Landtag Brandenburg **Drucksache 3/559**
3. Wahlperiode

Neudruck

Tätigkeitsbericht 1998

des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht

Berichtszeitraum: 1. April 1998 bis 31. Dezember 1998

Dieser Tätigkeitsbericht schließt an den Sechsten Tätigkeitsbericht des Landesbeauftragten für den Datenschutz an und deckt den Berichtszeitraum vom 1. April bis zum 31. Dezember 1998 ab. In Zukunft sollen sich die Tätigkeitsberichte jeweils auf das vergangene Kalenderjahr beziehen.

Anders als seine Vorläufer ist dieser Tätigkeitsbericht nicht mehr nummeriert, sondern verweist ausschließlich auf das Berichtsjahr. Dem liegt die Entscheidung zugrunde, den 7. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz nach § 27 des Brandenburgischen Datenschutzgesetzes (Teil A) mit dem 1. Tätigkeitsbericht des Landesbeauftragten für das Recht auf Akteneinsicht nach § 11 Abs. 3 des Akteneinsichts- und Informationszugangsgesetzes vom 10. März 1998[1] (Teil B) zu verbinden. Dies ist zwar gesetzlich nicht vorgeschrieben, erscheint aber sinnvoll. Denn mit gutem Grund hat der Landesgesetzgeber dem Landesbeauftragten für den Datenschutz zugleich die Funktion eines Landesbeauftragten für das Recht auf Akteneinsicht übertragen, weil zahlreiche Berührungspunkte zwischen beiden Materien eine institutionelle Verknüpfung nahelegen. Dann aber ist es auch konsequent, über die Tätigkeit in beiden, durchaus unterschiedlichen Bereichen mit einem einheitlichen Bericht Rechenschaft abzulegen.

Dieser Bericht ist trotz der neuen Aufgabe des Landesbeauftragten für das Recht auf Akteneinsicht schlanker ausgefallen als die bisherigen Berichte des Landesbeauftragten für den Datenschutz, weil er sich auf den Ausschnitt der Prüf- und Beratungstätigkeit beschränkt, dessen öffentliche Darstellung angezeigt erscheint.

---

[1] GVBl. I S. 46

Datum des Eingangs: 24.01.2000 / Ausgegeben: 14.02.2000

Inhaltsverzeichnis Seite

Einleitung

Brandenburgs Weg in die Informationsgesellschaft

47 von je 100 Befragten im Rahmen einer Repräsentativ-Umfrage, die im vergangenen Jahr mit unserer Unterstützung durchgeführt wurde, meinten, dass in Deutschland zu wenig für den Datenschutz getan wird[1]. In Ostdeutschland lag dieser Prozentsatz mit 57 Prozent sogar erheblich höher als in Westdeutschland (45 Prozent). 56 Prozent aller Befragten hielten Ärzte im Umgang mit privaten Daten für absolut zuverlässig gegenüber 35 Prozent, die dies von Sozialämtern meinten. 55 Prozent der Befragten (66 Prozent in Ostdeutschland gegenüber 52 Prozent in Westdeutschland) wünschten, dass dem Datenschutz künftig eine erhöhte Bedeutung zukommen solle. Von je 100 Befragten erklärten die meisten, nämlich 46 Prozent, dass sie aus dem Angebot an multimedialen Dienstleistungen (z. B. über das Internet) behördliche Teledienste in Anspruch nehmen wollen, um sich Behördenbesuche zu ersparen. Zugleich zeigten sich 51 Prozent bei Verstößen gegen den Datenschutz hilflos und konnten keine Möglichkeit benennen, was in einem solchen Fall zu unternehmen sei.

Gerade die zuletzt genannte Zahl verdeutlicht, welcher Aufgabe sich die Datenschutzbeauftragten in Bund und Ländern trotz einer in einzelnen Ländern (z. B. Hessen) 30-jährigen Datenschutztradition vorrangig stellen müssen: Beratungs- und Hilfsangebote sollten den Bürgern mit neuen Formen der Öffentlichkeitsarbeit nahegebracht werden.

Die verstärkte Information der Bürger über den Umgang mit ihren Daten ist auch ein Hauptanliegen der Europäischen Datenschutzrichtlinie, die im Berichtszeitraum (bis zum 24. Oktober 1998) in den Mitgliedstaaten umzusetzen war. Sie zielt vor allem auf verbesserte Auskunfts- und Informationsrechte der Betroffenen. Während der Bundesgesetzgeber die Anpassungsfrist ungenutzt verstreichen ließ, hat das Land Brandenburg mit dem novellierten Brandenburgischen Datenschutzgesetz vom 21. Dezember 1998[2] einen wesentlichen Beitrag zur Modernisierung des Datenschutzrechts in Deutschland geleistet (A 1.2). Die in diesem Gesetz enthaltenen Elemente eines neuen Datenschutzes werden wahrscheinlich auch die bevorstehende Datenschutzgesetzgebung im Bund und in den Ländern beeinflussen, die bisher mit der erforderlichen Novellierung noch im Rückstand sind.

Datenschutz - auch das hat die eingangs erwähnte Umfrage gezeigt - hat viel mit einem Vertrauen zu tun, das mehr ist als eine subjektive Befindlichkeit des Einzelnen. Neue Telekommunikationsdienste, die die Bürger offenbar gerade auch im Verkehr mit den Behörden, z. B. in "virtuellen Rathäusern" (dazu A 2.1), nutzen wollen, werden nur dann angenommen werden, wenn die Benutzer darauf vertrauen können, dass ihre Privatsphäre unangetastet bleibt[3].

Vertrauen wird auch durch Transparenz und Zugang zu Informationen erzeugt. Die Regierungen der Mitgliedstaaten der Europäischen Union haben bei der Unterzeichnung des Vertrags von Maastricht ihre Auffassung bekräftigt, "das die Transparenz des Beschlussverfahrens den demokratischen Charakter der Organe und das Vertrauen der Öffentlichkeit in die Verwaltung stärkt"[4]. Das trifft nicht nur für die Organe der Europäischen Union, sondern auch für die Behörden auf Landes- und Kommunalebene zu.

Mit dem Akteneinsichts- und Informationszugangsgesetz hat das Land Brandenburg das in der Landesverfassung verankerte Grundrecht auf Informationszugang präzisiert und den Bürgern und Verbänden ein wichtiges Mittel zur politischen Mitgestaltung an die Hand gegeben. Damit wird ein zusätzlicher Schritt zum Aufbau einer Infrastruktur des Vertrauens getan.

Max Weber hat bei seiner Analyse der öffentlichen Verwaltung in Preußen 1922 in der Abschottung des geheimen Verwaltungswissens vor parlamentarischer Kontrolle einen wesentlichen Grund für die Staatsverdrossenheit gesehen. Sein Ergebnis lässt sich - mit gewissen sprachlichen Abwandlungen - auch auf das Verhältnis zwischen der Verwaltung und den Bürgern anwenden: "Selten ... ist das Verhältnis des Publikums zum öffentlichen Dienst so verständnislos wie in Deutschland. Die Probleme, mit welchen die öffentlichen Bediensteten bei ihrer Arbeit zu ringen haben, treten hier nirgends sichtbar hervor. Ihre Leistung kann niemals verstanden und bewertet, das anstelle positiver Kritik stehende sterile Schelten über den "heiligen Bürokratius" niemals überwunden werden, wenn der Zustand unkontrollierter Beamtenherrschaft anhält"[5].

Der 62. Deutsche Juristentag hat 1998 die Schaffung einer Informationsordnung vorgeschlagen, die u. a. den Zugang zu Informationen und den Umgang mit Informationen insbesondere im Hinblick auf den Schutz personenbezogener Daten regelt[6]. Eine entsprechende "Datenverkehrsordnung" soll nach diesen Vorschlägen, die auch die Konferenz der Datenschutzbeauftragten unterstützt hat[7], in einem Informationsgesetzbuch zusammengefasst werden.

Das Land Brandenburg hat im Jahr 1998 mit der Verabschiedung des Akteneinsichts- und Informationszugangsgesetzes und des novellierten Datenschutzgesetzes seinen Einwohnern zwei wichtige Bausteine für ein entstehendes Brandenburgisches Informationsgesetzbuch zur Verfügung gestellt. Diese Bausteine sind Meilensteine auf dem Weg Brandenburgs in die Informationsgesellschaft. Datenschutz und Akteneinsicht können dazu beitragen, dass der Einzelne vom passiven Objekt zum aktiven Subjekt einer zivilen und demokratischen Informationsgesellschaft wird. Brandenburg hat dafür die rechtlichen Rahmenbedingungen gesetzt. Jetzt gilt es, sie mit Leben zu erfüllen. Dazu sollten besonders die Bürger stärker als bisher von ihren Rechten und Möglichkeiten des Selbstschutzes Gebrauch machen.

Nach dem In-Kraft-Treten des Akteneinsichts- und Informationszugangsgesetzes sind wir in Teilen der Verwaltung der irrigen Auffassung begegnet und entgegengetreten, dieses Gesetz führe zu einer Abwertung und Relativierung des Datenschutzes, weil jetzt die Behörden personenbezogene Daten der Bürger leichter untereinander austauschen könnten. Dem liegt ein gravierendes Missverständnis zu Grunde: Öffentlichen Stellen ist die Berufung auf Informationszugangsrechte der Bürger ohnehin verwehrt. Etwas anderes mag allenfalls für die Gemeinden gelten[8], soweit sie als Träger der kommunalen Selbstverwaltungsgarantie betroffen sind. Vielmehr dient das neue Informationszugangsgesetz der politischen Mitgestaltung und soll Grundrechte des Einzelnen durchsetzbar machen. Der Gesetzgeber wollte und konnte den verfassungsrechtlich garantierten Datenschutz mit diesem Gesetz nicht aufweichen.

Dieser Bericht enthält deutliche europäische und internationale Akzente. Das ist nicht verwunderlich, weil personenbezogene Daten vielfach auch grenzüberschreitend verarbeitet werden und der Persönlichkeitsschutz mit der Nutzung des Internets neuen Gefährdungen ausgesetzt ist. Das allgemeine Informationszugangsrecht ist in Brandenburg zwar als erstem deutschen Bundesland gesetzlich verankert worden. Dies ist aber das Ergebnis einer europäischen und internationalen Entwicklung, die weiterhin auch unsere Situation beeinflussen wird. Im Übrigen ist zu hoffen, dass Brandenburg in Deutschland nicht mehr lange eine Insel der Informationsfreiheit bleiben wird. Mit der konsequenten Umsetzung des Akteneinsichts- und Informationszugangsgesetzes erhält der Begriff der "öffentlichen Verwaltung" eine neue, bürgernahe Bedeutung. Es kommt jetzt darauf an, in den Landes- und Kommunalbehörden eine Kultur der kontrollierten Verwaltungsöffentlichkeit zu entwickeln.

Teil A

Datenschutz

1. Modernisierung des Datenschutzrechts

Weitgehend besteht Einvernehmen darüber, dass die Datenschutzgesetze in Bund und Ländern, die sich zum Teil noch an der inzwischen überholten Großrechnertechnologie orientieren, grundlegend modernisiert werden müssen, wenn sie den Anforderungen der Informationsgesellschaft entsprechen sollen. Die europäische Rechtsvereinheitlichung hat hierzu einen neuen Anstoß gegeben, der allerdings im Berichtszeitraum nur in zwei Bundesländern (Hessen und Brandenburg) zu Änderungen des Datenschutzrechts führte. Eine Modernisierung des Bundesdatenschutzgesetzes steht noch aus.

1.1 Passivität des Bundesgesetzgebers

Die Frist zur Umsetzung der EG-Datenschutzrichtlinie von 1995 verstrich am 24. Oktober 1998, ohne dass der Bundesgesetzgeber aktiv geworden wäre. Ein Referentenentwurf des Bundesinnenministeriums erlangte vor der Bundestagswahl nicht einmal Kabinettsreife. Da er sich auf minimale Korrekturen im Bundesdatenschutzgesetz beschränkte, hätte er allerdings auch nichts zur Modernisierung des deutschen Datenschutzrechts beitragen können.

Die neue Bundesregierung ist offenbar bemüht, die Peinlichkeit eines von der Europäischen Kommission angestrengten Vertragsverletzungsverfahrens auf Grund der fehlenden Umsetzung der Datenschutzrichtlinie während der deutschen EU-Ratspräsidentschaft zu vermeiden, indem zügig eine Novelle zum Bundesdatenschutzgesetz auf den Weg gebracht wird. Ob diese allerdings tatsächlich Elemente eines neuen Datenschutzkonzepts enthalten wird, ist gegenwärtig noch völlig offen. Wie verlautet, soll die Novellierung des Datenschutzrechts auf Bundesebene weiterhin in zwei Stufen erfolgen, wobei die erste Stufe nur die nötigsten Änderungen zur Umsetzung der EG-Richtlinie enthalten und die eigentliche Modernisierung auf die zweite Stufe verschoben werden soll. Ob bei diesem Vorgehen in absehbarer Zeit mit einem modernen Bundesdatenschutzgesetz zu rechen ist, bleibt zweifelhaft.

Der 24. Oktober 1998 hat gleichwohl juristische Konsequenzen für die Bundesrepublik: Nach der Rechtsprechung des Europäischen Gerichtshofs können Richtlinien des Parlaments und des Rates, die nicht rechtzeitig oder nicht vollständig in die Mitgliedstaaten umgesetzt worden sind, unter bestimmten Voraussetzungen unmittelbare Wirkung entfalten[9]. Damit könnten sich möglicherweise auch Betroffene in Deutschland auf bestimmte Vorschriften der EG-Datenschutzrichtlinie berufen. Dies gilt

jedenfalls zu Gunsten der Bürger in ihrem Verhältnis gegenüber dem Staat[10]. Die Frage der unmittelbaren Anwendbarkeit ist für die einzelnen Richtlinienvorschriften jeweils gesondert zu prüfen; sie setzt voraus, dass die Vorschrift dem Bürger in hinreichend bestimmter und unbedingter Form Rechte einräumt.

Dies gilt bei Regelungen, die besondere Kategorien personenbezogener Daten betreffen. Hier enthält die EG-Richtlinie ein grundsätzliches Verbot, personenbezogene Daten zu verarbeiten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie ein prinzipielles Verarbeitungsverbot von Daten über Gesundheit oder Sexualleben[11]. Unmittelbar anwendbar kann auch das Recht des Einzelnen sein, Widerspruch gegen eine rechtmäßige Verarbeitung seiner Daten zu erheben und eine begründete Entscheidung über seinen Widerspruch zu verlangen. Auch die Informations- und Auskunftsrechte der Betroffenen werden durch die Richtlinie unmittelbar erweitert. Dies entlässt den Bundesgesetzgeber allerdings nicht aus seiner Verantwortung, die Richtlinie insgesamt - wenn auch mit Verzug - in innerstaatliches Recht umzusetzen. Bereits jetzt muss das geltende Bundesdatenschutzgesetz richtlinien-konform ausgelegt werden.

1.2 Neues Brandenburgisches Datenschutzgesetz

Positiver ist das Bild der datenschutzrechtlichen Entwicklung in Brandenburg: Am 24. Dezember 1998 ist das Zweite Gesetz zur Änderung des Brandenburgischen Datenschutzgesetzes (BbgDSG) in Kraft getreten[12]. Damit hat Brandenburg nach Hessen als zweites Bundesland die Vorgaben der Europäischen Datenschutzrichtlinie weitgehend umgesetzt. Die Novellierung des Brandenburgischen Datenschutzgesetzes stand nicht nur wegen des Ablaufs der gemeinschaftsrechtlichen Anpassungsfrist unter Zeitdruck, sondern auch, weil ohne Gesetzesänderung mit Ablauf des Jahres 1998 die Verarbeitung personenbezogener Daten nicht mehr auf das Brandenburgische Datenschutzgesetz hätte gestützt werden können. Der Vorrang bereichsspezifischer Regelungen als Verarbeitungsgrundlage für personenbezogene Daten, der nach bisherigem Recht ausnahmslos galt, ist im neuen Datenschutzgesetz in sinnvoller Weise dahingehend abgeändert worden, dass eine bereichsspezifische Rechtsgrundlage außerhalb des Datenschutzgesetzes nur noch für die besonders sensiblen Daten im Sinne des Artikels 8 der EG-Richtlinie vorgeschrieben ist.

Der Landesgesetzgeber hat sich aber nicht damit begnügt, das Landesdatenschutzgesetz den europäischen Mindestanforderungen anzupassen; er hat darüber hinaus auch auf Grund unserer Vorschläge Regelungen in das Gesetz aufgenommen, die es zu einem der modernsten Datenschutzgesetze der Bundesrepublik Deutschland machen. Vor allem die Rechte der Betroffenen sind wesentlich gestärkt worden.

Hervorzuheben sind im Einzelnen:

- die Schaffung *eines Widerspruchsrechts der Betroffenen* gegen die rechtmäßige Verarbeitung ihrer Daten, wenn sie ein schutzwürdiges persönliches Interesse darlegen, das dem öffentlichen Interesse an der Datenverarbeitung vorgeht;

- das grundsätzliche *Verbot einer* die Person belastenden Entscheidung, die auf einer *automatisierten Bewertung* einzelner Merkmale dieser Person beruht;

- die Pflicht der Verwaltung, die Datenverarbeitung so zu organisieren, dass die *Daten* nach den jeweiligen Zwecken und nach unterschiedlichen Betroffenen *getrennt werden* können; diese Vorschrift hat besondere Bedeutung auch für die Umsetzung des ebenfalls im vergangenen Jahr in Kraft getretenen Akteneinsichts- und Informationszugangsgesetzes; nicht erforderliche Daten, die untrennbar mit erforderlichen Daten verbunden sind, unterliegen einem *Verwertungsverbot*;

- die strikte *Beschränkung der Verarbeitung besonders sensibler personenbezogener Daten*, z. B. über die rassische und ethnische Herkunft, über politische Meinungen, religiöse oder weltanschauliche Überzeugungen, die Gewerkschaftszuhörigkeit, die Gesundheit oder das Sexualleben;

- die Verpflichtung aller Behörden zur *Bestellung behördlicher Datenschutzbeauftragter*; damit wird die dezentrale Datenschutzkontrolle entscheidend gestärkt;

- detaillierte Vorschriften für die immer häufigere Form der *Datenverarbeitung im Auftrag* und der *Wartung* von Datenverarbeitungsanlagen;

- die Verpflichtung der Behörden, sich bei der Gestaltung und Auswahl informationstechnischer Produkte und Verfahren an dem Ziel auszurichten, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten (*Grundsatz der* Datensparsamkeit); dieser Grundsatz ist damit in Deutschland erstmals in einem allgemeinen Datenschutzgesetz verankert worden;

- die Einführung einer *Vorabkontrolle*, bei der vor dem erstmaligen Einsatz von automatisierten Verfahren zu untersuchen ist, ob von ihm spezifische Risiken für die Rechte und Freiheiten der Betroffenen ausgehen können; die Freigabe darf nur erklärt werden, wenn diese Risiken nicht bestehen oder beherrscht werden können;

- eine Regelung der mit der Ausgabe und Verwendung von *Chipkarten* verbundenen datenschutzrechtlichen Probleme;

- die Einführung eines freiwilligen *Datenschutzaudits* für öffentliche Stellen nach dem Vorbild des Umweltaudits könnte zusätzliche Impulse für eine datenschutzfreundliche Gestaltung der Verfahren in der öffentlichen Verwaltung bringen;

- die Ermöglichung einer *elektronischen Einwilligungserklärung*, soweit technisch sichergestellt ist, dass die Erklärung dem Betroffenen eindeutig zugeordnet und nicht heimlich verändert werden kann;

- das *Verbot der erzwungenen Einwilligung* in eine Zweckentfremdung der Daten bei der Leistungsgewährung an Bürgerinnen und Bürger;

- die Festlegung der Voraussetzungen, unter denen die Landesregierung personenbezogene Daten etwa zur *Beantwortung parlamentarischer Anfragen* an den Landtag übermitteln darf;

- die Möglichkeit der *Nutzung personenbezogener Daten für Forschungszwecke,* wenn die oberste Aufsichtsbehörde festgestellt hat, dass das öffentliche Interesse an der Durchführung des Forschungsvorhabens die schutzwürdigen Belange des Betroffenen überwiegt und der Forschungszweck sonst mit verhältnismäßigem Aufwand nicht erreicht werden kann.

Im Bereich der Auftragsdatenverarbeitung hat der Gesetzgeber - entgegen unserer Empfehlung - auch die auftragsweise Verarbeitung von Daten, die besonderen Geheimhaltungspflichten unterliegen, durch Private weitergehend als bisher zugelassen. So können z. B. Patientendaten durch private Unternehmen im Auftrag öffentlicher Krankenhäuser erfasst, mikroverfilmt oder vernichtet werden, wenn die Daten entweder verschlüsselt, anonymisiert oder pseudonymisiert wurden oder sofern technische und organisatorische Maßnahmen ergriffen worden sind, durch die sichergestellt wird, dass der Auftragnehmer die Patientendaten nur zur Kenntnis nehmen kann, soweit es für die Aufgabenerfüllung unerlässlich ist (§ 11 Abs. 5 Satz 3 BbgDSG). Mit dieser Regelung ist eine Offenbarungsbefugnis für die schweigepflichtigen Ärzte geschaffen worden, die in jedem Fall restriktiv auszulegen ist. So wäre etwa das manuelle Erfassen von Patientenakten durch private Auftragnehmer trotz des weiten Gesetzeswortlauts unzulässig, weil dies zur Offenbarung der gesamten Patientenakte führen würde. Gerechtfertigt ist nur das Einscannen solcher Akten zum Zwecke der Archivierung, bei dem in der Regel eine Kenntnisnahme des Akteninhalts nicht erforderlich ist und nicht erfolgt[13]. Die Vorschrift - auch darauf haben wir hingewiesen - ist allerdings im Datenschutzgesetz systematisch verfehlt, weil es sich um eine Regelung zur Verarbeitung besonders sensibler Daten handelt, die nach § 4 a BbgDSG in einer bereichsspezifischen Rechtsvorschrift geregelt werden sollte.

Entsprechend der EG-Datenschutzrichtlinie regelt das neue Brandenburgische Datenschutzgesetz die Übermittlung personenbezogener Daten an Behörden in Mitgliedstaaten der Europäischen Union in der Weise, dass diese deutschen Behörden gleichgestellt werden. Damit wird ein wesentliches Ziel der Richtlinie erreicht, die einen möglichst ungehinderten Datenverkehr innerhalb der Mitgliedstaaten der Europäischen Union ermöglichen will, in denen von einem einheitlichen Mindestniveau des Datenschutzes auszugehen ist. Ein Export personenbezogener Daten an Stellen außerhalb der Europäischen Union ist nur zulässig, wenn im Empfängerland ein angemessenes Datenschutzniveau herrscht, darüber hinaus nur in bestimmten Ausnahmefällen[14]. Gegen unseren Rat hat der Landesgesetzgeber den datenverarbeitenden Stellen selbst die Möglichkeit eröffnet, den Export personenbezogener Daten auch in Drittländer ohne angemessenes Datenschutzniveau zuzulassen, wenn die empfangende Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts vorweist. Die datenverarbeitenden Stellen sollen dem Ministeri-

um des Innern diese Fälle mitteilen.

Die EG-Richtlinie sieht zwar ausnahmsweise Genehmigungen zum Datenexport vor, wenn der Datenschutz etwa auf vertraglicher Grundlage zwischen den beteiligten Stellen gewährleistet wird, wobei vor allem darauf zu achten ist, dass den betroffenen Bürgern unmittelbare Rechte eingeräumt werden. An der brandenburgischen Regelung verwundert allerdings, dass die datenverarbeitenden Stellen sich gewissermaßen selbst solche Exportgenehmigungen erteilen können. Mit der Richtlinie ist dies kaum in Einklang zu bringen. Zumindest muss das Brandenburgische Datenschutzgesetz in diesem Punkt richtlinien-konform dahingehend ausgelegt werden, dass der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht die Rechtmäßigkeit des Datenexports zu überprüfen hat.

Auch die gegenwärtige Struktur der Datenschutzkontrolle im Land Brandenburg stimmt noch nicht mit den Vorgaben der EG-Datenschutzrichtlinie überein. Die Datenschutzaufsicht ist zur Zeit in Brandenburg in der Weise organisiert, dass der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht die Verarbeitung personenbezogener Daten in der öffentlichen Verwaltung kontrolliert, während das Ministerium des Innern für den Datenschutz im nicht-öffentlichen Bereich (in der Privatwirtschaft) zuständig ist. Die EG-Datenschutzrichtlinie sieht vor, dass die Mitgliedstaaten öffentliche Kontrollstellen mit der Überwachung der Anwendung der einzelstaatlichen Datenschutzvorschriften zu beauftragen haben. Diese Kontrollstellen sollen ihre Aufgaben "in völliger Unabhängigkeit" wahrnehmen.

Während der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in der Ausübung seines Amtes unabhängig und nur dem Gesetz unterworfen ist (§ 22 Abs. 4 Satz 2 BbgDSG), hat die Landesregierung bereits durch Rechtsverordnung vom 10. August 1992[15] die Datenschutzkontrolle im nicht-öffentlichen Bereich dem Ministerium des Innern zugewiesen, wo diese Aufgabe von einem Referat wahrgenommen wird. Damit ist die Datenschutzaufsicht in der Privatwirtschaft in die normalen Organisations- und Weisungsstränge eines Ministeriums eingebunden. Sie erfolgt nicht in der von der Richtlinie vorgesehenen völligen Unabhängigkeit. Zwar ist das Ministerium des Innern unabhängig von den zu kontrollierenden Unternehmen; diese Unabhängigkeit ist aber selbstverständlich und genügt nicht den Vorgaben des Gemeinschaftsrechts, das ausdrücklich die verstärkende Formulierung "völlige Unabhängigkeit" gewählt hat. Auch der 62. Deutsche Juristentag hat 1998 in Bremen die Bedeutung einer wirksamen Datenschutzkontrolle hervorgehoben, die weisungsfrei und verselbständigt durchgeführt werden sollte[16].

Dem gemeinschaftsrechtlichen Gebot der völlig unabhängigen Datenschutzkontrolle würde es am ehesten entsprechen, wenn der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht zugleich für den Datenschutz im öffentlichen und im nicht-öffentlichen Bereich zuständig wäre und den Status einer obersten Landesbehörde erhielte, den die Datenschutzbeauftragten in Berlin, Hessen und Rheinland-Pfalz bereits haben. Dazu ist keine Änderung der Landesverfassung, sondern nur des einfachen Gesetzesrechts erforderlich. Landesregierung und Landtag haben sich unseren Empfehlungen insoweit bisher nicht anschließen können.

Dennoch sollte ein modernes materielles Datenschutzrecht, wie es in Brandenburg inzwischen gilt, auch durch eine moderne und richtlinien-konforme Struktur der Datenschutzkontrolle ergänzt werden.

Die Schaffung einer unabhängigen Datenschutzkontrolle aus einer Hand für den öffentlichen und den privaten Bereich bleibt auf der Tagesordnung in Brandenburg; sie sollte spätestens nach der Neufassung des Bundesdatenschutzgesetzes wieder aufgegriffen werden.

2. Technik und Organisation

2.1 Landesverwaltungsnetz

2.1.1 Noch immer kein vollständiges Sicherheitskonzept

Auch im Berichtszeitraum wurde das Landesverwaltungsnetz (LVN) weiter zu einem modernen Kommunikationsnetz des Landes ausgebaut.

Bereits in unserem letzten Tätigkeitsbericht (s. 6. TB, unter 1.4.1) sind wir auf die Notwendigkeit der frühzeitigen Erstellung von Sicherheitskonzepten eingegangen. Das Landesamt für Datenverarbeitung und Statistik hat inzwischen die 1997 festgestellten Mängel beim Anschluss des LVN an das Internet behoben und auch ein vorbildliches Sicherheitskonzept für sein eigenes Fachnetz erstellt. Dagegen ist nicht nachvollziehbar, dass derzeit ausgerechnet für das Kernnetz sowie für die Fachnetze der Polizei und der Oberfinanzdirektion von den Betreibern noch keine Sicherheitskonzepte erstellt wurden. Im April 1998 forderten wir die zuständigen Netzbetreiber schriftlich auf, uns die ausstehenden Sicherheitskonzepte gem. § 26 Abs. 1 Nr. 1 BbgDSG zur datenschutzrechtlichen Stellungnahme zur Verfügung zu stellen. Da wir bis zum jetzigen Zeitpunkt von den zuständigen Stellen noch keine Antwort erhalten haben, können wir über diese besonders sensiblen Teile des LVN keine positive Aussage treffen.

Wir haben stets betont, dass die Erstellung von Sicherheitskonzepten eine Grundvoraussetzung für die Einführung von so komplexen Verfahren wie der Aufbau eines Landesverwaltungsnetzes ist. Erst in einem Sicherheitskonzept kann man die Gefährdungen und Risiken, die bei der Übertragung von personenbezogenen Daten im LVN entstehen, umfassend analysieren und darauf aufbauend entsprechende technisch-organisatorische Maßnahmen planen und umsetzen.

Es ist Aufgabe der Landesregierung, für die zügige Umsetzung der von den Betreibern des Landesverwaltungsnetzes selbst gestellten Ziele, nämlich "die Erarbeitung von Datenschutz- und Datensicherheitskonzepten"[17] zu sorgen.

2.1.2 Verzeichnisdienst der Landesverwaltung

Im Landesverwaltungsnetz Brandenburg kommt der elektronischen Post eine wachsende Bedeutung zu. Sie dient der schnellen und unbürokratischen Kommunikation innerhalb der Verwaltung und - über das Internet - zunehmend auch mit Bürgern.

Mit den stetig steigenden Benutzerzahlen wird die Einrichtung eines Verzeichnisdienstes, aus dem Adressinformationen von Beschäftigten und Behörden abgerufen werden können, erforderlich. In der 58. Sitzung des Interministeriellen Ausschusses für Informationstechnik (IMA-IT) wurde daher die Bildung einer Arbeitsgruppe "Verzeichnisdienst" beschlossen. Aufgabe der Arbeitsgruppe, an der wir uns beteiligen, ist die Erarbeitung eines Fachkonzeptes für einen behördenübergreifenden Verzeichnisdienst unter Beteiligung der zuständigen Stellen.

Die Einstellung von personenbezogenen Daten in Verzeichnisdienste wirft grundsätzliche Fragen auf. Aufgrund der Komplexität der Problematik beschränken wir uns auf folgende drei Szenarien:

Verzeichnisdienst innerhalb einer öffentlichen Stelle

Nutzer dieses Verzeichnisdienstes dürfen nur die Beschäftigten der jeweiligen öffentlichen Stelle sein.

In diesem Fall gehen wir derzeit davon aus, dass gem. § 29 Abs. 1 BbgDSG die Basiskommunikationsdaten des Beschäftigten (z. B. Name, Vorname, akademischer Grad, dienstliche Postanschrift, Telefon, Fax, e-mail-Adresse, öffentlicher Schlüssel, Stellenzeichen, Funktionsbezeichnung und Aufgabengebiet) ohne Einwilligung des Betroffenen in einen Verzeichnisdienst innerhalb der jeweiligen Behörde aufgenommen werden können. Zusätzliche personenbezogene Daten dürfen nur mit der Zustimmung des Beschäftigten in dem Verzeichnis behördenintern veröffentlicht werden.

Verzeichnisdienst der öffentlichen Stellen des Landes (z. B. GroupWise-Verbund)

Nutzer dieses Verzeichnisdienstes dürfen nur die Beschäftigten der öffentlichen Stellen des Landes sein. Es muss sich um ein geschlossenes Netz (Intranet) der Landesverwaltung handeln, das effektiv vor Zugriffen aus dem Internet geschützt ist.

Auch in diesem Fall gehen wir derzeit davon aus, dass gem. § 29 Abs. 1 BbgDSG Basiskommunikationsdaten des Beschäftigten (z. B. Name, Vorname, dienstliche

Postanschrift, Telefon, Fax, e-mail-Adresse, öffentlicher Schlüssel, Stellenzeichen, Funktionsbezeichnung und Aufgabengebiet) ohne Einwilligung des Betroffenen in einen Verzeichnisdienst innerhalb der jeweiligen Behörde aufgenommen werden können. Zusätzliche personenbezogene Daten dürfen nur mit der Zustimmung des Beschäftigten in dem Verzeichnis veröffentlicht werden.

Beschäftigte, die zu einem "gefährdeten" Mitarbeiterkreis gehören (z. B. Sicherheits- und Strafverfolgungsbehörden, Soziale Dienste, Richter) dürfen nicht ohne Einwilligung personenbezogen in diesen Verzeichnisdienst aufgenommen werden. Eine Einstellung dieser Beschäftigten in den Verzeichnisdienst unter Verwendung von Pseudonymen (z. B. Struktureinheit, Poststelle) wäre aus Sicht des Datenschutzes eine denkbare Alternative. Folgende Basiskommunikationsdaten wären in diesem Fall möglich: Pseudonym, Telefon, Fax, e-mail-Adresse, öffentlicher Schlüssel und das Aufgabengebiet. Bei der Verwendung von Pseudonymen darf im Verzeichnisdienst keine Zuordnungsmöglichkeit zu natürlichen Personen bestehen.

Veröffentlichung von Beschäftigtendaten in einem Verzeichnisdienst mit der Möglichkeit des Zugriffs Dritter (z. B. Internet)

Will der Bürger mit der Verwaltung online Kontakt aufnehmen, muss er dazu offene Netze wie etwa das Internet nutzen. Verzeichnisdienste können dafür ein wichtiges Hilfsmittel sein. Die Entscheidung über ihren Inhalt erfordert eine besondere Abwägung zwischen dem Informationsinteresse des Bürgers und dem Recht der öffentlichen Bediensteten auf Schutz ihrer informationellen Selbstbestimmung. Diese Abwägung ist nicht gleichzusetzen mit der im Akteneinsichts- und Informationszugangsgesetz (AIG) getroffenen Regelung, nach der Amtsträger eine Offenbarung ihrer Mitwirkung an Verwaltungsvorgängen bei der Akteneinsicht grundsätzlich und unabhängig von ihrer Funktion hinnehmen müssen, es sei denn, ihre schutzwürdigen Belange stehen dem entgegen (§ 5 Abs. 3 AIG). Denn das Akteneinsichts- und Informationszugangsgesetz betrifft nur die Einsichtnahme im Einzelfall und auf Antrag, nicht aber die Nutzung von Verzeichnisdiensten, die als Mediendienst im Internet angeboten werden. Für derartige Informationsangebote der Verwaltung ist eine differenzierende Lösung notwendig: Die oben genannten Basiskommunikationsdaten von Behördenleitern und politischen Beamten (z. B. Mitgliedern der Landesregierung, Staatssekretären, Abteilungsleitern), aber auch von weiteren Bediensteten mit starkem Öffentlichkeitsbezug können in globale Verzeichnisdienste zum Abruf eingestellt werden. Die damit verbundene Einschränkung ihrer informationellen Selbstbestimmung haben diese Träger herausgehobener Funktionen hinzunehmen.

Bei anderen öffentlichen Bediensteten wäre auch in globalen Verzeichnisdiensten eine Verwendung von Pseudonymen vorstellbar, wenn der Betroffene vor der Einstellung seines Namens nicht eingewilligt hat. So könnte z. B. ein Bürger aus dem Organigramm einer Behörde im WorldWideWeb den entsprechenden Ansprechpartner auswählen, und ihm eine elektronische Nachricht unter Verwendung der pseudonymisierten e-mail-Adresse des jeweiligen Ansprechpartners - und damit ohne Personenbezug - übersenden. Nur auf diese Weise lassen sich die Risiken für die Bediensteten ohne herausgehobene Funktion begrenzen, die mit jeder Einstellung personenbezogener Daten in das Internet angesichts der systematischen Erfassung derartiger

Daten durch Suchmaschinen für Marketingzwecke verbunden sind[18].

Die vorgenannten Punkte sind nicht als abschließend zu betrachten. Einer genaueren Analyse müssten weiterhin auch die erforderlichen technischen und organisatorischen Maßnahmen unterzogen werden.

Bei der Aufnahme personenbezogener Daten in Verzeichnisdienste der Verwaltung gilt die Regel: je offener das Netz, in dem dieses Verzeichnis bereitgestellt wird, desto sparsamer sollten Namen von Bediensteten ohne herausgehobene Funktion verwendet werden. Auch pseudonymisierte e-mail-Adressen ermöglichen dem Bürger die Kontaktaufnahme mit dem gewünschten Ansprechpartner.

2.2 Verschlüsselung im Verfahren "Haushalts-, Kassen- und Rechnungswesen"

In unserem letzten Tätigkeitsbericht (s. 6. TB unter 1.4.1.6) hatten wir die Verschlüsselung der beim Verfahren "Haushalts-, Kassen- und Rechnungswesen" (HKR-Verfahren) über das Landesverwaltungsnetz übertragenen personenbezogenen Daten gefordert. Das zuständige Ministerium der Finanzen hat in enger Zusammenarbeit mit dem Landesamt für Datenverarbeitung und Statistik im Berichtszeitraum ein Verfahren entwickelt, in dem die Transferdateien des HKR-Verfahrens verschlüsselt, und damit datenschutzgerecht, im Landesverwaltungsnetz übertragen werden. Als Verschlüsselungssoftware wird Pretty Good Privacy (PGP) eingesetzt. Die Länge der asymmetrischen Schlüssel beträgt 1024 Bit. Die verwendeten öffentlichen Schlüssel werden vom Trust-Center des Landesamtes für Datenverarbeitung und Statistik zertifiziert. Die am HKR-Verfahren beteiligten Stellen wurden vom Ministerium der Finanzen durch eine Dienstanweisung zum „Verschlüsseln der Transferdateien im HKR-Verfahren Profiskal (DA Profiskal - PGP)“ über das Verfahren informiert.

Unsere Forderung nach verschlüsselter Übertragung von personenbezogenen Haushalts-, Kassen- und Rechnungs-Daten mittels Dateitransfer im Landesverwaltungsnetz wurde damit vorbildlich erfüllt.

2.3 Stand der Kryptodebatte

In ihrem 4. Zwischenbericht hat die Enquete-Kommission des Bundestages "Zukunft der Medien in Wirtschaft und Gesellschaft - Deutschlands Weg in die Informationsgesellschaft"[19] festgestellt: "Die Möglichkeiten der Nutzer zum Selbstschutz durch kryptografische Verfahren sollten nach dem derzeitigen Erkenntnisstand rechtlich nicht eingeschränkt werden. Eine Einschränkung der freien Verwendung solcher Verfahren kann bei einer Abwägung von Nutzen und Schaden nach diesem Erkenntnisstand

nicht gerechtfertigt werden. Denn während sie rechtstreue Unternehmen und Bürger bei ihren Bemühungen, vertraulich zu kommunizieren, erheblich behindern würde, dürfte der Nutzen für die öffentliche Sicherheit aufgrund der Umgehungsmöglichkeiten gering sein".

Im Wahlkampf zur Bundestagswahl 1998 wurden die sechs medienpolitischen Experten der im Bundestag vertretenen Parteien von einer Zeitschrift u. a. darüber befragt[20], was sie vom Einsatz von Verschlüsselungssystemen im Spannungsfeld der Schlagworte "Innere Sicherheit" und "Standort Deutschland" hielten und welche Maßnahmen Staat, Bürger und Wirtschaft ergreifen sollten, um sich gegen die "Key Recovery Alliance"[21] der USA zu schützen. Alle Befragten lehnten dabei das von den USA angestrebte weltweite Zugriffssystem auf Nutzerdaten - teilweise mit dem Hinweis auf die Verletzung deutscher Souveränitätsrechte - ab. Das Recht der Unternehmen und der Bürger auf Selbstschutz ihrer sensiblen Daten sollten durch keine Kryptoregulierung eingeschränkt werden.

Nach dem Regierungswechsel bleibt abzuwarten, wie Bundestagsfraktionen und neue Bundesregierung nun zu diesen Ansichten stehen. Anfang November 1998 forderten die Datenschutzbeauftragten Berlins, Brandenburgs, Bremens, Nordrhein-Westfalens und Schleswig-Holsteins mit einem 10-Punkte-Papier zu einem Politikwechsel zum wirksameren Schutz der Privatsphäre auf[22]. Zur Verschlüsselung heißt es darin:

"Die Nutzung offener Netze für geschäftliche oder persönliche Zwecke steht und fällt mit der Möglichkeit, die Vertraulichkeit und Unverfälschtheit der ausgetauschten Informationen zu garantieren. Das wichtigste Instrument dazu sind starke Verschlüsselungsverfahren. Die staatliche Politik sollte auf eine Förderung dieser Technik und ihre Verfügbarkeit für jeden einzelnen Bürger gerichtet sein. Überlegungen, das Recht zur Verschlüsselung zugunsten der Sicherheitsbehörden einzuschränken, gehen schon deswegen fehl, weil derartige Regelungen technisch - etwa durch Doppelverschlüsselung oder Steganographie - leicht umgangen werden können. Die Vorstellung, jede elektronische Kommunikation müsse vom Staat überwachbar sein, ist unter den Bedingungen des Internet illusorisch."

Für eine gewisse Irritation sorgte im Dezember 1998 die Bundesregierung, als sie im sog. Wassenaar-Abkommen[23] offenbar dem Druck der US-Regierung bei der umstrittenen Verschlüsselungstechnik teilweise nachgab[24]. Zwar wurden einerseits Exportkontrollen für symmetrische Verschlüsselungsprodukte mit einer kleineren Schlüssellänge als 56 bzw. 64 Bit gelockert, andererseits unterliegen höherwertige Produkte einer nationalen Genehmigungspflicht. Es kursierten deshalb Gerüchte, dass nun auch die Bundesrepublik Deutschland die Ausfuhr starker Verschlüsselungsprodukte verbieten würde. Diese Meldungen hat das Bundeswirtschaftsministerium aber umgehend dementiert. Die Genehmigungspflicht soll den Export solcher Produkte nicht ausschließen; eine Hinterlegungspflicht für die Schlüssel bestehe in der

Bundesrepublik nicht[25]. Außerdem erklärte die Bundesregierung, sie wolle sich für einen echten genehmigungsfreien Binnenmarkt für Verschlüsselungstechnik in der EU einsetzen, und sehe in der Streichung dieser Technik von der sog. "Sensitive List" des Wassenaar-Abkommens einen ersten Schritt in diese Richtung[26].

Der brandenburgische Landesgesetzgeber hat der unaufhaltsamen Technikentwicklung vorbildlich Rechnung getragen und in dem neuen Brandenburgischen Datenschutzgesetz erstmals den Begriff der Verschlüsselung von Daten in § 11 a definiert. Es bleibt zu hoffen, dass auch der Bundesgesetzgeber ähnliche Regelungen in das neue Bundesdatenschutzgesetz aufnehmen wird.

Zur Sicherung der informationellen Selbstbestimmung und des Selbstschutzes müssen Verschlüsselungsmöglichkeiten für alle Interessierten völlig frei sein. Nach wie vor gilt: Eine sichere und anspruchsvolle Kryptographie ohne Zugriffsmöglichkeit für den Staat oder andere Dritte ist der beste Schutz für Bürger, Unternehmen und staatliche Verwaltung.

2.4 Muster-Dienstanweisung für den Einsatz von IuK-Technik

Die Arbeitsgruppe "Organisatorisch-technische Leitlinien" des Interministeriellen Ausschusses für Informationstechnik des Landes (IMA-IT) hat im Berichtzeitraum eine Muster-Dienstanweisung für den Einsatz von Informationstechnik erarbeitet, in der aufgrund unserer Empfehlungen auch datenschutzrechtliche Belange berücksichtigt wurden. Die Erstellung von Muster-Dokumenten für Behörden des Landes ist aus unserer Sicht eine sinnvolle Initiative, um den Arbeitsaufwand in den öffentlichen Einrichtungen zur Erstellung eigener Dienstanweisungen zu senken und gleichzeitig ein einheitliches Sicherheitsniveau zu erreichen.

Nach Bestätigung der Muster-Dienstanweisung durch den IMA-IT wird diese in unserem Internet-Angebot zum Abruf bereitgehalten.

2.5 Das "virtuelle Rathaus"

Unter der Federführung des Ministeriums für Wissenschaft, Forschung und Kultur erarbeitet die Landesregierung gegenwärtig einen Strategie- und Aktionsplan für eine Brandenburger InformationsStrategie 2006 (BIS 2006). Darin werden Initiativen zum Aufbau einer leistungsfähigen Kommunikationsinfrastruktur gebündelt, die Brandenburg den Weg in die Informations- und Wissensgesellschaft ebnen soll. In vier Strategie- und Handlungsfeldern (Informations- und Kommunikations-Offensive/Bildungs-Offensive/Regional-Initiative und Modernisierung der Verwaltung) sollen Konzepte entwickelt und mit Hilfe von Mitteln aus europäischen Strukturfonds realisiert werden. BIS 2006 enthält zahlreiche Projekte, die den Datenschutz wie auch den Informations-

zugang für Bürger berühren.

Der Minister für Wissenschaft, Forschung und Kultur hat deshalb den Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht in den Lenkungsausschuss für BIS 2006 berufen. Der Landesbeauftragte hat im Berichtszeitraum in erster Linie die Stadt Rathenow beraten, die zugleich im Rahmen des Bundeswettbewerbes Media@Komm das NetCity-Modell Rathenow als Brandenburger Referenzmodell für ein "Virtuelles Rathaus" entwickelt. Das Modell Rathenow soll allen Kommunen des Landes zur Übernahme empfohlen werden und der Entwicklung der Informationsgesellschaft vor Ort dienen. Ein Bürger- und Wirtschaftsnetzverein übernimmt die Funktion eines entstehenden lokalen Teledienstleistungszentrums. Es ist deshalb von zentraler Bedeutung, dass dieses Modellprojekt datenschutzfreundlich organisiert wird und von vornherein - gerade wegen seines Pilotcharakters - die gesetzlichen Vorgaben berücksichtigt.

Antragstellung über Internet

Im Projekt NetCity Rathenow ist zunächst geplant, dem Bürger die Erledigung bestimmter melderechtlicher Vorgänge (insbesondere der Anmeldung bei Zuzug) über das Internet anzubieten. Um einen elektronischen Antrag (auch in anderen Verwaltungsverfahren) sicher zu authentifizieren, d. h. festzustellen, ob er tatsächlich vom Antragsteller herrührt, ist eine digitale Signatur (elektronische Unterschrift) zu verwenden. Diese muss allerdings - jedenfalls bei dem in Rathenow geplanten Meldeverfahren - nicht formell den Anforderungen des Signaturgesetzes genügen. Da es sich um einen von der Verwaltung angebotenen Teledienst handelt, können entsprechende Anträge nach dem Rechtsgedanken des § 3 Abs. 7 des Teledienstedatenschutzgesetzes digital mit allgemein verfügbarer Verschlüsselungssoftware signiert werden, wenn sie auf diese Weise eindeutig dem Urheber zugeordnet werden können. Dies ist allerdings nur für einen Übergangszeitraum hinnehmbar, bis die Regulierungsbehörde als Wurzelinstanz nach dem Signaturgesetz Zertifizierungsstellen im Land Brandenburg zugelassen hat, die die Aufgabe von Vertrauensstellen (Trustcentern) übernehmen. Ein solches Verfahren ist auch übergangsweise nur unter der Voraussetzung hinnehmbar, dass der Bürger - schon aus Gründen des Melderechts - in jedem Fall nach der elektronischen Antragstellung persönlich bei der Meldebehörde vorsprechen und seinen Personalausweis vorlegen muss.

Risikobegrenzung durch Verschlüsselung

Außerdem sollte eine Stadtverwaltung, die diesen Teledienst "Interaktives Meldeverfahren" anbietet, den Bürger auf die Risiken der Nutzung offener Netze wie das Internet hinweisen. Zu diesen Risiken gehört vor allem die unbefugte Kenntnisnahme sowie das Abfangen, Umleiten und unbemerkte Verändern von Nachrichten im Internet. Der Bürger muss, um sich gegen die unbefugte Kenntnisnahme durch Dritte sichern zu können, über die Möglichkeit der inhaltlichen Verschlüsselung seiner Daten im Netz aufgeklärt werden. Zweckmäßigerweise sollte die Verwaltung ihn auch auf entsprechende Verschlüsselungssoftware, die allgemein zugänglich ist, hinweisen und sie ihm möglicherweise sogar zur Verfügung stellen. Während die Authentifikation mit Hilfe digitaler Signaturen zwingend geboten ist, kann der Bürger zur inhaltlichen Ver-

schlüsselung seiner Nachricht nicht gezwungen werden. Er muss aber unmissverständlich auf die Risiken hingewiesen werden, die entstehen, wenn er dies nicht tut.

Zwingend geboten wiederum ist die inhaltliche Verschlüsselung des personenbezogenen Nachrichtenaustauschs zwischen Behörden und für die Erteilung von Melderegisterauskünften durch die Meldebehörde an Private nach dem Meldegesetz. Auch die im Rathenower Modellprojekt vorgesehenen elektronischen Bescheide im interaktiven Baugenehmigungsverfahren sind zu verschlüsseln.

Besonders wichtig ist der Einsatz sicherer Verschlüsselungssoftware bei telemedizinischen Angeboten, die im Projekt NetCity Rathenow ebenfalls vorgesehen sind, wenngleich dafür noch keine detaillierten Planungen vorliegen. Soweit regionale Datenbanken an das Internet gekoppelt werden sollen, darf dies nur geschehen, wenn der gesamte Inhalt der Datenbank auch unabhängig von etwaigen Übermittlungen sicher verschlüsselt wird. Andernfalls machen sich die beteiligten Ärzte wegen Verletzung der ärztlichen Schweigepflicht möglicherweise strafbar. Wir haben die Stadtverwaltung Rathenow zu dem Teilprojekt Telemedizin um nähere Informationen gebeten. Eine endgültige Bewertung dieses Teilprojekts steht noch aus.

Abruf von Antragsformularen und Rathaus-Infos

Die ebenfalls im Rathenower Projekt geplante Bereitstellung von Informationen über die Verwaltung, Rechtsvorschriften und Antragsformularen im Internet ist als Mediendienst im Sinne des Mediendienstestaatsvertrages anzusehen. Dies hat zur datenschutzrechtlichen Konsequenz, dass die Stadt dem Bürger die Inanspruchnahme anonym oder unter Pseudonym ermöglichen muss, soweit dies technisch möglich und zumutbar ist. Wir haben bisher keine Anhaltspunkte dafür, dass die technische Möglichkeit und Zumutbarkeit fehlen könnte. Der Nutzer ist über diese Möglichkeit zu informieren. Er muss also Gelegenheit haben, die elektronisch verfügbaren Verlautbarungen der Stadt zur Kenntnis zu nehmen und Antragsformulare abzurufen, ohne elektronische Spuren zu hinterlassen.

"Virtuelle Rathäuser", die dem Bürger die elektronische Erledigung von Behördengängen ermöglichen, haben nur dann eine Zukunft, wenn in ihnen der Datenschutz auf demselben Niveau gewährleistet ist wie in realen Rathäusern.

3. Telekommunikation und Medien

3.1 Entwicklung des Telekommunikationsrechts

Wie bei der Europäischen Datenschutzrichtlinie[27] endete am 24. Oktober 1998 auch die Anpassungsfrist für die Richtlinie des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation[28] (Telekommunikationsrichtlinie). Diese Richtlinie dient der Harmonisierung der Vorschriften über den Datenschutz in der Telekommunikation und enthält zum Teil sehr detaillierte Regelungen, die ergänzend zur allgemeinen EG-Datenschutzrichtlinie anzuwenden sind.

Die Bundesregierung hat es versäumt, rechtzeitig vor Ablauf der Anpassungsfrist die seit langem überfällige Rechtsverordnung nach dem Telekommunikationsgesetz unter Berücksichtigung der Telekommunikationsrichtlinie zu erlassen. Deshalb stellt sich hier wie bei der Datenschutzrichtlinie die Frage, ob einzelne ihrer Vorschriften bereits jetzt unmittelbar anwendbar sind. Das gilt auch im Verhältnis zu Landesbehörden, die Telekommunikationsdienstleistungen z. B. durch den Betrieb von Nebenstellenanlagen geschäftsmäßig erbringen. Insofern ist die Telekommunikationsrichtlinie bereits jetzt bei der Anwendung in Brandenburg geltender Vorschriften in diesem Bereich zu berücksichtigen, die daraufhin zu überprüfen sind, ob ein Änderungsbedarf besteht. So wie Brandenburg bei der Umsetzung der allgemeinen Datenschutzrichtlinie zu Recht nicht auf den Bundesgesetzgeber gewartet und das Landesrecht bereits im Dezember 1998 verändert hat, sollte es auch hier nicht abwarten, bis die Bundesregierung die notwendige Rechtsverordnung nach dem Telekommunikationsgesetz erlässt. Die Pflicht zu europarechts-konformem Verhalten trifft auch die Bundesländer.

3.2 Telekommunikation in der Landesverwaltung

3.2.1 Neue Gebührendatenverarbeitung im Telekommunikationsverbund

Eine umfangreiche Kontrolle des zentralen TK-Verbundes der obersten Landesbehörden im Jahre 1996[29] ergab, dass sich mit der vorhandenen Software zur Gebührendatenverarbeitung wesentliche Forderungen der Dienstanschlussvorschrift - DAV -[30] nicht realisieren ließen.

Nach Verhandlungen mit dem Lieferanten der zentralen TK-Anlage, an denen wir beteiligt waren, erklärte sich die Staatskanzlei als Betreiber des TK-Verbundes der obersten Landesbehörden bereit, die Software zur Gebührendatenverarbeitung auf eine neue Fassung etappenweise umzurüsten. Die Umstellung wurde im Jahre 1998

vollständig abgeschlossen und während eines Kontrollbesuches im Dezember 1998 konnten wir uns davon überzeugen, dass sich mit der neuen Software für die Gebührendatenverarbeitung unter Berücksichtigung bestimmter technisch-organisatorischer Maßnahmen nun alle Forderungen der DAV datenschutzgerecht erfüllen lassen. Eine abschließende Bewertung unserer Kontrolle war bis zum Ende des Berichtszeitraumes nicht möglich, da sich die Bereitstellung der erforderlichen Unterlagen für die neue Gebührendatenverarbeitungssoftware von Seiten der Staatskanzlei verzögert hat.

Um für die Zukunft zu verhindern, dass im Land Brandenburg mit den Festlegungen in der DAV nicht konforme TK-Anlagen angeschafft werden und sich nachträglich zusätzliche Kosten für erforderliche Anpassungsmaßnahmen ergeben, haben wir gemeinsam mit dem Ministerium der Finanzen einen Forderungskatalog zum Datenschutz erarbeitet. Dieser soll künftig bereits in die Ausschreibungsunterlagen für neue TK-Anlagen aufgenommen werden und sichern, dass nur datenschutzgerechte Anlagen beschafft werden können.

Dies entspricht zugleich der Verpflichtung im neuen Brandenburgischen Datenschutzgesetz, wonach automatisierte Verfahren erst dann eingesetzt werden dürfen, wenn festgestellt worden ist, ob von ihnen besondere Risiken für Rechte und Freiheiten der Betroffenen ausgehen können und dass die Beherrschung dieser Risiken durch technisch-organisatorische Maßnahmen sichergestellt ist.

3.2.2 Vollständige Rufnummer im Einzelverbindungsnachweis

Im Mai 1998 wandten sich Mitarbeiter von Landesministerien mit folgendem Problem an uns:

Der Einzelverbindungsnachweis zur monatlichen Abrechnung ihrer im TK-Verbund der obersten Landesbehörden geführten Privatgespräche wies die Telefonnummer des angerufenen Teilnehmers in vollständiger Länge aus.

Die Beschwerden waren berechtigt, denn die Dienstanschlussvorschrift - DAV -[31] fordert im Punkt 3.1.3, dass bei privaten Verbindungen nur die um die letzten drei Ziffern verkürzte Rufnummer und ggf. die Vorwahl des angerufenen Teilnehmers gespeichert werden dürfen. Mit dieser sehr sinnvollen und datenschutzfreundlichen Festlegung soll verhindert werden, dass über die Kenntnis der vollständigen Rufnummer auf den angerufenen Teilnehmer geschlossen werden kann.

Eine Rückfrage bei der Staatskanzlei ergab, dass es sich um einen einmaligen Fehler handelt, der im Zusammenhang mit der Umstellung der zentralen TK-Anlage auf eine neue Software für die Gebührendatenverarbeitung auftrat, und dass in Zukunft die letzten drei Ziffern der Zielrufnummer wieder gekürzt werden, wie in der DAV vorgesehen. Der Fehler war dem Betreiber bereits beim Druck der Einzelverbindungsnachweise aufgefallen. Trotzdem hatte er sich zur Auslieferung der fehlerhaften

Belege entschlossen, da er die Unterlassung der sonst üblichen Verkürzung der Zielrufnummer als nicht so wesentlich ansah, und die unzulässige Speicherung der vollen Zielrufnummer ohnehin nicht mehr rückgängig gemacht werden konnte.

Sicher hätte das Auftreten des Fehlers bei einer gewissenhaften Teststrategie durch den Auftragnehmer für die neue Software der Gebührendatenverarbeitung vermieden werden können. Auch nach Erkennen der fehlerhaften Ausdrucke durch den Betreiber des TK-Verbundes wären aus unserer Sicht noch Programmkorrekturen für einen fehlerfreien Ausdruck der Einzelverbindungsnachweise sinnvoll gewesen.

Die Verkürzung der Zielrufnummer verhindert die nachträgliche Ermittlung der angerufenen Stelle oder Person und leistet damit einen entscheidenden Beitrag zur Wahrung des Fernmeldegeheimnisses.

3.2.3 Verhaltenskontrolle eines Mitarbeiters mit Hilfe der Telefon-Anlage

Während der Bearbeitung einer Bürgereingabe baten wir eine untergeordnete Landesbehörde um die Zusendung von Organisations- und Dienstanweisungen, die den Betrieb ihrer internen Telekommunikationsanlage regeln, und um Erläuterungen, in welcher Form Kontrollen von Dienst- und Privatgesprächen durchgeführt werden. Dem Antwortschreiben konnten wir entnehmen, dass in der Vergangenheit in einem Fall zielgerichtete Überprüfungen aller Telefongespräche eines Mitarbeiters vorgenommen wurden, obwohl die betreffenden Organisations- und Dienstanweisungen lediglich begrenzte Kontrollen von Dienstgesprächen, die stichprobenartig nach dem Zufallsprinzip auszuwählen sind, zulassen.

Auf Nachfrage schildert uns die Leitung der Behörde den folgenden Sachverhalt:

> *Einem Mitarbeiter wurde wegen verschiedener Dienstvergehen die weitere Ausübung seiner leitenden Tätigkeit untersagt, ihm wurde dafür eine andere Aufgabe übertragen. In der Folgezeit entstand jedoch der Eindruck, dass er sich telefonisch weiterhin mit Angelegenheiten seines früheren Aufgabengebietes beschäftigte. Um diesem Verdacht nachzugehen, entschied sich die Behördenleitung kurzer Hand, die Verbindungsdaten aller Privat- und Dienstgespräche, die der Betreffende von seinem dienstlichen Telefonapparat aus führte, in einem Zeitraum von ca. 5 Wochen lückenlos zu speichern und für Kontrollzwecke auszudrucken.*

Zur Rechtfertigung der Maßnahmen sagte uns ein Vertreter der Behördenleitung: "Man wollte doch mal sehen, mit wem der Betreffende so telefonierte“. Doch gerade dieses Ziel konnte mit der eingeleiteten Maßnahme nur sehr lückenhaft erreicht werden, da lediglich die abgehenden Telefonate erfasst wurden, während alle ankommenden Telefongespräche, die sich an den Mitarbeiter in seiner früheren Funktion richteten, unberücksichtigt blieben.

Wir betrachten die vorgenommene zielgerichtete Speicherung und Auswertung von Verbindungsdaten der dienstlichen und privaten Telefongespräche des Mitarbeiters als unzulässig, da keine gesetzliche Grundlage dafür vorliegt. Nach Artikel 10 des

Grundgesetzes ist das Fernmeldegeheimnis unverletzlich. Beschränkungen dürfen nur aufgrund eines Gesetzes angeordnet werden. Dabei gilt für die Verbindungsdaten von Telekommunikationsvorgängen, die im allgemeinen Auskunft darüber geben, wer wann mit wem telefoniert hat, das gleiche Schutzniveau wie für die Gesprächsinhalte von Telefonaten. Die für Brandenburg geltenden Dienstanschlussvorschriften - DAV - [32] und die Dienstvereinbarungen der betreffenden Landesbehörde über die Nutzung der internen Telekommunikationsanlage lassen lediglich in bestimmten, konkret definierten Fällen die Speicherung und Auswertung von Verbindungsdaten, u. a. für Abrechnungszwecke und zur Unterbindung von Missbrauchsmöglichkeiten, zu. Sie verbieten aber ausdrücklich die Nutzung der TK-Anlage zur Durchführung von Verhaltenskontrollen, wie sie im vorliegenden Fall stattgefunden hat.

Wir sehen in der vorgenommenen Überwachungsmaßnahme der dienstlichen und privaten Telefongespräche des Mitarbeiters einen schwerwiegenden Verstoß gegen die genannten Vorschriften. Von einer Beanstandung gem. § 25 Abs. 1 Brandenburgisches Datenschutzgesetz haben wir jedoch abgesehen, da uns die Behördenleitung zugesichert hat, dass es sich dabei um einen einmaligen Vorgang handelt, der sich in Zukunft nicht wiederholen wird und dass alle im vorliegenden Fall gewonnenen Daten und die durch ihre Auswertung erlangten Erkenntnisse unverzüglich gelöscht werden.

Das dargestellte Beispiel zeigt aber deutlich, dass einfache organisatorische Festlegungen allein, wie hier in der Dienstvereinbarung der Behördenleitung mit dem Personalrat, noch keinen sicheren Schutz vor Missbrauchsmöglichkeiten bieten. Ihre Einhaltung sollte deshalb durch geeignete Kontrollmechanismen, die ein zielgerichtetes Umgehen der organisatorischen Festlegungen verhindern, ergänzt werden.

Das Fernmeldegeheimnis ist unverletzlich und Beschränkungen dürfen nur aufgrund eines Gesetzes angeordnet werden. Das gilt nicht nur für die Inhalte, sondern bereits für die Verbindungsdaten von Telekommunikationsvorgängen. Für Abrechnungszwecke gespeicherte Verbindungsdaten dürfen nicht zur Verhaltens- und Leistungskontrolle von Mitarbeitern genutzt werden.

3.3 Entwicklung des Medienrechts

3.3.1 Evaluierung der Multimediagesetzgebung

Entsprechend einem Beschluss des Deutschen Bundestages bereitet die Bundesregierung gegenwärtig einen Bericht zur Evaluierung des Informations- und Kommunikationsdienstegesetzes von 1997 vor, das insbesondere in seinen datenschutzrechtlichen Regelungen, dem Teledienstedatenschutzgesetz, weitgehend mit dem gleichzeitig in Kraft getretenen Mediendienste-Staatsvertrag der Länder übereinstimmt. Zur Vorbereitung dieses Berichts hat das Bundesministerium für Bildung, Wissenschaft, Forschung und Technologie einen Arbeitskreis "Datenschutz" gebildet, an dem wir

uns gemeinsam mit der Landesbeauftragten für den Datenschutz Nordrhein-Westfalen und dem Hamburgischen Datenschutzbeauftragten auf Länderseite beteiligt haben.

Wir haben darauf hingewiesen, dass sich insbesondere die Regelungen des Teledienstedatenschutzgesetzes in der kurzen Zeit seit ihrem In-Kraft-Treten durchaus bewährt haben. Weder im Bundesrecht noch im Mediendienste-Staatsvertrag besteht insoweit Änderungsbedarf. Das erstmals im Mediendienste-Staatsvertrag geregelte Datenschutzaudit ist darüber hinaus ein zukunftsweisendes Instrument der marktorientierten Durchsetzung von datenschutzfreundlichen Angeboten, das gerade im internationalen Zusammenhang besondere Bedeutung erhalten wird. Daher haben wir empfohlen, dass der Bundesgesetzgeber eine entsprechende Vorschrift in das Teledienstedatenschutzgesetz aufnimmt. Auch in das allgemeine Datenschutzrecht des Bundes könnte das freiwillige Datenschutzaudit aufgenommen werden. Damit würde das Beispiel des novellierten Brandenburgischen Datenschutzgesetzes Schule machen, das seit Dezember 1998 in § 11 c ein freiwilliges Datenschutzaudit für öffentliche Stellen vorsieht. Allerdings sollten die besonderen Datenschutzbestimmungen für Multimediadienste nicht völlig im allgemeinen Datenschutzrecht aufgehen, denn sie sind zur Begrenzung der spezifischen Risiken dieser Dienste unverzichtbar.

Zweifellos muss im Bereich der Tele- und Mediendienste noch sehr viel mehr getan werden, um die technischen Möglichkeiten ihrer anonymen oder pseudonymen Inanspruchnahme und Bezahlung zu schaffen und auszubauen. Deshalb sollte die Bundesregierung Projekte zur Entwicklung von Sicherheitsinfrastrukturen und zur Umsetzung des Gebotes der Datensparsamkeit verstärkt fördern.

Auch wenn bestimmte Elemente eines modernen Datenschutzrechts aus der Multimediagesetzgebung in das allgemeine Datenschutzrecht übernommen werden sollten, besteht keine Veranlassung, auf die besonderen Datenschutzvorschriften für den Bereich der Tele- und Mediendienste insgesamt zu verzichten. Den spezifischen Risiken der Nutzung von Online-Diensten kann mit den Mitteln des allgemeinen Datenschutzrechts nicht wirksam begegnet werden.

3.3.2 Unabhängigkeit der Datenschutzkontrolle beim Ostdeutschen Rundfunk Brandenburg

Zur Gewährleistung des Datenschutzes im Bereich der Medien hat der Gesetzgeber abzuwägen zwischen dem Grundrecht der Betroffenen auf informationelle Selbstbestimmung einerseits und der Medien- bzw. Rundfunkfreiheit andererseits. Diese Abwägung hat der brandenburgische Gesetzgeber im Gesetz über den Ostdeutschen Rundfunk Brandenburg (ORB) dadurch vorgenommen, dass das Landesdatenschutzgesetz uneingeschränkt nur für den nicht-publizistischen Bereich anzuwenden ist. Im publizistischen (journalistisch-redaktionellen) Bereich gelten dagegen nur die Vorschriften über die Datensicherung. Diese differenzierte Regelung trägt den Besonderheiten der freien Berichterstattung durch Rundfunk und Fernsehen Rechnung, denn eine Anwendung der Zulässigkeitsvoraussetzungen für die Datenverarbeitung durch öffentliche Stellen im Datenschutzgesetz auf den öffentlich-rechtlichen Rundfunk würde eine unzulässige Beschränkung der Recherchefreiheit der Journalisten be-

deuten.

Diese verfassungsrechtlich gebotene Unterscheidung im materiellen Recht findet aber keine Entsprechung auf der Ebene der Datenschutzkontrolle. Bisher überwacht eine vom Rundfunkrat des ORB gestellte interne Beauftragte für den Datenschutz die Einhaltung der datenschutzrechtlichen Vorschriften bei der gesamten (publizistischen und nicht-publizistischen) Tätigkeit der Rundfunkanstalt. Demgegenüber hat der vom Parlament gewählte Landesbeauftragte für den Datenschutz Kontrollbefugnisse bisher weder im publizistischen noch im nicht-publizistischen Bereich. Eine Beschränkung ist allerdings nur im publizistischen Bereich gerechtfertigt. Für eine Sonderbehandlung des ORB im Bereich der nicht-publizistischen, administrativ-wirtschaftlichen Verarbeitung personenbezogener Daten sprechen weder sachliche noch rechtliche Gründe.

Die Rundfunkanstalt ist unserem Vorschlag, das ORB-Gesetz dementsprechend zu ändern und die Kontrollbefugnis des Landesbeauftragten auf den administrativ-wirtschaftlichen Bereich ihrer Datenverarbeitung zu erstrecken, mit dem Argument entgegengetreten, damit würde die verfassungsrechtlich gebotene Staatsferne des Rundfunks beeinträchtigt. Dem ist entgegenzuhalten, dass der Landesbeauftragte für den Datenschutz keine Befugnisse hat, die einer klassischen Staatsaufsicht gleichkommen, sondern lediglich datenschutzrechtliche Mängel feststellen und beanstanden kann. Für deren Behebung bleibt die Rundfunkanstalt selbst verantwortlich. Auch nach unserem Vorschlag würde der ORB keiner weitergehenden staatlichen Aufsicht unterworfen als nach geltendem Recht. Außerdem ist nicht erkennbar, weshalb eine staatsfreie Rundfunkberichterstattung gefährdet werden soll, wenn der Landesdatenschutzbeauftragte z. B. die ordnungsgemäße Verarbeitung von Daten der Rundfunkteilnehmer bei der Gebühreneinzugsstelle des ORB oder dessen Auftragnehmerin, der Gebühreneinzugszentrale in Köln, prüfen würde. Auch gegen die unabhängige Rechnungsprüfung des Jahresabschlusses der Rundfunkanstalt durch den Landesrechnungshof sind bisher keine verfassungsrechtlichen Einwände erhoben worden.

Außerdem gibt es seit dem Ablauf der Anpassungsfrist für die EG-Datenschutzrichtlinie im Oktober 1998 triftige europarechtliche Gründe dafür, die gegenwärtige Organisation der Datenschutzkontrolle im Rundfunkbereich zu verändern. Artikel 9 dieser Richtlinie lässt Ausnahmen vom europäischen Datenschutz-Mindeststandard nur insoweit zu, als sie notwendig sind, um das Recht auf Privatsphäre mit den Vorschriften über die freie Meinungsäußerung in Einklang zu bringen. Mit anderen Worten: der Gesetzgeber ist zur Differenzierung verpflichtet, und zwar sowohl auf der Ebene des materiellen Datenschutzrechts als auch auf der Ebene der Datenschutzkontrolle. Eine Privilegierung des Rundfunks auf beiden Ebenen ist nur im publizistischen Bereich zulässig. Die Richtlinie schreibt außerdem vor, dass die datenschutzrechtlichen Kontrollstellen ihre Aufgaben "in völliger Unabhängigkeit" wahrnehmen. Dem entspricht es nicht, wenn die Rundfunkanstalt auch außerhalb des journalistisch-redaktionellen Bereichs ausschließlich von einer Datenschutzbeauftragten kontrolliert wird, die der datenverarbeitenden Stelle "Ostdeutscher Rundfunk Brandenburg" angehört.

Der Vorschlag des Landesbeauftragten zur Modifizierung der Datenschutzkontrolle

beim Ostdeutschen Rundfunk Brandenburg ist in die Beratungen der Landtagsausschüsse über den Gesetzentwurf der Landesregierung zur Änderung des ORB-Gesetzes[33] einbezogen worden. Diese Beratungen sind noch nicht abgeschlossen.

Die Verarbeitung personenbezogener Daten bei der Landesrundfunkanstalt sollte nur insoweit einer unabhängigen Kontrolle durch den Landesbeauftragten für den Datenschutz entzogen sein, als sie zu journalistisch-redaktionellen Zwecken erfolgt.

4. Inneres

4.1 Polizei

4.1.1 Datenschutzaspekte der polizeilichen Informationsverarbeitung

Als die brandenburgische Polizei 1990 ihre Arbeit aufnahm, erhielt sie mit den von der ehemaligen DDR und aus der Übergangszeit übernommenen polizeilichen Sammlungen zwar einen großen Datenbestand, dem die in den einzelnen Polizeipräsidien und im Landeskriminalamt zur Verfügung stehende Informations- und Kommunikationstechnik (IuK) jedoch nicht entsprach. Qualität und Ausbaustand waren in den einzelnen Standorten höchst unterschiedlich. Es dauerte mehrere Jahre, bis in einer ersten Ausbaustufe überall ein weitgehend einheitlicher Standard der IuK erreicht war.

POLIKS

Die zweite Ausbaustufe begann 1994 mit den Vorbereitungen für die Einführung eines polizeilichen Datenverarbeitungssystems unter dem Namen **POL**izei **I**nformation **K**ommunikaton **S**achbearbeitung (POLIKS), das zusammen mit Berlin entwickelt werden soll. Auf der Grundlage eines Verwaltungsabkommens haben die beiden Länder 1994 ein gemeinsames Soll-Konzept erarbeitet und eine Voruntersuchung erstellen lassen[34]. Eine gemeinsame Arbeitsgruppe hat bisher im Wesentlichen die Datenverarbeitungssysteme anderer Bundesländer auf ihre Geeignetheit für POLIKS Berlin-Brandenburg geprüft. Ungeachtet der gemeinsamen Planung besteht Einvernehmen, dass die Polizeien beider Bundesländer weiterhin eigenständige Landessysteme auf der Grundlage ihrer unterschiedlichen gesetzlichen Vorschriften betreiben.

Unterdessen sind mit der Automation in der Zentralen Bußgeldstelle der brandenburgischen Polizei und dem Einsatzleitsystem für die brandenburgische Polizei (ELBOS) einzelne Komponenten von POLIKS landesweit in Betrieb gegangen[35]. Im Berichtszeitraum ist durch die bevorstehende bzw. bereits abgeschlossene Einführung weiterer Anwendungen ein neuer Ausbaustand erreicht, der zugleich auch ein deutli-

cher Qualitätssprung ist und nicht ohne Auswirkungen auf die mit der polizeilichen Datenverarbeitung verbundenen Grundrechtseingriffe für die Betroffenen bleiben wird.

PASS

Mit der Entscheidung für das sächsische Polizeiauskunftssystem wird der brandenburgischen Polizei unter dem Namen **P**olizeiliches **A**uskunfts**s**ystem - **S**traftaten (PASS) Ende 1999 eine wichtige weitere POLIKS-Komponente zur Verfügung stehen. Bis dahin muss das sächsische System an das brandenburgische Polizeiaufgabengesetz, den im Vergleich mit Sachsen anderen Organisationsaufbau sowie an die verwaltungsinternen Arbeitsabläufe der brandenburgischen Polizeibehörden angepasst werden.

Mit PASS hat sich die Landesregierung für ein Auskunftssystem entschieden, das nur eine zentrale Speicherung aller Ermittlungsvorgänge zulässt, ohne dass landesweite Bedeutung, Deliktschwere, Überregionalität des Täters u. ä. berücksichtigt werden können. Unter datenschutzrechtlichen Gesichtspunkten wäre ein Systemaufbau zu bevorzugen, der es ermöglicht, einen Ermittlungsvorgang solange auf Präsidiumsebene zu speichern, bis die Ermittlungsergebnisse eine Einstellung in den zentralen Bestand - mit landesweitem Zugriff - rechtfertigen. Es bleibt abzuwarten, ob die Zugriffsfunktionen und Rechtevergabemodalitäten, die erst nach Beendigung des derzeit laufenden Pilotbetriebs festgelegt werden, den datenschutzrechtlichen Anforderungen an das System genügen.

Das Datenverarbeitungssystem PASS ist ein Nachweissystem zu Personen und Sachen im Zusammenhang mit Straftaten, das u. a. Auskunft darüber gibt, ob eine Ausschreibung zur Personen- bzw. Sachfahndung vorliegt und ob erkennungsdienstliche Unterlagen vorhanden sind. Zu jedem Personendatensatz gehört eine ausführliche Personenbeschreibung.

Allgemeiner Zweck von PASS ist es, die brandenburgische Polizei bei der Wahrnehmung ihrer Aufgaben zu unterstützen. Die Datei wird betrieben, um Informationen

- für die Aufklärung von Straftaten und die Feststellung von Tatverdächtigen,
- zur Gefahrenabwehr einschließlich der vorbeugenden Bekämpfung von Straftaten,
- für die Personenidentifizierung,
- für das taktische Vorgehen und die Eigensicherung der Polizei,
- für die Erstellung von Lagebildern und Führungsaufgaben

bereitzustellen.

Mit Hilfe von PASS werden

- die polizeiliche Kriminalstatistik (PKS),

- die kriminalpolizeilichen Meldedienste (KPMD und KPMD-S)

erstellt.

Durch verschiedene Auswertungsfunktionen, wie z. B. die Täterlichtbildsuche über erkennungsdienstlich behandelte Personen oder die Recherche auf der Grundlage von Hinweisen über die Begehungsweise einer Straftat (modus operandi-Recherche), werden die Ermittlungen zur Aufklärung von Straftaten unterstützt. Eine Recherchefunktion für Finger- bzw. Handflächenabdrücke ist allerdings nicht vorgesehen, weil der brandenburgischen Polizei dazu bereits das Automatisierte Fingerabdruck-Identifizierungssystem (AFIS) zur Verfügung steht. Der Personendatensatz in PASS enthält lediglich einen Hinweis auf Fingerabdruckunterlagen.

Im Regelfall löst der für den technischen Betrieb der Datenbank zuständige Zentraldienst der Polizei für Technik und Beschaffung (ZTB) den Löschungsvorgang aus. Er teilt den kriminalaktenführenden Stellen der Polizeipräsidien, die für die Datenbankpflege verantwortlich sind, das bevorstehende Aussonderungsprüfdatum mit, so dass diese bei den sachbearbeitenden Dienststellen die Prüfung veranlassen können, ob das in Rede stehende Datum zur Aufgabenerfüllung weiterhin gespeichert werden muss. Der Datensatz wird automatisch gelöscht, wenn der ZTB keine Rückmeldung über die erforderliche Speicherungsverlängerung von der kriminalaktenführenden Stelle erhält. Diese automatische Löschungsvariante, bei der nur ein erneuter Arbeitsschritt die Verlängerung bewirkt, wird von uns als datenschutzgerecht begrüßt.

Im Gegensatz dazu werden Einzelfalllöschungen von der Kriminalaktenhaltung veranlasst. Die endgültige Festlegung des dazu vorgesehenen Verfahrens wird erst nach Beendigung des Pilotprojekts erfolgen.

Zur Sicherung der im PASS-Betrieb notwendigen Datenübermittlungen werden die Verschlüsselungsprogramme des polizeiinternen Datenübertragungsnetzes bzw. des Landesverwaltungsnetzes genutzt.

In PASS wird jeder Zugriff mit

- abgefragtem Datensatz,

- Bearbeiter und Nutzergruppe,

- PC,

- Datum,

- Abfragetyp,

- Abfrageklasse

protokolliert. Wie lange die Protokolldateien aufbewahrt werden, ist noch nicht festgelegt.

Zum Jahresbeginn 1999 ist im Landeskriminalamt und im Polizeipräsidium Cottbus der Pilotbetrieb mit Echtdaten angelaufen. In einem Zeitraum von vier Monaten sollen die sich aus der brandenburgischen Polizeistruktur und der Bearbeitungsorganisation ergebenden Verfahrensabläufe in PASS erprobt werden. Getestet werden sowohl das Sachbearbeiterprinzip als auch die zentrale Dateneingabe. Im ersten Fall gibt der Sachbearbeiter im Schutzbereich die Daten direkt über seinen PC in den Server im Polizeipräsidium ein. In einer nächtlichen Aktualisierungsphase werden sie in den Zentralrechner beim ZTB überspielt und stehen dann landesweit zur Verfügung. Im zweiten Fall stellt der Sachbearbeiter im Schutzbereich am PC den Eingabebeleg her, der von der zentralen Datenstelle des Präsidiums auf seine Richtigkeit geprüft und dann erst in den PASS-Rechner eingestellt wird. Die Entscheidung, welche Variante die geeignetere ist, fällt erst nach Abschluss des Pilotbetriebs. Ab Mai 1999 sollen die anderen Polizeipräsidien an PASS angeschlossen werden.

Im Berichtszeitraum hat uns das Innenministerium den Entwurf einer Dateibeschreibung zu PASS zugeschickt. Von einer Stellungnahme haben wir abgesehen, weil wegen des bevorstehenden Pilotbetriebs der Datei im Landeskriminalamt und im Polizeipräsidium Cottbus datenschutzrechtlich relevante Aspekte noch nicht geregelt sind. Einzelne Fragen, die sich aus der Dateibeschreibung ergeben haben, wurden im Zuge einer Vorführung der Datei erörtert.

Bei der Erläuterung des in jedem Datenbankbereich vorhandenen Datenfelds "Sondervermerke" stellte sich heraus, dass das Handbuch dazu Festlegungen enthält, die dem beabsichtigten Zweck, nämlich durch ein Freitext-Datenfeld die Möglichkeit zusätzlicher nicht vorgegebener Hinweise zur Verfügung zu stellen, zuwiderlaufen. Aufgrund der Formulierungen war zu befürchten, dass weitere, für die Aufgabenerfüllung nicht unbedingt erforderliche Informationen erhoben würden mit dem Ziel, sie in das Datenfeld einzustellen. Das Innenministerium hat eine Überarbeitung des Handbuchs zugesagt.

POLYGON

Die brandenburgische Polizei betreibt seit Jahren sog. ad-hoc-Dateien im Rahmen größerer Ermittlungsverfahren. Nach rechtskräftigem Abschluss der Gerichtsverfahren sind die Dateien bisher aufgelöst und die Datensätze gelöscht worden. Eine Übernahme in auf Dauer betriebene Dateien fand nur statt, wenn zu dem Betroffenen eine Kriminalakte geführt wurde.

Bei den mit der Anwendungssoftware POLYGON betriebenen Dateien "Komplexe Ermittlungsverfahren - KEV" handelt es sich jedoch nur vordergründig um ein den bisherigen ad-hoc-Dateien vergleichbares Instrument kriminalpolizeilicher Ermittlungen. Wie die ad-hoc-Anwendungen erfüllen die KEV-Dateien die Funktion einer Personen-,

Sachen- und Ereignisregistratur. POLYGON stellt jedoch weit darüber hinausgehende Recherche- und Analysemöglichkeiten zur Verfügung, die zudem durch die grafische Darstellungsform und einfache Handhabung benutzerfreundlicher sind als vergleichbare Anwendungen. KEV-Dateien sind ein Verdachtsgewinnungs- bzw. Verdachtsverdichtungsinstrument. Wie auch schon die ad-hoc-Dateien enthält KEV neben Daten, deren Tatbezug bzw. -relevanz zu Straftaten aufgrund von Ermittlungen schon bestätigt worden ist, auch solche Daten, die lediglich aufgrund bestimmter Merkmale eingestellt werden, ohne dass ihre Relevanz bereits nachweisbar ist. Solange die Datei zu dem Zweck betrieben wird, Aufklärung und Verfolgung bereits begangener Straftaten in einem bestimmten Ermittlungsverfahren zu unterstützen, ergibt sich keine besondere datenschutzrechtliche Problematik.

Datenschutzrechtlich problematisch wird die Anwendung "KEV" allerdings durch die beabsichtigte Nutzung zur vorbeugenden Bekämpfung von Straftaten. Damit wird der Rahmen, der durch die Verarbeitung personenbezogener Daten im Zusammenhang mit einem bestimmten Ermittlungsverfahren vor allem zeitlich begrenzt war, erheblich ausgeweitet.

Ausschlaggebend für die weitere Speicherung in der Anwendung ist der Bezug zu als besonders gemeingefährlich angesehenen Straftaten, z. B. aus dem Bereich der organisierten Kriminalität oder des politischen Strafrechts. Maßstab, ob die Speicherungsschwelle erreicht worden ist, ist weniger das Delikt als solches, als vielmehr die jeweils gültigen Definitionen unklarer Rechtsbegriffe, wie z. B. "Straftat von besonderer Bedeutung" in der Definition des § 10 Abs. 3 Brandenburgisches Polizeigesetz (BbgPolG)[36], der bei Kontakt- und Begleitpersonen der Beschuldigten die Voraussetzung ist, ihre Daten in die Datei einzustellen. Auch wenn die Daten aus strafrechtlichen Ermittlungsverfahren übernommen werden und sich damit noch ein Bezug zu einem bestimmten Ermittlungsverfahren herstellen lässt, handelt es sich dennoch um eine verfahrensübergreifende Datei. Die Verarbeitung personenbezogener Daten erreicht dadurch eine andere Qualität, die tiefer in die Persönlichkeitsrechte der Betroffenen eingreift als bisherige Verarbeitungsformen.

Dies stellt nicht nur in datenschutzrechtlicher Hinsicht besondere Anforderungen an die Datenpflege. Die Betroffenen müssen eine Speicherung personenbezogener Daten zu ihrer Person nur hinnehmen, wenn die Erforderlichkeit durch Tatsachenfeststellungen belegt ist. Dies gilt insbesondere für Kontakt- und Begleitpersonen.

1996 wurde die Beschaffung des Informationssystems "POLYGON" beschlossen. Nach einer Systemerprobung im LKA und in einem Polizeipräsidium ist das System im vergangenen Jahr in allen Polizeipräsidien zu Ermittlungen in den Deliktsbereichen Organisierte Kriminalität und Staatsschutz installiert worden. Derzeit läuft die Anwendung als lokal in den jeweiligen Präsidien betriebene Datei, abgeschottet von anderen Dateien. Ein landesweiter Datenverbund der POLYGON-Anwendungen wird jedoch bereits geprüft.

4.1.2 Datenverarbeitungssystem zur Unterstützung von Telefonüberwachungsmaßnahmen

Im Berichtszeitraum ist das Landeskriminalamt mit einem modernen digitalen Datenverarbeitungssystem zur Abwicklung der Telefonüberwachungsmaßnahmen ausgestattet worden (TÜ-Maßnahmen).

Bei einer Vorführung des System im Landeskriminalamt fanden sich keine datenschutzrechtlichen Mängel bei den automatisierten Verfahrens- und Organisationsabläufen.

Das System zeichnet im Rahmen einer Überwachung die Gespräche des betroffenen Anschlusses auf, speichert die vom Betreiber an das LKA übermittelten Verbindungsdaten dem aufgezeichneten Telefongespräch hinzu und legt den gesamten Datensatz in einem Zwischenspeicher ab. Für jede Telefonüberwachungsmaßnahme steht in dem Zwischenspeicher eine eigene Magnetic Optical Disk (MOD) zur Verfügung. Die Auswertung erfolgt nur auf der MOD des Zwischenspeichers. Im Endausbaustand ist vorgesehen, dass der Sachbearbeiter die aufgezeichneten Telefongespräche an einem gewidmeten Arbeitsplatzrechner im Polizeipräsidium über das Landesverwaltungsnetz auswertet.

Die Durchführung einer TÜ-Maßnahme ist in drei Phasen unterteilt:

- Aktive Phase

Das System speichert alle Informationen, die während des von der richterlichen Anordnung umfassten Zeitraums eingehen.

- Zwischenphase

Auch nach Ablauf des richterlich angeordneten Überwachungszeitraums stehen die aufgezeichneten Gespräche dem Sachbearbeiter noch ca. 1/4 Jahr zur Verfügung.

- Archivierungsphase

Die MOD wird geschlossen und der dazugehörige Datensatz im Zwischenspeicher gelöscht. Danach ist der Zugriff auf die aufgezeichneten Gespräche nur noch unter besonderen Voraussetzungen möglich.

Der Wortlaut der richterlichen Anordnung bestimmt den Zeitraum, innerhalb dessen die Überwachung durchgeführt wird. Unabhängig vom tatsächlichen Beginn der Gesprächsaufzeichnung schalten sowohl die Datenbank im Landeskriminalamt als auch der Betreiber die Aufzeichnung automatisch ab, wenn das vor Beginn der Aufzeichnung eingegebene Fristende erreicht ist.

Da alle unter dem überwachten Anschluss ein- bzw. ausgehenden Gespräche aufge-

zeichnet werden, enthält die Datei auch Telefonate mit Personen, denen aus persönlichen Gründen, z. B. als Familienangehörige, oder aus beruflichen Gründen, z. B. als Rechtsanwälte oder Ärzte, ein Zeugnisverweigerungsrecht zusteht (§§ 52, 53 Strafprozessordnung). Neben Gesprächen, die für das Ermittlungsverfahren von Bedeutung sein können, gibt es Gespräche, bei denen sich im Verlauf der Auswertung herausstellt, dass sie nicht ermittlungsrelevant sind. Zur Auswertung hört der ermittelnde Polizeibeamte zumindest in alle aufgenommenen Telefonate hinein und kennzeichnet die jeweiligen Gespräche entsprechend ihrer Verwertbarkeit für das Ermittlungsverfahren. Die Entscheidung, ob und in welcher Weise einzelne Gespräche in das Ermittlungsverfahren einfließen, trifft der ermittlungsführende Staatsanwalt. Nach der Entscheidung des Staatsanwalts über den Status werden nicht zu verwertende Gespräche durch einen Sperrvermerk der Auswertung entzogen. Die Aufhebung des Sperrvermerks bedarf einer erneuten staatsanwaltschaftlichen Entscheidung.

Jeder Zugriff auf die Datei wird umfassend einschließlich des Zwecks (Anhören/Auswerten/Sperren) protokolliert.

Die Entwürfe von Dateibeschreibungen zur "Informations- und Wiedergabedatei von Einzelgesprächen der Telekommunikations-Überwachungsmaßnahmen" und zur "Benutzerverwaltung - TKÜ" enthielten noch keine Festlegung zu Prüf- bzw. Löschungsfristen. Gem. § 100 b Abs. 6 Strafprozessordnung (StPO) müssen die durch eine TÜ-Maßnahme erlangten Unterlagen sowie die aufgezeichneten Gespräche unter Aufsicht der Staatsanwaltschaft unverzüglich vernichtet werden, wenn sie zur Strafverfolgung nicht mehr erforderlich sind. Um sicherzustellen, dass solche Unterlagen und die aufgezeichneten Gespräche nicht länger als unbedingt erforderlich aufbewahrt werden, haben wir angeregt, in der Dateibeschreibung festzulegen, dass das für die Durchführung der TÜ-Maßnahmen zuständige Landeskriminalamt innerhalb regelmäßiger Fristen bei der Staatsanwaltschaft nachfragt, ob die weitere Aufbewahrung noch erforderlich ist. Endgültige Dateibeschreibungen sind uns im Berichtszeitraum noch nicht zugegangen.

Insgesamt ist festzustellen, das dieses polizeiliche Informationsverarbeitungssystem bei entsprechender Nutzung eine datenschutzrechtliche Verbesserung bringt.

Problematisch ist allerdings, dass die Zahl der angeordneten Telefonüberwachungsmaßnahmen in den letzten Jahren stark angestiegen ist, ohne dass Erkenntnisse darüber vorliegen, ob diese Eingriffe in das Fernmeldegeheimnis konkrete Erfolge bei der Verbrechensbekämpfung gebracht haben. Der Bundesgesetzgeber sollte eine Berichtspflicht der anordnenden Richter nach dem Vorbild der USA (wiretap-reports) einführen. Anhand der so gesammelten Erkenntnisse über den Einfluss von Telefonüberwachungsmaßnahmen auf den Ausgang von Strafverfahren sollte der in den letzten Jahren ständig erweiterte Katalog von Straftaten, zu deren Aufklärung abgehört werden darf, einer kritischen Prüfung unterzogen werden.

4.1.3 DNA-Analysedatei

Neue Rechtsgrundlagen

Nachdem im vergangenen Jahr mehrere Sexualverbrechen, in deren Verlauf die minderjährigen Opfer getötet worden waren, die Öffentlichkeit erschüttert hatten, beschloss das Bundesministerium des Inneren, beim Bundeskriminalamt eine Datei für die DNA-Identifizierungsmuster von Sexualstraftätern einzurichten. Die heftige Kritik der Datenschutzbeauftragten des Bundes und der Länder an dem Vorhaben richtete sich nicht gegen die Datei, deren Erforderlichkeit nicht von der Hand zu weisen ist, sondern vielmehr gegen die Absicht der Bundesregierung, die Datei auf der unzureichenden Grundlage des Bundeskriminalamtgesetzes[37] zu errichten.

Der Auffassung, die Verarbeitung personenbezogener Daten einschließlich der DNA-Identifizierungsmuster zur Aufklärung von Straftaten sowie zur vorbeugenden Verbrechensbekämpfung bedürfe als Eingriff in die Grundrechte der Betroffenen einer normenklaren Spezialvorschrift, hat sich schließlich auch die Bundesregierung angeschlossen und einen Gesetzentwurf zur Änderung der Strafprozessordnung vorgelegt. Mit dem DNA-Identitätsfeststellungsgesetz[38] ist die Strafprozessordnung um Regelungen zur Nutzung der DNA-Analyse-Datei für die Strafverfolgung und zur vorbeugenden Bekämpfung von Straftaten (§ 81 g StPO) ergänzt worden. Der Katalog der Straftaten, bei denen den Beschuldigten Körperzellen entnommen und ein DNA-Identifizierungsmuster erstellt werden darf, beschränkt sich nicht mehr nur auf Straftaten gegen die sexuelle Selbstbestimmung. Voraussetzung für die Durchführung einer DNA-Analyse ist vielmehr, dass der Beschuldigte einer Straftat von erheblicher Bedeutung, insbesondere

- eines Vergehens gegen die sexuelle Selbstbestimmung,
- einer gefährlichen Körperverletzung,
- eines Diebstahls in besonders schwerem Fall,
- einer Erpressung oder
- eines Verbrechens

verdächtig ist.

Eine DNA-Analyse konnte schon bisher in allen Ermittlungsfällen durchgeführt werden, in denen das Spurenaufkommen auf diese Weise eine Identifizierung des Täters erwarten ließ. Erst die neuerliche Ergänzung der Strafprozessordnung lässt die Durchführung und Nutzung von DNA-Analysen auch außerhalb eines konkreten Strafverfahrens für künftige Strafverfahren zu, wenn eine Prognoseentscheidung

ergibt, dass der Beschuldigte wahrscheinlich erneut eine der genannten Straftaten begehen wird. § 2 DNA-Identitätsfeststellungsgesetz erstreckt die Regelungen bezüglich des Beschuldigten in § 81 g StPO auf bereits verurteilte und ihnen gleichzustellende Personen. § 3 regelt die Speicherung der Daten in der DNA-Analyse-Datei beim Bundeskriminalamt sowie ihre Nutzung. Sowohl die Entnahme von Zellmaterial als auch die anschließende DNA-Analyse und die Speicherung in der DNA-Analyse-Datei setzen jeweils eine richterliche Anordnung voraus (§ 1 DNA-Identitätsfeststellungsgesetz).

Freiwillige Aufnahme in die DNA-Datei?

Im vergangenen Jahr hat uns das Ministerium des Innern den Entwurf einer Errichtungsanordnung mit Stand vom 01.12.1998 zugesandt, zu dem wir Stellung genommen haben. Wir haben insbesondere die Regelung abgelehnt, nach der Identifizierungsmuster, die auf freiwilliger Basis (auch bei sog. Massengentests) gewonnen wurden, zusammen mit den personenbezogenen Daten des Betroffenen in die Datei eingestellt werden können, wenn dieser auch in die Speicherung eingewilligt hat. Die Erstellung und Speicherung von Identifizierungsmustern auf der Basis der Freiwilligkeit wirft vielfältige rechtliche und praktische Probleme auf.

Selbst wenn § 81 a StPO so ausgelegt werden könnte, dass für die Entnahme von Körperzellen die richterliche Anordnung nicht zwingend vorgeschrieben ist, und sie daher auch mit Einwilligung des Betroffenen auf freiwilliger Basis erfolgen kann, bedarf die Analyse der Körperzellen dennoch einer richterlichen Anordnung gem. § 81 f StPO.

Insbesondere aber ist nicht nachvollziehbar, wie die Einwilligung des Betroffenen sich auch auf die Einstellung der Daten zu seiner Person einschließlich des Identifizierungsmusters in die DNA-Analyse-Datei erstrecken sollte. Einzige Voraussetzung für die Speicherung der gewonnenen Daten ist der Richtervorbehalt, der in diesem Falle eine Prognoseentscheidung des Richters darüber ist, ob wegen der Ausführung der Tat, seiner Persönlichkeit oder aufgrund sonstiger Erkenntnisse mit hinreichender Wahrscheinlichkeit angenommen werden kann, dass in Zukunft wieder gegen den Betroffenen ermittelt werden muss. Die richterliche Prognoseentscheidung ist durch die Einwilligung des Betroffenen nicht zu ersetzen. Auch nach umfassender Aufklärung des Betroffenen über die Konsequenzen seiner Einwilligung - gemäß Datenschutzgesetz (§ 4 Abs. 2 BbgDSG) unabdingbarer Bestandteil einer Einwilligung - ist schlechterdings nicht zu erwarten, dass der Betroffene für sich selbst die Wiederholungsgefahr prognostiziert.

Unabhängig davon muss bezweifelt werden, ob der Betroffene überhaupt ausreichend über die Konsequenzen aufgeklärt werden kann, die sich aus der Einstellung seines Identifizierungsmusters in die Datei ergeben. Eine solche Aufklärung schließt ein, dass er über den Verwendungszweck der Daten, bei einer beabsichtigten Übermittlung über die Empfänger der Daten sowie den Zweck der Übermittlung informiert wird.

Da der Betroffene seine Einwilligung jederzeit widerrufen kann, ist auch der Nutzen einer Speicherung von Identifizierungsmustern auf freiwilliger Basis fraglich. Nach dem

Widerruf können die Daten nicht mehr genutzt werden, so dass spätestens dann ohnehin eine richterliche Anordnung für eine erneute Entnahme von Körperzellen, eine weitere richterliche Anordnung für die Untersuchung der entnommenen Körperzellen und, nachdem das Identitätsmuster erstellt worden ist, eine richterliche Prognoseentscheidung über die Einstellung der Daten in die DNA-Analyse-Datei erforderlich sind.

Grundsätzlich sind im Zusammenhang mit der Erstellung und Nutzung von DNA-Identitätsmustern Zweifel an der Freiwilligkeit angebracht. In den weitaus meisten Fällen werden DNA-Analysen bei Personen durchgeführt, bei denen als Beteiligte in einem Ermittlungsverfahren ein Tatverdacht nicht von Vornherein auszuschließen ist. Tatverdächtige in Strafermittlungsverfahren, aber auch Inhaftierte, werden wohl nicht selten nur deshalb in die Speicherung ihrer Daten einwilligen, weil sie hoffen, dann Nachteilen zu entgehen. In solchen Fällen kann nicht mehr von Freiwilligkeit gesprochen werden.

Da im Identitätsfeststellungsgesetz nicht geregelt ist, dass DNA-Identitätsmuster mit Zustimmung des Betroffenen - also ohne richterliche Anordnung - erhoben und in die Datei eingestellt werden dürfen, fehlt dafür die Rechtsgrundlage. Die Regelung der Datenerhebung und Speicherung auf freiwilliger Basis sollte deshalb aus der Errichtungsanordnung gestrichen werden.

4.1.4 Umgang mit Kriminalakten und anderen Daten

- Wie einmal alle alles richtig machten

  Ein Petent hat sich mit der Bitte an uns gewandt, ihn dabei zu unterstützen, dass seine im Zusammenhang mit einem staatsanwaltschaftlichen Ermittlungsverfahren angelegte Kriminalakte vernichtet und die Speicherung im Kriminalaktennachweis Brandenburg (KANBB) gelöscht wird. Der Eingabe war die Einstellungsverfügung der Staatsanwaltschaft beigelegt, der zufolge das Verfahren nach § 170 Abs. 2 StPO eingestellt worden war. Gleichzeitig mit seiner Eingabe hat er selbst beim zuständigen Polizeipräsidium die Löschung bzw. Vernichtung der zu seiner Person geführten Unterlagen beantragt.

Auf Anfrage in der Angelegenheit informierte uns das Polizeipräsidium, dass die in Rede stehenden Unterlagen bereits vernichtet und die dazugehörigen Datenspeicherungen gelöscht seien. Die Staatsanwaltschaft hatte nicht nur dem Betroffenen, sondern auch der Polizei den Verfahrensausgang entsprechend dem zwischen Justiz- und Innenministerium festgelegten Rückmeldeverfahren[39] mitgeteilt. Im Zuge der durch die Benachrichtigung der Staatsanwaltschaft veranlassten Erforderlichkeitsprüfung hatte die Polizei festgestellt, dass die in Rede stehenden Unterlagen zur Aufgabenerfüllung nicht mehr erforderlich waren und sie daraufhin vernichtet.

Im vorliegenden Fall hatten die beteiligten Behörden bereits durch die Beachtung der

gesetzlichen und verwaltungsinternen Vorschriften ein datenschutzgerechtes Behördenhandeln bewirkt. Da jedoch nicht immer davon ausgegangen werden kann - wie der folgende Fall zeigt - sollte jeder Bürger in begründeten Fällen seine Auskunfts- und Einsichtsrechte aktiv wahrnehmen.

- Wie es allzu häufig gemacht wird

So wie im folgenden Fall, der uns auch durch die Eingabe eines Petenten bekannt wurde, wird leider in den beteiligten Behörden - Polizeipräsidien und Staatsanwaltschaften - allzu häufig mit kriminalpolizeilichen Unterlagen umgegangen.

> *Vor mehreren Jahren war der Petent im Verlauf eines gegen ihn geführten Ermittlungsverfahrens erkennungsdienstlich behandelt worden. In dem anschließenden Gerichtsverfahren wurde er von allen Tatvorwürfen freigesprochen. Darauf bemühte er sich um die Vernichtung der erkennungsdienstlichen Unterlagen bei der Staatsanwaltschaft und beantragte Aktenauskunft beim Polizeipräsidium. Das Polizeipräsidium informierte ihn, dass es drei Lichtbilder aus der seinerzeitigen erkennungsdienstlichen Behandlung in der Lichtbildvorzeigekartei führe. Es begründete die Aufbewahrung damit, dass "es auf der Grundlage von polizeirechtlichen und strafprozessualen Bestimmungen" möglich gewesen war, erkennungsdienstliche Unterlagen anzufertigen und verwies auf die Tatvorwürfe, die der Petent ja selbst mitgeteilt habe. Weiterhin erfuhr der Petent, dass eine Kriminalakte dort nicht vorhanden sei, sie werde aber womöglich in dem Polizeipräsidium geführt, in dessen Einzugsbereich er früher seinen Hauptwohnsitz gehabt hatte. Eine Nachfrage ergab, dass dem tatsächlich so war.*

Der Umgang mit den Unterlagen zu dem Petenten entsprach nicht den gesetzlichen Vorschriften und verstieß gegen datenschutzrechtliche Grundsätze.

Gemäß den Richtlinien für die Führung der Lichtbildvorzeigekartei[40] ist die Einstellung in die Kartei an die Voraussetzung geknüpft, dass der Betroffene rechtskräftig verurteilt oder einer rechtswidrigen Tat verdächtig ist und dass Wiederholungsgefahr besteht. Um beurteilen zu können, ob die Voraussetzungen erfüllt sind, bedarf es eines Aktenrückhaltes in Form einer Kriminalakte (Richtlinien zur Führung kriminalpolizeilicher Sammlungen in Verbindung mit dem Erlass über die Führung von Kriminalakten[41]). Wenn die im Polizeigesetz (§ 39 Brandenburgisches Polizeigesetz - BbgPolG) aufgestellten Voraussetzungen zur Registrierung personenbezogener Daten nicht oder nicht mehr erfüllt sind, liegen auch die Voraussetzungen nicht vor, aufgrund derer es zulässig ist, Lichtbilder in einer Lichtbildvorzeigekartei vorrätig zu halten. Die Aufnahme ihrer Fotos in die Kartei ist ein tiefer Eingriff in die Persönlichkeitsrechte der Betroffenen, da sie es hinnehmen müssen, dass sie abgebildet als Tatverdächtige bzw. Verurteilte immer wieder Zeugen und Opfern von Straftaten gezeigt werden. Durch die Verpflichtung, die Kartei in regelmäßigen Abständen, mindestens jedoch einmal jährlich, zu bereinigen, soll sichergestellt werden, dass Fotos derjenigen

---

ABl. (1993) Nr. 84 S. 1605

Personen, bei denen der Tatverdacht entfallen ist, nicht länger als unbedingt erforderlich in der Kartei verbleiben.

Solche regelmäßige Bereinigungen seiner Lichtbildvorzeigekartei hat das Polizeipräsidium offensichtlich unterlassen und damit ebenso wie mit der Aufbewahrung der Fotos ohne Aktenrückhalt gegen die gesetzlichen Bestimmungen verstoßen. Das Gleiche gilt für das Polizeipräsidium, das die Kriminalakte jahrelang aufbewahrt hatte, ohne die Erforderlichkeit zu prüfen (s. unten).

Zur Begründung, warum kriminalpolizeiliche Unterlagen zu lange aufbewahrt werden, verweisen die Polizeipräsidien darauf, dass ihnen der Ausgang des staatsanwaltschaftlichen bzw. des gerichtlichen Verfahrens nicht bekannt sei und sie aufgrund der in der Kriminalakte enthaltenen Anhaltspunkte weiterhin von Tatverdacht und Wiederholungsgefahr ausgehen müssten. Die Kriminalakte sei daher zur polizeilichen Aufgabenerfüllung erforderlich. Dies ist so nicht hinzunehmen.

Gemäß Polizeigesetz (§ 47 Abs. 2 Nr. 3 BbgPolG) sind in Dateien suchfähig gespeicherte personenbezogene Daten und die dazugehörigen zu der Person suchfähig angelegten Akten zu löschen oder zu vernichten, wenn aus Anlass einer Einzelfallbearbeitung festgestellt wird, dass die Daten für die Erfüllung der Aufgaben der speichernden Stelle nicht mehr erforderlich sind. Einzelfallbearbeitung kann beispielsweise ausgelöst werden durch die Mitteilung der Meldebehörden über den neuen Hauptwohnsitz des Betroffenen und die daraufhin erforderliche Übergabe der Kriminalakte an das Polizeipräsidium des neuen Wohnortes. Mit Einzelfallbearbeitung im Sinne des Polizeigesetzes ist jedoch nicht die Ablage einer Bescheinigung in der entsprechenden Kriminalakte gemeint, sondern vor allem eine Erforderlichkeitsprüfung, die immer auch die Nachfrage bei der Staatsanwaltschaft über den Verfahrensausgang einschließt, wenn er der Kriminalakte noch nicht zu entnehmen ist. Dies gilt erst recht für die zu festgelegten Fristen erfolgenden regelmäßigen Erforderlichkeitsprüfungen. Für Kriminalakten ist in der Errichtungsanordnung zum KANBB eine jährliche Prüfung vorgeschrieben. Im Fall des Petenten haben die beteiligten Polizeipräsidien sowohl anlassbezogene als auch regelmäßige Erforderlichkeitsprüfungen nicht mit der gebotenen Sorgfalt durchgeführt.

Die Polizeibehörden als datenverarbeitende Stellen können die weitere Aufbewahrung einer Kriminalakte nicht damit begründen, dass die Staatsanwaltschaft den Verfahrensausgang nicht mitgeteilt habe. Vielmehr werden sie ihrer Verantwortung für die Richtigkeit der gespeicherten Daten nur dann in vollem Umfang gerecht, wenn bei der Erforderlichkeitsprüfung auch der Verfahrensausgang des staatsanwaltschaflichen bzw. des gerichtlichen Verfahrens berücksichtigt worden ist. Es gehört zu den Aufgaben der datenverarbeitenden Stelle, die zur Aufgabenerfüllung erforderlichen Daten selbst aktiv zu erheben, wenn die zuständige Stelle die Mitteilung unterlässt.

4.2 Verfassungsschutz

4.2.1 Sicherheitsüberprüfungsgesetz

Bereits im vergangenen Berichtszeitraum hatte das Ministerium des Innern den Entwurf eines Gesetzes über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen im Land Brandenburg (Sicherheitsüberprüfungsgesetz) vorgelegt, über den wir im 6. Tätigkeitsbericht[42] berichtet haben. In ihrer Stellungnahme zum 6. Tätigkeitsbericht[43] hat sich die Landesregierung auch mit unseren Einwendungen gegen einzelne Regelungen des Entwurfs befasst und dabei an mehreren Stellen unsere Anregungen aufgegriffen. Insgesamt sehen wir jedoch dadurch unsere Bedenken gegen zahlreiche Vorschriften des Entwurfs noch nicht ausgeräumt. Dem Vernehmen nach liegt im Ministerium unterdessen ein neuer, überarbeiteter Entwurf für ein Sicherheitsüberprüfungsgesetz vor, der uns jedoch noch nicht zur Stellungnahme zugegangen ist.

Die zügige Verabschiedung eines datenschutzgerechten Sicherheitsüberprüfungsgesetzes ist dringend geboten, weil der derzeitige Zustand fehlender Rechtssicherheit bei den Sicherheitsüberprüfungen nicht länger hingenommen werden kann.

4.2.2 Automatisierte Bearbeitung von Auskunfts- und Einsichtsbegehren

1997 hat die brandenburgische Verfassungsschutzbehörde ein automatisiertes Registraturprogramm eingeführt, das der Vorgangsverwaltung dient. In dieser Anwendung werden auch die Vorgänge registriert, die bei Anträgen auf Aktenauskunft bzw. Akteneinsicht entstehen. Aus datenschutzrechtlichen Gründen haben wir zur Bearbeitung solcher Anträge folgendes Verfahren vorgeschlagen:

Die Anträge zur Auskunftserteilung sowie weitere bei der Bearbeitung anfallende Unterlagen sollten in einem ausschließlich der Auskunftserteilung vorbehaltenen Vorgang des Bereichs Allgemeine Verwaltung oder des Referats Öffentlichkeitsarbeit aufbewahrt werden. Zur notwendigen Abfrage und Recherche, inwieweit Datenspeicherungen zu den Antragstellern in den einzelnen Referaten vorhanden sind, sollten Laufzettel verwendet werden, die nach der Erledigung der Abfrage wieder an das mit der Auskunftserteilung betraute Referat zurückgehen. Es wäre nicht hinnehmbar, wenn der Antrag auf Erteilung einer Auskunft über evtl. bei der Verfassungsschutzbehörde vorhandene Datenspeicherungen zu weiteren - oder gar erstmaligen - Registrierungen des Antragstellers in den Informationssammlungen führen würde, die die Verfassungsschutzbehörde zur Aufgabenerfüllung gem. § 3 Brandenburgisches Verfassungsschutzgesetz (BbgVerfSchG)[44] beispielsweise zur Beobachtung von verfassungsschutzrelevanten Bestrebungen vorhält.

Die Verfassungsschutzbehörde hat mitgeteilt, dass sie bei der Auskunftserteilung so verfährt.

Unter der Voraussetzung, dass

- der Zugriff auf die personenbezogenen Daten mit der Erledigung des Auskunftsersuchens endet,

- eine Nutzung der personenbezogenen Daten der Antragsteller zur Aufgabenerfüllung der Verfassungsschutzbehörde gem. § 3 BbgVerfSchG, also z. B. zur Beobachtung verfassungsschutzrelevanter Bestrebungen ausgeschlossen wird und

- die Speicherungsdauer das zur Auskunftserteilung unbedingt erforderliche Maß nicht übersteigt,

haben wir keine grundsätzlichen Bedenken gegen die Einstellung der Identdaten (Name, Vorname, Geburtsdatum und -ort sowie Anschrift der Antragsteller in das Registraturprogramm erhoben.

Ein Antrag auf Akteneinsicht beim Verfassungsschutz darf nicht zu einer weiteren oder gar erstmaligen Registrierung des Antragstellers in solchen Dateien führen, die z. B. zur Beobachtung von verfassungsschutzrelevanten Bestrebungen vorgehalten werden.

4.3 Meldewesen

Kein verbesserter Datenschutz im Meldegesetz

Der Landtag Brandenburg hat am 27. Januar 1999 das Erste Gesetz zur Änderung des Brandenburgischen Meldegesetzes[45] (BbgMeldeG) beschlossen. Noch vor Beginn der parlamentarischen Beratung war es im Vorfeld der Bundestagswahl zu zahlreichen Beschwerden und Anfragen zur Weitergabe von Meldedaten an politische Parteien für Wahlwerbezwecke gekommen. Einzelne Städte und Gemeinden hatten generell die Weitergabe von Meldedaten an politische Parteien abgelehnt, was sowohl nach altem als auch nach neuem Landesmelderecht zulässig ist. Das Oberverwaltungsgericht Brandenburg hat ausdrücklich bestätigt, dass politische Parteien und Wählervereinigungen keinen Anspruch auf Auskünfte aus dem Melderegister z. B. über Jungwähler haben[46]. Das Meldegesetz berechtigt die Meldebehörden lediglich, unter bestimmten Voraussetzungen entsprechende Auskünfte an Parteien und Wählervereinigungen zu erteilen, wobei der Gleichbehandlungsgrundsatz beachtet werden muss. Es sah bisher vor, dass die betroffenen Bürger dies nur durch einen Widerspruch unterbinden können. Darauf sind sie bei der Anmeldung hinzuweisen.

Der Regierungsentwurf, der insoweit unverändert Gesetzeskraft erlangt hat, sieht nur eine verstärkte Hinweispflicht auf dieses Widerspruchsrecht durch öffentliche Bekanntmachungen mindestens einmal jährlich vor, wobei angemessene Fristen für die Ausübung des Widerspruchsrecht festgesetzt werden sollen.

Wir hatten demgegenüber empfohlen, die Erteilung von Melderegisterauskünften an Parteien und politische Vereinigungen von der ausdrücklichen Einwilligung der Bürger abhängig zu machen. Die Widerspruchslösung hat sich in der Vergangenheit als nicht praktikabel erwiesen, weil die Bürger entweder den Hinweis darauf übersehen oder aus nicht vertretbaren Gründen die Möglichkeit zum Widerspruch nicht genutzt haben. Auch die verfassungsrechtliche Stellung der Parteien rechtfertigt es nicht, das informationelle Selbstbestimmungsrecht in der Weise einzuschränken, dass das Schweigen der Bürger als Zustimmung gewertet wird. Zudem müsste es gerade im Interesse der politischen Parteien liegen, nur die Daten solcher Bürger für Wahlwerbezwecke zu erhalten, die ausdrücklich erklärt haben, dass sie daran interessiert sind. Allerdings könnte die Einwilligungslösung im Landesrecht nur bei den Wahlen zum Landtag Brandenburg und bei Kommunalwahlen, Volksbegehren und Volksentscheiden sowie Bürgerentscheiden eingeführt werden. Eine vom Melderechtsrahmengesetz des Bundes abweichende Regelung auch für die Wahlen zum Europäischen Parlament und zum Deutschen Bundestag wäre verfassungsrechtlich problematisch, weil die bundesweite Chancengleichheit der Parteien berührt würde.

Auch bei Auskünften an Adressbuchverlage haben wir uns im Gesetzgebungsverfahren für die Einführung der Einwilligungslösung eingesetzt, so wie sie auch schon in Nordrhein-Westfalen gilt. Es ist nicht einsehbar, weshalb Adressbuchverlage und Parteien hinsichtlich des Zugangs zum Melderegister gegenüber anderen gesellschaftlichen Gruppen in dieser Weise privilegiert werden. Zudem besteht im Fall der Adressbuchverlage auch die zusätzliche Gefahr, dass Meldedaten in elektronischen Adressdateien auf CD-ROM gepresst und vermarktet werden, was zusätzliche Verknüpfungsmöglichkeiten und Risiken für das informationelle Selbstbestimmungsrecht der betroffenen Bürger verursacht. Daher hat auch die Konferenz der Datenschutzbeauftragten die Einführung der Einwilligungslösung gefordert[47].

Nach Einbringung des Gesetzentwurfs in den Landtag hatten wir uns mit dem Ministerium des Innern auf einen Änderungsvorschlag verständigt, der sowohl die Einwilligungslösung bei der Weitergabe an Adressbuchverlage als auch die Beschränkung der Verwendung von Meldedaten auf gedruckte Adressbücher vorsah. Selbst dieser abgestimmte Vorschlag fand im Landtag keine Mehrheit.

Jetzt bleibt abzuwarten, ob der Bundesgesetzgeber durch eine entsprechende Regelung im neuen Bundesdatenschutzgesetz den Risiken von elektronischen Adressdateien wirksam begegnen kann.

Der Minister des Innern hatte dem Landesbeauftragten noch vor der Verabschiedung des geänderten Meldegesetzes außerdem in Aussicht gestellt, sich auf Bundesebene für die Einführung der Einwilligungslösung einzusetzen.

Die Landesregierung sollte im Bundesrat eine Initiative zur Änderung des Melderechtsrahmengesetzes ergreifen, um die Weitergabe von Meldedaten an politische Parteien und Adressbuchverlage von der ausdrücklichen Einwilligung der Betroffenen abhängig zu machen.

4.4 Ausländer

4.4.1 Eine datenschutzgerechte Verpflichtungserklärung des Gastgebers

Die Einladung eines visumpflichtigen Gastes ist für den Gastgeber damit verbunden, dass er gem. § 84 Ausländergesetz (AuslG) gegenüber der Ausländerbehörde eine Verpflichtungserklärung abgibt. Diese Verpflichtungserklärung seines Gastgebers muss der ausländische Gast dem zuständigen Konsulat bei der Beantragung des Visums vorlegen. Das von den Ausländerbehörden zur Abgabe der Verpflichtungserklärung verwendete Formular sowie der weitere Umgang mit den dabei erhobenen Daten waren bisher nicht datenschutzgerecht.

Obwohl es an einer ausreichenden Rechtsgrundlage für die Verarbeitung personenbezogener Daten fehlt, mussten die Gastgeber Angaben über ihre wirtschaftliche und häusliche Situation machen, die weit über den Zweck der Verpflichtungserklärung hinausgingen. Darüber hinaus wurden die zum Nachweis der Angaben vorgelegten Unterlagen von den Ausländerbehörden zu den Akten genommen.

Gem. § 84 AuslG gibt der Gastgeber eine Haftungsverpflichtung ab, in der er zusichert, für alle Kosten einschließlich Versorgung im Krankheits- oder Pflegefall aufzukommen, die durch seinen Gast verursacht werden. Aus der Vorschrift ist die Befugnis der Ausländerbehörde für die Erhebung und Verarbeitung der Identdaten (Name, Vorname, Geburtsdatum und -ort, Anschrift und Passdaten) des Gastgebers sowie des Gastes abzuleiten, weil ohne sie die Verpflichtungserklärung ins Leere laufen würde. Eine Befugnis für die Verarbeitung von Daten über die wirtschaftlichen und häuslichen Verhältnisse ist ihr nicht zu entnehmen.

Wie bereits früher berichtet[48], kann die Ausländerbehörde zum Nachweis, ob der Gastgeber in der Lage ist, seine freiwillig eingegangene Haftungsverpflichtung zu erfüllen, höchstens die Vorlage neutraler Einkommensnachweise (aus denen nur das Monatsnettoeinkommen ersichtlich ist) verlangen und darüber einen Vermerk zur Akte nehmen. Die Verpflichtung, mittels Mietvertrag ausreichenden Wohnraum zur Unterbringung eines ausländischen Gastes nachzuweisen sowie das Verfahren, die vorgelegten Unterlagen in Kopie zur Akte des ausländischen Gastes zu nehmen, hielten wir für unzulässig. Das Ministerium des Innern schloss sich zwar unserer Auffassung an, in der Praxis bewirkte dies jedoch keine datenschutzgerechten Änderungen, weil Formular und Verfahren bundeseinheitlich geregelt sind.

Im Herbst vergangenen Jahres hat nun die Bundesregierung endlich ein neues Formular in Aussicht gestellt und die "Hinweise zur Verwendung des bundeseinheitlichen Formulars der Verpflichtungserklärung - §§ 84, 82 und 83 AuslG - Stand Oktober 1998" so geändert, dass im Wesentlichen den datenschutzrechtlichen Anforderungen Rechnung getragen wird. Seit Oktober vergangenen Jahres bestätigt die Ausländerbehörde auf dem Formular lediglich, dass sie keine Zweifel an der finanziellen Leistungsfähigkeit des Gastgebers hat. Zum Nachweis seiner Bonität kann der Gastgeber entweder

- Sparbücher (mit Sperrvermerk),
- neutrale Einkommensnachweise,
- Bankbürgschaften,
- Steuerbescheid oder
- die Bescheinigung eines Steuerberaters

vorlegen.

Die Ausländerbehörde nimmt lediglich einen Vermerk über die vorgelegte Unterlage zu den Akten. Ob ausreichend Wohnraum für die Unterbringung des ausländischen Gastes zur Verfügung steht, muss der Gastgeber nur noch nachweisen, wenn ein langfristiger Aufenthalt geplant ist. Die Durchschrift des Formulars kommt zur Akte. Der Gastgeber erhält das Original, das er an seinen ausländischen Gast weiterleitet, damit dieser es bei der Visumsbeantragung vorlegen kann.

Auch wenn die brandenburgischen Ausländerbehörden noch die ursprünglichen Formulare verwenden, entfallen die dort vorgesehenen Angaben über Einkommen, Arbeitgeber und Wohnungsgröße.

4.4.2 Ausreisepapiere für iranische Staatsbürger

Wie wir erfahren haben, händigen die Ausländerbehörden ausreisewilligen iranischen Asylbewerbern zur Beschaffung der notwendigen Unterlagen ein Formular der iranischen Botschaft aus, das Fragen enthält, die nach deutschem Recht unzulässig sind. Von der Grenzschutzdirektion Koblenz war zu erfahren, dass ein iranischer Reisepass jedoch nicht unbedingt erforderlich ist, weil die Einreise in den Iran auch mit einem Rückreiseschein erfolgen kann. Der für die Ausstellung eines solchen Rückreisescheins von der iranischen Botschaft erstellte Fragebogen enthält im Gegensatz zu dem o. g. Formular nur Fragen, die auch nach deutschem Recht zulässig sind.

Wir haben das Ministerium des Innern gebeten, sicherzustellen, dass die brandenburgischen Ausländerbehörden bei der Erteilung von iranischen Reisepässen nicht mehr mitwirken, sondern ausreisewilligen iranischen Staatsbürgern nur noch den Fragebogen zur Ausstellung des Rückreisescheins aushändigen.

Unter Verweis auf unsere datenschutzrechtlich begründete Ablehnung des Formulars

zur Beantragung eines iranischen Reisepasses ist das brandenburgische Innenministerium unserer Bitte in einem Erlass an die Ausländerbehörden gefolgt.

Das Grundgesetz garantiert jedem, der sich in der Bundesrepublik Deutschland aufhält, den Schutz seiner Persönlichkeitsrechte einschließlich des Rechts auf informationelle Selbstbestimmung unabhängig von seiner Staatsbürgerschaft. Daher dürfen deutsche Behörden auch nicht an Verwaltungsakten ausländischer Staaten mitwirken, die unzulässig in die Grundrechte des Betroffenen eingreifen.

4.5 Personaldaten

4.5.1 Großzügiger Informationsaustausch zwischen Dienstbehörde und ärztlichem Gutachter?

Mit dem Gesetz zur Änderung beamten- und richterrechtlicher Vorschriften vom 21. Dezember 1998[49] ist auch das Landesbeamtengesetz (LBG) in einigen Punkten geändert worden. Von datenschutzrechtlicher Relevanz ist eine Ergänzung in § 115 a, bei der es um den Informationsaustausch zwischen Dienstbehörde und ärztlichem Gutachter bzw. Amtsarzt im Falle der Feststellung der Dienst(un)fähigkeit geht.

Zwar hatten wir rechtzeitig vor der parlamentarischen Behandlung des Regierungsentwurfs die Möglichkeit der Stellungnahme, jedoch sind unsere Vorschläge zu einer datenschutzgerechteren Regelung ohne weitere Rückäußerung der Landesregierung unberücksichtigt geblieben.

Mit der Regelung ist lediglich die fast gleichlautende, datenschutzrechtlich defizitäre Formulierung in § 46 a Bundesbeamtengesetz (BBG) übernommen worden, so dass wir an folgenden Kritikpunkten in der Hoffnung festhalten, dass unsere Überlegungen Anlass zu bundesweiten Diskussionen über eine diesbezüglich möglichst einheitliche datenschutzgerechtere Verfahrensregelung bieten, bevor auch andere Bundesländer gleichlautende, nicht hinreichend normenklare Ergänzungen vornehmen, mit denen den schutzwürdigen Interessen Betroffener nicht angemessen Rechnung getragen wird, und die zudem Gefahren bezüglich der vom Gutachter zu wahrenden ärztlichen Schweigepflicht mit sich bringen.

Zwar wird in der Begründung zu § 115 a LBG darauf hingewiesen, dass die Dienstbehörde ihre Entscheidung nur treffen kann, wenn sie die erforderlichen Entscheidungsgrundlagen kennt (z. B. zur Klärung der Frage, ob eine anderweitige Verwendungsmöglichkeit des Beamten gegeben ist). Ebenfalls zutreffend ist die Feststellung, dass das dienstliche Informationsinteresse und das persönliche Geheimhaltungsinteresse des Beamten in einen gerechten Ausgleich gebracht werden müssen und die Dienstbehörde (daher) nur die Feststellungen und Gründe verlangen kann, die für eine sachgemäße Entscheidung erforderlich sind.

Mit dem allgemeinen Hinweis darauf, dass dabei der Grundsatz der Verhältnismäßigkeit strikt eingehalten werden muss und die Übermittlung medizinischer Einzelheiten wegen der Schwere des Eingriffs in das Persönlichkeitsrecht des Beamten auf das unbedingt erforderliche Maß reduziert ist, wird bei der jetzt geltenden Regelung die gesamte Verantwortlichkeit bezüglich des Erfordernisses offenbarter medizinischer Daten auf den Amtsarzt/ärztlichen Gutachter mit der Gefahr abgewälzt, dass dieser sicherheitshalber oder unsicherheitsbedingt auch Anamnese- und Diagnosedaten in nicht erforderlichem Umfang an die veranlassende Behörde übermittelt.

Demgegenüber müssten aber zumindest insoweit normenklare Vorgaben für die Dienstbehörde festgeschrieben sein, um den Arzt in jedem Einzelfall in die Lage zu versetzen, die Zielrichtung der Untersuchung mit möglichen Alternativen klar erkennen zu können. Dem wird die eingefügte Ergänzung nicht gerecht. Wir hatten daher für § 115 a Abs. 1 LBG folgende Formulierung vorgeschlagen, mit der die veranlassenden Stellen zumindest indirekt veranlasst worden wären, dem untersuchenden Arzt ganz konkrete Angaben zu den Untersuchungsgründen und möglichen Entscheidungszielen zu geben:

"Wird in den Fällen der §§ 111 bis 115 LBG eine ärztliche Untersuchung durchgeführt, darf der die Untersuchung veranlassenden Behörde nur das Ergebnis der Untersuchung übermittelt werden. Abweichend von Satz 1 dürfen die Anamnese und einzelne Untersuchungsergebnisse nur übermittelt werden, soweit deren Kenntnis zur Entscheidung über die konkrete Maßnahme, zu deren Zweck die Untersuchung durchgeführt worden ist, erforderlich ist."

Wir hoffen, dass eine solche Regelung, die im Übrigen bereits im baden-württembergischen Landesbeamtengesetz Berücksichtigung fand, letztlich auch Eingang in das Bundesbeamtengesetz und in die Beamtengesetze der Bundesländer einschließlich Brandenburgs finden wird.

Die gerade erfolgte Ergänzung des Landesbeamtengesetzes weist Mängel auf: Die Übermittlung ärztlicher Daten bei Feststellung der Dienst(un)fähigkeit ist zu unpräzise geregelt. Eine alsbaldige Novellierung des Gesetzes ist deshalb erforderlich.

4.5.2 Behandlung von Einzelpersonalangelegenheiten in Gemeindevertretungen

Unbestritten kann sich jeder Gemeindevertreter oder Stadtverordnete im Rahmen des Haushaltsplans und dessen Anlagen, insbesondere des Stellenplans informieren. Er hat das Recht, allgemeine Anfragen zu Personalgrundsatzangelegenheiten zu stellen. Zunehmend erreichen uns in letzter Zeit Anfragen, die Unsicherheiten dahingehend erkennen lassen, inwieweit Gemeindevertretungen und Stadtverordnetenversammlungen auch berechtigt sind, Informationen über Einzelpersonalangelegenheiten anzufordern und hierüber möglicherweise öffentlich zu befinden. Zudem ist festzustellen, dass selbst bei ordnungsgemäßer Behandlung in nicht-öffentlichen Sitzungen Einzelpersonaldaten an die Öffentlichkeit gelangen und die persönlichen Belange einzelner Bediensteter nicht mehr ausreichend geschützt sind.

Soweit lediglich auf § 36 Gemeindeordnung (GO) abgestellt werden kann, sind ohnehin nur allgemeine Personalinformationen und keine Informationen zu Einzelpersonalangelegenheiten zulässig.

Sollten dem Amtsdirektor oder Bürgermeister durch Beschluss der Gemeindevertretung bzw. Stadtverordnetenvertretung gem. § 73 Abs. 2 Satz 4 GO die Entscheidungszuständigkeiten in Personalangelegenheiten übertragen werden, ist diese Übertragung umfassend, es besteht insoweit kein Rechtsgrund (mehr) zu einer personenbezogenen Einzelinformation im Rahmen laufender Bearbeitung von Personalangelegenheiten.

Anders stellt sich die Situation dar, wenn eine Übertragung der Entscheidungszuständigkeit nicht vorgenommen worden ist und "die Gemeindevertretung auf Vorschlag des hauptamtlichen Bürgermeisters oder Amtsdirektors über die Ernennung, die Anstellung und Entlassung von Beamten sowie die Einstellung, Eingruppierung und Entlassung von Angestellten und Arbeitern entscheidet". Auch hier muss jedoch zum Schutz der Persönlichkeitsrechte der Betroffenen sichergestellt werden, dass eine Offenbarung ihrer Daten nur in dem Umfang erfolgt, der zur Erfüllung des jeweiligen Entscheidungszwecks unabdingbar erforderlich ist.

Diesem Erfordernis ist aber nur zum Teil Rechnung getragen, wenn die Gemeindevertretung bzw. die Stadtverordnetenversammlung einen speziellen Ausschuss einrichtet, der die Einzelfälle in nicht-öffentlicher Sitzung berät und hierüber - ohne Personenbezug - im Plenum mit einem Beschlussvorschlag berichtet. Um die Gefahr einer - möglicherweise auch unbeabsichtigten - Offenbarung von konkreten Einzelpersonaldaten so gering wie möglich zu halten, bedarf es weiterer Verfahrensregelungen. So könnten z. B. für die Behandlung im Ausschuss nummerierte Kopien der erforderlichen Unterlagen an die Ausschussmitglieder verteilt, nach Befassung im Ausschuss eingesammelt und bis auf ein Belegexemplar (für das Sitzungsprotokoll) ordnungsgemäß vernichtet werden.

Die Problematik gewinnt besondere Bedeutung, wenn es sich um die Behandlung konkreter Vorgänge im Rahmen von Widerspruchsverfahren in Beihilfeangelegenheiten handelt.

Auch für Gemeindevertretungen gilt selbst im Rahmen unmittelbarer Zuständigkeit in Einzelpersonalangelegenheiten: Der Umfang der offenbarten Daten und der Empfängerkreis müssen auf das unbedingt erforderliche Maß beschränkt werden.

4.5.3 Lohn- und Personalaktenverwaltung durch Private

Das Ministerium für Ernährung, Landwirtschaft und Forsten informierte uns über die Absicht, Lohn- und Personalunterlagen der nach dem Einigungsvertrag abgewickelten Einrichtungen des Bereichs Ernährung, Landwirtschaft und Forsten Brandenburg durch die DISOS GmbH aufbewahren zu lassen (vgl. Artikel II, § 15 b Viertes Buch Sozialgesetzbuch). Das Unternehmen soll auch Auskünfte an ehemalige Beschäftigte (z. B. zur Altersversorgung) erteilen.

Bei der DISOS GmbH handelt es sich um eine nichtöffentliche Stelle nach § 2 Abs. 4 Satz 1 Bundesdatenschutzgesetz (BDSG), die aus der Bundesanstalt für vereinigungsbedingte Sonderaufgaben hervorgegangen ist[50]. Gegen eine Verwaltung der in Rede stehenden Akten (es wurde ausdrücklich versichert, dass Gesundheitsakten nicht betroffen sind) durch die DISOS GmbH hatten wir keine grundsätzlichen datenschutzrechtlichen Bedenken, soweit die gesetzlichen Anforderungen über die Datenverarbeitung im Auftrag nach § 11 Brandenburgisches Datenschutzgesetz (a. F.) vertraglich erfüllt werden. Besonders hingewiesen haben wir darauf, dass

- nach außen erkennbar ist, dass die DISOS nur im Auftrag des Ministeriums handelt,

- die datenschutzrechtliche Verantwortung beim Ministerium verbleibt,

- das Ministerium festlegt, wer außer den ehemaligen Beschäftigten zur Einholung von Auskünften berechtigt ist,

- die Mitarbeiter der DISOS auf das Datengeheimnis nach § 5 BDSG verpflichtet werden und

- das Unternehmen sich der Kontrolle des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht unterwirft.

Erfreulicherweise wurden diese Hinweise umfassend in den Vertrag aufgenommen.

Der bisher im Ministerium vorhandene hohe datenschutzrechtliche Schutzstandard der sensiblen Lohn- und Personaldaten bleibt durch die vertragliche Ausgestaltung, insbesondere die Unterwerfung der DISOS GmbH unter die Kontrolle des Landesbeauftragten erhalten.

4.6 Statistik

4.6.1 Stand der Vorbereitung für die Volkszählung 2001

Im August 1998 hat die Arbeitsgruppe "Gemeinschaftsweiter Zensus", die im Auftrag der Innenministerkonferenz tätig war, einen Bericht zur Volkszählung 2001 vorgelegt. Es werden im wesentlichen zwei Lösungsvarianten vorgestellt: das sog. Bundesmodell und das sog. Ländermodell. Auch die Innenministerkonferenz selbst hat sich im November 1998 nicht auf eines dieser Modelle verständigen können.

Für beide Modelle ist ein Totalabgleich aller erforderlichen personenbezogenen Daten aus allen Einwohnermelderegistern der Bundesrepublik im Statistischen Bundesamt

vorgesehen, um die sog. Mehrfachfälle festzustellen.

Das Bundesmodell basiert auf den für die Bevölkerungsstatistik bedeutsamen Grunddaten der Melderegister, der Erwerbsstatistik und einem zeitnahen Mikrozensus. Eine personenbezogene Verknüpfung zwischen diesen Statistikteilen ist nicht vorgesehen. Die Schwäche dieses Modells besteht darin, dass die Melderegister nicht ausreichend aktuell sind. Bei diesem Modell werden die Ergebnisse mehr dem Bund und weniger den Ländern und den Kommunen nützen. Allerdings soll das Bundesmodell nur ca. 10 % des Aufwandes für das Ländermodell kosten.

Das Ländermodell geht ebenfalls von den Melderegistern aus. Weil diese aber nach ihrem jetzigen Stand für die Statistik keine zuverlässige Basis bilden, soll zusätzlich eine Gebäude- und Wohnungszählung durchgeführt werden, bei der die Gebäudebesitzer und -verwalter postalisch befragt werden (sog. Ländergrundmodul). Damit könnten die Meldedaten bei den Statistischen Ämtern aktualisiert werden. Wegen der klaren Trennung zwischen Statistik und Verwaltungsvollzug verdient dieser Ansatz aus Datenschutzsicht den Vorzug.

Die auf diese Weise "qualifizierten" personenbezogenen Datensätze der Melderegister sollen dann beim Ländermodell zusätzlich personenbezogen mit den Dateien der Bundesanstalt für Arbeit und mit Dateien anderer Behörden verknüpft werden, um so zu verbesserten erwerbsstatistischen Angaben zu kommen. Zusätzlich ist noch eine Ergänzungsstichprobe im Erwerbsbereich vorgesehen. Datenschutzgerechter wäre es allerdings, wenn diese zusätzlichen Verwaltungsregister so qualifiziert werden könnten, dass die aus ihnen gewonnenen sekundären Einzelstatistiken eine gute Aussagekraft erhielten. Dadurch würde eine personenbezogene Verknüpfung überflüssig.

In unserer Stellungnahme zu diesem Vorhaben, für das es übrigens keine rechtliche Verpflichtung durch die EU gibt, haben wir auch grundsätzliche datenschutzrechtliche Bedenken vorgetragen. Denn die Verfasser des Berichts sind von vornherein und grundsätzlich von einer sekundärstatistischen registergestützten Volkszählung ausgegangen, wobei sie politische Vorgaben und knappe Kassen bei Bund, Ländern und Gemeinden als Begründung anführen. Eine umfassende Primärerhebung ist wegen der hohen Kosten gar nicht diskutiert worden.

Als Motiv für eine Registerzählung wird in dem Bericht die größere Akzeptanz der Bürger genannt. Dabei wird der Begriff der "Belastung" aber nur technisch verstanden. Die eigentliche Belastung besteht vielmehr in der Intensität des Eingriffs in das Recht der Bürger auf informationelle Selbstbestimmung[51]. In diesem Sinn ist die Belastung für die Bürger durch die sekundärstatistische Datenerhebung (hinter ihrem Rücken) mindestens ebenso hoch wie durch eine Primärerhebung. Außerdem ist eine Primärerhebung für die Bürger grundsätzlich durchschaubarer als die Verarbeitung und Verknüpfung riesiger Datenbestände aus der Verwaltung. Auch dürfte die vermutete größere Akzeptanz der Bürger bei einer Registerzählung vor allem darauf beruhen, dass die Bürger bisher über die dann erforderlichen Datenverarbeitungsverfahren nicht aufgeklärt worden sind.

Wie schon das Bundesverfassungsgericht im Volkszählungsurteil festgestellt hat, ist die Verknüpfung vorhandener Verwaltungsdateien gegenüber der Totalerhebung nicht das mildere Eingriffsmittel. Das Gericht hat die Einführung eines Personenkennzeichens als unzulässig abgelehnt[52]. Im Gegensatz zu 1983 ist es heute wegen der modernen Hard- und Software viel leichter möglich, riesige Datenbestände in kurzer Zeit zu verarbeiten und kostengünstig wiederholt zu recherchieren. Dadurch werden Suchbegriffe wie Name, Vorname und Geburtstag eindeutig und entsprechen einem Personenkennzeichen.

Besonders die schon erwähnte geplante zentralistische Zusammenführung der Grunddaten aus allen Einwohnermelderegistern der Bundesrepublik im Statistischen Bundesamt stößt auf datenschutzrechtliche Bedenken. Bisher wurden im Rahmen der Statistik noch nie die personenbezogenen Daten aller Bürger gleichzeitig in einem Verfahren und an einem Ort verarbeitet, weder bei der Volkszählung 1987 noch bei der Gebäude- und Wohnungszählung 1995. Mit diesem neuen Verfahren würde ein Präzedenzfall geschaffen und eine Infrastruktur erprobt, die nicht das Ziel datenschutzrechtlicher Innovation sein kann. Außerdem wäre dieser zentrale Melderegisterabgleich kaum verhältnismäßig, weil hierbei nur die sog. Mehrfachfälle in den Melderegisterdaten dokumentiert werden können. Andere Fälle können nicht oder nur unzureichend erkannt werden (sog. Über- und Untererfassungen in den Melderegistern).

Für die notwendigen vorbereitenden Testrechnungen und für die Volkszählung selbst sind bundesgesetzliche Regelungen erforderlich. Welche Variante der statistischen Erhebung dabei letztlich von Bundestag und Bundesrat bevorzugt wird, lässt sich derzeit noch nicht absehen.

Aus datenschutzrechtlicher Sicht sind folgende Varianten einer Volkszählung vertretbar:

- eine abgerüstete Totalerhebung (postalische Befragung) mit weniger Erhebungsmerkmalen, für die Auskunftspflicht besteht, und einem größeren Fragenkatalog auf freiwilliger Basis oder
- eine Kombination des sog. Ländergrundmoduls mit dem sog. Bundesmodell. Dies bedeutet: Außer beim sog. Ländergrundmodul erfolgen keine personenbezogenen Verknüpfungen zwischen den Statistiken und kein Totalabgleich der Einwohnermeldedaten im Statistischen Bundesamt.

4.6.2 Brandenburgische Beherbergungsstatistik

Im Sommer 1998 wurde im Land Brandenburg eine Statistik über Beherbergungseinrichtungen mit weniger als 9 Betten durchgeführt. Hierfür besteht ein besonderes Interesse, weil die entsprechende Bundesstatistik nur Einrichtungen mit einer Kapazität von mehr als 8 Betten erfasst.

Erhoben wurden bei den Kommunalverwaltungen auf freiwilliger Basis zusammen-

gefasste Angaben zur Anzahl der Beherbergungsstätten und Gästebetten, und zwar getrennt nach Betriebsarten (z. B. Gasthof, Pension, Ferienwohnung, Privatquartier usw.). Diese Erhebung soll alle 3 Jahre durchgeführt werden.

Wir wurden frühzeitig in die Vorbereitungen des Landesamtes für Datenverarbeitung und Statistik (LDS) einbezogen. Da es sich hier um eine Landesstatistik handelt, haben wir darauf aufmerksam gemacht, dass hierfür nach § 7 Abs. 4 Brandenburgisches Statistikgesetz (BbgStatG) eine Verwaltungsvorschrift erforderlich sei. Diese muss die Anforderungen des § 20 BbgStatG bzgl. der Unterrichtung der zu Befragenden berücksichtigen. Eine entsprechende Verwaltungsvorschrift wurde vom Minister für Wirtschaft, Mittelstand und Technologie im Einvernehmen mit dem Minister des Innern im Juli 1998 in Kraft gesetzt.

Zeitgleich wurde bei dieser Erhebung ein weiterer Fragebogen eingesetzt, auf dem auf freiwilliger Basis im Rahmen der Bundesbeherbergungsstatistik gem. § 6 Bundesstatistikgesetz nach neueren Anschriften von Beherbergungsstätten bei den Kommunalverwaltungen gefragt wurde. Gegen beide Erhebungen bestanden aus datenschutzrechtlicher Sicht keine Bedenken.

Bei der brandenburgischen Beherbergungsstatistik haben etwa 97 % der Kommunalverwaltungen statistische Angaben geliefert. Diese Beteiligungsquote zeigt, dass einsehbare und sinnvolle Erhebungen auf freiwilliger Basis einen hohen Zustimmungsgrad erreichen können.

Bei statistischen Erhebungen mehr auf Freiwilligkeit und weniger auf Auskunftszwang zu setzen, war schon immer ein Anliegen der Datenschutzbeauftragten.

4.6.3 Soll es wieder Wahlstatistiken geben?

Neuerdings mehren sich wieder Stimmen von Wahlforschern, Demoskopen und Journalisten, die die 1994 und 1998 ausgesetzte repräsentative Wahlstatistik zukünftig wieder eingeführt sehen wollen. Auch die neue Bundesregierung spricht sich dafür aus.

Begründet wird dies u. a. damit, dass nur aufgrund der amtlichen Wahlstatistik Genaueres über die Wahlbeteiligung und über die Bevorzugung einzelner Parteien von Männern und Frauen in verschiedenen Altersgruppen ausgesagt werden könne. Auch das Lager der Nichtwähler könne anders nicht näher untersucht werden. Wohl auch deshalb titelte eine Zeitung im vergangenen Juli: “Die Bürger sind nicht dumm. Aber gemein. Deshalb belügen sie die Umfrage-Institute“[53].

Die Datenschutzbeauftragten haben sich bereits 1995 für eine datenschutzgerechte Wahlstatistik ausgesprochen und entsprechende Maßnahmen vorgeschlagen[54]. In einem Referentenentwurf vom März 1996, der das Bundeswahlgesetz novellieren

sollte, ist der Vorschlag aufgegriffen worden. Danach sollten folgende Schutzmaßnahmen getroffen werden: die Festlegung einer Mindestgröße für die Stichprobenwahlbezirke; eine Zusammenfassung der Geburtsjahrgänge, die keine Rückschlüsse auf das Wahlverhalten ermöglicht; die Trennung der für die Stimmenauszählung und für die statistische Auswertung zuständigen Stellen; das Verbot der Zusammenführung von Wählerverzeichnis und gekennzeichneten Stimmzetteln; die strenge Zweckbindung für die Statistikstellen bzgl. der ihnen zur Auswertung übergebenen Wahlunterlagen; die Information der Wahlberechtigten in ihrem Wahllokal über die Durchführung der repräsentativen Wahlstatistik durch Aushang. Der Entwurf ist jedoch bei späteren Änderungen des Wahlrechts nicht berücksichtigt worden.

Eine datenschutzgerechte Wahlstatistik ist bei entsprechenden gesetzlichen Vorgaben möglich.

5. Justiz

5.1 Der Große Lauschangriff

Im Berichtszeitraum ist die unter dem Namen "Großer Lauschangriff" seit Jahren heftig umstrittene Änderung des Art. 13 Grundgesetz (GG) zum Abhören in Wohnungen mit denkbar knapper Mehrheit im Bundestag und Bundesrat verabschiedet worden. Damit kann von der Unverletzlichkeit der Wohnung - so lautet immer noch die inoffizielle Bezeichnung des Grundrechtsartikels - kaum noch die Rede sein. Akustisch überwacht werden darf eine Wohnung schon dann, wenn die Strafverfolgungsbehörden annehmen, dass sich dort jemand aufhält, der im Zusammenhang mit besonders schweren Straftaten gesucht wird, selbst wenn der Wohnungsinhaber mit der Straftat nicht in Verbindung gebracht werden kann. Jeder unverdächtige und unbescholtene Bürger muss es nun hinnehmen, dass im Verlauf von Ermittlungsverfahren seine Wohnung abgehört wird, weil die Strafverfolgungsbehörden hier eine "Gangsterwohnung" vermuten. Verschont von einem Großen Lauschangriff bleiben nur Personen, denen aufgrund ihrer Berufstätigkeit ein Zeugnisverweigerungsrecht (§ 53 Strafprozessordnung - StPO) zusteht.

Grundrechte können auch dadurch zu leeren Worthülsen verkommen, dass sie nach und nach ausgehöhlt werden. Obwohl sie weiterhin im Grundgesetz stehen, sind sie ihrer Wirkungskraft beraubt. Ob es mit dem Grundrecht der Unverletzlichkeit der Wohnung durch die Änderung schon so weit gekommen ist, wird sich bei der praktischen Anwendung der gesetzlichen Vorschriften herausstellen. Zu Befürchtungen, dass dieses Grundrecht in seinem Wesensgehalt angetastet sein könnte, besteht jedoch Anlass.

Parlamentarische Kontrolle von Lauschangriffen in Brandenburg

Wegen der grundrechtlichen Sensibilität von Maßnahmen der akustischen Wohnraumüberwachung ist in Art. 13 Abs. 6 GG ein besonderes Kontrollverfahren vorgesehen,

nach dem die Exekutive einmal jährlich dem Parlament Bericht über die durchgeführten Maßnahmen erstattet. Auf der Grundlage dieses Berichts soll ein vom Parlament gewähltes Gremium über evtl. erforderliche Schritte befinden. Die Länder sind verpflichtet ein entsprechendes Kontrollverfahren einzurichten.

Im Berichtszeitraum waren Pläne bekannt geworden, dem G 10-Gremium bzw. der Parlamentarischen Kontrollkommission (PKK) auch die parlamentarische Kontrolle von Lauschangriffen nach Art. 13 Abs. 6 GG zu übertragen und dazu die Geschäftsordnung der jeweiligen Parlamente zu ändern. Wir halten es nicht für sachgerecht, den o. g. Gremien die Kontrolle von Lauschangriffen nach Art. 13 Abs. 6 GG zu übertragen, da hier grundlegende Unterschiede bestehen. In beiden Fällen hat die Ausgestaltung des Verfahrens allerdings erhebliche Bedeutung für die Grundrechtssicherung.

G 10-Gremium und G 10-Kommission kontrollieren die Post- bzw. Telefonüberwachungsmaßnahmen der Geheimdienste (Verfassungsschutz, Bundesnachrichtendienst und Militärischer Abschirmdienst) auf der Grundlage des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldeverkehrs (Gesetz zu Art. 10 GG - G 10-Gesetz). Da diese Eingriffe in das Post- und Fernmeldegeheimnis nach Art. 10 Abs. 2 GG nicht der richterlichen Kontrolle unterliegen, wird der individuelle Rechtsschutz nach §§ 2 und 3 des Ausführungsgesetzes Brandenburg zum G 10-Gesetz (G 10 AGBbg) durch die G 10-Kommission ersetzt. Demgegenüber unterliegen die Lauschangriffe der Strafverfolgungsbehörden und der Polizei in vollem Umfang der gerichtlichen Kontrolle, so dass eine parlamentarische Kontrolle der Einzelfälle dem Gewaltenteilungsgrundsatz zuwiderlaufen würde. Dass die in Artikel 13 GG vorgeschriebene Kontrolle eine ganz andere Funktion hat, ist auch der amtlichen Begründung des Entwurfs zu Art. 13 Abs. 6 GG zu entnehmen, der zufolge die "parlamentarische Kontrolle der gesetzgeberischen Normeffizienz dient und ... Ausdruck der allgemeinen politischen Kontrollfunktion des Parlaments im Rahmen seiner Zuständigkeit gegenüber der Exekutive ist". Diese politische Kontrollfunktion muss auch der Landtag Brandenburg sowohl im Bereich der Gefahrenabwehr als auch der Strafverfolgung wahrnehmen können. Während die Arbeit des G 10-Gremiums und der G 10-Kommission aus nachvollziehbaren Gründen strengster Geheimhaltung unterliegt, ist der Ausschluss der Öffentlichkeit oder gar eine Geheimhaltung des Berichts sowie der Beratung im Fall der Kontrolle von Lauschangriffen nicht vorgeschrieben.

Der Innenausschuss hat das Justizministerium gebeten, in Absprache mit dem Landesbeauftragten einen Vorschlag zur Umsetzung des Artikels 13 Abs. 6 GG auszuarbeiten. Die Gespräche hierüber sind noch nicht abgeschlossen.

Der brandenburgische Landtag muss die Möglichkeit haben, den Bericht der Landesregierung, der nur in anonymisierter Form abzugeben ist, öffentlich zu erörtern und durch einen zuständigen Ausschuss die parlamentarische Kontrolle über die Tätigkeit der Exekutive bei Maßnahmen der akustischen Wohnraumüberwachung auszuüben.

5.2 Großzügige Auskünfte aus dem Grundbuch

Im Jahr 1998 hatten sich wiederum mehrere Petenten an uns gewandt, weil ihrer Meinung nach die Grundbuchämter zu locker im Umgang mit Informationen aus dem Grundbuch gewesen seien.

Einerseits ging es um die Definition des"berechtigten Interesses", dessen Darlegung § 12 der Grundbuchordnung (GBO) bei der Beantragung eines Grundbuchauszugs fordert. Zum anderen wurden uns Fälle vorgetragen, in denen das Grundbuchamt bei seinen Mitteilungen von Eintragungen im Grundbuch, die es vorgenommen hatte, u. a. gegenüber den "aus dem Grundbuch ersichtlichen Personen, zu deren Gunsten die Eintragung erfolgt ist oder deren Recht durch sie betroffen wird" (vgl. § 55 Abs. 2 GBO), nicht korrekt vorgegangen war. In den uns bekannt gewordenen Fällen war der Kreis der Mitteilungsempfänger zu groß gewesen, was die betroffenen Eigentümer empört hatte, nachdem sie zufällig von solchen Informationsmitteilungen erfahren hatten.

Den Grundbuchämtern sollte mehr als bisher verdeutlicht werden, dass die Weitergabe von Informationen über Eintragungen mit Augenmaß zu erfolgen hat. Immer dann, wenn die Mitteilung z. B. an den bisherigen Eigentümer eines Grundstücks oder an Nachbarn erfolgen soll, sollte die Erforderlichkeit der Informationsweiterleitung geprüft werden. Dass das Grundbuchamt berechtigt ist, seine Informationspolitik z. B. über neue Eigentumsverhältnisse oder über eine Belastung restriktiv zu gestalten, ergibt sich schon daraus, dass gem. § 55 Abs. 7 GBO auf die Bekanntmachung solcher Eintragungen teilweise oder sogar ganz verzichtet werden kann.

Aus Gründen des informationellen Selbstbestimmungsrechts der Betroffenen hat das Grundbuchamt zunächst zu prüfen, ob und in welchem Umfang an welche Adressaten Mitteilungen über Eintragungen erforderlich sind, bevor es sich zu einer Informierung Dritter entscheidet.

6. Finanzen

6.1 Unterlassungserklärungen für die "interessierte" Öffentlichkeit

Im gesamten Bundesgebiet setzen sich die Landesbeauftragten für den Datenschutz dafür ein, dass Veröffentlichungen der Verurteilungen und strafbewehrten Unterlassungserklärungen von Steuerberatern wegen Gesetzesverstößen mit Namen und Adressen der Betroffenen nicht mehr in den Mitteilungsblättern der jeweiligen Steuerberaterkammern veröffentlicht wurden. Die Erfolge dieser Bemühungen sind unterschiedlich: einige Steuerberaterkammern halten derartige Veröffentlichungen für unverzichtbar oder meinen, die Mitteilungsblätter seien nicht "für die Öffentlichkeit" bestimmt; andere Kammern verzichten auf die Nennung personenbezogener Daten. Die Steuerberaterkammer Brandenburg hat sich bereit erklärt, bis "zur Schaffung einer einschlägigen Rechtsgrundlage" von solchen Veröffentlichungen abzusehen, da sie mit

uns der Auffassung ist, dass die "Mitteilungsblätter" als Veröffentlichungen für eine breitere Öffentlichkeit bestimmt sind, weil sie nicht nur die Mitglieder der Kammer erreichen sollen.

Die Steuerberaterkammer Brandenburg geht allerdings davon aus, dass die Bekanntgabe "mittels eigens und ausschließlich an die Kammermitglieder gerichteter Rundschreiben" ein Weg sei, der sowohl den Belangen der Kammer als auch denen des Datenschutzes gerecht zu werden sucht. Ein Exemplar des Rundschreibens geht auch an die Oberfinanzdirektion Cottbus, da sie als die Bußgeld- und Strafsachenstelle der Finanzverwaltung die Informationen über Verstöße gegen das Steuerberatungsgesetz und das Gesetz gegen den unlauteren Wettbewerb benötigt. Unsere Dienststelle ist in die Überlegungen zur Einführung dieses Vorgehens einbezogen gewesen. Den Aussagen der Steuerberaterkammer zufolge soll sich das Verfahren bewähren.

6.2 Überraschende Weitergabe von Finanzdaten

Im Berichtsjahr haben sich mehrere Handwerksmeister an den Landesbeauftragten für den Datenschutz gewandt, weil sie es nicht für korrekt hielten, dass das Finanzamt die Handwerkskammer über die finanzielle Situation der Petenten informiert hatte. Die Kammer hatte diese Finanzmitteilungen als Grundlage für die Beitragsfestsetzung verwendet; die Folge war, dass die jeweils Betroffenen im Vergleich zu früheren Jahren erheblich höhere Kammerbeiträge zu zahlen hatten.

In jedem dieser Fälle mussten wir den Betroffenen mitteilen, dass sich sowohl die Handwerkskammer als auch das Finanzamt korrekt verhalten hatten; denn in der Handwerksordnung (§ 113 HandwO) und in der Abgabenordnung (§ 31) ist das Mitteilungsverfahren gesetzlich geregelt worden. Nachdem die Übergangsregelung, die gem. § 113 Abs. 2 Satz 5 HandwO in dem "in Artikel 3 des Einigungsvertrages genannten Gebiet" gegolten hatte, mit dem Ende des Jahres 1997 ausgelaufen war, hatte die Kammer die Beiträge nicht mehr nach den bis dahin geltenden besonderen Berechnungsgrundlagen berechnen können, sondern statt dessen die rechtlich zulässigen Informationen der Finanzämter herangezogen.

6.3 Anprangerung im Adressfeld

Im Rahmen eines Verwaltungsvorgangs wurde ein Petent zur Abgabe einer eidesstattlichen Versicherung aufgefordert. Die entsprechende Vorladung wurde dem Petenten mit Postzustellungsauftrag im Wege der vereinfachten Zustellung übersandt. Auf dem Briefumschlag befand sich neben der Adresse auch die Geschäftsnummer, unter der das Finanzamt die betreffende Angelegenheit führt, und außerdem der Zusatz: "Vorl. z. eid. Vers.".

Der Petent fühlte sich in seinem Recht auf informationelle Selbstbestimmung verletzt und wandte sich an uns. Das Finanzamt, dem wir unsere Auffassung, dass ein so weitgehender Zusatz zu der Geschäftsnummer nicht erforderlich sei, vorgetragen

hatten, wollte unseren Argumenten nicht folgen. Das Ministerium der Finanzen hingegen hat sich unseren Überlegungen angeschlossen. Es hat demzufolge die zuständige Oberfinanzdirektion gebeten, "den Inhalt derartiger Vorladungen künftig durch verschlüsselte Kennzahlen anzugeben, die für Außenstehende keine Rückschlüsse zulassen".

Niemand muss es hinnehmen, durch einen Zusatz im Adressfeld eines an ihn gerichteten Schreibens bloßgestellt zu werden.

7. Arbeit, Soziales, Gesundheit und Frauen

7.1 Arbeit

Die erzwungene Einwilligung

Einem Auszubildenden wurde von seinem Ausbildungsbetrieb eine Einverständniserklärung vorgelegt, mit der er einer Auswertung seiner personenbezogenen Angaben zu nicht näher erläuterten statistischen Zwecken zustimmen sollte. Dies stand im Zusammenhang mit der Förderung des Ausbildungsbetriebes durch die Landesagentur für Struktur und Arbeit Brandenburg GmbH. Auf Nachfrage des Betroffenen soll die Landesagentur darauf hingewiesen haben, dass für den Fall der Verweigerung der Einverständniserklärung das Ausbildungsverhältnis gekündigt werden könne.

Wesensmerkmal einer Einverständniserklärung ist es, dass sie freiwillig erfolgt. Führt die Verweigerung einer Einwilligung zu einem Rechtsverlust, steht die Freiwilligkeit in Frage. Das Formular entsprach auch nicht den Voraussetzungen des § 4 Abs. 2 Brandenburgisches Datenschutzgesetz, wonach der Betroffene im Rahmen einer Einverständniserklärung darauf hinzuweisen ist, dass er die Einwilligung verweigern und mit Wirkung für die Zukunft widerrufen kann, ohne dass ihm hierdurch rechtliche Nachteile entstehen.

Der Schlüssel für die Lösung lag in der Klärung der Frage, welche Statistik in dem Formular angesprochen war. Eine Landesstatistik kann auch in einer Richtlinie vorgesehen sein, darf aber nur auf der Grundlage freiwilliger Auskünfte durchgeführt werden. Werden personenbezogene Daten ausschließlich für eine Statistik erhoben, muss hierfür eine abgeschottete Statistikstelle bestehen. Es muss festgelegt werden, welche personenbezogenen Hilfsmerkmale herangezogen werden und wann diese zu löschen sind. Die Voraussetzungen für eine Landesstatistik sind auch nach Ansicht des Ministeriums nicht gegeben. Vielmehr hat es sich zwischenzeitlich für eine Geschäftsstatistik ausgesprochen, weil letztere nach dem Landesstatistikgesetz ohne weitere Befragung und Einwilligung des Betroffenen mit den für die Antragsbearbeitung erhobenen Daten erstellt werden kann. Dementsprechend hat das Ministerium die Landesagentur informiert und gebeten, ihre Handhabung daran anzupassen. Das

Ministerium wird sich aufgrund unseres Hinweises dafür einsetzen, dass in allen vergleichbaren Fällen gesetzesgemäß verfahren wird. Es hat zugesagt, die Förderrichtlinien, die unter der Überschrift „Statistik“ Zwecke der Antragsbearbeitung, Wirkungskontrolle und Erstellung einer Förderstatistik zusammenfassen, eindeutiger zu formulieren.

Besteht eine gesetzliche Datenverarbeitungsbefugnis, ist es irreführend und damit unzulässig, eine Einwilligungserklärung vom Betroffenen zu erbitten. Eine Einverständniserklärung kommt nur dann in Betracht, wenn die Datenverarbeitung allein vom freien Willen des Betroffenen abhängig ist und die Verweigerung der Erklärung keine rechtlichen Nachteile nach sich zieht. Seine Aufklärung darüber ist eine Voraussetzung für die Wirksamkeit der Einverständniserklärung.

7.2 Soziales

7.2.1 Sozialleistungsträger als verlängerter Arm der Polizei

Früher durften Sozialleistungsträger (z. B. Sozialämter und Krankenkassen) nach § 68 Zehntes Buch Sozialgesetzbuch (SGB X) a. F. anderen Behörden ohne richterliche Anordnung unter bestimmten Voraussetzungen nur genau benannte Sozialdaten, darunter auch die "derzeitige Anschrift" des Hilfeempfängers oder Versicherten, übermitteln. Umstritten war dabei, ob dazu auch der - vorübergehende - aktuelle Aufenthalt in der Sozialleistungsbehörde zählte. Bei den anfragenden Stellen (z. B. der Polizei) war in anderen Bundesländern darüber hinaus die Tendenz zu erkennen, auch Informationen über den nächsten Vorsprachetermin des Betroffenen abzufordern. Beides lässt § 68 SGB X in seiner neuen Fassung nunmehr zu.

In der Gesetzesbegründung wird die Änderung lediglich als Klarstellung bezeichnet. Solchermaßen verharmlost und unter dem Deckmantel des Ersten Gesetzes zur Änderung des Medizinproduktegesetzes hatte die erweiterte Vorschrift bereits den Bundestag passiert, ehe die Landesbeauftragten für den Datenschutz auf sie aufmerksam wurden. Aber weder die Intervention in der Presse, noch die durch unseren Hinweis ausgelösten Aktivitäten der Brandenburgischen Landesregierung im Bundesrat konnten eine Abänderung des Gesetzentwurfs erreichen.

Die Gesetzesbegründung führt aus, es könne "nicht hingenommen werden, dass eine polizeilich gesuchte Person die Sozialverwaltung aufsuchen und aufgrund unterschiedlicher Auffassungen in der Praxis darauf vertrauen kann, dass die Polizei von dem Besuch nichts erfährt". Damit wurde ein besonders krasser Fall herausgegriffen. Dieser hätte aber mit Hilfe einer richterlichen Anordnung auch schon nach dem bisherigen Recht zur Zufriedenheit der anfragenden Ermittlungsbehörde gelöst werden können. Es bestand kein vernünftiger Anlass, der Polizei unter Umgehung des Richtervorbehalts den "kurzen Dienstweg" zu eröffnen und das aus gutem Grund besonders geschützte Sozialgeheimnis in diesem Punkt zu durchbrechen, zumal es bei den Fällen, in denen die Vorschrift angewandt wird, nicht immer um einen polizeilich gesuchten Schwerverbrecher gehen wird, sondern es sich bei dem Grund für die Suche nach einer Person auch um eine Zeugenaussage oder um eine Geldforderung

in Höhe von 1000,-- DM handeln kann.

Die Folgen, die die Vorschrift beispielsweise im Bereich der Jugendämter oder Krankenkassen haben kann, dürften nicht bedacht worden sein. Es ist zu befürchten, dass die eigentliche Zielgruppe des Gesetzgebers künftig nicht mehr oder nicht mehr unter ihrem wirklichen Namen Sozialleistungen in Anspruch nehmen wird. Die Gefahr, dass auch sie sich ihre Hilfe zum Lebensunterhalt künftig ganz auf illegale Weise beschaffen wird, erhöht sich daher durch die Regelung. Dieser Erfolg dürfte kaum gewünscht sein, erst recht rechtfertigt er die drastischen Einschränkungen des Sozialgeheimnisses nicht.

Das Ministerium für Bildung, Jugend und Sport hat sehr schnell auf die Gesetzesänderung reagiert und den obigen Bedenken entsprechend für die Jugendämter im Land Brandenburg eine restriktive Empfehlung herausgegeben, die dem besonderen Vertrauensverhältnis zu deren Klientel grundsätzlich mehr Bedeutung beimisst als dem o. g. Anliegen des Gesetzgebers. Diese Initiative, von der wir allerdings nur zufällig erfuhren, ist zu begrüßen.

Auch beim Ministerium für Arbeit, Soziales, Gesundheit und Frauen, das uns in dieser Angelegenheit bisher sehr unterstützt hat, haben wir ein Rundschreiben an die Sozialbehörden mit Hinweisen zur Anwendung des § 68 SGB X n. F. angeregt. Wesentlich sind uns dabei folgende Punkte:

- Sozialbehörden sollten nicht als Ersatzmeldebehörden fungieren, sondern die anfragenden Behörden müssen sich die Daten primär auf andere Weise beschaffen (§ 68 Abs. 1 Satz 2 SGB X). Dem Sozialleistungsträger sind die vorangegangenen Maßnahmen zur Aufenthaltsermittlung und ihr Fehlschlagen darzustellen. Fehlt in dem Ersuchen eine entsprechende Aussage, ist es unter Hinweis darauf zurückzuweisen.

- Ein pauschaler Abgleich, Regelanfragen oder die Vorlage vollständiger Fahndungslisten würden das Erforderlichkeitsprinzip verletzen. Eine Sozialleistungsbehörde, die ein Ersuchen erhält, das sich auf einen Betroffenen bezieht, der nicht ihr Klient ist und bei dem auch nicht plausibel dargelegt wird, wieso der Gesuchte bei ihr vorsprechen sollte, sollte das Ersuchen ablehnen.

- Eine normenklare Speicherbefugnis für Anfragen, bei denen Fehlanzeige zu erstatten wäre, besteht nicht. Keinesfalls ist es daher zulässig, eine Eintragung über eine solche Anfrage in eine EDV-mäßig geführte Akte vorzunehmen oder amtsinterne Fahndungslisten, sei es für einen einzelnen Sachbearbeiter oder gar für alle Sachbearbeiter eines Amtes, zu erstellen. Bis zur Entscheidung darüber, ob und in welchem Umfang Amtshilfe nach § 68 SGB X geleistet werden darf, ist die Anfrage deshalb beispielsweise in der entsprechenden Sozialleistungsakte oder gesondert davon bei dem nach § 68 Abs. 2 SGB X für die Entscheidung zuständigen Bediensteten aufzubewahren.

- Die neu eingeführte 6-Monatsfrist begrenzt den Zeitraum für die Entscheidung des

Sozialleistungsträgers und deren Durchführung. Sie beginnt mit dem Eingang des Ersuchens bei dieser Stelle. Muss die ersuchende Stelle ihre Anfrage nachbessern, beispielsweise vorangegangene erfolglose Ermittlungsversuche darstellen, so geht diese zeitliche Verzögerung zu ihren Lasten; Fristbeginn bleibt der Eingang der ursprünglichen Anfrage. Eine erneute gleichlautende Anfrage darf die ersuchende Behörde in dem konkreten Fall ebenfalls nach Fristablauf nicht mehr an dieselbe Stelle richten, weil sonst die zeitliche Beschränkung umgangen würde.

- Die Berücksichtigung schutzwürdiger Interessen des Betroffenen führt dazu, dass anstelle eines Vorsprachetermins im Amt vorrangig die aktuelle Anschrift des Betroffenen mitzuteilen ist. Beim Erscheinen eines anderen Behördenvertreters zu einem Vorsprachetermin mit einer Sozialleistungsbehörde müssten nämlich unter Umständen vielfältige Maßnahmen ergriffen werden, um der Gefahr zu begegnen, dass dieser weitere Sozialdaten des Betroffenen wahrnimmt.

- Nur aufgrund richterlicher Anordnung dürfen bei Straftaten, die weder ein Verbrechen darstellen noch erhebliche Bedeutung haben, derzeitige und frühere Anschriften des Betroffenen mitgeteilt werden (§ 73 Abs. 2 SGB X). Eine Umgehung dieser Vorschrift unter Berufung auf § 68 SGB X n. F. ist nicht hinzunehmen. Vielmehr sollte ihre Berücksichtigung dazu führen, dass bei vergleichbaren Straftaten oder bei noch geringfügigeren Gründen grundsätzlich ein schutzwürdiges Interesse des Betroffenen anzunehmen ist, das der Übermittlung eines zukünftigen Aufenthaltes nach § 68 SGB X entgegensteht.

Das Sozialgeheimnis ist eine wichtige Voraussetzung dafür, dass Hilfsbedürftige die für ein menschenwürdiges Leben erforderlichen Leistungen des Staates in Anspruch nehmen können. Diese Vertrauensbasis darf nicht jedem öffentlichen Interesse z. B. an der Verfolgung von geringfügigen Straftaten geopfert werden.

7.2.2 Sozialämter

Arbeitskreis zur Verhinderung von Obdachlosigkeit

Ein Petent beschwerte sich darüber, dass ein aus Vertretern privater und öffentlicher Stellen bestehendes Gremium mieterbezogen über fristlose Kündigungen wegen Zahlungsverzuges informiert wurde und selbst weitere Datenverarbeitungen vornahm.

Die Errichtung dieses Arbeitskreises ging auf eine gemeinsame Empfehlung verschiedener Ministerien zurück, die eine Zusammenarbeit der betroffenen Ämter, sozialer Institutionen, der Wohnungswirtschaft, der Gerichte, ... anregt, um der Querschnittsaufgabe "Vermeiden von Obdachlosigkeit" möglichst effektiv und zeitnah gerecht zu werden. In einem konkreten Fall waren Ämter der Stadt (Sozialamt, Amt für Wohnungswesen, Ordnungsamt), des Landkreises (Kreisjugendamt, Allgemeiner Sozialer Dienst) sowie drei Vermietungsgesellschaften in dem Arbeitskreis vertreten.

Der Arbeitskreis erhielt Informationen über Namen und Anschrift des betroffenen Mieters sowie Grund und Termin der fristlosen Kündigung. Der Allgemeine Soziale Dienst des Landkreises bzw. das städtische Sozialamt übernahmen es, die Notlage und Lösungsmöglichkeiten abzuklären und den Arbeitskreis allgemein über das Ergebnis ihrer Bemühungen zu informieren.

Gesetzliche Übermittlungsbefugnisse kamen dabei nur zwischen wenigen beteiligten Stellen in Betracht, im Übrigen war für die Verfahrensweise eine informierte Einwilligungserklärung der Mieter notwendig.

Die Stadt entschied sich aufgrund unserer Empfehlung dafür, eine Fachstelle zur Vermeidung von Obdachlosigkeit beim Sozialamt zu errichten, weil die Sozialleistungsbehörden eine Großzahl der Fälle allein lösen können und Übermittlungen zwischen ihnen vom Gesetz eher zugelassen werden.

Für die Zusammenarbeit mit anderen Stellen wurde eine Einwilligungserklärung entwickelt. Diese sah zunächst vor, dass stets alle in dem Formular genannten Stellen über Name, Anschrift und Mietschulden des Betroffenen informiert werden. Es ist jedoch zu beachten, dass die Beteiligung einiger Stellen nur in Ausnahmefällen notwendig ist. Das Erforderlichkeitsprinzip wäre ebenso verletzt, wenn einer Stelle die Höhe der Mietschulden offenbart würde, die sich mit diesem Aspekt der Obdachlosigkeit gar nicht befasst. Bietet eine Stelle freiwillige Hilfen an, so kann eine Übermittlung an sie nur erforderlich sein, wenn der Betroffene sich überhaupt helfen lassen will. Die Fachstelle zur Vermeidung von Obdachlosigkeit hat sich daher für eine variable Gestaltung des Formulars - mit Feldern zum Ankreuzen - entschieden. Besondere Sorgfalt will sie auf eine umfassende Aufklärung der Betroffenen legen.

Die Stadt hat von sich aus zugesagt, uns über ihre Erfahrungen oder eventuellen weiteren Beratungsbedarf in einigen Monaten zu informieren.

Auch ein guter Zweck - die Vermeidung von Obdachlosigkeit - rechtfertigt nicht jedes Mittel. Außerdem fördern Datenübermittlungen über den Kopf des Betroffenen hinweg weder sein für die Annahme eines Hilfsangebotes notwendiges Vertrauen zu den beteiligten Stellen noch regen sie die unterstützenswerte Eigeninitiative an.

Datenschutz auch für Obdachlose

Petenten ohne einen festen Wohnsitz beschwerten sich bei uns über folgende Vorgehensweise eines Sozialamtes: Vor 9.00 Uhr mussten die obdachlosen Antragsteller ihre Personalausweise in den Behördenbriefkasten einwerfen, ab 11.00 Uhr erhielten sie mit der Auszahlung des Tagessatzes ihre Ausweise zurück. Dies bedeutete, dass sie zwei Stunden ohne Ausweispapiere waren und ihre Dokumente sich mit der allgemeinen Eingangspost mischten.

Diese Verfahrensweise beruhte auf einem Rundschreiben des Landkreises als örtlichem Träger der Sozialhilfe. Mit der Maßnahme sollte der verstärkten Gefahr von Sozialhilfemissbrauch durch Wohnsitzlose im S-Bahn-Bereich gegengesteuert werden.

Durch die Stellungnahme des betroffenen Sozialamtes erfuhren wir darüber hinaus, dass bei der ersten Antragstellung eine Kopie der Ausweispapiere des Antragstellers gefertigt wurde. Mit diesen Unterlagen wollte man nicht nur selbst den Betroffenen immer wieder identifizieren können, sondern beabsichtigte außerdem Meldeämter und Polizei bei der Wiederausstellung abhanden gekommener Ausweise zu unterstützen. Auch der Betroffene selbst sei im Falle des Verlustes seines Personalausweises dankbar, wenn ihm das Sozialamt dann aufgrund dieser Kopie bei der raschen Wiederbeschaffung des Papiers helfen könne.

Die Praxis, Ablichtungen der Personalausweise von Obdachlosen - oder Kopien von Abmeldebescheinigungen - zur Sozialakte zu nehmen, konnten wir noch bei etlichen anderen Sozialämtern, die gut mit S-Bahnen von Berlin aus zu erreichen waren, feststellen.

Bei diesen Maßnahmen ist die Verhältnismäßigkeit zweifelhaft, da mit den Kopien mehr Daten als erforderlich erhoben und gespeichert werden. Diese unzulässig erhobenen Angaben müssten unverzüglich gelöscht werden. Sie dürfen keinesfalls aus bloßer Hilfsbereitschaft weiteren Behörden zur Verfügung gestellt werden. Auch für zulässigerweise erhobene Daten existieren mit den §§ 68 und 73 SGB X ausreichende Übermittlungsvorschriften für die Offenbarung von Sozialdaten an die Polizei. Durch einen Vermerk in der Sozialhilfeakte über den vorgelegten Personalausweis kann dem Betroffenen auch im Fall des Verlustes seines Ausweises weitergeholfen werden.

Aufgrund unserer Intervention änderten die Sozialämter - soweit sie nicht bereits datenschutzgerecht verfuhren - ihre Vorgehensweise.

1. Weder Ausweispapiere noch Abmeldebescheinigungen der Betroffenen dürfen in Kopie zur Sozialakte genommen werden. Die Vorlage eines Ausweises für die Identitäts- oder Zuständigkeitsprüfung ist lediglich mit seiner näheren Bezeichnung, der ausstellenden Behörde und dem Ausstellungsdatum in der Sozialhilfeakte zu dokumentieren.

2. Unzulässigerweise gefertigte Kopien von Personalausweisen/Abmeldebescheinigungen sind unverzüglich zu vernichten.

3. Statt des Einsammelns von Personalausweisen bei wohnsitzlosen Soziahilfeempfängern können z. B. kurzbemessene feste Zeiten für die Antragstellung und Ausbezahlung festgelegt werden. Diese Zeiten sollten möglichst alle Sozialämter im Land miteinander absprechen.

Meldekarte für Arbeitssuchende

Eine Petentin machte uns auf eine vom Sozialamt ausgestellte Meldekarte aufmerksam, mit der sowohl eigene Arbeitssuchbemühungen als auch regelmäßige Vorsprachen beim Arbeitsamt nachgewiesen werden sollten. Die Petentin erklärte, mit einer Meldekarte des Sozialamtes auf Arbeitssuche gehen zu müssen, sei nicht

nur diskriminierend und stehe der informationellen Selbstbestimmung entgegen, sondern bringe bei der Arbeitssuche auch die gängigen Vorurteile gegen Sozialhilfeempfänger zu Tage. Sie sei daher nicht hilfreich, um einen Arbeitsplatz zu erlangen.

Wir stellten auch bei anderen Sozialämtern fest, dass nur in seltenen Fällen individuelle Bescheinigungen der Vorsprache bei einem Arbeitgeber, Bewerbungsschreiben u. ä. als Arbeitssuchnachweise akzeptiert wurden. Viele Sozialämter setzten die "Meldekarte" ein.

Unser Hinweis darauf, dass mit der Meldekarte unnötigerweise nicht nur zwangsläufig jedem potentiellen Arbeitgeber offenbart werde, dass der Arbeitssuchende Sozialhilfeempfänger sei, sondern dass der Arbeitgeber auch noch einen Überblick darüber erhalte, bei welchen anderen Stellen der Betreffende sich zuvor vorgestellt hatte, überzeugte einige Sozialämter sehr schnell davon, dass die datenschutzrechtlichen Bedenken sich mit den praktischen Hinweisen der Petentin deckten.

Es entspricht dem datenschutzrechtlichen Gebot der Erforderlichkeit, wenn den Betroffenen neutrale Vordrucke für die Bescheinigung ihrer Bewerbung bei einem einzelnen Arbeitgeber zur Verfügung gestellt werden. Zudem hat die Arbeitssuche von Sozialhilfeempfängern ohne Meldekarte mehr Aussicht auf Erfolg.

Missbrauch - anders als erwartet

Anfang Oktober 1998 hatte ein Landkreis die Telefonnummer eines Bürgertelefons bekannt gegeben, über die einem neu eingerichteten "Prüfdienst zur Feststellung von Sozialhilfemissbrauch" vermutete Fälle von Leistungserschleichung mitgeteilt werden konnten. Weiteren Presseberichten war zu entnehmen, dass der Landkreis dabei vor allem auf anonyme Tips hoffte. Es war zunächst von einer über 90 %igen Erfolgsquote der durch die Hinweise aufgedeckten Missbrauchsfälle die Rede. Letztlich erhielt das Sozialamt im Verlauf eines Monats 15 Hinweise auf Leistungsmissbrauch, von denen 14 anonym waren. Als begründet erwies sich lediglich der namentliche Telefonanruf. Der Landkreis hat unterdessen bekannt gegeben, dass anonymen Mitteilungen nicht mehr nachgegangen wird.

Wir halten diese Form der Bekämpfung von Sozialhilfemissbrauch nicht für datenschutzgerecht. Immer dann, wenn über die bloße Entgegennahme eines Hinweises hinaus einem Anrufer Rückfragen durch die Mitarbeiter des Sozialamtes gestellt werden, liegt eine Datenerhebung vor. Diese ist ebenso wie die folgende Datenverarbeitung bzw. -nutzung im Sozialamt nur dann zulässig, wenn sie für die Erfüllung der gesetzlichen Aufgaben des Sozialamtes erforderlich ist. Die Mehrzahl der überprüften Hinweise waren jedoch nicht leistungsrelevant. Dies lässt den Schluss zu, dass die Aufforderung zu anonymen Hinweisen ein ungeeignetes Mittel ist, um Sozialhilfemissbrauch aufzudecken.

Die Entgegennahme anonymer Hinweise begegnet aber noch weiteren datenschutz-

rechtlichen Bedenken: Falls nämlich durch Anrufe Dritter Ermittlungen gegen einen Sozialhilfeempfänger ausgelöst werden und diese Hinweise sich als unbegründet erweisen, könnte der Anrufer eine Straftat (Verleumdung, üble Nachrede o. ä.) begangen haben. Für den Betroffenen, der eine solche Tat geahndet wissen möchte, wäre es wesentlich, beim Sozialamt Auskunft über den Namen des Denunzianten zu erhalten. Erfolgte ein Hinweis allerdings berechtigt, überwiegen grundsätzlich die schutzwürdigen Interessen des Hinweisgebers, seine Identität, auch wenn sie dem Sozialamt bekannt ist, nicht dem Betroffenen preiszugeben.

Aufrufe zum anonymen Anschwärzen sind kein geeignetes Mittel, den Sozialhilfemissbrauch effektiv zu bekämpfen. Sie fördern auch nicht die Zivilcourage der Bevölkerung, sondern bringen die Verwaltung in Gefahr, Personen, die andere verleumden oder ihnen übel nachreden, zu unterstützen.

Zugriffsbefugnisse auf Sozialdaten

Ein Informations- und Beratungsbesuch in einem Sozialamt brachte folgende aus datenschutzrechtlicher Sicht verbesserungswürdige Umstände an den Tag:

Sowohl für die Systemanmeldung als auch für die Anmeldung im Programm war eine Passworteingabe zwingend vorgesehen, bei der jedoch nicht alle Möglichkeiten des Systems voll genutzt wurden. So wurde bei der Systemanmeldung beispielsweise eine Maximallänge festgelegt, jedoch keine Mindestlänge vorgeschrieben, so dass ein Passwort auch aus einem einzigen Zeichen hätte bestehen können.

Durch die permanente Aktivierung des Passwortteils für den Vertretungsfall hatten sowohl der erste als auch der zweite Vertreter eines Sachbearbeiters im Sozialamt unabhängig von der Abwesenheit des Vertretenen eine Zugriffsmöglichkeit auf die in dessen Zuständigkeitsbereich angefallenen Sozialdaten. Zu den im Sozialamt vorhandenen Papierakten war allen Mitarbeitern freier Zugang eingeräumt. Die Wahrung des Sozialgeheimnisses umfasst nach § 35 Abs. 1 Satz 2 SGB I aber die Verpflichtung, auch innerhalb des Leistungsträgers sicherzustellen, dass die Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden. Eine Befugnis besteht nur für den jeweils Zuständigen.

Zugriff auf die Daten des Sozialamtes hatte außer den dort Beschäftigten und - in eingeschränktem Umfang - zwei Mitarbeitern der Stadtkasse auch der Administrator. Dieser war jedoch zugleich zum behördlichen Datenschutzbeauftragten bestellt. Damit waren in seiner derjenige, dem die Kontrolle des Datenschutzes in der Stadtverwaltung obliegt mit der Person vereint, die er primär zu kontrollieren hätte. Das novellierte Brandenburgische Datenschutzgesetz (BbgDSG) schreibt in § 7 a Abs. 1 jedoch vor, dass zum behördlichen Datenschutzbeauftragten nur bestellt werden darf, wer dadurch keinem Interessenkonflikt mit sonstigen dienstlichen Aufgaben ausgesetzt wird. Wir haben die Stadtverwaltung daher aufgefordert, diese beiden Aufgaben auf zwei verschiedene Mitarbeiter zu verteilen.

Mitarbeiter privater Firmen, die mit personenbezogenen Daten der Stadtverwaltung in

Berührung kommen könnten, wurden bisher nach § 6 BbgDSG auf das Datengeheimnis verpflichtet. Die Vorschrift beschränkt sich jedoch auf die Mitarbeiter öffentlicher Stellen. Beauftragte Firmen haben ihre Mitarbeiter auf das Datengeheimnis nach § 5 Bundesdatenschutzgesetz zu verpflichten. Wir haben der Stadtverwaltung dazu entsprechende Musterformulare überlassen.

Im Einzelfall wurden der Wartungsfirma personenbezogene Daten auf einem Streamerband mit einigen allgemeinen datenschutzrechtlichen Festlegungen übersandt. Der novellierte § 11 a BbgDSG gibt für solche Fälle Mindestanforderungen an den Inhalt des Wartungsvertrags sowie einen Katalog für die grundsätzlich erforderlichen technisch-organisatorischen Maßnahmen vor. Der Landesgesetzgeber hat sich dafür entschieden, Wartung und Fernwartung getrennt von der Datenverarbeitung im Auftrag (§ 11 BbgDSG) zu regeln, weil bei der Wartung eine Datenverarbeitung allenfalls eine notwendige Folge, nicht jedoch Hauptpflicht des Vertrages ist. Dementsprechend halten wir auch im Bereich des Sozialgesetzbuches § 80 SGB X auf die Wartung nicht für anwendbar. Ist eine Fremdwartung notwendig, um die Aufgaben im Sozialamt weiter erfüllen zu können, kann eine Übermittlung der dafür erforderlichen Sozialdaten nach § 69 Abs. 1 Nr. 1 SGB X zulässig sein. Wegen des Erforderlichkeitsprinzips ist aber primär eine Lösung zu suchen, bei der eine Offenbarung von Sozialdaten nicht notwendig ist. Wenn eine verschlüsselte Weitergabe nicht möglich ist, dürfen nur die für die Wartung erforderlichen Sozialdaten übermittelt werden.

Nach § 78 Abs. 1 Satz 1 SGB X darf die Wartungsfirma die Daten nur zu dem Zweck verarbeiten oder nutzen, zu dem sie rechtmäßig übermittelt worden sind. Übermitteln bedeutet jedoch nicht, dass die Daten das Sozialamt verlassen müssten. Im Gegenteil ist aus Gründen des Datenschutzes und der Datensicherheit zu fordern, dass die Wartung primär dort unter Aufsicht städtischer Mitarbeiter stattfindet. Die Firma ist darauf hinzuweisen, dass sie nach § 78 Abs. 1 Satz 2 SGB X die Daten in demselben Umfang geheimzuhalten hat wie das Sozialamt. Die Datenschutzvorkehrungen richten sich dementsprechend insoweit auch bei der Wartungsfirma nach den Vorschriften des Sozialgesetzbuches. Technische und organisatorische Maßnahmen zum Schutz der Sozialdaten sind deshalb nach § 78 a SGB X nebst Anlage zu treffen. Das Sozialamt hat sich über die beim Empfänger getroffenen Maßnahmen vor einer Beauftragung zu informieren und darf einen Auftrag nur erteilen, wenn diese Maßnahmen getroffen worden sind.

Die Stadtverwaltung hat zu unseren Anregungen und Mängelfeststellungen noch nicht Stellung genommen.

7.2.3 Sozialversicherungsträger

Weitergabe von Rezepten an Drittfirmen

Ein Sanitätshaus beschwerte sich bei uns über folgenden Sachverhalt:

Bekommt ein Patient vom Arzt ein Hilfsmittel (Prothese, orthopädische Schuhe, Rollstuhl, ...) verschrieben, geht er zum Orthopädie-Haus seines Vertrauens und

hinterlässt dort auch sein Rezept mit Diagnose. Diese Firma schickt dann ihren Kostenvoranschlag mit dem Rezept an die zuständige Krankenkasse, die in vielen Fällen dazu das Angebot eines weiteren Lieferanten einholt. Hierfür werden auch die Rezeptdaten übermittelt. In einem Fall informierte die Krankenkasse dabei als Drittfirma das Sanitätshaus, bei dem der Patient bisher Kunde war und von dem er gerade nicht mehr bedient werden wollte.

Die Krankenkasse hat dazu ausgeführt, dass der Anbieter als Geschäftsmann seine Leistung profitabel verkaufen wolle, während die Krankenkasse dem Wirtschaftlichkeitsgebot verpflichtet sei. Da weder der Sachbearbeiter der Krankenkasse noch der für die Beurteilung medizinischer Sachverhalte zuständige Medizinische Dienst der Krankenversicherung in der Lage sei, die handwerklichen Leistungen zu beurteilen, sei es unverzichtbar, Gegenkostenvoranschläge einzuholen. Diese Praxis wollte die Krankenkasse auf § 127 Abs. 3 SGB V stützen. Danach können Krankenkassen bei Leistungserbringern Preisvergleiche über Hilfsmittel durchführen, um die Versicherten sowie die Ärzte über preisgünstige Versorgungsmöglichkeit zu informieren. Im übrigen vertrat die Krankenkasse einerseits die Auffassung, dass die Übermittlung der anonymisierten ärztlichen Verordnung inklusive der angegebenen Diagnose an einen Zweitanbieter notwendig sei, damit dieser eine dem jeweiligen Versorgungsfall entsprechende Leistung vorschlagen könne. Zum anderen erklärte sie, dass der Leistungserbringer Informationen zu den Besonderheiten des Einzelfalles benötige, die er nur beim Versicherten selbst einholen könne, ging also von einer Übermittlung mit Personenbezug aus.

Wir baten um Klärung dieser Widersprüche. § 127 Abs. 3 SGB V scheidet als Übermittlungsgrundlage aus. Die Vorschrift bezieht sich nicht auf einen konkreten Fall eines Preisvergleiches, sondern zielt auf allgemeine Informationen ab. Auch das Ministerium für Arbeit, Soziales, Gesundheit und Frauen vertrat die Auffassung, dass sich die Zulässigkeit der Übermittlung von Sozialdaten ausschließlich nach den Vorschriften der §§ 67 ff. SGB X richtet. Grundsätzlich sei beim Einholen von alternativen Kostenvoranschlägen zu gewährleisten, dass eine anonymisierte ärztliche Verordnung einschließlich der angegebenen Diagnose der Anforderung des Zweitangebotes beigefügt werde, so dass ein Personenbezug nicht hergestellt werden könne. In den Fällen, in denen ein Hilfsmittel körpergerecht angefertigt werden müsse, sei eine Weitergabe der erforderlichen personenbezogenen Daten an die anderen Leistungserbringer zulässig. Die Gründe für diese Übermittlung sowie die übermittelten Daten seien stets im Vorgang zu dokumentieren.

Wir haben uns dieser Auffassung angeschlossen. Dabei gehen wir davon aus, dass der Begriff "körpergerecht" eng auszulegen ist. Kann ein Hilfsmittel allein aufgrund von Maßangaben erstellt werden, so sind an Stelle der Übermittlung von Name und Adresse des Betroffenen nur die Maße an die Drittfirma zu offenbaren. Unter körpergerechten Anfertigungen, bei denen die Weitergabe des Namens und der Adresse des Betroffenen notwendig werden kann, sind Spezialanfertigungen zu verstehen, die sich mit Maßangaben nicht bzw. nicht hinreichend beschreiben lassen. Dem Betroffenen sollte aber in solchen Fällen die Möglichkeit eröffnet werden, sich selbst um verschiedene Kostenvoranschläge zu bemühen, denn nur so lässt es sich vermeiden, dass er zuletzt gerade mit dem Anbieter konfrontiert wird, den er aufgrund früherer

Erfahrungen meiden möchte.

Bei der Prüfung, ob eine Übermittlung erforderlich ist, ist zunächst zu klären, ob die Bekanntgabe anonymisierter Angaben ausreichend ist. Kommt diese Lösung nicht in Betracht, dürfen nur die für den jeweiligen Zweck unverzichtbaren Daten übermittelt werden.

Ein Datenschutzbeauftragter zuviel

Ein Sozialversicherungsträger hatte gleich zwei behördliche Datenschutzbeauftragte bestellt, die ihre Zuständigkeit von Fall zu Fall selbst bestimmten. Unser Hinweis auf die damit verbundenen Datenschutzprobleme hat dazu geführt, dass ein hauptverantwortlicher Datenschutzbeauftragter benannt wurde.

Zum einen umfasst die Wahrung des Sozialgeheimnisses nach § 35 Abs. 1 SGB I auch die Verpflichtung, innerhalb des Leistungsträgers sicherzustellen, dass Sozialdaten nur Befugten zugänglich sind und nur an diese weitergegeben werden. Dabei sollte es so wenig Befugte wie möglich geben, um ein hohes Maß an Datenschutz zu gewährleisten. Die Regelung dieser Befugnisse - und damit der zugrunde liegenden Zuständigkeit - kann naturgemäß nicht Sache der Mitarbeiter selbst sein. Außerdem ist sie grundsätzlich allgemein und nicht erst angesichts eines konkreten Falles zu treffen.

Hinzu kommt, dass nach § 81 Abs. 4 Satz 1 SGB X i. V. m. § 36 Abs. 1 BDSG eine datenverarbeitende Stelle nur einen behördlichen Datenschutzbeauftragten bestellen darf. Dafür spricht auch § 81 Abs. 4 Satz 2 SGB X, der für räumlich getrennte Organisationseinheiten vorsieht, dass auch dort der Beauftragte für den Datenschutz bei der Erfüllung seiner Aufgaben unterstützt wird. Das Gesetz geht also nicht davon aus, dass die Aufgabe des behördlichen Datenschutzbeauftragten angesichts räumlich getrennter Organisationseinheiten auf mehrere Personen verteilt wird. Dies trägt u. a. dazu bei, dass in datenschutzrechtlichen Fragen einheitlich entschieden wird.

Außerdem könnte die Bestellung mehrerer behördlicher Datenschutzbeauftragter auch die gebotene unabhängige Wahrnehmung dieser Aufgabe gefährden. Insbesondere dann, wenn Zuständigkeitsbereiche nicht eindeutig in generellen Organisationsentscheidungen festgelegt sind, könnte von der Stellenleitung jeweils der behördliche Datenschutzbeauftragte zuständig gemacht werden, der eine der Leitung genehmere Ansicht vertritt. Die Weisungsfreiheit des behördlichen Datenschutzbeauftragten, das Verbot seiner Benachteiligung in § 36 Abs. 3 Satz 3 BDSG sowie der Schutz gegen den Widerruf seiner Bestellung aus anderen als in § 36 Abs. 3 Satz 4 BDSG genannten Gründen könnten so indirekt ausgehebelt werden. Dies muss vermieden werden.

Mehr Datenschutzbeauftragte in einer Stelle bedeuten zugleich mehr Zugriffsbefugte als notwendig. Diese könnten gegeneinander ausgespielt werden, so dass ihre gesetzlich vorgesehenen Rechte beeinträchtigt würden. Außerdem besteht die Gefahr, dass nicht immer einheitliche Entscheidungen durch die verschiedenen Beauftragten getroffen würden. Deshalb darf eine datenverarbeitende Stelle nicht mehr als einen hauptverantwortlichen Datenschutzbeauftragten bestellen. Vertretungsregelungen sind damit nicht ausgeschlossen.

Die Krankenkasse war immer dabei ...

In jedem Bundesland bilden die Landesverbände der Orts-, Betriebs- und Innungskrankenkassen, die landwirtschaftlichen Krankenkassen und die Verbände der Ersatzkassen die Arbeitsgemeinschaft "Medizinischer Dienst der Krankenversicherung (MDK)". In manchen Bundesländern ist diese Arbeitsgemeinschaft eine rechtsfähige Körperschaft des öffentlichen Rechts, in Brandenburg besteht sie in Form eines eingetragenen Vereins. Der Medizinische Dienst der Krankenversicherung hat die Aufgabe, ärztliche Gutachten für die gesetzlichen Krankenkassen zu erstellen. Die notwendigen Grundlagen für das Gutachten erhält der Medizinische Dienst sowohl von den Krankenkassen als auch unmittelbar von den beteiligten Leistungserbringern wie z. B. Ärzte, Krankenhäuser, Hebammen, Krankengymnasten. Durch die Schaffung des Medizinischen Dienstes der Krankenversicherung sollte gewährleistet werden, dass die Krankenkassen gerade nicht im Einzelnen über sämtliche medizinischen Daten ihrer Versicherten informiert werden. Mitzuteilen sind ihnen beispielsweise nur das Ergebnis der Begutachtung und erforderliche Angaben über den Befund.

> *Die Ärzte des MDK, denen ein Gutachtenauftrag einer Krankenkasse zur Überprüfung der Notwendigkeit und Dauer der stationären Behandlung eines Krankenversicherten übertragen wurde, dürfen erforderlichenfalls zwischen 8.00 Uhr und 18.00 Uhr die Räume des Krankenhauses betreten, um dort Krankenunterlagen einzusehen und den Versicherten untersuchen zu können. Eine vergleichbare Vorschrift für Sachbearbeiter der Krankenkassen gibt es nicht. Trotzdem wurde uns berichtet, dass in verschiedenen Fällen die Ärzte des MDK in Begleitung eines Krankenkassenmitarbeiters erschienen.*

Manchmal versuchte die Krankenkasse die Anwesenheit ihrer Mitarbeiter durch eine Einwilligung des Patienten abzusichern. Aber auch hier gilt, dass der vom Gesetzgeber in § 276 SGB V vorgeschriebene Weg der Datenübermittlung - direkt vom Krankenhausarzt zum MDK-Arzt - nicht zur Disposition der Beteiligten steht und mit Hilfe einer Einwilligungserklärung des Versicherten also nicht abgeändert werden kann[55].

Selbst die bloße Begleitung des MDK durch einen Krankenkassenmitarbeiter, ohne dass dieser Einsicht in Krankenunterlagen nimmt, erscheint uns nicht unbedenklich. Wenn ein Krankenkassenmitarbeiter auf Wunsch eines Versicherten diesen vor Ort im Krankenhaus besucht, um persönliche Anliegen zu besprechen, so verfolgt er dabei ganz andere Ziele und benötigt andere Informationen vom Patienten als der mit einer Begutachtung beauftragte MDK-Arzt. Dementsprechend dürfte auch der Betroffene

daran interessiert sein, die Gespräche getrennt zu führen und nicht dem faktischen Zwang ausgesetzt zu werden, dem einen oder anderen situationsbedingt etwas zu offenbaren, was er in diesem Verhältnis an sich nicht ansprechen wollte. Die Krankenkasse, mit der wir diese Verfahrensweise diskutierten, hat sich deshalb schließlich dafür entschieden, künftig den MDK allein prüfen zu lassen.

Die Erteilung eines Gutachtenauftrages an den MDK berechtigt die Krankenkasse nicht, gemeinsam mit den Ärzten des MDK das Krankenhaus zu betreten, Krankenunterlagen einzusehen und an Untersuchungen des Versicherten teilzunehmen. Diese Rechte sind dem MDK-Gutachter vorbehalten und können auch nicht durch Einwilligung des Betroffenen einem Krankenkassen-Mitarbeiter zugestanden werden.

Besucht ein Krankenkassen-Mitarbeiter einen Versicherten auf dessen Wunsch hin im Krankenhaus, hat dies, auch um den Betroffenen vor einem faktischen Zwang zu Datenoffenbarungen an den einen oder anderen der Besucher zu bewahren, getrennt vom MDK-Arzt zu erfolgen.

Neugierige Unfallversicherungen

Die Unfallversicherungsträger können von den Krankenkassen Auskünfte über Vorerkrankungen eines Versicherten verlangen, soweit dies für die Feststellung des Versicherungsfalles erforderlich ist (§ 188 SGB VII). Erfragt werden dürfen dabei grundsätzlich nur Vorerkrankungen, die den Versicherungsfall möglicherweise verursacht haben.

Außerdem ist bei der Anfrage einer gesetzlichen Unfallversicherung der sog. Ersterhebungsgrundsatz des § 67 a Abs. 2 Satz 1 SGB X zu beachten, d. h. Sozialdaten sind möglichst beim Betroffenen selbst zu erheben. Eine Erhebung bei Dritten ist nur in Ausnahmefällen zulässig.

Der Bundesbeauftragte für den Datenschutz hatte festgestellt, dass diese gesetzlichen Vorgaben häufig nicht beachtet werden. Wir sind dem in unserem Zuständigkeitsbereich nachgegangen.

Erfreulicherweise konnten wir feststellen, dass das Anfragemuster der Unfallkasse Brandenburg den gesetzlichen Voraussetzungen gerecht wird. Dass eine solche datenschutzgerechte Verfahrensweise durchaus nicht selbstverständlich ist, wurde uns anhand verschiedener anonymisierter Mustervordrucke anderer Unfallversicherungsträger deutlich, die uns von Krankenkassen vorgelegt wurden.

Wir haben die Krankenversicherungen darum gebeten, vom anfragenden Unfallversicherungsträger eine Begründung für die Erforderlichkeit des kompletten Vorerkrankungsverzeichnisses sowie eine Versicherung, dass der Ersterhebungsgrund-

satz beachtet wurde, zu fordern.

7.3 Gesundheit

7.3.1 Krankenhäuser

Novellierung der Krankenhausdatenschutzverordnung notwendig

Im 6. Tätigkeitsbericht[56] hatten wir darauf hingewiesen, dass die inzwischen drei Jahre alte Krankenhausdatenschutzverordnung (KHDsV) verbesserungsbedürftig ist. Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hält die bisher in zweifelhaften Fällen von uns praktizierte gemeinsame Interpretation des Willens des Verordnungsgebers jedoch derzeit noch für ausreichend. Solche korrigierenden Auslegungen sollten im Hinblick auf die Normenklarheit nur für einen Übergangszeitraum akzeptiert werden.

Darüber hinaus zwingt Art. 8 der EG-Datenschutzrichtlinie ohnehin zu einer kritischen Überprüfung aller Datenverarbeitungsregelungen im Gesundheitsbereich. Aber auch die Novellierung des Brandenburgischen Datenschutzgesetzes zieht einen Änderungsbedarf in diesem Bereich nach sich: Im Land ist nunmehr die Bestellung behördlicher Datenschutzbeauftragter verpflichtend vorgesehen. Es erscheint deshalb auch im Rahmen der Krankenhausdatenschutzverordnung notwendig, möglichst bald festzulegen, wie diese Funktion in den öffentlichen Krankenhäusern ausgestaltet werden soll. Die zusätzliche Berücksichtigung der ärztlichen Schweigepflicht im Gesundheitswesen erfordert nämlich spezielle Regelungen für die dort tätigen behördlichen Datenschutzbeauftragten.

In zahlreichen weiteren Punkten sehen wir Aktualisierungsbedarf für die Krankenhausdatenschutzverordnung und sind in dieser Frage zu einer engen Zusammenarbeit mit dem Ministerium für Arbeit, Soziales, Gesundheit und Frauen bereit.

Eine Novellierung der Krankenhausdatenschutzverordnung, aber auch Änderungen bzw. Ergänzungen der Regelungen im übrigen Gesundheitsbereich sind notwendig. Der Umstand, dass in den speziellen Gesetzen für das Gesundheitswesen häufig dieselben Punkte zur Datenverarbeitung und zum Datenschutz neu geregelt werden müssen, spricht für die Überlegung, diese Regelungen einheitlich in einem Gesetz für den Datenschutz im Gesundheitswesen zu treffen. Dies hätte auch den Vorteil, dass notwendige spätere Änderungen nur in diesem einheitlichen Regelungswerk vorgenommen werden müssten.

Hospitanten und Praktikanten

Durch eine Petition wurden wir über folgenden Vorfall in einem Krankenhaus informiert:

Ein Arbeitnehmer begab sich wegen Alkoholproblemen, die seinem Arbeitgeber bisher unbekannt geblieben waren, auf eigenen Wunsch in stationäre Therapie. Während des Aufenthaltes in der Klinik wurde er unvorbereitet und ohne Ausweichmöglichkeit, mit seinem Vorgesetzten und einem Kollegen konfrontiert. Diese nahmen als Hospitanten an einer Fortbildung im Bereich der Früherkennung und innerbehördlichen Behandlung von Suchtkrankheiten teil.

Eine Umfrage bei ausgewählten Krankenhäusern im Land ergab, dass einzelne Kliniken überhaupt keine Hospitationen anbieten, während andere regen Gebrauch davon machen. Häufig wurden auch Hospitationen und Praktika gleichgestellt.

Praktika werden überwiegend zur Vorbereitung auf einen Beruf erfolgen. Ist der Ausbilder ein Schweigepflichtiger i. S. d. § 203 Abs. 1 StGB, so unterliegt regelmäßig auch der Praktikant nach § 203 Abs. 3 StGB der Schweigepflicht.

Ein Hospitant ist jedoch nicht zwingend zugleich ein Schweigepflichtiger i. S. d. § 203 Abs. 1 StGB, berufsmäßig tätiger Gehilfe i. S. d. § 203 Abs. 3 StGB oder bei einem Schweigepflichtigen zur Vorbereitung auf seinen Beruf tätig. Der strafrechtliche Schutz der Schweigepflicht gem. § 203 StGB greift dann nicht. Eine Offenbarung von Patientendaten an solche Hospitanten hat damit für die Patienten einen erheblichen Verlust an Vertraulichkeit für ihre sensiblen Daten zur Folge. Darüber hinaus dient die Hospitation in der Regel nicht der Behandlung, sondern vorwiegend Informationsinteressen des Hospitanten selbst.

Hospitationen solcher Personen, die keiner Schweigepflicht i. S. d. § 203 StGB unterliegen, sollten ebenso unterbleiben wie Hospitationen bei Maßnahmen, bei denen die Gruppenprozesse zu einem unkalkulierbaren Gesprächsverlauf führen können. Will ein Schweigepflichtiger im eigenen Interesse Kontakt mit dem Patienten aufnehmen, ist dafür eine Einwilligungserklärung des Betroffenen notwendig, die nur dann als wirksam gelten kann, wenn er zuvor über den Zweck der Hospitation und die Identität des Hospitanten informiert wurde.

7.3.2 Gesundheitsämter

Altakten in privater Hand

Im Frühjahr 1998 informierte uns ein Landkreis darüber, dass er bereits Mitte 1996 eine GmbH unter ärztlicher Leitung mit der Verwaltung der Patientenakten einer ehemaligen Einrichtung beauftragt hatte. Die GmbH war von ehemaligen Ärzten der Poliklinik gegründet worden. Die Zustimmung des Ministeriums des Innern zu einer Datenverarbeitung im Auftrag war schon damals erfolgt. Bei einer Prüfung der

beauftragten Stelle Ende 1997 hatte das Ministerium keine Verstöße gegen datenschutzrechtliche Vorschriften festgestellt. Es hatte jedoch dem Landkreis empfohlen, die Meldung an unsere Behörde nachzuholen, da uns vertraglich ebenfalls eine Kontrollbefugnis bei der GmbH eingeräumt worden war.

Obwohl nach dem sog. Patientenerlass nur Kreisarchive Altakten im Auftrag des Gesundheitsamtes aufbewahren dürfen, waren wir nach genauer Prüfung der Angelegenheit wegen der besonders gelagerten Umstände nach Rücksprache mit dem Ministerium des Innern bereit, in diesem Fall eine Datenverarbeitung im Auftrag durch eine private Stelle zu akzeptieren. Voraussetzung für diese Ausnahme war jedoch, dass der bereits geschlossene Vertrag den Voraussetzungen einer Datenverarbeitung im Auftrag angepasst wird und zusätzliche technisch-organisatorische Vorgaben beinhaltet.

Insbesondere muss sichergestellt sein, dass die GmbH auch in Zukunft unter ärztlicher Leitung steht und das Personal, das mit den Altakten in Kontakt kommt, sowohl der ärztlichen Schweigepflicht unterliegt als auch nach § 5 BDSG auf das Datengeheimnis verpflichtet wird.

Damit auch aus den einzelnen Rechten der Vertragspartner hervorgeht, dass der Landkreis Herr der Daten ist und bleibt, muss sich dieser ein Kontrollrecht im Rahmen des Auftrages einräumen lassen. Er muss weiter möglichst exakt regeln, an wen und unter welchen Voraussetzungen Originale oder Kopien von Krankenakten herausgegeben werden dürfen. Dafür soll der Landkreis eine Mustereinwilligungserklärung vorgeben, die von der GmbH beispielsweise bei der Aktenherausgabe an andere Ärzte zu verwenden ist. Die Fälle, die eine Abwägung des Rechtes auf informationelle Selbstbestimmung und der ärztlichen Schweigepflicht mit anderen Rechten erfordern, müssen der Entscheidungsbefugnis des Gesundheitsamtes vorbehalten bleiben.

Der Landkreis hat uns mitgeteilt, dass er bestrebt sei, die vorgeschlagenen Nachbesserungen in den Vertrag einzuarbeiten. Nun werde dieser Entwurf hinsichtlich Praktikabilität und Finanzierbarkeit gemeinsam mit dem Vertragspartner geprüft.

Berufsrechtliche Warnmeldungen

Werden Erlaubnisse zur Ausübung nichtärztlicher Heilberufe (z. B. Heilpraktiker) aufgehoben, widerrufen oder zum Ruhen gebracht, melden die zuständigen Stellen im Bundesgebiet dies an ihre jeweiligen obersten Landesgesundheitsbehörden, die sich wiederum gegenseitig unterrichten. Dies soll dazu dienen, im Interesse des Patientenschutzes eine Berufsausübung in einem anderen Bundesland zu verhindern oder eine Neubeantragung von Approbation und Berufserlaubnis angemessen zu beurteilen. Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hat uns mitgeteilt, dass es dieses Verfahren zum Schutz gesundheitspolitischer Interessen der Allgemeinheit für notwendig hält.

Für diese Warnmeldungen gibt es keine Rechtsgrundlage. Es ist schon fraglich, ob sie der Erfüllung einer Aufgabe der obersten Landesgesundheitsbehörden dienen. Jeden-

falls werden bei der Verfahrensweise Daten auf Vorrat erhoben und übermittelt. Dies verletzt das Erforderlichkeitsprinzip. Notwendig könnte eine Datenverarbeitung erst dann werden, wenn ein Betroffener trotz eines entgegenstehenden Verwaltungsaktes erneut seine Zulassung beantragt und die Vorgeschichte verschweigt oder wenn er seinen Beruf einfach wieder aufgenommen hat.

Da allerdings ein gewisses praktisches Bedürfnis an solchen Meldungen bestehen kann, haben wir signalisiert, die Warnmeldungen dann zu tolerieren, wenn folgende Voraussetzungen erfüllt sind:

- die ausgetauschten Daten werden auf ein Minimum reduziert,

- die tatsächliche Entscheidungserheblichkeit der Warnmeldungen wird uns dargelegt, um die Verhältnismäßigkeit beurteilen zu können,

- und das Ministerium setzt sich für eine ausdrückliche gesetzliche Übermittlungsbefugnis ein.

Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hat inzwischen darauf hingewirkt, dass sich der bundesweite Berufeausschuss mit einer datenschutzgerechteren Ausgestaltung der bisherigen Verfahrensweise befassen wird.

Einzelne schwerwiegende Missbrauchsfälle verleiten häufig dazu, auch über die Vielzahl der Personen, die sich korrekt verhalten, vorsorglich umfangreiche Daten auszutauschen. Eine solche Datenübermittlung auf Vorrat ist unzulässig und verletzt die Rechte der zu Unrecht Mitbetroffenen. Dies wird im Eifer der Missbrauchsbekämpfung häufig übersehen.

Projekt "easy-card Gesundheit"

Im Herbst 1995 informierte das Ministerium für Arbeit, Soziales, Gesundheit und Frauen uns darüber, dass in einem Großteil der Gesundheitsämter das Programm "easy-card Gesundheit" eingeführt werden solle. Einige Module befanden sich damals noch in der Entwicklung, aber auch auf die endgültige Fassung bereits vorhandener Module konnten wir noch Einfluss nehmen. Inzwischen läuft die Software teilweise im Echtbetrieb, teilweise noch im Probelauf.

Auf unsere Empfehlung hin werden

- im Modul "Zahnärztliche Reihenuntersuchung" das Merkmal "Behindert" nicht mehr erhoben und

- im Tuberkulose-Zählblatt die Angaben von Risikofaktoren, die "Durchführung einer BCG-Impfung" und "chemotherapeutische Behandlung" nicht mehr an das Landesamt für Datenverarbeitung und Statistik übermittelt.

Da diese Übermittlungen auf veraltete Meldebögen zurückgehen, hat das Ministerium hier eine Überarbeitung zugesagt. Das einzige Datum, das entgegen unseren Hinweisen weiterhin erhoben und übermittelt werden soll, ist die regelmäßige Angabe des Herkunftslandes bei Ausländern. Dies halten wir nicht für erforderlich.

Das Modul "Personal im öffentlichen Gesundheitsdienst" enthielt vor unserer Intervention auch das Geburtsdatum und die Personalnummer jedes einzelnen Bediensteten. Noch ungeklärt ist derzeit, ob das Merkmal "Teilzeitbeschäftigung", das auf unsere Veranlassung hin entfernt wurde, gegen unseren Rat doch wieder aufgenommen werden wird.

Im Ärzteverzeichnis wurden die Gründe für das Berufsende und das für Erläuterungen dazu vorgesehene Bemerkungsfeld gestrichen. Das Ministerium für Arbeit, Soziales, Gesundheit und Frauen hatte sich dabei unserer Argumentation angeschlossen, dass weder für den Katastrophenschutz noch für das Rettungswesen diese Angaben nötig seien, denn sowohl § 22 Abs. 3 als auch § 14 Abs. 1 Brandenburgisches Katastrophenschutzgesetz sprechen von "niedergelassenen und angestellten Ärzten", gehen also eindeutig von Medizinern aus, die noch aktiv am Berufsleben teilnehmen. Bei einem Besuch in einem Gesundheitsamt stellten wir allerdings fest, dass zwar die Gründe für das Berufsende nicht mehr erfasst wurden, die Gesundheitsämter aus ihren Ärzteverzeichnissen jedoch nur diejenigen Ärzte löschten, die verstorben waren. Auf unseren Wunsch hin hat das Ministerium die Gesundheitsämter per Rundschreiben darauf hingewiesen, dass alle Ärzte, die - ganz gleich aus welchem Grund - aus dem Berufsleben ausgeschieden sind, unverzüglich aus dem Ärzteverzeichnis im Gesundheitsamt zu löschen sind.

Durch den Besuch in dem Gesundheitsamt erhielten wir auch Kenntnis davon, dass im Modul "Totenscheine - anonyme Statistik" inzwischen statt des Geburtsjahres nunmehr das vollständige Geburtsdatum erhoben wird. Bei Kenntnis dieses Datums, des ebenfalls erhobenen exakten Sterbedatums sowie der anzugebenden Postleitzahl kann jedoch eine Deanonymisierung nicht ausgeschlossen werden.

Geklärt werden sollte bei unserem Besuch in dem Gesundheitsamt vor allem, ob in das sog. "Adressbuch" das Geburtsdatum der Patienten wieder aufgenommen werden sollte. Da das Adressbuch eigentlich nur dem Schreibprogramm die Anschrift liefert, war uns zunächst erklärt worden, dass auf das Geburtsdatum verzichtet werden könne. Inzwischen hat sich jedoch herausgestellt, dass das Adressbuch in der ihm zugedachten Funktion nicht genutzt wird, sondern als Zugangsdatei und Aktennachweis des jeweiligen Sachgebiets dient. Für eine exaktere Recherche und um Verwechslungen auszuschließen setzten sich die Gesundheitsämter deshalb für die Wiedereinführung des Merkmals ein. Derzeit kann bei der Eingabe eines Namens auf eine Liste zurückgegriffen werden, die nicht nur die gleichlautenden Namen aufführt, sondern weitere im alphabetischen Umfeld liegende, ähnliche Namen anzeigt. Demgegenüber erschien uns eine zielgenauere Recherche mit dem Geburtsdatum datenschutzgerechter.

Das Gesundheitsamt wollte das Adressbuch sogar für die zentrale Aktenverwaltung nutzen. Derzeit verwalten einzelne Sachgebiete ihre Akten unter besonderen Kenn-

ziffern, so dass andere Sachgebiete nicht zugreifen können. Diese Lösung ist datenschutzgerecht und entspricht auch den Anforderungen, die sich aus der ärztlichen Schweigepflicht des einzelnen Amtsarztes oder Gesundheitsamts-Mitarbeiters ergeben. Das Gesundheitsamt strebte demgegenüber an, dass auch diese Abteilungen die Identifikationsmerkmale ihrer Klientel in das Adressbuch eintragen. Akten, aber auch schon die Information, bei welcher Abteilung eine Person vorgesprochen hat, dürfen grundsätzlich nur der zuständigen Abteilung zugänglich sein. Das ist auch deshalb wichtig, weil die Bürger sich zum einen freiwillig zu Beratungszwecken, zum anderen aber auch um einer gesetzlichen Pflicht zur Meldung oder Untersuchung nachzukommen, an das Gesundheitsamt wenden. Die dabei entstehenden Informationen dürfen nicht pauschal miteinander verknüpft werden.

Hinweise auf weitere Akten sollten primär vom Betroffenen selbst kommen, der dann auch in die Offenbarung an eine andere Abteilung einwilligen könnte. Denkbar wäre allenfalls, dass ein für das gesamte "Archiv“ des Gesundheitsamtes zuständiger Mitarbeiter Informationen darüber erhält, welche Sachgebiete Akten über welche Betroffenen führen. Wahrscheinlich wird das Gesundheitsamt aber von der Nutzung des Adressbuches als Klientendatei schon deshalb absehen, weil es inzwischen den Einsatz einer anderen Software plant.

Der Besuch in dem Gesundheitsamt brachte auch zu Tage, dass unsere bereits im Jahre 1996 geäußerte Forderung, beim Einsatz von Laptops durch die Gesundheitsämter Sicherheitssoftware einzusetzen, bisher nicht umgesetzt wurde. Das Gesundheitsamt hat allerdings darauf hingewiesen, dass mit der neuen Software künftig eine Verschlüsselung der Daten erfolgen könne. Wir haben das Ministerium für Arbeit, Soziales, Gesundheit und Frauen aufgefordert, den derzeit bestehenden, Zustand umgehend zu ändern, da wir anderenfalls den Einsatz der Laptops, der vor allem bei Schulreihenuntersuchungen erfolgt, beanstanden müssten.

Auch in Gesundheitsämtern muss die eingesetzte Software der ärztlichen Schweigepflicht Rechnung tragen. Daten über Klienten sind vor allem dann sicher zu verschlüsseln, wenn sie auf tragbaren Computern verarbeitet werden sollen.

8. Bildung, Jugend und Sport

8.1 Informationsbesuch in einem Oberstufenzentrum

Im Berichtszeitraum haben wir gemeinsam mit Vertretern des Ministeriums für Bildung, Jugend und Sport ein Oberstufenzentrum aufgesucht, um zu sehen, wie es organisiert ist, geleitet wird und welche datenschutzrechtlichen Probleme auftreten. Zu deren Lösung haben wir Hinweise gegeben. Das Oberstufenzentrum ist eine Schule mit mehreren Bildungsgängen, das als berufliche Schule mehrere Schulformen zusammenfasst. So ist auch die gymnasiale Oberstufe ein Teil des Oberstufenzentrums. An dem Oberstufenzentrum unterrichten ca. 100 Lehrer über

3.000 Schüler.

Angaben im Klassenbuch

Die Schulleitung hat eine Dienstanweisung zum Datenschutz für die Lehrer und die Mitglieder der Schulleitung erstellt. Darin heißt es, dass Angaben über ausgeliehene Unterrichtsmittel im Klassenbuch erfasst werden. Da die Lehrer über die Bücherausgabe rechenschaftspflichtig sind und der Eintrag in dem Schülerstammblatt der Datenschutzverordnung Schulwesen (DSV)[57] unpraktikabel ist - zumal für die Berufsfachschule, Berufsschule sowie Fachoberschule im Schülerstammblatt keine solche Rubrik vorgesehen ist - ist diese Angabe im Klassenbuch auch nach unserer Auffassung erforderlich.

Darüber hinaus ist zum Teil der Ausbildungsbetrieb im dualen System im Klassenbuch vermerkt. Die Nennung des Ausbildungsbetriebes der Schüler im Klassenbuch kann nur auf freiwilliger Basis erfolgen. Deshalb haben wir empfohlen, die Einverständniserklärung über die Zulässigkeit der Datenspeicherung im Klassenbuch in der Schülerakte abzuheften. Hintergrund der Notwendigkeit dieses zusätzlichen Datums ist die Nachfrage des Klassenlehrers beim Ausbildungsbetrieb, soweit der Schüler ohne Abmeldung abwesend ist. Die Kommunikation zwischen der Schule und dem Ausbildungsbetrieb wird durch eine Einverständniserklärung des Auszubildenden zugelassen. Damit erklärt sich der Auszubildende bereit, dass im Laufe seiner Ausbildung der Ausbildungsbetrieb berechtigt ist, Auskünfte über Verhaltensweise und Leistungen des Schülers zu erhalten. Diese Einverständniserklärung hat das Ministerium für Bildung, Jugend und Sport in Abstimmung mit uns als Muster veröffentlicht[58]. Wegen der im jeweiligen Ausbildungsverhältnis begründeten Mitteilungspflichten ist die Übermittlung entsprechender Daten keine Aufgabe der Schule. Informationen durch das Oberstufenzentrum an den Ausbilder sind daher nur nach vorheriger Einwilligung möglich. Soweit die Einwilligung nicht oder teilweise nicht erteilt bzw. widerrufen wird, dürfen dem Auszubilder daraus keine Nachteile entstehen. Für die Übermittlung der Informationen an den Ausbilder ist der Auszubildende dann selbst verantwortlich. Sofern nicht bereits im Ausbildungsvertrag eine entsprechende Festlegung getroffen wurde, soll die Einwilligung auf dem Formblatt eingeholt werden. Die Einwilligungserklärungen sind getrennt von den Schülerakten aufzubewahren.

Ausbildungsvertrag in der Schülerakte

Die erste Seite des Ausbildungsvertrages wird in der Schülerakte aufbewahrt. Die darin enthaltenen Angaben sind erforderlich, um nachprüfen zu können, welcher Betrieb den Schüler ausbildet, was er lernt sowie die Dauer des Lehrvertrages. Im Schülerstammblatt gemäß der Datenschutzverordnung Schulwesen[59] ist eine Spalte vorgesehen, in der eingetragen wird, ob der Ausbildungsvertrag vorgelegen hat. Problematisch ist nun die spätere Eintragung des bestehenden Berufsausbildungsverhältnisses in die Lehrlingsrolle seitens der Handwerkskammer. Der Ausbildende hat

gem. § 30 Abs. 1 Handwerksordnung unverzüglich nach Abschluss des Berufsausbildungsvertrages die Eintragung in die Lehrlingsrolle zu beantragen, wobei eine Ausfertigung des Vertrages beizufügen ist. Eine Rückmeldung von der Handwerkskammer an die Schule ist nicht vorgesehen. Sobald der Schüler den Ausbildungsvertrag abgeschlossen hat, legt er diesen dem Oberstufenzentrum vor, wobei die Schule so schnell wie möglich, d. h. innerhalb von zwei Tagen, das Kästchen in der Anlage 3 S. 1 DSV ("Ausbildungsvertrag hat vorgelegen") ankreuzt und dem Schüler den Vertrag zurückgibt. Die Kopien verbleiben drei Jahre in der Schülerakte.

Unabhängig von der Tatsache, ob eine Eintragung in die Lehrlingsrolle stattgefunden hat, reicht die Vorlage des Ausbildungsvertrages allein nicht aus, um überprüfen zu können, ob die Berufsangabe tatsächlich stimmt. Für die Einteilung in bestimmte Klassen ist die genaue Berufsbezeichnung erforderlich. Nach Rücksprache mit dem Ministerium kann nach dem Eintrag und der Bestätigung des Ausbildungsberufes die Kopie der ersten Seite des Berufsausbildungsvertrages dem Schüler zurückgegeben werden, da alle erforderlichen Angaben im Schülerstammblatt bereits enthalten sind. Der Ausbildungsvertrag darf nicht länger als ein halbes Jahr in der Schülerakte gespeichert werden.

Technisch-organisatorische Aspekte

Das besuchte Oberstufenzentrum wurde vor kurzem rekonstruiert. Dabei sind bei der Planung auch die Aspekte des Datenschutzes und der Datensicherheit berücksichtigt worden. Eine wichtige Maßnahme, den Server des lokalen Verwaltungsnetzes in einem separaten Raum unterzubringen, musste jedoch aus Platzgründen wieder verworfen werden. Das Oberstufenzentrum hat in dem Serverraum einen Arbeitsplatz eingerichtet. Dies haben wir bemängelt und gefordert, den Server in einem Raum unterzubringen, der nur von berechtigten Personen betreten werden darf.

Bei jeder Datenerhebung gilt der Grundsatz der Datensparsamkeit. Es sollen nur solche Daten erfasst werden, die unbedingt erforderlich und nicht bereits schon an einer anderen Stelle vermerkt worden sind. Auch bei der Gestaltung eines Schulrechnernetzes sind technisch-organisatorische Aspekte des Datenschutzes zu berück-sichtigen.

8.2 Wer ist für Vordrucke verantwortlich?

Ein Petent wandte sich an uns mit der Bitte, das Formular "Bescheinigung über Arbeitsverdienst" zu überprüfen, mit dem das Jugendamt die Einkommensverhältnisse des Unterhaltsverpflichteten ermitteln wollte. Der Petent rügte darin u. a. Fragen nach der Kirchenzugehörigkeit, dem Arbeitgeber des Ehegatten, einer zweiten Lohnsteuerkarte.

Bereits im 6. Tätigkeitsbericht[60] haben wir zu Teilaspekten des Formulars Stellung

genommen. Das hier betroffene Jugendamt räumte ein, dass die Kirchenzugehörigkeit sowie die Anschrift des Arbeitgebers des Ehegatten für die Unterhaltsberechnung nicht erforderlich seien. Es teilte mit, dass es üblich sei, bei Versendung des zusätzlichen Formulars die Spalte "Auskünfte über den Ehepartner" zu streichen. Aufgrund der Arbeitsintensität im Jugendamt sei dies hier versehentlich unterblieben.

Weiterhin führte das Jugendamt aus, dass der Arbeitgeber die Frage nach der zweiten Lohnsteuerkarte nur nach den vorliegenden Kenntnissen beantworten könne. Sollte eine zweite Karte vorhanden sein, müsse das Jugendamt prüfen, inwieweit dieses Einkommen für die Unterhaltsberechnung herangezogen werden könne. Hierzu vertreten wir die Auffassung, dass die Beantwortung dieser Frage nicht generell verlangt werden kann. Eine Beantwortung würde in vielen Fällen auf Vermutungen basieren, da der Arbeitgeber in der Regel über ein weiteres Arbeitsverhältnis des Unterhaltsverpflichteten keine Kenntnis haben dürfte. Eine andere Beurteilung würde sich nur dann ergeben, wenn der Arbeitgeber seine Aussagen zu einem Arbeitsverhältnis mit der Versteuerung nach Lohnsteuerklasse VI treffen würde. Nur in diesem Fall muss einer Lohnsteuerkarte eine weitere Steuerkarte zugeordnet werden. Dann dürfte dem Arbeitgeber häufig bekannt sein, welche Steuerklasse bei dem Haupterwerbsverhältnis gilt. Soweit die Frage die letztere Konstellation betrifft, haben wir das Jugendamt aufgefordert, diese Frage zu präzisieren.

Das Jugendamt wies im Übrigen darauf hin, dass es sich bei dem Vordruck um keine eigene Entwicklung des Jugendamtes handele, sondern um ein Exemplar, das über einen Vordruckverlag vertrieben werde und somit unsere Bedenken gegenüber dem Verlag deutlich zu machen seien. Für die Rechtmäßigkeit der Datenerhebung sind jedoch ausschließlich die datenverarbeitenden Stellen verantwortlich, nicht deren private Vertragspartner. Das Jugendamt als datenerhebende Stelle ist unser alleiniger Ansprechpartner und hat selbst sicherzustellen, dass das Formular den datenschutzrechtlichen Vorgaben entspricht.

Hersteller von Vordrucken und Formularen überprüfen ihre Produkte nicht immer in datenschutzrechtlicher Hinsicht. Vor der Abnahme solcher Formulare empfehlen wir den betroffenen Behörden deshalb, diese im Zweifel von uns überprüfen zu lassen oder die Abnahme von einer Zusicherung des Verlages abhängig zu machen, dass die Formulare datenschutzgerecht sind. Auch dann bleibt die Behörde, die die Formulare verwendet, datenschutzrechtlich in der Pflicht.

8.3 Weiterleitung von Prüfungsunterlagen an externen Schulrat

Ein Schulrat erhielt von dem Schulrat eines anderen Landkreises eine schriftliche Aufforderung, ihm über das staatliche Schulamt Prüfungsunterlagen aus dem mündlichen Abitur für das Fach Chemie weiterzuleiten. Der Schulrat wies darauf hin, dass die Schülernamen unkenntlich zu machen seien. Die Kenntnis der Daten (z. B. Aufgabenstellung für die Prüfung, Verlaufsprotokoll sowie tragende Erwägungen für die Begründung der Entscheidung) seien für die Untersuchung der Qualitätsentwicklung der mündlichen Prüfung im Fach Chemie erforderlich.

Alle im Zusammenhang mit der Abiturprüfung erworbenen Informationen und Unterlagen - ausgenommen die Aufgabenstellungen nach Abschluss des gesamten Abiturs - sind nach § 41 Gymnasiale Oberstufen-Verordnung geheim zu halten. Die Tatsache der mündlichen Abiturprüfung in einem Spezialfach in Verbindung mit der Schule, insbesondere wenn es - wie hier - um einen Einzelfall geht, kann einem bestimmten Schüler zugeordnet werden. Es handelt sich somit um personenbezogene Daten, d. h. eine Unkenntlichmachung der Schülernamen allein stellt entgegen der Auffassung des Schulrates noch keine ausreichende Anonymisierung dar. Die Ergebnisse können daher nur in anonymisierter Form, d. h. ohne konkrete Bezeichnung der Schule und der an dem Prüfungsausschuss Beteiligten (insbesondere Schulleiter, Lehrkräfte der Schule), dem Schulrat des anderen Landkreises zur Verfügung gestellt werden. Hierfür dürfen Kopien angefertigt werden, die keinen Rückschluss auf die jeweilige Person des Schülers sowie der Schule zulassen und dementsprechende Schwärzungen enthalten.

Dem Schulamt haben wir empfohlen, sofern weitere Schulen betroffen seien, darauf hinzuweisen, dass nur anonymisierte Daten abgefordert werden dürfen.

8.4 Organisation von Klassentreffen

Ein privates Unternehmen mit Sitz in Brandenburg organisiert und führt geschäftsmäßig bundesweite Klassentreffen durch. Hierfür benötigt es die Namen und Anschriften ehemaliger Schüler. Da die Schule diese Daten nur mit Einwilligung der betroffenen Schüler an Dritte herausgeben darf, empfahlen wir ein Adressmittlungsverfahren. Dabei gibt der Interessent der angeschriebenen Schule - falls diese zustimmt - vorfrankierte (nicht adressierte) Kuverts mit dem zu übersendenden Material. Dort werden die Kuverts dann aufgrund des dort vorliegenden Anschriftenmaterials adressiert und verschickt. Der Adressat entscheidet selbst durch seine Rückantwort, dass er sich mit dem Interessenten in Verbindung setzen will. Nachträglich erfuhren wir, dass als Absender nicht die Schulen, sondern das Unternehmen benannt war.

Ein datenschutzrechtliches Problem entsteht dadurch, dass bei Unzustellbarkeit und Rücksendung der Briefe das Unternehmen die Namen und früheren Anschriften ehemaliger Schüler erfährt. Der Auffassung des Unternehmens, dass diese Daten unverwertbar seien, steht die Möglichkeit entgegen, anhand des veralteten Adressmaterials über eine einfache Melderegisterauskunft (§ 32 Abs. 1 Brandenburgisches Meldegesetz) Auskunft u. a. über gegenwärtige Anschriften, Haupt- und Nebenwohnungen sowie über Familiennamen zu erhalten. Auf diesem Wege sind auch im Falle eines Namenswechsels durch Heirat die Neuanschriften ermittelbar. Über diese unzulässige Umgehung des Adressmittlungsverfahrens hinaus wiesen wir darauf hin, dass in dem Begleitschreiben das Verfahren an sich erläutert werden sollte, was mittlerweile geschehen ist. Wenn dem Empfänger das Verfahren nicht transparent gemacht wird, vermutet er möglicherweise einen Missbrauch seiner Daten. Des weiteren ist er im Begleitschreiben über die Art und Weise der Speicherung der Daten,

die Dauer der Speicherung sowie den Nutzungszweck der Daten zu informieren.

Soweit diese Voraussetzungen nicht erfüllt sind, werden wir die Unbedenklichkeit des Adressmittlungsverfahrens nicht bestätigen können.

Die Schule ist nicht verpflichtet, das Adressmittlungsverfahren durchzuführen. Bei dessen Durchführung ist darauf zu achten, dass die vorfrankierten Kuverts den Absender der Schule tragen und auf das Verfahren im Begleitschreiben hingewiesen wird. Das Verfahren darf durch den Einsatz von Privatpersonen zur Entlastung der Schule nicht umgangen werden.

8.5 Vorlage von Betreuungsverträgen

Ein Amt teilte uns mit, dass zur Erstattung von Personalkosten für Kinder, die in einem anderen Landkreis betreut werden, dem aufnehmenden Landkreis die Betreuungsverträge in Kopie zum Nachweis der Kosten übermittelt werden sollten. Angaben, wie Name des Kindes, Betreuungszeitraum u. a. sollten ursprünglich erfasst werden.

Die Wohnortgemeinde hat auf Verlangen der aufnehmenden Gemeinde oder des Gemeindeverbandes nach § 16 Abs. 3 Kita-Gesetz einen angemessenen Kostenausgleich zu gewähren, wenn es in der Wohnortgemeinde kein ausreichendes Angebot gibt und in Kindertagesstätten Kinder aus anderen Gemeinden oder Gemeindeverbänden aufgenommen werden. Soweit überhaupt ein Informationsaustausch stattfinden muss, dürfen dem aufnehmenden Landkreis nur die Angaben, die für den Nachweis erforderlich sind, zur Kenntnis gebracht werden. Angaben z. B. über die Arbeitsstätte der Eltern mit Telefonnummern sind für die Nachweisprüfung nicht erforderlich.

Der abgebende Landkreis hat uns schließlich mitgeteilt, dass die Kopien der Betreuungsverträge für die Bearbeitung des Kostenausgleiches weder herangezogen wurden noch in Zukunft vorgelegt werden sollen. Der Landkreis benötigt lediglich die Angaben zum Namen, Vornamen und Wohnort des jeweiligen Kindes und zur Dauer der Betreuung.

Vor einer Datenübermittlung zwischen öffentlichen Stellen ist zunächst vom Grundsatz des rechtmäßigen Verwaltungshandelns auszugehen: Ämter untereinander müssen sich auf behördliche Auskünfte verlassen können. Den Angaben der rechnungsstellenden Ämter soll grundsätzlich ohne Vorlage von Kopien der Betreuungsverträge vertraut werden.

8.6 Kontrolle der Zentralen Adoptionsstelle Berlin-Brandenburg

Im letzten Jahr berichteten wir darüber, dass wir gemeinsam mit dem Berliner Datenschutzbeauftragten eine gemeinsame Ländereinrichtung, die Zentrale Adoptionsstelle Berlin-Brandenburg, kontrolliert hatten. Wir haben dem Ministerium für Bildung, Jugend und Sport mitgeteilt, anstelle des externen Wartungstechnikers sei ein Mitarbeiter des Landesjugendamtes zum Systemverwalter zu qualifizieren und diesem sämtliche Wartungsaufgaben zu übertragen. Das Ministerium unterrichtete uns darüber, dass eine solche Qualifizierung aus personalrechtlichen Gründen nicht möglich sei. Als Alternative dazu bot es an, ab sofort die Wartungsarbeiten des externen Technikers ausschließlich unter Aufsicht des jeweils betroffenen PC-Arbeitsplatzinhabers bzw. seines persönlichen Vertreters durchführen und die jeweiligen Wartungsvorgänge von dem für die Überwachung zuständigen Bediensteten protokollieren zu lassen.

Diese Maßnahme ist jedoch nur übergangsweise aufgrund der knappen personellen Ressourcen ausreichend. Deshalb wiesen wir darauf hin, dass vor dem Hintergrund der Wahrung des Sozialgeheimnisses sobald als möglich die Qualifizierung eines Bediensteten des Landesjugendamtes sichergestellt sein muss. Um die jeweiligen Wartungsvorgänge ordnungsgemäß überwachen zu können, sind entsprechende technische Kenntnisse unverzichtbar. Zudem dürfte eine solche Weiterqualifizierung mit relativ geringem Aufwand möglich sein.

Im Übrigen hat die Zentrale Adoptionsstelle Berlin-Brandenburg alle weiteren Forderungen aus unserem Prüfbericht in Abstimmung mit dem Berliner Datenschutzbeauftragten erfüllt.

9. Wissenschaft, Forschung und Kultur

9.1 Evaluation der Lehre und des Studiums

Zur Qualitätsverbesserung der Lehre hat eine Fachhochschule die Lehre durch eine Befragung von Studenten evaluiert. Studierende haben die Lehrleistung einzelner Dozenten in bestimmten Lehrfächern mittels Fragebogen anonym (ohne Nennung des eigenen Namens) beurteilt. Die Evaluation erfolgte nach dem Zufallsprinzip, indem ein abgeschlossenes Trimester bewertet wurde. Erfasst wurden die Fächer hauptamtlich Lehrender und Lehrbeauftragter. Der Personalrat hat die vorgesehene personenbezogene Veröffentlichung der Evaluationsergebnisse aus Gründen nachteiliger Auswirkungen im Beurteilungsverfahren von Lehrenden abgelehnt. Der Direktor und die Leitung der Hochschule hingegen vertreten die Auffassung, dass die einbezogenen Studierenden ein Recht darauf haben zu erfahren, wie die Leitung auf studentische Veranstaltungskritik reagiert, und wird deshalb die durch die Dozenten erreichten Punktwertzahlen veröffentlichen. Die Hochschule bat uns zu prüfen, ob diesem Vorhaben datenschutzrechtliche Bedenken entgegen stehen.

Die Leitung der Fachhochschule beruft sich auf die am 25. August 1998 in Kraft getretene Neufassung des § 6 Hochschulrahmengesetz[61], wonach u. a. die Arbeit der Hochschulen in Forschung und Lehre regelmäßig bewertet werden soll. Die Studierenden sind bei der Bewertung der Qualität der Lehre zu beteiligen. Die Ergebnisse der Bewertungen sollen veröffentlicht werden. Datenerhebungen zum Zwecke der Evaluation sind nach dem Entwurf zur Novellierung des Brandenburgischen Hochschulgesetzes[62] zwar zulässig, jedoch enthält weder das Hochschulrahmengesetz noch das Landesrecht Aussagen über die Art und Weise der Veröffentlichungen. Da die Lehrtätigkeit Gegenstand der Evaluierung ist, muss die Zulässigkeit der Umfrage an der spezifischen Stellung und Rolle der Dozenten gemessen werden.

Sie sind Amtsträger und kommen mit der Lehrtätigkeit den sich aus dieser Eigenschaft ergebenden Aufgaben nach. Solange Amtsträger im Rahmen ihrer Funktionen handeln, haben sie gewisse Einschränkungen ihres Rechts auf informationelle Selbstbestimmung hinzunehmen. Hierbei ist jedoch folgendes zu beachten:

Zweck und Folgen der Umfrage, also auch und gerade die Grenzen der Verwertbarkeit, sind von Anfang an klar anzugeben. Umfragen, die auf Initiative der Hochschule vorgenommen werden, unterliegen den spezifischen personal- und hochschulverfassungsrechtlichen Bedingungen, insbesondere den Mitwirkungsrechten der jeweiligen Vertretungen der Beschäftigten. Die Befragung darf nur zu dem Zweck der Beurteilung der Qualität der Lehre und nicht zu der personalrechtlichen Beurteilung des einzelnen Hochschullehrers mit evtl. Sanktionen aufgrund der Evaluationsergebnisse durchgeführt werden. Unter dieser Voraussetzung halten wir die von der Fachhochschule vorgesehene Veröffentlichung der Bewertungsergebnisse datenschutzrechtlich für zulässig.

Die Hochschule hat in ihrer Eigenschaft als Dienstbehörde auf das informationelle Selbstbestimmungsrecht ihrer Bediensteten zu achten. Aus der Veröffentlichung dürfen sich keine personellen Konsequenzen ergeben: So dürfen die Ergebnisse nicht in die Personalakte aufgenommen werden.

9.2 Pauschale Meldung an das BAföG-Amt?

Das Staatliche Rechnungsprüfungsamt empfahl einer Universität, dem Amt für Ausbildungsförderung die monatlichen Exmatrikulationen aller Studenten mitzuteilen, auch soweit sie keine BAföG-Empfänger sind. Damit sollen Überzahlungen vermieden werden, falls der frühere Student dem Amt für Ausbildungsförderung seine Exmatrikulation nicht rechtzeitig mitteilt. Dem Studierenden wird über zwei Semester Ausbildungsförderung gewährt, wenn er mit Stellung des Antrages eine Studienbescheinigung vorlegt. Bricht der Studierende in dieser Zeit das Studium ab, so hat er dies gem. § 60 SGB I i. V. m. § 47 Abs. 4 BAföG-Gesetz dem Amt für Ausbildungsförderung sofort mitzuteilen. Das Amt für Ausbildungsförderung wandte sich an uns mit der Bitte, die beabsichtigte Datenübermittlung der Universität zu

beurteilen.

Nach § 14 Brandenburgisches Datenschutzgesetz ist die Kenntnis der Daten dann erforderlich, wenn die öffentliche Stelle im jeweiligen konkreten Einzelfall ihre Aufgaben anderenfalls nicht, nicht vollständig oder nicht in rechtmäßiger Weise erfüllen kann. Das Amt für Ausbildungsförderung benötigt zwar Informationen über die Exmatrikulationen, jedoch nur hinsichtlich derjenigen Studenten, die BAföG-Empfänger sind. Da nur rund ein Drittel der gesamten Studentenschaft BAföG-Empfänger sind, würde die Übermittlung der Daten aller übrigen Studenten an das BAföG-Amt zu einer unzulässigen Bekanntgabe personenbezogener Daten führen. Eine Möglichkeit, die Studenten, die Ausbildungsförderung beziehen, aus der Anzahl der exmatrikulierten Studenten herauszufiltern, besteht für die Universität nicht. Wir haben deshalb der Hochschule eine datenschutzgerechte Alternative empfohlen. Die Universität weist alle Studierenden, die die zweite Wiederholungsprüfung endgültig nicht bestanden haben, schriftlich darauf hin, dass sie, soweit sie BAföG-Empfänger sind, unverzüglich nach der Exmatrikulation das BAföG-Amt zu informieren haben.

Eine Datenübermittlung an das Amt für Ausbildungsförderung bei allen Exmatrikulationen ist nicht erforderlich und im übrigen unverhältnismäßig.

9.3 Studie: Situation von Einelternfamilien

Teilnehmerinnen dieser Studie sollen alleinerziehende Mütter und Väter sein, bei denen für mindestens ein Kind der Unterhaltsvorschuss weggefallen ist. In den verschiedenen Phasen der Studie setzt die forschende Fachhochschule eine schriftliche Befragung, teilstrukturierte Interviews, Experten - und Gruppengespräche als Erhebungsmethoden ein. Die Gewinnung der Teilnehmerinnen für die schriftliche Befragung soll mit Unterstützung der Jugendämter der Landkreise und der kreisfreien Städte u. a. durch einen schriftlichen Teilnahmeaufruf erfolgen. Die Mitarbeiter der Ämter sehen den Datenschutz gefährdet, so dass uns die Fachhochschule um eine fachliche Stellungnahme bat.

Für die Übermittlung von Sozialdaten zu Forschungszwecken sind die Voraussetzungen des § 75 SGB X vorrangig zu prüfen und nicht - wie die Fachhochschule angenommen hat - die des § 28 Brandenburgisches Datenschutzgesetz. Danach ist eine Übermittlung von Sozialdaten zulässig, soweit sie für ein bestimmtes Vorhaben der wissenschaftlichen Forschung im Sozialleistungsbereich erforderlich ist und schutzwürdige Interessen des Betroffenen nicht beeinträchtigt werden oder das öffentliche Interesse an der Forschung oder Planung das Geheimhaltungsinteresse des Betroffenen *erheblich* überwiegt. Eine Übermittlung ohne Einwilligung des Betroffenen ist nicht zulässig, soweit es zumutbar ist, die Einwilligung des Betroffenen einzuholen oder den Zweck der Forschung oder Planung auf andere Weise zu erreichen.

Mit Hilfe des Adressmittlungsverfahrens[63] werden der Fachhochschule die Adressen

der alleinerziehenden Mütter und Väter - soweit diese dem Teilnahmeaufruf folgen - zugänglich gemacht. Wir haben empfohlen, in dem Teilnahmeaufruf auf die Organisation des Versandes hinzuweisen, damit den Betroffenen transparent wird, wie die Fachhochschule mit den ausgewählten Jugendämtern in Kontakt getreten ist. Die potentiellen Teilnehmerinnen müssen in der schriftlichen Befragung über die Studie und die freiwillige Teilnahme ausreichend aufgeklärt werden.

"Dürfen namentlich benannte Projektmitarbeiterinnen aus der Fachhochschule die Jugendämter bei der Versendeaktion unterstützen?", lautete eine der Fragen des Projektleiters. Die Beteiligung der Projektmitarbeiterinnen würde zu einer Datenübermittlung von Sozialdaten führen, die dem Sozialgeheimnis unterliegen. Es müssten die Voraussetzungen des § 75 SGB X i. V. m. § 61 Abs. 1 Satz 1 SGB VIII erfüllt sein, insbesondere müsste das Ministerium für Bildung, Jugend und Sport dieses Vorhaben genehmigen. Einfacher und weniger aufwendig wäre die Möglichkeit, mit den für Unterhaltsangelegenheiten zuständigen Sachbearbeitern des Jugendamtes einen Werkvertrag abzuschließen, wonach diese z. B. nach Feierabend die Versendeaktion vornehmen könnten. In dem Werkvertrag sollte klargestellt werden, dass die Jugendamtsmitarbeiter gegenüber den Forschern nicht weisungsgebunden sind und ihre Schweigeverpflichtung fortgilt. Durch die Art der Nutzung der Adressdaten im Wege des Adressmittlungsverfahrens werden schutzwürdige Rechte der Betroffenen nicht berührt, so dass eine Übermittlung von Sozialdaten an Dritte zum Schutz des Rechts auf informationelle Selbstbestimmung vermieden werden könnte.

Für Forschungsprojekte gilt der Grundsatz: Je transparenter für den Betroffenen der Umgang des forschenden Institutes mit seinen personenbezogenen Daten wird, desto eher wird der Betroffene bereit sein, mit dem forschenden Institut bei der anschließenden Befragung auf freiwilliger Basis zusammenzuarbeiten.

9.4 Nachbeobachtung der Studie "Gesundheit, Ernährung und Krebs"

Die Brandenburger Ernährungs- und Krebsstudie ist Bestandteil eines europäischen Projektes "Europa gegen den Krebs"[64]. Die Rekrutierung für diese Langzeitstudie hat das Forschungsinstitut im September 1998 mit insgesamt 27 616 Teilnehmern abgeschlossen. Daran schließt sich eine Nachbeobachtungsphase an, in der alle aufgetretenen Krebserkrankungen sowie das Auftreten von 24 weiteren chronischen Erkrankungen erhoben werden. Die Nachbeobachtung hat bereits 1997 begonnen und wird über die nächsten 10 bis 15 Jahre fortgesetzt werden. Sie geht zunächst von Selbstangaben in einem Fragebogen über aufgetretene Erkrankungen aus. Wissenschaftlich verwendbar werden diese Angaben jedoch erst durch entsprechende medizinische Unterlagen oder Arztauskünfte. Dazu ist vor der Erstuntersuchung nach entsprechender Aufklärung eine Einverständniserklärung unterschrieben worden. Die einzelnen Schritte hat das Institut mit uns abgestimmt.

Im Gespräch mit dem Projektleiter traten zwei neue Fragen auf:

1. *Müssen die Fragebogen unmittelbar nach ihrer Auswertung vernichtet werden?*

Aufgrund der in der Vergangenheit aufgetretenen Missbrauchsfälle wird ein Nachweis zu Beweiszwecken bis zum Abschluss des Forschungsvorhabens für nötig gehalten. Daher scannt das Institut die Fragebogen ein und archiviert sie gleichzeitig. Erst nach dieser Reproduktion der Originaldaten werden die Fragebogen vernichtet. Gegen diese Verfahrensweise bestehen aus unserer Sicht keine Bedenken, da auf den Fragebogen lediglich die Studiennummer ohne den betreffenden Namen angegeben ist. Auch aus technisch-organisatorischer Sicht ist hiergegen nichts einzuwenden. Es werden personenbezogene Daten verschlüsselt auf dem Server gespeichert und Zugriffsrechte restriktiv vergeben. Der Serverraum wurde unseren Forderungen entsprechend gesichert.

2. *Gibt es eine Pflicht des Forschungsinstitutes zur Vorlage der Einverständniserklärungen gegenüber Kliniken und Ärzten?*

Da Teilnehmer Kliniken und Ärzte in Brandenburg und Berlin angeben, muss das Forschungsinstitut die Möglichkeit haben, diese Angaben zu überprüfen. Das Institut vertritt hierzu die Auffassung, dass das Versenden der Einverständniserklärung zu schützende Daten offenlegen würde, und legte bisher lediglich das Muster einer Schweigepflichtentbindungserklärung vor. Die Ärztekammer Berlin hat dies - im Gegensatz zur Landesärztekammer Brandenburg - als unzureichend abgelehnt, weil es sich um pauschale Einverständniserklärungen handele, die die Probanden bei der ca. 5 Jahre zurückliegenden Basiserhebung abgegeben hätten und für den Arzt aufgrund ihrer pauschalen Aussagen z. T. nicht nachvollziehbar seien. In dem Informationsschreiben an den Arzt oder an das Krankenhaus ist deshalb klarzustellen, aus welchen Gründen die vorliegende Einverständniserklärung immer noch hinreichend bestimmt für eine Nachbeobachtung ist. Die Probanden aktualisieren - wenn sie sich an der Nachbeobachtung beteiligen wollen - mit ihren Angaben über die behandelnden Ärzte in dem Nacherhebungsbogen ihre Einverständniserklärung. Auf diesen Umstand sind die Ärzte ausdrücklich hinzuweisen.

Da der Arzt, der die Verantwortung für den Bruch der ärztlichen Schweigepflicht ggf. auch strafrechtlich tragen müsste, darüber entscheidet, welcher Nachweis ihm für das Vorliegen der Schweigepflichtentbindungserklärung bei einer anderen Stelle genügt, muss ihm das Institut im Zweifelsfall eine Kopie der Einwilligungserklärungen mit geschwärztem Code der Probanden zur Verfügung stellen.

9.5 Benutzungsordnung und Verwaltungsvorschriften für das Brandenburgische Landeshauptarchiv

Für das Landeshauptarchiv fehlt noch immer eine aktualisierte Benutzungsordnung. Nach erneuter Prüfung halten wir eine Aufnahme des Formulars des Benutzungsantrags in die Benutzungsordnung nicht mehr für erforderlich. Das Ministerium für Wissenschaft, Forschung und Kultur hat uns zugesichert, dass Änderungen der

Antragsformulare zuvor mit uns abgestimmt werden. Dem In-Kraft-Treten der Benutzungsordnung stehen somit keine datenschutzrechtlichen Einwände mehr entgegen.

Bisher verwendet das Landeshauptarchiv Benutzungsbestimmungen, die auf dem Bundesarchivgesetz vom 6. Januar 1988 beruhen und Benutzern der DDR-Bestände diese mit dem Brandenburgischen Archivgesetz unvereinbare Bestimmung als Handreichung zur Verfügung stellen. Ein Benutzer wandte sich an uns und rügte, dass mit dieser Bestimmung den Benutzern eine vollkommen falsche Information gegeben werde.

Der Petent hat zusammen mit dem Landeshauptarchiv und dem Ministerium ein klärendes Gespräch geführt, in dem folgender Kompromiss gefunden wurde: ein Vorblatt informiert die Benutzer darüber, dass die Bestimmungen, die mit dem Archivgesetz nicht übereinstimmen, nicht gelten. So berief sich die Benutzungsbestimmung z. B. auf eine dreißigjährige Schutzfrist, die jedoch durch § 10 Abs. 6 Brandenburgisches Archivgesetz für DDR-Bestände aufgehoben worden ist und deshalb mit dem Landesrecht unvereinbar ist.

Im Anschluss an den sechsten Tätigkeitsbericht[65] hat uns das Ministerium für Wissenschaft, Forschung und Kultur mitgeteilt, dass es den Entwurf der Verwaltungsvorschriften unter Berücksichtigung unserer damaligen Stellungnahme mit den Archivaren überarbeiten und uns bis Ende Januar 1999 zuleiten werde. Anschließend soll mit uns eine Beratung über den Entwurf stattfinden.

Rechtsunsicherheiten in der Praxis im Rahmen der Benutzung von Archivgut können durch die neu zu erlassende Benutzungsordnung und die Verwaltungsvorschriften weitgehend vermieden werden.

10. Stadtentwicklung, Wohnen und Verkehr

10.1 Verkehr

10.1.1 Datenschutz bei der Transrapid-Planung

Für den Bau der Magnetschnellbahnstrecke Berlin - Hamburg muss ein Planfeststellungsverfahren i. S. v. §§ 72 ff. Verwaltungsverfahrensgesetz (VwVfG) durchgeführt werden, wobei die Strecke in 20 Planungsabschnitte unterteilt wurde, von denen ein Teil auf brandenburgischem Gebiet liegt.

In einem gemeinsamen Gespräch der Datenschutzbeauftragten der betroffenen

Länder bei der Trägerin des Vorhabens, der Magnetschnellbahnplanungsgesellschaft mbH, informierte diese über die Absicht, das Planfeststellungsverfahren möglichst effizient und papierlos mittels eines Datenverarbeitungssystems durchzuführen, das alle Einwendungen verarbeitet, Texte für deren Erwiderung erzeugt und anschließend auch Textbausteine für die Planfeststellungsbeschlüsse generieren kann. Praktisch sollte dies so vonstatten gehen: Die jeweilige Anhörungsbehörde (hier das Brandenburgische Landesamt für Verkehr und Straßenbau) scannt alle Einwendungen ein und übermittelt sie in personenbezogener Form an die Trägerin des Vorhabens, so dass diese der Anhörungsbehörde Erwiderungen auf die Einwendungen über das System zur Verfügung stellt. Im Anschluss daran findet der in § 73 Abs. 6 VwVfG vorgesehene Erörterungstermin statt.

Derartige Übermittlungen personenbezogener Daten an Stellen außerhalb des öffentlichen Bereichs sind nach § 16 Abs. 1 lit. a Brandenburgisches Datenschutzgesetz (BbgDSG) zulässig, wenn sie zur rechtmäßigen Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen des § 13 Abs. 1 BbgDSG vorliegen.

Obwohl die Anhörungsbehörde nach § 73 Abs. 6 VwVfG die Aufgabe hat, die erhobenen Einwendungen gegen den Plan sowie die Stellungnahmen der Behörden zum Plan mit der Trägerin des Vorhabens, den Behörden, den Betroffenen sowie den Personen, die Einwendungen erhoben haben, zu erörtern, wofür eigentlich der Vortrag gegenüber der Anhörungsbehörde genügen würde, halten wir die personenbezogene Datenübermittlung an die Vorhabenträgerin unter dem Aspekt einer sachbezogenen Erörterung der Einwendungen im Erörterungstermin in den Fällen für erforderlich, in denen Bürger die Verletzung eigener Rechte, z. B. ihrer Gesundheit oder ihres Eigentums, geltend machen. Auch unter Berücksichtigung des Rechtsgedankens aus § 29 Abs. 1 VwVfG kann eine Befugnis zur Übermittlung personenbezogener Daten an die Vorhabenträgerin in den Fällen abgeleitet werden, in denen die Kenntnis der Daten für die Geltendmachung der rechtlichen Interessen der Beteiligten erforderlich ist. Dies kann nur dann als gegeben vorausgesetzt werden, wenn die Erörterung aufgrund betroffener Individualrechtsgüter unmittelbar personenbezogen durchgeführt werden muss. Dagegen halten wir eine Übermittlung personenbezogener Daten von Pauschaleinwendern, die sich für allgemeine Belange - z. B. den Naturschutz - einsetzen und keine Verletzung eigener Individualrechte geltend machen, für unzulässig. Dass die spätere unverschlüsselte Veröffentlichung von personenbezogenen Einwendungen im Planfeststellungsverfahren ein unverhältnismäßiger Eingriff in die Grundrechte der Einwender wäre, hat bereits das Bundesverfassungsgericht festgestellt[66]. Sie wurde deshalb bei der Transrapid-Planung auch nicht ins Auge gefasst.

Das Brandenburgische Landesamt für Verkehr und Straßenbau hat unseren Vorgaben für eine differenzierte Datenübermittlung zugestimmt und wird Einwendungen von Pauschaleinwendern unter Schwärzung der personenbezogenen Daten an die Vorhabenträgerin übermitteln.

Die Transrapid-Planung macht deutlich, dass in Planfeststellungsverfahren stets differenziert zu entscheiden ist, in welchem Umfang personenbezogene Daten über Einwender übermittelt werden dürfen.

10.1.2 Neues Führerscheinrecht

- Änderung des Straßenverkehrsgesetzes und anderer Gesetze

Am 1. Januar 1999 ist das Gesetz zur Änderung des Straßenverkehrsgesetzes und anderer Gesetze[67] in Kraft getreten. Es enthält wesentliche datenschutzrechtliche Neuerungen.

Alle Fahrerlaubnisinhaber werden fortan in einem beim Kraftfahrtbundesamt eingerichteten Zentralen Fahrerlaubnisregister gespeichert (mit ihren Ident- und Führerscheindaten). Der Gesetzgeber hat für die Auflösung der örtlichen Fahrerlaubnisregister eine Frist bis zum 31. Dezember 2005 gesetzt, so dass ein Nebeneinander dieser Register auf einen Übergangszeitraum beschränkt bleibt.

Neu ist des Weiteren, dass die Protokolldaten über Abrufe aus dem Verkehrszentralregister, dem Zentralen Fahrzeugregister und dem Zentralen Fahrerlaubnisregister zur Aufklärung oder Verhütung von schwerwiegenden Straftaten gegen Leib, Leben und Freiheit einer Person genutzt werden dürfen. Dazu werden die Protokolldaten nunmehr sechs Monate aufbewahrt. Sie erhalten den Charakter polizeilicher Fachdateien.

Mit der Änderung des Straßenverkehrsgesetzes wurden erstmalig Festlegungen für die Datenverarbeitung in Führerscheinakten getroffen. Registerauskünfte, Führungszeugnisse, Gutachten und Gesundheitszeugnisse sind spätestens nach zehn Jahren zu vernichten, es sei denn, sie stehen im Zusammenhang mit einer Eintragung im Verkehrszentralregister oder im Zentralen Fahrerlaubnisregister. Die Vernichtung solcher Unterlagen müssen allerdings erst dann vernichtet und Altakten berichtigt werden, wenn die Fahrerlaubnisbehörde aus anderem Anlass mit dem Vorgang befasst ist. Eine Überprüfung aller Akten soll innerhalb der nächsten 15 Jahre erfolgen.

- Fahrerlaubnisverordnung

Im August 1998 ist die neue Verordnung über die Zulassung von Personen zum Straßenverkehr und zur Änderung straßenverkehrsrechtlicher Vorschriften (Fahrerlaubnisverordnung)[68] in Kraft getreten. Entgegen den unter der Mitwirkung des Bundesbeauftragten für den Datenschutz im Regierungsentwurf enthaltenen Regelungen wurden aufgrund des Beschlusses des Bundesrates vom 19.06.1998 datenschutzrechtlich bedenkliche Änderungen vorgenommen. Es handelt sich hierbei um § 11 Abs. 6 Sätze 2 und 4 der Verordnung. Die im Mitwirkungsverfahren einver-

nehmlich festgelegte Ergänzung des Satzes 2, dass der Betroffene vor Übersendung der Fahrerlaubnisunterlagen an eine Gutachterstelle die Unterlagen einsehen kann, ist entfallen, so dass ein Hinweis auf die Akteneinsichtsrechte der Betroffenen fehlt. Satz 4 der Verordnung enthält die Regelung zur Übersendung vollständiger Unterlagen von der Fahrerlaubnisbehörde an die untersuchenden Stellen. Der Regierungsentwurf hielt statt dessen eine Übermittlung der erforderlichen Unterlagen für ausreichend. Der Verordnungsgeber hat den Umfang der zu ermittelnden Daten erweitert, obwohl der Gesetzgeber in § 2 Abs. 14 Satz 1 Straßenverkehrsgesetz die Übersendung auf die für die Aufgabenerfüllung benötigten Daten beschränkt. Der Bundesbeauftragte für den Datenschutz ist bereits für eine entsprechende Änderung der Verordnung eingetreten. Wie unsere Kollegen in den anderen Bundesländern haben wir das zuständige Ministerium für Stadtentwicklung, Wohnen und Verkehr gebeten, sicherzustellen, dass die Fahrerlaubnisbehörden regelmäßig Akteneinsicht anbieten und nur die erforderlichen Fahrerlaubnisunterlagen an die Gutachterstellen übersenden.

- Antrag auf Erteilung einer Fahrerlaubnis für Kraftfahrzeuge

In Anbetracht der zu erwartenden Gesetzesänderungen wurde Anfang 1997 in Zusammenarbeit mit dem Ministerium für Stadtentwicklung, Wohnen und Verkehr bereits Einvernehmen über die datenschutzgerechte Formulargestaltung eines Antrages auf Erteilung einer Fahrerlaubnis hergestellt. Ende 1998 setzte uns das Ministerium über die neugestalteten, der Rechtsänderung angepassten Antragsformulare in Kenntnis. Entgegen der Absprachen wurde dem Aufklärungsgebot der §§ 12 Abs. 3, 4 Abs. 2 Brandenburgisches Datenschutzgesetz a. F. nicht entsprochen. Beispielsweise fehlte bei den Hinweisen zur Datenverarbeitung eine drucktechnische Hervorhebung.

Als nicht unerheblichen Eingriff in das informationelle Selbstbestimmungsrecht werten wir den Umstand, dass die Frage nach dem "derzeitigen Gesundheitszustand", deren Beantwortung dem Betroffenen freigestellt ist, nicht als solche gekennzeichnet wurde. Um dem Betroffenen die Freiwilligkeit der Beantwortung dieser Frage zu verdeutlichen hätte sich angeboten, darauf entweder am Anfang des Erhebungsbogens hinzuweisen, damit der Betroffene von vornherein freiwillige Angaben als solche erkennen kann oder einen entsprechenden Hinweis mit der Frage selbst zu verbinden bzw. in einer Fußnote gut sichtbar aufzunehmen.

Nach der zweiten Änderung des Brandenburgischen Datenschutzgesetzes ist die Verarbeitung von Gesundheitsdaten, soweit sie nicht bereichsspezifisch geregelt ist, sogar nur noch dann zulässig, wenn der Betroffene ausdrücklich eingewilligt hat (vgl. § 4 a BbgDSG n. F.). Diese Vorschrift sollte vor allem bei künftig neu zu gestaltenden Formularvordrucken Beachtung finden.

10.2 Wohnen

Prüfung des Jahreseinkommens im Rahmen eines Wohngeldantrages

Um einen Wohngeldantrag bearbeiten zu können, verlangte die zuständige Behörde vom Antragsteller Unterlagen, aus denen sein Einkommen hervorgeht. Der Petent übte eine private Lehrtätigkeit aus und war sich aus Gründen der Diskretion nicht sicher, ob er der Wohngeldstelle Unterrichtsvertragskopien, auf denen neben den Konditionen auch die Adressen und Telefonnummern der Schüler vermerkt waren, zur Verfügung stellen darf.

In diesem Fall konnten wir dem Antragsteller mitteilen, dass § 25 Wohngeldgesetz (WoGG) i. V. m. § 60 Abs. 1 Nr. 1 Erstes Buch Sozialgesetzbuch (SGB I) die Auskunftspflicht begründen. Nach § 25 Abs. 1 WoGG besteht die Verpflichtung, wenn und soweit die Durchführung des Gesetzes es erfordert, der zuständigen Stelle Auskunft über die Einnahmen und über andere für das Wohngeld maßgebende Umstände zu geben. Die Auskunftspflicht über die Einnahmen ist insoweit erforderlich, als die Behörde nach § 11 WoGG das Jahreseinkommen zu ermitteln hat, um Art und Umfang des Wohngeldanspruchs zu prüfen.

Wer Sozialleistungen beantragt oder erhält, hat nach dem Sozialgesetzbuch alle Tatsachen anzugeben, die für die Leistung erheblich sind. Die Angabe der wirtschaftlichen Verhältnisse ist für die Leistung nach dem Wohngeldgesetz eine erhebliche Tatsache, weil die Behörde ohne deren Vorliegen den Anspruch auf Wohngeld nicht prüfen kann.

Nach § 60 Abs. 1 Nr. 3 SGB I besteht eine Beweismittelbezeichnungspflicht. Welcher Beweismittel sich die Behörde bedienen möchte, entscheidet sie gem. § 21 Zehntes Buch Sozialgesetzbuch (SGB X) nach pflichtgemäßem Ermessen. Auf Verlangen des zuständigen Leistungsträgers sind Beweisurkunden vorzulegen.

Die angeforderten Unterrichtsvertragskopien müssen, um als Beweismittel Verwendung zu finden, die Vertragspartner sowie die Konditionen erkennen lassen. Sollten die Schüler bzw. deren Erziehungsberechtigte direkt Vertragspartner sein, ist eine Unkenntlichmachung ihrer Namen nicht möglich, weil die Behörde imstande sein muss nachzuvollziehen, von wem die Einnahmen bezogen werden. Anders verhält es sich, wenn die Lehrtätigkeit an einer Einrichtung unterrichtet wird; in diesem Fall ist die Unkenntlichmachung von Namen und Telefonnummern der Schüler geboten. Das Wohngeldamt ist im Regelfall nicht berechtigt, hinter dem Rücken des Antragstellers bei den Schülern oder deren Eltern rückzufragen und damit den Umstand offenzulegen, dass Wohngeld beantragt wurde.

Im Rahmen der Prüfung eines Wohngeldantrages sind für die Ermittlung des Jahreseinkommens alle erforderlichen Auskünfte zu erteilen, so auch die Einnahmen aus privater Lehrtätigkeit. Auf Verlangen des Leistungsträgers sind Beweisurkunden mit personenbezogenen Daten der Schüler vorzulegen, soweit dies zur Einkommensermittlung erforderlich ist. Dieses Erfordernis besteht nicht, wenn der Antragsteller in einer Einrichtung unterrichtet.

11. Umwelt, Naturschutz und Raumordnung

Änderungen beim Immissionsschutz

Im Rahmen der Umsetzung der EG-Richtlinie[69] zur Beherrschung der Gefahren bei schweren Unfällen mit gefährlichen Stoffen ("SEVESO II-Richtlinie") beabsichtigt das Ministerium für Umwelt, Naturschutz und Raumordnung, das Vorschaltgesetz zum Immissionsschutz zu novellieren. Der Gesetzentwurf enthält eine Neufassung der Datenverarbeitungsvorschrift, wobei Anpassungen an das Brandenburgische Datenschutzgesetz und das Brandenburgische Abfallgesetz vorgesehen sind. Besonders begrüßt haben wir das Bestreben, zur regelungstechnischen Vereinfachung und zur Eindämmung von Normenflut die speziellen Regelungen für den Immissionsschutz und die Abfallwirtschaft über die Anpassung der Verordnungsermächtigung zusammenzuführen. Das Gesetzgebungsverfahren ist noch nicht abgeschlossen und auch die Erarbeitung einer entsprechenden Datenschutzverordnung bleibt abzuwarten.

Der Gesetzentwurf regelt auch Aspekte des Informationszugangs[70].

12. Bürgerbüros und Bürgerämter

Immer mehr setzt sich die Erkenntnis durch, dass Gemeinden und Ämter als Dienstleister näher an die Bürger heranrücken müssen. Die Kommunen wollen sich dem nicht entziehen und suchen deshalb nach Wegen, diesem Bedürfnis entsprechen zu können.

Die Gemeinden sehen sich derzeit zusätzlich in der finanziellen Zwangssituation, ihre Ausgaben reduzieren zu müssen. Dies geschieht häufig durch das Zusammenlegen von Verwaltungstätigkeiten, und zwar sowohl funktionell als auch räumlich. Die zunehmend gute Ausstattung der Gemeindeverwaltungen mit Geräten zur elektronischen Datenverarbeitung lässt beides zu. Der Anforderung, Ausgaben zu reduzieren und dennoch zu größerer Bürgernähe zu gelangen, kann jedenfalls durch die Einrichtung von Bürgerbüros oder Bürgerämtern entsprochen werden. Die Begriffe "Bürgerbüro" und "Bürgeramt" werden hier ohne Unterscheidung benutzt.

Aus der Sicht des Bürgers liegt die größere Bürgernähe im Folgenden: er hat nur einen statt mehrerer Gesprächspartner, und er kann sein Anliegen möglichst zu einem einzigen Zeitpunkt und an einem einzigen Platz erledigen bzw. erledigen lassen. Der Bürger spart auf diese Weise Zeit. Nicht mehr die Bürger, sondern die Akten "laufen" von Behörde zu Behörde.

Aus der Sicht der Verwaltung lässt sich ein Bürgeramt am leichtesten dadurch verwirklichen, dass es in einem Großraumbüro untergebracht wird: so wird Raum eingespart, die ungemütlichen Flure werden überflüssig, die Kommunikation untereinander wird erleichtert. Der Appell an den Bürger, der Dienste und Rat sucht, ist augenfällig: hier sind an einem Ort, in einem Raum gleich mehrere Bedienstete, die alle technisch gut ausgestattet sind und die mit Kompetenz und Fleiß ihre Aufgaben - die dem Bürger dienen - in kürzester Zeit erledigen.

Aus der Sicht des Datenschutzes ist ebenso leicht nachzuvollziehen, dass es in diesem Ambiente besonderer Vorkehrungen bedarf, um das Recht auf informationelle Selbstbestimmung, das der einzelne Bürger ja nicht vor dem Großraumbüro aufgibt, ebenso zu berücksichtigen wie die Ansprüche an Kompetenz und Schnelligkeit, die er an die Mitarbeiter des Bürgeramtes stellt. Die Umsetzung des Datenschutzgedankens steht vielem von dem, was das Bürgerbüro so attraktiv macht, geradezu konträr gegenüber. Die größere Nähe der Arbeitsplätze der Gemeindebediensteten zueinander hat unvermeidlich auch eine größere Nähe der gerade anwesenden Bürger zueinander zur Folge: das Mit-Hören und Mit-Sehen dessen, was an den Nachbararbeitsplätzen geschieht, ist kaum zu vermeiden, wenn keine besonderen Maßnahmen getroffen werden.

Zudem ergibt sich in jedem Bürgerbüro aus der Forderung des Bundesverfassungsgerichts, Behördentätigkeiten und -leistungen nach Funktionen zu trennen[71] ein grundsätzliches Problem. Das Gericht hat aus dem Recht auf informationelle Selbstbestimmung das Gebot der informationellen Gewaltenteilung abgeleitet, das zugleich auch der Zweckbindung bei der Verarbeitung personenbezogener Daten dient: Daten, die eine Behörde beim Bürger zu einem bestimmten Zweck erhebt, darf sie nicht ohne weiteres für andere Zwecke oder in einer anderen Funktion weiterverarbeiten. Auch die Stadtverwaltung ist keine einheitliche, allwissende Behörde, sondern besteht aus einer Vielzahl funktional getrennter Behörden. Diese Funktionstrennung dient der Sicherung des Grundrechts auf informationelle Selbstbestimmung, und folglich kann auch nur der Bürger als Grundrechtsträger durch seine informierte Einwilligung eine Aufhebung der Funktionentrennung ermöglichen, wenn er die Vorzüge des Bürgerbüros nutzen will.

Das bedeutet zum einen, dass den Menschen, die ein Bürgerbüro aufsuchen, zumindest bei der Verarbeitung besonders sensibler Daten (z. B. Sozialhilfeangelegenheiten) weiterhin zusätzlich die Möglichkeit geboten werden muss, ihre Anliegen in dem jeweils ursprünglich zuständigen Amt erledigen zu lassen. Auf diese Möglichkeit müssen alle Personen, die ein Bürgeramt aufsuchen, deutlich hingewiesen werden; Nachteile dürfen ihnen daraus nicht erwachsen. Zum anderen wäre es mittelfristig aus der Sicht des Datenschutzes wünschenswert, wenn der Bürger auch die technischen Mittel an die Hand bekäme, um selbst nach Einsichtnahme in die zu seiner Person gespeicherten Daten (z. B. an einem abgesetzten Bildschirm) den Zugriff auf die funktional getrennten Dateien für den Sachbearbeiter im Bürgerbüro zu eröffnen. Dazu könnte er eine persönliche Chipkarte nutzen, mit der er "seine Daten" stets lesen kann.

Einige der Stadtverwaltungen, die im Land Brandenburg bereits ein Bürgerbüro eingerichtet haben, haben von sich aus unseren Rat gesucht. Daneben haben sich aber auch Bürger mit Eingaben zu datenschutzrechtlich problematischen Aspekten dieser neuen Verwaltungsform an uns gewandt. Aus den Erfahrungen, die wir im Zusammenhang mit Bürgerämtern gemacht haben, seien hier die Maßnahmen aufgeführt, die grundsätzlich zu beachten sind,

1. Das Mithören vermeiden

Vorgänge, derentwegen der Bürger in ein Bürgerbüro kommt, sind grundsätzlich die gleichen, die er bisher im Rathaus hat erledigen lassen, dort meist in einer Einzelgesprächssituation mit dem sachbearbeitenden Bediensteten, z. B. eine Zuzugsmeldung. Geht es um die Erledigung eines vergleichbaren Vorgangs im Großraumbüro, kann von anderen Arbeitsplätzen aus mitgehört werden, was der Bürger dem Verwaltungsbediensteten mitteilt. Selbst dann, wenn ein Anmeldeformular bereits vorher ausgefüllt worden war, werden üblicherweise noch etliche Angaben besprochen.

Je weiter Arbeitsplätze voneinander entfernt stehen, umso weniger kann mitgehört werden. Trennwände vermindern die Wort- und Geräuschübertragung und damit das Mithören.

Das Einrichten einer Warteabteilung oder eines Warteraumes oder -vorraumes für diejenigen, die noch nicht an einem "Schalterplatz" bedient werden, ist unverzichtbar. Gerade der Warteraum muss im Verhältnis zu den Arbeitsplätzen räumlich so angeordnet sein, dass Mithören durch Wartende soweit irgend möglich ausgeschlossen ist.

2. Das Mit-Sehen vermeiden

Die Bearbeitung von Vorgängen in einem Bürgerbüro erfolgt regelmäßig auf einem PC mit Bildschirm. Um Mit-Sehen durch Dritte möglichst auszuschließen sollten die Bildschirme nicht in einer Reihe, sondern gestaffelt oder als völlige Einzelplätze angeordnet werden. Damit lässt sich im Übrigen auch leichter vermeiden, dass Dritte mithören.

3. Den Zugriff auf Daten verhindern

Die Frage des Zugriffs auf Daten stellt sich in erster Linie in Bezug auf die sachbearbeitende Person, die den Bürger gerade bedient. Da die PC´s in Bürgerbüros so geschaltet sind, dass von jedem einzelnen Bildschirm-Arbeitsplatz aus auf den gesamten Datenbestand zugegriffen werden kann, der irgendeinem der zugelassenen Bearbeitungsfelder zuzurechnen ist, muss die Zugriffsmöglichkeit jeweils auf das zur jeweiligen Aufgabenerledigung unbedingt Erforderliche eingegrenzt werden. Durch die Verwendung von Masken kann der Zugriff - unabhängig von der zugreifenden Person - begrenzt werden.

4. Die Anforderungen an den Datenschutz bewusst machen

Als weitere Forderung zum Datenschutz ist zu beachten, dass die sachbearbeitenden, aber auch alle anderen in dem Großraumbüro tätigen Personen ihren Aufgabenbereich kennen und durch eine geeignete Dienstanweisung auf ihr Verhalten und ihre Pflichten hingewiesen und in Datenschutzfragen qualifiziert werden.

5. Erforderliche technisch-organisatorische Maßnahmen treffen

Die im Brandenburgischen Datenschutzgesetz genannten technisch-organisatorischen Maßnahmen sind zu ergreifen. Dazu gehört auch, dass die Bearbeitungsvorgänge präzise protokolliert werden.

6. Bei Bürgeraktivitäten den Datenschutz ermöglichen

Sofern Bürgern die Gelegenheit gegeben werden soll, "vorbereitend" tätig zu werden, z. B. Formulare auszufüllen, müssen sie dies so erledigen können, dass keine andere Person zuschaut und erkennen kann, was eingetragen wird. Im Warteraum sollte es deshalb abgesonderte Schreibtischplätze oder Schreibpulte geben sollte, an denen die betreffende Person unbeobachtet schreiben kann.

7. Sensible Daten besonders schützen

Bei der Organisation des Bürgeramtes muss schon bei der Aufgabenzuweisung bedacht werden, welche Aufgaben dort überhaupt zulässigerweise bewältigt werden dürfen. Vor allem sind alle Bearbeitungsvorgänge, die Sozialdaten betreffen, grundsätzlich zur Bearbeitung im einem Großraumbüro nicht geeignet. Sollen dennoch Aufgaben nach dem Sozialgesetzbuch in einem Bürgeramt erfüllt werden, so kann dies nur durch speziell in diesem Bereich tätige Mitarbeiter und unter Wahrung größtmöglicher Diskretion (z. B. in einem gesonderten Beratungsraum) erfolgen.

Die Schritte, die wir hier und gegenüber denjenigen, die ein Bürgerbüro eingerichtet haben, vorgeschlagen haben, sind vielfach auch von betroffenen Bürgern eingefordert worden. Aus Eingaben wissen wir, wie unangenehm es Betroffenen ist, wenn andere mithören können. Anders formuliert: Bürgerbüros, in denen die Abstände der Arbeitsplätze zu gering gewählt worden sind, sind Stellen, die ungern aufgesucht werden; Bürgerbüros, in denen nicht sorgfältig darauf geachtet wird, dass Informationen aus dem Sozialbereich in einem Großraumbüro nichts zu suchen haben, werden gemieden.

Trotz der beschriebenen Datenschutzprobleme unterstützen wir die Einrichtung von Bürgerbüros.

Bürgerbüros können durchaus datenschutzgerecht gestaltet werden, wenn unsere Empfehlungen beachtet werden.

Teil B

Akteneinsicht und Informationszugang

Dies ist der erste Bericht, den der Landesbeauftragte für das Recht auf Akteneinsicht nach § 11 Abs. 3 des Akteneinsichts- und Informationszugangsgesetzes[72] vorlegt. Es ist zugleich der erste Bericht eines Informationszugangsbeauftragten in der Bundesrepublik Deutschland. Das Brandenburgische Akteneinsichts- und Informationszugangsgesetz muss dabei in einen größeren Zusammenhang gestellt werden, denn es ist sowohl die einfachgesetzliche Ausformung des Grundrechts auf Informationszugang nach Artikel 21 Abs. 3 und 4 der Landesverfassung als auch das Ergebnis einer Rechtsentwicklung in der Europäischen Union und in anderen europäischen und außereuropäischen Staaten. Diese Entwicklung wird auch das brandenburgische Landesrecht weiter beeinflussen. Das in der Bundesrepublik einmalige Brandenburgische Informationszugangsgesetz wird - voraussichtlich - seinerseits die Rechtsentwicklung in der Bundesrepublik beeinflussen.

1. Entwicklung des Informationszugangsrechts

1.1 Europa

Mit dem Vertrag von Amsterdam, dessen In-Kraft-Treten in diesem Jahr zu erwarten ist, wird jedem Unionsbürger und jeder Person mit Wohnsitz in einem Mitgliedstaat das grundsätzliche Recht auf Zugang zu Dokumenten des Europäischen Parlaments, des Ministerrats und der Kommission zuerkannt[73]. Dies stellt nach dem Willen der Mitgliedstaaten eine "neue Stufe bei der Verwirklichung einer immer engeren Union der Völker Europas dar, in der die Entscheidungen möglichst offen und möglichst bürgernah getroffen werden"[74]. Das Recht des Einzelnen auf Information wird auch im europäischen Zusammenhang als ein demokratisches Recht angesehen, das einer der Ecksteine einer bürgernahen Gemeinschaft ist[75]. Dementsprechend gewährleistet die Verfassung des Landes Brandenburg für jeden das Recht auf politische Mitgestaltung (Artikel 21 Abs. 1) und in diesem Zusammenhang das Recht auf Information und Akteneinsicht (Artikel 21 Abs. 3 und 4). Letztlich sind diese Grundrechte Voraussetzung dafür, dass das Volk Träger der Staatsgewalt ist (Artikel 2 Abs. 2 der Landesverfassung).

Der Europäische Bürgerbeauftragte (Ombudsman), Jacob Söderman, hat in einem Sonderbericht an das Europäische Parlament die Regeln untersucht, die von den

Institutionen der Europäischen Gemeinschaft über den Zugang zu Verwaltungsdokumenten erlassen wurden und festgestellt, dass diese Regeln keinen Anspruch des Bürgers auf Informationszugang enthalten. Er hat darüber hinaus bemängelt, dass die Institutionen der Gemeinschaft sich bisher nicht zur Erstellung von Dokumentenverzeichnissen verpflichtet haben, obwohl dies sowohl den Bürgern die Wahrnehmung des Zugangsrechts erleichtern als auch eine ordnungsgemäße Verwaltung unter Verhinderung des Dokumentenverlusts fördern könnte[76]. Der Europäische Bürgerbeauftragte hat die Organe der Europäischen Gemeinschaft aufgefordert, ihre Regeln zum Informationszugang zu veröffentlichen und Dokumentenverzeichnisse zu erstellen, die ebenfalls der Öffentlichkeit zugänglich gemacht werden sollten. Mit Recht hat der Bürgerbeauftragte darauf hingewiesen, dass ein Informationszugangsrecht für den Bürger wenig Sinn macht, solange dieser von der Existenz der Dokumente oder zumindest bestimmter Dokumentarten keine Kenntnis hat.

Dieses grundsätzliche Dilemma jedes Informationszugangsrechts besteht auch in Brandenburg. Das Akteneinsichts- und Informationszugangsgesetz und die zugrundeliegenden Grundrechte der Landesverfassung würden allerdings missverstanden, wenn die Verwaltung sich darauf beschränken würde, Anträge der Bürger auf Akteneinsicht und Informationszugang abzuwarten und positiv oder negativ zu bescheiden. Vielmehr sollten die Behörden auf Landes- und Kommunalebene selbst die Initiative ergreifen und über die bisherige Öffentlichkeitsarbeit hinaus grundsätzlich alle bisher nicht publizierten verwaltungsinternen Regelungen wie Verwaltungsvorschriften und Runderlasse auch unter Nutzung des Internets der Öffentlichkeit zugänglich machen. Darüber hinaus sollten die Behörden auch die Struktur ihrer Informationsbestände dadurch offenlegen, dass sie ihre Aktenpläne publizieren. Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht veröffentlicht deshalb erstmals seinen Aktenplan in diesem Tätigkeitsbericht[77].

Das Europäische Parlament hat in seiner Entschließung zum Sonderbericht des Europäischen Bürgerbeauftragten unterstrichen, dass in allen Institutionen der Gemeinschaft öffentliche Dokumentenregister unter verstärkter Nutzung des Internets geschaffen werden sollten[78].

Neben dem allgemeinen Informationszugangsrecht, das demnächst allen Unionsbürgern gegenüber den Institutionen der Gemeinschaft zustehen wird, enthält das Europäische Gemeinschaftsrecht auch bereichsspezifische Informationsrechte. Dies betrifft vor allem den Umweltbereich, für den die Richtlinie über den freien Zugang zu Informationen über die Umwelt[79] die Mitgliedstaaten zur Angleichung ihrer Rechtsordnungen verpflichtet hat. Die Europäische Kommission hat angekündigt, dass diese Richtlinie mit dem Ziel überarbeitet werden soll, die Rechte der Bürger auf freien Zugang zu Informationen über die Umwelt zu verbessern[80]. Die Kommission hat außerdem vorgeschlagen, dass die Gemeinschaft das Übereinkommen der UN-Wirtschaftskommission für Europa über den Zugang zu Informationen, die Öffentlich-

keitsbeteiligung an Entscheidungsverfahren und den Zugang zu Gerichten in Umweltangelegenheiten unterzeichnen solle. Diese sogenannte Aarhus-Konvention vom Juni 1998 ist gegenwärtig noch nicht in Kraft getreten, aber kurz vor Ende des Berichtszeitraums auch von der Bundesregierung unterzeichnet worden. Das ist deshalb bedeutsam, weil die Aarhus-Konvention die Vertragsparteien z. B. dazu verpflichtet, der Öffentlichkeit auf Antrag Informationen über die Umwelt spätestens innerhalb eines Monats nach Antragstellung zugänglich zu machen[81]. In diesem und anderen Punkten wird das Umweltinformationsgesetz des Bundes, das zur Umsetzung der Europäischen Umweltinformationsrichtlinie verabschiedet wurde und bisher keine Fristen für den Informationszugang enthält, zugunsten der Bürger verbessert werden müssen. Ein vergleichbares Problem stellt sich bei der Anwendung des Brandenburgischen Akteneinsichts- und Informationszugangsgesetzes, das den Behörden bisher ebenfalls keine Frist für Entscheidung über die Akteneinsicht setzt[82].

1.2 Bund

Auf Bundesebene wie auch in allen anderen Bundesländern außer in Brandenburg gibt es bisher keine allgemeine Informationszugangsgesetzgebung. Möglicherweise wird es auf Bundesebene aber eine entsprechende Gesetzesinitiative gebe, wenn die Koalitionsvereinbarung zwischen der Sozialdemokratischen Partei Deutschlands und Bündnis 90/Die Grünen vom 20.10.1998 in diesem Punkt umgesetzt wird. Dort heißt es: "Durch ein Informationsfreiheitsgesetz wollen wir unter Berücksichtigung des Datenschutzes den Bürgerinnen und Bürgern Informationszugangsrechte verschaffen"[83]. Damit besteht die Chance, dass Informationszugangsrechte nicht nur gegen Behörden in Brandenburg, sondern auch auf Bundesebene durchgesetzt werden können. Die in Brandenburg gesammelten Erfahrungen werden bei dem bevorstehenden Gesetzgebungsverfahren zu berücksichtigen sein.

Das Umweltinformationsgesetz des Bundes, das dem brandenburgischen Landesrecht in diesem speziellen Bereich vorgeht, ist vom Europäischen Gerichtshof im vergangenen Jahr in zwei Punkten korrigiert worden[84]: Der Begriff der Umweltinformation, die nach der entsprechenden EG-Richtlinie frei zugänglich sein muss, ist weit auszulegen. Er umfasst auch Stellungnahmen von Behörden in einem Planfeststellungsverfahren mit Umweltbezug. Zum anderen ist die Ausnahme vom Informationsrecht der Öffentlichkeit, die das Umweltinformationsgesetz bisher während "verwaltungsbehördlicher Verfahren" vorsieht, eng, d. h. zu Gunsten der Öffentlichkeit, auszulegen. Der Informationszugang kann dementsprechend nicht pauschal dann verwehrt werden, wenn die Verwaltung einen Verwaltungsakt vorbereitet oder bereits erlassen hat und über einen Widerspruch hiergegen zu entscheiden hat. Dies könnte auch Konsequenzen für die Auslegung des Akteneinsichts- und Informationszugangsgesetzes haben, dass seinerseits eine sehr weit gefasste Ausnahme für "laufende Verfahren" enthält (§ 2 Abs. 5 AIG). Eine unterschiedliche Einschränkung des Anspruchs auf Zugang zu Umweltinformationen und des allgemeinen Informationszugangsanspruchs, die in Branden-

burg beide Verfassungsrang haben[85], ist nicht gerechtfertigt.

Außerdem muss sich die Bundesrepublik gegenwärtig noch in einem Vertragsverletzungsverfahren vor dem Europäischen Gerichtshof verantworten, das die Kommission wegen mangelhafter Umsetzung der EG-Umweltinformationsrichtlinie in einem anderen Punkt angestrengt hat: Die Kommission bemängelt die Höhe der Gebühren, die für Amtshandlungen nach dem Umweltinformationsgesetz erhoben werden können[86]. Eine Entscheidung in diesem Verfahren steht noch aus. Beobachter erwarten allerdings, dass auch in diesem Punkt das deutsche Recht mit europäischen Gemeinschaftsrecht nicht übereinstimmt. Es bleibt abzuwarten, ob der Europäische Gerichtshof sich nur zur zulässigen Höhe der Gebühr äußern wird (nach Bundesrecht bis zum 10.000,- DM; nach der Brandenburgischen Umweltinformationsgebührenordnung bis zu 200,- DM) oder ob er die Gebührenpflicht des Informationszugangs grundsätzlich einschränken wird. Diese Entscheidung wird auch bei der Anwendung des Akteneinsichts- und Informationszugangsgesetzes zu berücksichtigen sein, das eine Bemessung der Gebühren für Amtshandlungen in der Weise vorschreibt, dass zwischen dem Verwaltungsaufwand einerseits und dem Recht auf Akteneinsicht andererseits ein angemessenes Verhältnis besteht (§ 10 Abs. 1 Satz 2 AIG)[87].

1.3 Land Brandenburg

1.3.1 Wie ist das Akteneinsichts- und Informationszugangsgesetz auszulegen?

Das am 20. März 1998 in Kraft getretene Akteneinsichts- und Informationszugangsgesetz (AIG)[88] enthält zahlreiche unbestimmte Rechtsbegriffe, Ermessensspielräume und abschreckend lange Ausnahmekataloge vom Grundsatz des Informationszugangs für alle. Dies darf jedoch nicht den Blick dafür verstellen, dass dieses Gesetz die Landesverfassung und darin insbesondere das Grundrecht auf Information für einzelne Bürger, Bürgerinitiativen und Verbände (Artikel 21 Abs. 3 und 4) konkretisiert.

Das Gesetz ist deshalb stets so auszulegen, dass diesen Grundrechten die größtmögliche Wirkung zukommt. Alle Auslegungsspielräume sind verfassungskonform im Lichte dieser Grundrechte zu Gunsten der Bürger auszuschöpfen. Ermessensspielräume ("die Akteneinsicht kann gewährt werden, soweit ...") sind - juristisch gesprochen - in aller Regel auf Null reduziert, d. h. sie werden von "Kann"- zu "Muss"-Vorschriften, soweit die gesetzlichen Voraussetzungen vorliegen. Alle Ausnahmetatbestände des AIG sind vor dem Hintergrund des Grundrechts auf Informationszugang einschränkend zu Gunsten der Antragsteller auszulegen.

Allerdings findet das Grundrecht auf Informationszugang seine Grenzen im Grundrecht auf Datenschutz, das sich ebenfalls im Ausnahmekatalog des AIG findet (§ 5 Abs. 2 Nr. 1). In diesem Fall sind die beiden sich gegenüberstehenden Grund-

rechtsverbürgerungen zu einem Ausgleich zu bringen, für den der Gesetzgeber bereits bestimmte Vorgaben gemacht hat. So dürfen personenbezogene Daten im Rahmen der Akteneinsicht in der Regel nur mit Zustimmung des Betroffenen offenbart werden, ausnahmsweise aber auch dann, wenn sie aus allgemein zugänglichen Quellen entnommen werden können und schutzwürdige Belange des Betroffenen nicht entgegenstehen oder wenn auf Grund besonderer Umstände des Einzelfalls im Hinblick auf den Zweck der politischen Mitgestaltung das Interesse am Informationszugang gegenüber dem Interesse an der vertraulichen Behandlung überwiegt (§ 5 Abs. 2 Nr. 2 und 3 AIG). Schließlich müssen auch Amtsträger, die an Verwaltungsvorgängen mitwirken, die Offenbarung bestimmter personenbezogener Daten im Rahmen der Akteneinsicht regelmäßig hinnehmen, es sei denn, ihre schutzwürdigen Belange stehen der Offenbarung entgegen (§ 5 Abs. 3 AIG).

Entscheidend ist bei der Anwendung des Akteneinsichts- und Informationszugangsgesetzes, das alle Rechtsanwender sich dessen bewusst sind, dass dieses Gesetz die Ausübung von Grundrechten ermöglichen soll, die ihrerseits eine zentrale Voraussetzung für das demokratische Recht auf politische Mitgestaltung (Artikel 21 Abs. 1 Landesverfassung) sind.

Das Ministerium des Innern hat zunächst davon abgesehen, allgemeine Verwaltungsvorschriften zur Durchführung des Akteneinsichts- und Informationszugangsgesetzes zu erlassen, und hat statt dessen "erste Hinweise zur Anwendung" dieses Gesetzes im September 1998 veröffentlicht[89]. Diese Hinweise richten sich in erster Linie an die Mitarbeiter in den Landes- und Kommunalverwaltungen, nicht an die Bürger. Ein Teil unserer Anregungen zu einem ersten Entwurf allgemeiner Verwaltungsvorschriften[90] sind in die "ersten Hinweise" übernommen werden. Sobald etwas mehr Erfahrungen mit der praktischen Anwendung des AIG vorliegen, sollten die ursprünglich geplanten allgemeinen Verwaltungsvorschriften ergänzt und erlassen werden.

Wir schließen nicht aus, dass das AIG selbst vom Gesetzgeber geändert werden muss, wenn sich zeigt, das die oben entwickelten Grundsätze für eine verfassungskonforme Auslegung dieses Gesetzes nicht hinreichend berücksichtigt werden oder eine verfassungskonforme Informationszugangspraxis durch Auslegung allein nicht zu erreichen ist.

1.3.2 Der Kostenfaktor

Für die Praxis des Informationszugangsrechts wird viel davon abhängen, was es den Bürger kosten wird, von seinem Grundrecht Gebrauch zu machen. Das AIG ermächtigt die Landesregierung, im Benehmen mit dem Innenausschuss des Landtages eine entsprechende Gebührenordnung zu erlassen (§ 10 Abs. 2). Dies ist bisher nicht geschehen. Uns liegt zwar seit September 1998 ein erster Entwurf dieser Gebührenordnung vor, der aber innerhalb der Landesregierung noch nicht endgültig abgestimmt ist. Uneinigkeit herrscht offenbar über die gesetzliche Vorgabe, die Gebühren so zu bemessen, das zwischen dem Verwaltungsaufwand einerseits und dem Recht auf

Akteneinsicht andererseits ein angemessenes Verhältnis besteht (§ 10 Abs. 1 Satz 2 AIG). Diese Regelung schließt die Erhebung einer kostendeckenden Gebühr aus. Jede Gebührenordnung, die die Akteneinsicht mit prohibitiven, abschreckenden Kosten belasten würde, wäre mit dem Gesetz unvereinbar und hätte auch vor der Verfassung keinen Bestand.

Möglicherweise wird dieses Problem durch die technische Entwicklung wenn nicht gelöst, so doch etwas entschärft. Ein Mitglied der Landesregierung wies vor Kurzem im Innenausschuss des Landtages sinngemäß zu Recht darauf hin, das Akteneinsicht zu vertretbaren Kosten nur elektronisch realisiert werden könne[91]. In dem Maße, wie Akteneinsicht elektronisch z. B. über das Internet gewährt werden kann, sinken die Kosten der Übermittlung. Allerdings ist dies von zahlreichen rechtlichen und organisatorischen Voraussetzungen abhängig, die noch nicht geschaffen sind[92].

In jedem Fall muss eine verfassungskonforme Gebührenregelung für den konventionellen Informationszugang in der öffentlichen Verwaltung getroffen werden.

1.3.3 Öffentlichkeitsbeteiligung beim Katastrophenschutz

Die Landesregierung bereitet mit dem Entwurf eines Gesetzes zur Änderung des Brandenburgischen Katastrophenschutzgesetzes und des Landesimmissionsschutzgesetzes die Umsetzung der sogenannten SEVESO II-Richtlinie[93] der Europäischen Gemeinschaft vor, die Konsequenzen aus der Umweltkatastrophe von Seveso zieht. Das Ministerium des Innern hat uns den entsprechenden Gesetzentwurf zur Stellungnahme zugeleitet[94]. Wir haben darauf hingewiesen, dass der ursprüngliche Entwurf die Vorgaben der Richtlinie insofern nur unvollständig umsetzte, als eine Beteiligung der Öffentlichkeit nur bei der erstmaligen Aufstellung von externen Notfallplänen vorgesehen war. Die Öffentlichkeit muss aber auch bei der regelmäßig erforderlichen Überarbeitung dieser Notfallpläne von den Katastrophenschutzbehörden durch öffentliche Auslegung beteiligt werden. Auch sind bei der Aufstellung interner Notfallpläne (betriebliche Alarm- und Gefahrenabwehrpläne) die Beschäftigten des jeweiligen Betriebes zu beteiligen. Aufgrund unserer Hinweise wurde der Gesetzentwurf, über den die Landesregierung bisher nicht beschlossen hat, entsprechend ergänzt. Die geheimhaltungsbedürftigen Teile der externen Notfallpläne, insbesondere dem Datenschutz unterliegende personenbezogene Angaben, Betriebs- und Geschäftsgeheimnisse, verdeckte Telefonnummern oder interne Anweisungen sind nicht auszulegen.

2. Erste praktische Erfahrungen mit dem Akteneinsichts- und Informationszugangsgesetz

Die während des Gesetzgebungsverfahrens vielfach geäußerten Befürchtungen, das AIG würde den Wirtschaftsstandort Brandenburg gefährden und die Verwaltung lahmlegen, haben sich bisher als unbegründet erwiesen. Die Behörden auf Landes- und Kommunalebene haben sich zum Teil selbständig, zum Teil auf Grund unserer Beratung vielfach intensiv auf die Umsetzung des neuen Gesetzes vorbereitet. Der Leiter einer Landesbehörde zeigte sich gegenüber dem Landesbeauftragten überrascht, wie wenig Bürger bisher das Akteneinsichtsrecht genutzt hätten. Die Gründe für diese Zurückhaltung der Bürger sind nicht mit letzter Sicherheit zu ermitteln und dürften vielfältig sein. Einer der Gründe ist sicherlich die äußerst restriktive und für den juristischen Laien auch schwer verständliche Fassung des Gesetzes. Selbst für Juristen ist dieses Gesetz in der Bundesrepublik ja ein Novum, weil es das Regel-Ausnahme-Verhältnis zwischen Geheimhaltung und Informationszugang zu Gunsten des Bürgers und zu Gunsten der Transparenz umkehrt. Gerade insofern bietet das Gesetz in verfassungskonformer Auslegung aber auch Chancen, die es zu nutzen gilt.

2.1 Endlich "Einsicht in meine Akte"?

Überraschend viele Anfragen erreichten uns nach dem In-Kraft-Treten des Gesetzes, mit denen die Bürger Einsicht in Unterlagen verlangten, die bei der öffentlichen Verwaltung *zu ihrer Person* geführt wurden. Einige Petenten zeigten sich erfreut, dass dies jetzt erstmals möglich sei. In Wirklichkeit besteht dieses Recht seit In-Kraft-Treten des Brandenburgischen Datenschutzgesetzes vom Januar 1992 (§ 18) und der Verfassung des Landes Brandenburg vom August 1992 (Artikel 11). Das Auskunfts- und Akteneinsichtsrecht des Betroffenen bezüglich seiner Daten galt schon immer als Magna Charta des Datenschutzes. Dies ist den Bürgern - trotz der erheblichen Anstrengungen des Landesbeauftragten für den Datenschutz in der Vergangenheit - offenbar bisher nicht hinreichend deutlich gewesen. Dieses Missverständnis ist vermutlich auch nicht auf Brandenburg beschränkt. Mit dem Akteneinsichts- und Informationszugangsgesetz soll ein darüber hinausgehendes Grundrecht in die Praxis umgesetzt werden: Jeder kann im Grundsatz Einsicht in alle Akten und Unterlagen bei Behörden und Einrichtungen des Landes sowie bei Gemeinden und Gemeindeverbänden nehmen, auch dann, wenn diese Unterlagen keine Informationen zu seiner Person enthalten.

Einsicht in die "eigene Akte" kann der Bürger unter Hinweis auf sein Grundrecht auf Datenschutz verlangen. Das Grundrecht auf Akteneinsicht erstreckt sich darüber hinaus auf Akten, die nicht zu seiner Person geführt werden.

2.2 Akteneinsicht als Mittel zur politischen Mitgestaltung

Das Grundrecht auf Informationszugang und mit ihm das Akteneinsichts- und Informationszugangsgesetz sollen eine wesentliche Voraussetzung zur Ausübung des Rechts auf politische Mitgestaltung (Artikel 21 Abs. 1 Landesverfassung) schaffen. Dieser zentrale Zweck des neuen Gesetzes trat zum ersten Mal in den Vordergrund, als sich mehrere Bürger im Zusammenhang mit den Auseinandersetzungen um das *Potsdam-Center* ratsuchend an uns wandten. Sie wollten Einsicht in die Baugenehmigungsakten zu diesem umstrittenen Vorhaben nehmen oder hatten dies bereits versucht und waren nach ihren Angaben von der Stadtverwaltung unter Hinweis auf den Datenschutz abgewiesen worden. Der Fall warf mehrere komplizierte Fragen zur Anwendung des AIG auf, die wir jedoch letztlich nicht zu beantworten hatten, weil die Petenten ihr Anliegen offensichtlich auf Grund der zunehmend transparenteren Informationspolitik der Stadt Potsdam und des vom Minister für Stadtentwicklung, Wohnen und Verkehr einberufenen Runden Tisches zu diesem Problemkreis nicht weiter verfolgt wurden.

Festzuhalten bleibt zu diesem Fall immerhin Folgendes: Das Akteneinsichtsrecht bezieht sich auch auf Baugenehmigungsakten. Die Anwendung des Akteneinsichtsgesetzes ist auch nicht von vornherein dadurch ausgeschlossen, dass die Stadtverwaltung die Rücknahme einer bereits erteilten Baugenehmigung prüfte, denn hinsichtlich der abgeschlossenen Teile des Baugenehmigungsverfahrens ist nicht das Verwaltungsverfahrensgesetz, sondern das Akteneinsichts- und Informationszugangsgesetz anzuwenden. Die Frage, ob ein Verwaltungsverfahren läuft, während dessen das AIG nicht anzuwenden ist, muss im Einzelnen genau geprüft und differenziert entschieden werden.

Auch der Umstand, dass Amtsträger in diesen Genehmigungsverfahren mitgewirkt haben, führt in der Regel nicht dazu, das dem Bürger die Akteneinsicht unter Hinweis auf den Datenschutz der Amtsträger verwehrt werden kann. Etwas anderes gilt nur insoweit, als schutzwürdige Belange der Verwaltungsmitarbeiter der Offenbarung entgegenstehen, etwa weil auf Grund des Verhaltens eines Amtsträgers gegen diesen die Einleitung eines Disziplinarverfahrens geprüft wird, was im Fall des Potsdam-Centers nach Presseberichten der Fall war.

Schließlich darf die Akteneinsicht auch nicht unter Hinweis auf den Schutz personenbezogener Daten Dritter oder auf geheimhaltungsbedürftige Unternehmensdaten verwehrt werden, wenn das Offenbarungsinteresse des Bürgers im Hinblick auf den Zweck der politischen Mitgestaltung das Interesse der betroffenen Person oder des Unternehmens an der vertraulichen Behandlung der Information überwiegt (§ 5 Abs. 2 Nr. 3 AIG). Im Fall des umstrittenen Potsdam-Centers wären diese Voraussetzungen mit hoher Wahrscheinlichkeit gegeben, denn immerhin steht zur Debatte, ob das Bauvorhaben einen Teil des Weltkulturerbes der UNESCO beeinträchtigt.

Der Zweck der politischen Mitgestaltung kann dazu führen, dass der Datenschutz Betroffener hinter dem Informationsinteresse der Öffentlichkeit zurücktreten muss.

2.3 Der Zeitfaktor

Informationen veralten schnell. Deshalb ist es so wichtig, dass über einen Antrag auf Akteneinsicht oder Informationszugang schnell entschieden wird. Jede dilatorische Behandlung solcher Anträge kann den Grundrechtsschutz vereiteln und zur Rechtsverweigerung werden. Einer der wesentlichen Schwächen des Akteneinsichts- und Informationszugangsgesetzes besteht darin, dass es keine Vorgaben darüber enthält, wie schnell der Antrag auf Informationszugang beschieden werden muss. Es versteht sich von selbst, dass dies unverzüglich, d. h. ohne schuldhaftes Zögern zu erfolgen hat. Auch dies lässt allerdings noch einen zu weiten Spielraum. Zumindest kann der Bürger erwarten, dass die Verwaltung den Eingang seines Antrages auf Akteneinsicht innerhalb von zwei Wochen bestätigt.

Eine Bürgerinitiative begehrte beim Ministerium für Stadtentwicklung, Wohnen und Verkehr Akteneinsicht in Planungsunterlagen zum Bau einer Ortsumgehungsstraße. Aus der Befürchtung heraus, dass der Antrag auf Akteneinsicht seitens des Ministeriums so spät beschieden wird, dass die Bürgerinitiative ihre politische Mitwirkungsrechte nur noch eingeschränkt ausüben kann, bat sie uns um Unterstützung.

Aus diesem Grund haben wir das Ministerium für Stadtentwicklung, Wohnen und Verkehr gebeten, dass Akteneinsichtsgesuch unter dem Aspekt einer bürgernahen Verwaltung möglichst zeitnah zu prüfen (seit Antragstellung waren drei Wochen vergangen) und bereits im Vorfeld Hinderungsgründe, die zu einer Ablehnung des Antrages hätten führen können, zu benennen. Nach weiteren drei Wochen hat das Ministerium erfreulicherweise dem Antrag zugestimmt und der Bürgerinitiative Akteneinsicht gewährt.

Ein Bürger wartete bereits drei Monate auf die Bescheidung seines Antrages auf Akteneinsicht in Genehmigungsunterlagen eines Flugzeugsonderlandeplatzes.

Die Voraussetzungen des § 6 Abs. 1 Akteneinsichts- und Informationszugangsgesetz lagen mit der hinreichenden Bestimmung des Antrages vor, so dass das Brandenburgische Landesamt für Verkehr und Straßenbau diesen hätte in angemessener Frist bearbeiten können. Neben einem entsprechenden Hinweis an das Landesamt haben wir dem Bürger mitgeteilt, dass die Bescheidung eines Antrages letztendlich nur durch das Erheben einer Untätigkeitsklage gem. § 75 Verwaltungsgerichtsordnung erzwungen werden kann. Diesen Weg brauchte der Petent jedoch nicht zu gehen; auf unsere dringende Nachfrage hin wurde der Antrag positiv beschieden und Akteneinsicht gewährt. Als Grund für die Zeitverzögerung nannte die Behörde den seinerzeit noch bestehenden Klärungsbedarf bei der Ausübung ihres Ermessens hinsichtlich des neuen Akteneinsichts- und Informationszugangsgesetzes. Nunmehr seien die Voraussetzungen für zeitnahe Entscheidungen bei Anträgen auf Akteneinsicht geschaffen.

Um politische Mitbestimmungsrechte zu wahren, ist die Behörde unter dem Aspekt einer bürgernahen Verwaltung gehalten, ein Akteneinsichtsgesuch möglichst zeitnah zu bescheiden.

Werden Anträge auf Akteneinsicht nicht innerhalb von drei Monaten beschieden, kann der Bürger Untätigkeitsklage vor dem Verwaltungsgericht erheben.

3. Technisch-organisatorische Voraussetzungen der Akteneinsicht

Das Grundrecht auf Informationszugang wird nicht allein dadurch verwirklicht, dass die Bürger verstärkt ihre Rechte geltend machen. Vielmehr muss die Verwaltung ihrerseits sowohl ihre konventionelle Aktenhaltung als auch ihr elektronisches Informationsmanagement grundrechtskonform gestalten.

3.1 Aktenpläne und Datenbankstrukturen

Neben einer Veröffentlichung von Aktenplänen[95] ist auch ein bürgernahes und zugangsfreundliches Informationsmanagement erforderlich. Sowohl die konventionellen Aktenbestände als auch die automatisiert gespeicherten Informationen müssen schrittweise so umgestaltet werden, dass Entscheidungen über Akteneinsichts- und Informationszugangsanträge schneller und unkomplizierter getroffen werden können. Eine Vorgabe hierfür enthält § 4 Abs. 5 des novellierten Brandenburgischen Datenschutzgesetzes, wonach die Datenverarbeitung so organisiert sein soll, dass die Daten nach den jeweils verfolgten Zwecken und nach unterschiedlichen Betroffenen in jeder Phase der Verarbeitung getrennt werden können. Dementsprechend müssen in einem ersten Schritt zur Umsetzung des AIG die Aktenbestände, die keine personenbezogenen Daten oder ausschließlich personenbezogene Daten von beteiligten Amtsträgern enthalten, von den Aktenbeständen mit Daten von Bürgern oder Unternehmen getrennt werden. Dies ist sicherlich im Bereich der konventionellen Informationsverarbeitung aufwendiger als auch bei der elektronischen Datenverarbeitung. Auch bei herkömmlicher Aktenhaltung gibt es aber Vorbilder für eine differenzierte Informationsverarbeitung bei der Personalaktenführung, wo bereits seit einiger Zeit bundesrechtliche Vorgaben gelten.

Die elektronische Datenverarbeitung eröffnet insoweit zusätzliche Chancen für ein zugangsfreundliches Informationsmanagement, wenn bereits bei der Ausschreibung neuer EDV-Systeme die verfassungsrechtlichen Vorgaben des allgemeinen Informationszugangsrechts beachtet werden. Zugleich müssen möglichst frühzeitig die technisch-organisatorischen Voraussetzungen für eine *elektronische Akteneinsicht* geschaffen werden, die das Akteneinsichts- und Informationszugangsgesetz trotz seines umständlichen und an Ärmelschoner erinnernden Namens etwa durch elek-

tronische Post ermöglicht. Allerdings sind hier die rechtlichen Voraussetzungen im Einzelnen sorgfältig zu klären.

Soweit es sich um nicht-personenbezogene Datenbestände wie Aktenpläne, Erlasse und Rechtsvorschriften handelt, können diese ohne Weiteres als Mediendienst ins Internet eingestellt werden. Dabei ist - worauf wir im Projekt NetCity Rathenow hingewiesen haben[96] - darauf zu achten, dass die Nutzung dieses Mediendienstes anonym und ohne elektronische Spuren ermöglicht wird. Demgegenüber ist in all den Fällen, in denen nach dem Akteneinsichts- und Informationszugangsgesetz eine Abwägung zwischen den Interessen des Informationssuchenden und den Interessen betroffener Personen und Unternehmen an der vertraulichen Behandlung der Information vorschreibt, eine elektronische Durchführung der Akteneinsicht komplizierter. Im Regelfall wird sich der Antragsteller in diesen Fällen, in denen er das Überwiegen seines Offenbarungsinteresses darlegen muss (§ 6 Abs. 1 Satz 2 AIG), identifizieren müssen. Das Gesetz schreibt für den Antrag auf Akteneinsicht ohnehin die Schriftform vor und lässt nur für den umgekehrten Weg der Information von der Verwaltung zum Bürger das Mittel der elektronischen Post zu. Technisch vorstellbar ist demgegenüber durchaus auch ein elektronisches Antragsverfahren unter Verwendung von digitalen Signaturen.

3.2 Behördliche Ansprechpartner für den Informationszugang

Wesentlich ist für die Durchführung des Akteneinsichts- und Informationszugangsgesetzes, dass die Behördenleitung organisatorische Vorkehrungen dafür trifft, dass die Bürger schnell zu ihrem Recht kommen. Dies kann durch Dienstanweisungen geschehen. In jedem Fall sollte es zumindest einen Mitarbeiter in jeder öffentlichen Stelle geben, der für die Entgegennahme, Sichtung, Eingangsbestätigung und möglicherweise auch die weitere Bearbeitung in Zusammenarbeit mit fachlich zuständigen Verwaltungsmitarbeitern verantwortlich ist. Es bietet sich an, diese Aufgabe den behördlichen Datenschutzbeauftragten zu übertragen, die nach § 7 a des neuen Brandenburgischen Datenschutzgesetzes in allen datenverarbeitenden Stellen benannt werden müssen. So wie der Landesbeauftragte für den Datenschutz vom Gesetzgeber aus gutem Grund auch die Funktion eines Landesbeauftragten für das Recht auf Akteneinsicht übertragen bekommen hat, macht es Sinn, auf der Ebene der einzelnen Dienststellen diese Funktionen ebenfalls zu bündeln, selbst wenn der Informationszugang häufig auch ohne Berührung zum Datenschutz zu behandeln sein wird.

Die Verwaltung muss ihre Akten- und Informationsbestände zugangsfreundlich, d. h. so organisieren, dass dem Informationsinteresse der Bürger schnell und unbürokratisch entsprochen werden kann.

Die behördlichen Datenschutzbeauftragten sollten zugleich in der jeweiligen öffentlichen Stelle Ansprechpartner für Fragen des allgemeinen Informationszugangsrechts sein.

4. Sonstige Probleme des Informationszugangs

Journalisten waren die ersten, die sich auf das gerade in Kraft getretene Akteneinsichts- und Informationszugangsrecht beriefen. Tatsächlich sind Journalisten nicht darauf beschränkt, Auskunftsansprüche nach Presserecht geltend zu machen, sondern können auch das Akteneinsichtsrecht ausüben. Dieses wird nur durch bereichsspezifische Regelungen verdrängt, die für einen unbeschränkten Personenkreis gelten (§ 1 AIG). Ein Journalist muss bei seiner Recherche jeweils abwägen, ob es ihm wichtiger ist, von der Behörde eine gebührenfreie Auskunft zu erhalten, oder gegen Zahlung einer Gebühr Einsicht in die Originalunterlagen zu nehmen.

4.1 Archivrecht

Ein Redakteur wollte Einsicht in Unterlagen über Kaderbefehle der früheren Volkspolizei nehmen, die in einem Polizeipräsidium lagerten. Er berief sich darauf, dass er vergleichbare Unterlagen im Landeshauptarchiv habe einsehen können. Sein presserechtlicher Auskunftsanspruch wurde zunächst ebenso abgelehnt wie sein Antrag auf Akteneinsicht.

In Abstimmung mit dem Ministerium des Innern haben wir festgestellt, dass die Kaderakten Unterlagen enthielten, die zur Personalsachbearbeitung noch benötigt wurden und deshalb in Personalakten hätten eingefügt werden müssen. Die übrigen Unterlagen hätten ausgesondert, dem Landeshauptarchiv angeboten und bei Ablehnung vernichtet werden müssen. Der Umstand, dass sie - auch aus Kapazitätsgründen - noch bei der Polizei aufbewahrt werden, führt dazu, dass Akteneinsicht in derartige Unterlagen (soweit sie nicht den Personalakten zuzurechnen sind) ausschließlich nach dem Brandenburgischen Archivgesetz zu gewähren ist, auch wenn die Akten (noch) nicht im Landeshauptarchiv lagern. Während für die Personalunterlagen nach dem Informationszugangsgesetz die Akteneinsicht wegen fehlender Einwilligung der Betroffenen regelmäßig abzulehnen sein wird, gilt für den Teil der Kaderakten, der als dezentral gelagertes Archivgut einzuordnen ist, ausschließlich Archivrecht.

4.2 Presserecht

Ein weiterer Journalist erbat vom Landesrechnungshof eine Liste der Prüfthemen, mit der diese oberste Landesbehörde sich im vergangenen Jahr beschäftigt habe. Eine Einsicht in die Prüfvorgänge selbst verlangte er nicht. Der Rechnungshof lehnte dieses Ansinnen ab.

Das Akteneinsichts- und Informationszugangsgesetz war in diesem Fall nicht anwendbar, weil der Landesrechnungshof diesem Gesetz nur insoweit unterliegt, als seine Verwaltungsvorgänge betroffen sind (§ 2 Abs. 2 Satz 1 AIG). Nach unserer Auffas-

sung hatte der Journalist aber einen medienrechtlichen Auskunftsanspruch entsprechend § 5 des Brandenburgischen Landespressegesetzes, wonach die Behörden verpflichtet sind, den Vertretern der Presse die der Erfüllung ihrer öffentlichen Aufgabe dienenden Auskünfte zu erteilen. Von den Ausnahmen zu dieser Auskunftspflicht kam nur in Frage, dass möglicherweise ein überwiegendes öffentliches Interesse, nämlich die Unabhängigkeit der Prüftätigkeit des Landesrechnungshofes hätte beeinträchtigt werden können.

Wir verkennen nicht, dass die Prüftätigkeit des Landesrechnungshofes von Versuchen der Einflussnahme von außen jedenfalls solange frei gehalten werden muss, bis der jeweilige Prüfvorgang abgeschlossen ist. Auch danach ist das Beratungsgeheimnis des Rechnungshofes zu schützen. Schließlich besteht keine Verpflichtung des Landesrechnungshofes, gegenüber den Medien die Art und Weise der Durchführung einer Prüfung oder die Gründe dafür, dass eine bestimmte Behörde nicht geprüft wurde, darzulegen. Außerdem veröffentlicht der Landesrechnungshof einen Jahresbericht, der allerdings nicht alle Prüfthemen und -ergebnisse enthält. Die Landeshaushaltsordnung verbietet dem Landesrechnungshof allerdings keine über den Jahresbericht hinausgehende Veröffentlichung von Prüfthemen (insbesondere wenn sie medienrechtlich geboten ist). Überwiegende öffentliche Interessen, die einer Auskunftserteilung über die abschließend behandelnden Prüfthemen entgegenstehen könnten, sind für uns deshalb nicht erkennbar.

Der Rechnungshof hatte dem entgegengehalten, mit der erwünschten Auskunftserteilung würden der Presse weitergehende Auskunftsrechte als dem Landtag eingeräumt. Auch dem können wir nicht zustimmen. Den Mitgliedern des Landtags steht (anders als den Medien) ein verfassungsrechtlicher Auskunftsanspruch und Aktenvorlageanspruch selbst gegen den Landesrechnungshof bei abgeschlossenen Rechnungsprüfungsvorgängen zu, der über den medienrechtlichen Auskunftsanspruch hinausgeht (Artikel 56 Abs. 3 Landesverfassung). Den Umfang dieser Ansprüche der Abgeordneten hat das Verfassungsgericht des Landes Brandenburg schon 1997 im Einzelnen umrissen[97]. Während der verfassungsrechtliche Auskunftsanspruch der Abgeordneten sich auf den Inhalt der Prüfungsergebnisse erstreckt, würde dem presserechtlichen Auskunftsanspruch durch Bekanntgabe der geprüften Themen ausreichend Rechnung getragen.

Die Präsidentin des Landesrechnungshofes teilt diese Auffassung nicht, hat uns aber in Aussicht gestellt, die Frage einer stärkeren Transparenz der Tätigkeit der Rechnungshöfe im Rahmen der Konferenz der Präsidentinnen und Präsidenten der Rechnungshöfe des Bundes und der Länder zur Sprache zu bringen. Dies ist ohnehin im Hinblick auf die genannte Entscheidung des Verfassungsgerichts des Landes Brandenburg erforderlich.

5. Informationszugang für Abgeordnete

Das Ministerium des Innern hat uns den Entwurf von einheitlichen Verfahrensregelungen zur Behandlung von Informationsverlangen von Abgeordneten des Landtages gemäß Artikel 56 Abs. 3 der Landesverfassung zur Stellungnahme zugeleitet, die von der Landesregierung beschlossen und zu einem späteren Zeitpunkt in die Gemeinsame Geschäftsordnung übernommen werden sollen.

Zum Akteneinsichts- und Auskunftsanspruch der Abgeordneten, der sich vom Informationszugangsanspruch der Bürger und Verbände nach Artikel 21 Abs. 3 und 4 der Landesverfassung unterscheidet, hat das Verfassungsgericht des Landes Brandenburg in zwei Entscheidungen[98] detaillierte Grundsätze entwickelt. An diesen haben sich auch Verfahrensregelungen der Landesregierung zu orientieren.

In unserer Stellungnahme gegenüber dem Ministerium haben wir darauf hingewiesen, dass alle verfassungsrechtlichen Ansprüche des Abgeordneten nach Artikel 56 Abs. 3 unverzüglich zu befriedigen sind. Das Beschleunigungsgebot gilt nicht nur für Auskunft und Aktenvorlage, sondern erst recht für den bloßen Zugang zu Behörden. Es dürfen auch keine verfahrensmäßigen Hindernisse errichtet werden, die zu einer zeitlichen Verzögerung der Bearbeitung führen würden, soweit derartige Hindernisse nicht ihrerseits verfassungsrechtlich geboten sind.

Der Entstehungsgeschichte des Artikels 56 Abs. 3, auf die sich auch das Verfassungsgericht in seiner Rechtsprechung stützt, ist zu entnehmen, dass Abgeordnete ausdrücklich weitergehende Informationszugangsrechte haben als Bürger außerhalb des Parlaments. Das ergibt sich zugleich aus dem Recht zur wirksamen parlamentarischen Kontrolle der Landesregierung, wie es das Bundesverfassungsgericht im Verhältnis zur Bundesregierung betont hat[99]. Dieses effektive Kontrollrecht darf nicht durch Verfahrensregelungen beschnitten werden. Zwar finden auch Zugangsrechte der Abgeordneten ihre Grenze am Kernbereich der Exekutive. Nicht jeder Zugang zu einer Behörde betrifft aber bereits diesen Kernbereich. Insofern erscheint es auch zu restriktiv, wenn der Entwurf der Verfahrensregelungen vorsieht, es solle darauf hingewirkt werden, dass Abgeordnete den Zugang zu Behörden und Dienststellen schriftlich beantragen. Abgeordnete müssen Behörden auch spontan und ohne Verwaltungsaufwand aufsuchen können, soweit ihnen dies erforderlich erscheint.

Insbesondere die vorgesehene Regelung, dass die Landesregierung über jedes Begehren von Abgeordneten auf Auskunft oder Aktenvorlage zu entscheiden habe, ist aus unserer Sicht ebenfalls zu restriktiv. Das Verfassungsgericht hat nicht ausgeschlossen, dass die Landesregierung die Entscheidung über derartige Ersuchen auch auf einzelne Ministerien übertragen kann. Dies würde sich zur Beschleunigung der Auskunftserteilung und Aktenvorlage jedenfalls in Fällen anbieten, die weder andere Ressorts noch die Landesregierung insgesamt betreffen oder erkennbar nicht von

politischer Bedeutung sind.

Die Landesregierung hat über die Verfahrensregelungen bisher nicht entschieden.

In einem konkreten Fall wandte sich ein Landtagsabgeordneter an uns mit der Bitte um Beratung bezüglich seines Akteneinsichtsverlangens, dem das Ministerium der Finanzen nur teilweise entsprechen wollte. Zur Begründung verwies das Ministerium auf schutzwürdige Belange von Geschäftspartnern einer landeseigenen Gesellschaft, die es erforderten, die betreffenden Stellen in der vom Abgeordneten einzusehenden Unterlage abzudecken.

Der Bitte des Landesbeauftragten um nähere Erläuterungen zu dieser Begründung entsprach die Ministerin der Finanzen nicht, wobei sie zutreffend darauf hinwies, dass es nicht zu den Aufgaben des Landesbeauftragten für das Recht auf Akteneinsicht gehöre, die organschaftlichen Ansprüche gegenüber der Exekutive zu wahren. Da der Landesbeauftragte es jedoch als seine Aufgabe betrachtet, Abgeordnete ebenso wie andere Bürger zu beraten, die sich an ihn wenden, hat er dem Landtagsabgeordneten allgemeine rechtliche Hinweise zu seinem Anliegen gegeben. Darin hat er vor dem Hintergrund der Rechtsprechung des Verfassungsgerichts verdeutlicht, dass erhebliche Zweifel angebracht sind, ob die schutzwürdigen Belange privater Geschäftspartner der landeseigenen Gesellschaft gegenüber dem verfassungsrechtlichen legitimierten Informationsinteresse des Abgeordneten überwiegen und deshalb die Ablehnung des Vorlagebegehrens zwingend erforderlich ist.

Letztlich kann dies nur das Verfassungsgericht beurteilen, nach dessen Rechtsprechung nicht einmal das Grundrecht des Einzelnen, selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen, als überwiegend gegenüber dem Aktenvorlageanspruch des Abgeordneten anzusehen sei. Selbst wenn die privaten Belange der Geschäftspartner schutzwürdig wären, hätte das Informationsinteresse des Abgeordneten verfassungsrechtlich erst recht dann den Vorrang, wenn die privaten Geheimhaltungsinteressen nicht - wie der Datenschutz - grundrechtliche Qualität hätten.

Da das Verfassungsgericht seine Bewertung unter der Voraussetzung getroffen hat, dass die Kenntnis der umstrittenen Informationen für die Wahrnehmung der parlamentarischen Kontrollkompetenz des Abgeordneten erforderlich ist, haben wir dem Abgeordneten empfohlen, zunächst die von der Ministerin der Finanzen angebotenen Unterlagen einzusehen, um danach zu entscheiden, ob er sein parlamentarisches Kontrollrecht vor dem Verfassungsgericht des Landes Brandenburg weiterverfolgen soll.

Zu Recht hat die Ministerin der Finanzen den Abgeordneten allerdings auf die Verpflichtung zur Geheimhaltung der Informationen hingewiesen, die er durch Einsicht in die Unterlage erhält. Das Verfassungsgericht hat in seiner Entscheidung von 1996[100] festgestellt, dass die Landesregierung den Schutz privater Geheimhaltungsinteressen bei gleichzeitiger Aktenvorlage an Abgeordnete nach Maßgabe der Verschluss-Sa-

chenanordnung des Landtages Brandenburg (Anlage 5 zu dessen Geschäftsordnung) sicherstellen kann.

Teil C

Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

1. Die Dienststelle

Am 31. Mai 1998 endete die Amtszeit des ersten Landesbeauftragten für den Datenschutz, Dr. sc. Dietmar Bleyl. Er hat nicht nur mit großem persönlichem Engagement die Dienststelle des Datenschutzbeauftragten aufgebaut, sondern viel dazu beigetragen, den Gedanken des Datenschutzes den Bürgern nahe zu bringen und in der Verwaltung zu verankern. Ich habe bei meinem Amtsantritt sachkundige und motivierte Mitarbeiterinnen und Mitarbeiter in einer funktionierenden Dienststelle vorgefunden. Wir werden auch in der neuen Amtsperiode gemeinsam das Ziel, Recht und Technik zur Durchsetzung der Grundrechte auf Datenschutz und Informationszugang einzusetzen, zur Grundlage unserer Arbeit machen.

Die Dienststelle des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht ist seit ihrer Bildung in Kleinmachnow untergebracht. Bei seinem Amtsantritt hat der neu gewählte Landesbeauftragte die Notwendigkeit unterstrichen, dass der Standort verlegt werden muss. Die Dienststelle dieses "Bürgerbeauftragten" muss für den Bürger an zentraler Stelle und in der Nähe des Landtags und der Landesregierung erreichbar sein. Alle Mitglieder der Landesregierung haben dem Landesbeauftragten bestätigt, dass dieses Anliegen legitim sei. Wir sind intensiv darum bemüht, ein Dienstgebäude in der Landeshauptstadt zu finden. Der Präsident des Landtags und das Ministerium der Finanzen haben uns dabei ihre Unterstützung zugesichert.

Die personelle Situation in der Dienststelle war im Berichtszeitraum deshalb äußerst angespannt, weil nicht alle etatmäßigen Planstellen zur Verfügung standen. Darüber hinaus hat der Landesbeauftragte sich bei den Haushaltsberatungen dafür eingesetzt, dass ein eigenständiger Bereich "Akteneinsicht" mit insgesamt fünf Planstellen geschaffen wird. Hiervon hat der Landtag für das Haushaltsjahr 1999 lediglich eine Stelle des gehobenen Dienstes bewilligt. Auf die Dauer können die Kontrolle des Datenschutzes im öffentlichen Bereich gerade im Hinblick auf die zunehmende Vernetzung der Datenverarbeitung auch auf Landesebene und die Aufgaben nach dem Akteneinsichts- und Informationszugangsgesetz mit den vorhandenen Dienstkräften jedoch nicht im erforderlichen Umfang erfüllt werden. Deshalb ist hier zumindest ein schrittweiser Aufbau des gesonderten Bereichs "Akteneinsicht" notwendig. Anderenfalls müssten Prüfaktivitäten im Bereich des Datenschutzes zurückgestellt werden, was der Gesetzgeber mit der Übertragung der zusätzlichen Aufgabe des Informationszugangs sicherlich nicht beabsichtigt hat.

2. Zusammenarbeit mit dem Landtag

Der Landesbeauftragte hat im Berichtszeitraum besonders intensiv mit dem Innenausschuss des Landtags zusammengearbeitet, der federführend über die Novellierung des Brandenburgischen Datenschutzgesetzes und des Meldegesetzes beriet. Dabei erhielt der Landesbeauftragte ausführlich Gelegenheit, seine Auffassung darzulegen. Für einen Teil seiner Vorschläge konnte er auch die Unterstützung des Ausschusses gewinnen. In gleicher konstruktiver Weise wurden der Sechste Tätigkeitsbericht des Landesbeauftragten für den Datenschutz und die Stellungnahme der Landesregierung hierzu im Innenausschuss und später im Plenum des Landtagserörtert.

Der Landesbeauftragte hat mehrere Mitglieder des Landtags in Fragen des Datenschutzes und des Informationszugangsrechts beraten. Er hat seine Vorstellungen auch den Fraktionen erläutern können.

3. Kooperation mit anderen Datenschutzbehörden

Besonders wichtig und fruchtbar ist die Zusammenarbeit im Rahmen der regelmäßig zweimal jährlich tagenden Konferenz der Datenschutzbeauftragten des Bundes und der Länder, die im vergangenen Jahr unter dem Vorsitz des Hessischen Datenschutzbeauftragten, Prof. Dr. Rainer Hamm, zahlreiche Entschließungen zu aktuellen Fragen des Datenschutzes gefasst hat[101]. Den Vorsitz in der Konferenz wird 1999 der Landesbeauftragte für den Datenschutz Mecklenburg-Vorpommern, Dr. Werner Kessel, turnusgemäß übernehmen.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat dem Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht den Vorsitz im Arbeitskreis "Medien" dieser Konferenz übertragen, der bisher - seit seiner Gründung - vom Berliner Datenschutzbeauftragten geleitet worden war.

Als Vorsitzender des nationalen Arbeitskreises "Medien" hat der Landesbeauftragte auch an der internationalen Arbeitsgruppe zum "Datenschutz in der Telekommunikation" mitgearbeitet, die Fragen des grenzüberschreitenden Datenschutzes bei Telekommunikation und Medien erörtert und entsprechende Empfehlungen abgibt.

Die Zusammenarbeit mit der Aufsichtsbehörde im nicht-öffentlichen Bereich, dem Ministerium des Innern, war gerade bei der Vorbereitung der Novelle zum Brandenburgischen Datenschutzgesetz sehr konstruktiv.

Fortgesetzt und intensiviert wurde die Zusammenarbeit mit dem Berliner Datenschutz-

beauftragten. Die Zunahme länderübergreifender Verfahren der Datenverarbeitung machen eine verstärkte Kooperation der Datenschutzkontrollbehörden in Brandenburg und Berlin unabweisbar. Erstmals zu diesem Tätigkeitsbericht hat der Landesbeauftragte mit dem Berliner Datenschutzbeauftragten außerdem einen gemeinsamen Band "Dokumente zum Datenschutz" veröffentlicht, der zahlreiche Entschließungen und Empfehlungen der Datenschutzbeauftragten enthält, auf die in diesem Bericht verwiesen wird. Er kann ebenso wie der Tätigkeitsbericht gesondert bei uns angefordert werden.

Im Zeitalter der grenzüberschreitenden Datenflüsse gewinnt auch die Kooperation mit ausländischen Datenschutzbeauftragten zunehmende Bedeutung. Dies gilt für Brandenburg insbesondere im Verhältnis zum Nachbarland Polen. Deshalb hat der Landesbeauftragte mit der neuen polnischen Datenschutzbeauftragten, Frau Dr. Ewa Kulesza, einen Informationsaustausch vereinbart.

Die immer wichtiger werdende internationale Koordination im Bereich des Datenschutzes ist einmal jährlich Thema der Internationalen Datenschutzkonferenz, die im vergangenen Jahr in Santiago de Compostela stattfand. Dabei wurde der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht in den Programmbeirat für die kommende XXI. Internationale Datenschutzkonferenz berufen, die im Herbst 1999 in Hong Kong stattfinden wird.

Gerade im Bereich des Informationszugangsrechts ist die Auswertung der Erfahrungen ausländischer Informationszugangsbeauftragter, insbesondere soweit sie zugleich Datenschutzbeauftragte sind, wesentlich. Der Landesbeauftragte hat deshalb Kontakte zu den entsprechenden Beauftragten in Ungarn und den kanadischen Provinzen Britisch Columbia, Québec und Ontario geknüpft und mit ihnen ebenfalls einen Informationsaustausch begonnen.

4. Öffentlichkeitsarbeit

Die Wahrnehmung des Datenschutzes und der Informationsfreiheit hängt wesentlich von einer verstärkten Öffentlichkeitsarbeit ab. Dabei hatte das neue Akteneinsichts- und Informationszugangsgesetz im Berichtszeitraum Vorrang, zumal es in diesem Bereich bisher keine Informationsmaterialien für die Bürger gab. Der Landesbeauftragte hat deshalb ein Faltblatt "Wegweiser zur Akteneinsicht" herausgegeben, in dem in erster Linie den Bürgern möglichst leicht verständliche Erläuterungen der neuen rechtlichen Möglichkeiten in diesem Bereich gegeben werden. Dieses Faltblatt wurde allen Mitgliedern des Landtags und der Landesregierung zur Verfügung gestellt. Daneben erhalten es in der Folge auch die Kreise und Gemeinden sowie auf Anfrage kostenlos alle Bürger zugesandt. Die Reaktionen zeigen, dass dieses Faltblatt auf großes Interesse stößt. Wir werden die Anstrengungen in diesem Bereich im Rahmen unserer begrenzten Möglichkeiten weiter erhöhen.

Eine wichtige Rolle spielt in diesem Zusammenhang auch das Internetangebot unserer Dienststelle, mit dem wir kostengünstig Informationen an Bürger mit Netzanschluss

verteilen. Auch dieser Tätigkeitsbericht ist über das Internet abrufbar unter <http://www.lda.brandenburg.de>. Zugleich kann das Internet auch genutzt werden, um Verbindung zu uns aufzunehmen oder sogar Beschwerden an uns zu richten. Dabei sind allerdings einige Vorsichtsmaßnahmen notwendig, denn wenn personenbezogene Daten im Klartext über das Internet übertragen werden, können diese von Unbefugten mitgelesen und sogar verfälscht werden. Um diese Gefährdungen weitestgehend auszuschließen, kann ab sofort über einen Internet-Anschluss mit unserer Behörde verschlüsselt kommuniziert werden. Dazu stellen wir in unserem WWW-Angebot einen vom Landesamt für Datenverarbeitung und Statistik zertifizierten PGP-Schlüssel zur Verfügung. Nähere Erläuterungen zur verwendeten Verschlüsselungssoftware sind auf der Internetseite **http://www.pgpi.com** zu finden.

Kleinmachnow, den 3. März 1999

Dr. Alexander Dix

Landesbeauftragter für den Datenschutz
und für das Recht auf Akteneinsicht

A. Forderungen für einen Politikwechsel zum wirksameren Schutz der Privatsphäre

Datenschutzbeauftragte appellieren an die neue Bundesregierung:

10 Punkte für einen Politikwechsel zum wirksameren Schutz der Privatsphäre

Die Datenschutzbeauftragten Berlins, Brandenburgs, Bremens, Nordrhein-Westfalens und Schleswig-Holsteins fordern einen Politikwechsel zum Schutz der Privatsphäre.

Deutschland befindet sich auf dem Weg in die Informationsgesellschaft. Niemand kann zuverlässig abschätzen, welche Veränderungen sich aus dieser Entwicklung für Staat und Gesellschaft und für nahezu alle Lebensbereiche der Bürgerinnen und Bürger ergeben. Sicher ist aber, daß ohne Garantien für Datenschutz und Datensicherheit die Informationsgesellschaft nicht zu verantworten ist. Eine Informationsverarbeitung, bei der die Bürgerinnen und Bürger nicht mehr wissen, an welcher Stelle welche Daten über sie gesammelt werden, beeinträchtigt nicht nur ihre eigenen Rechte, sondern ist auch mit dem demokratischen Rechtsstaat unvereinbar.

1) Grundrecht auf Datenschutz

Es ist an der Zeit, das Recht auf informationelle Selbstbestimmung als ausdrückliches Grundrecht auch im Grundgesetz zu verankern. Grundrechte reflektieren das Schutzbedürfnis der Menschen im jeweiligen historischen Zusammenhang.

Unter den Bedingungen der Informationsgesellschaft erlangt der Schutz der Privatsphäre jedes einzelnen Menschen hohe Priorität. Das Grundgesetz sollte sich dazu um so mehr ausdrücklich bekennen, als durch die verfassungsrechtliche Zulassung des Großen Lauschangriffs empfindliche Einschränkungen der Privatsphäre vorgenommen wurden.

FORDERUNG: ***In das Grundgesetz ist ein Grundrecht auf Datenschutz aufzunehmen.***

2) Datensicherheit

Fragen der Datensicherheit werden in Deutschland bislang vernachlässigt. Das derzeitige Datenschutzrecht verlangt lediglich “angemessene” Datensicherheitsmaßnahmen. Dies genügt nicht. Ohne wirksame Umsetzung auf der technischen Ebene nützen allerdings auch die besten Datenschutzbestimmungen nichts. Die Verhältnisse im Internet zeigen, daß bei der Datensicherheit Nachholbedarf besteht. Auch die Ungewißheit bezüglich des Verhaltens der Computer beim Jahrtausendwechsel am 1.

Januar 2000 legen es nahe, Fragen der Ordnungsmäßigkeit der Datenverarbeitung künftig ein anderes Gewicht zu geben. Die Umstellung der Programme auf den Jahrtausendwechsel kostet jetzt Milliarden.

Nicht nur die Interessen der Systembetreiber, sondern auch die der Bürgerinnen und Bürger als Nutzer und Kunden müssen künftig angemessen im Rahmen sogenannter “mehrseitiger Sicherheit” berücksichtigt werden.

FORDERUNG: ***Sicherheit und Ordnungsmäßigkeit der Datenverarbeitung müssen eine höhere Priorität erhalten.***

3) Verschlüsselung

Die Nutzung offener Netze für geschäftliche oder persönliche Zwecke steht und fällt mit der Möglichkeit, die Vertraulichkeit und Unverfälschtheit der ausgetauschten Informationen zu garantieren. Das wichtigste Instrument dazu sind starke Verschlüsselungsverfahren. Die staatliche Politik sollte auf eine Förderung dieser Technik und ihre Verfügbarkeit für jeden einzelnen Bürger gerichtet sein. Überlegungen, das Recht zur Verschlüsselung zugunsten der Sicherheitsbehörden einzuschränken, gehen schon deswegen fehl, weil derartige Regelungen technisch - etwa durch Doppelverschlüsselung oder Steganographie - leicht umgangen werden können. Die Vorstellung, jede elektronische Kommunikation müsse vom Staat überwachbar sein, ist unter den Bedingungen des Internet illusorisch.

FORDERUNG: ***Wirksame Verschlüsselungsverfahren müssen gefördert werden; Überlegungen, das Recht auf Kryptographie zu beschränken, müssen eingestellt werden.***

4) Modernisierung der Datenschutzgesetze

Die bisherige Datenschutzgesetzgebung muß überprüft und neu gewichtet werden. Das Bundes- und die Landesdatenschutzgesetze basieren auf der Großrechnertechnologie und berücksichtigen nicht die neuen technischen Gegebenheiten. Die ohne-hin überfällige Anpassung der Gesetze an die Europäische Datenschutzrichtlinie muß zur umfassenden Modernisierung genutzt werden. Dabei spielen Stichworte wie Verschlankung, Datenschutz durch Technik, Datenschutzaudit, Förderung von Selbstdatenschutz, Datenvermeidung, Anonymisierung und Pseudonymisierung eine entscheidende Rolle.

FORDERUNG: ***Die Datenschutzgesetze müssen gründlich modernisiert und effektiviert werden.***

5) Bereichsspezifisches Datenschutzrecht

Die bereichsspezifische Datenschutzgesetzgebung kann in der bisherigen Form nicht fortgeführt werden. Es nützt den Bürgerinnen und Bürgern wenig, wenn die Fachgesetze durch immer mehr Vorschriften aufgebläht, zugleich aber in ihrer datenschutzrechtlichen Substanz ausgehöhlt werden.

Jüngstes Beispiel ist die Änderung des Sozialgesetzbuches X, bei der - ohne daß der Sozialdatenschutz in seinem äußeren Zuschnitt verändert wurde - die Sozialbehörden quasi zu Außenstellen der Polizei gemacht wurden. Ähnlich wurde das Ausländerzentralregister als Informationsdrehscheibe und Fahndungsregister für alle deutschen Behörden ausgestaltet. In Zukunft muß im bereichsspezifischen Recht Qualität vor Quantität gehen. Es ist ein Wesensmerkmal des Datenschutzes und des daraus abgeleiteten Zweckbindungsprinzips, daß sich die Bürgerinnen und Bürger darauf verlassen können, daß das, was sie einer Behörde mitteilen, nicht automatisch an alle anderen Behörden weitergegeben werden darf.

FORDERUNG: ***Die bereichsspezifische Datenschutzgesetzgebung muß substantielle Rechtsgarantien gewährleisten.***

6) Sicherheitsbereich

Im Sicherheitsbereich ist in den vergangenen Jahren bei der Abwägung zwischen Datenschutz und Sicherheitsinteressen fast stets zugunsten letzterer entschieden worden. Die Sicherheitsbehörden verfügen inzwischen über eine derartige Fülle von Befugnissen, daß es schwer geworden ist, den Überblick zu bewahren. Viele rechtsstaatlich problematische, auf die Terrorismusfahndung zugeschnittene Instrumente können jetzt ohne Sicherheitsverlust zurückgenommen werden.

Generell ist bei sensiblen Eingriffsbefugnissen ein Evaluierungsmechanismus einzuführen, der es dem Parlament ermöglicht, nach einer angemessenen Frist die Erforderlichkeit der Eingriffsbefugnisse anhand objektiver Kriterien zu überprüfen.

FORDERUNG: ***Die besonders sensiblen Eingriffsbefugnisse im Sicherheitsbereich müssen systematisch auf ihre Effektivität und ihre Grundrechtsverträglichkeit untersucht werden.***

Sonderbefugnisse aus der Terrorismusfahndung müssen zurückgenommen werden.

7) Verwaltungsmodernisierung

In nahezu allen Bereichen der Verwaltung laufen umfangreiche Modernisierungsbestrebungen. Häufig sehen sie auch die Straffung der Abläufe, Privatisierung der Aufgabenerfüllung oder jedenfalls zunehmende Einschaltung externer Dienstleister vor. Gegen eine Effektivierung der Verwaltung ist nichts einzuwenden. Wer sie aber nur unter den Aspekten der Beschleunigung und Kosteneinsparung betreibt, wird schnell entdecken, daß rechtsstaatliche Verfahrensgarantien nicht zum Nulltarif zu haben sind.

Verwaltungsleistungen unterscheiden sich von privaten Dienstleistungen wesentlich dadurch, daß sie nicht nur unter marktwirtschaftlichen, sondern gerade unter rechtsstaatlichen Gesichtspunkten erbracht werden. Dazu gehört die Gewährleistung des Datenschutzes. Solange das Datenschutzniveau im Bereich der Privatwirtschaft deutlich niedriger als in der öffentlichen Verwaltung ist, verschlechtert die Privatisierung von Verwaltungsleistungen die Rechtsposition der Bürgerinnen und Bürger.

FORDERUNG: ***Datenschutz darf nicht einer rigorosen Verwaltungsmodernisierung zum Opfer fallen.***

8) Informationszugang

In der Informationsgesellschaft kommt der Verfügung über die Informationsressourcen herausragende Bedeutung zu. Deshalb gewinnen Informationszugangsrechte in einer demokratischen Gesellschaft immer mehr Gewicht. Nur wenn die Bürgerinnen und Bürger das Recht auf Zugang zu Informationen bei öffentlichen Stellen erhalten, können sie ihr Gemeinwesen wirksam gestalten. Deutschland kann in dieser Beziehung mit vielen europäischen Nachbarstaaten noch nicht Schritt halten. Auch die Europäische Union hat im Vertrag von Amsterdam allen Bürgerinnen und Bürgern Zugang zu ihren Informationen zugesagt. Es wäre falsch, Datenschutz und Informationszugang gegeneinander ausspielen zu wollen. Beide Prinzipien bedingen und ergänzen einander vielmehr.

FORDERUNG: ***Es ist ein allgemeines Informationszugangsrecht einzuführen.***

9) Telekommunikation

Das Zusammenwachsen von Computertechnologie und neuen Medien und die zunehmende Allgegenwärtigkeit der Informationstechnik im täglichen Leben führen dazu, daß von den Menschen an den unterschiedlichsten Stellen elektronische Datenspuren hinterlassen werden (Electronic Cash, Nutzung elektronischer Medien, Einsatz von Chipkarten, elektronische Kommunikation). Diese Spuren sind für Sicherheitsbehörden ebenso von Interesse wie für Marketingabteilungen in der Wirtschaft. Die Politik hat

die Aufgabe zu verhindern, daß die Bürgerinnen und Bürger durch faktischen Zwang zu gläsernen Menschen werden. Die Multimediagesetzgebung enthält insofern erste Ansätze zur Datenvermeidung. Diese müssen umgesetzt und fortgeschrieben werden. Zugleich hat der Gesetzgeber im Telekommunikationsrecht aufwendige Kontrollinstrumente vorgesehen. So sollen Telekommunikationsanbieter verpflichtet werden, viele Milliarden Mark teure Abhörmöglichkeiten für Sicherheitsbehörden auf eigene Kosten einzurichten, damit jede Nebenstelle abhörbar wird. Der Anspruch der Kontrollierbarkeit jeglicher Telekommunikation kann nicht aufrechterhalten werden.

FORDERUNG: ***Das Recht der Bürgerinnen und Bürger auf unüberwachte telekommunikative Selbstbestimmung muß ein zentrales Anliegen der Politik werden.***

10) Datenschutz in der Wirtschaft

Neben die Angst vor der Überwachung durch den Staat als “Big Brother” ist aus guten Gründen die Furcht vor der informationellen Bevormundung durch dessen “Geschwister” aus der Wirtschaft getreten. Während staatliche Einrichtungen einem relativ strengen Datenschutzregime unterworfen sind, entwickeln sich die privatwirtschaftlich betriebenen personenbezogenen Datenbanken oft fast schon wildwüchsig. Bei Informations-, Finanz- oder sonstigen Dienstleistungsunternehmen oder bei großen Versandhändlern werden Daten über Konsumgewohnheiten, über Bonität und über sonstige, teilweise sehr private Sachverhalte systematisch gesammelt und unter verschiedenen Gesichtspunkten ausgewertet und genutzt. Nicht weniger sensibel sind Datenbanken über Arbeitnehmerinnen und Arbeitnehmer. Das derzeitige Datenschutzrecht gibt den Betroffenen wenig Schutz. Es fehlen konkrete Regelungen und Sanktionen für den Fall des Regelverstoßes. Nicht zuletzt sind die Datenschutzkontrollinstanzen bislang nicht so ausgestattet, daß sie der exponentiell wachsenden Datenverarbeitung in der Wirtschaft gewachsen sind.

FORDERUNG: ***Der Datenschutz im privaten Bereich muß rechtlich und organisatorisch ausgebaut werden.***

B. Beschlüsse und Entschließung der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

I. Entschließungen der 55. Konferenz am 19./20. März 1998 in Wiesbaden

Datenschutzprobleme der Geldkarte

(Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder wiederholt ihre Forderung aus ihrer Entschließung vom 13.10.1995 nach einem anonymen elektronischen Zahlungsverfahren bei elektronischen Geldbörsen. Dies gilt insbesondere für die Geldkarte des deutschen Kreditwesens, bei der in kartenbezogenen "Schattenkonten" der Evidenzzentralen nicht nur der Kaufbetrag und ein identifizierbarer Händlerschlüssel, sondern auch der Kaufzeitpunkt gespeichert werden. Mit diesen Daten können sämtliche mit der Geldkarte getätigten Kaufvorgänge jahrelang nachvollzogen werden, wenn die Daten mit den persönlichen Kundendaten zusammengeführt werden. Diese Geldkarte erfüllt nicht die Forderungen der Datenschutzbeauftragten.

Außerdem werden die Kundinnen und Kunden über diese "Schattenkonten" noch nicht einmal informiert. Die Herausgeber solcher Karten bzw. die Kreditinstitute haben aber die Pflicht, ihre Kundinnen und Kunden über Art und Umfang der im Hintergrund laufenden Verarbeitungsvorgänge zu informieren.

Unabhängig davon müssen bei der Geldkarte des deutschen Kreditwesens sämtliche Umsatzdaten in den Evidenzzentralen und auch bei den Händlern nach Abschluss der Verrechnung (Clearing) gelöscht oder zumindest anonymisiert werden.

Die Datenschutzbeauftragten fordern die Kartenherausgeber und die Kreditwirtschaft erneut dazu auf, vorzugsweise kartengestützte Zahlungssysteme ohne personenbezogene Daten -sog. White Cards - anzubieten. Die Anwendung ist so zu gestalten, dass ein karten- und damit personenbezogenes Clearing nicht erfolgt.

Der Gesetzgeber bleibt aufgerufen sicherzustellen, dass auch in Zukunft die Möglichkeit besteht, im wirtschaftlichen Leben im gleichen Umfang wie bisher bei Bargeldzahlung anonym zu bleiben.

Datenschutz beim digitalen Fernsehen

(Entschließung der 55. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 19./20. März 1998)

Die Datenschutzbeauftragten des Bundes und der Länder machen darauf aufmerksam, dass bei elektronischen Diensten immer umfangreichere Datenspuren über das Verhalten der Einzelnen entstehen. Mit der Digitalisierung der Fernseh- und Hörfunkübertragung entsteht die technische Infrastruktur dafür, dass erstmals auch das individuelle Mediennutzungsverhalten registriert werden kann. Sie bekräftigen deshalb ihre Forderung, dass auch bei der Vermittlung und Abrechnung digitaler Fernsehsendungen eine flächendeckende Registrierung des individuellen Fernsehkonsums vermieden wird. Im digitalen Fernsehen ("Free TV" und "Pay TV") muss die unbeobachtete Nutzung des Mediums ohne Nachteile möglich bleiben.

Die Datenschutzbeauftragten begrüßen es deshalb, dass die Staats- und Senatskanzleien Vorschläge für die Änderung des Rundfunkstaatsvertrags vorgelegt haben, mit denen Belangen des Datenschutzes Rechnung getragen werden soll. Besonders hervorzuheben sind folgende Punkte:

Die Gestaltung technischer Einrichtungen muss sich an dem Ziel ausrichten, dass so wenige personenbezogene Daten wie möglich erhoben, verarbeitet und genutzt werden;

die Rundfunkveranstalter müssen die Nutzung und Bezahlung von Rundfunkangeboten anonym oder unter Pseudonym ermöglichen, so weit dies technisch möglich und zumutbar ist;

personenbezogene Daten über die Inanspruchnahme einzelner Sendungen dürfen für Abrechnungszwecke nur gespeichert werden, wenn ein Einzelnachweis verlangt wird;

wie bereits im Mediendienstestaatsvertrag enthält auch der Entwurf des Rundfunkstaatsvertrags eine Vorschrift zum Datenschutzaudit, d. h. Veranstalter können ihr Datenschutzkonzept und ihre technischen Einrichtungen von unabhängigen Gutachtern prüfen und das Prüfungsergebnis veröffentlichen lassen.

Die Datenschutzbeauftragten halten diese Grundsätze für geeignet, eine datenschutzgerechte Nutzung digitaler Fernsehangebote zu ermöglichen. Die technischen Möglichkeiten, diesen datenschutzrechtlichen Vorgaben zu entsprechen, sind gegeben. Die Datenschutzbeauftragten konnten sich bereits 1996 hiervon praktisch überzeugen. Die Systementscheidung von Veranstaltern für einen Decodertyp, der möglicherweise weniger geeignet ist, die Datenschutzanforderungen zu erfüllen, kann kein Maßstab für die Angemessenheit dieser Anforderungen sein, wenn zugleich andere Geräte ihnen ohne Probleme genügen.

Der Forderung von Inhabern von Verwertungsrechten, einen Nachweis über die Inanspruchnahme von pay-per-view-Angeboten vorzulegen, kann ohne Personenbezug - etwa durch zertifizierte Zähleinrichtungen oder den Einsatz von Pseudonymen - entsprochen werden.

Die Datenschutzbeauftragten bitten deshalb die Ministerpräsidentin und die Ministerpräsidenten der Länder, an den datenschutzrechtlichen Regelungen des Entwurfs fest zu halten. Damit würden das bisherige Datenschutzniveau für die Fernsehnutzung im digitalen Zeitalter abgesichert und zugleich die Vorschriften für den Bereich des Rundfunks und der Mediendienste harmonisiert.

Die Datenschutzbeauftragten fordern die Rundfunkveranstalter und Hersteller auf, den Datenschutz bei der Gestaltung von digitalen Angeboten schon jetzt zu berücksichtigen.

II. Epidemiologie und Datenschutz

Deutsche Arbeitsgemeinschaft für Epidemiologie (DAE)

Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Epidemiologie und Datenschutz

(Umlaufbeschluss der Konferenz der Datenschutzbeauftragten des Bundes und der Länder im Mai 1998)

Inhaltsübersicht:

Epidemiologie und Datenschutz

Redaktion:

Wichmann, H. E.;
Raspe, H. H.;
Jöckel, K. H.

für die Deutsche Arbeitsgemeinschaft für Epidemiologie;

Hamm, R.;
Wellbrock, R.

für den Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder

Einleitung

Die epidemiologische Forschung zielt nicht auf personenbezogene, sondern auf bevölkerungsbezogene wissenschaftliche Aussagen. Hierbei stützt sie sich jedoch in der Regel auf personenbezogene Daten zum Gesundheitszustand der Probanden, soziodemographische Angaben, Informationen über Risikofaktoren und oftmals medizinische Untersuchungsbefunde und Ergebnisse aus der Analyse biologischer Materialien. Die individuellen Untersuchungsergebnisse werden üblicherweise den Probanden mitgeteilt. Zur Durchführung der Forschungsprojekte werden vielfach Namen und Anschriften zur Kontaktaufnahme benötigt. Darüber hinaus muss eine korrekte Zuordnung von Follow-up-Ergebnissen sowie die Zusammenführung von Daten aus verschiedenen Quellen sichergestellt werden.

Epidemiologie und Datenschutz stehen traditionell im Spannungsfeld des Schutzes der Persönlichkeitsrechte der von der Datenverarbeitung Betroffenen und dem wissenschaftlichen Anliegen, durch das Auswerten von Gesundheitsdaten zu wichtigen und auf andere Weise nicht erreichbaren Kenntnissen zu gelangen.

Im Anschluss an eine Diskussion der datenschutzrechtlichen Fragen zwischen der Deutschen Forschungsgemeinschaft und dem Arbeitskreis Wissenschaft der Konferenz der Datenschutzbeauftragten des Bundes und der Länder haben Epidemiologen und Datenschützer versucht, typische Problemfelder zu identifizieren und zu gemeinsamen Lösungsvorschlägen zu kommen. Die folgenden Vorschläge sollen den mit Datenschutzfragen bei epidemiologischen Studien befassten Wissenschaftlern, Datenschützern, Ethikkommissionen, Behörden und Forschungsförderern zur Information und Orientierung dienen, um Probleme zu vermeiden, die durch fehlende Kenntnis der datenschutzrechtlichen Vorschriften, ungeeignet formulierte Einverständniserklärungen oder durch eine falsche oder übervorsichtige Interpretation der Rechtsvorschriften zur Datenübermittlung für Forschungszwecke etc. bedingt sind.

1. Rechtliche Rahmenbedingungen für die Forschung mit personenbezogenen Daten

1.1 Forschung mit anonymisierten Daten

Die datenschutzrechtlichen Bestimmungen finden nur Anwendung, wenn für ein Forschungsprojekt personenbezogene Daten benötigt werden. Forschung mit anonymisierten Daten ist jederzeit ohne datenschutzrechtliche Vorgaben möglich. Ob es sich im konkreten Fall um personenbezogene oder um anonymisierte Daten handelt, bedarf allerdings sorgfältiger Prüfung. § 3 Abs. 7 BDSG enthält eine gesetzliche Definition des Anonymisierens. Dieser Definition zufolge ist Anonymisieren das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können (sog. "faktische Anonymisierung"). Anonymisierung wird in der wissenschaftlichen bzw. datenschutzrechtlichen Diskussion ganz überwiegend im Sinne einer faktischen Anonymisierung verstanden. Einzelangaben sind z. B. dann keine anonymisierten Daten, wenn beim Forschungsinstitut bzw. beim Forscher lediglich eine organisatorische Trennung der Hilfsmerkmale von den übrigen Daten vorgenommen wurde oder wenn lediglich Name und Adresse der Betroffenen weggelassen wurden und die Betroffenen anhand der weiteren Angaben noch identifizierbar sind. Auch aggregierte Daten können nicht immer als anonymisiert qualifiziert werden. Im Einzelfall muss eine Risikoanalyse unter Berücksichtigung insbesondere des eventuellen Wertes der in Frage stehenden Daten für potentielle Interessenten sowie der dem Empfänger oder den potentiellen Interessenten zur Verfügung stehenden Ressourcen (Zusatzwissen, technische Möglichkeiten der Datenverarbeitung etc.) durchgeführt werden.

In einigen wenigen Bundesländern wird Anonymisierung im Sinne einer absoluten Anonymisierung verstanden, d.h. Einzelangaben werden nur dann als anonym qualifiziert, wenn sie unter keinen Umständen mehr zuzuordnen sind.

1.2 Forschung mit Einwilligung der Betroffenen

Personenbezogene Daten können im Rahmen der epidemiologischen Forschung auf der Basis einer Einwilligung der Betroffenen verarbeitet werden. Nach den datenschutzrechtlichen Regelungen muss die Einwilligung der Betroffenen bestimmte inhaltliche und formale Voraussetzungen erfüllen, damit sie rechtswirksam ist. Insbesondere müssen die Betroffenen über die vorgesehene Verarbeitung ihrer Daten informiert werden (Träger und Leiter des Forschungsprojekts, Zweck des Forschungsvorhabens, Art und Weise der Datenverarbeitung, Personenkreis, der von den personenbezogenen Daten Kenntnis erhält, Zeitpunkt der Löschung der personenbezogenen Daten etc.), damit sie die Tragweite ihrer Entscheidung erkennen können. Die Einwilligung muss in der Regel schriftlich erteilt werden, die gesetzlichen Regelungen sehen jedoch Ausnahmen vor. Ferner ist ein Hinweis erforderlich, dass die Einwilligung freiwillig ist, aus der Verweigerung der Einwilligung keine Nachteile entstehen und ein Widerruf der Einwilligung möglich ist. Einzelheiten sind den jeweils einschlägigen Regelungen zu entnehmen.

Verfügt die Forschungsstelle nicht über die Namen und Adressen der Personen, bei denen Einwilligungen eingeholt werden sollen, und kann sie sich diese Daten aufgrund der rechtlichen Regelungen (z. B. Meldegesetz) nicht beschaffen, so kann die Forschungsstelle die Betroffenen in der Weise kontaktieren, dass sie ihre Anschreiben, Merkblätter etc. in verschlossenen Umschlägen der Stelle übergibt, die über

die Daten verfügt, damit letztere auf die Umschläge Namen und Adressen schreibt und die Anschreiben dann versendet. Auf diese Weise wird vermieden, dass die Daten Dritten zur Kenntnis gelangen. Dabei sollte für die Betroffenen in dem Anschreiben eindeutig erkennbar sein, dass ihre geschützten Daten von der Stelle, die über die Daten verfügt, nicht an die forschende Stelle weitergegeben wurden.

1.3 Forschung mit personenbezogenen Daten ohne Einwilligung der Betroffenen

Das Grundgesetz gewährleistet das Recht auf informationelle Selbstbestimmung als Bestandteil des allgemeinen Persönlichkeitsrechts im Sinne von Artikel 2 i.V.m. Artikel 1 Grundgesetz. Ebenso gewährleistet das Grundgesetz die Freiheit von Wissenschaft und Forschung in Artikel 5 Grundgesetz. Diese beiden Grundrechte können bei Forschungsvorhaben, für die - zumindest vorübergehend - personenbezogene Daten benötigt werden, miteinander in Konflikt geraten. In dieser Situation ist es -wie auch bei anderen Grundrechtskonflikten - in erster Linie Aufgabe des Gesetzgebers, diese potentiellen Konflikte so zu regeln, dass beide Grundrechte möglichst weit gehend realisiert werden können. Der Gesetzgeber muss die rechtlichen Rahmenbedingungen festlegen, unter denen personenbezogene Daten zu Forschungszwecken ohne Einwilligung der Betroffenen verwendet werden dürfen. Dabei sind auch die besonderen Schweigepflichten wie z. B. die ärztliche Schweigepflicht i.S. der Berufsordnung und des § 203 StGB zu beachten. Nach der Rechtsprechung des Bundesverfassungsgerichts ist eine Einschränkung des Rechts auf informationelle Selbstbestimmung nur im überwiegenden Allgemeininteresse und unter Beachtung des Grundsatzes der Verhältnismäßigkeit zulässig. Die Verarbeitung personenbezogener Daten muss für den angestrebten Zweck geeignet und notwendig sein und es darf keine Alternative geben, die die Betroffenen weniger belastet (z. B. Anonymisierungs- bzw. Pseudonymisierungsverfahren, Einwilligung der Betroffenen).

Gesetzliche Forschungsregelungen, die das Recht auf informationelle Selbstbestimmung und die Freiheit von Wissenschaft und Forschung in diesem Sinne zuordnen, sind z. B. in Landeskrankenhausgesetzen, Meldegesetzen, im Sozialgesetzbuch X, Krebsregistergesetzen, im Bundesdatenschutzgesetz und in Landesdatenschutzgesetzen enthalten. Entgegen dem allgemeinen Grundsatz der Zweckbindung personenbezogener Daten können nach diesen Regelungen unter bestimmten Voraussetzungen Daten, die zu einem anderen Zweck als wissenschaftlicher Forschung erhoben wurden, zu Forschungszwecken weiterverwendet werden.

2. Forschungsansätze in der Epidemiologie, Datenbedarf und Rechtsgrundlagen der Datenverarbeitung

Die Epidemiologie ist die Lehre von der Verteilung der Krankheiten und ihrer Risikofaktoren in der Bevölkerung. Aussagen epidemiologischer Forschung betreffen nicht das Individuum, sondern eine Bevölkerungsgruppe. Daher werden personenbezogene Daten nur für die Datenerfassung und ggf. spätere Kontaktaufnahmen sowie für die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen benötigt.

Als wichtigste epidemiologische Studientypen sind beispielhaft anzusehen:

Bei Querschnittserhebungen wird typischerweise einmalig eine Befragung und/oder Untersuchung

von Probanden durchgeführt. Diese werden persönlich um ihr Einverständnis gebeten. Die epidemiologische Fragestellung umfasst z. B. die Charakterisierung von Erkrankungshäufigkeiten in der untersuchten Bevölkerungsgruppe oder den Zusammenhang zwischen dem Auftreten von Erkrankungen und Risikofaktoren. Aus datenschutzrechtlicher Sicht sind hier – wie auch bei den anderen Studienformen – die formalen und inhaltlichen Voraussetzungen der Einwilligungserklärung der Betroffenen zu beachten, ferner die jeweils einschlägigen Vorschriften zur Verarbeitung und Nutzung personenbezogener Daten durch die Forschungseinrichtungen (z. B. § 40 BDSG).

Als zweiter Studientyp ist die Kohortenstudie zu nennen. Hierbei werden - z. B. ausgehend von einer Querschnittstudie - wiederholt Untersuchungen an denselben Probanden durchgeführt. Für diese Follow-up-Untersuchungen ist es erforderlich, personenbezogene Daten zu speichern, Anschriften zu aktualisieren etc. Diese Datenverarbeitung muss von den Einwilligungserklärungen umfasst sein. Als epidemiologische Fragestellungen werden das Auftreten neuer Erkrankungen oder bestimmter Todesursachen im Zusammenhang mit bestimmten Risikofaktoren bearbeitet. Im letzteren Fall ist es zusätzlich erforderlich, über Einwohnermeldeämter und Gesundheitsämter den Vitalstatus sowie im Falle des Versterbens die Todesursache zu erheben. Als Rechtsgrundlage hierfür kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.

Einen Spezialfall von Kohortenstudien stellen retrospektive Kohortenstudien (mit zurückverlagertem Beginn) dar, die insbesondere im Bereich der Berufsepidemiologie häufig eingesetzt werden. Bei solchen Studien wird typischerweise aufgrund von betrieblichen Unterlagen die Exposition gegenüber bestimmten Arbeitsstoffen am Arbeitsplatz erhoben. Häufig interessiert das Auftreten von Krebserkrankungen oder das Versterben an bestimmten Todesursachen im Zusammenhang mit den beruflichen Expositionen. Hierbei ist es nicht ungewöhnlich, dass die Personen selbst nicht befragt werden, sondern dass ihre Exposition aus den betrieblichen Unterlagen bestimmt wird und die Krebserkrankung oder Todesursache durch Auswertung eines Krebsregisters oder über Einwohnermeldeamt und Gesundheitsamt in Erfahrung gebracht wird. Als Rechtsgrundlage für die Verarbeitung personenbezogener Daten kommen die gesetzlichen Forschungsregelungen oder die Einwilligung der Betroffenen in Betracht.

Als weiterer epidemiologischer Studientyp ist die Fall-Kontroll-Studie zu nennen. Hierbei werden als Fälle Personen mit bestimmten Erkrankungen bezeichnet, die Kontrollpersonen gegenübergestellt werden. Fälle und Kontrollen werden im Hinblick auf in der Vergangenheit liegende Risikofaktoren befragt. Häufig ist es sinnvoll, Fälle aus Registern, z. B. Krebsregistern, einzubeziehen. Als Rechtsgrundlage kommen die gesetzlichen Forschungsregelungen, z. B. in Krebsregistergesetzen, oder die Einwilligung der Betroffenen in Betracht.

3. Typische Problemfelder

3.1 Zweckbindung von personenbezogenen Daten

Problem:

Personenbezogene Daten werden auf der Grundlage einer Einwilligung der Betroffenen oder einer gesetzlichen Forschungsregelung zu einem bestimmten Zweck, d.h. für eine konkrete epidemiologische Studie, erhoben. Aus wissenschaftlicher Sicht kann es allerdings später wichtig werden, diese Daten für die Bearbeitung neuer Fragestellungen zu nutzen, die zum Zeitpunkt der Einwilligungserklärung der Betroffenen bzw. der Übermittlungen der Daten noch nicht bekannt waren und daher in die Angaben zum Zweck der Verwendung der Daten nicht einbezogen wurden. Eine erneute Kontaktierung der Probanden ist häufig nicht möglich oder wäre mit zusätzlichem hohem Aufwand und Kosten verbunden und könnte wegen Umzug, Tod, Desinteresse etc. der Betroffenen auch zu Problemen im Hinblick auf die Repräsentativität der Daten führen.

Lösungsansätze:

So weit es sich um anonymisierte Daten handelt, unterliegt eine Zweckänderung der Daten keinen rechtlichen Beschränkungen. Die datenschutzrechtlichen Regelungen sind nicht anzuwenden. Dies gilt entsprechend für die Verwendung biologischer Materialien.

Es besteht die Möglichkeit, Einwilligungserklärungen so zu formulieren, dass eine eventuelle inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfasst ist. Grundsätzlich muss eine Einwilligungserklärung hinreichend bestimmt sein. Die Anforderungen an die Vollständigkeit und Präzision der Einwilligungserklärungen können jedoch je nach der konkreten Verarbeitungssituation variieren. Bei der Verarbeitung personenbezogener Daten für eine wissenschaftliche Studie ist eine weitere Formulierung des Zwecks vertretbar und angemessen. Es ist die Entscheidung der Betroffenen, inwieweit sie auch eine Einwilligungserklärung mit einer weiteren Formulierung des Zwecks der Studie unterschreiben, d.h. es handelt sich um eine Frage der Akzeptanz. Die Einwilligungserklärung kann auch verschiedene Varianten der Verwendung der Daten enthalten, über die die Betroffenen entscheiden.

Bei einer Übermittlung personenbezogener Daten auf der Grundlage einer gesetzlichen Forschungsregelung ist es vertretbar und angemessen, den Zweck der Übermittlung der Daten (d.h. die Darstellung des Forschungsvorhabens) so zu formulieren, dass eventuelle inhaltliche Änderungen bzw. Ausweitungen der Fragestellungen der Studie mit umfasst sind.

In Betracht kommt auch eine Anwendung der datenschutzrechtlichen Regelungen über die Zweckänderung personenbezogener Daten. Die rechtlichen Voraussetzungen für eine Zweckänderung sind im Einzelfall zu prüfen.

Verfahrensrechtliche Lösungen wie z. B. Einschaltungen von Ethikkommissionen, Datenschutzbeauftragten etc. kommen im Regelfall nur dann in Betracht, wenn Rechtsvorschriften vorhanden sind, die grundsätzlich eine Zweckänderung der Daten unter bestimmten Voraussetzungen zulassen, denn weder Ethikkommissionen noch Datenschutzbeauftragte können ihre Entscheidung an die Stelle der Entscheidung der Betroffenen setzen.

3.2 Löschung der Daten nach Beendigung des Forschungsvorhabens

Problem:

Es ist offen, in welchem Umfang die Daten nach Beendigung des Forschungsvorhabens gelöscht werden müssen.

Lösungsansätze:

So weit die Daten anonymisiert sind, sind die datenschutzrechtlichen Regelungen nicht anzuwenden und die weitere Verarbeitung der Daten unterliegt keinen rechtlichen Beschränkungen.

Werden personenbezogene Daten verarbeitet, sollte der Zeitpunkt der Löschung der personenbezogenen Daten in dem Text der Einwilligungserklärung bzw. dem Antrag auf Übermittlung der Daten konkret benannt werden. Ist im Einzelfall eine Speicherung anonymisierter Daten für die wissenschaftliche Nachprüfbarkeit der Forschungsergebnisse nach ihrer Publikation nicht ausreichend. so kann eine Speicherung der personenbezogenen Daten für einen bestimmten Zeitraum nach der Publikation der Forschungsergebnisse zur wissenschaftlichen Nachprüfbarkeit der Forschungsergebnisse zulässig sein. Der Zeitpunkt für die Löschung der personenbezogenen Daten sollte in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst konkret benannt werden.

3.3 Weitergabe anonymisierter Daten

Problem:

In einem Forschungsvorhaben erweist es sich als sinnvoll, anonymisierte Daten aus mehreren Studien zu poolen, d.h. zusammenzuführen und gemeinsam statistisch auszuwerten, weil sich für viele Fragestellungen nur dadurch ausreichend große Fallzahlen erreichen lassen. Auch eine Weitergabe von anonymisierten Daten in Form von Public Use Files kann sinnvoll sein, um die Daten anderen Wissenschaftlern für ihre Forschung zugänglich zu machen.

Lösungsansätze:

Grundsätzlich können anonymisierte Daten ohne rechtliche Beschränkungen weitergegeben werden. Es muss allerdings im Einzelfall geprüft werden, ob es sich tatsächlich um anonymisierte Daten handelt und ob die Daten auch nach der Zusammenführung mit den Daten aus den anderen Studien noch als anonymisiert qualifiziert werden können. Eine Zusammenführung anonymisierter Daten aus mehreren Studien führt häufig dazu, dass eine Deanonymisierung der Daten noch schwieriger wird. Im Einzelfall kann es jedoch durchaus auch die Konstellation geben, dass anonymisierte Daten durch ihre Zusammenführung mit Daten aus anderen Studien leichter deanonymisiert werden können und dann u.U. als personenbezogen qualifiziert werden müssen. In diesem Fall sind die datenschutzrechtlichen Regelungen zu beachten.

Eine Übermittlung personenbezogener Daten ist nicht in jedem Fall ausgeschlossen. Es gilt das oben unter 3.1 Gesagte entsprechend.

3.4 Optimale Gestaltung der Einverständniserklärung bzw. des Antrags auf Übermittlung der Daten

Problem:

Einerseits sollten in der Einverständniserklärung bzw. in dem Antrag auf Übermittlung der Daten möglichst präzise die zu untersuchende Fragestellung, die Vorgehensweise und die an der Studie beteiligten Institutionen angegeben werden. Andererseits kann es sich im Laufe einer Studie ergeben, dass Kooperationspartner wechseln und sich Fragestellungen erweitern bzw. neue Fragestellungen auftauchen. Wie kann dies in der Einverständniserklärung bzw. in dem Antrag optimal berücksichtigt werden?

Lösungsansätze:

Die Formulierung des Zwecks der epidemiologischen Studie kann so erfolgen, dass eine evtl. inhaltliche Änderung bzw. Ausweitung der Fragestellungen der Studie mit umfasst ist (vgl. oben 3.1).
Die Daten verarbeitende Stelle - im Regelfall die Institution (Klinikum, Institut etc.) - muss in der Einwilligungserklärung bzw. in dem Antrag auf Übermittlung personenbezogener Daten konkret und verbindlich benannt werden. Aus datenschutzrechtlicher Sicht ist es von zentraler Bedeutung, dass die Verantwortlichkeit für die personenbezogenen Daten dauerhaft klar geregelt ist und der Bürger eindeutig darüber informiert ist, an wen er sich wo bei Auskunftsersuchen, Widerruf seiner Einwilligung etc. wenden kann. Die Namen der Kooperationspartner müssen nur dann konkret aufgeführt werden.

Im Einzelfall ist es auch möglich, eine Klausel dahingehend aufzunehmen, daß Abweichungen von der angegebenen Vorgehensweise und Erweiterungen der Fragestellungen nur nach Rücksprache mit dem zuständigen Datenschutzbeauftragten bzw. der Ethikkommission erfolgen.

3.5 Verknüpfung personenbezogener Datensätze (record linkage), z. B. bei Kohortenstudien

Problem:

Es soll eine Studie durchgeführt werden, bei der ein Abgleich verschiedener Datenbestände vorgenommen wird, die Betroffenen jedoch zu keinem Zeitpunkt direkt kontaktiert bzw. um Einwilligung gebeten werden. Ein Beispiel hierfür ist eine Studie, bei welcher die Expositionsbedingungen am Arbeitsplatz aus betrieblichen Unterlagen der dort tätigen Arbeitnehmer zusammengestellt werden. Die Erhebung der aufgetretenen Erkrankungen erfolgt über vorhandene Krankheitsregister (z.B. Krebsregister) oder über Einwohnermeldeämter und Gesundheitsämter zur Erhebung des Vitalstatus und der Todesursache.

Lösungsansätze:

In einzelnen gesetzlichen Regelungen wie z.B. Krebsregistergesetzen ist ein Abgleich verschiedener Datenbestände vorgesehen. Im übrigen sehen die bundes- bzw. landesrechtlichen Regelungen - mit Unterschieden im einzelnen - grundsätzlich die Möglichkeit von Datenübermittlungen durch Betriebe, Einwohnermeldeämter, Gesundheitsämter, Krebsregister etc. vor (vgl. z.B. § 28 Abs. 2 Nr. 2 BDSG, Meldegesetze, Gesetze über den öffentlichen Gesundheitsdienst, Krebsregistergesetze, Forschungsregelungen im Bundesdatenschutzgesetz und in den Landesdatenschutzgesetzen). Die rechtlichen Voraussetzungen dieser Übermittlungsbestimmungen müssen im Einzelfall geprüft werden.

Vor der Durchführung einer Studie sollte der Einsatz eines Treuhänders, d.h. eines vertrauenswürdigen Dritten, geprüft werden, der insbesondere personenbezogene Daten aus verschiedenen Quellen zuordnet, speichert und anonymisiert an die Forschungsinstitution übermittelt. Die Übermittlung personenbezogener Daten an einen Treuhänder bedarf ebenso wie die Übermittlung personenbezogener Daten an die Forschungsinstitution selbst einer Rechtsgrundlage. Der Einsatz eines Treuhänders kann jedoch im Einzelfall den Eingriff in das Recht der Betroffenen auf informationelle Selbstbestimmung minimieren, indem der Kreis derjenigen Personen, die personenbezogene Daten zur Kenntnis erhalten, reduziert wird und die Datensicherheit umfassender gewährleistet wird. Diese Aspekte haben Relevanz für die in vielen Forschungsregelungen vorgesehene Abwägung zwischen den schutzwürdigen Belangen der Betroffenen und dem öffentlichen Interesse an der Durchführung des Forschungsvorhabens.

3.6 Nutzung der amtlichen Statistik

Problem:

Häufig werden von den statistischen Ämtern des Bundes und der Länder in der Praxis nur Daten übermittelt, bei denen eine Mindestzahl auftretender Konstellationen pro Zelle erfüllt ist. Hierdurch werden bestimmte Aussagen unmöglich gemacht, z. B. die Unterteilung einer Untersuchungsgruppe nach Altersklassen oder nach genaueren diagnostischen Einheiten wie Todesursachen.

Lösungsansätze:

Die statistischen Ämter des Bundes und der Länder dürfen faktisch anonymisierte Einzelangaben für wissenschaftliche Vorhaben an Hochschulen und andere Einrichtungen mit der Aufgabe unabhängiger wissenschaftlicher Forschung übermitteln, wenn die Empfänger Amtsträger, für den öffentlichen Dienst Verpflichtete oder nach § 16 Abs. 7 Bundesstatistikgesetz Verpflichtete sind (§ 16 Abs. 6 BStatG). Die Daten sind zu löschen, sobald das Vorhaben durchgeführt ist, eine verbindliche Löschungsfrist besteht nicht (§ 16 Abs. 8 BStatG).

Es besteht die Möglichkeit, aus bereits vorliegenden Individualdaten faktisch anonymisierte Einzelangaben zu bestellen. Von diesem Weg wird jedoch häufig aus Kostengründen Abstand genommen. Für einige Bereiche sind faktisch anonyme Daten auf Vorrat erstellt worden, z.B. aus dem Mikrozensus 1995 und der Einkommens- und Verbrauchsstichprobe 1993. Einzelangaben aus solchen Beständen können gegen geringe Gebühr bezogen werden, die breite Anwendung dieser Verfahren wird aber durch Geldmangel behindert.

Leichter verfügbar sind statistische Tabellen, die i.a. dadurch anonymisiert sind, daß Felder mit geringen Belegungen so zusammengefaßt wurden, daß Zahlen kleiner als 3 nicht mehr auftreten. Dies ist für Forschungszwecke oft hinderlich. Soweit jedoch die Angaben aus Feldern mit zu geringer Belegung nicht mehr erkennen lassen, als nach § 16 Abs. 6 BStG übermittelt werden darf, und auch die weiteren Bedingungen dieser Vorschrift erfüllt werden, bestehen keine datenschutzrechtlichen Bedenken gegen die Übermittlung auch solcher Tabellen mit faktisch anonymisierten Einzelangaben.

3.7 Aufbewahrung von Daten der amtlichen Statistik

Problem:

Die Löschung älterer Datenbestände kann der epidemiologischen Forschung unwiederbringlich Grundlagen entziehen.

Lösungsansätze:

Abgesehen von den Hilfsmerkmalen (insbesondere Namen und Anschriften) gibt es i.a. keine gesetzlichen Löschungsfristen für statistische Einzelangaben. Die Löschungspraxis richtet sich nach der Einschätzung des zu erwartenden Nutzens aus der weiteren Aufbewahrung im Verhältnis zu deren Kosten. Datenschutzrechtlich zulässig wäre eine weitere Speicherung statistischer Einzelangaben auch für zukünftig erwartete, aber noch nicht im einzelnen bekannte Zwecke. Vor Löschung der Daten sind diese nach den jeweils geltenden archivrechtlichen Bestimmungen den zuständigen Archiven anzubieten. Zur Dauer der Speicherung der Daten bei den statistischen Ämtern bzw. bei den Archiven sollte aus dem Wissenschaftsbereich der Bedarf dargelegt werden. Die Aufbewahrung der Totenscheine (im Original) richtet sich nach dem jeweiligen Landesrecht.

3.8 Nutzung von Krebsregistern für Fall-Kontroll-Studien

Problem:

Bei Fall-Kontroll-Studien wird häufig ein (möglichst repräsentativer) Zugang zu bestimmten Erkrankungsgruppen benötigt. Dieser kann unter hohen Kosten auf der Grundlage von Einwilligungen der Betroffenen oder gesetzlichen Forschungsregelungen über Krankenhäuser erfolgen, in denen diese Patienten behandelt werden. Ein effektiverer und vollständigerer Zugang ist aber derjenige über Krankheitsregister (z. B. Krebsregister). Der Zugang über das Register dient dabei nur der Auffindung des Patienten und der Kontaktaufnahme mit ihm, alles weitere kann durch die Einverständniserklärung der beteiligten Personen abgedeckt werden. Diesen Patienten werden dann Kontrollpersonen aus der Bevölkerung gegenübergestellt, die auf anderem Wege kontaktiert und in die Studie einbezogen werden.

Lösungsansätze:

Gemäß § 8 des Krebsregistergesetzes des Bundes (KRG) können für Maßnahmen des Gesund-

heitsschutzes und bei wichtigen und auf andere Weise nicht durchzuführenden, im öffentlichen Interesse stehenden Forschungsaufgaben die zuständigen Behörden der Vertrauensstelle des Krebsregisters die Abgleichung Personen identifizierender Daten mit Daten des Krebsregisters und die Entschlüsselung der erforderlichen verschlüsselten Identitätsdaten und deren Übermittlung im erforderlichen Umfang genehmigen.

Vor der Übermittlung personenbezogener Daten hat die Vertrauensstelle über den meldenden behandelnden Arzt oder Zahnarzt die schriftliche Einwilligung des Patienten einzuholen. Ist der Patient verstorben, hat die Vertrauensstelle vor der Datenübermittlung die schriftliche Einwilligung des nächsten Angehörigen einzuholen, soweit dies ohne unverhältnismäßigen Aufwand möglich ist.

Die Länder können in ihren Gesetzen zur Ausführung des Krebsregistergesetzes abweichende Regelungen treffen (§ 13 Abs. 5 Nr. 2 KRG). Einige Länder haben vom Krebsregistergesetz des Bundes abweichende datenschutzrechtliche Modelle (z. B. keine Aufgliederung des Registers in Vertrauensstelle und Registerstelle) gewählt. Im Einzelfall sind die einschlägigen Übermittlungsbestimmungen zu prüfen und zu beachten.

3.9 Datenschutzfragen bei bundesweiten Studien

Problem:

Bei Studien, die in mehreren Bundesländern stattfinden, sind häufig die unterschiedlichen datenschutzrechtlichen Regelungen der Bundesländer zu berücksichtigen.

Lösungsansätze:

Zur Vereinfachung des Verfahrens kann der Studienleiter den für ihn zuständigen Datenschutzbeauftragten bzw. denjenigen Datenschutzbeauftragten, in dessen Bundesland die zentrale Speicherung der Daten des Forschungsprojekts erfolgen soll, darum bitten, die Stellungnahmen der anderen Datenschutzbeauftragten (soweit von dem konkreten Forschungsprojekt betroffen) zu koordinieren.

III. Entschließungen der 56. Konferenz am 5./6. Oktober 1998 in Wiesbaden

Verweigerung der Auskunft durch das Bundesamt für Finanzen auf Anfragen Betroffener über ihre Freistellungsaufträge

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Datenschutzbeauftragten des Bundes und der Länder betonen das Recht der Bürgerinnen und Bürger auf Auskunft über ihre Daten auch gegenüber der Finanzverwaltung (§ 19 BDSG). Die Betroffenen haben Anspruch, von dem Bundesamt für Finanzen Auskunft über die Freistellungsaufträge zu erhalten, die sie ihrer Bank im Zusammenhang mit dem steuerlichen Abzug von Zinsen erteilt haben.

Der Bundesbeauftragte für den Datenschutz hat die Verweigerung der Auskünfte gegenüber dem Bundesministerium der Finanzen beanstandet und dieses aufgefordert, den entsprechenden Erlass an das Bundesamt aufzuheben. Bisher hat das Ministerium in der Sache allerdings nicht eingelenkt.

Für die Betroffenen ergibt sich hierdurch ein unhaltbarer Zustand. Ihnen wird die Auskunft zu Unrecht vorenthalten.

Die Datenschutzbeauftragten der Länder unterstützen mit Nachdruck die Forderung des Bundesbeauftragten für den Datenschutz gegenüber dem Bundesministerium der Finanzen, seinen Erlass an das Bundesamt für Finanzen aufzuheben und dieses anzuweisen, dem Auskunftsanspruch der Auftraggeber von Freistellungsaufträgen nachzukommen.

Dringlichkeit der Datenschutzmodernisierung

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder begrüßt und unterstützt grundsätzlich die vom 62. Deutschen Juristentag (DJT) im September 1998 in Bremen gefassten Beschlüsse zum Umgang mit Informationen einschließlich personenbezogener Daten. Von den gesetzgebenden Körperschaften erhofft sich die Konferenz die Berücksichtigung dieser Beschlüsse bei der nunmehr dringend erforderlichen Umsetzung der EG-Datenschutzrichtlinie in Bundes- und Landesrecht.

Insbesondere betont die Konferenz folgende Punkte:

Die materiellen Anforderungen des Datenschutzrechts sind angesichts der wachsenden Datenmacht in privater Hand auf hohem Niveau grundsätzlich einheitlich für den öffentlichen wie für den privaten Bereich zu gestalten.

Die analysiere Aufsicht für die Einhaltung des Datenschutzes im privaten Bereich muss in gleicher Weise unabhängig und weisungsfrei ausgestaltet werden wie die Datenschutzkontrolle bei öffentlichen Stellen.

Die Rechte der Bürgerinnen und Bürger sind zu stärken; als Voraussetzung für die Ausübung des Rechts auf informationelle Selbstbestimmung der Betroffenen sind die Verpflichtungen zu ihrer Information, Aufklärung und ihren Wahlmöglichkeiten ohne faktische Zwänge auszuweiten.

Ein modernisiertes Datenschutzrecht hat die Grundsätze der Datenvermeidung, des Datenschutzes durch Technik, der Zweckbindung der Daten und ihres Verwendungszusammenhangs in den Mittelpunkt zu stellen.

Zur Sicherstellung vertraulicher und unverfälschter elektronischer Kommunikation ist die staatliche Förderung von Verschlüsselungsverfahren geboten, nicht eine Reglementierung der Kryptographie.

Prüfungskompetenz der Datenschutzbeauftragten bei den Gerichten

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Datenschutzbeauftragten des Bundes und der Länder stellen fest, dass in der Praxis die Abgrenzung ihrer Zuständigkeiten bei den Gerichten immer wieder Anlass von Unsicherheiten ist. Sie weisen daher darauf hin, dass die Beschränkung der Prüfkompetenz bei den Gerichten einzig und allein den Zweck hat, den grundgesetzlich besonders geschützten Bereich der richterlichen Unabhängigkeit von Kontrollen freizuhalten.

Deshalb erstreckt sich die Kontrolle der Datenschutzbeauftragten bei den Gerichten u.a. auch darauf, ob die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherung getroffen und eingehalten werden, insbesondere bei automatisierter Datenverarbeitung.

Die Datenschutzbeauftragten des Bundes und der Länder halten eine gesetzliche Klarstellung für hilfreich, dass Gerichte der Kontrolle des Bundesbeauftragten bzw. der Landesbeauftragten für den Datenschutz unterliegen, so weit sie nicht in richterlicher Unabhängigkeit tätig werden.

Fehlende bereichsspezifische Regelungen bei der Justiz

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Derzeit werden in allen Bereichen der Justiz - bei Staatsanwaltschaften, Gerichten und Gerichtsvollziehern - im Zuge von Modernisierungsvorhaben umfassende Systeme der automatisierten Datenverarbeitung eingeführt mit der Folge, dass sensible personenbezogene Daten auch hier in viel stärkerem Maße verfügbar werden als bisher. Sogar die Beauftragung Privater mit der Verarbeitung sensibler Justizdaten wird erwogen. Gerade vor dem Hintergrund dieser vollkommen neuen Qualität der Datenverarbeitung in der Justiz wird deutlich, dass die Rechtsprechung des Bundesverfassungsgerichts zum so genannten Übergangsbonus hier keine tragfähige Grundlage für Eingriffe in die informationelle Selbstbestimmung mehr darstellen kann. Vielmehr müssen die Entscheidungen des Gesetzgebers den Maßstab für die weitere technische Ausgestaltung der Datenverarbeitung innerhalb der Justiz bilden und nicht umgekehrt. Dabei ist nicht nur für formell ausreichende Rechtsgrundlagen Sorge zu tragen. Auch Fragen der Datensicherheit und der Ordnungsmäßigkeit der Datenverarbeitung bedürfen der Regelung.

Seit dem Volkszählungsurteil des Bundesverfassungsgerichts sind 15 Jahre vergangen. Dennoch werden ausgerechnet im Bereich der Justiz sensible personenbezogene Daten nach wie vor ohne die vom Bundesverfassungsgericht geforderten bereichsspezifischen gesetzlichen Grundlagen erhoben und verarbeitet.

Die Datenschutzbeauftragten des Bundes und der Länder bekräftigen deshalb im Anschluss an ihren Beschluss der 48. Konferenz vom 26./27.09.1994 in Potsdam ihre wiederholten Forderungen zu bereichsspezifischen Regelungen bei der Justiz.

Zwar hat der Gesetzgeber in der abgelaufenen Legislaturperiode zumindest Regelungen über Datenerhebung, -verarbeitung und -nutzung im Strafvollzug sowie über die Datenübermittlung von Amts wegen durch Gerichte und Staatsanwaltschaften an Gerichte, Behörden und sonstige öffentlichen Stellen geschaffen.

Trotzdem sind in wichtigen Bereichen gesetzliche Regelungen weiterhin überfällig. Ausreichende gesetzliche Regelungen fehlen vor allem für

weite Bereiche der Datenverarbeitung im Strafverfahren, insbesondere in automatisierten Dateien namentlich die

- Übermittlung von Strafverfahrensdaten an nicht am Strafverfahren beteiligte dritte Stellen;

- Rechte der Betroffenen (nicht nur der Beschuldigten, sondern auch von Zeugen und sonstigen Personen, deren Daten gespeichert werden) in Bezug auf Daten, die im Zusammenhang mit einem Strafverfahren gespeichert werden.

Aufbewahrung von Akten, Karteien und sonstigen Unterlagen sowie die Dauer der Speicherung in automatisierten Dateien;

Datenübermittlung zu wissenschaftlichen Zwecken;

Datenverarbeitung in der Zwangsvollstreckung;

Datenverarbeitung im Jugendstrafvollzug;

Datenverarbeitung im Vollzug der Untersuchungshaft.

Der Gesetzgeber sollte daher in der kommenden Legislaturperiode zügig die notwendigen Novellierungen, für die zum Teil ja schon erhebliche Vorarbeiten geleistet worden sind, aufgreifen. Dabei ist nicht die jeweils geübte Praxis zu legalisieren, sondern es muss vorab unter datenschutzrechlichen Gesichtspunkten geprüft werden, welche Form der Datenerhebung und -verarbeitung in welchem Umfang erforderlich ist. Ferner hat der Gesetzgeber jeweils bereichsspezifisch zu prüfen, inwieweit Aufgaben der Justiz und damit verbundene Datenverarbeitungen Privaten übertragen werden dürfen.

Der Entwurf für ein "StVÄG 1996" erfüllt diese Voraussetzungen nicht, im Gegenteil fällt er teilweise hinter den bereits erreichten Standard der allgemeinen Datenschutzgesetze und anderer bereichsspezifischer Regelungen (wie z. B. dem Bundeszentralregistergesetz und den Polizeigesetzen der Länder) zurück.
Zu kritisieren sind vor allem:

Mangelnde Bestimmtheit der Voraussetzungen für Maßnahmen der Öffentlichkeitsfahndung

Unangemessen weite Auskunfts- und Akteneinsichtsmöglichkeiten für nicht Verfahrensbeteiligte

Unzureichende Regelungen über Inhalt, Ausmaß und Umfang von staatsanwaltlichen Dateien und Informationssystemen

Die Datenschutzbeauftragten halten es deshalb zum Schutz des Rechts des Einzelnen auf informationelle Selbstbestimmung für geboten, wegen der mit der Datenerhebung, Verarbeitung und Nutzung verbundenen Rechtseingriffe unverzüglich in der neuen Legislaturperiode bereichsspezifische Regelungen der materiellen Voraussetzungen sowie der organisatorischen und verfahrensrechtlichen Vorkehrungen zu schaffen, welche der Gefahr einer Verletzung des Persönlichkeitsrechtes der Bürgerinnen und Bürger entgegenwirken.

Weitergabe von Meldedaten an Adressbuchverlage und Parteien

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Bei den Datenschutzbeauftragten des Bundes und der Länder gehen viele Beschwerden ein, in denen deutlicher Unmut über veröffentlichte Daten in Adressbüchern und unverlangt erhaltene Werbesendungen geäußert wird. Vor Wahlen nehmen die Beschwerden noch zu. Überrascht stellten Betroffene fest, dass sie persönlich adressierte Wahlwerbung der Parteien bekommen. Ihnen ist unerklärlich, wie Adressbuchverlage und Parteien an ihre Adressen gekommen sind. Sie erhalten auf Anforderung Daten aus den kommunalen Melderegistern. Damit sind die Adressbuchverlage und Parteien gegenüber anderen gesellschaftlichen Gruppen privilegiert.

Dieser Umgang mit Meldedaten ist weder transparent noch angemessen. Die Konferenz tritt dafür ein, die Rechte der Bürgerinnen und Bürger zu verbessern. Die Information über die Widerspruchsmöglichkeit erreicht die Menschen häufig nicht. Vorzuziehen ist deshalb eine Einwilligungslösung. Sie würde das Grundrecht auf informationelle Selbstbestimmung konsequent umsetzen - erst fragen, dann handeln. Nach der Einwilligungslösung ist eine Erklärung informierter Bürgerinnen und Bürger gegenüber dem Meldeamt nötig, ob sie mit den Datenweitergaben an die genannten Empfänger einverstanden sind oder nicht.

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder empfiehlt den gesetzgebenden Körperschaften, künftig die Einwilligungslösung vorzusehen.

Entwicklungen im Sicherheitsbereich

(Entschließung der 56. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 5./6. Oktober 1998)

Die Konferenz der Datenschutzbeauftragten des Bundes und der Länder stellt fest, dass die Sicherheitsbehörden in den vergangenen Jahren umfangreiche zusätzliche Eingriffsbefugnisse erhalten haben. Demgegenüber fehlen in weiten Teilen Erkenntnisse über die Wirksamkeit und Grundrechtsverträglichkeit der Anwendung dieser Instrumente, wie z. B. bei der Schleppnetzfahndung und der Ausweitung der Telefonüberwachung.

Die Datenschutzbeauftragten des Bundes und der Länder erwarten vom Bundesgesetzgeber und der Bundesregierung, dass die Erforderlichkeit und die Wirksamkeit aller Eingriffsbefugnisse anhand objektiver Kriterien überprüft werden (Evaluierung).

C. Beschlüsse und Arbeitspapiere der Datenschutzbeauftragten der Europäischen Union (16./17. September 1998, Santiago de Compostela)

Entschließung der Europäischen Konferenz der Datenschutzbeauftragten gegen die Veröffentlichung herabsetzender Informationen im Internet

Die unabhängigen Datenschutzbehörden der Europäischen Union zusammen mit denjenigen von Island, Norwegen und der Schweiz, die sich im Anschluss an die 20. Internationale Konferenz in Santiago de Compostela am 16. und 17. September 1998 getroffen haben, sind überzeugt, dass das Internet als ein Mittel dienen kann, die Demokratie zu stärken, indem es den Bürgern erlaubt, besser an öffentlichen Debatten teilzunehmen, und indem es öffentliche Angelegenheiten höhere Publizität verschafft.

Sie machen darauf aufmerksam,

dass der Gebrauch eines Mittels wie des Internet zur Verbreitung und Sammlung von Informationen und die Folgen, die dies für die Grundwerte hat, die Anerkennung der Notwendigkeit von Garantien erfordert und

dass derartige Garantien international geschaffen werden müssen, ohne dass damit Hindernisse für die Meinungsfreiheit und das Recht auf Information errichtet werde.

Sie sind der Ansicht, dass auf der Basis der Grundsätze des Schutzes personenbezogener Daten, die in vielen Staaten bereits anerkannt sind und die auch für das Internet gelten, alle Staaten, uns insbesondere diejenigen, in denen die Nutzung der neuen Technologien am weitesten verbreitet ist, Maßnahmen zum Schutz personenbezogener Daten ergreifen und verstärken und eine internationale Kooperation fördern müssen, die auf den weltweit anerkannten Werten beruhen und die sicherstellen, dass die steigende Nutzung des Internet keine Folgen hervorbringt, die mit dem Schutz personenbezogener Daten und der Persönlichkeitsrechte nicht vereinbar sind.

Sie weisen insbesondere darauf hin,

dass Daten, die dafür missbraucht werden könnten, Personen Gefahren auszusetzen oder sie herabzusetzen, auf dem Internet nicht in einer Weise verbreitet werden dürfen, die einen solchen Missbrauch ermöglicht,

dass effektive rechtliche und technische Maßnahmen entwickelt werden sollten, die es den betroffenen Personen ermöglichen, die Nutzung ihrer personenbezogenen Daten selbst zu bestimmen und zu kontrollieren,

dass effektive Maßnahmen ergriffen werden sollten, um die Übereinstimmung mit den Prinzipien des Datenschutzes durch alle Beteiligten, die verantwortlich für die Verbreitung oder Sammlung personenbezogener Daten im Internet sind oder die technische Infrastruktur des Internet zur Verfügung stellen, sicherzustellen.

Arbeitspapier 12 der Gruppe nach Art. 29 der Datenschutzrichtlinie der EU

Übermittlungen personenbezogener Daten an Drittländer:

Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU

Von der Arbeitsgruppe am 24. Juli 1998 angenommen
(WP 12 - GD XV D/ 5025/ 98 - DE endgültig)

Inhaltsübersicht:

Einführung

Ziel diese Arbeitsunterlage ist es, die bislang geleistete Arbeit der nach Artikel 29 der Datenschutzrichtlinie eingesetzten Arbeitsgruppe von EU- Datenschutzbeauftragten

[Siehe

"Erste Leitlinien für die Übermittlung personenbezogener Daten in Drittländer - Mögliche Ansätze für eine Bewertung der Angemessenheit", von der Arbeitsgruppe am 26. Juni 1997 angenommene Diskussionsgrundlage;

Arbeitsunterlage: "Beurteilung der Selbstkontrolle der Wirtschaft: Wann ist sie ein sinnvoller Beitrag zum Niveau des Datenschutzes in einem Drittland?", von der Arbeitsgruppe am 14. Januar 1998 angenommen;

Arbeitsunterlage: "Erste Überlegungen zur Verwendung vertraglicher Bestimmungen im Rahmen der Übermittlungen personenbezogener Daten an Drittländer", von der Arbeitsgruppe am 22. April 1998 angenommen]

zu einer allgemeinen Übersicht über ihre Ansichten zu sämtlichen zentralen Fragen zusammenzufassen, die sich aus der Übermittlung personenbezogener Daten in Drittländer im Zusammenhang mit der Anwendung der Datenschutzrichtlinie der EU (95/46/EG) ergeben. Der Aufbau folgt dabei dem System, wie es für internationale Übermittlungen personenbezogener Daten in Artikel 25 und 26 der Richtlinie vorgesehen ist.

In Artikel 25 Absatz 1 ist der Grundsatz aufgeführt, dass die Mitgliedstaaten die Übermittlung in ein Drittland nur gestatten, wenn das betreffende Drittland ein angemessenes Schutzniveau gewährleistet. In Absatz 2 wird darauf verwiesen, dass "die Angemessenheit ... unter Berücksichtigung aller Um-

stände beurteilt" wird. Nach Absatz 6 kann die Kommission feststellen, dass bestimmte Länder ein angemessenes Schutzniveau gewährleisten. Kapitel 1 dieses Papiers ist dieser zentralen Frage des angemessenen Schutzniveaus gewidmet. Zunächst wird erklärt, was unter "angemessen" zu verstehen ist, und danach ein Rahmen für die Frage vorgestellt, wie die Angemessenheit des Schutzes im konkreten Fall beurteilt werden kann.

In Kapitel 2 und 3 wird dieser Ansatz weiterverfolgt. Kapitel 2 beschäftigt sich mit Übermittlungen in Länder, die das Übereinkommen Nr. 108 des Europarates ratifiziert haben, während Kapitel 3 Fragen im Zusammenhang mit Übermittlungen behandelt, bei denen der Schutz personenbezogener Daten hauptsächlich oder vollständig über Mechanismen der freiwilligen Selbstkontrolle und nicht auf gesetzlichem Wege erfolgt.

Fehlt das angemessene Schutzniveau im Sinne von Artikel 25 Absatz 2, so ist in Artikel 26 Absatz 2 der Richtlinie die Möglichkeit von Ad-hoc-Maßnahmen vorgesehen, die insbesondere vertraglicher Art sein und zur Festlegung angemessener Garantien führen können, auf deren Basis die betreffende Übermittlung erfolgen kann.

In Kapitel 4 des vorliegenden Beitrags werden die Umstände geprüft, unter denen vertragliche Lösungen geeignet erscheinen, und Empfehlungen zur möglichen Form und zum Inhalt dieser Lösungen gegeben.

Kapitel 5 beschäftigt sich mit der dritten und letzten Situation, die in der Richtlinie vorgesehen ist, d.h. bestimmten Fällen nach Artikel 26 Absatz 1, in denen vom Erfordernis des "angemessenen Schutzniveaus" praktisch abgewichen werden kann. Der genaue Umfang dieser Ausnahmen wird unter Zuhilfenahme von Beispielen von Fällen geprüft, in denen diese Möglichkeit genutzt werden kann bzw. dies nicht möglich erscheint.

Im abschließenden Kapitel 6 finden sich Bemerkungen zu Verfahrensfragen, die sich in Verbindung mit der Beurteilung der Angemessenheit (bzw. des Mangels an Angemessenheit) des Schutzniveaus und der Erzielung eines gemeinschaftsweit einheitlichen Ansatzes zu diesen Fragen ergeben.

Als Anhang sind mehrere anschauliche Fallstudien beigefügt, mit denen demonstriert werden soll, wie der im vorliegenden Dokument beschriebene Ansatz in der Praxis umgesetzt werden könnte.

Kapitel 1:

Bewertung der Angemessenheit des Schutzes

Was ist ein "angemessenes Schutzniveau"?

Sinn und Zweck des Datenschutzes ist es, Personen, deren Daten verarbeitet werden, Schutz zu gewährleisten. Erreicht wird dies durch eine Kombination von dem Betroffenen eingeräumten Rechten und bestimmten Pflichten für die Stellen, bei denen die Daten verarbeitet werden oder in deren Zuständigkeit die Verarbeitung der Daten fällt. Die in der Richtlinie 95/46/EG verankerten Pflichten und Rechte

orientieren sich an den Festlegungen des Übereinkommens Nr. 108 des Europarates, die sich wiederum kaum von den diesbezüglichen Leitlinien der OECD (1980) oder der UNO (1990) unterscheiden. Dementsprechend kann davon ausgegangen werden, dass zum Inhalt von Datenschutzvorschriften weit gehend Einigkeit besteht, die weit über die fünfzehn Mitgliedstaaten der Gemeinschaft hinausgeht.

Mit Datenschutzvorschriften werden die Rechte des Einzelnen aber nur dann geschützt, wenn sie auch in die Praxis umgesetzt werden. Daher ist nicht nur der Inhalt der für die Übermittlung personenbezogener Daten in Drittländer geltenden Vorschriften, sondern auch das System zu betrachten, mit dem die Durchsetzung der Regeln gesichert werden soll. In Europa ist es bislang so, dass die Datenschutzvorschriften gesetzlich festgeschrieben werden und bei Nichteinhaltung Strafen auferlegt werden können bzw. dem Einzelnen das Recht auf Wiedergutmachung eingeräumt wird. Darüber hinaus sind in derartigen Gesetzen zusätzliche verfahrensrechtliche Mechanismen wie die Einrichtung von Kontrollstellen vorgesehen, denen Überwachungsaufgaben und die Verfolgung von Beschwerden obliegen. Die Verfahrensaspekte spiegeln sich auch in der Richtlinie 95/46/EG wider, die Bestimmungen über Haftung, Sanktionen, Rechtsbehelfe, Kontrollstellen und Meldung bei der Kontrollstelle enthält. Außerhalb der Gemeinschaft sind derartige verfahrensrechtliche Mittel zur Sicherung der Einhaltung der Datenschutzvorschriften weniger üblich. Die Parteien des Übereinkommens Nr. 108 sind zur gesetzlichen Verankerung der Grundsätze des Datenschutzes verpflichtet, doch sind zusätzliche Mechanismen wie eine Kontrollstelle nicht vorgesehen. In den OECD-Leitlinien wird lediglich "ihre Berücksichtigung" in der Landesgesetzgebung angemahnt, und es fehlen verfahrensrechtliche Mittel, mit denen gesichert würde, dass die Leitlinien tatsächlich zu einem wirksamen Schutz des Einzelnen führen. In den später verabschiedeten Leitlinien der UNO sind andererseits Bestimmungen über Kontrolle und Sanktionen enthalten, was zeigt, dass sich weltweit die Erkenntnis durchsetzt, dass auf die ordnungsgemäße Umsetzung von Datenschutzvorschriften nicht verzichtet werden kann.

Vor diesem Hintergrund wird deutlich, dass die Analyse des angemessenen Schutzniveaus ohne die Einbeziehung der beiden folgenden Grundelemente sinnlos ist: Inhalt der geltenden Vorschriften und Mittel zur Sicherung ihrer wirksamen Anwendung.

Geht man von der Richtlinie 95/46/EG aus und berücksichtigt dabei die Bestimmungen weiterer internationaler Dokumente zum Datenschutz, so sollte es möglich sein, für den Datenschutz einen "Kern" von "inhaltlichen" Grundsätzen und "verfahrensrechtlichen" bzw. mit der "Durchsetzung im Zusammenhang stehenden" Erfordernissen herauszuarbeiten, deren Einhaltung als Mindestanforderung an eine Situation gilt, in der von einem angemessenen Schutzniveau gesprochen werden kann. Dabei sollte nicht starr auf bestimmte Mindestanforderungen gepocht werden, denn während die Liste in einem Fall erweitert werden muss, reicht im anderen möglicherweise ein vermindertes Anforderungsspektrum. Bei der Bestimmung der genauen Anforderungen an einen konkreten Fall ist das Ausmaß der Gefahren, die für den Betroffenen der Datenübermittlung entstehen, ein wichtiger Faktor. Doch ungeachtet dieser Einschränkungen ist eine grundlegende Aufstellung von Mindestanforderungen in jedem Fall ein nützlicher Ausgangspunkt für eine Analyse.

i. Inhaltliche Grundsätze

Die folgenden Grundsätze sind unbedingt zu berücksichtigen:

1. Der Grundsatz der Beschränkung der Zweckbestimmung -
   Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insofern zu verwenden oder weiter zu übermitteln, als dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist. Die einzigen Ausnahmen von dieser Regel sind die in einer demokratischen Gesellschaft aus einem der in Artikel 13 der Richtlinie aufgeführten Gründe notwendigen Fälle [Artikel 13 gestattet eine Einschränkung auf den "Grundsatz der Zweckbestimmung", sofern eine solche Beschränkung für die Sicherheit des Staates, die Landesverteidigung, die öffentliche Sicherheit, die Verhütung, Ermittlung, Feststellung und Verfolgung von Straftaten oder Verstößen gegen die berufsständischen Regeln bei reglementierten Berufen, ein wichtiges wirtschaftliches oder finanzielles Interesse oder den Schutz der betroffenen Person und der Rechte und Freiheiten anderer Personen notwendig ist].
2. Der Grundsatz der Datenqualität und -verhältnismäßigkeit -
   Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Die Daten sollten angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiterverarbeitet werden, nicht exzessiv seien.
3. Der Grundsatz der Transparenz -
   Natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Drittland des für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist. Ausnahmen sind lediglich im Einklang mit den Artikeln 11 Absatz 2 und 13 der Richtlinie möglich [Artikel 11 Absatz 2 sieht vor, dass für den Fall, dass die Daten nicht bei der betroffenen Person erhoben wurden, die betroffene Person nicht informiert zu werden braucht, wenn dies unmöglich ist, unverhältnismäßigen Aufwand erfordert oder die Speicherung oder Weitergabe durch Gesetz ausdrücklich vorgesehen ist].
4. Der Grundsatz der Sicherheit -
   Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Verarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5. Das Recht auf Zugriff, Berichtigung und Widerspruch -
   Die betroffene Person muss das Recht haben, eine Kopie aller sie betreffender Daten zu erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muss sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können. Die einzigen Ausnahmen von diesen Rechten haben mit Artikel 13 der Richtlinie im Einklang zu stehen.
6. Beschränkungen der Weiterübermittlung in andere Drittländer -
   Weitere Übermittlungen personenbezogener Daten vom ursprünglichen Bestimmungsdrittland in ein anderes Drittland sind lediglich zulässig, wenn das zweite Drittland (d. h. der Empfänger der Weiterübermittlung) ebenfalls ein angemessenes Schutzniveau aufweist. Die einzigen zulässigen Ausnahmen haben mit Artikel 26 Absatz 1 der Richtlinie im Einklang zu stehen.

(Diese Ausnahmen werden in Kapitel 5 untersucht.)

Beispiele weiterer, auf spezifische Arten der Verarbeitung anwendbarer Grundsätze:

1. Sensible Daten -

   Sind "sensible" Kategorien von Daten betroffen (die in Artikel 8 der Richtlinie aufgelistet sind [Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie Daten über Gesundheit oder Sexualleben und Daten, die Straftaten, strafrechtliche Verurteilungen oder Sicherungsmaßregeln betreffen.]), so haben zusätzliche Sicherheitsmaßnahmen wie das Erfordernis zu gelten, dass die betroffene Person ausdrücklich in die Verarbeitung einwilligt.

2. Direktmarketing -

   Werden Daten zum Zwecke des Direktmarketings übermittelt, so muss die betroffene Person die Möglichkeit haben, sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke zu entscheiden.

3. Automatisierte Einzelentscheidung -

   Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Einzelentscheidung im Sinne von Artikel 15 der Richtlinie zu treffen, so muss die natürliche Person das Recht haben, die dieser Entscheidung zugrunde liegende Logik zu erfahren, und andere Maßnahmen müssen getroffen werden, um die berechtigten Interessen der Person zu schützen.

ii. Verfahrensrechtlicher Mechanismus/ Durchsetzungsmechanismus

In Europa besteht weit gehend Einigkeit darüber, dass die Datenschutzgrundsätze gesetzlich verankert werden müssen. Im Wesentlichen bestehen auch keine Zweifel über die Notwendigkeit der "externen Kontrolle" in Form einer unabhängigen Stelle, die Teil eines Systems zur Einhaltung des Datenschutzes ist. In anderen Teilen der Welt hingegen ist dies nicht immer der Fall. Als Grundlage für die Beurteilung der Angemessenheit des vorhandenen Datenschutzniveaus sind zunächst die Ziele des zugrunde liegenden verfahrensrechtlichen Systems für den Datenschutz zu bestimmen; darauf aufbauend ist das Spektrum der verschiedenen in Drittländern bestehenden gerichtlichen und außergerichtlichen verfahrensrechtlichen Mechanismen zu bewerten.

Ein Datenschutzsystem verfolgt im Wesentlichen drei Ziele:

1. Gewährleistung einer guten Befolgungsrate der Vorschriften. (Kein System kann eine 100%ige Einhaltung garantieren, aber einige sind besser als andere). Ein gutes System zeichnet sich im Allgemeinen dadurch aus, dass sich die für die Verarbeitung Verantwortlichen ihrer Pflichten und die betroffenen Personen ihrer Rechte und der Mittel für deren Wahrnehmung sehr stark bewusst sind. Die Existenz wirksamer, abschreckender Sanktionen ist wichtig, um die Einhaltung der Bestimmungen sicherzustellen; ebenso relevant sind natürlich auch Systeme der direkten Überprüfung durch Behörden, Buchprüfer oder unabhängige Datenschutzbeauftragte.
2. Unterstützung und Hilfe für einzelne betroffene Personen bei der Wahrnehmung ihrer Rechte. Der Einzelne muss seine Rechte rasch und wirksam, ohne überhöhte Kosten durchsetzen können. Dafür muss es eine Art institutionellen Mechanismus geben, der eine unabhängige Prüfung von Beschwerden ermöglicht.
3. Gewährleistung angemessener Entschädigung für die geschädigte Partei bei Verstoß gegen die Bestimmungen. Für dieses Schlüsselelement muss ein System unabhängiger Schlichtung vorhanden sein, das die Zahlung von Entschädigungen oder auch die Auferlegung von Sanktionen ermöglicht.

Kapitel 2:

Anwendung des Ansatzes auf Länder, die das Übereinkommen Nr. 108 des Europarates ratifiziert haben

Das Übereinkommen Nr. 108 ist neben der Richtlinie das einzige internationale Instrument, das auf dem Gebiet des Datenschutzes bindend ist. Die Mehrzahl der Parteien des Übereinkommens sind auch Mitgliedstaaten der Europäischen Union (die Ratifizierung ist inzwischen durch alle 15 Staaten erfolgt) bzw. Länder wie Norwegen und Island, für die die Richtlinie aufgrund des Abkommens über den Europäischen Wirtschaftsraum ohnehin gilt. Doch auch von Slowenien, Ungarn und der Schweiz ist das Übereinkommen ratifiziert worden, und insbesondere angesichts der Tatsache, dass das Übereinkommen auch Ländern offen steht, die dem Europarat nicht angehören, dürften weitere Drittländer in der Zukunft folgen. Aus diesem Grund ist die Prüfung, ob die Länder, die das Übereinkommen ratifiziert haben, ein angemessenes Schutzniveau im Sinne von Artikel 25 der Richtlinie bieten, nicht nur von rein akademischem Interesse.

Als Ausgangspunkt ist es zunächst günstig, den Wortlaut des Übereinkommens unter dem Aspekt der theoretischen Annahme eines "angemessenen Schutzniveaus", wie es in Kapitel 1 dieses Dokuments beschrieben ist, zu beleuchten.

Was den Inhalt der Grundprinzipien betrifft, so enthält das Übereinkommen praktisch die ersten fünf der sechs "Mindestanforderungen" (Hinsichtlich des Grundsatzes der Transparenz mögen gewisse Zweifel bestehen. Artikel 8 Absatz a) des Übereinkommens kann mit der aktiven Pflicht zur Bereitstellung von Informationen, die den Kern von Artikel 10 und 11 der Richtlinie darstellt, kaum gleichgesetzt werden. Im Übrigen sind im Übereinkommen keine konkreten Rechte zur Verwehrung der Verwendung der Daten vorgesehen, wenn diese für Zwecke des Direktmarketings eingesetzt werden sollen. Es fehlen auch Bestimmungen für automatisierte Einzelentscheidungen (Profilerstellung). Auch das Erfordernis geeigneter Sicherungsmaßnahmen für sensible Daten ist vorgesehen, die als Angemessenheitskriterium für Fälle, in denen derartige Daten vorkommen, angesehen werden können.

Ein Mangel des Inhalts der wesentlichen Vorschriften des Übereinkommens besteht darin, dass für die Übermittlung an Länder, die nicht Vertragsparteien des Übereinkommens sind, Beschränkungen nicht vorgesehen sind. Dies birgt die Gefahr, dass ein dem Übereinkommen Nr. 108 beigetretenes Land bei der Übermittlung von Daten aus der Gemeinschaft in ein weiteres Drittland mit völlig unangemessenem Schutzniveau als "Zwischenstation" benutzt wird.

Der zweite Aspekt des "angemessenen Schutzniveaus" betrifft die bestehenden verfahrensrechtlichen Mechanismen, mit denen den Grundprinzipien Geltung verschafft werden soll. Dem Übereinkommen zufolge sind ihre Grundsätze in das innerstaatliche Recht aufzunehmen und geeignete Sanktionen und Rechtsmittel für den Fall der Verletzung festzulegen. Dies müsste für die Gewährleistung eines angemessenen Niveaus der Einhaltung der Vorschriften und der angemessenen Entschädigung für die betroffenen Personen im Falle der Nichteinhaltung der Vorschriften ausreichen (Ziel 1 und 3 eines Systems zur Einhaltung des Datenschutzes). Allerdings verpflichtet das Übereinkommen die Vertragsparteien nicht, institutionelle Mechanismen zur unabhängigen Untersuchung von Beschwerden festzulegen, obwohl die Länder, von denen die Ratifizierung vorgenommen wurde, dies in der Regel getan haben. Dies ist ein Nachteil, da angemessene Unterstützung und Hilfe für die einzelnen betroffenen Personen bei der Wahrnehmung ihrer Rechte (Ziel 2) ohne diese institutionellen Mechanismen möglicherweise nicht garantiert sind.

Diese kurze Analyse lässt den Schluss zu, dass von den meisten Übermittlungen personenbezogener Daten in Länder, von denen das Übereinkommen Nr. 108 ratifiziert worden ist, angenommen werden kann, dass sie gemäß Artikel 25 (1) der Richtlinie unter der Bedingung statthaft sind, dass

> das betreffende Land über geeignete Mechanismen für die Gewährleistung der Einhaltung der Vorschriften, die Unterstützung betroffener Personen und die Möglichkeit einer Entschädigung

(beispielsweise eine unabhängige Kontrollstelle mit entsprechenden Befugnissen) verfügt und

das betreffende Land das Endbestimmungsland der Übermittlung und keine Zwischenstation ist, über die die Daten geleitet werden, es sei denn, es handelt sich um die Weiterübermittlung zurück in die EU oder einen anderen Bestimmungsort mit angemessenem Schutzniveau [Das Übereinkommen Nr. 108 wird derzeit einer Prüfung unterzogen, in deren Verlauf es zu Änderungen kommen kann, mit denen diese und weitere Schwierigkeiten angesprochen werden].

Dies ist natürlich eine recht vereinfachte und oberflächliche Prüfung des Übereinkommens. Im Zusammenhang mit konkreten Fällen der Übermittlung von Daten in Länder, die dem Übereinkommen beigetreten sind, dürften neue, an dieser Stelle nicht in Betracht gezogene Probleme auftreten.

Kapitel 3:

Anwendung des Ansatzes auf die Selbstkontrolle der Wirtschaft

Einführung

Entsprechend Artikel 25 Absatz 2 der Datenschutzrichtlinie (95/ 46/ EG) ist die Angemessenheit des Schutzniveaus, das ein Drittland bietet, unter Berücksichtigung aller Umstände zu beurteilen, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen eine Rolle spielen. Nicht nur auf Rechtsvorschriften, sondern insbesondere auf "die dort geltenden Standesregeln und Sicherheitsmaßnahmen" wird Bezug genommen.

Im Text der Richtlinie ist daher festgelegt, dass in dem betreffenden Drittland möglicherweise geltende außergerichtliche Vorschriften berücksichtigt werden, sofern diese Regeln auch eingehalten werden. In diesem Zusammenhang ist auch die Rolle zu betrachten, die die Selbstkontrolle spielt.

Was ist Selbstkontrolle?

Der Begriff "Selbstkontrolle" mag nicht für jeden dieselbe Bedeutung haben. Im Sinne dieser Unterlage beinhaltet ein Selbstkontrollkodex (oder jedes andere Instrument) alle Datenschutzbestimmungen, die auf eine Vielzahl von für die Verarbeitung Verantwortlichen in einer Berufsgruppe oder einem Wirtschaftsbereich Anwendung finden und deren Inhalt ursprünglich von Angehörigen des betreffenden Wirtschaftszweiges oder der betreffenden Berufsgruppe festgelegt wurde.

Diese weit gefasste Definition würde sowohl einen freiwilligen Datenschutzkodex am einen Ende der Skala einschließen, der von einem kleinen Wirtschaftsverband mit nur wenigen Mitgliedern entwickelt wurde, als auch den detaillierten Kodex von Standesregeln am anderen Ende, die für ganze Berufsgruppen wie Ärzte und Bankiers gelten und oft quasigerichtliche Kraft haben.

Ist das für den Kodex verantwortliche Gremium repräsentativ für den Sektor?

Wie aus diesem Kapitel hervorgeht, ist ein wichtiges Kriterium für die Beurteilung des Wertes eines Kodexes das Ausmaß, in dem seine Regeln durchgesetzt werden können. In diesem Zusammenhang ist die Frage, ob der für den Kodex zuständige Verband oder das zuständige Gremium alle Wirtschaftsteilnehmer in einem Sektor repräsentiert oder nur einen kleinen Prozentsatz von ihnen, wahrscheinlich von geringerer Bedeutung als die Stärke des Verbands im Hinblick auf seine Fähigkeit, beispielsweise seinen Mitgliedern wegen Nichterfüllung des Kodexes Sanktionen aufzuerlegen. Daneben gibt es allerdings einige Gründe, die branchen- oder berufsweite Kodizes mit klar abgegrenztem Geltungsbereich zu sehr viel nützlicheren Schutzinstrumenten machen als die, die von kleinen Unternehmensgruppierungen innerhalb von Wirtschaftssektoren entwickelt werden. Zunächst ist es eine Tatsache, dass aus der Sicht des Verbrauchers eine aufgespaltene und durch einige rivalisierende Verbände - mit jeweils eigenem Datenschutzkodex - gekennzeichnete Wirtschaft verwirrend ist. Das Nebeneinanderbestehen unterschiedlicher Kodizes schafft ein allgemeines Bild, dem es für die betroffene Person an Transparenz fehlt. Außerdem können sich insbesondere in Bereichen wie dem Direktmarketing, in denen regelmäßig personenbezogene Daten zwischen verschiedenen Unternehmen desselben Sektors ausgetauscht werden, Situationen ergeben, in denen das Unternehmen, das die personenbezogenen Daten weitergibt, nicht demselben Datenschutzkodex unterliegt wie das Unternehmen, das die Daten erhält. Dies führt hinsichtlich der anwendbaren Regeln zu einem beträchtlichen Maß an Unsicherheit und dürfte auch die Untersuchung und Bearbeitung von Beschwerden einzelner betroffener Personen außerordentlich erschweren.

Beurteilung der Selbstkontrolle - der Ansatz

Angesichts der Vielfalt der Instrumente, die unter den Begriff der Selbstkontrolle fallen, ist klar, dass zwischen den verschiedenen Formen der Selbstkontrolle je nach ihrer tatsächlichen Auswirkung auf das Niveau des Datenschutzes bei der Übermittlung personenbezogener Daten in ein Drittland zu differenzieren ist.

Grundlage für die Bewertung bestehender Datenschutzregeln muss (unabhängig davon, ob sie aufgrund von freiwilliger Selbstkontrolle oder von Vorschriften bestehen) der in Kapitel 1 vorgestellte generelle Ansatz sein. Ein Eckpunkt dieses Ansatzes ist die Prüfung nicht nur des Inhalts des Instruments (es sollte eine Reihe wesentlicher Grundsätze enthalten), sondern auch seine Effizienz im Hinblick auf:

eine hohe allgemeine Befolgungsrate,

Unterstützung und Hilfe für die einzelne betroffene Person,

und, als entscheidenden Faktor, eine angemessene Entschädigung (einschließlich ggf. Schadensersatz).

Beurteilung des Inhalts eines Instruments der Selbstkontrolle

Dies ist eine relativ leichte Aufgabe. Es geht darum, sicherzustellen, dass die erforderlichen, in Kapitel 1 dargelegten inhaltlichen Grundsätze erfüllt sind. Das ist eine objektive Beurteilung. Die Frage ist, was

der Kodex enthält, und nicht, wie er erstellt wurde. Die Tatsache, dass ein Wirtschaftszweig oder eine Berufsgruppe selbst die wichtigste Rolle bei der Ausarbeitung des Inhalts des Kodexes gespielt haben, ist an sich nicht relevant, obwohl es natürlich wahrscheinlicher ist, dass der Kodex die erforderlichen wesentlichen Grundsätze des Datenschutzes genauer wiedergibt, wenn die Meinungen der betroffenen Personen und der Verbraucherorganisationen bei seiner Ausarbeitung berücksichtigt wurden. Die Transparenz des Kodexes ist ein Schlüsselelement; insbesondere sollte der Kodex in allgemein verständlicher Sprache abgefasst sein und konkrete Beispiele enthalten, die seine Bestimmungen veranschaulichen. Darüber hinaus sollte der Kodex die Offenlegung von Daten nicht angeschlossener Unternehmen verbieten, die nicht unter den Kodex fallen, wenn keine anderen angemessenen Schutzmaßnahmen vorgesehen sind.

Beurteilung der Effizienz eines Instruments der Selbstkontrolle

Die Bewertung der Effizienz eines bestimmten Selbstkontrollkodexes oder -instruments ist ein schwierigeres Unterfangen, das die Kenntnis der Mittel und Wege voraussetzt, durch die sichergestellt wird, dass man sich dem Kodex verpflichtet, und mit denen Probleme der Nichtbefolgung behandelt werden. Alle drei funktionellen Kriterien für die Beurteilung der Effizienz des Schutzes müssen erfüllt sein, wenn ein Selbstkontrollkodex bei der Bewertung der Angemessenheit des Schutzes berücksichtigt werden soll.

Gute Befolgungsrate

Ein Wirtschafts- oder Standeskodex wird normalerweise von einem repräsentativen Gremium des betreffenden Wirtschaftszweigs oder der betreffenden Berufsgruppe erstellt und gilt dann für die Mitglieder dieses speziellen repräsentativen Gremiums. Das Niveau der Einhaltung des Kodexes wird wahrscheinlich von der Bekanntheit seiner Existenz und seines Inhaltes unter den Mitgliedern, den zur Sicherstellung der Transparenz des Kodexes für die Verbraucher ergriffenen Schritten, mit denen ermöglicht werden soll, dass die Marktkräfte einen wirksamen Beitrag leisten, der Existenz eines Systems der externen Überprüfung (wie dem Erfordernis einer Überprüfung der Einhaltung in regelmäßigen Abständen) und, was vielleicht am wichtigsten ist, der Art und Durchsetzung von Sanktionen im Fall der Nichtbefolgung abhängen.

Wichtige Fragen sind deshalb:

Welche Bemühungen des repräsentativen Gremiums sind erforderlich, um sicherzustellen, dass seine Mitglieder den Kodex kennen?

Fordert das repräsentative Gremium von seinen Mitgliedern Nachweise darüber, dass sie die Bestimmungen des Kodexes umgesetzt haben? Wie oft?

Ist ein solcher Nachweis von den angeschlossenen Unternehmen selbst vorgesehen oder kommt er von außen (z. B. von einem zugelassenen Wirtschaftsprüfer)?

Untersucht das repräsentative Gremium mutmaßliche oder vermutete Verstöße gegen den Kodex?

Ist die Einhaltung des Kodexes eine Voraussetzung für die Mitgliedschaft des repräsentativen Gremiums oder ist sie rein ”freiwillig"?

Welche Formen disziplinarischer Maßnahmen stehen dem repräsentativen Gremium zur Verfügung (Ausschluss u. Ä.), wenn ein Mitglied nachweislich gegen den Kodex verstoßen hat?

Besteht für eine Person oder ein Unternehmen in der betreffenden Berufsgruppe oder dem betreffenden Wirtschaftszweig auch nach Ausschluss aus dem repräsentativen Gremium die Möglichkeit zur Weiterarbeit?

Ist die Einhaltung des Kodexes mit anderen Mitteln durchsetzbar, beispielsweise auf gerichtlichem Wege oder durch eine spezielle Stelle? Standesrechtliche Kodizes haben in einigen Ländern Gesetzeskraft. Unter bestimmten Umständen könnte es möglich sein, die Durchsetzung von Branchenkodizes über allgemeine Gesetze zu lauteren Handelspraktiken oder auch zum Wettbewerb zu bewirken.

Bei der Prüfung der vorhandenen Sanktionsarten ist es wichtig, zwischen der "die Situation abstellenden" Sanktion, die im Fall der Nichterfüllung von einem für die Verarbeitung Verantwortlichen lediglich fordert, seine Praktiken dahingehend zu ändern, dass sie dem Kodex entsprechen, und einer Sanktion, die weitergeht und den für die Verarbeitung Verantwortlichen für die Nichterfüllung tatsächlich bestraft, zu unterscheiden. Nur diese zweite Kategorie der ”Strafsanktion" wirkt sich tatsächlich auf das künftige Verhalten der für die Verarbeitung Verantwortlichen aus, indem sie einen gewissen Anreiz für die Erfüllung des Kodex bietet.

Fehlen in einem Kodex tatsächlich abschreckende Strafmaßnahmen, so ist dies ein gravierender Nachteil. Ohne derartige Sanktionen ist schwer zu sehen, wie ohne ein striktes System externer Überprüfung (beispielsweise eine öffentliche oder private Stelle, die für die Intervention im Fall der Nichteinhaltung des Kodexes zuständig ist, oder eine zwingende Vorschrift für eine regelmäßige externe Prüfung) ein hohes Niveau allgemeiner Erfüllung erreicht werden kann.

Unterstützung und Hilfe für einzelne betroffene Personen

Von einem angemessenen und wirksamen Datenschutzsystem ist zu fordern, dass der Einzelne bei einem Problem im Zusammenhang mit den eigenen personenbezogenen Daten nicht allein gelassen wird, sondern institutionelle Hilfe erhält, um die Schwierigkeiten zu beheben. Diese institutionelle Unterstützung sollte idealerweise neutral, unabhängig und mit den erforderlichen Befugnissen für die Prüfung jeder Beschwerde einer betroffenen Person ausgestattet sein. Im Hinblick auf die Selbstkontrolle ergeben sich in diesem Zusammenhang folgende Fragen:

Existiert ein System, das die Prüfung von Beschwerden einzelner betroffener Personen ermöglicht?

Wie erhalten betroffene Personen Kenntnis von diesem System und den Entscheidungen im

Einzelfall?

Entstehen der betroffenen Person Kosten irgendwelcher Art?

Wer führt die Prüfung durch? Sind die Prüfer mit den erforderlichen Befugnissen ausgestattet?

Wer entscheidet über eine mutmaßliche Verletzung des Kodexes? Sind diese Personen unabhängig und neutral?

Die Neutralität des Schiedsmanns oder Schiedsrichters bei mutmaßlichen Verletzungen des Kodexes ist ein Schlüsselelement. Eine solche Person oder ein solches Gremium darf zum Verantwortlichen der Verarbeitung in keinem Abhängigkeitsverhältnis stehen. Allerdings reicht dies allein noch nicht aus, um die Neutralität zu gewährleisten. Im Idealfall sollte der Schiedsrichter nicht der betroffenen Berufsgruppe oder dem betroffenen Wirtschaftszweig angehören, weil zwischen dem Verantwortlichen der Verarbeitung, der gegen den Kodex verstoßen haben soll, und den der gleichen Berufsgruppe oder dem gleichen Wirtschaftszweig angehörenden Mitgliedern eindeutig eine Interessengemeinschaft besteht. Die Neutralität des Schiedsgremiums könnte durch die Einbeziehung von Vertretern der Verbraucher neben den Vertretern der Wirtschaft (in gleicher Zahl) gewährleistet werden.

Angemessene Entschädigung

Wenn nachweislich gegen den Selbstkontrollkodex verstoßen wurde, sollten der betroffenen Person Rechtsmittel offen stehen, mit deren Hilfe das Problem behoben werden muss (Berichtigung oder Löschen aller fehlerhaften Daten; Gewährleistung, dass die Verarbeitung für unvereinbare Zweckbestimmungen eingestellt wird); wenn der betroffenen Person Schaden entstanden ist, muss die Zahlung einer angemessenen Entschädigung vorgesehen sein. Dabei ist zu berücksichtigen, dass "Schaden" im Sinne der Datenschutzrichtlinie nicht nur materiellen Schaden und finanziellen Verlust einschließt, sondern darunter auch jeglicher psychischer und moralischer Schaden fällt (im Recht des Vereinigten Königreichs und der USA als "distress" bezeichnet).

Viele der Fragen im Hinblick auf die oben im Abschnitt "Gute Befolgungsrate" aufgelisteten Sanktionen sind hier von Bedeutung. Wie bereits dargelegt wurde, haben Sanktionen eine doppelte Funktion: Den Täter zu bestrafen (und somit die Einhaltung der Regeln durch den Täter und andere zu fördern) und einen Verstoß gegen die Bestimmungen abzustellen. Hier geht es hauptsächlich um die zweite Funktion. Zusätzliche Fragen wären deshalb:

Lässt sich überprüfen, ob ein Mitglied, das nachweislich gegen den Kodex verstoßen hat, seine Praktiken geändert und das Problem beseitigt hat?

Können Personen nach dem Kodex einen Entschädigung erhalten, und wie?

Ist der Verstoß gegen den Kodex einem Vertragsverstoß gleichzusetzen oder auf dem Wege des öffentlichen Rechts geltend zu machen (beispielsweise Verbraucherschutz, unlauterer Wettbewerb), und kann das zuständige Gericht auf dieser Grundlage zur Leistung von Schadenersatz verurteilen?

Schlussfolgerungen

Selbstkontrolle sollte unter Verwendung des objektiven, funktionellen Ansatzes beurteilt werden, der in Kapitel 1 dargelegt wurde.

Ein Instrument der Selbstkontrolle, das als wirksamer Bestandteil eines "angemessenen Schutzes" anzusehen ist, muss für alle Mitglieder bindend sein, an die personenbezogene Daten übermittelt werden, und angemessene Sicherungsmaßnahmen vorsehen, wenn die Daten an Nichtmitglieder weitergeleitet werden.

Das Instrument muss transparent sein und den grundlegenden Inhalt aller maßgeblichen Datenschutzgrundsätze enthalten.

Das Instrument muss über Mechanismen verfügen, die ein gutes allgemeines Befolgungsniveau wirksam gewährleisten. Ein System abschreckender Strafmaßnahmen ist eine Möglichkeit, dies zu erreichen. Zwingende externe Prüfungen sind ein weiteres Mittel.

Das Instrument muss Unterstützung und Hilfe für einzelne betroffene Personen bieten, die ein Problem im Zusammenhang mit der Verarbeitung ihrer personenbezogenen Daten haben. Ein leicht zugängliches, neutrales und unabhängiges Gremium zur Anhörung von Beschwerden betroffener Personen und zur Schlichtung bei Verstößen gegen den Kodex muss deshalb eingerichtet werden.

Das Instrument muss für den Fall der Verletzung von Vorschriften eine angemessene Entschädigung gewährleisten. Die betroffene Person muss die Möglichkeit haben, das Problem zu beseitigen und ggf. Schadensersatz zu erhalten.

Kapitel 4:

Die Rolle der vertraglichen Bestimmungen

1. Einführung

Nach Artikel 25 Absatz 1 der Datenschutzrichtlinie (95/ 46/ EG) gilt der Grundsatz, dass die Übermittlung personenbezogener Daten lediglich erfolgen darf, wenn das Drittland ein angemessenes Schutzniveau gewährleistet. In diesem Kapitel soll die Möglichkeit einer Ausnahme von dem Grundsatz des angemessenen Schutzniveaus nach Artikel 25 geprüft werden, die aufgrund von Artikel 26 Absatz 2 möglich ist. Diese Bestimmung erlaubt einem Mitgliedstaat eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland ohne angemessenes Schutzniveau, ”wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet". Weiter wird ausgeführt, dass "diese Garantien sich insbesondere aus entsprechenden Vertragsklauseln ergeben können". Wenn die Kommission nach dem Verfahren des Artikels 31 tätig wird, so befugt Artikel 26 Absatz 4 sie ferner zu beschließen, dass bestimmte Standardvertrags-

klauseln ausreichende Garantien gemäß Artikel 26 Absatz 2 bieten.

Die Idee der Verwendung von Verträgen als Mittel der Regelung internationaler Übermittlungen personenbezogener Daten ist natürlich nicht erst durch die Richtlinie entstanden. Bereits 1992 waren der Europarat, die Internationale Handelskammer und die Europäische Kommission gemeinsam für eine Studie zu diesem Thema verantwortlich ["Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flow, with Explanatory Memorandum", gemeinsame Studie des Europarates, der Kommission der Europäischen Gemeinschaften und der Internationalen Handelskammer, Straßburg, 2. November 1992]. In jüngerer Zeit haben sich immer mehr Sachverständige und Kommentatoren in Studien und Artikeln zur Verwendung vertraglicher Bestimmungen geäußert - vielleicht, weil sie die ausdrückliche Bezugnahme in der Richtlinie festgestellt haben. Auch in der Praxis werden Verträge weiterhin als ein Mittel zur Behandlung von Datenschutzproblemen eingesetzt, die sich aus der Ausfuhr personenbezogener Daten aus bestimmten EU- Mitgliedstaaten ergeben. Seit Ende der 80er Jahre werden sie in Frankreich häufig verwendet, und in Deutschland fand jüngst das Beispiel der "BahnCard" große Beachtung, da ein Teil des Angebots auf der Einbeziehung der Citibank beruht [vgl. Darstellung dieses Falls durch Alexander Dix auf der Internationalen Konferenz der Datenschutzbeauftragten, September 1996 in Ottawa].

2. Die Verwendung von Verträgen als Grundlage für innergemeinschaftliche Datenflüsse

Vor der Prüfung der Anforderungen an vertragliche Bestimmungen im Rahmen von Datenströmen in Drittländer ist es wichtig, den Unterschied zwischen der Drittlandsituation und der Situation deutlich zu machen, bei der die Daten in der Gemeinschaft bleiben. Im letztgenannten Fall ist der Vertrag der Mechanismus, der verwendet wird, um die Aufteilung der Zuständigkeiten für den Datenschutz zu definieren und zu regeln, wenn mehr als eine Stelle an der fraglichen Datenverarbeitung beteiligt ist. Nach der Richtlinie trägt eine einzige Einheit, d. h. der "für die Verarbeitung Verantwortliche" die Hauptverantwortung für die Erfüllung der wesentlichen Grundsätze des Datenschutzes. Die zweite Einheit, der "Auftragsverarbeiter", ist lediglich für die Datensicherheit zuständig. Von einem "für die Verarbeitung Verantwortlichen" wird gesprochen, wenn eine Person die Entscheidungsbefugnis über die Zweckbestimmung und die Mittel der Datenverarbeitung besitzt, während der "Auftragsverarbeiter" lediglich die Stelle ist, die den Datenverarbeitungsdienst physisch erbringt. Die Beziehung zwischen den beiden wird durch Artikel 17 Absatz 3 der Richtlinie geregelt, der folgendes festlegt:

Die Durchführung einer Verarbeitung im Auftrag erfolgt auf der Grundlage eines Vertrags oder Rechtsakts, durch den der Auftragsverarbeiter an den für die Verarbeitung Verantwortlichen gebunden ist und in dem insbesondere folgendes vorgesehen ist:

> der Auftragsverarbeiter handelt nur auf Weisung des für die Verarbeitung Verantwortlichen
>
> die in Absatz 1 genannten Verpflichtungen (die materiellrechtlichen Bestimmungen zur Datensicherheit) gelten auch für den Auftragsverarbeiter, und zwar nach Maßgabe der Rechtsvorschriften des Mitgliedstaats, in dem er seinen Sitz hat.

Dies baut auf dem allgemeinen Grundsatz nach Artikel 16 auf, demzufolge Personen, die dem für die Verarbeitung Verantwortlichen oder dem Auftragsverarbeiter unterstellt sind, sowie der Auftragsverarbeiter selbst personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen

verarbeiten dürfen (es sei denn, es bestehen hierzu gesetzliche Verpflichtungen).

Bei der Übermittlung personenbezogener Daten in Drittländer wird normalerweise auch mehr als eine Partei beteiligt sein. Hier ist die betreffende Beziehung eine Beziehung zwischen der die Daten übermittelnden Stelle (dem "Übermittler") und der Stelle, die die Daten im Drittland entgegennimmt (dem "Empfänger"). Daher sollte der Zweck des Vertrags unter anderem darin bestehen, die Verteilung der Zuständigkeit für die Einhaltung des Datenschutzes auf die beiden Vertragsparteien festzulegen. Der Vertrag muss jedoch noch weiteren Anforderungen entsprechen: Er muss zusätzliche Sicherheiten für die betroffene Person bieten, die dadurch erforderlich werden, dass der Empfänger im Drittland keinem durchsetzbaren Regelwerk von Datenschutzbestimmungen unterliegt, das ein angemessenes Schutzniveau vorsieht.

3. Das Ziel einer vertraglichen Lösung

Im Rahmen der Drittlandübermittlungen ist deshalb der Vertrag ein Mittel, um angemessene Garantien durch den für die Verarbeitung Verantwortlichen vorzusehen, wenn Daten aus der Gemeinschaft (und somit außerhalb des durch die Richtlinie und natürlich durch das allgemeine Regelwerk des Gemeinschaftsrechts vorgesehenen Schutzes [Die Wahrnehmung der Datenschutzrechte der Personen wird innerhalb der Gemeinschaft durch das allgemeine Regelwerk erleichtert, beispielsweise das Europäische Übereinkommen über die Übermittlung von Rechtshilfeersuchen (Straßburg 1977)]) in ein Drittland übermittelt werden, in dem kein angemessenes allgemeines Schutzniveau vorhanden ist. Eine Vertragsbestimmung, die diese Funktion erfüllen soll, muss einen befriedigenden Ausgleich für das Fehlen eines allgemein angemessenen Schutzniveaus bieten, indem sie die wesentlichen Elemente des Schutzes enthält, die in einer bestimmten Situation nicht vorhanden sind.

4. Die spezifischen Erfordernisse einer vertraglichen Lösung

Ausgangspunkt für die Bewertung der Bedeutung der "ausreichenden Garantien" gemäß Artikel 26 Absatz 2 ist der Begriff des "angemessenen Schutzes", auf den in Kapitel 1 bereits recht ausführlich eingegangen worden ist. Er umfasst eine Reihe von Grundsätzen des Datenschutzes und drei weitere Voraussetzungen, ohne die diese wirkungslos blieben.

i. Die wesentlichen Datenschutzvorschriften

   Das wichtigste Erfordernis der vertraglichen Lösung besteht darin, dass sie auf eine Verpflichtung der an der Übermittlung Beteiligten hinauslaufen muss, sicherzustellen, dass alle in Kapitel 1 dargelegten grundlegenden Bestimmungen des Datenschutzes bei der Verarbeitung von den in das Drittland übermittelten Daten gelten. Diese Grundsätze sind:

   Der Grundsatz der Beschränkung der Zweckbestimmung

   Der Grundsatz der Datenqualität und -verhältnismäßigkeit

   Der Grundsatz der Transparenz

   Der Grundsatz der Sicherheit

Die Rechte auf Zugriff, Berichtigung und Widerspruch

Beschränkungen der Weiterübermittlung an Nichtvertragspartner

[Weiterübermittlungen personenbezogener Daten vom Empfänger an einen anderen Dritten sind lediglich zulässig, wenn Mittel gefunden werden, den betreffenden Dritten vertraglich zu binden und damit den betroffenen Personen dieselben Garantien des Datenschutzes zu gewährleisten].

In bestimmten Situationen müssen zusätzliche Grundsätze, die sich auf sensible Daten, das Direktmarketing und automatisierte Entscheidungen beziehen, angewandt werden.

Der Vertrag sollte detailliert darlegen, wie der Empfänger der Datenübermittlung diese Grundsätze anzuwenden hat (d.h. Spezifizierung der Zweckbestimmungen, der Datenkategorien, Begrenzung der Speicherzeit, Sicherheitsmaßnahmen usw.). In anderen Fällen, wenn beispielsweise der Schutz in einem Drittland durch ein allgemeines Datenschutzgesetz vorgesehen ist, das der Richtlinie ähnelt, sind wahrscheinlich andere Mechanismen vorhanden, aus denen hervorgeht, auf welche Art und Weise die Datenschutzvorschriften in der Praxis Anwendung finden (Verhaltenskodexe, Notifizierung, beratende Funktion der Aufsichtsbehörde). Da dies bei vertraglichen Beziehungen nicht der Fall ist, kommt der Festlegung der Einzelheiten besondere Bedeutung zu, wenn die Übermittlung auf der Grundlage eines Vertrags erfolgt.

ii. Den wesentlichen Vorschriften Geltung verschaffen

In Kapitel 1 sind für die Beurteilung der Effizienz eines Datenschutzsystems drei Kriterien dargelegt. Dabei handelt es sich um die Fähigkeit des Systems:

eine gute Befolgungsrate der Vorschriften zu bewirken,

Unterstützung und Hilfe für die einzelne betroffene Person bei der Wahrnehmung ihrer Rechte zu sichern

und - als besonders wichtiges Element - für eine angemessene Entschädigung des Geschädigten im Falle der Nichteinhaltung von Vorschriften zu sorgen.

Dieselben Kriterien müssen bei der Beurteilung der Effizienz einer vertraglichen Lösung gelten. Dies ist natürlich eine große, wenn auch zu bewältigende Herausforderung. Es geht darum, Mittel und Wege zu finden, um das Fehlen von Aufsichts- und Durchsetzungsmechanismen auszugleichen und der betroffenen Person, die vielleicht kein Vertragspartner ist, Hilfe, Unterstützung und letztendlich Entschädigung zu gewähren.

Jede dieser Fragen muss in allen Einzelheiten geprüft werden. Zur Erleichterung der Analyse werden sie hier in umgekehrter Reihenfolge behandelt.

Entschädigung für eine betroffene Person

Einer betroffenen Person mit Hilfe eines zwischen "Datenübermittler" und "Datenempfänger" abzuschließenden Vertrages die Möglichkeit des Rechtsbehelfs einzuräumen (d.h. das Recht auf eine durch einen unabhängigen Schiedsrichter beurteilte Beschwerde und gegebenenfalls das Recht auf eine Entschädigung) ist keine einfache Frage. Viel wird von der Art des gewählten Vertragsrechts sowie von dem auf

den Vertrag anwendbaren einzelstaatlichen Recht abhängen. Normalerweise dürfte das anwendbare Recht das des Mitgliedstaats sein, in dem die übermittelnde Partei niedergelassen ist. Das Vertragsrecht einiger Mitgliedstaaten erlaubt die Begründung von Rechten Dritter, die in anderen Mitgliedstaaten nicht möglich ist.

Es gilt die allgemeine Regel, dass die Rechtssicherheit für die betroffene Person umso größer ist, je mehr der Empfänger im Hinblick auf seine Freiheit beschränkt ist, die Zweckbestimmungen, Mittel und Bedingungen zu wählen, unter denen er die übermittelten Daten verarbeitet. Da es ja hier um Fälle unangemessenen allgemeinen Schutzes geht, bestünde die beste Lösung darin, im Vertrag festzulegen, dass der Empfänger der Übermittlung im Hinblick auf die übermittelten Daten oder die Art und Weise, in der diese anschließend verarbeitet werden, keine eigene Entscheidungsbefugnis hat. Der Empfänger hat in diesem Fall allein nach Anweisung des Übermittlers zu handeln. So verbleibt beispielsweise die Entscheidungskompetenz über die Daten auch dann, wenn die Daten nach außerhalb der Europäischen Union übermittelt wurden, bei der Stelle, die die Übermittlung vorgenommen und ihren Sitz in der Gemeinschaft hat. Der Übermittler bleibt somit der für die Verarbeitung Verantwortliche, während der Empfänger lediglich ein Verarbeiter mit einem Subunternehmervertrag ist. Da die Aufsicht über die Daten durch eine in einem Mitgliedstaat der EU niedergelassene Aufsichtsbehörde ausgeübt wird, gilt das Recht des betreffenden Mitgliedstaats für die in dem Drittland erfolgte Verarbeitung weiter [Aufgrund von Artikel 4 Absatz 1 Buchstabe a) der Richtlinie 95/46/EG]. Darüber hinaus ist der für die Verarbeitung Verantwortliche weiterhin nach dem Recht des Mitgliedstaats für jeden Schaden haftbar, der in Folge einer unzulässigen Verarbeitung entstanden ist [Vgl. Artikel 23 der Richtlinie 95/46/EG].

Diese Art der Übereinkunft ist der nicht unähnlich, die bei der interterritorialen Vereinbarung gefunden wurde, mit der der zuvor erwähnte Fall von BahnCard und Citibank gelöst wurde. In der vertraglichen Vereinbarung sind dabei insbesondere im Hinblick auf die Datensicherheit detaillierte Festlegungen für die Datenverarbeitung getroffen worden, die alle anderen Nutzungen der Daten durch den Empfänger der Übermittlung ausschließen. Damit wurde gesichert, dass für die im Drittland erfolgende Datenverarbeitung deutsches Recht gilt und den betroffenen Personen Rechtsbehelfe offen stehen [Obwohl für diesen Fall ein Gesetz galt, das vor der Richtlinie erlassen worden war, fand das Gesetz selbst nicht automatisch Anwendung auf alle Verarbeitungen, die durch einen in Deutschland niedergelassenen Verantwortlichen für die Datenverarbeitung kontrolliert wurden. Die Rechtsbehelfe für die betroffene Person wurden durch die Möglichkeit des deutschen Vertragsrechts geschaffen, Rechte Dritter zu begründen].

Natürlich wird es Fälle geben, in denen eine solche Lösung nicht möglich ist. Möglicherweise erbringt der Empfänger der Übermittlung nicht nur einen reinen Datenverarbeitungsdienst für den Verantwortlichen mit Sitz in der Europäischen Union, sondern hat die Daten beispielsweise für eine Verwendung zum eigenen Nutzen oder für eigene Zwecke gemietet oder erworben. Unter diesen Umständen muss der Empfänger über einen gewissen Handlungsspielraum verfügen, um die Daten nach seinem Belieben zu verarbeiten, wodurch er selbst zu einem Verantwortlichen für die Daten wird.

In einem derartigen Fall kann man sich nicht auf die ständige automatische Anwendbarkeit der Rechtsvorschriften eines Mitgliedstaats und die fortgesetzte Schadenshaftung des Übermittlers der Daten stützen. Andere, komplexere Mechanismen müssen gefunden werden, um der betroffenen Person angemessene Rechtsbehelfe an die Hand zu geben. Wie bereits erwähnt, ist es in einigen Rechtssystemen für Dritte möglich, Vertragsrechte geltend zu machen, so dass dies genutzt werden könnte, um über einen offenen, veröffentlichten Vertrag zwischen Übermittler und Empfänger Rechte für betroffene Personen zu begründen. Die Position dieser Personen würde weiter gestärkt, wenn sich im Rahmen des

Vertrages die Parteien selbst zu einer Art verbindlichen Schlichtung für den Fall verpflichten, dass die Vertragserfüllung durch eine betroffene Person angefochten wird. In den Selbstkontrollkodizes einiger Branchen sind derartige Schlichtungsmechanismen enthalten, und die Verwendung von Verträgen in Verbindung mit derartigen Kodexen wäre sicherlich nutzbringend.

Eine weitere Möglichkeit besteht darin, dass der Übermittler zum Zeitpunkt des Eingangs der ersten Daten der betroffenen Person eine gesonderte vertragliche Vereinbarung mit ihr abschließt und darin festlegt, dass er (der Übermittler) für jeden Schaden oder jede Notlage haftbar bleibt, die dadurch entsteht, dass der Empfänger einer Datenübermittlung das vereinbarte Paket an Grundprinzipien des Datenschutzes nicht einhält. Auf diese Weise verfügt die betroffene Person gegenüber dem Übermittler bei Verstößen durch den Empfänger über Rechtsmittel. Es ist dann Sache des Übermittlers, Maßnahmen wegen Vertragsbruchs gegen den Empfänger einzuleiten und etwaige Schadensersatzleistungen, zu deren Zahlung an die betroffene Person er genötigt war, anschließend von diesem zurückzufordern.

Diese ausgeklügelte dreiseitige Lösung ist vielleicht machbarer als dies scheinen mag. Der Vertrag mit der betroffenen Person könnte Teil der Allgemeinen Geschäftsbedingungen werden, zu denen beispielsweise eine Bank oder ein Reisebüro ihren Kunden Dienstleistungen anbietet. Sie hat den Vorteil der Transparenz: Die betroffene Person wird über ihre Rechte voll informiert.

Schließlich könnte als Alternative zum Vertragsabschluss mit der betroffenen Person auch vorgesehen werden, dass ein Mitgliedstaat für Schäden, die infolge der Handlungen des Empfängers der Übermittlung entstehen, eine fortgesetzte Haftpflicht der für die Verarbeitung Verantwortlichen, die Daten nach außerhalb der Gemeinschaft übermitteln, gesetzlich niederlegt.

Unterstützung und Hilfe für betroffene Personen

Eine der Hauptschwierigkeiten betroffener Personen, deren Daten in den Bereich einer ausländischen Rechtsprechung übermittelt werden, ist das Problem, dass sie nicht in der Lage sind, die Ursache des betreffenden Problems, mit dem sie zu kämpfen haben, zu finden, und deshalb nicht beurteilen können, ob die Vorschriften für den Datenschutz korrekt befolgt wurden oder ob Gründe für eine rechtliche Anfechtung bestehen [Auch wenn einer betroffenen Person Rechte durch einen Vertrag gewährt werden, wird sie oft nicht beurteilen können, ob ein Vertragsbruch vorliegt, und wenn, durch wen. Dafür ist ein Untersuchungsverfahren außerhalb der formellen zivilrechtlichen Verfahren erforderlich]. Deshalb muss für ein angemessenes Schutzniveau eine Art institutioneller Mechanismus vorhanden sein, der eine unabhängige Untersuchung von Beschwerden ermöglicht.

Die Überwachungs- und Untersuchungsfunktion der Kontrollstelle eines Mitgliedstaats beschränkt sich auf die Datenverarbeitung, die im Hoheitsgebiet des Mitgliedstaats erfolgt [Siehe Artikel 28 Absatz 1 der Richtlinie 95/46/EG]. Werden Daten in einen anderen Mitgliedstaat übermittelt, so gewährleistet ein System der gegenseitigen Unterstützung der Kontrollstellen, dass jede Beschwerde einer betroffenen Person in dem ersten Mitgliedstaat ordnungsgemäß bearbeitet wird. Erfolgt die Übermittlung in ein Drittland, besteht in den meisten Fällen eine solche Garantie nicht. Damit stellt sich die Frage, welche Art Ausgleichsmechanismus festgelegt werden kann, wenn die Datenübermittlung auf der Grundlage eines Vertrags erfolgt.

Eine Möglichkeit bestünde darin, die Aufnahme einer Vertragsklausel zu fordern, die der Kontrollstelle des Mitgliedstaats, in dem der Übermittler der Daten niedergelassen ist, ein Recht auf Einsichtnahme in die von dem Verarbeiter im Drittland vorgenommene Verarbeitung garantiert. Diese Einsichtnahme könnte in der Praxis durch einen gegebenenfalls von der Kontrollstelle ernannten Vertreter vorgenommen werden (beispielsweise eine spezialisierte Buchprüferfirma). Bei diesem Ansatz besteht allerdings das Problem, dass die Kontrollstelle im Allgemeinen keine Vertragspartei ist [Die französische Delegation könnte sich Situationen vorstellen, in denen die Kontrollstelle Vertragspartner ist] und bei der Forderung nach Zugang der Vertrag somit in einigen Rechtssystemen nicht geltend gemacht werden kann. Eine andere Möglichkeit wäre eine gesetzliche Verpflichtung des Empfängers im Drittland unmittelbar gegenüber der entsprechenden Kontrollstelle des EU- Mitgliedstaats, mit der der Empfänger der Daten einwilligt, der Kontrollstelle oder einem benannten Vertreter im Fall einer vermuteten Nichterfüllung der Grundsätze des Datenschutzes den Zugang zu erlauben. Zu dieser Verpflichtung könnte auch gehören, dass die an der Datenübermittlung Beteiligten die Kontrollstelle über jede Beschwerde unterrichten, die sie von einer betroffenen Person erhalten. Bei einer derartigen Vereinbarung wäre die Existenz einer solchen Verpflichtung eine Voraussetzung, die erfüllt sein müsste, bevor die Datenübermittlung stattfinden kann.

Unabhängig von der gewählten Lösung bleiben große Zweifel im Hinblick auf die Frage bestehen, ob es zweckmäßig, praktikabel oder hinsichtlich der Ressourcen für eine Kontrollstelle eines EU-Mitgliedstaats auch wirklich machbar ist, die Zuständigkeit für eine Untersuchung und Überprüfung der Datenverarbeitung zu übernehmen, die in einem Drittland erfolgt.

Gewährleistung einer hohen Befolgungsrate

Auch wenn keine Beschwerde oder kein Problem einer betroffenen Person vorliegt, muss man darauf vertrauen können, dass die Vertragsparteien den Vertrag tatsächlich erfüllen. Das Problem bei der vertraglichen Lösung ist die Schwierigkeit, Sanktionen für die Nichterfüllung festzulegen, die so abschreckend sind, dass von ihnen die für das Herstellen dieses Vertrauens erforderliche Wirkung ausgeht. Auch in Fällen, in denen eine tatsächliche Kontrolle über die Daten weiterhin von innerhalb der Gemeinschaft ausgeübt wird, droht dem Empfänger der Übermittlung möglicherweise keine direkte Strafe, wenn er Daten in Zuwiderhandlung gegen den Vertrag verarbeitet. Stattdessen bliebe die Haftung bei dem in der Gemeinschaft niedergelassenen Übermittler der Daten, der dann mögliche Verluste in einer gesonderten Rechtshandlung gegen den Empfänger eintreiben müsste. Eine solche indirekte Haftung ist möglicherweise nicht ausreichend, um den Empfänger zu veranlassen, den Vertrag in allen Einzelheiten zu erfüllen.

Angesichts dessen wird es wahrscheinlich in den meisten Fällen notwendig sein, eine vertragliche Lösung durch zumindest die Möglichkeit einer Art externer Überprüfung der Verarbeitungstätigkeiten des Empfängers zu ergänzen, z. B. ein Audit durch ein zuständiges Gremium oder ein spezialisiertes Prüfungsunternehmen.

5. Das Problem des vorrangigen Rechts

Eine besondere Schwierigkeit beim vertraglichen Ansatz ist die Möglichkeit, dass die allgemeinen Rechtsvorschriften des Drittlands den Empfänger einer Datenübermittlung verpflichten, unter bestimmten Umständen personenbezogene Daten gegenüber dem Staat offen zu legen (Polizei, Gerichte oder Steuerbehörden), und dass derartige gesetzliche Erfordernisse meist Vorrang vor Verträgen haben, bei denen der Verarbeiter Vertragspartei ist [Das Ausmaß der staatlichen Befugnis zur Forderung der Offenlegung von Informationen ist ebenfalls ein Punkt, der bei der allgemeinen Beurteilung der Angemessenheit des Schutzniveaus in einem Drittland zu berücksichtigen ist.]. Für Verarbeiter in der Gemeinschaft ist diese Möglichkeit in Artikel 16 der Richtlinie angesprochen, dem zufolge Auftragsverarbeiter personenbezogene Daten nur auf Weisung des für die Verarbeitung Verantwortlichen verarbeiten dürfen, es sei denn, es bestehen gesetzliche Verpflichtungen. Nach der Richtlinie müssen sich allerdings derartige Offenlegungen (die naturgemäß für Zweckbestimmungen erfolgen, die mit denen unvereinbar sind, für die die Daten erfasst wurden) auf solche beschränken, die in demokratischen Gesellschaften aus einem der Gründe der öffentlichen Sicherheit nach Artikel 13 Absatz 1 der Richtlinie erforderlich sind. Artikel 6 des Vertrags von Amsterdam garantiert die Einhaltung der in der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten enthaltenen Grundrechte. In Drittländern mag es ähnliche Beschränkungen der Möglichkeiten des Staates, die Bereitstellung personenbezogener Daten von Unternehmen und anderen in ihrem Hoheitsgebiet tätigen Organisationen zu fordern, nicht immer geben.

Es gibt keine einfache Möglichkeit, diese Schwierigkeit zu überwinden. Damit wird lediglich illustriert, welche Grenzen der vertragliche Ansatz hat. In einigen Fällen ist ein Vertrag ein zu schwaches Instrument, um angemessene Garantien für den Datenschutz zu bieten, und Übermittlungen in bestimmte Länder sollten nicht genehmigt werden.

6. Praktische Erwägungen zur Verwendung von Verträgen

Aus der vorstehenden Analyse geht hervor, dass für jeden einzelnen Fall der Datenübermittlung eine detaillierte, den jeweiligen Erfordernissen angepasste Lösung gefunden werden muss. Diese Notwendigkeit der Festlegung von Einzelheiten im Hinblick auf die genauen Zweckbestimmungen und die Voraussetzungen, unter denen die übermittelten Daten verarbeitet werden, schließt die Möglichkeit der Erstellung eines Mustervertrags nicht aus, macht es aber erforderlich, jeden auf diesen Mustervertrag aufbauenden Vertrag entsprechend den besonderen Umständen des Einzelfalls zu ergänzen.

Die Analyse hat zudem ergeben, dass besondere praktische Probleme bei der Untersuchung der Nichterfüllung eines Vertrags bestehen, wenn die Verarbeitung außerhalb der Europäischen Union erfolgt und von dem betreffenden Drittland keine Kontrollstelle vorgesehen ist. Diese beiden Erwägungen laufen darauf hinaus, dass es Situationen geben wird, in denen eine vertragliche Lösung geeignet ist, und andere, in denen ein Vertrag die erforderlichen "angemessenen Sicherheiten" in keiner Weise garantieren kann.

Die notwendige detaillierte Anpassung von Verträgen an die Besonderheiten der jeweiligen Übermittlung impliziert, dass ein Vertrag besonders für Situationen geeignet ist, in denen ähnliche Datenübermittlungen wiederholt vorgenommen werden. Die Schwierigkeiten bei der Überwachung bedeuten, dass eine vertragliche Lösung dann äußerst effizient sein kann, wenn es sich bei den Vertragsparteien um bedeu-

tende Wirtschaftsteilnehmer handelt, die bereits öffentlicher Prüfung und Regelung unterworfen sind [Im Fall von Citybank und "BahnCard" arbeitete der Berliner Datenschutzbeauftragte mit den amerikanischen Bankaufsichtsbehörden zusammen]. Große internationale Netze, wie sie für Kreditkartengeschäfte und Flugbuchungen bestehen, weisen diese beiden Merkmale auf und stellen somit Situationen dar, für die Verträge sehr gut geeignet erscheinen. Unter diesen Umständen könnten sie sogar noch durch multilaterale Vereinbarungen ergänzt werden, von denen eine größere Rechtssicherheit ausgeht.

Auch wenn die an der Übermittlung Beteiligten ein und derselben Unternehmensgruppe angehören oder Tochtergesellschaften sind, dürfte aufgrund der engen Bindungen zwischen dem Empfänger im Drittland und der Einheit mit Sitz in der Gemeinschaft eine weitaus größere Möglichkeit zur Untersuchung der Nichterfüllung des Vertrags bestehen. Unternehmensinterne Übermittlungen sind deshalb ein weiterer Bereich, in dem es ein deutliches Potential für die Entwicklung effizienter vertraglicher Lösungen gibt.

Wichtige Schlussfolgerungen und Empfehlungen

Verträge werden in der Gemeinschaft als Mittel zur Festlegung der Aufteilung der Zuständigkeit für die Erfüllung des Datenschutzes zwischen dem für die Verarbeitung Verantwortlichen und einem beauftragten Auftragsverarbeiter verwendet. Erfolgt bei Datenflüssen in Drittländer der Abschluss eines Vertrages, so muss dieser weiteren Anforderungen entsprechen: Er muss zusätzliche Sicherheiten für die betroffene Person bieten, die dadurch erforderlich werden, dass der Empfänger im Drittland keinem durchsetzbaren Regelwerk von Datenschutzbestimmungen unterliegt, das ein angemessenes Schutzniveau vorsieht.

Die Grundlage für die Beurteilung der Angemessenheit der Sicherheitsmaßnahmen aufgrund einer vertraglichen Lösung entspricht der Grundlage für die Beurteilung der Angemessenheit des allgemeinen Schutzniveaus in einem Drittland. Eine vertragliche Lösung muss die wichtigsten Grundsätze des Datenschutzes und die Mittel umfassen, mit denen die Grundsätze durchgesetzt werden können.

Im Vertrag sind die Zweckbestimmungen, die Mittel und Bedingungen, unter denen die Verarbeitung der übermittelten Daten zu erfolgen hat, genau festzulegen. Dies gilt auch für die Art und Weise, in der die grundlegenden Prinzipien des Datenschutzes anzuwenden sind. Die Rechtssicherheit für die betroffene Person ist umso größer, je mehr der Vertrag den Empfänger in seiner Freiheit beschränkt, die Daten ohne Kontrolle von außen im eigenen Namen zu verarbeiten. Der Vertrag sollte deshalb möglichst als ein Mittel verwendet werden, mit dem die die Daten übermittelnde Stelle die Entscheidungsbefugnis über die in dem Drittland erfolgende Verarbeitung behält.

Verfügt der Empfänger im Hinblick auf die Verarbeitung der übermittelten Daten in gewissem Maße über eigene Entscheidungsgewalt, so ist die Situation nicht so eindeutig, und ein einfacher Vertrag zwischen den an der Übermittlung Beteiligten reicht dann möglicherweise als Grundlage für die Wahrnehmung der Rechte durch Betroffene nicht aus. Vielleicht wird ein Mechanismus benötigt, auf dessen Grundlage der übermittelnde Beteiligte in der Gemeinschaft für alle Schäden haftbar bleibt, die sich aus der in dem Drittland erfolgten Verarbeitung ergeben können.

Weiterübermittlungen an Gremien oder Organisationen, die nicht durch den Vertrag gebunden sind, sollten vertraglich explizit ausgeschlossen werden, sofern es nicht möglich ist, derartige beteiligte Dritte vertraglich auf die Einhaltung derselben Datenschutzgrundsätze zu verpflichten.

Das Vertrauen in die Befolgung der Grundsätze des Datenschutzes nach der Übermittlung von Daten wird gestärkt, wenn die Einhaltung des Datenschutzes durch den Empfänger der Übermittlung einer

externen Überprüfung beispielsweise durch ein spezialisiertes Audit- Unternehmen oder ein Normungs-/Zertifizierungs-Gremium unterworfen ist.

Im Fall eines Problems einer betroffenen Person, das sich vielleicht aus einem Verstoß gegen die vertraglich garantierten Datenschutzbestimmungen ergibt, stellt sich das allgemeine Problem der Sicherstellung der ordnungsgemäßen Prüfung der Beschwerde einer betroffenen Person. Bei der Durchführung einer solchen Prüfung durch die Kontrollstellen des EU-Mitgliedstaats wird es zu praktischen Problemen kommen.

Vertragliche Lösungen sind wahrscheinlich am besten für große internationale Netze (Kreditkartengeschäfte, Flugbuchungen) geeignet, die durch große Mengen sich wiederholender Datenübermittlungen gleicher Art und eine relativ kleine Anzahl bedeutender Wirtschaftsteilnehmer in Branchen charakterisiert sind, die bereits in wesentlichem Umfang öffentlicher Prüfung und Regelung unterworfen sind. Unternehmensinterne Datenübermittlungen zwischen verschiedenen Zweigniederlassungen derselben Unternehmensgruppe sind ein weiterer Bereich, in dem es ein beträchtliches Potential für die Verwendung von Verträgen gibt.

Länder, in denen beim Informationszugang die Befugnisse der staatlichen Behörden über das hinausgehen, was durch die weltweit angenommenen Normen des Schutzes der Menschenrechte erlaubt ist, sind keine sicheren Bestimmungsorte für Übermittlungen auf der Grundlage von Vertragsklauseln.

Kapitel 5:

Ausnahmen von der Anforderung der Angemessenheit

In Artikel 26 Absatz 1 der Richtlinie ist eine begrenzte Zahl von Fällen aufgeführt, in denen Ausnahmen vom Erfordernis der Angemessenheit für Übermittlungen in Drittländer zulässig sind. Diese enggefassten Ausnahmen betreffen überwiegend Fälle, in denen die Risiken für die betroffene Person relativ gering sind oder in denen andere Interessen (Wahrung eines wichtigen öffentlichen Interesses oder des Interesses der betroffenen Person selbst) Vorrang vor dem Recht der betroffenen Person auf den Schutz der Privatsphäre genießen. Als Ausnahmen von der allgemeinen Regel müssen sie restriktiv ausgelegt werden. Zudem können die Mitgliedstaaten im innerstaatlichen Recht festlegen, dass die Ausnahmen in bestimmten Fällen nicht gelten. Dies trifft beispielsweise zu, wenn besonders schutzbedürftige Gruppen wie Arbeitnehmer oder Patienten zu schützen sind.

Bei der ersten Ausnahme muss die betroffene Person ihre Einwilligung ohne jeden Zweifel gegeben haben Es sei darauf verwiesen, dass entsprechend der Definition in Artikel 2 Buchstabe h) der Richtlinie die Einwilligung ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage gegeben worden sein muss. Das Erfordernis der Kenntnis der Sachlage ist insofern besonders wichtig, als damit verlangt wird, dass die betroffene Person über das konkrete Risiko der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau ordnungsgemäß in Kenntnis gesetzt werden muss. Geschieht dies nicht, so darf die Ausnahme nicht angewandt werden. Da die Einwilligung ohne jeden Zweifel erfolgen muss, führt jeglicher Zweifel daran, ob die Einwilligung tatsächlich gegeben worden ist, ebenfalls dazu, dass die Ausnahmeregelung nicht gilt. Damit würde auch in einer Vielzahl von Fällen, in denen die Einwilligung unterstellt wird (weil die betreffende Person beispielsweise auf die Übermittlung aufmerksam gemacht wurde und keinen Einwand dagegen erhoben hat), die Ausnahmeregelung nicht greifen. Von Nutzen dürfte die Regelung dann sein, wenn der Übermittler in direktem Kontakt mit der betroffenen Person

steht, die erforderlichen Informationen problemlos mitgeteilt werden können und die Einwilligung ohne jeden Zweifel erlangt wird. Dies ist z. B. bei Übermittlungen im Rahmen eines Versicherungsschutzes häufig der Fall.

Die zweite und die dritte Ausnahme beziehen sich auf Übermittlungen, die erforderlich sind für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen (oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person) oder zum Abschluss oder zur Erfüllung eines Vertrags, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll. Diese Ausnahmen erscheinen zunächst recht weitgefasst, doch wie die im Folgenden erörterte vierte und fünfte Ausnahme wird ihre Anwendung in der Praxis durch das Kriterium der Erforderlichkeit eingeschränkt: Die übermittelten Daten müssen ausnahmslos für die Erfüllung des Vertrages erforderlich sein. Werden also zusätzliche, nicht zu den wesentlichen Angaben zählende Daten übermittelt oder dient die Übermittlung nicht der Erfüllung des Vertrages, sondern einer anderen Zweckbestimmung (z. B. Nachfassmarketing), gilt die Ausnahme nicht. Was die vorvertraglichen Maßnahmen betrifft, so können dies nur von der betroffenen Person initiierte Situationen sein (wie die Anforderung von Informationen zu einem speziellen Dienst) und nicht solche, die sich aus den Marketingkonzepten der für die Verarbeitung Verantwortlichen herleiten.

Ungeachtet dieser Vorbehalte werden die zweite und die dritte Ausnahme nicht ohne Wirkung bleiben. So dürften sie etwa bei Übermittlungen für die Buchung eines Flugtickets für einen Passagier oder bei Übermittlungen personenbezogener Daten im Zusammenhang mit dem grenzüberschreitenden Zahlungsverkehr oder der Zahlung per Kreditkarte häufig angewandt werden. Die Ausnahmeregelung für Verträge "im Interesse der betroffenen Person" (Artikel 26 Absatz 1 Buchstabe c) deckt speziell auch die Übermittlung von Daten an den Empfänger von Bankzahlungen ab, der, obwohl betroffene Person, meist keine Vertragspartei des Verantwortlichen ist, der die Übermittlung vornimmt.

Zur vierten Ausnahme gehören zwei Komponenten, von denen sich die erste auf Übermittlungen bezieht, die für die Wahrung eines wichtigen öffentlichen Interesses erforderlich oder gesetzlich vorgeschrieben sind. Hierzu mögen bestimmte begrenzte Übermittlungen zwischen öffentlichen Verwaltungen zählen, obwohl Vorsicht geboten ist, damit diese Bestimmung nicht zu weit ausgelegt wird. Dabei reicht ein einfaches öffentliches Interesse nicht aus, sondern es muss sich um ein wichtiges öffentliches Interesse handeln. Aus Punkt 58 geht hervor, dass die Datenübermittlung zwischen Steuer oder Zollverwaltungen oder zwischen Diensten, die für Angelegenheiten der sozialen Sicherheit zuständig sind, generell abgedeckt ist. Auch Übermittlungen zwischen den Kontrollstellen im Finanzdienstleistungssektor können unter diese Ausnahmeregelung fallen. Die zweite Komponente betrifft Übermittlungen, die im Rahmen internationaler Rechtsstreitigkeiten oder Gerichtsverfahren vorgenommen werden, und speziell Übermittlungen, die für die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich sind.

Die fünfte Ausnahme bezieht sich auf Übermittlungen im Interesse der Wahrung lebenswichtiger Interessen der betroffenen Person. Ein einleuchtendes Beispiel wäre hier die dringende Übermittlung von medizinischen Unterlagen in ein Drittland, in dem ein zuvor in der EU behandelter Tourist in einen Unfall verwickelt ist oder sich eine gefährliche Erkrankung zugezogen hat. Allerdings wird in Punkt 31 der Richtlinie das "lebenswichtige Interesse" recht eng als "für das Leben der betroffenen Person wesentliches Interesse" ausgelegt. Ein Interesse aus finanziellen, eigentumsbezogenen oder familiären Gründen wäre im Normalfall ausgeschlossen.

Die sechste und letzte Ausnahme betrifft die Übermittlung aus einem Register, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist, so weit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind. Hinter dieser Ausnahme steht die Absicht, dass in Fällen, in denen ein Register in einem Mitgliedstaat zur Einsichtnahme durch die Öffentlichkeit oder Personen, die ein berechtigtes Interesse nachweisen können, offen steht, die Tatsache, dass die zur Einsichtnahme berechtigte Person in einem Drittland ansässig ist und der Vorgang der Einsichtnahme ohne Datenübermittlung unmöglich ist, die Übermittlung der Informationen nicht verhindert. Entsprechend Punkt 58 ist die Übermittlung der Gesamtheit oder ganzer Kategorien der im Register enthaltenen Daten nicht gestattet. Aufgrund dieser Einschränkungen darf diese Ausnahmebestimmung nicht als allgemeine Ausnahme für die Übermittlung der Daten aus öffentlichen Registern angesehen werden. So kann beispielsweise kein Zweifel darüber bestehen, dass die massenhafte Übermittlung von Daten aus öffentlichen Registern für kommerzielle Zwecke oder die Erfassung ganzer Bestände öffentlich zugänglicher Daten zum Zwecke der Erarbeitung von Profilen bestimmter Personen von den Ausnahmebestimmungen nicht abgedeckt sind.

Kapitel 6:

Verfahrensfragen

In Artikel 25 ist ein auf dem Einzelfall beruhendes Konzept vorgesehen, bei dem die Beurteilung der Angemessenheit sich auf die einzelne Datenübermittlung oder eine Kategorie von Datenübermittlungen bezieht. Dennoch ist natürlich klar, dass angesichts der enormen Anzahl der täglich aus der Gemeinschaft übermittelten personenbezogenen Daten und der zahllosen Akteure, die an den Übermittlungen beteiligt sind, kein Mitgliedstaat imstande ist, jeden einzelnen Fall im Detail zu prüfen, welches System er für die Umsetzung von Artikel 25 auch wählt [Von den Mitgliedstaaten können zur Erfüllung der Pflichten gemäß Artikel 25 unterschiedliche Verwaltungsverfahren festgelegt werden. Dazu gehört die direkte Verpflichtung des für die Verarbeitung Verantwortlichen ebenso wie die Einrichtung von Systemen zur vorherigen Genehmigung oder zur ExPost- Prüfung der Fakten durch die Kontrollstelle.]. Dies heißt natürlich nicht, dass überhaupt keine Fälle einer gründlichen Kontrolle unterzogen werden, sondern dass Mechanismen zu entwickeln sind, mit denen der Entscheidungsprozess für eine große Anzahl von Fällen gestrafft wird, so dass die Entscheidung oder zumindest eine vorläufige Entscheidung ohne unnötige Verzögerung oder übermäßigen Aufwand getroffen werden kann.

Eine solche Rationalisierung ist unabhängig davon notwendig, wer die Entscheidung trifft - der für die Verarbeitung Verantwortliche, die Kontrollstelle oder eine sonstige vom Mitgliedstaat festgelegte Stelle.

i. Anwendung von Artikel 25 Absatz 6 der Richtlinie
   Ein Beitrag zu einem rationelleren Verfahren bestünde, wie in der in der Richtlinie vorgesehen, in der Feststellung, dass bestimmte Drittländer ein angemessenes Schutzniveau gewährleisten. Derartige Feststellungen dienten "nur der Orientierung" und würde daher Fälle unberührt lassen, in denen es zu besonderen Schwierigkeiten kommt. Doch zumindest würde das Problem praktisch angegangen.

   Mit einer solchen Feststellung würde insbesondere für die Wirtschaftsteilnehmer ein Grad von Sicherheit hinsichtlich der Länder geboten, bei denen allgemein von der Gewährleistung eines

"angemessenen" Schutzniveaus ausgegangen werden kann. Zudem würde für Drittländer, die sich noch im Prozess der Entwicklung und Verbesserung der eigenen Schutzsysteme befinden, ein klarer und öffentlicher Anreiz gegeben. Würden obendrein mehrere solcher Feststellungen auf Gemeinschaftsebene getroffen, so wäre dies ein Beitrag zur Festlegung eines einheitlichen Ansatzes in dieser Frage, und es würde verhindert, dass von den Mitgliedstaaten bzw. den Datenschutzstellen unterschiedliche und womöglich einander widersprechende "weiße Listen" erstellt werden.

Dieser Ansatz birgt natürlich auch Schwierigkeiten. An erster Stelle ist dabei der Aspekt zu nennen, dass viele Drittländer über keinen für alle Wirtschaftszweige einheitlich geltenden Schutz verfügen. So gibt es in vielen Staaten Datenschutzbestimmungen für den öffentlichen Sektor, jedoch nicht für die Privatwirtschaft. In einigen Ländern, beispielsweise in den USA, bestehen besondere Gesetze für bestimmte Bereiche (Meldung von Kreditaufnahmen, Unterlagen über die Ausleihe von Videos im Fall der USA), für andere hingegen nicht. Zusätzliche Schwierigkeiten existieren in Ländern mit Föderalstruktur wie den USA, Kanada und Australien, wo sich die Bestimmungen vielfach von Bundesstaat zu Bundesstaat unterscheiden. Wie die Bilanz zeigt, ist es derzeit nicht wahrscheinlich, dass bei vielen Drittländern generell von der Gewährleistung eines angemessenen Schutzniveaus ausgegangen werden kann. Dabei wäre die Aktion dem Anliegen, den für die Verarbeitung Verantwortlichen größere Sicherheit zu bieten, umso weniger dienlich, je kleiner die Anzahl der Länder, für die sich eine positive Feststellung treffen ließe. Weiterhin besteht die Gefahr, dass einige Drittländer die Versagung der Feststellung, dass sie ein angemessenes Schutzniveau bieten, als politische Provokation oder zumindest als politisch diskriminierend ansehen, da die Versagung der Feststellung ebenso durch das Versäumnis, die Bedingungen in dem Land überhaupt zu prüfen, wie im Ergebnis der Beurteilung des Datenschutzsystems zustande gekommen sein kann.

Nach sorgfältiger Abwägung dieser unterschiedlichen Argumente ist die Arbeitsgruppe dessen ungeachtet der Ansicht, dass es nützlich wäre, Arbeiten auf den Weg zu bringen, um die Lage zu erfassen und Feststellungen entsprechend Artikel 25 Absatz 6 zu treffen. Dabei würde es sich um einen kontinuierlichen Prozess handeln, der nicht in einer endgültigen Liste mündet, sondern in einer Liste, die in Abhängigkeit von den Entwicklungen ständig ergänzt und überarbeitet würde. Die positive Feststellung sollte dabei grundsätzlich nicht auf Länder mit horizontalen Datenschutzgesetzen beschränkt sein, sondern auch einzelne Sektoren innerhalb eines Landes umfassen, in denen das Datenschutzniveau angemessen ist, obwohl dies in anderen Sektoren desselben Landes nicht der Fall ist.

Es sei darauf verwiesen, dass der nach Artikel 29 eingesetzten Datenschutzgruppe im Zusammenhang mit Entscheidungen zu einer bestimmten Datenübermittlung oder bei der Feststellung der ”Angemessenheit" gemäß Artikel 25 Absatz 6 keine spezielle Rolle zufällt, da in beiden Fällen das in Artikel 31 genannte Ausschussverfahren zur Anwendung kommt. Eine der speziellen Aufgaben der Datenschutzgruppe nach Artikel 29 besteht jedoch darin, gegenüber der Kommission zum Schutzniveau in der Gemeinschaft und in Drittländern Stellung zu nehmen (siehe Artikel 30 Absatz 1 Buchstabe b). Somit gehören zum Zuständigkeitsbereich der Gruppe nach Artikel 29 durchaus auch die Beurteilung der Lage in bestimmten Drittländern und die Erarbeitung einer vorläufigen Position zum jeweiligen Schutzniveau. Um nicht wirkungslos zu bleiben, sind positive Feststellungen entsprechend Artikel 25 Absatz 6 möglichst breit bekannt zu machen. Wird andererseits festgestellt, dass ein Land nicht über ein angemessenes Schutzniveau verfügt, so bedeutet dies

nicht unbedingt, dass es auf eine "schwarze Liste" gesetzt werden müsste. Gegenüber der Öffentlichkeit müsste erklärt werden, dass es gegenwärtig nicht möglich ist, für das betreffende Land eine allgemeine Orientierung zu geben.

ii. Risikoanalyse konkreter Übermittlungen

Obwohl die Anwendung von Artikel 25 Absatz 6, wie sie hier beschrieben wurde, im Entscheidungsprozess bezüglich einer großen Anzahl von Datenübermittlungen eine wertvolle Hilfe ist, wird es häufig vorkommen, dass für das betreffende Land (ganz oder partiell) eine positive Feststellung nicht möglich ist. Die Art und Weise, in der die Mitgliedstaaten mit diesen Fällen umgehen, hängt davon ab, wie Artikel 25 von ihnen in einzelstaatliches Recht (siehe Fußnote auf der vorherigen Seite) umgesetzt wurde. Ist der Kontrollstelle eine konkrete Handlungsweise vorgegeben, d.h. Datenübermittlungen noch vor der eigentlichen Übermittlung zu genehmigen oder Prüfungen ex post facto im Nachgang vorzunehmen, dürfte es schon allein von der Menge der Übermittlungen her notwendig sein, für die Kontrollstelle ein System der Aufgabenschwerpunkte festzulegen. Ein solches System könnte aus einem vereinbarten Bündel bestimmter Kriterien bestehen, anhand derer eine Übermittlung oder Kategorie von Datenübermittlungen aufgrund der Tatsache, dass sie für die Privatsphäre des Einzelnen eine besondere Gefahr darstellen, als prioritär eingestuft werden könnte.

Selbstverständlich würde sich damit nichts an der Verpflichtung jedes einzelnen Mitgliedstaats ändern, dafür zu sorgen, dass nur solche Übermittlungen zulässig sind, bei denen der Drittstaat ein angemessenes Schutzniveau gewährleistet. Es bestünde also eine Orientierung in der Frage, welche Fälle der Datenübermittlung als "vorrangige Fälle" für eine Prüfung oder sogar eine Untersuchung anzusehen sind. Damit würden auch die zur Verfügung stehenden Mittel in Richtung jener Übermittlungen gelenkt, die in puncto Schutz der betroffenen Personen besonderen Anlass zur Besorgnis geben.

Die Arbeitsgruppe ist der Ansicht, dass bei den folgenden Kategorien von Datenübermittlungen für den Schutz der Privatsphäre ein besonderes Risiko besteht und sie daher spezieller Aufmerksamkeit bedürfen:

Übermittlungen, bei denen auch sensible Kategorien von Datenübermittlungen entsprechend der Definition von Artikel 8 der Richtlinie weitergegeben werden;

Übermittlungen, mit denen die Gefahr finanzieller Schädigung verbunden ist (z. B. Kreditkartenzahlung über das Internet);

Übermittlungen, mit denen eine Gefahr für die persönliche Sicherheit verbunden ist;

Übermittlungen zum Zwecke einer Entscheidung von erheblicher Bedeutung für die betreffende Person (z. B. Entscheidung über die Einstellung oder Beförderung, über eine Darlehensgewährung usw.);

Übermittlungen, mit denen der Betreffende ernsthaft in eine peinliche Lage gebracht werden kann oder sein Ruf beschädigt wird;

Übermittlungen mit dem Ergebnis bestimmter Aktionen, die in bedeutendem Maße ein Eindringen in das Privatleben darstellen, z. B. unerwünschte Telefonanrufe;

Wiederholte Übermittlungen großer Datenbestände (wie über Fernmeldenetze, das Internet u.Ä. verarbeitete Transaktionsdaten);

Übermittlungen, bei denen unter Verwendung neuer Technologien Daten gesammelt werden und dies auf besonders verborgene oder heimliche Art geschieht (z. B. Internet-Cookies).

iii. Standardvertragsklauseln

Wie bereits in Kapitel 4 ausführlich dargestellt ist in der Richtlinie die Möglichkeit vorgesehen, dass in den Fällen, in denen das Schutzniveau nicht angemessen ist, der für die Verarbeitung Verantwortliche durch Vertragsabschluss angemessene Sicherheitsmaßnahmen herbeiführen kann. Nach Artikel 26 Absatz 2 der Richtlinie können die Mitgliedstaaten Übermittlungen auf der Grundlage von Vertragsklauseln genehmigen, wobei die Kommission anschließend von dieser Entscheidung in Kenntnis gesetzt werden muss. Bestehen gegen die Genehmigung Einwände, so kann die Kommission die Entscheidung entsprechend dem in Artikel 31 bestimmten Ausschussverfahren aufheben oder bestätigen. Doch kann die Kommission nicht nur hinsichtlich der Genehmigungen durch die Mitgliedstaaten tätig werden, sondern darf nach Artikel 26 Absatz 4 der Richtlinie auch darüber befinden, ob bestimmte Standardvertragsklauseln ausreichende Garantien bieten, wobei sie auch hier nach dem Ausschussverfahren von Artikel 31 vorgehen muss. Diese Feststellungen sind dann für die Mitgliedstaaten bindend.

Angesichts der nicht zu übersehenden Kompliziertheit vertraglicher Lösungen und der damit verbundenen Schwierigkeiten besteht zweifellos das Erfordernis, den für die Verarbeitung Verantwortlichen, die auf diese Weise mit Verträgen zu arbeiten beabsichtigen, eine abgestimmte Orientierung an die Hand zu geben. Auf der Ebene der Mitgliedstaaten tragen wahrscheinlich die zuständigen staatlichen Stellen ein Großteil der Verantwortung für diese Orientierung, insbesondere im Zusammenhang mit Genehmigungen entsprechend Artikel 26 Absatz 2. Die Behörden der Mitgliedstaaten und die Kommission sollten zusammenarbeiten und ihre Ansichten zu den ihnen vorgelegten Vertragsklauseln austauschen. Für vorgeschlagene Standardvertragsklauseln, die den Behörden der Mitgliedstaaten oder direkt der Kommission vorgelegt werden, sollte ein Verfahren entwickelt werden, mit dem gewährleistet wird, dass diese Klauseln im Interesse der Verhinderung des Entstehens voneinander abweichender einzelstaatlicher Praktiken auch von der Arbeitsgruppe geprüft werden. Bei Entscheidungen gemäß Artikel 26 Absatz 4 könnte sich die Kommission damit auf den Rat der entsprechenden Sachverständigen stützen.

Anhang und Beispiele:

Artikel 25 und 26 der Richtlinie und ihre praktische Auswirkung auf die Übermittlung personenbezogener Daten in Drittländer

Einführung

Im Hauptteil dieser Arbeitsunterlage wird ein allgemeiner Ansatz für die Problematik der Datenübermittlung in Drittländer dargelegt und dabei auf folgendes eingegangen:

Einschätzung des angemessenen Schutzniveaus im Sinne von Artikel 25 der Datenschutzrichtlinie

Einschätzung alternativer Möglichkeiten zur Herbeiführung angemessener Garantien mittels vertraglicher Lösungen, wie sie in Artikel 26 Absatz 2 vorgesehen sind;

Einschätzung der Ausnahmen vom Erfordernis des angemessenen Schutzniveaus entsprechend Artikel 26 Absatz 1.

Die Darlegung der Probleme wäre jedoch unvollständig ohne eine Beschreibung der Art und Weise, wie sich der allgemeine Ansatz dann tatsächlich auf die Übermittlung personenbezogener Daten auswirkt. In diesem Anhang werden daher einige realistische (wenn auch fiktive) Fallbeispiele für die Übermittlung von Daten so geprüft, wie dies aller Wahrscheinlichkeit mit dem In-Kraft-Treten der einzelstaatlichen Gesetze zur Umsetzung der Richtlinie geschehen soll.

Es werden drei Fälle vorgestellt, bei denen im ersten Schritt jeweils zu bewerten ist, ob das Schutzniveau im Bestimmungsland aufgrund der geltenden Gesetze oder der bestehenden freiwilligen Selbstkontrolle im Privatsektor als angemessen gelten kann. Ist dies nicht der Fall, so besteht der zweite Schritt darin, unter den in Artikel 26 Absatz 1 (Ausnahmen) und 2 (vertragliche Lösung) angebotenen Möglichkeiten eine Lösung für das Problem zu ermitteln. Der dritte Schritt, die Verhinderung der Übermittlung, darf nur dann getan werden, wenn keine der Lösungen geeignet ist.

FALL (1):

Datenübermittlung zur Feststellung der Kreditwürdigkeit

Ein Bürger der Gemeinschaft möchte in Land A außerhalb der EG ein Ferienhaus kaufen und stellt bei einem Kreditinstitut in jenem Land einen Kreditantrag. Vom Kreditinstitut wird daraufhin eine Auskunftei mit einer entsprechenden Recherche beauftragt. Der Auskunftei liegt zu der betreffenden Person keine Akte vor, doch lässt sie sich alle Angaben über die bisherige Kreditaufnahme dieser Person von ihrer "Schwesterauskunftei" im Vereinigten Königreich übermitteln. Bei Land A handelt es sich um ein fortgeschrittenes Industrieland mit seit langem bestehenden und stabilen demokratischen Institutionen. Das Justizsystem ist voll ausgebaut und arbeitet effektiv. Es handelt sich um einen föderal verfassten Staat.

ERSTER SCHRITT:

EINSCHÄTZUNG DER ANGEMESSENHEIT DES SCHUTZNIVEAUS

Die geltenden Vorschriften

Der für die Verarbeitung Verantwortliche unterliegt einem Bundesgesetz, das Vorschriften zu personenbezogenen Informationen zum Zwecke der Einschätzung von Kreditvergaberisiken enthält. Der für die Verarbeitung Verantwortliche behauptet zudem, eigene, öffentlich bekannt gemachte Datenschutznormen zu befolgen. Es ist keines der Gesetze der Teilstaaten anwendbar, und ein branchenweiter Selbstkontrollkodex besteht nicht.

Bewertung des Inhalts der anwendbaren Vorschriften

Zunächst sei vermerkt, dass die Mitteilung der im Vereinigten Königreich ansässigen Auskunftei wie jede andere Mitteilung an einen für die Verarbeitung Verantwortlichen im Vereinigten Königreich oder einem anderen Mitgliedstaat den normalen Anforderungen des Rechts des Vereinigten Königreichs unterworfen wäre, mit denen alle Artikel der Richtlinie mit Ausnahme der Artikel 25 und 26 umgesetzt werden. Dies ist deshalb so wichtig, weil sich dadurch die Prüfung der Rechtmäßigkeit der Mitteilung selbst erübrigt. Im Mittelpunkt der Aufmerksamkeit steht daher der Schutz der in das Land A übermittelten Daten.

Bei der Bewertung des Inhalts der Vorschriften sollte logischerweise mit der Bundesgesetzgebung begonnen werden. Werden hier Lücken festgestellt, so sind zunächst die "weniger strengen" Datenschutznormen des Unternehmens zu betrachten, um herauszufinden, ob die Lücken damit ausgefüllt werden. Danach wird eine Aufstellung zu den als notwendig erachteten inhaltlichen Punkten erarbeitet, und es wird beurteilt, ob die erforderlichen inhaltlichen Punkte im Gesetz oder in den Datenschutznormen des Unternehmens enthalten sind.

Der Grundsatz der Beschränkung der Zweckbestimmung kann in diesem Zusammenhang nur die Anforderung betreffen, dass die Sekundärnutzung und -offenlegung der übermittelten Daten mit der Zweckbestimmung, für die die Übermittlung erfolgte, nicht unvereinbar sein dürfen. Die Aufnahme der Daten in eine auf dem freien Markt zu verkaufende oder zu vermietende Versandliste dürfte ebenso als unvereinbar eingestuft werden wie die Offenlegung der Daten gegenüber potentiellen Arbeitgebern oder an der Solvenz der betroffenen Person interessierten Geschäftspartnern. Offenlegung der Daten gegenüber Kreditgebern (Banken, Kreditkartenunternehmen) könnte hingegen als vereinbar angesehen werden. Im hier geschilderten Fall ist im Bundesgesetz tatsächlich eine begrenzte Anzahl von Zweckbestimmungen festgelegt, bei denen die personenbezogenen Kreditinformationen legal offen gelegt werden können. Zu den Zweckbestimmungen gehören "Beschäftigung" und "rechtmäßige geschäftliche Erfordernisse im Zusammenhang mit einer geschäftlichen Transaktion, an der die betroffene Person beteiligt ist." Im letztgenannten Fall umfasst dies bestimmte Nutzungen der Daten für Marketingzwecke, die auch das Marketing von Waren oder anderen Leistungen als Kredite durch Dritte einschließen. Daraus ergibt sich, dass die Zweckbestimmung durch das Bundesgesetz nicht ausreichend begrenzt wird und das Schutzniveau in diesem Punkt nicht ausreicht. Auch die zum Schutz der Privatsphäre vom Unternehmen für sich festgelegten Datenschutznormen tragen nicht zur Verbesserung der Lage bei.

Nach dem Grundsatz der Transparenz müssten der betroffenen Person die Identität der Auskunftei in Land A und mögliche neue Zweckbestimmungen, für die die Daten verarbeitet werden sollen, mitgeteilt werden. Die Art und Weise, in der dies geschieht, sollte der Vorgehensweise in Artikel 11 der Richtlinie vergleichbar sein. Im vorliegenden Fall kennt das Bundesgesetz keine speziellen Transparenzvorschriften, die unmittelbar die Auskunftei betreffen würden. Allerdings muss der Kreditgeber in Land A die betroffene Person davon in Kenntnis setzen, dass er sich zwecks Kreditinformationen an eine Auskunftei wenden wird, deren Namen und Anschrift er jedoch nicht zu nennen braucht. Für die betroffene Person ist also rechtlich nicht garantiert, dass sie darüber informiert wird, dass ihre Daten durch die betreffende Auskunftei verarbeitet werden. Da die Auskunftei mit der betroffenen Person nicht in direktem Kontakt steht, erschiene die Pflicht der Auskunftei zur Kontaktaufnahme mit der betroffenen Person mit dem speziellen Ziel ihrer Unterrichtung als "unverhältnismäßiger Aufwand" im Sinne von Artikel 11 der Richtlinie. Das Schutzniveau in Bezug auf Transparenz ist also offensichtlich ausreichend.

Der Grundsatz der Datenqualität und -verhältnismäßigkeit umfasst mehrere unterschiedliche Elemente. Im Bundesgesetz ist keine Einschränkung für die Sammlung und Verarbeitung unnötiger Daten vorgesehen. Zur Dauer der Datenspeicherung bestehen Vorschriften, mit denen die Verbreitung veralteter Informationen (mehr als zehn Jahre zurückliegende Urteile in Konkursverfahren) verhindert wird, was praktisch zur Löschung dieser Informationen führt. Zwar besteht rechtlich keine Auflage zur Führung korrekter Daten, doch stellt eine betroffene Person, die auf Antrag Zugang zu der sie betreffenden Kreditauskunft bekommen hat, einen Teil der Informationen in Frage, so sind als nichtzutreffend nachweisbare Daten zu löschen. Erneut scheint das Schutzniveau nicht in vollem Umfang angemessen, und auch die Datenschutznormen des Unternehmens gehen über die Regelungen im Bundesgesetz nicht hinaus.

Der Grundsatz der Sicherheit spiegelt sich im Bundesgesetz in dem Erfordernis wider, geeignete Maßnahmen gegen die unrechtmäßige Datenoffenlegung zu ergreifen. Aus den Datenschutznormen des Unternehmens geht hervor, dass zur Verhinderung des unberechtigten Zugriffs auf die Kreditinformationen und ihrer Manipulation ein strenges Kontrollsystem besteht. Hierzu werden sowohl technische Mittel (Passwörter usw.) eingesetzt als auch die Mitarbeiter entsprechend unterwiesen, wobei eine Verletzung dieser Pflicht zu disziplinarischen Maßnahmen führen kann. Damit wäre ein angemessenes Sicherheitsniveau gewährleistet.

Das Recht auf Zugriff und Berichtigung ist bundesrechtlich geregelt und mit dem Recht, wie es diesbezüglich in der Richtlinie besteht, vergleichbar. Wurde einer betroffenen Person der Kredit verwehrt, so ist die Einsichtnahme in die Auskunft kostenlos. Es besteht kein Recht auf Widerspruch, doch kann ein Betroffener Beschwerde bei der zuständigen Bundesbehörde einreichen oder Klage vor Gericht (siehe unten) erheben, wenn seine nach dem Bundesgesetz bestehenden Rechte verletzt wurden.

Sensible Daten zum Gesundheitszustand der betroffenen Person sind Teil der übermittelten Daten. Im Bundesgesetz sind strengere Vorschriften für die Verarbeitung von Informationen im Zusammenhang mit strafrechtlichen Verurteilungen sowie zu Geschlecht, Rasse, ethnischer Herkunft, Alter und Familienstand enthalten, nicht jedoch zu Informationen über den Gesundheitszustand. In den Datenschutznormen der Auskunftei ist jedoch festgelegt, dass bei Kreditauskünften keine Gesundheitsdaten weitergegeben werden, sondern nur bei Überprüfungen im Zusammenhang mit

einer beabsichtigten Einstellung oder dem Abschluss einer Versicherung. In diesen beiden Fällen wird die Verwendung dieser Daten durch die betroffene Person auf den dazu erforderlichen Vordrucken genehmigt. Hier bestünde also für die in diesem Beispiel vorkommenden Gesundheitsdaten ein in der Sache verstärkter Schutz, auch wenn dieser Schutz vom Gesetz nicht vorgesehen ist.

Die Verwendung der Daten für Zwecke des Direktmarketing durch die Auskunftei (und die Offenlegung der Daten gegenüber anderen zu diesem Zweck) ist in diesem Zusammenhang ein wichtiger Punkt. Einer solchen Verwendung steht rechtlich nichts wirklich im Wege, und es gibt kein rechtliches Erfordernis, aus dem heraus dies verwehrt werden kann. Damit ist das Schutzniveau in diesem Punkt eindeutig unangemessen, da insbesondere in diesem Fall die Daten nicht nur durch die Auskunftei (zum Versand von Mailings an Kreditinstitute) verwendet werden, sondern auch gegenüber Dritten für das Vermarkten sowohl von finanztechnischen Produkten als auch branchenfremden Produkten wie Rasenmähern und Urlaubsangeboten offen gelegt werden.

Wie es scheint, kann angesichts der Zweckbestimmung der Übermittlung eine automatisierte Entscheidung darüber getroffen werden, ob der betroffenen Person ein Kredit gewährt werden soll. Für die betroffene Person müssen daher zusätzliche Garantien bestehen. Im Bundesgesetz gibt es Bestimmungen, mit denen die betroffene Person in der Auskunft enthaltene Informationen anfechten und der Auskunft erforderlichenfalls Erklärungen beifügen kann, aber es sind keine Regelungen vorgesehen, nach denen eine auf falschen oder unvollständigen Informationen beruhende Entscheidung angefochten, überprüft und, sollten sich die Einwände als berechtigt erweisen, geändert werden kann. Mit diesem Mechanismus können an einer Auskunft zwar Änderungen vorgenommen werden, um Probleme in der Zukunft zu vermeiden, doch wird das Problem einer bereits getroffenen Kreditentscheidung damit nicht unbedingt angesprochen. Dieser rückwirkende Rechtsschutz ist nicht ausreichend, da nicht vorhanden.

Beschränkungen der Weiterübermittlung der Daten an ein weiteres Drittland oder an Organisationen in anderen, den Vorschriften im Bundesgesetz nicht unterstellten Sektoren in Land A. Weder im Bundesgesetz noch in den Datenschutznormen des Unternehmens ist derartiges vorgesehen.

Anwendungsbereich des Bundesgesetzes und der Datenschutznormen des Unternehmens In einem weiteren Kontrollgang ist sicherzustellen, dass sowohl das Bundesgesetz als auch die Datenschutznormen des Unternehmens für die Daten aller betroffenen Personen und nicht nur für die Daten der Staatsangehörigen oder Bürger des Landes A gelten. Im vorliegenden Fall besteht eine solche Beschränkung des Anwendungsbereichs nicht.

Bewertung der Wirksamkeit des Schutzes

Das betreffende Bundesgesetz ist geltendes Recht, und nach seinen Bestimmungen ist auch eine öffentliche Stelle mit bestimmten externen Überwachungsbefugnissen eingerichtet worden. Zur Durchsetzung ihrer Rechte können die betroffenen Personen den Rechtsweg einschlagen. Allerdings ist die öffentliche Stelle nicht eindeutig dazu verpflichtet, sämtlichen Beschwerden von betroffenen Personen nachzugehen, und einigen Kommentatoren zufolge hat sie sich bei der Durchsetzung des Rechts auch nicht immer durch besondere Aktivität ausgezeichnet. Klagen vor Gericht zur Wiedergutmachung sind für die betroffenen Personen kostspielig und häufig auch zeit-

aufwendig - dies besonders dann, wenn die betroffene Person in einem anderen Land wohnt als in dem, wo das Gerichtsverfahren stattfindet.

Die Datenschutznormen des Unternehmens enthalten keinen eigenständigen Mechanismus, mit dem Betroffene ihre Rechte durchsetzen können, doch sind disziplinarische Strafen für Mitarbeiter vorgesehen, die die Grundsätze verletzen. Mehrere Beschäftigte sind bereits wegen entsprechender Vergehen disziplinarisch zur Verantwortung gezogen worden.

Die Kombination von gesetzlichen Regelungen und unternehmensinternen Datenschutznormen muss anhand der für die verfahrensrechtlichen Mechanismen festgelegten "Ziele" bewertet werden. Im vorliegenden Fall könnten folgende Schlüsselfragen geprüft werden:

Allgemein hohes Einhaltungsniveau

Für das Unternehmen besteht der Hauptanreiz zur Einhaltung der eigenen Datenschutznormen in der Gefahr eines negativen Echos in der Presse, sollte festgestellt werden, dass es sich nicht an die eigenen Vorgaben hält. Zudem werden den Mitarbeitern des Unternehmens für den Fall der Verletzung der Sicherheitsvorschriften disziplinarische Maßnahmen angedroht. Indes reichen diese Mechanismen allein wahrscheinlich nicht aus, um die Einhaltung der Datenschutznormen in der Praxis zu gewährleisten. Diese Schlussfolgerung würde anders ausfallen, wenn:

1. die Datenschutznormen des Unternehmens ihren Ausdruck in einem branchenweiten, vom Fachverband erarbeiten Verhaltenskodex gefunden hätten, nach dessen Bestimmungen ein Unternehmen, das gegen den Kodex verstößt, sofort aus dem Fachverband ausgeschlossen würde oder
2. es nach einem allgemeinen Rechtsgrundsatz möglich wäre, von einer staatlichen Stelle gegen Unternehmen, die die eigenen veröffentlichen Datenschutznormen verletzen, wegen "unlauterer und betrügerischer" Geschäftspraktiken strafrechtlich vorzugehen.

Was das Bundesgesetz angeht, so wird die Einhaltung dadurch gefördert, dass vom Betroffenen im Falle der Nichteinhaltung Klage erhoben werden kann. Die Aussicht, vor Gericht auf der Anklagebank zu sitzen, dürfte auf den für die Verarbeitung Verantwortlichen einen gewissen abschreckenden Effekt ausüben. Allerdings ist die Wahrscheinlichkeit einer direkten externen Prüfung der Datenverarbeitungsverfahren sehr gering, da die staatliche Stelle erst reagiert, wenn sie beispielsweise durch den Beschwerdeführer oder die Presse darauf aufmerksam gemacht wird.

Unterstützung und Hilfe für einzelne betroffene Personen

Es ist eindeutig so, dass eine staatliche Stelle vorhanden ist, bei der betroffene Personen Beschwerde gegen die für sie erstellten Kreditauskünfte einlegen können. Die Kosten der Untersuchungen im Zusammenhang mit der Beschwerde braucht die betroffene Person nicht zu tragen.

Angemessene Entschädigung

Zwar hat im Falle der Verletzung der recht enggefassten Regelungen im Bundesgesetz die betroffene Person die Möglichkeit, eine Wiedergutmachung auf dem Gerichtswege durchsetzen,

doch ist dies ein relativ kostspieliges Unterfangen, und häufig fehlt es hierbei an Unterstützung durch die staatliche Stelle. Das Gericht kann den für die Verarbeitung Verantwortlichen zur Leistung von Schadenersatz verurteilen (sofern es der Meinung ist, dass eine Schädigung erfolgte) und ihn anweisen, die Datenverarbeitungsverfahren und den Inhalt der betreffenden Kreditkartei zu ändern. Für die Verletzung der lediglich in den internen Datenschutznormen festgelegten Datenschutzgrundsätze ist eine solche Entschädigung nicht möglich.

Der Urteilsspruch

1. Etliche der Datenschutzgrundsätze, die im Diskussionspapier als "Kerngrundsätze" herausgearbeitet wurden, finden sich in der einen oder anderen Form im für die Kreditkartei geltenden Bundesgesetz, während andere in den Datenschutznormen des Unternehmens verankert sind. Doch auch wenn beide zusammen betrachtet werden, kann nicht behauptet werden, dass sämtliche "Kerngrundsätze" vorkommen. Selbst bei denen, die vorhanden sind (z. B. der Grundsatz der Beschränkung der Zweckbestimmung), sind einige nur in relativ abgeschwächter Form anzutreffen.
2. Hier ergibt sich als allgemeineres Problem die Frage, ob die Datenschutznormen des Unternehmens überhaupt als ausreichend wirksamer Mechanismus in Betracht gezogen werden können. Werden die Datenschutznormen nicht dadurch untermauert und durchsetzbarer gemacht, dass dem Fachverband oder einer staatlichen Stelle die Befugnis zur externen Kontrolle übertragen wird, so sind die Bestimmungen dieser Normen größtenteils nicht durchsetzbar und brauchen daher nicht berücksichtigt zu werden.
3. Auch wenn die zur Durchsetzung des Bundesrechts eingerichtete öffentliche Stelle nicht ganz mit denselben Befugnissen ausgestattet ist wie die typische Datenschutzbehörde in Europa, so bietet sich durch das Gesetz eine gewisse Rechtssicherheit, was insbesondere auf das gut funktionierende Rechtssystem und die "Prozesskultur" in Land A zurückzuführen ist. Das Gesetz enthält klar formulierte Vorschriften zum möglicherweise wichtigsten aller Datenschutzgrundsätze, dem Recht auf Zugriff und Berichtigung, und es grenzt die Zweckbestimmung der Datenverarbeitung in gewissem Maße ein.

Schlussfolgerung

Das Schutzniveau ist unangemessen, da das Gesetz zu wenige der "Kerngrundsätze" beinhaltet, und die unternehmensinternen Datenschutznormen sind für sich allein genommen kein wirksames Mittel zur Gewährleistung von Schutz. Der Urteilsspruch könnte auf Angemessenheit lauten, wenn das Gesetz in Richtung solcher Grundsätze wie Transparenz und Schutz von Daten zum Gesundheitszustand ausgebaut oder die unternehmensinternen Datenschutznormen mit Hilfe einer der vorgeschlagenen Methoden wirksamer gestaltet werden (d.h. Einhaltung als Voraussetzung für die Mitgliedschaft im Fachverband oder Bevollmächtigung einer staatlichen Stelle zur strafrechtlichen Verfolgung des Unternehmens wegen irreführender und betrügerischer Geschäftspraktiken im Falle der Verletzung der eigenen Datenschutznormen).

ZWEITER SCHRITT:

LÖSUNGSSUCHE

Von den in Artikel 26 Absatz 1 genannten möglichen Ausnahmen kommt nur der die Einwilligung der betroffenen Person betreffende Buchstabe a) in Frage. Die in Buchstabe b) geregelte Ausnahme im Interesse der Erfüllung eines Vertrags ist nicht anwendbar, da zwischen der übermittelnden Partei, der

im Vereinigten Königreich ansässigen Auskunftei, und der betroffenen Person kein Vertragsverhältnis besteht. Auch kann schwerlich darauf verwiesen werden, dass die Übermittlung zur Erfüllung eines Vertrags "im Interesse der betroffenen Person" erforderlich sei, wie dies für die Ausnahme in Buchstabe c) geregelt ist.

Mit der Einwilligung durch die betroffene Person würde für das Problem jedoch eine relativ unkomplizierte Lösung gefunden. Die Einwilligung könnte entweder direkt durch die im Vereinigten Königreich ansässige Auskunftei oder in ihrem Auftrag durch das Kreditinstitut in Land A erlangt werden, das hierzu die betroffene Person auf dem Kreditantragsformular um Einwilligung ersuchen könnte. Unabhängig vom gewählten Verfahren sollte die betroffene Person von den konkreten Gefahren in Kenntnis gesetzt werden, die mit der Übermittlung der Daten in ein Land ohne angemessenes Schutzniveau verbunden sind.

Solange Übermittlungen dieser Art noch relativ selten sind, besteht die zweckmäßigste Methode wahrscheinlich darin, die Einwilligung jeweils einzeln einzuholen. Kommt es jedoch zu einem systematischeren weltweiten Datenaustausch mit Auskunfteien, so können andere Vorkehrungen, wie vertragliche Lösungen oder ein internationaler Verhaltenskodex, getroffen werden.

FALL (2):

Übermittlung sensibler Daten in der Luftfahrt

Ein portugiesischer Bürger bucht in einem Lissabonner Reisebüro einen Flug an Bord einer Maschine einer in Land B ansässigen Luftfahrtgesellschaft. Dabei wird u.a. erfasst, dass der Bürger behindert ist und einen Rollstuhl benutzt. Die Daten werden in ein internationales Computerreservierungssystem eingegeben und von dort durch die Fluggesellschaft in ihre Passagierdatenbank in Land B heruntergeladen, in der sie auf unbegrenzte Zeit gespeichert werden. Von der Fluggesellschaft werden die Daten abgesehen von internen Planungszwecken dazu verwendet, die Dienstleistung für den Passagier bei künftigen Flügen mit dieser Fluggesellschaft zu verbessern [Dieser Fall weist gewisse Ähnlichkeiten mit einem tatsächlich geschehenen Fall auf, der schwedischem Recht unterliegt und in den amerikanische Fluggesellschaften und die Lufthansa verwickelt sind. Gegenwärtig läuft das Berufungsverfahren].

ERSTER SCHRITT:

EINSCHÄTZUNG DER ANGEMESSENHEIT DES SCHUTZNIVEAUS

Die geltenden Vorschriften

In Bezug auf die Daten in der Datenbank der Fluggesellschaft in Land B bestehen keine Datenschutzbestimmungen, obwohl es für Daten in Computerreservierungssystemen einen internationalen Verhaltenskodex gibt.

Bewertung des Inhalts der anwendbaren VorschriftenEs sind keine Vorschriften anwendbar.
Bewertung der Wirksamkeit des Schutzes

Nicht zutreffend
Der UrteilsspruchDas Schutzniveau in Land B ist insbesondere angesichts der Sensibilität der Daten nicht angemessen.

ZWEITER SCHRITT:
LÖSUNGSSUCHE

Die Übermittlung der Daten an das Computerreservierungssystem und ihre Verwendung durch die Fluggesellschaft zum Zwecke der Erbringung der entsprechenden Dienstleistung für den behinderten Passagier im Zusammenhang mit dem betreffenden Flug stellt eine Übermittlung dar, die für die Erfüllung des Vertrags zwischen dem Passagier und der Fluggesellschaft (Artikel 26 Absatz 1 Buchstabe b)) erforderlich ist. Für den weiteren Verbleib der Daten (einschließlich sensibler Daten zum Gesundheitszustand der betroffenen Person) in der Datenbank der Fluggesellschaft ist dies jedoch kein Grund. Folglich muss die Übermittlung der Daten an die Fluggesellschaft von einer anderen Ausnahmeregelung abgedeckt sein.

Wie in Fall (1) wäre die Einwilligung der betroffenen Person die beste Lösung. Sie könnte vom Reisebüro in Lissabon im Namen der Fluggesellschaft eingeholt werden. Dabei sollten der betroffenen Person die mit der Speicherung der Daten in Land B verbundenen Risiken ebenso mitgeteilt werden wie die Tatsache, dass die Übermittlung und die Speicherung der Daten in der Datenbank der Fluggesellschaft aus Gründen, die mit dem gebuchten Flug in Verbindung stehen, nicht erforderlich sind.

FALL (3):

Übermittlung von Daten für Marketinglisten

Ein Unternehmen in den Niederlanden ist auf die Erstellung von Versandlisten spezialisiert. Unter Verwendung der Vielzahl unterschiedlicher Quellen, die es in den Niederlanden für öffentliche Informationen gibt, sowie von Kundenverzeichnissen von anderen niederländischen Unternehmen entstehen Listen, in denen Personen aufgeführt sind, die einem bestimmten sozio-ökonomischen Profil entsprechen. Verkauft werden diese Listen an die Kunden dieser Firma nicht nur in den Niederlanden und der EU, sondern auch in zahlreichen Drittländern. Die Empfängerunternehmen nutzen die Listen (in denen die Postanschrift, die Telefonnummer und häufig auch die E- Mail-Adresse angegeben sind), um mit den in den Listen aufgeführten Personen in Kontakt zu treten und ihnen die unterschiedlichsten Erzeugnisse und Dienstleistungen zu verkaufen. Sehr viele der auf den Listen genannten Personen haben bei der niederländischen Datenschutzbehörde Beschwerde gegen die Marketingangebote eingelegt.

Die geltenden Vorschriften

Einige der Unternehmen, die die Versandlisten der niederländischen Firma kaufen, sind in Ländern ansässig, in denen allgemeine gesetzliche Datenschutzvorschriften gelten, die das Recht der betroffe-

nen Personen beinhalten, die Entgegennahme von Marketingangeboten zu verwehren. Andere befinden sich in Ländern ohne derartige gesetzliche Regelungen, sind jedoch Mitglied von Selbstkontrollvereinigungen, von denen Datenschutzkodizes erarbeitet worden sind. Weitere Firmen unterliegen überhaupt keinen Datenschutzvorschriften.

Bewertung des Inhalts der anwendbaren Vorschriften

In diesem Fall müssten zahllose Gesetze und Kodizes bewertet werden. Bleibt die in den Niederlanden ansässige Firma ihrem Grundsatz treu, ihre Listen an Unternehmen in jedem beliebigen Land der Welt zu verkaufen bzw. zu vermieten, so kommt es zwangsläufig zu Situationen, in denen das Schutzniveau nicht angemessen ist.

ZWEITER SCHRITT:

LÖSUNGSSUCHE

Im vorliegenden Beispiel wäre es für die niederländische Firma kaum möglich, die Einwilligung jeder einzelnen Person zur Aufnahme in die Versandlisten zu erlangen, da die Daten aus öffentlichen Quellen stammen und ohne direkten Kontakt mit der betroffenen Person erfasst wurden. Es ist daher nicht wahrscheinlich, dass hier eine der Ausnahme von Artikel 26 Absatz 1 greift.

Der niederländischen Firma stehen zwei Möglichkeiten offen, die sie alternativ oder im Verbund nutzen kann. Zum einen könnte sie den Handel mit den Versandlisten auf Unternehmen in Ländern begrenzen, in denen aufgrund von gesetzlichen Regelungen bzw. entsprechenden Instrumenten der freiwilligen Selbstkontrolle eindeutig feststeht, dass ein angemessenes Schutzniveau gewährleistet ist. Bei der Entscheidung könnte sich die Firma an möglicherweise bestehenden "weißen Listen" orientieren.

Als zweite Möglichkeit könnten von allen Kunden (oder zumindest von den Kunden in Ländern mit quot unangemessenem" Schutzniveau) vertragliche Verpflichtungen hinsichtlich der übermittelten Daten gefordert werden. Bei den vertraglichen Regelungen sollten die in Kapitel 4 des Haupttextes gegebenen Hinweise befolgt werden. Insbesondere sollte dabei gesichert werden, dass die niederländische Firma gemäß niederländischem Recht für alle Verletzungen der Datenschutzgrundsätze seitens der Empfängerunternehmen der übermittelten Versandlisten haftbar bleibt.

Mit einer solchen vertraglichen Lösung würde bei ordnungsgemäßer Umsetzung ein Beitrag zur Überwindung des Handelshemmnisses geleistet, das das Fehlen eines angemessenen Schutzniveaus in bestimmten Drittländern darstellt.

Geschehen zu Brüssel, 24. Juli 1998

Für die Arbeitsgruppe
Der VorsitzendeP. J. HUSTINX

D. Beschlüsse der International Working Group on Data Protektion in Telecommunications

Gemeinsamer Standpunkt zu
Datenschutz bei Suchmaschinen im Internet
angenommen auf der 23. Sitzung
in Hong Kong SAR, China
15. April 1998

- Übersetzung -

Gegenwärtig enthält das Internet eine riesige Menge an Informationen über fast jeden Sachverhalt, den man sich vorstellen kann. Zum Auffinden der gewünschten Information im Internet sind Suchmaschinen in den letzten Jahren immer beliebter geworden.

Mit diesen Suchmaschinen kann man auch nach personenbezogenen Daten suchen. Als Ergebnis erhält man ein Profil der Aktivitäten der gesuchten Person auf dem Internet. Suchmaschinen können auch für das “data-mining” genutzt werden. Da das Internet für den Austausch von Informationen und andere Aktivitäten (z. B. den elektronischen Geschäftsverkehr) immer populärer wird, kann dies zu einer Gefährdung der Privatsphäre führen.

Die Datenschutzbeauftragten haben sich bereits in der Vergangenheit besorgt über die Möglichkeit gezeigt, Persönlichkeitsprofile von Bürgern zu erstellen. Dies ist jetzt in einem gewissen Maß auf globaler Ebene durch die im Internet zur Verfügung gestellte Technologie möglich geworden. Darüber hinaus könnte die geplante Einführung von Filterprogrammen für Datenschutzzwecke zu weiteren Gefährdungen führen, falls die Datenschutzpräferenzen, die vom Benutzer in diesen Programmen festgelegt werden, von Suchmaschinen überwacht werden. Die Arbeitsgruppe empfiehlt daher, dass jedes Filterprogramm so konstruiert sein muss, dass die Datenschutzpräferenzen der Nutzer nicht durch die Betreiber von Websites oder Dritten überwacht und aufgezeichnet werden können.

Schließlich erinnert die Arbeitsgruppe im Hinblick auf übermittelte oder veröffentlichte personenbezogene Daten an zwei Prinzipien, auf die sich ihr gemeinsamer Standpunkt stützt:

auch personenbezogene Daten, die der Nutzer freiwillig veröffentlicht hat, unterliegen den für sie geltenden Schutzbestimmungen;

der Einzelne sollte in jedem Fall und zu jedem Zeitpunkt das Recht haben, der Veröffentlichung seiner personenbezogenen Daten in einem Internet-Angebot zu widersprechen. Er oder sie sollte das Recht haben zu verlangen, dass der Zweck respektiert wird, für den die Daten veröffentlicht worden sind.

Empfehlungen

Die Arbeitsgruppe hat bereits in der Vergangenheit auf die mit der Nutzung des Internets verbundenen Datenschutzprobleme hingewiesen und Empfehlungen zu Möglichkeiten, diese Probleme zu lösen, ausgesprochen. Die Regulierungsbehörden könnten das Angebot von Suchmaschinen auf die Suche nach Namen beschränken und die Abfrage von ausufernden und komplexen Suchprofilen verbieten. Allerdings dürfte es aufgrund der internationalen Struktur des Internets unmöglich sein, das Netz umfassend durch gesetzliche Maßnahmen zu regulieren.

Die Nutzer des Internets können gleichzeitig auch Informationsanbieter sein. Sie sollten sich darüber im Klaren sein, dass jedes personenbezogene Datum, das sie auf dem Netz publizieren (z. B. bei der Einrichtung ihrer eigenen Homepage, einem bei den großen Online-Diensteanbietern üblichen Angebot), von Dritten für die Erstellung eines Profils genutzt werden kann. Die Nutzer sollten die Möglichkeit haben, die Nutzung ihrer Daten auf bestimmte Zwecke zu beschränken.

Darüber hinaus können mit Suchmaschinen auch Nachrichten, die in News Groups eingestellt worden sind, durchsucht werden, womit den Profilen weitere Informationen darüber hinzugefügt werden können, wer welche Meinung über welchen Sachverhalt geäußert hat. Eine Möglichkeit, diese Gefährdung der Privatsphäre zu minimieren, könnte in der Nutzung von Pseudonymen bei der Teilnahme an News-Diensten bestehen. Daher sollten Diensteanbieter und Softwarehersteller im Internet ihren Nutzern solche Pseudonymdienste anbieten. Die Nutzung solcher Dienste könnte auch die Bedrohung für die Privatsphäre des Nutzers minimieren, da die Erstellung eines Profils über seine oder ihre Interessen dann unmöglich wäre. Gleichzeitig sollten die Nutzer auf das Risiko aufmerksam gemacht werden, das sie eingehen, wenn sie an News-Diensten unter ihrer echten E-mail-Adresse oder sogar ihrem wirklichen Namen teilnehmen.

Die Nutzer sollten darüber hinaus in die Lage versetzt werden, Teile ihrer eigenen Informationsangebote auf dem Netz gegen die Überwachung durch Suchmaschinen zu schützen. Dies kann durch das Setzen einer “no-robots”-Option in ihrem Website-Programm erreicht werden. Allerdings setzt die Wirksamkeit dieser Einrichtung voraus, dass sie von den Anbietern von Suchmaschinen beachtet wird.

In dem Vertrag oder der Übereinkunft, die zwischen dem Betreiber einer Suchmaschine und dem Benutzer geschlossen wird, sollte festgelegt werden, dass der Betreiber sich an die Richtlinie zum Schutz personenbezogener Daten der Europäischen Union hält. Aussagen wie: “Der Betreiber der Suchmaschine wird keine Informationen über den Suchvorgang oder den Benutzer der Suchmaschine speichern. Nach Beendigung der Suche bleiben keine Daten gespeichert” sollten in den Vertrag aufgenommen und umgesetzt werden.

Im Hinblick auf die Notwendigkeit, die Konformität von Suchmaschinen mit den grundlegenden Prinzipien des Datenschutzes herzustellen, ist eine Möglichkeit zur Kontrolle erforderlich. Die genauen Methoden dafür (z. B. Auditing, Evaluierung, Zertifizierung) sollten in einer Studie untersucht werden, die unterschiedliche Situationen berücksichtigt.

Zum Schutz der Privatsphäre der Benutzer ist der umfassende Einsatz von datenschutzfreundlichen Technologien erforderlich, wo dies möglich ist. Auf Wunsch des Benutzers muss ein technisches Mittel zum Schutz seiner Identität verfügbar sein, das vollständige Anonymität während der Suche ermöglicht. Der Austausch von Daten muss in technischer Hinsicht dem Prinzip der Angemessenheit entsprechen, wie es in den Leitlinien der OECD von 1980 und der Richtlinie der Europäischen Union von 1995 festgelegt ist.

Um eine Analyse des Datenverkehrs zu verhindern, sollten konventionelle Sicherheitsmaßnahmen wie die permanente Übertragung zufällig generierter Zeichenfolgen angewandt werden.

Gemeinsamer Standpunkt
im Hinblick auf Invert-Suche in Teilnehmerverzeichnissen
angenommen bei der 23. Sitzung in Hong Kong, SAR, China
15. April 1998

- Übersetzung -

Inverse Verzeichnisse werden durch Verarbeitung personenbezogener Daten aus Teilnehmerverzeichnissen erzeugt. Die Nutzung inverser Verzeichnisse zur Erlangung der Identität und der Adresse einer Person aufgrund einer Telefon- oder Telefax-Nummer oder einer E-mail-Adresse kann erhebliche negative Auswirkungen auf den Datenschutz haben und sollte daher spezifischen Regelungen zum Schutz des Persönlichkeitsrechts unterliegen.

In einigen Staaten existieren Regelungen, die den auf ihrem Territorium ansässigen Anbietern von Telekommunikation das Angebot von inversen Verzeichnissen verbieten. In diesem Zusammenhang stellen die Teilnehmer an der Sitzung der Internationalen Arbeitsgruppe zum Datenschutz in der Telekommunikation am 14. und 15. April 1998 in Hong Kong fest, dass

- die Existenz inverser Verzeichnisse ohne spezielle Schutzvorschriften zur Gefährdung des Datenschutzes im Rahmen privater Beziehungen zwischen Personen führen kann;

- die kommerzielle Nutzung inverser Verzeichnisse möglicherweise schädliche Konsequenzen für Personen haben kann, die ausschließlich ihre Telefonnummer angeben wollten, insbesondere im Zusammenhang mit Kleinanzeigen in Zeitungen;

- der Zweck eines inversen Verzeichnisses nicht identisch mit dem Zweck eines Telefonverzeichnisses ist; mit einem Telefonverzeichnis ist es möglich, die Telefonnummer einer bekannten Person auf Grundlage ihres Namens und eines geographischen Kriteriums zu erhalten, während der Zweck eines inversen Verzeichnisses in der Suche nach der Identität und der Adresse von Teilnehmern besteht, bei denen nur die Telefonnummer bekannt ist;

- Teilnehmer das Recht haben müssen, nicht in Telefonverzeichnisse aufgenommen zu werden oder der kommerziellen Nutzung ihrer Daten zu widersprechen, wie dies bereits in der Gemeinsamen Erklärung der Arbeitsgruppe bei ihrer Sitzung in Berlin im Jahre 1989 dargelegt wurde. Dass eine Person, der nur die Telefonnummer des Teilnehmers bekannt ist, dessen Adresse und Identität durch Nutzung eines inversen Verzeichnisdienstes erhält, sollte nur mit Einwilligung des Teilnehmers möglich sein;

- obwohl das Umsortieren in ein inverses Verzeichnis in manchen Fällen legitimen Interessen dienen kann, wie dem Schutz von Menschenleben oder der öffentlichen Sicherheit, die regelmäßige Bekanntgabe der Identität und der Adresse eines Teilnehmers auf der Basis seiner Telefonnummer eine unzulässige Erhebung von Informationen darstellt, wenn die Teilnehmer der Bekanntgabe ihrer Daten durch einen solchen Dienst nicht im Vorhinein widersprechen konnten;

- auch die Verarbeitung von Abrechnungsdaten, Einzelverbindungsnachweisen oder der Anzeige der Nummer des Anrufenden im Hinblick auf die Möglichkeit zur Invert-Suche oder von inversen Verzeichnissen analysiert werden muss.

Sie stimmen darin überein, dass, wo inverse Verzeichnisse nicht durch Gesetz verboten sind,

- diese Dienste eine ausdrückliche freiwillige Einwilligung erfordern. Wenigstens ein Widerspruchsrecht und das Recht auf Auskunft, die generell von existierenden nationalen und internationalen Regelungen über den Schutz personenbezogener Daten anerkannt sind, sollten garantiert werden;

- es in jedem Fall notwendig ist, den Teilnehmern bei der Datenerhebung ein Recht auf Information durch die Anbieter von Telefon- oder E-mail-Diensten über die Existenz von Diensten zur Invert-Suche einzuräumen. Falls die ausdrückliche Einwilligung nicht erforderlich ist, müssen die Teilnehmer das Recht zum Widerspruch haben und auf dieses Recht hingewiesen werden.

Gemeinsamer Standpunkt
über die öffentliche Verantwortung im Hinblick auf das Abhören privater Kommunikation
angenommen bei der 23. Sitzung in Hong Kong SAR, China
15. April 1998

- Übersetzung -

1. Während der Einzelne die vertrauliche Behandlung seiner privaten Kommunikation erwarten können muss, können andere öffentliche Interessen in bestimmten Fällen das Abhören durch die zuständigen Behörden rechtfertigen.

2. Das Abhören sollte nur unter besonderen Umständen erlaubt sein, wo es aufgrund schwerer Verbrechen gerechtfertigt ist, und angemessenen Schutzmaßnahmen unterliegen - wie der richterlichen Anordnung, der Benachrichtigung der Betroffenen, Beschränkungen der Nutzung und Anforderungen an die Vernichtung von Tonbändern und Protokollen. (Dieses Papier behandelt weder diese Angelegenheiten noch Fälle, in denen das Abhören möglicherweise für den technischen Betrieb von Netzen oder Zwecke der Regulierungsbehörden erforderlich ist.)

3. Das autorisierte Abhören muss notwendigerweise ohne das vorherige Wissen der Betroffenen ausgeführt werden. Allerdings sollten zur Einhaltung der Prinzipien der Offenheit, der Transparenz und der Verantwortlichkeit Mechanismen geschaffen werden, um die Öffentlichkeit zu versichern, dass die Möglichkeit zum Abhören gesetzmäßig, angemessen und verhältnismäßig genutzt wird.

4. Solche Mechanismen sollten einschließen:

   das Führen von Protokollen

   Überwachung und Kontrolle

   regelmäßige öffentliche Berichterstattung.

5. *Protokollierung*: Behörden, die Abhörmaßnahmen durchführen, sollten angemessene Protokolle zum Nachweis der gesetzlichen Befugnis und der Rechtmäßigkeit jeder Abhörmaßnahme führen. Die Verpflichtung zur Führung von Protokollen könnte auch auf die beteiligten Anbieter von Telekommunikationsdiensten ausgedehnt werden.

6. *Überwachung und Kontrolle*: Einer Einrichtung, die unabhängig von der untersuchenden Behörde ist, sollte die Aufgabe zugewiesen werden, die Einhaltung der Abhörgesetze zu überprüfen; sie sollte die notwendigen Befugnisse, Möglichkeiten und Ressourcen haben, Untersuchungen durchzuführen.

7. *Öffentliche Berichterstattung:* In regelmäßigen Abständen sollten Übersichten öffentlich zugänglich gemacht werden, die den Umfang und die Merkmale von Abhöraktivitäten dokumentieren, umso den gesamten Grad des Eindringens in die Privatsphäre anzuzeigen. Berichte können Statistiken enthalten über:

   die Anzahl der angeordneten Abhörmaßnahmen und ihre Dauer

   die Anzahl der abgelehnten Anträge auf eine Abhörmaßnahme

Genehmigungen mit besonderen Merkmalen oder Bedingungen (wie z. B. die Befugnis, private Grundstücke zu betreten)

die Anzahl der abgehörten Kommunikationsvorgänge und der identifizierten Einzelpersonen

die Art der verschiedenen abgehörten Kommunikationsdienste (wie Telefon, Fax, E-mail, Pager und Sprachbox-Dienste)

generelle Klassifizierungen von Orten, an denen Abhörmaßnahmen durchgeführt wurden (z. B. Geschäftsräume, Privatwohnungen, Fahrzeuge)

die Art der untersuchten Straftaten

die Resultate und die Effektivität von Abhörmaßnahmen, wie z. B. Fälle, in denen keine Hinweise für Verstöße gefunden wurden, in denen Anklage erhoben wurde und in denen Abhörprotokolle als Beweismittel verwendet wurden und ein Schuldspruch erreicht wurde

die Kosten von Abhörmaßnahmen.

Die Informationen in den Berichten sollten in klarer und verständlicher Weise gefasst sein; sie sollten Trends und besondere Eigenschaften von Abhöraktivitäten während des Berichtszeitraums enthalten.

Gemeinsamer Standpunkt
zu grundlegenden Eigenschaften datenschutzfreundlicher Technologien (z. B. P3P) im WorldWideWeb
angenommen bei der 23. Sitzung in Hong Kong SAR, China
15. April 1998

- Übersetzung -

Die Internationale Arbeitsgruppe zum Datenschutz in der Telekommunikation unterstützt jegliche Bemühungen zur Entwicklung von Technologien, die den Schutz der Privatsphäre der Benutzer im WorldWideWeb verbessern helfen.

Unter diesem Gesichtspunkt hat die Arbeitsgruppe mit besonderem Interesse auf ihrer 22. Sitzung in Berlin am 2. September 1997 und der 23. Sitzung in Hong Kong am 14. April 1998 von dem Platform for Privacy Preferences Project (P3P) Kenntnis genommen, das gegenwärtig durch das WorldWideWeb-Konsortium durchgeführt wird.

Obwohl noch eine Reihe von technischen Details zu klären ist, einschließlich des Ausmaßes, in dem Punkte wie Datensicherheit, Qualität der Daten, Speicherungsdauer sowie Auskunft und Berichtigung von Daten behandelt werden sollen, möchte die Arbeitsgruppe die folgenden grundlegenden Bedingungen darlegen, die von jeder technischen Plattform für den Datenschutz im WorldWideWeb mit dem Ziel der Verhinderung einer systematischen Sammlung personenbezogener Daten berücksichtigt werden sollten:

1. Technologie allein kann nicht die Lösung zur Sicherstellung des Datenschutzes im Web sein. Sie muss innerhalb eines regulatorischen Rahmens angewandt werden (dieser kann sowohl in gesetzlichen Regelungen als auch in Verträgen und Verhaltensregeln bestehen, die gleichartige Garantien im Hinblick auf ihre Durchsetzung bieten, einschließlich Sanktionen, eines effektiven und unabhängigen Überwachungssystems und Rechtsschutzes für den Einzelnen).

2. Jeder Nutzer sollte die Möglichkeit haben, das Web anonym zu benutzen. Das betrifft auch das Herunterladen öffentlich zugänglicher Informationen. Personenbezogene Informationen sollten in diesem Fall nur für den Zeitraum verarbeitet werden, in dem der Nutzer die Website liest, mit Ausnahme der Verbindungsdaten, so weit diese für Sicherheitszwecke erforderlich sind.

3. Bevor personenbezogene Daten, insbesondere solche, die durch den Benutzer offenbart wurden, durch den Anbieter einer Website verarbeitet werden, ist eine informierte Einwilligung des Benutzers erforderlich. Darüber hinaus sollten einige unabdingbare Grundregeln in die Standardkonfiguration der technischen Plattform eingebaut werden. Personenbezogene Daten dürfen nicht in einem automatischen Verfahren zu einer Website ohne vorherige Information des Betroffenen übertragen werden, der stets die Möglichkeit haben sollte, die Übertragung zu verhindern.

4. Die Implementierung des P3P-Projekts wird von entscheidender Bedeutung sein und sollte genau beobachtet werden.

Rede
des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht, Dr. Alexander Dix, vor dem Landtag Brandenburg am 28. Januar 1999

Herr Präsident,
sehr geehrte Damen und Herren,

Sie beraten heute über den 6. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz, der unter der Federführung meines Vorgängers im Amt, Herrn Dr. Bleyl, entstanden ist. Dies ist zunächst für mich Anlass, daran zu erinnern, dass Herr Dr. Bleyl sich in seiner sechsjährigen Amtszeit als erster Landesbeauftragter für den Datenschutz in Brandenburg große Verdienste um den Aufbau des Datenschutzes in unserem Land erworben hat. Dafür gebührt ihm unser aller Dank.

Zugleich möchte ich den Blick aber nach vorn richten und einige Anmerkungen zur Entwicklung des Datenschutzes und des Informationszugangs in Brandenburg machen.

Der Landtag hat am 21. Dezember des vergangenen Jahres ein novelliertes Datenschutzgesetz beschlossen, das man als eines der modernsten in der Bundesrepublik Deutschland bezeichnen kann. Ich will nicht versäumen, in diesem Zusammenhang vor allem den Mitgliedern des Innenausschusses für die konstruktive Zusammenarbeit bei der Beratung des Gesetzentwurfes zu danken, auch wenn Sie nicht alle meine Empfehlungen berücksichtigt haben.

Das neue Brandenburgische Datenschutzgesetz enthält neben dem Grundsatz der Datensparsamkeit und dem Datenschutzaudit noch eine weitere wichtige Weichenstellung: Die Verarbeitung besonders sensibler Datenarten ist nur auf Grund einer speziellen Rechtsvorschrift zulässig, die angemessene Garantien zum Schutz des Rechts auf informationelle Selbstbestimmung vorsieht. Zu diesen besonders schutzwürdigen Daten gehören patientenbezogene Informationen. Natürlich muss sich auch die moderne medizinische Versorgung der Datenverarbeitungstechnik, z. B. bei der Telemedizin, bedienen. Dabei müssen aber die ärztliche Schweigepflicht und das Patientengeheimnis als Grundlage eines vertrauensvollen Arzt-Patienten-Verhältnisses gewahrt bleiben.

Soweit sich etwa Arzt-Praxen eines Praxis-Netzes bedienen, entsteht eine Lücke im Schutz vor Beschlagnahme von Patientenunterlagen, weil diese sich nicht mehr im Besitz eines bestimmten Arztes befinden. Diese Lücke kann nur der Bundesgesetzgeber schließen, aber auch der Landesgesetzgeber und die Landesregierung müssen im Gesundheitsbereich noch für angemessene Schutzvorkehrungen sorgen. Dies könnte durch eine Überarbeitung der bereits vorhandenen Regelungen etwa im Gesundheitsdienstgesetz und in der Krankenhausdatenschutzverordnung, am zweckmäßigsten aber durch ein einheitliches Gesetz zum Datenschutz im Gesundheitswesen geschehen. Für die Erarbeitung entsprechender Regelungen habe ich unsere Unterstützung und Beratung angeboten.

Sobald der Bundesgesetzgeber die überfällige Novellierung des Bundesdatenschutzgesetzes abgeschlossen hat, womit dem Vernehmen nach noch in diesem Jahr zu rechnen ist, sollten in Brandenburg die Voraussetzungen für eine unabhängige, einheitliche Datenschutzkontrolle im öffentlichen und im privaten Bereich geschaffen werden. Es geht mir nicht darum, die bisherige Arbeit der Aufsichtsbehörde für den Datenschutz im nicht-öffentlichen Bereich, also des Ministeriums des Innern, fachlich zu kritisieren; dazu besteht auch kein Anlass. Ich halte es aber

im Interesse einer bürgernahen, schlanken Verwaltung für notwendig, die gegenwärtige Kompetenzaufteilung zu beseitigen und den Landesbeauftragten für den Datenschutz zur einheitlichen Beratungs- und Kontrollinstanz, zu einem Kompetenz-Zentrum in Sachen Datenschutz im öffentlichen und privaten Bereich zu machen.

Ich hoffe außerdem, dass es noch in dieser Legislaturperiode gelingt, mit der Verabschiedung eines Sicherheitsüberprüfungsgesetzes ein weiteres Regelungsdefizit in einem besonders sensiblen Bereich zu beheben. Zumindest sollte es möglich sein, Einigung über die Grundzüge eines Gesetzentwurfs zu erreichen.

Neben der Gesetzgebung gewinnt die datenschutzgerechte Gestaltung der technischen Infrastruktur in der Landes- und Kommunalverwaltung immer mehr an Bedeutung. Insbesondere sollte die Entwicklung von Sicherheitskonzepten für das gesamte Landesverwaltungsnetz zügig vorangebracht und abgeschlossen werden.

Meine Damen und Herren, mit der Wahl zum Landesbeauftragten für den Datenschutz haben Sie mir zugleich die Aufgabe des Landesbeauftragten für das Recht auf Akteneinsicht übertragen. In den ersten neun Monaten der Geltung des Akteneinsichts- und Informationszugangsgesetzes haben die Menschen in Brandenburg - entgegen manchen Befürchtungen - nur in verhältnismäßig wenigen Fällen von ihrem neuen Recht Gebrauch gemacht oder sich zumindest nur in wenigen Fällen über eine Verweigerung des Informationszugangs bei uns beschwert.

Überraschend ist dies allerdings nicht: Das allgemeine Recht auf Akteneinsicht bedeutet eine ähnlich einschneidende Neuerung wie das Recht auf Datenschutz, das in den alten Bundesländern schon seit zwanzig, in Hessen seit fast dreißig Jahren gilt. Auch der Datenschutz ist erst in einem jahrzehntelangen Zeitraum realisiert worden. Die Erfahrungen in Ländern mit einer Tradition der Informationsfreiheit wie den USA und Kanada zeigen, dass die Eröffnung von Zugangsmöglichkeiten der Bürgerinnen und Bürger zu Informationsquellen der öffentlichen Verwaltung ein längerer Prozess ist.

Ein Teil der Behörden in Brandenburg auf Landes- und Kommunalebene hat sich entweder selbstständig oder mit Hilfe unserer Beratung sehr intensiv auf die Umsetzung des Akteneinsichts- und Informationszugangsgesetzes vorbereitet. Es gibt sicherlich auch Verwaltungen, die sich noch nicht von einer gewissen "Wagenburg-Mentalität" verabschiedet haben.

Das Recht auf Informationszugang schafft für die Menschen in Brandenburg eine wesentliche Voraussetzung zur politischen Mitgestaltung. Ich bin deshalb überzeugt davon, dass größere Transparenz der Verwaltung und erweiterte Mitgestaltungsmöglichkeiten zu einer stärkeren Identifikation der Bürgerinnen und Bürger mit Brandenburg beitragen werden.

Herzlichen Dank für Ihre Aufmerksamkeit.

Auszug aus dem Geschäftsverteilungsplan des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Stand: 31. Dezember 1998

Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht	Dr. Alexander Dix
Stellvertreter	Kurt Urban
Sekretariat	Christine Objartel App. 10

Bereich Recht

Bereichsleiter	Dr. Alexander Dix
Arbeitsgebiete: - Rechtliche Grundsatzfragen - Landtag, Staatskanzlei - Internationales Datenschutz- und Informationszugangsrecht	
Koordinatorin der Aufgaben im Bereich Recht	Marie-Luise Franzen App. 20
Arbeitsgebiete: - Finanzen - Justiz (außer Staatsanwaltschaften) - Landesrechnungshof - Inneres (insbes. Verfassung, Kommunalrecht) - Steuer- und Finanzdaten allgemein	
Arbeitsgebiete: - Inneres (insbes. Melderecht, Personenstandsrecht, Einbürgerung, Wahlen) - Personaldaten allgemein	Manfred Groß App. 40
Arbeitsgebiete: - Arbeit, Soziales, Gesundheit, Frauen - Sozial- und Gesundheitsdaten allgemein	Marion Bultmann App. 44

Arbeitsgebiete: - Inneres (insbes. Polizei, Verfassungsschutz, Verkehrsordnungswidrigkeiten, Ausländer, Asylverfahren) - Staatsanwaltschaften - Presse- und Öffentlichkeitsarbeit	Lena Schraut App. 41
Arbeitsgebiete: - Bildung, Jugend, Sport - Wissenschaft, Forschung, Kultur	Gabriele Peschenz App. 22
Arbeitsgebiete: - Ernährung, Landwirtschaft, Forsten - Umwelt, Naturschutz, Raumordnung - Wirtschaft, Mittelstand, Technologie - Stadtentwicklung, Wohnen, Verkehr	Susann Burghardt App. 45
Arbeitsgebiete - Bibliothek - Literaturbeschaffung - Schreibdienst - Informationsmaterialien	Christel Kern App. 43

Bereich Technik

Bereichsleiter Arbeitsgebiete: - Technisch/organisatorische Grundsatzfragen - Landesverwaltungsnetz - komplexe IT-Verfahren	Kurt Urban App. 30
Arbeitsgebiete: - Großrechner - Datenbanksysteme - kryptographische Verfahren - Organisations-/ Dienstanweisungen - Statistik	Ulrich Wiener App. 31
Arbeitsgebiete: - UNIX-Systeme - Sicherheitsprodukte - Kartentechnologien - Kommunikationsnetze - Medien und Telekommunikation	Veikko Müller App. 32

Arbeitsgebiete: - Systemverwalter - Gebäudesicherung - Datenträgerentsorgung - Isolierte und vernetzte PC	Udo Thiele App. 33
Arbeitsgebiete: - Teilaufgaben der autom. Vorgangsverwaltung - Mailboxkommunikation - Schreibdienst - Informationsmaterialien	Gabriela Berndt App. 12

Verwaltung

Verwaltungsleiter Arbeitsgebiete: - Personal- und Verwaltungsangelegenheiten des LDA - Redaktion von Veröffentlichungen - Beauftragter des Haushalts	Manfred Groß App. 40
Arbeitsgebiete: - Büroleitungsaufgaben - Haushaltsangelegenheiten - Beschaffungen allgemein	Ursel Leunig App. 42

Gleichstellungsbeauftragte	Frau Kern App. 43
Personalrat	Herr Wiener App. 31

Aktenplan des Landesbeauftragten für den Datenschutz und für das Recht auf Akteneinsicht (LDA)

Problemkreis	Bezeichnung
002	Akteneinsichts- und Informationszugangsgesetz
003	Arbeit
008	Ausländer
009	Bau-/Wohnungswesen
010	Landesregierung
024	Landtag/Parteien
027	Bildung/Kultur/Wissenschaft
028	BRD/Bund/Bundesländer
034	Allgemeines Datenschutzrecht
046	Zusammenarbeit Bundesbeauftragter für den Datenschutz/Landesbeauftragte für den Datenschutz
054	Dateienregister LDA
056	Internationale Datenschutzangelegenheiten
061	Finanzen
062	Ernährung/Landwirtschaft/Forsten
066	Gesundheitswesen
078	Familie/Frauen/Jugend
082	Justiz
086	Kommunalrecht
089	Interne Verwaltung LDA
100	Öffentlichkeitsarbeit LDA
104	Inneres
108	Personaldatenverarbeitung
110	Polizei
128	Sozialwesen
132	Statistik
135	Technik
136	Medien/Telekommunikation/Post
138	Umwelt/Raumordnung/Stadtentwicklung
146	Verfassungsschutz
147	Verkehr
154	Wirtschaft/Technologie
163	Nicht-öffentlicher Datenschutz

180	Personalräte
999	Sonstiges

Abkürzungsverzeichnis

a. F.	=	alte Fassung
ABl.	=	Amtsblatt
Abs.	=	Absatz
AFIS	=	Automatisiertes Fingerabdruck-Identifizierungssystem
AIG	=	Akteneinsichts- und Informationszugangsgesetz
Anl.	=	Anlage
AuslG	=	Gesetz über die Einreise und den Aufenthalt von Ausländern im Bundesgebiet
BAföG	=	Bundesausbildungsförderungsgesetz
BBG	=	Bundesbeamtengesetz
Bbg.	=	Brandenburgisch(es)
BbgDSG	=	Brandenburgisches Datenschutzgesetz
BbgGDG	=	Brandenburgisches Gesundheitsdienstgesetz
BbgMeldeG	=	Brandenburgisches Meldegesetz
BbgPolG	=	Brandenburgisches Polizeigesetz
BbgStatG	=	Brandenburgisches Statistikgesetz
BbgVerfSchG	=	Brandenburgisches Verfassungsschutzgesetz
BCG-Impfung	=	Bazillus Calmette-Guérin-Impfung
BDSG	=	Bundesdatenschutzgesetz
BGBl.	=	Bundesgesetzblatt
BIS	=	Brandenburger InformationsStrategie
BR-Drs.	=	Bundesrats-Drucksache
BStatG	=	Bundesstatistikgesetz
BT-Drs.	=	Bundestags-Drucksache
BVerfGE	=	Bundesverfassungsgerichtsentscheidung
bzgl.	=	bezüglich
bzw.	=	beziehungsweise
ca.	=	circa
CD-ROM	=	Compact Disc - Read Only Memory
c't	=	ct magazin für computertechnik
DAE	=	Deutsche Arbeitsgemeinschaft für Epidemiologie
DAV	=	Verwaltungsvorschrift über die Errichtung und Benutzung dienstlicher Telekommunikationsanlagen für die Verwaltung des Landes Brandenburg
DDR	=	Deutsche Demokratische Republik
d. h.	=	das heißt
DJT	=	Deutscher Juristentag
DNA	=	desoxyribonucleic acid (deutsch: Desoxyribonucleinsäure)
DSV	=	Datenschutzverordnung Schulwesen
DuD	=	Datenschutz und Datensicherheit
EDV	=	Elektronische Datenverarbeitung
EG	=	Europäische Gemeinschaft

ELBOS	=	Einsatzleitsystem für die brandenburgische Polizei
etc.	=	et cetera
EU	=	Europäische Union
EuGH	=	Europäischer Gerichtshof
e. V.	=	eingetragener Verein
evtl.	=	eventuell
FAZ	=	Frankfurter Allgemeine Zeitung
ff.	=	folgende
FITUG	=	Förderverein Informationstechnik und Gesellschaft
GBO	=	Grundbuchordnung
geänd.	=	geändert
gem.	=	gemäß
GG	=	Grundgesetz
ggf.	=	gegebenenfalls
GmbH	=	Gesellschaft mit beschränkter Haftung
GO	=	Gemeindeordnung
GVBl.	=	Gesetz- und Verordnungsblatt
G 10-Gesetz	=	Gesetz zu Artikel 10 Grundgesetz
G 10 AG Bbg	=	Gesetz zur Ausführung des Gesetzes zu Art. 10 Grundgesetz im Land Brandenburg
HandwO	=	Handwerksordnung
HKR	=	Haushalt-, Kassen-, Rechnungswesen
i. d. Fass.	=	in der Fassung
IMA-IT	=	Interministerieller Ausschuss für Informationstechnik
i. S. d.	=	im Sinne des
i. S. v.	=	im Sinne von
IuK	=	Informations- und Kommunikationstechnik
i. V. m.	=	in Verbindung mit
IuK-Technik	=	Informations- und Telekommunikationstechnik
KAN-BB	=	Kriminalaktennachweis Land Brandenburg
KEV	=	komplexe Ermittlungsverfahren
KHDsV	=	Verordnung zum Schutz von Patientendaten im Krankenhaus
Kita-Gesetz	=	Zweites Gesetz zur Ausführung des Achten Buches des Sozialgesetzbuches - Kinder- und Jugendhilfe - Kindertagesstättengesetz
KOM	=	Dokument der Europäischen Kommission
KPMD	=	kriminalpolizeiliches Meldesystem
KRG	=	Krebsregistergesetz
LBG	=	Landesbeamtengesetz
LDA	=	Landesbeauftragter für den Datenschutz und für das Recht auf Akteneinsicht
LDS	=	Landesamt für Datenverarbeitung und Statistik
lit.	=	litera
LKA	=	Landeskriminalamt
LT-Drs.	=	Landtags-Drucksache
LVN	=	Landesverwaltungsnetz

MBJS	=	Ministerium für Bildung, Jugend und Sport
MDK	=	Medizinischen Dienst der Krankenkassen
MOD	=	Magnetic Optical Disk
n. F.	=	neue Fassung
NJW	=	Neue Juristische Wochenschrift
Nr.	=	Nummer
o. ä.	=	oder ähnliches
o. Ä.	=	oder Ähnliches
o. g.	=	oben genannte
ORB	=	Ostdeutscher Rundfunk Brandenburg
PASS	=	Polizeiliches Auskunftssystem-Straftaten
PC	=	Personalcomputer
PGP	=	Pretty Good Privacy
PKK	=	Parlamentarische Kontrollkommission
PKS	=	polizeiliche Kriminalstatistik
POLIKS	=	Polizei Information Kommunikation Sachbearbeitung
S.	=	Seite
s.	=	siehe
SGB	=	Sozialgesetzbuch
SGB I	=	Erstes Buch Sozialgesetzbuch
SGB X	=	Zehntes Buch Sozialgesetzbuch
sog.	=	sogenannt
SopV	=	Verordnung über Unterricht und Erziehung für junge Menschen mit sonderpädagogischem Förderbedarf
StGB	=	Strafgesetzbuch
StPO	=	Strafprozessordnung
StVÄG	=	Strafverfolgungs-Änderungsgesetz
TB	=	Tätigkeitsbericht
TK	=	Telekommunikation
TÜ-Maßnahmen	=	Telefonüberwachungsmaßnahmen
u. a.	=	unter anderem
u. ä	=	und ähnliches
u. Ä.	=	und Ähnliches
UN	=	United Nations
UNESCO	=	United Nations Educational, Scientific and Cultural Organization
usw.	=	und so weiter
u. U.	=	unter Umständen
VfGBbg	=	Verfassungsgericht des Landes Brandenburg
VG	=	Verwaltungsgericht
vgl.	=	vergleiche
VwVfG	=	Verwaltungsverfahrensgesetz
VwVfGBbg	=	Verwaltungsverfahrensgesetz des Landes Brandenburg
WoGG	=	Wohngeldgesetz
WWW	=	World Wide Web
z. B.	=	zum Beispiel

ZRP	=	Zeitschrift für Rechtspolitik
z. T.	=	zum Teil
ZTB	=	Zentraldienst der Polizei für Technik und Beschaffung

Stichwortverzeichnis

Angegeben sind nur Fundstellen des Tätigkeitsberichts 1998. Auf diese Weise soll die Lesbarkeit des Stichwortverzeichnisses und die Erschließung des Tätigkeitsberichts verbessert werden. Ein vollständiges Stichwortverzeichnis aller Tätigkeitsberichte seit 1992 (1. - 6. TB) ist im 6. Tätigkeitsbericht des Landesbeauftragten für den Datenschutz abgedruckt, der bei uns angefordert oder im Internet unter http://www.lda.brandenburg.de abgerufen werden kann.