Krankenhäusern

Das Bundessozialgericht hat die Rechtsauffassung der Datenschutzbeauftragten bestätigt.

Seit Jahren bestehen unterschiedliche Auffassungen zwischen den Datenschutzbeauftragten des Bundes und der Länder sowie den Krankenhäusern auf der einen Seite und einigen Krankenkassen auf der anderen Seite darüber, welche ärztlichen Unterlagen die Krankenkassen zur Überprüfung der Krankenhausbehandlung anfordern dürfen (vgl. 18. TB, 10.1). Hierzu hat das Bundessozialgericht nunmehr durch Urteil vom 23. Juli 2002 (Az. B 3 KR 64/01 R) eindeutig Stellung bezogen und ist anderslautenden Auffassungen der Vorinstanzen entgegen getreten.

In dem verhandelten Fall hatte die Krankenkasse die Begleichung eines Rechnungsbetrages davon abhängig gemacht, dass ihr das Krankenhaus die Behandlungsunterlagen zur Überprüfung unter Einschaltung des Medizinischen Dienstes der Krankenversicherung (MDK) übersendet. Sie hatte Zweifel, ob das Krankenhaus die abgerechneten Leistungen auch tatsächlich erbracht hat. Das Krankenhaus hatte die Überlassung der Unterlagen unter Hinweis auf eine fehlende rechtliche Verpflichtung sowie den Datenschutz verweigert und geltend gemacht, dass nach der gegenwärtigen Rechtslage

weder den Krankenkassen noch dem MDK ein Einsichtsrecht in die Behandlungsunterlagen zum Zwecke der Rechnungsprüfung zustehe. Was den Krankenkassen im Rahmen der Abrechnung an Daten zur Verfügung zu stellen sei, sei abschließend in § 301 Fünfter Teil Sozialgesetzbuch (SGB V) geregelt.

Das Gericht ist dieser Auffassung im wesentlichen gefolgt. Zwar hätten die Krankenkassen nach § 275 SGB V in erweiternder Auslegung des Gesetzeswortlauts auch ein Prüfungsrecht hinsichtlich der tatsächlichen Erbringung einer abgerechneten Leistung; sie könnten die dafür erforderliche Einsichtnahme in die Behandlungsunterlagen aber nicht aus eigenem Recht verlangen, sondern seien insoweit auf ein Tätigwerden des MDK angewiesen. Dies entspricht der seit Jahren von den Datenschutzbeauftragten des Bundes und der Länder vertretenen Auffassung, dass die im Sozialgesetzbuch festgelegte Aufgabenverteilung zwischen Krankenkassen und MDK nicht durch abweichende Verfahren unterlaufen werden darf. Die medizinische Bewertung von Einzelfällen ist nach § 275 SGB V allein dem MDK vorbehalten.

Nach diesem Ergebnis werden wir näher untersuchen müssen, ob möglicherweise sogar das vor Jahren mit der AOK Hamburg abgesprochene und mittlerweile auch von der BKK Hamburg praktizierte Einwilligungsverfahren datenschutzrechtlich noch vertretbar ist (vgl. 13. TB, 21.8.2). Wir werden dies sorgfältig mit den anderen Datenschutzbeauftragten des Bundes und der Länder abklären und sowohl die unserer Aufsicht unterliegenden Krankenkassen als auch die Behörde für Umwelt und Gesundheit über das dabei erzielte Ergebnis unterrichten.

5.3 Pflegedokumentation bei pflegen & wohnen

Die Risikoanalyse wurde entgegen der gesetzlichen Anforderung erst nach der Produktionsaufnahme erstellt. Weitere Datenschutzanforderungen sind noch offen.

Mit einem neuen EDV-Verfahren will pflegen & wohnen die Probleme lösen, die mit der bisher eingesetzten Software in der Pflegedokumentation und bei der Abrechnung mit den Bewohnern und Kostenträgern auftraten. Hierfür soll in dem Unternehmen eine veränderte Organisationsstruktur und eine neue IT-Landschaft geschaffen werden (vgl. 17.TB, 6.7). Da im Rahmen der Pflegedokumentation zahlreiche zum Teil sehr sensible personenbezogene Daten verarbeitet werden, sind vor der Entscheidung über die Einführung des Verfahrens eine Risikoanalyse und Vorabkontrolle nach § 8 Abs. 4 Hamburgisches Datenschutzgesetz (HmbDSG) durchzuführen sowie die erforderlichen technischen und organisatorischen Maßnahmen zu ergreifen, um eine Gefährdung der Rechte der Betroffenen auszuschließen.

Wir haben im Rahmen der Beteiligung wiederholt eingefordert, dass in einer Risikoanalyse die Gefahren für die Rechte der Betroffenen systematisch

analysiert werden. Eine solche Ausarbeitung wurde von pflegen & wohnen jedoch erst erstellt, nachdem das Verfahren bereits produktiv genutzt wird. Die Risikoanalyse wies noch Punkte auf, bei denen das Restrisiko mit „mittel“ bzw. „mittel/hoch“ bewertet wurde.

Dieser Ablauf führt dazu, dass wichtige Sicherungsmaßnahmen erst während der Produktionsphase datenschutzgerecht geplant und umgesetzt werden können. Dies ist nicht hinnehmbar, da in der Pflegedokumentation sehr sensible personenbezogene Daten verarbeitet werden und ein erhebliches Risiko besteht, dass die Vertraulichkeit der verarbeiteten Daten nicht gewährleistet werden kann. So wurde beispielsweise im Berichtszeitraum das Administrationskonzept erst auf Grund unserer Anforderung dahingehend geändert, dass die einzelnen Administratoren nur noch die erforderlichen Berechtigungen erhalten. Administratoren, die die Berechtigungen vergeben, haben nach der Änderung keinen Zugriff mehr auf die Echtdaten der Bewohner.

Weitere konzeptionelle Festlegungen wie das Archiv- und Löschkonzept liegen immer noch nicht vor. Wir werden darauf drängen, dass zum einen die noch offenen Punkte umgehend geklärt und entsprechende technische und organisatorische Maßnahmen ergriffen werden. Zum anderen wird es darum gehen, dass bei weiteren Projekten von pflegen & wohnen der Datenschutz entsprechend den gesetzlichen Anforderungen im gesamten Projektablauf von vornherein umfassend berücksichtigt wird.

6. Bildung

6.1 Neues Datenbanksystem bei der Hamburger Volkshochschule

An der Sicherstellung des Datenschutzes muss noch gearbeitet werden.

Seit 1999 betreibt die Hamburger Volkshochschule (VHS) die Einführung eines neuen Seminarverwaltungsprogrammes, mit dem zahlreiche personenbezogene Daten von Dozenten, Mitarbeitern und Teilnehmern verarbeitet werden. Die Daten zeichnen sich durch eine unterschiedliche Sensibilität aus; beispielsweise wird festgehalten, wo die Personen wohnen, welche Kurse im einzelnen belegt worden sind und früher belegt wurden und welche Honorarsätze vereinbart worden sind.

Unsere nach §23 Abs. 4 Satz 2 Hamburgisches Datenschutzgesetz (HmbDSG) erforderliche Beteiligung erfolgte von Beginn an nur sehr schleppend. Wiederholt mussten wir die Beantwortung datenschutzrechtlich relevanter Fragen nicht nur bei der Projektleitung, sondern auch bei der Geschäftsführung der VHS anmahnen. Hinzu kommt, dass das neue Datenbanksystem bereits in Produktion gegangen war, ohne dass vorher die nach dem Hamburgischen Datenschutzgesetz vorgeschriebenen Untersuchungen durch die VHS vorgenommen und abgeschlossen worden waren. Eine deswegen von uns erwogene datenschutzrechtliche Beanstandung nach §25

HmbDSG konnte die VHS letztlich noch abwenden, weil sie glaubhaft versicherte, den datenschutzrechtlichen Aspekten zukünftig den gebotenen Stellenwert beizumessen.

Danach hat uns die VHS zügiger in die weiteren Planungen eingebunden. Insbesondere liegt uns nun ein Berechtigungskonzept vor, das allerdings noch datenschutzrechtliche Defizite aufweist. Es mangelt beispielsweise noch an einer eindeutigen Festlegung, wer aus welchen Gründen in welcher Funktion und mit welchen Rechten auf welche Daten zugreifen darf. Wir haben deshalb die VHS dringend gebeten, entsprechende Nachbesserungen kurzfristig vorzunehmen.

Datenschutzrechtlich ebenfalls bedenklich ist, dass die VHS ein Duplikat der Datenbank für Testzwecke einsetzt, ohne den Personenbezug der Daten zu entfernen. Ziel und Zweck des Testens ist es, vorhandene Fehler im Verfahren aufzudecken und zu lokalisieren, die Fehlerursache zu ermitteln und notwendige Berichtigungen zu veranlassen. Testarbeiten sind grundsätzlich mit zu diesem Zweck erstellten Testfällen durchzuführen, welche systematisch erstellt werden sollten. Testfälle sind in der Regel speziell für den Test konstruierte Fälle (Berücksichtigung von Plausibilitäten, Grenzwerten, Verfahrenssicherungen). Werden echte Fälle als Testfälle verwendet, ist sicherzustellen, dass die dabei verwendeten Daten so verfremdet werden, dass sie keine Originaldaten mehr sind bzw. kein Personenbezug mehr besteht.

Unter Anlegung besonders restriktiver Maßstäbe können den für den Test verantwortlichen Stellen ausnahmsweise Kopien von Originaldaten in Testdatenbeständen zur Verfügung gestellt werden, um damit in der Entwicklung oder Pflege befindliche, noch nicht freigegebene Anwendungsprogramme zu prüfen. Eine Übertragung von sensiblen Daten wie z.B. personenbezogenen Daten ist für diese Testzwecke jedoch grundsätzlich ausgeschlossen.

Die Diskussion mit der VHS über die noch offenen datenschutzrechtlichen Fragen dauerte bis zum Redaktionsschluss an. Über den weiteren Fortgang werden wir berichten.

6.2 Projekt Hoch7 der Universität Hamburg

Die Hochschulen gehen neue Wege in der Zusammenarbeit, bei der die Datenschutzanforderungen einzuhalten sind.

Die Universität Hamburg, die Fachhochschule Hamburg, die Hochschule für bildende Künste, die Hochschule für Musik und Theater, die Technische Universität Hamburg-Harburg sowie die Staats- und Universitätsbibliothek Carl von Ossietzky sind bereits seit November 2000 durch ein Kooperationsabkommen im Hamburger Hochschul-Kooperations-Modell (HHKM) verbunden. Gemeinsames Ziel ist es, das kaufmännische Rechnungswesen auf der Grundlage der integrierten Standardsoftware SAP R/3 einzuführen. Zur

Planung und Realisierung dieses IuK-Vorhabens haben die Hochschulen das Projekt Hoch7 eingesetzt. Eine Produktionsaufnahme des SAP-Systems ist für den Januar 2003 vorgesehen.

Unsere nach §23 Abs. 4 Satz 2 Hamburgisches Datenschutzgesetz (HmbDSG) erforderliche Beteiligung erfolgte leider erst zu einem bereits fortgeschrittenen Planungsstand und hat sich bisher auf Fragen zur Netzarchitektur sowie das Berechtigungskonzept konzentriert. Wir werden das Projekt weiter begleiten, wobei neben den zentralen Konzeptionen des Projektes die individuelle, d.h. die hochschulspezifische Ausgestaltung des Verfahrens zu betrachten sein wird. Dabei werden wir sorgfältig darauf achten, dass die Hochschulen die datenschutzrechtlichen Anforderungen, die bei einer solchen komplexen Verfahrensentwicklung zu beachten sind, auch umsetzen.

7. Verfassungsschutz

Änderung des Hamburgischen Verfassungsschutzgesetzes

Bei den neuen landesrechtlichen Regelungen auf dem Gebiet des Verfassungsschutzes hätte eine stärkere Gewichtung der Freiheitsrechte und der Privatsphäre unverdächtiger Personen nahe gelegen.

Am 27. November 2002 hat die Bürgerschaft das Gesetz zur Änderung von Vorschriften auf dem Gebiet des Verfassungsschutzes beschlossen. Dabei wurde der Gesetzentwurf, den der Senat am 10. September 2002 vorgelegt hatte, nach einer Sachverständigenanhörung im Rechtsausschuss und auf Grund massiver öffentlicher Kritik in wesentlichen Punkten nachgebessert. Diese Kritik, die über die Grenzen Hamburgs hinaus Beachtung fand, ging insbesondere auf unsere Presseerklärung vom 19. September 2002 und unsere Stellungnahme gegenüber dem Innen- und Rechtsausschuss der Bürgerschaft zurück (s. o. 2.3).

Die Novelle zum Hamburgischen Verfassungsschutzgesetz (HmbVerfSchG), zum Hamburgischen Sicherheitsüberprüfungsgesetz (HmbSÜG) und zum Ausführungsgesetz zu Artikel 10 Grundgesetz dient dem Ziel, das Landesrecht an das Terrorismusbekämpfungsgesetz des Bundes vom 9. Januar 2002 (vgl. 18. TB, 6.1, 17.1, 19.1, 19.2) anzupassen.

Die Vorschriften zur akustischen und optischen Überwachung in Wohnungen gehen im Interesse der inneren Sicherheit allerdings deutlich über die Rechtslage im Bund hinaus. Wohnungstechnische Eingriffe dürfen sich nach den neuen Bestimmungen grundsätzlich auch gegen Personen richten, die selbst nicht im Verdacht stehen, an der Planung oder Begehung einer terroristischen oder einer sonstigen schweren extremistischen Straftat aktiv mitzuwirken. Eine Ausnahme gilt lediglich für Geistliche, Ärzte, Rechtsanwälte, Steuerberater, Journalisten und andere Berufsgeheimnisträger, denen die Strafprozess-

ordnung (StPO) ausdrücklich ein Zeugnisverweigerungsrecht zubilligt. Die Angehörigen dieser Berufsgruppen müssen heimliche technische Überwachungsmaßnahmen in ihren Räumen nur hinnehmen, wenn sich auf Grund bestimmter Tatsachen ein Verdacht gegen sie richtet. Diese Regelung, die erst nach lebhaftem Protest der Kirchen, Berufsverbände und Gewerkschaften mit unserer Unterstützung abweichend vom Gesetzentwurf des Senats durchgesetzt werden konnte, ist zu begrüßen. Auch ohne ausdrückliche Regelung im Gesetz können die Mitglieder anderer Berufsgruppen (z.B. Heilpraktiker, Krankenpfleger) mit Rücksicht auf besondere Vertrauensverhältnisse und den Grundsatz der Verhältnismäßigkeit im Einzelfall von wohnungstechnischen Eingriffen ausgenommen bleiben.

Der verdeckte Einsatz besonderer technischer Mittel in Wohnungen nicht verdächtiger Personen setzt eine „unmittelbar bevorstehende Gefahr“ voraus. Diese Formulierung, die auf einem Änderungsantrag der Koalitionsfraktionen beruht, knüpft an die Gefahrenschwelle des Polizeirechts an. Das Gesetz über die Datenverarbeitung der Polizei erlaubt wohnungstechnische Eingriffe nur zur Abwehr einer unmittelbar bevorstehenden Gefahr für Leib, Leben oder Freiheit einer Person. Die Anhebung der Gefahrenschwelle gegenüber dem Gesetzentwurf des Senats weist zwar in die richtige Richtung. Allerdings hätte bei den Eingriffsvoraussetzungen auch danach differenziert werden müssen, ob die Tätigkeit als Nachrichtenmittler für Verdächtige nur gelegentlich oder in erheblichem Umfang ausgeübt wird.

Das Landesamt für Verfassungsschutz (LfV) erhält, entsprechend den Vorschriften im Terrorismusbekämpfungsgesetz, umfangreiche Auskunftsbefugnisse gegenüber Kreditinstituten, Finanzdienstleistungsinstituten, Finanzunternehmen, Luftfahrtunternehmen sowie Unternehmen in den Bereichen Post, Telekommunikation und Teledienste. Zur Durchsetzung seiner Auskunftsersuchen stehen dem LfV allerdings keine Zwangs- und Vollstreckungsbefugnisse gegenüber den Unternehmen zu. Zur Lokalisierung des Standorts von Mobilfunkgeräten und für die Vorbereitung von Maßnahmen zur inhaltlichen Überwachung der Telekommunikation darf das LfV den IMSI – Catcher einsetzen.

Die Wahrnehmung der neuen Auskunftsbefugnisse und die Verwendung des IMSI – Catchers unterliegen der parlamentarischen Kontrolle durch die G 10 – Kommission der Bürgerschaft. Wir konnten erreichen, dass uns im Zuständigkeitsbereich der G 10 – Kommission ein selbstständiges Kontrollrecht gegenüber dem LfV eingeräumt wurde, das wir unabhängig von einem Ersuchen oder Auftrag der Kommission ausüben können. Diese Kontrollbefugnis dient nicht der personenbezogenen Überprüfung bestimmter Vorgänge, sondern der Gewinnung struktureller Erkenntnisse und Aussagen zur Datenverarbeitungspraxis des LfV. Darüber werden wir der G 10 – Kommission berichten, um eine aussagefähige Grundlage für die gesetzlich vorgeschriebene Erfolgskontrolle (Evaluierung) hinsichtlich der neuen Befugnisse des LfV zu gewinnen.

8. Polizei

Rasterfahndung

Nach den Rasterfahndungen im Herbst 2001 hat die Polizei ein Jahr lang alle herausgerasterten Personen in einer Datei gespeichert. Erst im Dezember 2002 und Januar 2003 werden die weitaus meisten Datensätze 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. Sie benennt für Rasterfahndungen sowohl gemäß § 98 a Strafprozessordnung (StPO) als auch gemäß § 23 des Gesetzes über die Datenverarbeitung der Polizei (PolDVG) die zu beachtenden Verfahrensschritte und soll kurz nach Redaktionsschluss in Kraft treten.

Im Berichtszeitraum haben wir die Datenübermittlungen durch Einwohnermelde- und Ausländerdienststellen sowie Hochschulen an die Polizei anlässlich der Rasterfahndungen im Herbst 2001 überprüft. 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) hat 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 werden bei rund 95 % der Trefferfälle die Personen über die bisherige Speicherung vom LKA unterrichtet und die Datensätze gelöscht.

§ 23 PolDVG

Absatz 3 Satz 1

Ist der Zweck der Maßnahme erreicht oder zeigt sich, dass er nicht erreicht werden kann, sind die übermittelten und im Zusammenhang mit der Maßnahme zusätzlich angefallenen Daten zu löschen und die Akten zu vernichten, soweit sie nicht für ein mit dem Sachverhalt zusammenhängendes Verfahren erforderlich sind.

Absatz 5

Nach Durchführung des Abgleichs sind die von weiterführenden polizeilichen Maßnahmen betroffenen Personen hiervon zu unterrichten, soweit dadurch nicht die Erfüllung polizeilicher Aufgaben vereitelt oder erheblich gefährdet würde oder sich an den auslösenden Sachverhalt ein strafrechtliches Ermittlungsverfahren anschließt.

Im Hinblick auf § 23 Abs. 3 und 5 PolDVG erscheint es nicht unproblematisch, dass die Polizei erst Ende 2002 im Wesentlichen gleichzeitig die meisten Betroffenen benachrichtigt und ihre Datensätze löscht. 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 feststeht, 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 können wir jedoch zurückstellen, da für diese große Personengruppe mit den Benachrichtigungen und Löschungen die bislang andauernden Grundrechtseingriffe insgesamt beendet werden.

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 anschließenden Änderung des Landesrechts hat dort ein neuer Versuch einer Rasterfahndung erst Mitte September 2002 begonnen und ist zwischenzeitlich erneut gerichtlich gestoppt worden. 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.

9. Strafvollzug

Übersendung von Gefangenenpersonalakten an die Ausländerbehörde

Wir konnten erreichen, dass Gefangenenpersonalakten der Ausländerbehörde nur in geeigneten Fällen und unter Beachtung des Grundsatzes der Verhältnismäßigkeit zugänglich gemacht werden.

Mit dem Einwohner – Zentralamt (EZA) der Behörde für Inneres (BfI), dem Strafvollzugsamt und der Justizvollzugsanstalt (JVA) Glasmoor haben wir eingehend die Voraussetzungen, den Umfang und das Verfahren der Übersendung von Gefangenenpersonalakten (GPA) erörtert, die dem EZA als

Ausländerbehörde zur Vorbereitung von Ausweisungsentscheidungen dienen sollen. In der Diskussion haben wir unterstrichen, dass es nach dem Strafvollzugsgesetz (StVollzG) unzulässig ist, dem EZA auf ein bloßes Stichwort wie „Ausweisung“ hin die vollständige GPA zu übermitteln und damit die datenschutzrechtliche Verantwortung allein dem EZA zuzuweisen.

Mit den beteiligten Stellen konnten wir uns schließlich auf folgendes Verfahren verständigen: Das EZA legt in seinem Ersuchen den Zweck der Aktenanforderung näher dar. Hierfür kann ein mit uns abgestimmtes Formschreiben verwendet werden. Auf dieser Grundlage prüft die JVA, ob die GPA für den angegebenen Zweck überhaupt einschlägige Erkenntnisse vermitteln kann.

Von Bedeutung ist dies insbesondere für anerkannte Asylberechtigte, die einen besonderen Ausweisungsschutz genießen, und für türkische Staatsangehörige mit assoziationsrechtlichem Aufenthaltsrecht. Bei diesen Personen kommt eine Ausweisung nur in Betracht, wenn die konkrete Gefahr neuer erheblicher Straftaten besteht. Die JVA muss vor der Aktenübersendung klären, ob die GPA hinreichende Anhaltspunkte für eine konkrete Wiederholungsgefahr enthält. Besondere Zurückhaltung bei der Annahme von Wiederholungsgefahr ist insbesondere dann angezeigt, wenn die Vollstreckung des Restes der Freiheitsstrafe zur Bewährung ausgesetzt wurde, da bei dieser Entscheidung das Sicherheitsinteresse der Allgemeinheit und das Verhalten des Verurteilten im Strafvollzug bereits zu berücksichtigen waren.

Ferner muss die Übersendung der GPA auf den für den Zweck des Ersuchens erforderlichen Umfang beschränkt bleiben. Sind die für das EZA wesentlichen Informationen in bestimmten Gutachten oder Berichten zusammengefasst, so sind nur die entsprechenden Aktenteile zu übermitteln.

10. Gesundheit

Prüfung des Zentralinstituts für Transfusionsmedizin

Durch eine Prüfung des Zentralinstituts für Transfusionsmedizin (ZIT) konnten einige Verbesserungen der Datensicherheit erreicht werden.

Im April 2002 führten wir eine datenschutzrechtliche Prüfung des ZIT, der zentralen Blutspendeeinrichtung des Landesbetriebs Krankenhäuser (LBK), durch. Das Institut verarbeitet jährlich 70.000 Vollblutspenden und kauft Blutprodukte von weiteren 20.000 Vollblutspenden aus Norddeutschland hinzu. Die Datenverwaltung erfolgt seit 1996 über die Schweizer Spezialsoftware BLUES.

Besondere Aufmerksam richteten wir auf die Datenerhebung durch den Blutspendebogen, enthält er doch sehr sensible Angaben z.B. über die Zugehörigkeit zu einer besonderen Risikogruppe oder über einen Intimkontakt mit einer Person einer Risikogruppe. Diese bezieht sich auf mögliche Infektionen durch

HIV und Hepatitis B oder C. Trotz der hohen Sensibilität dieser Daten haben wir uns von ihrer Erforderlichkeit für eine sichere Blutspende überzeugen lassen.

Zu konkretisieren war jedoch die zu allgemein gefasste Einwilligungserklärung im Blutspendebogen für „wissenschaftliche Untersuchungen an den mir entnommenen Blutproben". In Zukunft willigt der Spender darin ein, dass „...auch Untersuchungen zum Zweck der Qualitätssicherung (z.B. Bildung von Kontroll-Kollektiven) in anonymer Form durchgeführt werden können".

Angesichts der hohen Schutzbedürftigkeit der Blutspendebogen-Daten vereinbarten wir mit dem ZIT ein sicheres Ablageverfahren für die Bogen: Die bei der Prüfung vorgefundene Lagerung in offenen Kartons in einem nicht besetzten Nebenraum mit offener Tür wird durch einen stabilen verschließbaren Schlitz-Kasten ersetzt.

Die Daten von Personen, die dauerhaft von einer Blutspende ausgeschlossen werden, werden in Zukunft gelöscht, es sei denn, dass Blutprodukte aus früheren Spenden bis zum Blutspender zurückverfolgt werden müssen.

Schließlich einigten wir uns mit dem ZIT auf eine Verbesserung der Benutzerkennungs-Verwaltung, auf die Implementierung einer datenschutzgerechten Archivierungsfunktion in BLUES und auf eine Verschlüsselung der Daten, die zwischen den einzelnen Stellen des ZIT übermittelt werden.

Insgesamt trafen wir auf durchaus datenschutzbewusste und -freundliche Mitarbeiter. Mit der Zentralisierung der Datenschutzkontrolle im LBK gab die bisherige betriebliche Datenschutzbeauftragte des ZIT ihre Aufgaben an die betriebliche Datenschutzbeauftragte des LBK ab.

11. Forschung

Forschungsprojekt „Gesundes Altern"

Unsere Beratung des Genforschungsprojekts „Gesundes Altern" konnte erreichen, dass die weitere Verarbeitung der Probandendaten in nicht personenbezogener Form erfolgt.

Durch eine Mitteilung des Melderegisters über eine Gruppenauskunft erfuhren wir von einem interessanten Forschungsprojekt: Ein Hamburger Krankenhaus und die Universitätsklinik Kiel erheben von hochbetagten Personen (ab 80 bzw. 90 J.) Gesundheits- und Lebensqualitätsdaten per Fragebogen und untersuchen ihr Blut nach möglichen genetischen Dispositionen für das hohe Alter. Das Projekt hat eine Laufzeit von „zunächst 10 Jahren" und strebt einen möglichst großen Proben- und Gendatenpool von sehr alt gewordenen und im wesentlichen gesund gebliebenen Menschen an.

Die Unterlagen für dieses bereits begonnene „Aging-Projekt“ sahen vor, dass die Probanden im Fragebogen ihre Initialen, das volle Geburtsdatum und darüber hinaus den Namen sowie die Adresse von Geschwistern eintragen und in der Einwilligungserklärung Name und Geburtsdatum nennen. Beide Papiere versah das Krankenhaus dann mit derselben laufenden Code-Nummer für die jeweilige teilnehmende Person. Mit dieser Nummer wurde auch die Blutprobe kennzeichnet. Die Erfassung im Computer erfolgte ebenfalls über diese Codenummer.

Die Fragebogen und Einwilligungserklärungen sollten über die ganze Laufzeit des Projekts aufbewahrt werden, um bei Bedarf eine personenbeziehbare Nachvollziehbarkeit der Forschungsergebnisse zu gewährleisten. Die Papierbögen dienten dabei als Schlüsselliste für die Codenummer der Blutprobe und des EDV-Datensatzes.

Bei unserer datenschutzrechtlichen Beratung stellte sich heraus, dass nach der Erfassung der Daten für das Forschungsprojekt ein Personenbezug der Angaben und Proben gar nicht erforderlich war. Weder war eine spätere Kontaktaufnahme mit den Probanden vorgesehen noch sollten später erhobene Daten den bisher gespeicherten zugeordnet werden.

Durch verschiedene Gespräche und Briefwechsel mit der Universitätsklinik Kiel und dem Hamburger Krankenhaus konnten wir folgende Modifikationen des Verfahrens erreichen:

- Nur noch die Einwilligungserklärung enthält die Personalien des Probanden. Bei einer wissenschaftlichen Forschungskontrolle können hiermit die an der Untersuchung beteiligten Probanden ermittelt (und ggf. befragt) werden.
- Der Fragebogen, die Probe und der EDV-Datensatz werden ausschließlich mit derselben Codenummer gekennzeichnet. Diese Einweg-Pseudonymisierung lässt einen Rückschluss auf die Probandenidentität nicht mehr zu.
- Die Angabe der Personalien von teilnahmebereiten Geschwistern erfolgt auf einem gesonderten Blatt, das nach Kontaktaufnahme vernichtet wird.

Angesichts der Laufzeit des Projekts und der Sensibilität der verarbeiteten Daten bedeuten diese Änderungen eine erhebliche Verbesserung des Datenschutzes, ohne dass das Ziel des Forschungsprojekts beeinflusst wurde. Die Richtlinien für die Wissenschaftskontrolle können eine personenbezogene Nachvollziehbarkeit aller Forschungsergebnisse nicht erzwingen, wenn das Forschungsprojekt selbst einen Personenbezug nicht erfordert. In diesen Fällen gilt vielmehr das gesetzliche Gebot der Datensparsamkeit und Datenvermeidung, wie §§ 3a, 40 Bundesdatenschutzgesetz und §§ 5 Abs. 4, 27 Abs. 3 Hamburgisches Datenschutzgesetz es umschreiben.

12. Finanzen und Steuern

Angabe der Steuernummer auf Rechnungen

Durch gesetzliche Regelungen werden Steuernummern einem größeren Personenkreis zugänglich, so dass zur Wahrung des Steuergeheimnisses zusätzliche Maßnahmen erforderlich werden.

Durch das Steuerverkürzungsbekämpfungsgesetz vom 27. Dezember 2001 (BGBl. I S. 3922) ist der § 14 Umsatzsteuergesetz (UStG) um einen Absatz 1a ergänzt worden, wonach der leistende Unternehmer in Rechnungen, die ab 1. Juli 2002 ausgestellt sind, die ihm vom Finanzamt erteilte Steuernummer anzugeben hat. Diese Verpflichtung soll die Überprüfung von Lieferketten erleichtern und beschleunigen und somit zur verstärkten Bekämpfung des Umsatzsteuerbetruges und Wahrung der Steuergerechtigkeit beitragen.

Bisher konnte davon ausgegangen werden, dass aufgrund des Steuergeheimnisses die Steuernummer nur dem jeweiligen Steuerpflichtigen bzw. seinem steuerlicher Vertreter (z.B. Steuerberater) bekannt ist, so dass das Finanzamt nach Nennung der Steuernummer problemlos telefonische Auskünfte an diese Berechtigten erteilen konnte. Durch diese neue Regelung findet aber eine „breitere“ Streuung der Steuernummer statt, so dass die Gefahr besteht, dass auch Unberechtigte (z.B. Kunden, Geschäftspartner) versuchen könnten, auf diese Weise steuerrelevante Auskünfte über den Leistenden beim zuständigen Finanzamt einzuholen, und diese auch erhalten.

Die gleiche Problematik ergibt sich auch durch den § 48 b Abs. 6 Einkommensteuergesetz (EStG), der durch das Steueränderungsgesetz 2001 vom 20. Dezember 2001 (BGBl. I S. 3794) angefügt wurde. Danach erteilt das Bundesamt für Finanzen dem Leistungsempfänger im Wege einer elektronischen Abfrage Auskunft über die beim Bundesamt für Finanzen gespeicherten Freistellungsbescheinigungen. Hierzu gehört u.a. auch die Steuernummer.

Wir haben daher die Finanzbehörde Hamburg gebeten, die Beschäftigten der Finanzämter auf die Gefahr einer leichteren Zugänglichkeit der Steuernummer und damit auf die mögliche Durchbrechung des Steuergeheimnisses gegenüber unberechtigten Anrufern hinzuweisen und Anweisungen zu erlassen, wie die Berechtigung des Anrufers sichergestellt werden kann. Auch andere Datenschutzbeauftragte haben ihre Finanzverwaltungen um entsprechende Anweisungen gebeten.

Die Finanzbehörde Hamburg – Steuerverwaltung – hat unsere Auffassung geteilt, so dass die Oberfinanzdirektion (OFD) Hamburg in Absprache mit der Finanzbehörde vorsorglich am 18. April 2002 eine Verwaltungsanweisung herausgegeben hat, in der diese Problematik und die sich daraus ergebenden Verhaltensweisen erläutert werden.

Nach dieser OFD-Verfügung dürfen geschützte Verhältnisse eines Steuerpflichtigen einer unbekannten Person anlässlich eines Telefonanrufs nicht schon aufgrund der Nennung des Namens bzw. der Firma und der entsprechenden Steuernummer offenbart werden. Sofern es sich nicht bereits aus dem Vortrag des Anrufenden ergibt, dass es sich bei ihm um den Steuerpflichtigen selbst handelt oder um seinen Bevollmächtigten oder gesetzlichen Vertreter, ist der Anrufer um zusätzliche Angaben zu bitten, die Zweifel hinsichtlich seiner Person ausschließen.

Nachdem diese Problematik verstärkt auch von den Medien und verschiedenen Verbänden (z.B. Bund der Steuerzahler) aufgegriffen worden ist, hat auch das Bundesministerium der Finanzen (BMF) das Thema aufgegriffen. Mit Schreiben vom 24. Juli 2002 hat das BMF die Obersten Finanzbehörden der Länder aufgefordert, zur Wahrung des Steuergeheimnisses sicherzustellen, dass sich die Beschäftigten der Finanzverwaltung vor der Erteilung von Auskünften am Telefon von der Berechtigung des Anrufers überzeugen.

Wir gehen davon aus, dass durch diese Verfügungen ein Missbrauch der Steuernummer weitgehend verhindert wird.

13. Ausländerwesen

Prüfung des Ausländerdaten-Systems PAULA GO!

Bei der Prüfung des modernisierten Ausländerdatensystems zeigte sich Handlungsbedarf beim Zugriffsberechtigungskonzept.

Nach der Modernisierung des alten Datenverarbeitungssystems PAULA ließen wir uns im September 2002 in der Ausländerbehörde die Funktionen der Neufassung PAULA GO! zeigen und erläutern. Mit ihr soll auch ein neues Verfahren zur Stichprobenkontrolle für Zugriffe nicht aktenführender Ausländerdienststellen umgesetzt werden, § 3 Abs. 3 Ausländerdatenverarbeitungsverordnung.

Eine datenschutzrechtliche Prüfung des Stichprobenverfahrens im Mai 2002 hatte einerseits offenbart, dass das mit der Ausländerbehörde vereinbarte Verfahren nur in einer von drei Abschnitten der zentralen Ausländerabteilung tatsächlich durchgeführt wurde. Sie hatte aber andererseits auch gezeigt, dass das Verfahren sehr aufwändig und wenig zielgenau ist. Wir hatten deswegen vorgeschlagen, von der stichprobenweisen Auswertung einer flächendeckenden Protokollierung der Datenzugriffe zu einer stichprobenweisen Protokollierung der Zugriffe mit ergänzender Begründung im Einzelfall zu wechseln.

Die Ausländerabteilung hatte dieser Anregung zugestimmt, ihre Umsetzung in PAULA GO! verzögert sich jedoch. Zunächst sollen die Fachdienststellen nach dem sinnvollen Stichprobenumfang (wie viel mal muss ein Sachbearbeiter im

Monat damit rechnen, dass sein Zugriff protokolliert und er zu einer nachvollziehbaren Begründung dafür aufgefordert wird) befragt werden. Wegen der Umstellungskosten kommt nach Auskunft der Ausländerabteilung eine Implementierung erst 2003 in Betracht.

Bei der Präsentation von PAULA GO! im September 2002 wurde deutlich, dass vor allem das Berechtigungskonzept für die Zugriffe auf die zentrale Ausländerdatenbank datenschutzrechtlich von Bedeutung ist. Den verschiedenen Funktionseinheiten in den Ausländerabteilungen (z.B. Visum, Abschiebungen, Poststelle) werden bestimmte Zugriffsberechtigungen (z.B. Suchvorgang mit Ausländerzentralregister-Auskunft, Aufenthaltstitel, Einbürgerung/Wegfall) zugeordnet, die jeweils bestimmte Einzelzugriffe bündeln. Eine umfassende Datenschutzkontrolle setzt die genaue Aufgabendefinition aller Funktionseinheiten, die Ermittlung der dafür erforderlichen Datenkenntnis und die Übersicht über die jeweils in den Berechtigungen gebündelten Einzelzugriffe voraus. Angesichts der beschränkten Kapazität des Datenschutzbeauftragten haben wir uns in dieser Hinsicht Stichprobenprüfungen vorbehalten.

Die erste bezog sich bei der Vorstellung im September 2002 auf die Zugriffsrechte der Poststelle. Diese ist eine gesonderte Verwaltungsabteilung der Behörde für Inneres und zuständig für die Postverteilung an die zentrale und die bezirklichen Ausländerabteilungen. Eine solche Aufgabe erfordert jedoch keinen umfassenden Suchzugriff auf die Angaben zum Aufenthaltsstatus eines Ausländers und darüber hinaus auf die zum Teil hochsensiblen Einträge im Ausländerzentralregister. Die Ausländerabteilung teilte unsere Auffassung, dass ein solcher Zugriff unzulässig ist, und sagte zu, für die Poststelle eine eigene Zugriffsberechtigung mit stark reduzierten Rechten zu konzipieren.

14. Bauen, Wohnen und Wirtschaftsverwaltung

Selbstauskünfte aus dem Gewerbezentralregister

Der Gesetzgeber hat die erforderlichen gesetzlichen Grundlagen für Auskünfte und Selbstauskünfte aus dem Bundeszentralregister und dem Gewerbezentralregister bei der öffentlichen Auftragsvergabe geschaffen.

Am 1. August 2002 ist das Gesetz zur Erleichterung der Bekämpfung von illegaler Beschäftigung und Schwarzarbeit in Kraft getreten (BGBl. I S. 2787). Nach Art. 9 (Gesetz zur Bekämpfung der Schwarzarbeit) sowie Art. 12 (Arbeitnehmer-Entsendegesetz) und Art. 11 (Gewerbeordnung) können die öffentlichen Auftraggeber im Rahmen der Vergabe von Bauaufträgen oder anderen Leistungen Auskünfte des Bundeszentralregisters gemäß § 30 Abs. 5, § 31 Bundeszentralregistergesetz und des Gewerbezentralregisters gemäß § 150a Gewerbeordnung über rechtskräftige Bußgeldentscheidungen wegen einer Straftat oder Ordnungswidrigkeit einholen. Sie können statt dessen auch vom

Bewerber die Vorlage entsprechender Auskünfte aus dem Bundeszentralregister oder Gewerbezentralregister verlangen, die nicht älter als drei Monate sein dürfen.

Mit diesen Regelungen ist die von uns im 16. TB (10.3) und 18. TB (15.2) aufgezeigte Problematik, dass im Rahmen der Vergabe öffentlicher Bauaufträge von Bewerbern und Bietern zum Nachweis ihrer Zuverlässigkeit eine Selbstauskunft aus dem Gewerbezentralregister verlangt wird, nunmehr datenschutzkonform gelöst worden.

15. Personaldaten

Outsourcing für Beihilfe und Versorgungsleistungen

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

Der Senat prüft, ob bestimmte Aufgaben an private Stellen ausgelagert werden können. Aus datenschutzrechtlicher Sicht sind dabei die Überlegungen zur Auslagerung der Bearbeitung von Beihilfe 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
- 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.

Wenn eine Übermittlung der Daten von Beschäftigten an nicht öffentliche Stellen erfolgen soll, ist sie nach § 28 Abs. 4 HmbDSG 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.

Diese Zulässigkeitstatbestände finden keine Anwendung bei der Auslagerung der Bearbeitung von Beihilfe und Versorgungsleistungen.

Zulässig ist eine Übermittlung auch, 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.

Datenschutz im nichtöffentlichen Bereich

16. Videoüberwachung

16.1 Videoüberwachung der Hamburger U-Bahnen

Nach Abschluss des Testversuchs plant die Hamburger Hochbahn AG (HHA) in den kommenden Jahren die flächendeckende Ausstattung aller U-Bahn-Züge mit Videoaufzeichnungsanlagen unter Beachtung datenschutzgerechter Auflagen.

Wir haben als Aufsichtsbehörde für den Datenschutz zu dem von der HHA vorgestellten Konzept Stellung genommen und halten das Vorhaben bei Beachtung konkret definierter datenschutzrechtlicher Auflagen für vertretbar. Die HHA hat zugesagt, diese Auflagen zu beachten.

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

In den kommenden Jahren sollen nun über den bisherigen Testbetrieb hinaus (vgl. 18. TB, 25.3.2) alle weiteren U-Bahn-Züge mit Videokameras und digitalen Aufzeichnungsgeräten ausgerüstet werden. Einer der Gründe ist, dass die Zahl der Sachbeschädigungen im Zeitraum des Testversuchs in den überwachten Wagen praktisch völlig zurückgegangen ist.

Die Videoaufzeichnung erfolgt durch zwei Kameras pro Wagen auf ein zentrales, digitales Aufzeichnungsgerät je Fahrzeug. Die Datenaufzeichnungen werden nach 24 Stunden automatisch überschrieben, falls die Aufnahmen nicht wegen eines Schadensfalls sichergestellt und ausgewertet werden. Dies ist der Fall, wenn Fahrgäste eine Meldung machen oder Schäden in 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. An den überwachten Wagen ist ein Hinweisschild mit dem Text „Dieser Wagen wird zu Ihrer Sicherheit videoüberwacht“ angebracht.

Wir werden die weitere Entwicklung des Vorhabens datenschutzrechtlich begleiten.

16.2 Videoüberwachung an einem Gebäude

Datenschutzrechtliche Mängel bei einer Videoüberwachung von öffentlich zugänglichen Räumen sind beseitigt worden.

In einem in Hamburg-Bergedorf befindlichen Gebäude ist eine Videoüberwachungsanlage installiert worden, mit der eine Hausfassade dieses Gebäudes und Teile des angrenzenden öffentlichen Weges überwacht werden sollen.

Damit sollen die seit Jahren zunehmenden Störungen, die von Personen an der Hausfassade durch unbefugtes Plakatieren oder mutwillige Farbschmierereien ausgehen, festgestellt und dokumentiert werden. Die Identifizierung der potentiellen Täter soll eine Aufklärung derartiger Delikte durch die Ermittlungsbehörden erleichtern.

Die Prüfung der Videoüberwachungsanlage hat ergeben, dass

- die konkreten Zwecke der Anlage nicht festgelegt worden sind,
- die Passanten, die den öffentlichen Weg benutzen, nicht auf den Umstand der Videoüberwachung hingewiesen wurden (z.B. durch Schilder),
- die organisatorischen und technischen Maßnahmen zur Ausführung der Vorschriften des Bundesdatenschutzgesetzes (BDSG) hinsichtlich der Zutritts-, Zugangs- und Zugriffskontrolle zu den zentralen Komponenten der Videoüberwachungsanlage (z.B. Videorecorder, Monitor) unzureichend waren,
- die Speicherdauer (ca. 96 Std.) der Videoaufnahmen als unverhältnismäßig lang anzusehen war.

Da weder eine konkrete Festlegung des Zweckes gemäß § 6b Abs. 1 BDSG noch Hinweise auf die Videoüberwachung gemäß Absatz 2 erfolgt und keine bzw. nur unzureichende technische und organisatorische Datenschutzmaßnahmen gemäß § 9 BDSG getroffen worden sind, fehlen die Zulässigkeitsvoraussetzungen für den ordnungsgemäßen Betrieb einer Videoüberwachungsanlage von öffentlich zugänglichen Räumen. Aus diesem Grund war diese Videoüberwachungsanlage datenschutzrechtlich als unzulässig anzusehen.

Wir haben daher der verantwortlichen Verwaltungsgesellschaft mitgeteilt, dass auf die Videoüberwachungsanlage insgesamt zu verzichten und die Anlage zu demontieren ist, wenn nicht die von uns dargestellten Voraussetzungen innerhalb einer angemessenen Frist noch erfüllt werden. Die Verwaltungsgesellschaft hat auf eine entsprechende Nachbesserung verzichtet und den Abbau der Videoüberwachungsanlage vorgezogen.

17. Medizinische Dienstleistungen

Prüfung eines privaten Labors für klinische Prüfungen

Die Prüfung eines privaten Labors führte zu einer Verbesserung der Datenschutzorganisation und des Schutzes von Probandendaten.

Das geprüfte Labor führt im Auftrag von Arzneimittel- und Kosmetikherstellern klinische Prüfungen an Probanden durch. Grundlage ist jeweils eine allgemeine und eine für jede Prüfung gesonderte Einwilligung. Neben einer Probandenakte führt das Labor für jede klinische Prüfung eigene Prüfungsbogen (sog. Case Report Forms, CRF). In einem EDV-System verwaltet es die Patientenstammdaten und wertet die Prüfungsergebnisse aus. In den CRF werden Probandendaten an die Auftraggeber übermittelt, besondere Beauftragte des Auftraggebers und – im Ausnahmefall – Aufsichtsbehörden erhalten Akteneinsicht.

Die Prüfung ergab zunächst, dass weder ein betrieblicher Datenschutzbeauftragter bestellt noch eine Meldung nach § 4 d BDSG (Fallgruppe: automatisierte Datenverarbeitung zum Zweck der anonymisierten Übermittlung) erfolgt war. Dies wurde unverzüglich nachgeholt. Kritisieren mussten wir auch eine unzureichende Pseudonymisierung der CRFs bei ihrer Übermittlung an die Auftraggeber: Sie enthielten neben einer Codenummer und den Initialen der Probanden regelmäßig das vollständige Geburtsdatum. Dies widersprach nach unserer Auffassung § 40 des Arzneimittelgesetzes (AMG), der eine nicht personenbezogene Übermittlung an die Auftraggeber vorsieht. In Zukunft ersetzt das Labor das Geburtsdatum durch das Alter der Probanden. Für die Auftraggeber erscheint damit eine Reidentifizierung hinreichend ausgeschlossen.

Die Aufbewahrungsfrist für Probandenakten wird entsprechend unserer Forderung nun differenziert: Die Daten von Personen, die bereits nach Ausfüllung des Anamnesebogens und einem Informationsgespräch als Probanden ausscheiden, werden nicht in die Datei aufgenommen und unverzüglich vernichtet. Unterlagen von Probanden, die an einer medizinischen Eignungsuntersuchung, aber an keiner klinischen Prüfung teilgenommen haben, werden nach 2 Jahren vernichtet bzw. gelöscht. Die Unterlagen von Teilnehmer/inne/n an klinischen Prüfungen müssen dagegen nach einer europäischen Richtlinie für klinische Prüfungen 15 Jahre aufbewahrt werden.

Zu klären war schließlich, welche datenschutzrechtlichen Folgen es hat, wenn ein Proband seine Einwilligung in die Teilnahme an einer klinischen Prüfung widerruft. Auch hier war entsprechend zu unterscheiden: Bevor ein Proband als Teilnehmer einer bestimmten klinischen Prüfung dokumentiert ist, führt ein Widerruf zur Rückabwicklung der personenbezogenen Datenverarbeitung: Die Akte wird vernichtet, der EDV-Datensatz gelöscht. Ist der Proband dagegen bereits als Prüfungsteilnehmer registriert, verlangen die Wissenschaftskontrolle einerseits und der medizinische Probandenschutz andererseits, dass die erfassten personenbezogenen Daten weiter gespeichert bleiben. Uns lag besonders daran, dass die Probanden hierüber aufgeklärt werden.

Nur teilweise durchsetzen konnten wir eine Differenzierung der Zugriffsrechte der Labor-Mitarbeiter/innen. Es wurde uns plausibel vorgetragen, dass aus organisatorischen Gründen alle sachbearbeitenden Beschäftigten des Labors Zugang zu den jeweils aktuellen Akten und CRFs, nicht allerdings zum Aktenarchiv, und Zugriff auf die EDV-Daten erhalten müssen. Erreichen konnten wir dagegen eine deutliche Verbesserung der Passwortverwaltung für den EDV-Zugriff.

18. Meldepflicht und Prüftätigkeit

18.1 Meldepflicht

Zum Redaktionsschluss waren 19 Verfahren automatisierter Verarbeitungen nach § 4 d BDSG der Aufsichtsbehörde gemeldet.

18.2 Prüfungen

Im Berichtszeitraum wurden insgesamt 69 Firmen gemäß § 38 Abs. 1 BDSG geprüft. Davon waren 22 Unternehmen Anbieter von Tele- und Mediendiensten.

18.3 Bußgeldverfahren

Vier Bußgeldverfahren wurden im Berichtszeitraum durchgeführt.

Geschäftsverteilung (Stand: 1. Dezember 2002)

Der Hamburgische Datenschutzbeauftragte
Baumwall 7, 20459 Hamburg

Tel.: 040/42841-2044
Fax: 040/42841-2372

E-Mail: mailbox@datenschutz.hamburg.de
Internet-Adresse: www.hamburg.datenschutz.de

		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 Gebers	-1373-
Internationaler Datenverkehr, Auskunfteien/SCHUFA, Kreditwirtschaft	
Helga Naujok	-2556-
Versicherungswirtschaft, Handel, Industrie, Vereine	
Elisabeth Duhr	-2541-
Adresshandel/Werbung, Markt- und Meinungsforschung	
Birgit Danker	-2562-
(ab 1. 1. 2003 Annette Husten)	-1760-
Arbeitnehmerdatenschutz/Personalwesen, Auftragsdatenverarbeitung	
Evelyn Seiffert	-2468-
Meldepflicht, Transport und Verkehr, gewerbliche Dienstleistungen, Freie Berufe	
Bernd Uderstadt	-2276-

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 Multimedia und Telekommunikation

Datenschutz bei Windows NT

Datencheckheft, 6. Auflage

Mehr Service – weniger Datenschutz

Vom Bürgerbüro zum Internet

Windows 2000

Informationsblätter

Was tun wir für Sie ?

Handels- und Wirtschaftsauskunfteien

Die Gesundheits-Chipkarte

Datenschutz und Verbraucherschutz rund ums Telefon

Virtuelles Datenschutzbüro

Surfen, Klicken und Bestellen, Datenschutz und Verbraucherschutz im Internet

Datenschutz im Verein

Tipps und Informationen zu Adressenhandel und unerwünschter Werbung (Januar 2003)

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

Duhr, Naujok, Danker, Seiffert, Neues Datenschutzrecht für die Wirtschaft, DuD 1, 2001 und 1, 2003

Kühn, Schläger, Datenschutz in vernetzten Computersystemen, Datakontext-Fachverlag, 1997

Menzel, Regelungsvorschlag zur Selbstbestimmung bei genetischen Untersuchungen, DuD 3, 2002

Schaar, Datenschutz im Internet, Beck-Verlag, 2002

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

PAUL FLEMING
(1609 – 1640)

AN SICH

Sei dennoch unverzagt. Gib dennoch unverloren,
Weich keinem Glücke nicht. Steh höher als der Neid.
Vergnüge dich an dir, und acht es für kein Leid,
Hat sich gleich wider dich Glück, Ort und Zeit verschworen.

Was dich betrübt und labt, halt alles für erkoren,
Nimm dein Verhängnis an. Laß alles unbereut.
Tu, was getan muß sein, und eh man dir´s gebeut.
Was du noch hoffen kannst, das wird noch stets geboren.

Was klagt, was lobt man doch ? Sein Unglück und sein Glücke
Ist ihm ein jeder selbst. Schau alle Sachen an.
Dies alles ist in dir. Laß deinen eitlen Wahn,

Und eh du förder gehst, so geh in dich zurücke.
Wer sein selbst Meister ist und sich beherrschen kann,
Dem ist die weite Welt und alles untertan.